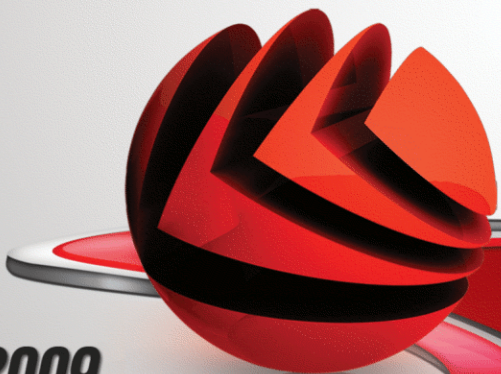


bitdefender



ANTIVIRUS₂₀₀₉

사용자 설명서



BitDefender Antivirus 2009

사용자 설명서

퍼냄 2009.02.03

저작권 2009 BitDefender

법적 고지

저작권 소유. 본 문서의 어느 부분도 BitDefender의 인가된 대표로부터의 서면허가 없이는 사진촬영, 기록 혹은 정보저장 및 검색시스템을 포함한 전자 혹은 기계적 수단이나 형태로 재생 혹은 전송될 수 없습니다. 검토 시 짧은 인용을 포함하는 것은 가능하지만 인용출처를 언급해야 합니다. 내용물은 어떤 식으로든 수정할 수 없습니다.

경고 및 거부. 본 제품과 관련 문서는 저작권법에 의해 보호됩니다. 이 문서에 포함되어 있는 정보는 “있는 그대로” 제공되며, 이에 관한 보증이 제공되지 않습니다. 본 문서를 준비함에 있어 모든 주의가 이루어졌으나, 저자들은 본 문서에 포함되어 있는 정보에 의해 직접 혹은 간접적으로 야기될 수 있는 모든 손실 및 손상에 관하여 어떠한 대인 및 조직에도 책임을 지지 아니합니다.

이 문서는 SOFTWIN과 무관한 제 3의 웹사이트에 대한 링크를 포함하고 있으며 SOFTWIN은 링크 사이트의 콘텐츠에 책임지지 않습니다. 고객이 이 문서에서 언급된 제 3의 웹사이트를 이용했을 때에는 고객이 스스로 위험 요소에 대처하셔야 합니다. SOFTWIN 은 고객의 편의를 위해 링크만을 제공하며 링크에 포함된 내용에 대해서는 책임지지 않습니다.

등록상표들. 등록상표명은 이 문서에 표기되어 있습니다.이 문서 내에 있는 등록된 혹은 등록되지 않은 등록상표 모두는 각 등록상표 소유주의 고유 재산입니다.



BitDefender Antivirus 2009





차례

최종 사용자 소프트웨어 라이선스 계약서	ix
서문	xiii
1. 이 문서에 사용된 기호들	xiii
1.1. 기호 표기들	xiii
1.2. 경고 사항	xiv
2. 문서 구조	xiv
3. 논평 요청	xv
설치	1
1. 시스템 요건들	2
1.1. 하드웨어 요건들	2
1.2. 소프트웨어 요건들	3
2. 비트펜더 설치하기	4
2.1. 등록마법사	6
2.1.1. 1/2 단계 - 비트펜더 바이러스차단 2009 등록하기	7
2.1.2. 단계 2/2 - 비트펜더 계정 만들기	8
2.2. 설정마법사	10
2.2.1. 1/8 단계 - 환영 창	11
2.2.2. 2/8 단계 - 보기모드 선택	12
2.2.3. 단계 3/8 - 비트펜더 네트워크 설정하기	13
2.2.4. 단계 4/8 - 신분제어 설정하기	14
2.2.5. 5/8 단계 - 바이러스 보고서 설정하기	18
2.2.6. 6/8 단계 - 실행될 작업들을 선택하십시오.	19
2.2.7. 단계 7/8 - 작업들이 완료되도록 기다리기	20
2.2.8. 8/8 단계 - 마침	21
3. 업그레이드	22
4. 비트펜더 수리 혹은 제거	23
기본 관리	25
5. 시작하기	26
5.1. 비트펜더 바이러스차단 2009 시작하기	26
5.2. 사용자 인터페이스 보기 모드	26
5.2.1. 기본 보기	26
5.2.2. 상세 보기	28
5.3. 알림영역 내의 비트펜더 아이콘	31



5.4. 검사활동 막대	32
5.5. 비트펜더 수동검사	32
5.6. 게임모드	33
5.6.1. 게임모드 사용하기	33
5.6.2. 게임모드 단축키 바꾸기	34
5.7. 웹브라우저로의 통합	34
5.8. 메신저로의 통합	36
6. 계기반	38
6.1. 개요	88
6.2. 작업들	40
6.2.1. 비트펜더를 사용해 검사하기	40
6.2.2. 비트펜더 업데이트하기	41
7. 바이러스차단	43
7.1. 감시되는 구성요소들	43
7.1.1. 지역보안	78
7.2. 작업들	45
7.2.1. 비트펜더를 사용해 검사하기	45
7.2.2. 비트펜더 업데이트하기	46
8. 개인정보불법수집차단	49
8.1. 감시되는 구성요소들	50
8.1.1. 온라인 보안	79
8.2. 작업들	51
8.2.1. 비트펜더를 사용해 검사하기	51
8.2.2. 비트펜더 업데이트하기	52
9. 취약성	55
9.1. 감시되는 구성요소들	55
9.1.1. 취약성 검사	80
9.2. 작업들	57
9.2.1. 취약성들 검색하기	57
10. 네트워크	65
10.1. 작업들	66
10.1.1. 비트펜더 네트워크에 동참하기	66
10.1.2. 비트펜더 네트워크에 컴퓨터들을 추가하기	67
10.1.3. 비트펜더 네트워크 관리하기	69
10.1.4. 모든 컴퓨터들 검사하기	71
10.1.5. 모든 컴퓨터들 업데이트하기	72
10.1.6. 모든 컴퓨터 등록	73
11. 기본 설정들	75
11.1. 지역보안	76



11.2. 온라인 보안	76
11.3. 일반설정들	76
12. 상태막대	78
12.1. 지역보안	78
12.2. 온라인 보안	79
12.3. 취약성 검사	80
13. 등록	82
13.1. 1/1 단계 - 비트펜더 바이러스차단 2009를 등록합니다.	82
14. 이력	84
상세 관리	86
15. 일반사항	87
15.1. 계기반	87
15.1.1. 통계	88
15.1.2. 개요	88
15.2. 설정들	89
15.2.1. 일반설정들	90
15.2.2. 바이러스 보고서 설정들	91
15.3. 시스템 정보	91
16. 바이러스차단	93
16.1. 실시한 보호	93
16.1.1. 보호수준 설정하기	94
16.1.2. 보호수준 맞추기	95
16.1.3. 거동검사기 설정	99
16.1.4. 실시간 보호 해제하기	101
16.1.5. 개인정보불법수집차단 보호 설정	102
16.2. 주문형 검사	103
16.2.1. 작업들 검사	105
16.2.2. 단축키 메뉴 사용하기	107
16.2.3. 검사작업 생성하기	108
16.2.4. 검사작업들 설정하기	108
16.2.5. 검사객체들	121
16.2.6. 검사로그들 보기	128
16.3. 검사에서 제외된 객체들	130
16.3.1. 검사에서 경로를 제외하기	132
16.3.2. 검사에서 확장자명 제외하기	136
16.4. 검역소 영역	140
16.4.1. 검역된 파일들 관리하기	141
16.4.2. 검역소 설정	142



17. 개인정보보호제어	144
17.1. 개인정보제어상태	144
17.1.1. 보호수준 설정하기	145
17.2. 신분제어	146
17.2.1. 신분규칙들 생성하기	148
17.2.2. 예외 정의	151
17.2.3. 규칙들 관리하기	152
17.3. 레지스트리 컨트롤	153
17.4. Cookie 컨트롤	155
17.4.1. 설정 창	158
17.5. 스크립트 컨트롤	159
17.5.1. 설정 창	162
18. 메신저 암호화	163
18.1. 특정 사용자에게 대한 암호화 해제	165
19. 취약성	166
19.1. 상태	166
19.1.1. 취약점 조치하기	167
19.2. 설정들	174
20. 게임 / 랩탑 모드	176
20.1. 게임모드	176
20.1.1. 자동게임모드 설정	177
20.1.2. 게임목록 관리	178
20.1.3. 게임모드 설정	179
20.1.4. 게임모드 단축키 바꾸기	180
20.2. 랩탑모드	181
20.2.1. 랩탑모드 설정	182
21. 네트워크	183
21.1. 비트펜더 네트워크에 동참하기	184
21.2. 비트펜더 네트워크에 컴퓨터들을 추가하기	184
21.3. 비트펜더 네트워크 관리하기	186
22. 업데이트	189
22.1. 자동 업데이트	189
22.1.1. 업데이트 요청	191
22.1.2. 자동업데이트 해제하기	191
22.2. 업데이트 설정들	192
22.2.1. 업데이트위치 설정	193
22.2.2. 자동업데이트 설정	193
22.2.3. 수동업데이트 설정	194
22.2.4. 고급설정	194



22.2.5. 프록시 관리	194
23. 등록	197
23.1. 비트펜더 바이러스차단 2009 등록하기	198
23.2. 비트펜더 계정 만들기	199
도움말 얻기	203
24. 지원	204
24.1. 비트펜더 지식창고	204
24.2. 도움말 요청	205
24.2.1. 웹 자가서비스로 가기	205
24.2.2. 지원티켓 열기	205
24.3. 연락처 정보	206
24.3.1. 웹주소	206
24.3.2. 지점들	206
응급복구 CD	209
25. 개요	210
25.1. 시스템 요건들	210
25.2. 포함된 소프트웨어	211
26. 비트펜더 응급복구 CD 사용법	214
26.1. 비트펜더 응급복구 CD 시작하기	214
26.2. 비트펜더 응급복구 CD첨하기	215
26.3. 어떻게 바이러스를 검사하나요?	216
26.4. 인터넷 연결은 어떻게 설정할 것인가?	217
26.5. 어떻게 비트펜더를 업데이트하나요?	218
26.5.1. 어떻게 프록시를 통해 비트펜더를 업데이트할 수 있나요?	219
26.6. 어떻게 내 데이터를 저장하나요?	220
용어집	223



최종 사용자 소프트웨어 라이선스 계약서

본 거래협정조건들에 동의하지 않는 경우, 이 소프트웨어를 설치하지 마십시오. "수락", "OK", "계속", "예"를 선택하거나 어떤 식으로든 이 소프트웨어를 설치 혹은 사용하면, 여러분은 본 계약의 조건들을 이해하고 받아들이는 것으로 인정됩니다.

제품 등록. 이 계약서에 동의함으로써, 사용자는 "내 계정"에 대한 사용, 소프트웨어 업데이트 사용조건과 유지보수에 대하여 동의합니다. 이는 소프트웨어 운영과 컴퓨터에 대한 라이선스 유효화와 유지보수 권한에 대한 유효화를 제어합니다. 등록을 위해서는 유효한 일련번호와 이메일 주소의 입력이 필요합니다.

이 조건은 구입된 라이선스 키 혹은 관련 서비스 동의에 따라 사용자에게 배송된 관련 문서 및 업데이트를 포함한, 사용자 라이선스 권한의 가정용, 개인용, BitDefender 솔루션과 소프트웨어 업데이트에 관한 것입니다.

이 사용면허 동의서는 SOFTWIN 소프트웨어 제품 사용을 위해 고객(개인이나 독립 유저)과 SOFTWIN의 합법적인 동의서이며 이는 컴퓨터 소프트웨어, 관련 미디어, 출력물, 온라인이나 전자 문서에 관한 정보를 포함합니다. 앞서 얘기한 모든 정보는 미국/국제 저작권법과 국제 보호 조약에 의해 보호됩니다. BitDefender의 설치, 복사, 그 외의 사용을 통하여 고객께서는 이 동의서 내용에 동의하셨습니다.

본 계약 조건들에 동의하지 않으시는 경우, 비트디펜더를 설치 혹은 사용하지 마십시오.

BitDefender 라이선스. 고객이 이 동의서에 동의하지 않으신다면 BitDefender를 설치 혹은 사용하지 마십시오. 그러나 구매 30일 내의 반품은 가능하며 구매 조퇴가 요구됩니다. 비트디펜더는 지적 재산권법과 협약 뿐만 아니라 저작권법과 국제 저작권 조약에 의해 보호됩니다. BitDefender는 사용면허되며 판매되지 않습니다.

사용면허부여. BitDefender는 이에 오직 여러분에게만 비트디펜더를 사용할 수 있는 비-독점적, 제한적, 비-양도성 및 로열티가 있는 사용면허를 부여합니다.

응용소프트웨어. 여러분은 사용면허된 사용자 전체 수 범위 내에서 필요한 수만큼의 컴퓨터에 BitDefender를 설치 및 사용할 수 있습니다. 여러분은 백업목적으로 하나의 추가 복사본을 만들 수 있습니다.

데스크탑 사용자 면허. 본 면허는 한 대의 컴퓨터에 설치할 수 있고 네트워크 서비스를 제공하지 않는 BitDefender 소프트웨어에 적용됩니다. 각 주 사용자는 이 소



소프트웨어를 한 대의 컴퓨터에 설치할 수 있으며 다른 장치에 하나의 추가 복사본을 만들 수 있습니다. 허가된 주 사용자의 수는 면허된 사용자 수입니다.

사용면허 조건들. 본 문서를 통해 부여된 사용면허는 BitDefender 구입일에 시작하며 사용면허가 구입된 기간 끝에 만료합니다.

만기. 면허만기 도래 즉시 제품은 기능 작동이 멈출 것입니다.

업그레이드. 만약 BitDefender가 업그레이드판으로 라벨 부착된 경우, 여러분은 BitDefender를 사용하기 위해 BitDefender로부터 업그레이드판에 대한 자격이 있는 것으로 인정된 제품을 사용하기에 적합한 면허를 취득해야 합니다. 업그레이드판으로 라벨이 붙은 BitDefender는 그 업그레이드에 대한 여러분의 자격의 기초를 이루는 제품을 대체 및/혹은 보완합니다. 여러분은 본 사용면허계약서의 조건들에 따라서면 업그레이드된 제품을 사용할 수 있습니다. 만약 BitDefender가 여러분이 하나의 제품에 대해 사용면허된 소프트웨어 프로그램들의 한 패키지 중 어느 구성요소에 대한 업그레이드판일 경우, BitDefender는 그 하나의 제품패키지의 일부로서만 사용 및 전송될 수 있으며 면허된 사용자 전체수보다 더 많은 사용에 대해 분리될 수 없습니다. 본 사용면허의 거래협정조건들은 원래의 제품 혹은 결과적으로 업그레이드된 제품에 관하여 여러분과 BitDefender 간에 존재했을 수 있는 모든 이전의 계약들을 대체 및 그에 우선합니다.

저작권. BitDefender에 관한 모든 권리, 소유권 및 이익과 BitDefender(BitDefender 제품에 포함된 모든 이미지, 사진, 로고, 만화동영상, 동영상, 소리, 음악, 텍스트 및 "애플릿들"을 포함하지만 이에 제한되지는 않는)와, 그에 수반되는 인쇄물들 및 비트디펜더의 모든 사본들에 대한 모든 저작권은 비트디펜더 회사의 소유입니다. 비트디펜더는 저작권법 및 국제협약 규정들의 보호를 받습니다. 따라서, 여러분은 비트디펜더 제품을 다른 모든 저작권이 있는 자료와 같이 취급해야 합니다. 여러분은 비트디펜더에 수반되는 인쇄물들을 복사할 수 없습니다. 여러분은 매체와 상관없이 생성된 모든 사본들의 원래의 형태로 혹은 비트디펜더 제품이 존재하는 형태로 모든 저작권 공지를 제시 및 포함해야 합니다. 여러분은 비트디펜더 제품 사용면허를 재분배, 대여, 판매 혹은 공유할 수 없습니다. 여러분은 비트디펜더 제품의 소스코드에 대한 기술적 재가공, 재편집, 분해, 유도결과물 생성, 수정, 변경, 혹은 분석시도할 수 없습니다.

제한적 보증. BitDefender 회사는 BitDefender 제품이 배포되는 매체에는 BitDefender 제품이 여러분에게 배송된 날로부터 삼십일동안 결함이 없을 것임을 보증합니다. 이 보증이 위반되는 경우 BitDefender회사는, 자체적 선택에 따라, 손상된 매체 수령 시 결함이 있는 매체를 교체해 주거나 여러분의 BitDefender 제품 구입비용을 환불할 수 있습니다. 비트디펜더 회사는 BitDefender 제품이 작동중단 혹은 오류가 없다가나 오류가 교정될 것이라는 보증을 하지 않습니다. BitDefender 회사는 BitDefender 제품이 여러분의 요건을 충족한다는 보증을 하지 않습니다.



본 계약서에 명시적으로 제시된 경우 외에는, BitDefender는 제품, 향상, 유지관리 혹은 지원, 혹은 어떤 다른 자료들(유무형의)이나 서비스들과 관련된 명시적 혹은 암시적인 모든 다른 보증을 거부합니다. 이에 BitDefender는 특정목적을 위한 상업성 및 적합성, 권리, 비간섭, 데이터의 정확성, 정보내용의 정확성, 시스템 통합 및 제3자 권리 불침해에 대한 암시된 보증들을 포함하지만 이에 제한되지는 않는 모든 암시적 보증 및 조건들을 명시적으로 거부합니다.

책임 한계. BitDefender를 사용하고 테스트하고 평가하는 누구라도 비트디펜더의 품질과 성능에 따른 위험 요소를 갖게 됩니다. BITDEFENDER는 어떠한 경우에도 제한 없이 사용함에 있어 발생하는 직접적이거나 간접적인 피해와 같은 어떤 종류의 피해에 대해서도 책임을 지지 않습니다. 가능한 위험에 대해서는 알려드린 바와 같습니다.

허용되지 않은 환경 또는 예외상황에서 사용으로 인하여 발생하는 피해에 대해서 BITDEFENDER는 어떠한 배상 또는 책임의 의무를 지지않습니다.

어떠한 경우에도 BITDEFENDER는 소비자가 구매 또는 사용을 위해 지불한 금액을 초과하는 금액에 대해서는 배상책임을 지지않습니다.

사용자들에 대한 중요한 공지. 이 소프트웨어는 과오-관용적이지 못하며 고장안전수행 혹은 작업을 요하는 어떤 위험한 환경에서의 사용을 위해 설계 혹은 의도되지 않았습니다. 이 소프트웨어는 항공기 운항, 원자력시설 혹은 통시체계, 무기체계, 직간접 생명지원체계, 항공관제, 혹은 고장으로 사망, 심각한 신체상해 혹은 재산피해를 초래할 수 있는 어떤 작업이나 설치에서의 사용에 대해 의도되지 않았습니다.

전자 통신에 대한 내용. BitDefender는 사용자에게 법적 고지 또는 소프트웨어, 유지보수 가입 및 정보사용에 대한 통지를 발송할 수 있습니다. BitDefender는 사용자가 제품사용에 있어서 제출한 이메일을 통하여 정보를 제공할 수 있습니다. 이 계약서에 동의함으로써 사용자는 모든 통신에 대한 수신을 허가함을 의미합니다.

일반사항. 본 계약은 로마니아 법률들 및 국제저작권법들 및 협정들의 지배를 받을 것입니다. 본 면허조건들로 인해 일어나는 모든 분쟁을 재판하는 독점적 관할은 로마니아 법원입니다.

비트디펜더 사용 가격, 비용 및 수수료들은 여러분에게 대한 사전 통지없이 변경될 수 있습니다.

본 계약의 어떤 조항이 무효가 되는 경우, 그 무효는 본 계약의 나머지 부분의 유효성에는 영향을 미치지 않습니다.

비트디펜더 및 비트디펜더 로고들은 비트디펜더의 등록상표입니다. 제품 혹은 관련 자료들에 사용된 모든 다른 등록상표들은 각각 소유자들의 재산입니다.



여러분이 거래협정조건들의 일부를 위반하는 경우 면허는 통지없이 즉시 파기됩니다. 여러분은 파기의 결과로 비트펜더 혹은 비트펜더의 재판매자들로부터 환불 받을 권리가 주어지지 않습니다. 사용에 관한 기밀 및 제한사항들에 관한 거래협정조건들은 파기 후에도 유효성을 유지합니다.

비트펜더는 언제든지 이 조건들을 수정할 수 있으며, 수정된 조건들은 수정된 조건들에 따라 배포된 소프트웨어의 해당 버전들에 자동으로 적용됩니다. 만약 이 조건들의 어떤 일부가 무효이기 때문에 적용될 수 없다고 드러나는 경우, 이 무효성은 조건들의 나머지 부분의 유효성에는 영향을 미치지 않고, 그 부분은 계속 유효하고 적용가능한 부분으로 남습니다.

이 조건들의 다른 언어판들 간에 경합 혹은 일관성결여가 일어나는 경우, 비트펜더가 발행한 영어판이 우선합니다.

BitDefender Korea, 서울시 마포구 상암동 DMC 산학협력연구센터 14층. 전화: 02-380-3377, 팩스: 02-380-3380, e-mail: support@bitdefenderkorea.com.



서문

이 안내서는 비트펜더 바이러스차단 2009를 자신들의 개인용 컴퓨터를 위한 보안 솔루션으로 선택한 모든 사용자들을 위한 것입니다. 이 문서에 제공된 정보는 컴퓨터 능숙자들에게만 적합한 것이 아니라 윈도우즈 환경에서 작업할 수 있는 모든 사람들이 사용할 수 있습니다.

이 문서는 여러분을 위해 비트디펜더 바이러스차단 2009, 이 회사 및 이 제품을 개발한 팀에 대해 설명하고, 여러분을 설치과정을 따라 안내하며, 여러분에게 이 제품을 어떻게 설정하는지를 가르칠 것입니다. 여러분은 비트펜더 바이러스차단 2009 사용방법, 업데이트, 시험 및 맞춤형 설정방법을 알게 될 것입니다. 여러분은 비트펜더를 가장 잘 이용하는 방법을 배울 것입니다.

이 책이 귀하에게 유용하고 즐거운 정보를 제공하기를 바랍니다.

1. 이 문서에 사용된 기호들

1.1. 기호 표기들

이 책에서는 쉽게 읽을 수 있도록 몇 가지의 텍스트 스타일이 사용되었습니다. 각 표현과 의미는 아래의 표와 같습니다.

외양	설명
sample syntax	체계에 대한 예는 등쪽문자로 인쇄되어 있습니다.
http://www.bitdefender.com	URL 링크는 HTTP 혹은 FTP 서버의 외부 위치를 나타냅니다.
support@bitdefender.com	연락처 정보 내에 이메일주소들이 포함되어 있습니다.
“서문” (p. xiii)	이것은 내부 문서의 특정 지점으로 이동하는 링크입니다.
filename	파일과 디렉토리는 등쪽 폰트를 사용하여 인쇄되어 있습니다.



외양	설명
option	모든 제품 옵션은 강조 체로 인쇄되어 있습니다.
sample code listing	코드 리스트는 등쪽 문자로 인쇄되어 있습니다.

1.2. 경고 사항

경고는 텍스트내의 주의 사항으로써, 현재 단락과 관련된 추가 정보에 대한 관심을 불러일으킬 수 있도록 시각화되어 있습니다.



참고

짧은 주목을 요약합니다. 참고는 생략할 수도 있지만, 구체적 특징 혹은 어떤 관련 주제로의 링크 등 값진 정보를 제공하기도 합니다.



중요

이것은 귀하가 주의해야 할 필요가 있으며, 건너뛰지 않도록 하십시오. 일반적으로 여기에서는 결정적이지는 않지만, 중요한 정보를 제공합니다.



주의

이것은 귀하가 주의를 해서 다루어야 할 중요한 정보입니다. 지시 사항을 따르는 것이 좋습니다. 지극히 위험한 사항을 설명하고 있으므로, 반드시 읽어보고 이해하도록 하십시오.

2. 문서 구조

이 책은 주요 주제들을 담은 몇 개의 편으로 이루어져 있습니다. 더욱이, 몇몇 기술용어들을 명확히 하기 위해 용어설명이 제공됩니다.

설치. 비트디펜더를 워크스테이션에 단계별로 설치하기 위한 지침들. 이 지침은 비트디펜더 바이러스차단 2009 설치에 관한 포괄적 설명서입니다. 성공적 설치를 위한 필수과정들로부터 시작해, 여러분은 전체 설치 과정을 통해 안내를 받으실 것입니다. 마지막으로 여러분이 비트디펜더를 삭제해야 할 경우를 대비해 제거절차가 설명됩니다.

기본 관리. 기본 관리 및 비트디펜더의 유지관리에 대한 설명



상세 관리. 비트디펜더에서 보안역량들에 대한 상세자료 제공 여러분은 여러분의 컴퓨터를 바이러스, 맬웨어, 등 모든 종류의 악성위협들로부터 효율적으로 보호하기 위해 모든 비트디펜더 모듈들의설정 및 사용방법을 배웁니다.

도움말 얻기. 예기치 않았던 일이 일어날 때 어디를 보고 어디서 도움말을 얻을 수 있나?

응급복구 CD. 부팅 가능한 CD를 사용하여 응급 복구를 수행하는데 필요한 기능을 설명합니다.

용어집. 본 문서에서 볼 수 있는 용어집에서는 일부 기술적이고 일상적이지 않은 용어들을 설명하고 있습니다.

3. 논평 요청

저희는 귀하께서 이 책자를 더욱 잘 만들 수 있도록 도움을 주시기를 바라고 있습니다. 저희는 최선을 다하여 모든 정보를 테스트 및 확인했습니다. 이 책자와 관련하여 귀하께서 발견한 일부 결함이나 책자 개선을 위해 생각하신 바가 있다면 최고의 문서를 작성할 수 있도록 알려주시면 감사하겠습니다.

documentation@bitdefender.com로 이메일을 보내주십시오.



중요

저희가 효율적으로 처리할 수 있도록 여러분의 모든 문서화 관련 이메일들은 영어로 작성해 주십시오.



BitDefender Antivirus 2009

설치



1. 시스템 요건들

여러분은 오직 다음 운영체제에서 작동하는 컴퓨터에만 비트펜더 바이러스차단 2009를 설치할 수 있습니다.

- 서비스팩 2 (32/64비트)가 있는 윈도우 XP 혹은 그 이상
- 윈도우 비스타 (32/64비트) 혹은 서비스팩 1이 있는 윈도우 비스타
- 윈도우즈 홈 서버

설치 전에, 여러분의 컴퓨터가 최소 하드웨어 및 소프트웨어 요건들을 충족하는지 확인하십시오.



참고

여러분의 컴퓨터가 작동하는 윈도우 운영체제정보를 찾으려면, 바탕화면 상의 My Computer를 오른쪽 클릭한 후 메뉴로부터 Properties를 선택하십시오.

1.1. 하드웨어 요건들

윈도우 XP용

- 800 MH 혹은 그 이상 속도의 CPU
- 256 MB 메인메모리 (1GB 권장)
- 170 MB 여유 하드디스크 공간 (200 MB 권장)

윈도우 비스타 용

- 800 MH 혹은 그 이상 속도의 CPU
- 512 MB 메인메모리 (1GB 권장)
- 170 MB 여유 하드디스크 공간 (200 MB 권장)

윈도우 홈 서버용

- 800 MH 혹은 그 이상 속도의 CPU
- 512 MB 메인메모리 (1GB 권장)
- 170 MB 여유 하드디스크 공간 (200 MB 권장)



1.2. 소프트웨어 요건들

- 인터넷 익스플로러 6.0 (혹은 그 이상)
- .NET 프레임 1.1 (설치키트에도 있음)

다음 목적을 위해 개인정보불법수집 방지보호가 제공됩니다:

- 인터넷 익스플로러 6.0 혹은 그 이상
- 모질라 파이어폭스 2.0
- 야후! 메신저 8.1
- 윈도 라이브 (MSN) 메신저 8.5

메신저 암호화는 다음 경우에만 제공됩니다:

- 야후! 메신저 8.1
- 윈도 라이브 (MSN) 메신저 8.5



2. 비트펜더 설치하기

설치파일을 찾아 더블클릭하십시오. 마법사가 실행되어 여러분을 설치과정 전체에 걸쳐 안내할 것입니다.

셋업 마법사를 시작하기 전에, BitDefender가 설치 패키지의 최신 버전을 확인할 것입니다. 최신 버전을 사용할 수 있다면, 최신 버전을 다운받도록 권장될 것입니다. 최신 버전을 다운 받으려면 예를 클릭하고, 셋업 파일 내에 있는 버전 설치를 계속하려면 아니오를 클릭하십시오.



설치단계들



빗디펜더 바이러스차단 2009를 설치하시려면 이 단계들을 따르십시오.

1. 설치를 계속 진행하려면 다음 버튼을 클릭하시고 설치를 취소하려면 취소 버튼을 클릭하십시오.
2. 다음을 클릭하십시오.

여러분 컴퓨터에 다른 바이러스 방지 제품이 있으면 여러분은 빗디펜더 바이러스차단 2009로부터 경고를 받으실 것입니다. 해당 제품을 삭제하려면 제거하기를 클릭하십시오. 탐지된 제품들을 제거하지 않고 계속하기 원하시면, 다음을 클릭하십시오.



주의

빗디펜더 설치 전에 탐지된 모든 다른 바이러스 방지 제품들을 제거하시도록 강력히 권장됩니다. 대개 한 대의 컴퓨터에 동시에 둘 혹은 그 이상의 바이러스 방지 제품들을 작동하면 시스템을 사용할 수 없게 됩니다.

3. 사용면허동의서를 읽고 동의를 클릭하십시오.



중요

이 조건들에 동의하지 않으실 경우, 취소를 클릭하십시오. 설치절차가 취소되고 설치과정이 중단될 것입니다.

4. 기본적으로, 빗디펜더 바이러스차단 2009는 C:\Program Files\BitDefender\BitDefender 2009에 설치될 것입니다. 설치경로를 변경하려면, 둘러보기를 클릭한 후 빗디펜더를 설치하려는 폴더를 선택하십시오.

다음을 클릭하십시오.

5. 설치과정에 관한 선택사항들을 선택하십시오. 그 중 다음과 같은 일부는 기본적으로 선택될 것입니다:

■ Readme 파일 열기 — 설치 종료 후 readme 파일을 엽니다.

■ 바탕화면에 단축키 만들기 — 설치 마지막에 여러분의 바탕화면에 빗디펜더 바이러스차단 2009에 대한 단축키를 만듭니다.

■ 설치 완료 시 CD빼내기 — 설치 마지막에 CD를 빼냅니다. 이 선택사항은 제품을 CD로 설치할 때에 나타납니다

■ 윈도 디펜더 끄기 — 윈도 디펜더를 끕니다. 이 선택사항은 윈도 비스타에서 만 나타납니다.



제품 설치를 시작하려면 설치를 클릭하십시오. .NET 프레임워크 1.1이 설치되어 있지 않으면, 비트디펜더는 우선 .NET 프레임워크 1.1을 설치할 것입니다.

설치가 완료될 때까지 기다리십시오.

6. 완료를 클릭하십시오. 설치마법사가 설치과정을 완료할 수 있도록 여러분은 시스템을 재시작하도록 요구받을 것입니다. 이 지시는 되도록 빨리 하시기를 권장합니다.



중요

설치 완료 및 컴퓨터 재시작 후, **등록마법사**와 **설치마법사**가 나타날 것입니다. 비트디펜더 바이러스차단 2009를 등록하고 비트디펜더 계정을 만들기 위해 이 마법사들을 완료하십시오.

설치경로에 대한 기본설정들을 받아들였으면, Program Files폴더 내에 BitDefender라는 새 폴더가 보일 것인데, 이 폴더에는 비트디펜더 2009라는 하부폴더가 있습니다.

2.1. 등록마법사

설치 후 여러분 컴퓨터를 처음 시작할 때에, 등록마법사가 나타날 것입니다. 마법사는 여러분이 비트디펜더를 등록하고 비트디펜더 계정을 설정하는 것을 도와줍니다.

BitDefender 업데이트를 받기 위해서는 BitDefender 계정을 생성해야 합니다. BitDefender 계정을 통하여 사용자에게 스페셜 오퍼 또는 무료 기술지원을 제공합니다. 만약 비트디펜더 면허 비밀번호를 잃어버릴 경우, <http://myaccount.bitdefender.com>에서 여러분 계정으로 들어가 다시 찾을 수 있습니다.



참고

이 마법사를 수행하기 원하지 않으실 경우, 취소를 클릭하십시오. 여러분은 사용자 인터페이스 맨 아래에 있는 등록하기를 클릭해서 언제든지 등록마법사를 열 수 있습니다.



2.1.1. 1/2 단계 — 비트펜더 바이러스차단 2009 등록하기

BitDefender Antivirus 2009

BitDefender 등록 마법사 - 단계 1 of 2

단계 1

BitDefender 제품 등록을 하려면 다음의 지시 사항에 따라 주십시오.

현재 사용자 BitDefender 라이선스 키 상태: **시험**

현재 BitDefender 라이선스 키: **704BE277EF7785580DF8**

라이선스 키 잔여일: **30 일**

라이선스 옵션

현재 키를 유지하시려면, 첫 번째 옵션을 선택하시기 바랍니다. 새로운 키를 추가 하시려면, 두 번째 옵션을 선택하고, 하단의 난제 키를 입력하십시오.

☒ 현재 키를 계속 사용합니다.

☐ 제품을 신규 라이선스 키로 등록합니다.

라이선스 키 입력

라이선스 키 구매

라이선스 키를 구입하시려면, 하단의 링크를 클릭하십시오.

BitDefender 라이선스 키 검색

사용자의 라이선스 키:

1) CD-Rom 라벨

2) 제품 등록 카드

3) 온라인 구입 이메일

현재의 라이선스키를 계속 사용하기를 원한다면, 본 옵션을 선택하시기 바랍니다. 이것은 설치 시점에서 귀하의 시스템에서 확인된 예전에 사용된 라이선스 키 혹은 30일 사용 가능 키입니다.

bitdefender

등록 다음 취소합니다

등록

여러분은 비트펜더 등록상태, 현재 면허 비밀번호 및 면허가 만기될 때까지 며칠이 남았는지를 볼 수 있습니다.

제품평가를 계속하기 위해서는, 현재 키 계속사용을 선택하십시오.

비트펜더 바이러스차단 2009를 등록하려면:

1. 새 비밀번호를 사용해 제품을 등록하기 원합니다를 선택하십시오.
2. 편집 필드에 면허번호를 입력하십시오.



참고

여러분의 면허번호를 다음에서 찾을 수 있습니다.

■ CD라벨 위



- 제품등록카드 위
- 온라인 구매 이메일 내

빗디펜더 면허번호가 없으시면, 제시된 링크를 클릭해서 빗디펜더 온라인 매장에서 하나를 구입하십시오.

계속하려면, 다음을 클릭하십시오.

2.1.2. 단계 2/2 — 빗디펜더 계정 만들기

BitDefender Antivirus 2009

BitDefender 등록 마법사 - 단계 2 of 2

단계 1 단계 2

내 계정 등록

사용제품 및 바이러스 엔진, 바이러스 시그니처를 최신의 상태로 유지하기 위해서는 제품을 등록하고 BitDefender 계정을 생성하십시오. 최신 상태 유지를 통하여 사용자 시스템을 안전하게 보호할 수 있습니다. 등록에 대한 자세한 정보는 BitDefender 고객센터센터에 문의하십시오. <http://www.bitdefenderkorea.com>

☐ **현존 BitDefender 계정에서 서명**

이메일 주소:

비밀번호:

비밀번호를 잊어버리셨습니까?

☐ **나중에 등록합니다.**

☒ **새로운 BitDefender 계정 만들기**

이메일 주소:

암호(6-16문자):

암호확인:

이름:

성:

국가:

☒ BitDefender의 모든 소식을 알려주세요.

☐ 가장 중요한 메시지만 전송하십시오.

☐ 아무런 메시지도 보내지 않습니다.

지금 새로운 BitDefender 계정을 생성하고자 한다면 이 옵션을 체크하십시오. 이미 계정이 있으시다면, 기존 계정에 서명하기 옵션을 선택하시기를 강력히 권해 드립니다.

bitdefender

뒤로 마침 취소합니다

계정만들기

지금 빗디펜더 계정을 만들기 원하지 않으시면, 등록건너뛰기를 선택 후, 마치기를 클릭하십시오. 그렇지 않으면, 여러분의 현재 상황에 따라 진행하십시오.

- “저는 빗디펜더 계정이 없습니다.” (p. 9)
- “이미 빗디펜더 계정을 가지고 있습니다.” (p. 10)



중요

BitDefender를 설치한 후 15일 이내에 사용자는 계정을 생성해야 합니다.(등록 시 30일로 연장됩니다.) 그렇지 않으면, BitDefender가 더이상 업데이트되지 않습니다.

저는 비트펜더 계정이 없습니다.

비트펜더 계정을 만들려면, 새 비트펜더 계정 만들기를 선택해서 필요한 정보를 제공하십시오. 여러분이 여기서 제공하시는 데이터는 기밀정보로 유지될 것입니다.

- 이메일 주소 - 사용자 메일주소를 입력하십시오.
- 비밀번호 - 여러분 비트펜더 계정의 비밀번호를 입력하십시오. 비밀번호는 최소 여섯 자리 글자가 되어야 합니다.
- 비밀번호 재입력 - 이전 비밀번호를 다시 입력하십시오.
- 이름 - 여러분의 이름을 입력하십시오.
- 성 - 여러분의 성을 입력하십시오.
- 국가 - 여러분의 거주국가를 선택하십시오.



참고

제공된 이메일 주소와 비밀번호를 사용해 <http://myaccount.bitdefender.com>에서 여러분 계정으로 들어가십시오.

계정을 성공적으로 만들기 위해, 여러분은 우선 여러분의 이메일 주소를 활성화해야 합니다. 여러분의 이메일 주소를 확인하고 비트펜더 등록서비스에서 여러분에게 보낸 이메일의 지침들을 따르십시오.

또한, 비트펜더는 여러분 계정의 이메일 주소를 사용해 여러분에게 특별제안 및 판매행사에 관한 정보를 보낼 수 있습니다. 다음 선택사항들 중 하나를 선택하십시오:

- 비트펜더로부터의 모든 메시지들을 보내주세요
- 가장 중요한 메시지만 보내주세요
- 아무 메시지도 보내지 말아주세요

완료를 클릭하십시오.



이미 비트펜더 계정을 가지고 있습니다.

비트펜더는 여러분 컴퓨터에 여러분이 이전에 등록한 비트펜더 계정이 있는지 자동으로 탐지합니다. 이 경우, 여러분 계정 비밀번호를 알려주십시오.

만약 여러분이 활성화된 계정이 이미 있지만 비트펜더가 그것을 탐지하지 못하는 경우, 기존 비트펜더 계정으로 들어가십시오. 선택한 후 여러분 계정의 이메일 주소와 비밀번호를 입력하십시오.

여러분의 비밀번호를 잊어버리신 경우, 비밀번호 분실을 클릭 후, 지시들을 따르십시오.

또한, 비트펜더는 여러분 계정의 이메일 주소를 사용해 여러분에게 특별제안 및 판매행사에 관한 정보를 보낼 수 있습니다. 다음 선택사항들 중 하나를 선택하십시오:

- 비트펜더로부터의 모든 메시지들을 보내주세요
- 가장 중요한 메시지만 보내주세요
- 아무 메시지도 보내지 말아주세요

완료를 클릭하십시오.

2.2. 설정마법사

등록마법사를 완료하면 설정마법사가 나타날 것입니다. 마법사는 여러분이 특정 제품모듈들을 설정하고 비트펜더의 중요한 보안작업들의 실행을 설정하는 것을 도와줄 것입니다.

반드시 요구되는 것은 아니지만, 시간을 줄이고 비트펜더 바이러스차단 2009 설치 전에도 여러분 시스템이 안전하게 되도록 저희는 여러분이 이 마법사를 완료하기를 권장합니다.

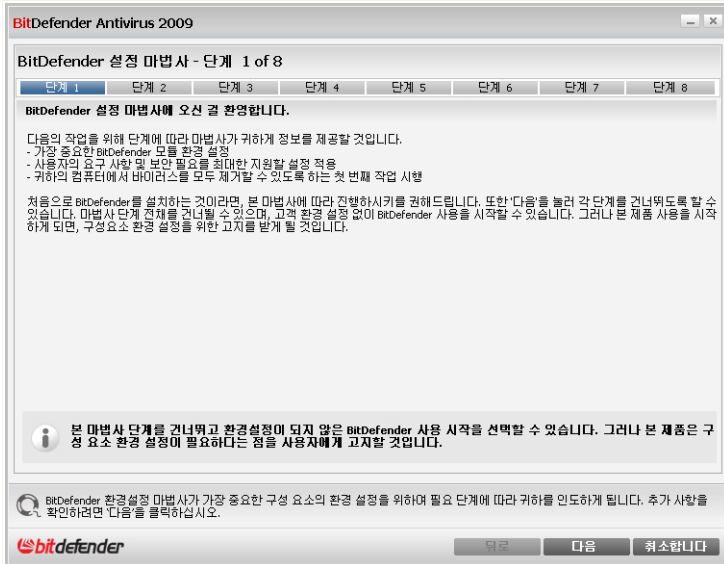


참고

이 마법사를 수행하기 원하지 않으실 경우, 취소를 클릭하십시오. 비트펜더는 여러분이 사용자 인터페이스를 열 때에 여러분이 설정할 필요가 있는 구성요소들에 대해 여러분에게 알려줄 것입니다.



2.2.1. 1/8 단계 – 환영 창

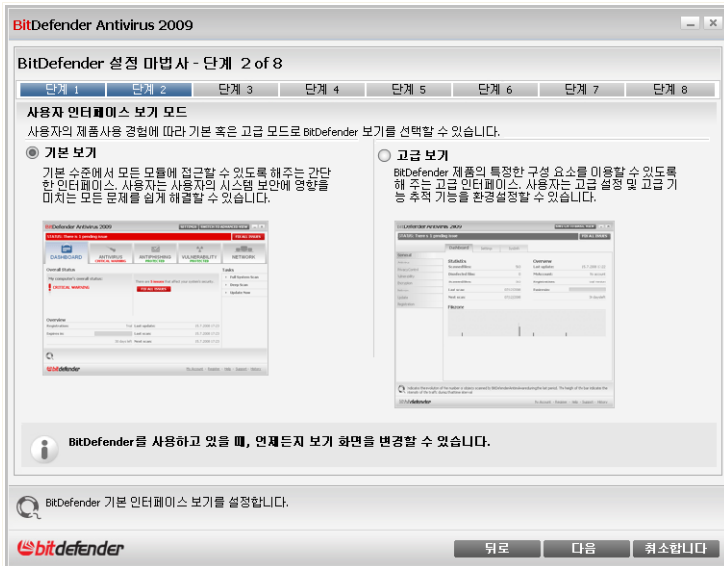


환영 창

계속하려면, 다음을 클릭하십시오.



2.2.2. 2/8 단계 – 보기모드 선택



보기 모드들

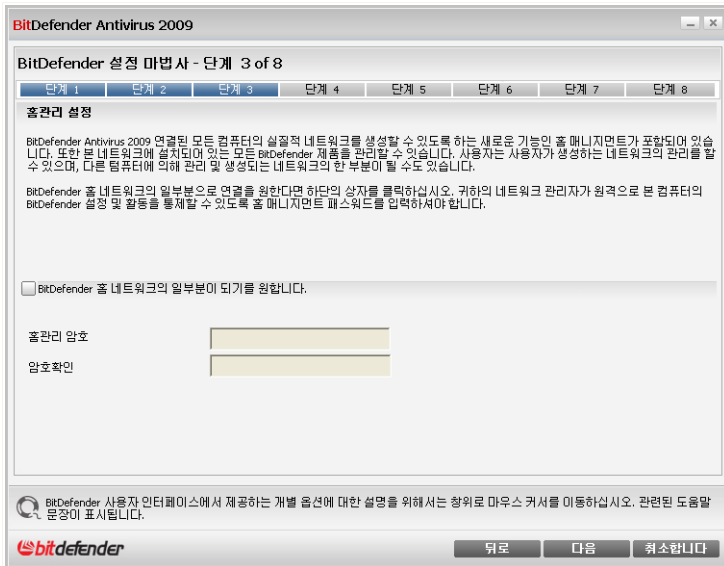
비트펜더에 대한 여러분의 사용자 경험에 따라 두 사용자 인터페이스 보기 모드들 중에서 선택하십시오.

- **기본 보기.** 초보자들과 기본 작업들을 수행하기 원하는 사용자들에게 맞춰진 간단한 인터페이스 여러분은 그저 비트펜더 경고들을 추적하고 나타나는 문제들을 고치기만 하면 됩니다.
- **상세 보기.** 제품을 완전히 설정하기 원하는 숙련된 사용자들에게 맞춰진 고급 인터페이스 여러분은 각 제품 구성요소를 설정하고 고급 작업을 수행할 수 있습니다.

계속하려면, 다음을 클릭하십시오.



2.2.3. 단계 3/8 – 비트펜더 네트워크 설정하기



비트펜더 네트워크 설정

비트펜더는 여러분이 여러분 가구 내 컴퓨터들의 가상네트워크를 생성하고 이 네트워크 내에 설치된 비트펜더 제품들을 관리할 수 있게 합니다.

만약 이 컴퓨터가 비트펜더 홈 네트워크의 일부가 되게 하기 원하시면, 이 단계들을 따르십시오:

1. 비트펜더 홈 네트워크의 일부가 되기를 원합니다
2. 각 편집필드 내에 같은 관리비밀번호를 입력하십시오.



중요

비밀번호가 있으면 관리자가 다른 컴퓨터로부터 이 비트펜더 제품을 관리할 수 있게 합니다.



2.2.4. 단계 4/8 - 신분제어 설정하기

1. 지금 설정합니다.를 선택하십시오.
2. 여러분의 민감한 데이터를 보호하기 위한 규칙들을 만드십시오. 추가 정보는, “신분제어규칙들 만들기” (p. 15)를 참조하십시오.



- 필요한 경우, 여러분이 만든 규칙들에 대한 구체적 예외를 정의하십시오. 추가 정보는, “신분제어예외 정의하기” (p. 16)를 참조하십시오.

계속하려면, 다음을 클릭하십시오.

신분제어규칙들 만들기

신분통제 규칙을 만들려면, 추가를 클릭하십시오. 설정창이 나타날 것입니다.

신분제어 규칙

여러분은 다음 매개변수들을 설정해야 합니다:

- 규칙 이름 — 이 편집칸에 규칙 이름을 입력하십시오.
- 규칙유형 — 주소, 이름, 신용카드, 비밀번호, 사회보장번호, 등 규칙유형을 선택합니다.
- 규칙데이터 — 이 편집칸 내에 여러분이 보호하기 원하시는 데이터를 입력하십시오. 예를 들면, 만약 여러분이 여러분의 신용카드번호를 보호하기 원하신다면, 이 번호의 전부 혹은 일부를 여기에 입력하십시오.



참고

만약 여러분이 세 글자 미만을 입력할 경우, 데이터를 확인하도록 여러분에게 알릴 것입니다. 메시지들 및 웹페이지들이 잘못 차단되는 경우를 피하기 위해 저희는 최소 세 글자 이상 입력하도록 권장합니다.



여러분은 규칙데이터가 전체 단어들에 맞거나 규칙데이터와 탐색된 문자열이 맞는 경우에만 규칙을 적용하도록 선택할 수 있습니다.

규칙이 막는 정보를 쉽게 찾을 수 있도록, 편집상자에 상세 규칙설명을 기입하십시오.

검사하고자 하는 교통의 유형을 지정하려면 이 선택사항들을 설정하십시오:

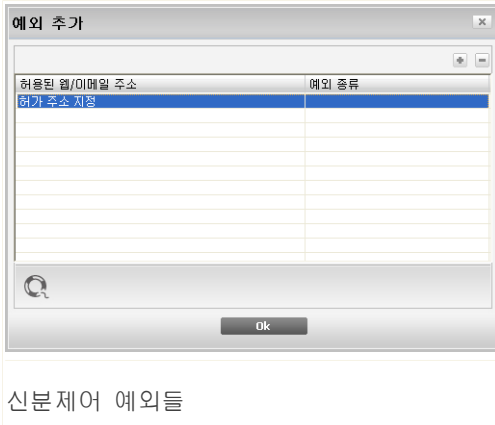
- HTTP검사 - HTTP(웹) 교통을 검사하고 규칙데이터에 맞는 송신데이터를 차단합니다.
- SMTP검사 - SMTP(메일)교통을 검사하고 규칙데이터를 담은 송신이메일메시지들을 차단합니다.
- 메신저 검사 - 메신저 교통을 검사하고 규칙데이터를 담은 송신문자대화 메시지들을 차단합니다.

규칙을 추가하려면, OK를 클릭하십시오.

신분제어예외 정의하기

특정신분규칙들에 대한 예외들을 지정할 필요가 있는 경우들이 있습니다. 여러분이 여러분의 신용카드번호가 HTTP(웹)으로 보내지는 것을 방지하는 규칙을 만드는 경우를 생각해 봅시다. 웹에서 여러분의 계정으로부터 여러분 신용카드번호가 제출될 때마다 각 페이지는 차단됩니다. 예를 들어, 만약 여러분이 어떤 온라인 매장(여러분이 안전하다는 것을 알고 있는)에서 신발류를 구입하기 원한다면, 여러분은 각 규칙에 대한 예외를 지정해야 할 것입니다.

예외를 관리할 수 있는 창을 열려면, 예외들을 클릭하십시오.



예외를 추가하려면, 이 단계들을 따르십시오:

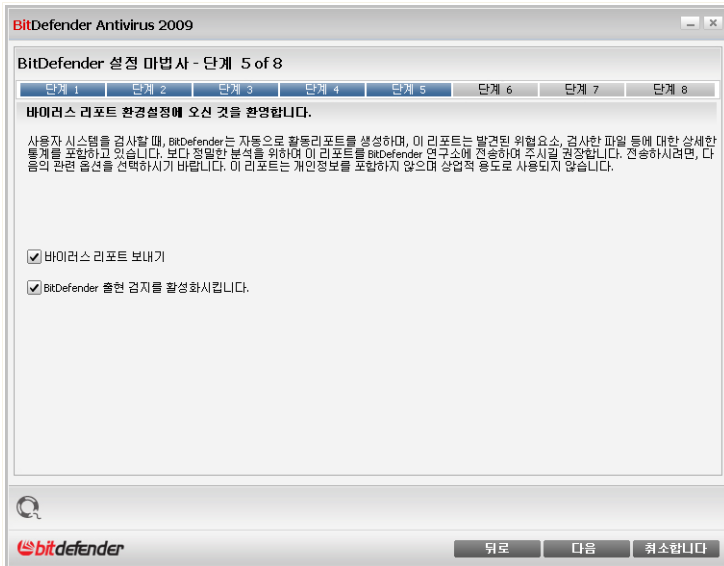
1. 표 안에 새 데이터를 추가하려면, 추가 버튼을 클릭하십시오.
2. 허가된 주로 지정하기를 더블클릭한 후, 여러분이 예외로 추가하기 원하는 웹 주소 혹은 이메일 주소를 입력하십시오.
3. 형태 선택하기를 더블클릭한 후 메뉴로부터 이전에 입력한 주소 형태에 해당하는 선택사항을 선택하십시오.
 - 만약 여러분이 웹주소를 지정했다면, HTTP를 선택하십시오.
 - 만약 여러분이 이메일 주소를 지정했다면, SMTP를 선택하십시오.

어떤 예외를 제거하려면, 그 예외를 선택한 후, 제거 버튼을 클릭하십시오.

윈도우를 닫으려면 확인을 클릭하십시오.



2.2.5. 5/8 단계 – 바이러스 보고서 설정하기



바이러스 보고 선택사항들

빗디펜더 제품은 바이러스 출현 추적을 위해 여러분 컴퓨터에서 찾아진 바이러스들에 관한 무기명 보고서들을 빗디펜더 연구소에 보낼 수 있습니다.

여러분은 다음 선택사항들을 설정할 수 있습니다:

- 바이러스 보고서 보내기 – 여러분 컴퓨터 내에서 찾아진 바이러스들에 관한 보고서들을 빗디펜더 연구소로 보냅니다.
- 빗디펜더 바이러스출현 탐지 가동 – 바이러스 출현가능성에 관한 보고서들을 빗디펜더 연구소에 보냅니다.



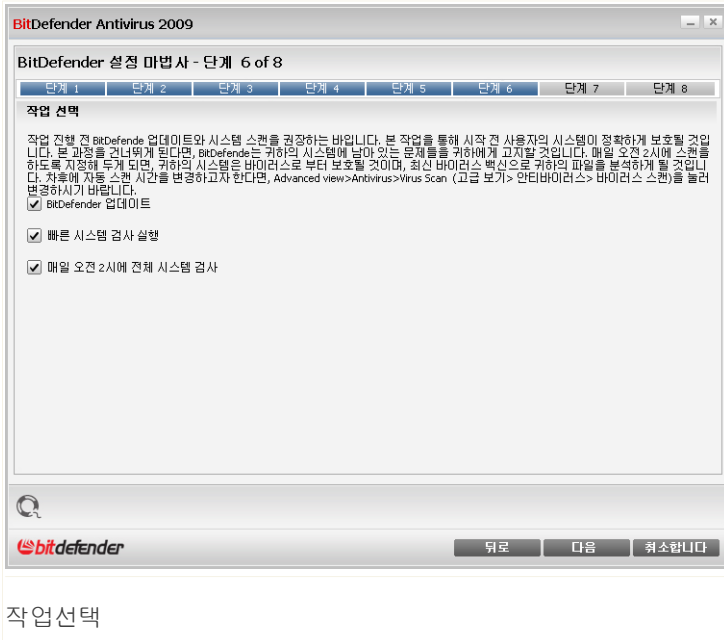
참고

보고서들에는 여러분의 성명 혹은 IP주소와 같은 어떤 기밀 데이터도 포함되지 않을 것이며, 여러분 정보는 상업목적으로 사용되지 않을 것입니다.



계속하려면, 다음을 클릭하십시오.

2.2.6. 6/8 단계 — 실행될 작업들을 선택하십시오.



여러분 시스템의 보안을 위한 중요한 작업들을 수행하기 위해 비트펜더 바이러스 차단 2009를 설정하십시오. 다음의 옵션을 사용할 수 있습니다.

- 비트펜더 엔진들을 업데이트 하기(컴퓨터를 다시 시작해야 할 수 있습니다) — 다음 단계동안 마지막 위협들로부터 여러분 컴퓨터를 보호하기 위해 비트펜더 엔진들에 대한 업데이트가 수행될 것입니다.
- 빠른 시스템 검사를 실행하기(컴퓨터 재시작이 필요할 수 있습니다) — 다음 단계동안 윈도우즈로부터의 여러분의 파일들과 프로그램 파일들 폴더들이 감염되지 않았음을 비트펜더가 확인할 수 있도록 빠른 시스템 검사가 실행될 것입니다.



- 매일 오전2시에 전체 시스템 검사 실행하기 - 매일 오전2시에 전체시스템검사를 실행합니다.



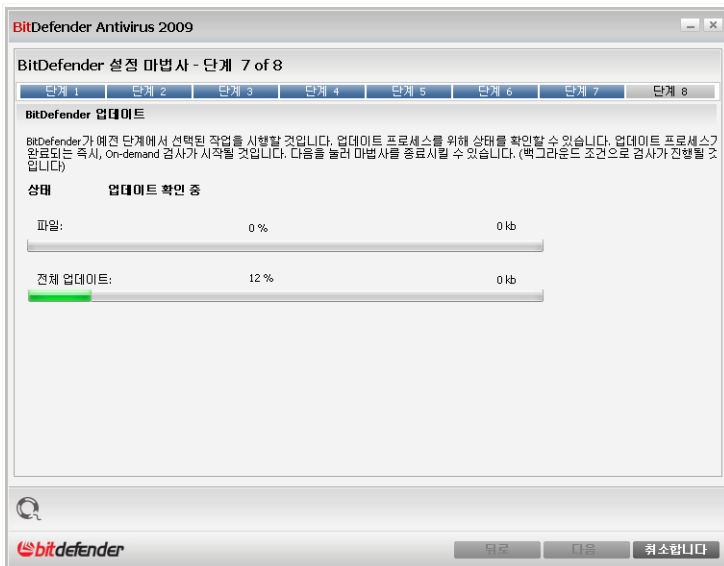
중요

여러분 시스템의 보안을 확보하기 위해 저희는 다음 단계로 넘어가기 전에 여러분이 이 선택사항을 가동시켜두도록 권장합니다.

만약 다른 선택사항은 아무 것도 선택하지 않고 오직 마지막 선택사항만 선택하는 경우, 여러분은 다음 단계를 건너뛸 것입니다.

계속하려면, 다음을 클릭하십시오.

2.2.7. 단계 7/8 - 작업들이 완료되도록 기다리기



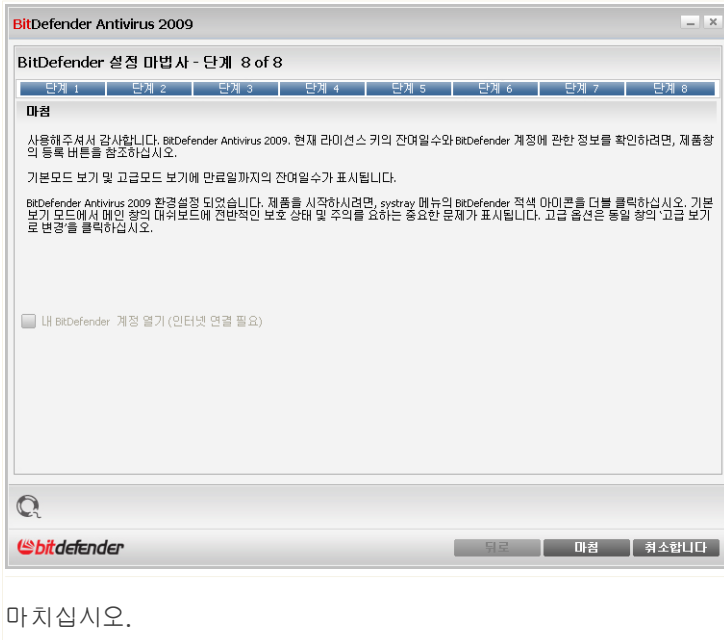
작업상태

작업(들)이 완료되도록 기다리십시오. 여러분은 이전 단계에서 선택된 작업(들)의 상태를 볼 수 있습니다.



계속하려면, 다음을 클릭하십시오.

2.2.8. 8/8 단계 — 마침



여러분의 비트펜더 계정으로 들어가려면, 내 비트펜더 계정 열기를 선택하십시오.
인터넷 연결이 필요합니다.

완료를 클릭하십시오.



3. 업그레이드

이전 버전의 BitDefender를 BitDefender Antivirus 2009로 업그레이드하려면 다음의 단계를 따릅니다.

1. 사용자 컴퓨터에서 이전버전의 BitDefender를 제거합니다. 상세정보는 도움말 파일 또는 사용자 설명서를 참조하시기 바랍니다.
2. 컴퓨터를 재시작 하십시오.
3. BitDefender Antivirus 2009를 사용설명서의 “**빗디펜더 설치하기**” (p. 4) 섹션에 따라서 설치합니다.



4. 비트펜더 수리 혹은 제거

비트펜더 바이러스차단 2009를 수리 혹은 제거하기 원하실 경우, 윈도우즈 시작메뉴로부터 다음 경로를 따르십시오: 시작 → 프로그램 → 비트펜더 2009 → 수리 혹은 제거

다음을 클릭하여 선택 사항을 확인하라는 요청을 받게 될 것입니다. 선택한 위치에 새 창이 나타날 것입니다.

■수리 — 이전 단계에서 설치된 모든 프로그램 구성요소들을 재설치합니다.

비트펜더를 수리하도록 선택하는 경우, 새 창이 나타날 것입니다. 수리과정을 시작하려면, 수리를 클릭하십시오.

메시지가 나타날 때 컴퓨터를 다시 시작하고, 그 후 비트펜더 바이러스차단 2009를 다시 설치하기 위해 설치하기를 클릭하십시오.

설치과정이 완료되었으면, 새 창이 나타날 것입니다. 완료를 클릭하십시오.

■삭제 — 설치된 구성 요소를 삭제합니다.



참고

깨끗하게 재설치하려면, 제거를 선택하도록 권장합니다.

비트펜더를 제거하기로 선택한 경우, 새 창이 나타날 것입니다.



중요

윈도우즈 비스타에만 해당! 비트펜더를 제거하면, 여러분은 바이러스와 악성 소프트웨어와 같은 악성위협들로부터 더 이상 보호되지 않을 것입니다. 비트펜더 삭제 후 윈도우즈 디펜더가 가동되기 원하실 경우, 해당 체크박스를 선택하십시오.

여러분 컴퓨터에서 비트펜더 바이러스차단 2009 제거를 시작하기 위해 제거하기를 클릭하십시오.

제거과정 중, 여러분은 저희에게 여러분의 피드백을 주시도록 메시지를 받을 것입니다. 다섯 개 이하의 짧은 질문들로 이루어진 온라인 설문에 응하려면, OK를 클릭하십시오. 설문에 응하기 원치 않으시면, 그냥 취소를 클릭하십시오.

제거과정이 완료되면, 새 창이 나타날 것입니다. 완료를 클릭하십시오.



참고

제거과정이 끝난 후, Program Files폴더로부터 비트디펜더를 삭제하도록 권장합니다.

비트디펜더를 제거하는 동안 오류가 일어났습니다.

비트디펜더를 제거하는 동안 오류가 일어나면, 제거과정이 취소되고 새 창이 나타날 것입니다. 비트디펜더가 완전히 제거되었는지 확인하기 위해 제거툴 실행하기를 클릭하십시오. 제거툴은 자동제거과정에서 제거되지 않은 모든 파일들과 레지스트리 키들을 제거할 것입니다.



기본 관리



5. 시작하기

빗디펜더가 설치되었으면 여러분 컴퓨터는 보호되어 있습니다.

5.1. 빗디펜더 바이러스차단 2009 시작하기

빗디펜더로부터 최상의 혜택을 받기 위한 첫 단계는 소프트웨어를 시작하는 것입니다.

빗디펜더 바이러스차단 2009 주 인터페이스에 접근하려면, 시작 → 프로그램 → 빗디펜더 2009 → 빗디펜더 바이러스차단 2009 경로를 따라서 위도 시작 메뉴를 사용하거나, 알림영역 안에 있는  빗디펜더 아이콘을 더블클릭하십시오.

5.2. 사용자 인터페이스 보기 모드

빗디펜더 바이러스차단 2009는 고급 사용자들이나 컴퓨터 초보자들 모두의 필요를 충족합니다. 따라서, 그래픽 사용자 인터페이스는 각각의 모든 사용자 그룹에 맞도록 설계되었습니다.

여러분은 저희 제품에 대한 여러분의 경험에 따라 빗디펜더를 기본 혹은 상세 모드로 보도록 선택할 수 있습니다.



참고

여러분은 각각 기본 보기로 전환 버튼 혹은 상세 보기로 전환 버튼을 클릭해서 이 창들 중 하나를 선택할 수 있습니다.

5.2.1. 기본 보기

기본 보기는 모든 모듈들을 기본적인 수준에서 접근할 수 있게 하는 간단한 인터페이스입니다. 여러분은 경고들과 심각한 경고들을 추적하고 바람직하지 않은 문제들을 해결해야 할 것입니다.



기본 보기

■창 위쪽에서 쉽게 찾으실 수 있듯 두 개의 버튼과 상태막대가 있습니다.

항목	설명
설정	중요한 보안 모듈들을 쉽게 가동 혹은 해제할 수 있는 창을 엽니다.
상세보기로 전환	상세보기 창을 엽니다. 이 창은 여러분이 모듈들의 전체 목록을 보고 각 구성요소의 상세사항을 설정할 수 있는 곳입니다. 비트디펜더는 여러분이 사용자 인터페이스를 열 때에 이 선택사항을 기억할 것입니다.
상태	여러분 컴퓨터의 보안 취약성들에 대한 정보를 담고 있으며, 여러분이 이런 취약성들을 고치는 것을 돕습니다.

■창 가운데에 다섯 개의 탭이 있습니다.



탭	설명
계기반	대부분의 중요한 주문형 작업들에 대한 링크들과 함께 의미있는 제품통계들과 여러분의 등록상태를 보여줍니다.
바이러스차단	여러분이 여러분의 비트펜더가 최신 상태를 유지하게 하고 여러분의 컴퓨터에 바이러스가 없도록 유지하는데 도움을 주는 바이러스 방지 모듈의 상태를 보여줍니다.
개인정보불법수집차단	여러분이 인터넷 익스플로러를 통해 하는 모든 웹페이지 접속이 안전하도록 하는 개인정보불법수집차단 모듈 상태를 보여줍니다.
취약성	여러분이 여러분 PC 상의 결정적으로 중요한 소프트웨어가 최신 상태를 유지하도록 돕는 취약성 모듈의 상태를 보여줍니다.
네트워크	비트펜더 홈 네트워크 구조를 보여줍니다.

■ 또한, 비트펜더 기본 보기 창은 몇몇 유용한 단축키들을 담고 있습니다.

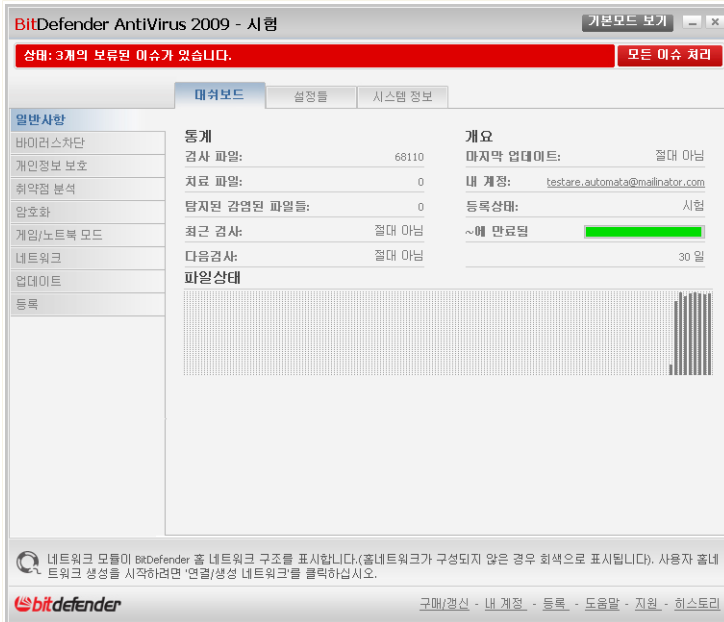
링크	설명
내 계정	여러분이 여러분의 비트펜더 계정을 만들거나 계정으로 들어갈 수 있게 합니다. 비트펜더 계정은 여러분이 기술지원에 무료로 접속할 수 있게 합니다.
등록하기	여러분이 새 면허번호를 입력하거나 현재 면허번호와 등록상태를 볼 수 있게 합니다.
도움말	비트펜더 사용법을 배울 수 있는 도움말 파일에 접속할 수 있게 합니다.
지원	비트펜더 지원팀에 연락할 수 있게 합니다.
이력	여러분 시스템의 비트펜더가 수행한 모든 작업들에 대한 상세 이력을 볼 수 있게 합니다.

5.2.2. 상세 보기

상세보기는 비트펜더 제품의 특정 구성요소에 접속할 수 있게 합니다. 여러분은 고급 기능들을 추적할 뿐 아니라 고급 설정값들을 설정할 수도 있을 것입니다.



BitDefender Antivirus 2009



상세 보기

■ 쉽게 아실 수 있듯, 창 상단에는 버튼 하나와 상태막대 하나가 있습니다.

항목	설명
기본보기로 전환	기본보기창을 엽니다. 이 창은 여러분이 주요 모듈들(보안, 튜업, 파일관리자, 네트워크)와 계기판을 포함한 기본 비트 디펜더 인터페이스를 볼 수 있는 곳입니다. 비트디펜더는 여러분이 사용자 인터페이스를 열 때 이 선택사항을 기억할 것입니다.
상태	여러분 컴퓨터의 보안 취약성들에 대한 정보를 담고 있으며, 여러분이 이런 취약성들을 고치는 것을 돕습니다.

■ 창 왼쪽에 모든 보안 모듈들을 포함하는 메뉴가 있습니다.



모듈	설명
일반사항	일반 설정에 접근하건 계기판과 상세 시스템정보를 볼 수 있게 합니다.
바이러스 방지	여러분의 바이러스 보호막과 스캐닝 작업을 상세하게 설정하고 예외를 설정하고 검역모듈을 설정할 수 있게 합니다.
개인정보보호 제어	여러분이 온라인에 있는 동안 여러분 컴퓨터에서의 데이터 도난을 예방하고, 여러분의 개인정보를 보호합니다.
암호화	여러분이 야후 및 윈도 라이브(MSN) 메신저 통신을 암호화할 수 있게 합니다.
취약성	여러분 PC 상의 중요 소프트웨어를 최신 상태로 유지할 수 있게 합니다.
게임 / 랩탑 모드	랩탑컴퓨터가 배터리로 작동하는 동안 비트디펜더 예약된 작업들을 연기하고 또한 작업 중 모든 경고 및 팝업창들을 제거할 수 있게 합니다.
네트워크	여러분 가구 내에 여러 대의 컴퓨터를 설정 및 관리할 수 있게 합니다.
업데이트	최신 업데이트 정보를 얻고 제품을 업데이트하며 업데이트 상세과정을 설정할 수 있게 합니다.
등록	비트디펜더 바이러스차단 2009를 등록하고 면허번호를 변경하고 비트디펜더 계정을 만들 수 있게 합니다.

■ 또한 비트디펜더 상세보기 창은 몇몇 유용한 단축키들을 포함합니다.

링크	설명
내 계정	여러분이 여러분의 비트디펜더 계정을 만들거나 계정으로 들어갈 수 있게 합니다. 비트디펜더 계정은 여러분이 기술지원에 무료로 접속할 수 있게 합니다.
등록하기	여러분이 새 면허번호를 입력하거나 현재 면허번호와 등록상태를 볼 수 있게 합니다.
도움말	비트디펜더 사용법을 배울 수 있는 도움말 파일에 접속할 수 있게 합니다.



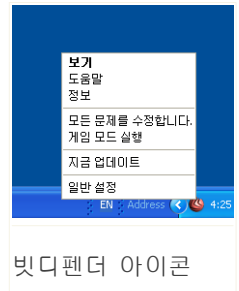
링크	설명
지원	빗디펜더 지원팀에 연락할 수 있게 합니다.
이력	여러분 시스템의 빗디펜더가 수행한 모든 작업들에 대한 상세 이력을 볼 수 있게 합니다.

5.3. 알림영역 내의 빗디펜더 아이콘

전체 제품을 더 빠르게 관리하기 위해, 여러분은 또한 알림영역 내의 빗디펜더 아이콘을 사용할 수도 있습니다.

이 아이콘을 더블클릭하면, 빗디펜더가 열릴 것입니다. 또한 이 아이콘을 오른쪽 클릭해서, 이어지는 메뉴를 통해 빗디펜더 제품을 빠르게 관리할 수 있습니다.

보기 - 빗디펜더를 엽니다.



- **도움말** - 빗디펜더 바이러스차단 2009에 관한 상세설명을 담은 도움말을 엽니다.
- **빗디펜더 정보** - 빗디펜더 웹페이지를 엽니다.
- **모든 문제 고치기** - 보안취약성을 제거하는 것을 돕니다.
- **게임모드를 ON/OFF하기** - **게임모드**를 ON/OFF합니다.
- **지금 업데이트하기** - 즉시 업데이트를 시작합니다. 업데이트 상태를 볼 수 있게 될 때 새 창이 열릴 것입니다.
- **기본 설정들** - 중요한 보안모듈들을 쉽게 가동 혹은 해제할 수 있게 합니다. 단순 클릭으로 활성화/비활성화시킬 수 있는 새 창이 나타날 것입니다.

게임모드에 있는 동안, 빗디펜더 아이콘 위에 G 문자가 보일 것입니다.

여러분 시스템 보안에 영향을 주는 중요한 문제가 있는 경우, 빗디펜더 아이콘 위에 감탄사 표시가 나타납니다. 마우스를 아이콘 위에서 움직여서 시스템의 보안에 영향을 주는 문제들의 수를 볼 수 있습니다.



5.4. 검사활동 막대

검사 활동 바는 사용자의 시스템에 대한 검사 활동을 그래픽적으로 시각화한 것입니다.

회색막대들(파일영역)에 초당 검사된 파일 수가 0에서 50까지 단위로 나타납니다.



참고

검사활동막대는 파일영역 위에 빨간 십자가를 보이면서 언제 실시간 보호가 해제되는지 여러분에게 알려줄 것입니다.



검사활동막대를 사용해 객체들을 검사할 수 있습니다. 검사하기 원하는 객체들을 끌어와서 막대 위에 놓으십시오. 추가 정보는, “**드래그 앤 드롭 검사**” (p. 122)를 참조하십시오.

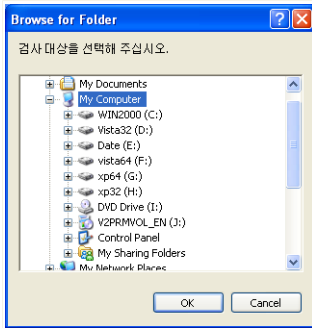
그래프를 더 이상 보고 싶지 않을 때는, 그래프를 우클릭하여 숨기기를 선택하십시오. 이 창을 완전히 감추려면, 이 단계들을 따르십시오:

1. 상세보기로 전환을 클릭하십시오.(기본보기모드에 있는 경우)
2. 왼쪽메뉴로부터 일반사항 모듈을 클릭하십시오.
3. 설정들 탭을 클릭하십시오.
4. (제품활동 화면그래프 상의) 검사활동막대 가동 체크박스를 지우십시오.

5.5. 비트펜더 수동검사

어떤 폴더를 빠르게 검사하기 원하실 경우, 비트펜더 설명서 검사를 사용할 수 있습니다.

비트펜더 수동 검사에 접속하려면, 시작 → 프로그램 → 비트펜더 2009 → 비트펜더 수동 검사 경로를 따라 윈도 시작 메뉴를 사용하십시오. 다음 창이 나타날 것입니다:



빗디펜더 수동검사

여러분은 폴더들을 둘러보고, 검사하기 원하는 폴더를 선택한 후 OK를 클릭하기만 하면 됩니다. **빗디펜더 검사기**가 나타나 여러분을 검사과정 동안 안내할 것입니다.

5.6. 게임모드

새 게임모드는 시스템성능에 대한 충격을 최소화하기 위해 보호설정들을 임시로 수정합니다. 게임모드 동안 다음 설정들이 적용됩니다:

- CPU시간과 메모리 소모를 최소화합니다.
- 자동 업데이트 & 검사를 연기하십시오.
- 모든 경고들과 팝업창들을 제거합니다.
- 가장 중요한 파일들만 검사합니다.

게임모드에 있는 동안,  빗디펜더 아이콘 위에 G 문자가 보일 것입니다.

5.6.1. 게임모드 사용하기

게임모드를 ON하기 원하시면, 다음 방법들 중 하나를 사용하십시오:

- 알림영역 내의 빗디펜더 아이콘을 오른쪽 클릭하고 게임모드ON하기를 선택하십시오.
- Ctrl+Shift+Alt+G (기본 핫키)를 누르십시오.



중요

마칠 때 게임모드를 끄는 것을 잊지 마십시오. 이를 위해, 여러분이 켤 때에 여러분이 선택한 모드와 같은 모드를 사용하십시오.

5.6.2. 게임모드 단축키 바꾸기

단축키를 변경하기 원하실 경우, 이 단계들을 따르십시오:

1. 상세보기로 전환을 클릭하십시오.(기본보기모드에 있는 경우)
2. 왼쪽의 사이트 메뉴에서 게임/노트북모드 메뉴를 클릭합니다.
3. 게임모드 탭을 클릭하십시오.
4. 고급설정들 버튼을 클릭하십시오.
5. 단축키 사용하기선택사양 아래에서 다음과 같은 방법으로 원하는 단축키를 설정하십시오:

■다음 중 하나를 클릭해서, 여러분이 사용하기 원하시는 수정키들을 선택하십시오: 제어키 (Ctrl), 시프트 키 (Shift) 혹은 알트 키 (Alt)

■편집 칸에서, 여러분이 사용하기 원하시는 일반적인 키에 해당하는 문자를 입력하십시오.

예를 들면, Ctrl+Alt+D 단축키를 사용하기 원하실 경우, 여러분은 오직 Ctrl와 Alt 만 체크하고 D를 입력해야 합니다.



참고

단축키 사용하기 옆의 체크포시를 제거하면 단축키가 불능화될 것입니다.

5.7. 웹브라우저로의 통합

비트펜더는 여러분이 인터넷을 향해하시는 동안 개인정보불법수집 시도로부터 여러분을 보호합니다. 개인정보불법수집 위협이 있는 경우 접속된 웹사이트들을 검사해서 여러분에게 경고를 합니다. 비트펜더가 검사하지 않는 웹사이트들에 대한 우량목록을 설정할 수 있습니다.

비트펜더는 직관적이고 사용이 쉬운 도구막대를 통해 다음 웹브라우저들 안으로 직접 통합됩니다:

■인터넷 익스플로러



BitDefender Antivirus 2009

■모질라 파이어폭스

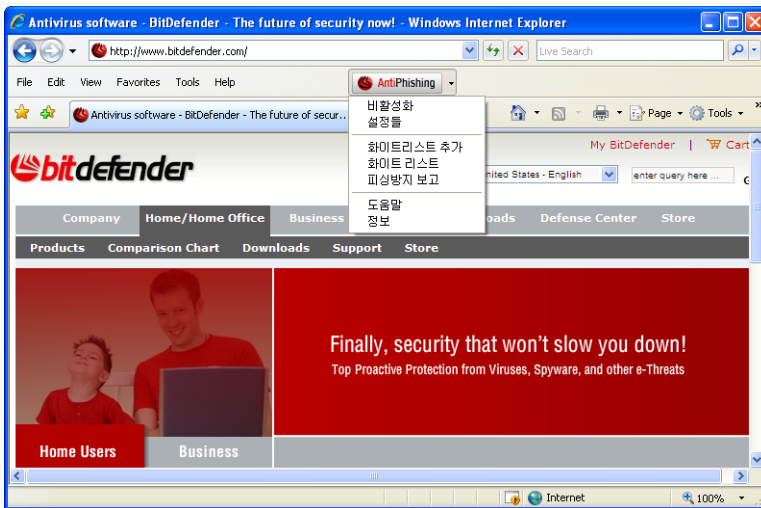
여러분은 위 웹브라우저들 중 하나에 통합된 비트펜더 개인정보불법수집차단 도구막대를 사용해 쉽고 효율적으로 개인정보불법수집차단 보호 및 우량목록을 관리할 수 있습니다.

⚙ 비트펜더 아이콘에 의해 나타나는 개인정보불법수집차단 도구막대는 브라우저 상단에 있습니다. 이것을 클릭해서 도구막대메뉴를 여십시오.



참고

도구막대가 보이지 않으면, 보기를 열고, 도구막대들로 옮긴 후 비트펜더 도구막대를 체크하십시오.



개인정보불법수집차단 도구막대

다음 명령들은 도구막대 메뉴에서 찾을 수 있습니다.

■가동 / 해제 — 비트펜더 개인정보불법수집차단 도구막대를 가동 / 해제합니다.



참고

개인정보불법수집차단 도구막대를 기능해제하도록 선택하실 경우, 여러분은 더 이상 개인정보불법수집시도들로부터 보호되지 않을 것입니다.

- 설정 — 개인정보불법수집차단 도구막대를 설정할 수 있는 창을 엽니다.

다음의 옵션을 사용할 수 있습니다.

검사가동 — 개인정보불법수집차단검사를 가동합니다.

우량목록에 추가하기 전에 알려주세요 — 어떤 웹사이트를 우량목록에 추가하기 전에 여러분에게 묻습니다.

- 우량목록에 추가 — 현재의 웹사이트를 우량목록에 추가합니다.



참고

어떤 사이트를 우량목록에 추가하는 것은 더 이상 비트펜더가 피싱시도들에 대해 그 사이트를 검사하지 않을 것임을 의미합니다. 여러분이 완전히 신뢰하는 사이트들만 우량목록에 추가하시기를 권장합니다.

- 우량목록보기 — 우량목록을 엽니다.

비트펜더 개인정보불법수집차단 엔진들에 의해 체크되지 않은 모든 웹사이트 목록들을 볼 수 있습니다.

해당 페이지에 대한 기존 개인정보불법수집위협들에 관해 여러분이 통지를 받을 수 있도록 우량목록에서 어떤 사이트를 제거하기 원하실 경우, 그 옆에 있는 제거 버튼을 클릭하십시오.

여러분이 완전히 신뢰하는 사이트들은 더 이상 개인정보불법수집차단 엔진들이 검사하지 않도록 우량목록에 추가할 수 있습니다. 어떤 사이트를 우량목록에 추가하려면, 해당 칸에 그 주소를 입력하고 추가를 클릭하십시오.

- 도움말 — 도움말 파일을 엽니다.

- 비트펜더 정보 — 비트펜더 정보를 얻고, 예기치 않은 일이 일어나는 경우 도움을 얻을 수 있는 창을 엽니다.

5.8. 메신저로의 통합

비트펜더는 야후 메신저 및 MSN 메신저를 통해 여러분의 기밀문서들과 여러분의 메신저 문자대화들을 보호하기 위해 암호화 기능들을 제공합니다.

기본값으로, 비트펜더는 여러분의 모든 메신저 문자대화 세션들을 다음과 같은 정책에 따라 암호화합니다:



- 여러분의 문자대화상대는 대화에 사용되는 메신저 응용소프트웨어에 맞도록 가동된 메신저 암호화를 지원하는 비트펜더 버전을 사용합니다.
- 여러분과 여러분의 문자대화상대는 야후 메신저 혹은 윈도 라이브(MSN) 메신저를 사용합니다.



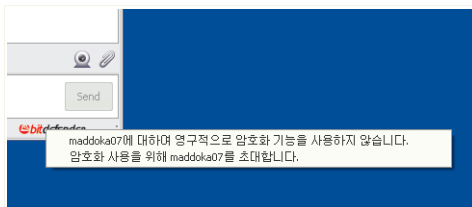
중요

문자대화상대가 Meebo 혹은 야후 메신저 혹은 MSN을 지원하는 다른 대화 응용 소프트웨어와 같은 웹기반 대화 응용소프트웨어를 사용하는 경우, 비트펜더는 대화를 암호화하지 않을 것입니다.

여러분은 문자대화 창으로부터 비트펜더 도구막대를 사용해 메신저 암호화를 쉽게 설정할 수 있습니다.

비트펜더 도구막대를 오른쪽 클릭하면 다음 선택사항들이 여러분에게 제시될 것입니다.

- 어떤 문자대화상대에 대한 암호화를 영구적으로 가동/해제하기
- 어떤 문자대화상대가 암호화를 사용하도록 안내하기
- 유해정보차단 악성목록으로부터 어떤 문자대화상대를 제거하기



메신저 암호화 선택사항들

위에 언급된 선택사항들 중 하나를 사용하기 위해 이 사항을 클릭하십시오.



6. 계기반

계기반 탭을 클릭하면, 대부분의 중요한 맞춤형 작업들에 대한 링크들과 함께 의미있는 제품통계 및 여러분의 등록상태가 제시될 것입니다.



계기반

6.1. 개요

여기는 업데이트 상태, 여러분의 계정 상태, 등록 및 면허정보에 관한 통계들의 요약 볼 수 있는 곳입니다.

항목	설명
마지막 업데이트	여러분의 비트펜더 제품이 마지막으로 업데이트된 날짜를 가리킵니다. 시스템이 완전히 보호되도록 정기적으로 업데이트를 실행하십시오.



항목	설명
내 계정	여러분의 잃어버린 비트펜더 면허번호를 찾고 비트펜더 지원 및 기타 맞춤형 서비스들의 혜택을 얻기 위해 여러분의 온라인 계좌로 접속하는데 사용할 수 있는 이메일주소를 가리킵니다.
등록 -	여러분의 면허번호 형태 및 상태를 가리킵니다. 여러분의 시스템을 안전하게 유지하려면 여러분 번호의 유효기간이 지났을 때 비트펜더를 갱신 혹은 업데이트해야 합니다.
유효기간 -	면허번호의 유효기간이 지날 때까지 남은 날 수를 가리킵니다.

비트펜더를 업데이트 하려면, 작업들 부분으로부터 지금 업데이트하기 버튼을 클릭하십시오.

여러분 비트펜더 계정을 생성 혹은 로그인하려면, 이 단계들을 따르십시오:

1. 창 하단의 내 계정 링크를 클릭하십시오. 한 웹페이지가 열릴 것입니다.
2. 여러분의 사용자이름과 비밀번호를 입력 후, 들어가기버튼을 클릭하십시오.
3. 비트펜더 계정을 만들려면, 계정이 없으세요?를 선택한 후 요구되는 정보를 제공하십시오.



참고

여러분이 여기서 제공하시는 데이터는 기밀정보로 유지될 것입니다.

비트펜더 바이러스차단 2009를 등록하시려면, 이 단계들을 따르십시오:

1. 창 하단의 내 계정 링크를 클릭하십시오. 한 단계 등록 마법사가 열릴 것입니다.
2. 새 키를 사용해 제품을 등록하기 원합니다 라디오 버튼을 클릭하십시오.
3. 해당 텍스트상자에 새 사용면허 번호를 입력하십시오.
4. 완료를 클릭하십시오.

새 면허번호를 구매하려면, 이 단계들을 따르십시오:

1. 창 하단의 내 계정 링크를 클릭하십시오. 한 단계 등록 마법사가 열릴 것입니다.
2. 사용자의 BitDefender 라이선스 키를 갱신하십시오 링크를 클릭하십시오. 웹페이지를 표시합니다.



3. 지금 구입하기 버튼을 클릭하십시오.

6.2. 작업들

여기는 가장 중요한 보안 작업들인, 전체시스템검사, 심층검사, 지금업데이트에 대한 링크를 찾을 수 있는 곳입니다.

다음 버튼들을 사용할 수 있습니다:

- 전체 시스템검사 - 여러분 컴퓨터에 대한 전체검사를 시작합니다(자료보관소 제외).
- 심층검사 - 여러분 컴퓨터에 대한 전체검사를 시작합니다(자료보관소 포함).
- 지금 업데이트하기 - 즉시 업데이트를 시작합니다.

6.2.1. 비트펜더를 사용해 검사하기

악성 소프트웨어가 있는지 여러분의 컴퓨터를 검사하시려면, 해당 버튼을 클릭해서 특정 검사작업을 실행하십시오. 다음 표는 그에 대한 설명과 함께 할 수 있는 검사작업들을 나타냅니다.

작업	설명
전체 시스템검사	자료보관소를 제외한 전체 시스템을 검사합니다. 기본 설정에서는, 바이러스, 염탐프로그램, 광고프로그램, 관리권 편취프로그램 등 여러분 시스템 보안을 위협하는 모든 형태의 악성프로그램이 있는지 검사합니다.
심층검사	전체 시스템을 검사합니다. 기본 설정에서는, 바이러스, 염탐프로그램, 광고프로그램, 관리권 편취프로그램 등 여러분 시스템 보안을 위협하는 모든 형태의 악성프로그램이 있는지 검사합니다.



참고

심층시스템검사와 전체시스템검사 작업들은 전체 시스템을 분석하기 때문에, 이런 검사는 제법 시간이 걸릴 수 있습니다. 따라서, 저희는 이런 작업들은 후 순위로 혹은 더 좋은 방법은 여러분 시스템이 공회전 중일 때 실행하도록 권장합니다.

빠른 검사든 전체 검사든 여러분이 주문형 검사과정을 시작할 때 비트펜더 검사기가 나타날 것입니다.

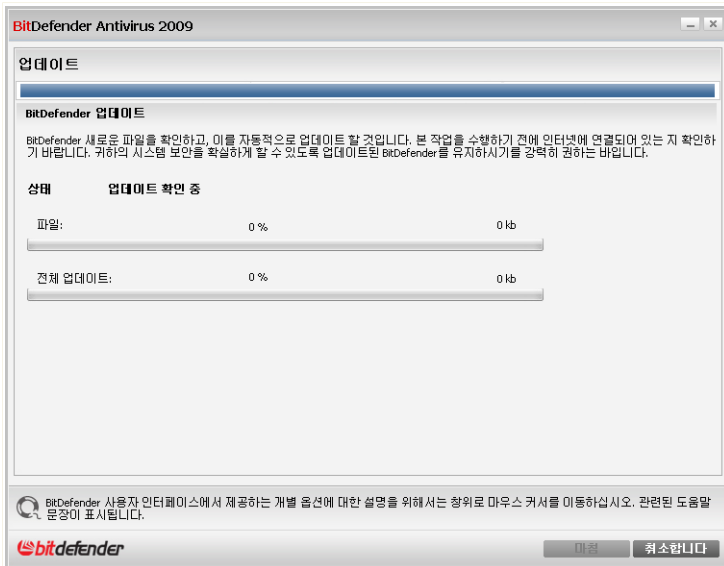
검사과정을 완성하기 위해 세 단계로 안내되는 절차를 따르십시오.



6.2.2. 비트펜더 업데이트하기

악성프로그램은 매일 찾아지게 마련입니다. 이는 비트펜더를 늘 최신 악성소프트웨어 서명된 상태로 두어야 하는 중요한 이유입니다.

기본적으로, 비트펜더는 여러분이 컴퓨터를 켤 때와 그 후 매 시간 업데이트가 있는지 확인합니다. 그러나, 비트펜더를 업데이트하기 원하실 경우, 그냥 지금 업데이트하기를 클릭하십시오. 업데이트 과정이 시작되고 즉시 다음 창이 나타날 것입니다:



비트펜더 업데이트하기

이 창에서 여러분은 업데이트 진행상태를 볼 수 있습니다.

업데이트 과정이 점진적으로 실행되는데 이는 업데이트하려는 파일들이 점진적으로 대체됨을 의미합니다. 이런 식으로, 업데이트 과정은 제품작동에 영향을 주지 않으면서도 모든 취약성들을 배제할 것입니다.

이 창을 닫기 원하실 경우, 그냥 취소만 클릭하십시오. 그러나, 이것이 업데이트 과정을 멈추지는 않습니다.



참고

전화선으로 인터넷에 연결되어 있다면, 사용자 요청을 통해 비트펜더를 정기적으로 업데이트하기를 권장합니다.

필요 시 컴퓨터를 재시작하십시오. 주요 업데이트의 경우, 여러분은 여러분 컴퓨터를 다시 시작하도록 요구받을 것입니다.

여러분의 컴퓨터를 즉시 재부팅하시려면, 재부팅을 클릭하십시오.

여러분 컴퓨터를 나중에 재부팅하시려면, 그냥 OK를 클릭하기만 하면 됩니다. 저희는 여러분의 컴퓨터를 되도록 빨리 재부팅하시기를 권장합니다.



7. 바이러스차단

비트펜더에는 여러분의 비트펜더를 업데이트된 상태로 유지하고 여러분의 컴퓨터에 바이러스가 없도록 하는데 도움을 주는 한 바이러스차단 모듈이 있습니다.

바이러스차단 모듈에 들어가려면, 바이러스 탭을 클릭하십시오.



바이러스차단

바이러스 방지 모듈에는 두 가지 영역이 있습니다:

- 감시되는 구성요소들 – 각 보안모듈에 대한 감시받는 구성요소들에 대한 전체 목록을 볼 수 있게 합니다. 여러분은 어느 모듈을 감시할지 선택할 수 있습니다. 모든 구성요소들을 감시할 수 있도록 설정하는 것을 권장합니다.
- 작업들 – 여기는 가장 중요한 작업들인 전체시스템검사, 심층검사, 지금 업데이트하기로의 링크를 찾을 수 있는 곳입니다.

7.1. 감시되는 구성요소들

감시되는 구성요소는 다음과 같습니다:



분류	설명
지역보안	여기는 파일, 레지스트리, 메모리 등 여러분 컴퓨터 상에 저장된 대상들을 보호하는 각 보안모듈의 상태를 확인할 수 있는 곳입니다.

카테고리를 열려면 “+” 표시되어 있는 상자를, 닫으려면 “-” 표시되어 있는 상자를 클릭하십시오.

7.1.1. 지역보안

저희는 어떤 문제가 여러분의 컴퓨터 보안에 영향을 줄 수 있을 때마다 알려주는 것이 중요하다는 것을 알고 있습니다. 각 보안모듈들을 감시하므로써, 비트펜더 바이러스차단 2009는 언제 여러분이 여러분의 컴퓨터의 보안에 영향을 줄 수 있는 설정들을 할 수 있는지 뿐 아니라 여러분이 중요한 작업을 잊어버렸을 때도 여러분에게 알려줍니다.

지역보안에 관한 문제들은 매우 명시적인 문장으로 설명됩니다. 각 문장과 관련하여, 여러분 컴퓨터의 보안에 영향을 줄 수 있는 것이 있으면, 고치기라고 불리는 빨간 상태 버튼이 보일 것입니다. 그렇지 않을 경우, 녹색의 OK 상태버튼이 나타납니다.

문제	설명
실시간 파일보호가 가동되었습니다	여러분 혹은 이 시스템 상에 실행되고 있는 한 응용소프트웨어가 접근해서 모든 파일을 검사하게 합니다.
여러분은 오늘 악성 소프트웨어가 있는 지 여러분의 컴퓨터를 검사했습니다	여러분 컴퓨터에 저장된 파일들에 악성소프트웨어가 없는지 확인하기 위해 되도록 빨리 주문형 검사를 실행하도록 권장합니다.
자동업데이트가 가동되었습니다	여러분의 비트펜더 제품에 대한 악성프로그램 서명들이 정기적으로 업데이트되도록 자동업데이트가 가동된 상태로 두십시오.
지금 업데이트하기	제품 및 악성프로그램 서명들의 업데이트가 실행 중입니다.

상태버튼들이 녹색일 때에는 여러분 시스템의 보안위험이 최소수준에 있습니다. 버튼들을 녹색으로 바꾸시려면, 이 단계들을 따르십시오:



1. 보안취약성들을 하나씩 고치려면 고치기 버튼들을 클릭하십시오.
2. 한 문제가 즉석에서 고쳐지지 않으면, 이 문제를 고치기 위해 마법사를 따르십시오.

어떤 문제를 감시에서 제외하기 원하실 경우, 예, 이 구성요소를 감시해 주세요 체크박스를 제거하기만 하면 됩니다.

7.2. 작업들

여기는 가장 중요한 보안 작업들인, 전체시스템검사, 심층검사, 지금업데이트에 대한 링크를 찾을 수 있는 곳입니다.

다음 버튼들을 사용할 수 있습니다:

- 전체 시스템검사 - 여러분 컴퓨터에 대한 전체검사를 시작합니다(자료보관소 제외).
- 심층검사 - 여러분 컴퓨터에 대한 전체검사를 시작합니다(자료보관소 포함).
- 내 문서 검사 - 여러분의 문서들과 설정들에 대한 빠른 검사를 시작합니다.
- 지금 업데이트하기 - 즉시 업데이트를 시작합니다.

7.2.1. 비트펜더를 사용해 검사하기

악성 소프트웨어가 있는지 여러분의 컴퓨터를 검사하시려면, 해당 버튼을 클릭해서 특정 검사작업을 실행하십시오. 다음 표는 그에 대한 설명과 함께 할 수 있는 검사작업들을 나타냅니다.

작업	설명
전체 시스템검사	자료보관소를 제외한 전체 시스템을 검사합니다. 기본 설정에서는, 바이러스, 염탐프로그램, 광고프로그램, 관리권 편취프로그램 등 여러분 시스템 보안을 위협하는 모든 형태의 악성프로그램이 있는지 검사합니다.
심층검사	전체 시스템을 검사합니다. 기본 설정에서는, 바이러스, 염탐프로그램, 광고프로그램, 관리권 편취프로그램 등 여러분 시스템 보안을 위협하는 모든 형태의 악성프로그램이 있는지 검사합니다.
내 문서 검사	이 작업을 사용해 중요한 현재 사용자 폴더들인 내 문서들, 바탕화면 및 시작을 검사하십시오. 이는 안전



작업	설명
	한 작업공간인 여러분의 문서들에 대한 안전성을 보장하고 시작시에 작동하는 응용소프트웨어들을 청소합니다.



참고

심층시스템검사와 전체시스템감사 작업들은 전체 시스템을 분석하기 때문에, 이런 검사는 제법 시간이 걸릴 수 있습니다. 따라서, 저희는 이런 작업들은 후 순위로 혹은 더 좋은 방법은 여러분 시스템이 공회전 중일 때 실행하도록 권장합니다.

빠른 검사든 전체 검사든 여러분이 주문형 검사과정을 시작할 때 비트펜더 검사기가 나타날 것입니다.

검사과정을 완성하기 위해 세 단계로 안내되는 절차를 따르십시오.

7.2.2. 비트펜더 업데이트하기

악성프로그램은 매일 찾아지게 마련입니다. 이는 비트펜더를 늘 최신 악성소프트웨어 서명된 상태로 두어야 하는 중요한 이유입니다.

기본적으로, 비트펜더는 여러분이 컴퓨터를 켤 때와 그 후 매 시간 업데이트가 있는지 확인합니다. 그러나, 비트펜더를 업데이트하기 원하실 경우, 그냥 지금 업데이트하기를 클릭하십시오. 업데이트 과정이 시작되고 즉시 다음 창이 나타날 것입니다:



이 창을 닫기 원하실 경우, 그냥 취소만 클릭하십시오. 그러나, 이것이 업데이트 과정을 멈추지는 않습니다.



필요 시 컴퓨터를 재시작하십시오. 주요 업데이트의 경우, 여러분은 여러분 컴퓨터를 다시 시작하도록 요구받을 것입니다.

바이러스 차단



BitDefender Antivirus 2009

여러분 컴퓨터를 나중에 재부팅하시려면, 그냥 OK를 클릭하기만 하면 됩니다. 저희는 여러분의 컴퓨터를 되도록 빨리 재부팅하시기를 권장합니다.



8. 개인정보불법수집차단

비트펜더에는 인터넷익스플로러 혹은 파이어폭스를 통해 여러분이 행하는 모든 웹페이지 접속이 안전하게 하는 개인정보불법수집차단 모듈이 있습니다.

개인정보불법수집차단 모듈로 들어가려면, 개인정보불법수집차단 탭을 클릭하십시오.



개인정보불법수집차단

개인정보불법수집차단 모듈에는 다음과 같은 두 영역들로 이루어집니다:

- 감시되는 구성요소들 – 각 보안모듈에 대한 감시받는 구성요소들에 대한 전체 목록을 볼 수 있게 합니다. 여러분은 어느 모듈을 감시할지 선택할 수 있습니다. 모든 구성요소들을 감시할 수 있도록 설정하는 것을 권장합니다.
- 작업들 – 여기는 가장 중요한 작업들인 전체시스템검사, 심층검사, 지금 업데이트하기로의 링크를 찾을 수 있는 곳입니다.



8.1. 감시되는 구성요소들

감시되는 구성요소는 다음과 같습니다:

분류	설명
온라인 보안	여기는 인터넷에 연결되어 있는 동안 여러분의 온라인 거래 및 여러분의 컴퓨터를 보호하는 각 보안모듈의 상태를 확인할 수 있는 곳입니다.

카테고리를 열려면 “+” 표시되어 있는 상자를, 닫으려면 “-” 표시되어 있는 상자를 클릭하십시오.

8.1.1. 온라인 보안

온라인 보안 관련 문제들은 매우 명시적인 문장들로 설명되어 있습니다. 각 문장에서, 만약 여러분 컴퓨터의 보안에 영향을 줄 수 있는 것이 있는 경우, 고치기라고 불리는 빨간상태버튼이 보일 것입니다. 그렇지 않을 경우, 녹색의 OK 상태버튼이 나타납니다.

문제	설명
메신저에 대한 문자 대화 암호화가 가동되어 있습니다	여러분의 메신저 연락처들에게 비트펜더 2009가 설치되어 있으면, 야후!메신저 및 윈도우즈 라이브 메신저를 통한 모든 논의는 암호화될 것입니다. 여러분의 메신저 문자대화가 사생활보호를 받을 수 있도록 메신저에 대한 대화 암호화가 가동된 상태로 두도록 권장합니다.
파이어폭스 개인정보불법수집차단 보호가 가동되어 있습니다	비트펜더는 여러분이 인터넷을 항해하시는 동안 개인정보불법수집 시도로부터 여러분을 보호합니다.
인터넷익스플로러 개인정보불법수집차단 보호가 가동되어 있습니다	비트펜더는 여러분이 인터넷을 항해하시는 동안 개인정보불법수집 시도로부터 여러분을 보호합니다.



상태버튼들이 녹색일 때에는 여러분 시스템의 보안위험이 최소수준에 있습니다. 버튼들을 녹색으로 바꾸시려면, 이 단계들을 따르십시오:

1. 보안취약성들을 하나씩 고치려면 고치기 버튼들을 클릭하십시오.
2. 한 문제가 즉석에서 고쳐지지 않으면, 이 문제를 고치기 위해 마법사를 따르십시오.

어떤 문제를 감시에서 제외하기 원하실 경우, 예, 이 구성요소를 감시해 주세요 체크박스를 제거하기만 하면 됩니다.

8.2. 작업들

여기는 가장 중요한 보안 작업들인, 전체시스템검사, 심층검사, 지금업데이트에 대한 링크를 찾을 수 있는 곳입니다.

다음 버튼들을 사용할 수 있습니다:

- 전체 시스템검사 - 여러분 컴퓨터에 대한 전체검사를 시작합니다(자료보관소 제외).
- 심층검사 - 여러분 컴퓨터에 대한 전체검사를 시작합니다(자료보관소 포함).
- 내 문서 검사 - 여러분의 문서들과 설정들에 대한 빠른 검사를 시작합니다.
- 지금 업데이트하기 - 즉시 업데이트를 시작합니다.

8.2.1. 비트디펜더를 사용해 검사하기

악성 소프트웨어가 있는지 여러분의 컴퓨터를 검사하시려면, 해당 버튼을 클릭해서 특정 검사작업을 실행하십시오. 다음 표는 그에 대한 설명과 함께 할 수 있는 검사작업들을 나타냅니다.

작업	설명
전체 시스템검사	자료보관소를 제외한 전체 시스템을 검사합니다. 기본 설정에서는, 바이러스, 염탐프로그램, 광고프로그램, 관리권 편취프로그램 등 여러분 시스템 보안을 위협하는 모든 형태의 악성프로그램이 있는지 검사합니다.
심층검사	전체 시스템을 검사합니다. 기본 설정에서는, 바이러스, 염탐프로그램, 광고프로그램, 관리권 편취프로그램 등 여러분 시스템 보안을 위협하는 모든 형태의 악성프로그램이 있는지 검사합니다.



작업	설명
내 문서 검사	이 작업을 사용해 중요한 현재 사용자 폴더들인 내 문서들, 바탕화면 및 시작을 검사하십시오. 이는 안전한 작업공간인 여러분의 문서들에 대한 안전성을 보장하고 시작시에 작동하는 응용소프트웨어들을 청소합니다.



참고

심층시스템검사와 전체시스템감사 작업들은 전체 시스템을 분석하기 때문에, 이런 검사는 제법 시간이 걸릴 수 있습니다. 따라서, 저희는 이런 작업들은 후 순위로 혹은 더 좋은 방법은 여러분 시스템이 공회전 중일 때 실행하도록 권장합니다.

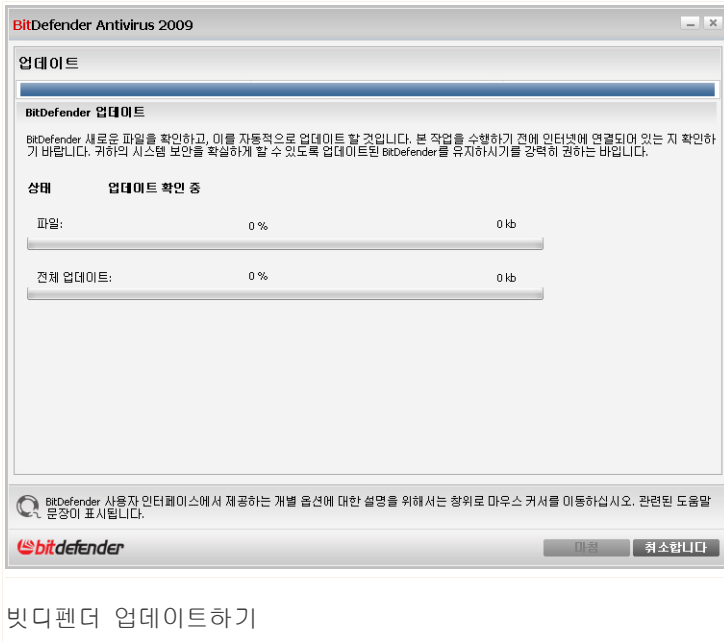
빠른 검사든 전체 검사든 여러분이 주문형 검사과정을 시작할 때 비트펜더 검사기가 나타날 것입니다.

검사과정을 완성하기 위해 세 단계로 안내되는 절차를 따르십시오.

8.2.2. 비트펜더 업데이트하기

악성프로그램은 매일 찾아지게 마련입니다. 이는 비트펜더를 늘 최신 악성소프트웨어 서명된 상태로 두어야 하는 중요한 이유입니다.

기본적으로, 비트펜더는 여러분이 컴퓨터를 켤 때와 그 후 매 시간 업데이트가 있는지 확인합니다. 그러나, 비트펜더를 업데이트하기 원하실 경우, 그냥 지금 업데이트하기를 클릭하십시오. 업데이트 과정이 시작되고 즉시 다음 창이 나타날 것입니다:



이 창에서 여러분은 업데이트 진행상태를 볼 수 있습니다.

업데이트 과정이 점진적으로 실행되는데 이는 업데이트하려는 파일들이 점진적으로 대체됨을 의미합니다. 이런 식으로, 업데이트 과정은 제품작동에 영향을 주지 않으면서도 모든 취약성들을 배제할 것입니다.

이 창을 닫기 원하실 경우, 그냥 취소만 클릭하십시오. 그러나, 이것이 업데이트 과정을 멈추지는 않습니다.



참고

전화선으로 인터넷에 연결되어 있다면, 사용자 요청을 통해 빗디펜더를 정기적으로 업데이트하시기를 권장합니다.

필요 시 컴퓨터를 재시작하십시오. 주요 업데이트의 경우, 여러분은 여러분 컴퓨터를 다시 시작하도록 요구받을 것입니다.

여러분의 컴퓨터를 즉시 재부팅하시려면, 재부팅을 클릭하십시오.



BitDefender Antivirus 2009

여러분 컴퓨터를 나중에 재부팅하시려면, 그냥 OK를 클릭하기만 하면 됩니다. 저희는 여러분의 컴퓨터를 되도록 빨리 재부팅하시기를 권장합니다.



9. 취약성

비트펜더에는 여러분이 여러분의 PC 상의 중요한 소프트웨어가 업데이트된 상태를 유지하는 것을 돕는 취약성 모듈이 있습니다.

취약성 모듈로 들어가려면, 취약성 탭을 클릭하십시오.



취약성 모듈은 다음과 같은 두 영역으로 구성됩니다.

- 감시되는 구성요소들 – 각 보안모듈에 대한 감시받는 구성요소들에 대한 전체 목록을 볼 수 있게 합니다. 여러분은 어느 모듈을 감시할지 선택할 수 있습니다. 모든 구성요소들을 감시할 수 있도록 설정하는 것을 권장합니다.
- 작업들 – 여기는 가장 중요한 보안작업들 중 하나에 대한 링크를 찾을 수 있는 곳입니다.

9.1. 감시되는 구성요소들

감시되는 구성요소는 다음과 같습니다:



분류	설명
취약성 검사	여기는 여러분 PC 상의 중요한 소프트웨어가 업데이트된 상태인지를 확인할 수 있는 곳입니다. 윈도우 계정들에 대한 비밀번호들이 보안규칙들에 맞는지 확인합니다.

카테고리를 열려면 “+” 표시되어 있는 상자를, 닫으려면 “-” 표시되어 있는 상자를 클릭하십시오.

9.1.1. 취약성 검사

취약성들과 관련된 문제들은 매우 명시적인 문장으로 설명되어 있습니다. 각 문장에서, 만약 여러분 컴퓨터의 보안에 영향을 주는 것이 있으면, 고치기라고 불리는 빨간 상태버튼이 보일 것입니다. 그렇지 않을 경우, 녹색의 OK 상태버튼이 나타납니다.

문제	설명
취약성 확인이 가동되어 있습니다.	여러분의 운영체계가 업데이트된 상태에 있으며 비밀번호가 취약하지 않게 하기 위해 마이크로소프트 윈도우즈 업데이트, 마이크로소프트 윈도우즈 오피스 업데이트 및 마이크로소프트 윈도우즈 계정들의 비밀번호들을 감사합니다.
중요 마이크로소프트 업데이트들	사용할 수 있는 중요 마이크로소프트 업데이트들을 설치하십시오.
기타 마이크로소프트 업데이트들	사용할 수 있는 중요하지 않은 마이크로소프트 업데이트들을 설치하십시오.
윈도우 자동 업데이트가 가동되어 있습니다	새 윈도우즈 보안 업데이트들이 나오는 즉시 그 업데이트들을 설치하십시오.
관리자 (강력한 비밀번호)	특정 사용자에 대한 비밀번호의 유효성을 가리킵니다.

상태버튼들이 녹색일 때에는 여러분 시스템의 보안위험이 최소수준에 있습니다. 버튼들을 녹색으로 바꾸시려면, 이 단계들을 따르십시오:

1. 보안취약성들을 하나씩 고치려면 고치기 버튼들을 클릭하십시오.



2. 한 문제가 즉석에서 고쳐지지 않으면, 이 문제를 고치기 위해 마법사를 따르십시오.

어떤 문제를 감시에서 제외하기 원하실 경우, 예, 이 구성요소를 감시해 주세요 체크박스를 제거하기만 하면 됩니다.

9.2. 작업들

여기는 가장 중요한 보안 작업들 중 하나에 대한 링크를 찾을 수 있는 곳입니다. 다음 버튼들을 사용할 수 있습니다:

■취약성 검사

9.2.1. 취약성들 검색하기

취약성 검사는 여러분의 운영체계가 최신 업데이트를 유지하게 하고 비밀번호 우회에 취약하지 않게 하도록 마이크로소프트 윈도우즈 업데이트, 마이크로소프트 윈도우즈 오피스 업데이트 및 여러분의 마이크로소프트 윈도우즈 계정들에 대한 비밀번호들을 확인합니다.

여러분 컴퓨터의 취약성을 검사하려면, 취약성 검사를 클릭한 후 마법사를 따르십시오.



1/6 단계 — 확인하려는 취약성들을 선택하십시오.

BitDefender 2009

BitDefender 취약점 마법사

Step 1Step 2Step 3Step 4Step 5Step 6

작업 선택

마법사가 뒤떨어진 어플리케이션과 취약한 패스워드를 가진 윈도우 계정을 확인하기 위한 단계로 귀하를 안내할 것입니다. 취약성을 확인할 항목을 아래의 리스트에서 선택하십시오.

- ☒ 윈도우 중요 업데이트 확인
- ☒ 윈도우 선택 업데이트 확인
- ☒ 응용프로그램 업데이트 확인
- ☒ 윈도우 계정 암호 확인

이 상자를 선택하여 BitDefender가 귀하의 윈도우 운영체제가 마이크로소프트 최신 보안 업데이트 사항을 적용하였는지를 확인하도록 하십시오.

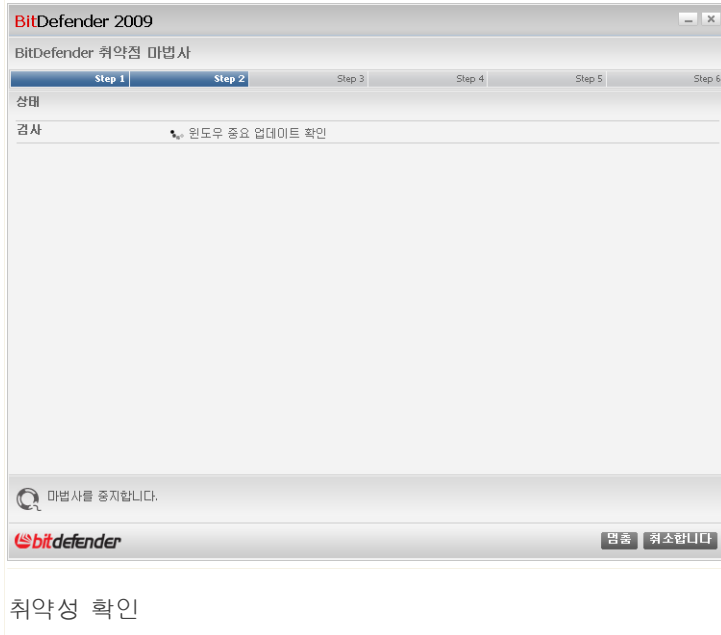
다음 취소합니다

취약성들

선택된 취약성들에 대해 시스템을 확인하려면 다음을 클릭하십시오.



2/6 단계 - 취약성 확인하기



비트펜더가 취약성 확인을 마칠 때까지 기다리십시오.



3/6 단계 — 약한 비밀번호 변경

BitDefender 2009

BitDefender 취약점 마법사

Step 1

Step 2

Step 3

Step 4

Step 5

Step 6

윈도우 업데이트

윈도우 중요 업데이트 확인

Security Update for Windows XP (KB901190)

MSXML 6.0 RTM Security Update (925673)

Security Update for Windows XP (KB943485)

Security Update for Windows XP (KB946026)

Security Update for Windows XP (KB943055)

Update for Office 2003 (KB907417)

Security Update for Windows XP (KB945553)

Microsoft .NET Framework 1.1 Service Pack 1

Security Update for Windows XP (KB950749)

Update for Windows XP (KB932823)

Office 2003 Service Pack 3 (SP3)

Security Update for Windows XP (KB950762)

Security Update for Windows XP (KB951376)

Security Update for Windows XP (KB951698)

Security Update for Windows XP (KB951748)

모든 시스템 업데이트를 설치합니다.

이것은 중요한 혹은 중요하지 않은 윈도우 어플리케이션 업데이트 리스트입니다.

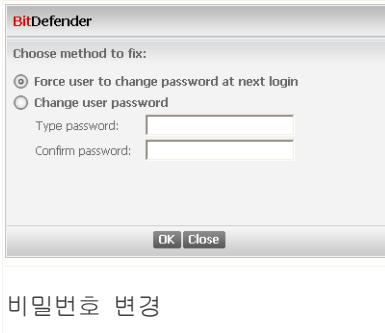
bitdefender

다음 취소합니다

사용자 비밀번호들

여러분 컴퓨터 상에 설정된 윈도우즈 사용자 계정들의 목록과 그 비밀번호들이 제공하는 보호 수준을 보여줍니다.

약한 비밀번호를 변경하려면 고치기를 클릭하십시오. 새로운 창이 나타날 것입니다.



다음 이 문제를 고치는 방법을 선택하십시오:

- 다음 로그인 시 사용자가 비밀번호를 고치도록 요구하십시오. 비트펜더는 사용자가 다음에 윈도우로 로그인할 때에 비밀번호를 바꾸도록 사용자에게 요구할 것입니다.
- 사용자 비밀번호 변경. 여러분은 편집 칸에 새 비밀번호를 입력해야 합니다.



참고

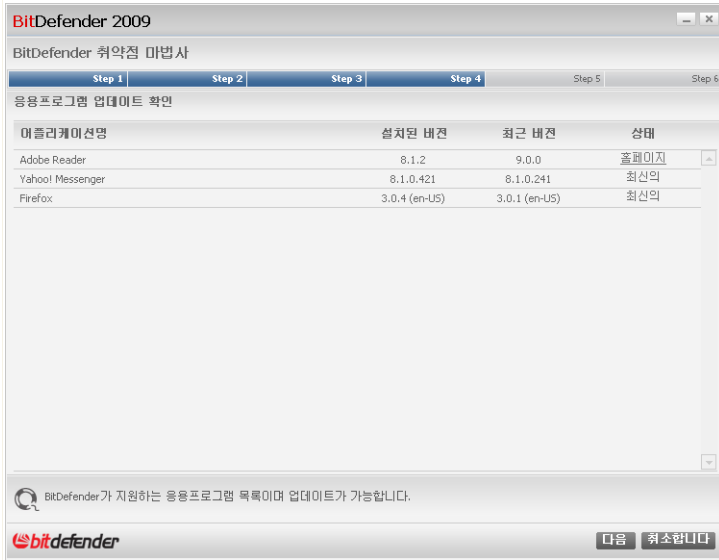
비밀번호를 튼튼하게 하기 위해 대문자와 소문자, 숫자와 #, \$ 혹은 @ 등 특수 문자들의 조합을 사용하십시오.

비밀번호를 변경하려면, OK를 클릭하십시오.

다음은 클릭하십시오.



4/6 단계 - 응용소프트웨어 업데이트



응용소프트웨어들

여러분은 비트펜더가 확인한 응용소프트웨어들의 목록과 업데이트 상황을 볼 수 있습니다. 약 어떤 응용소프트웨어가 최신업데이트되어 있지 않으면, 제공된 링크를 클릭해서 최신버전을 내림받으십시오.

다음을 클릭하십시오.



5/6 단계 - 윈도 업데이트



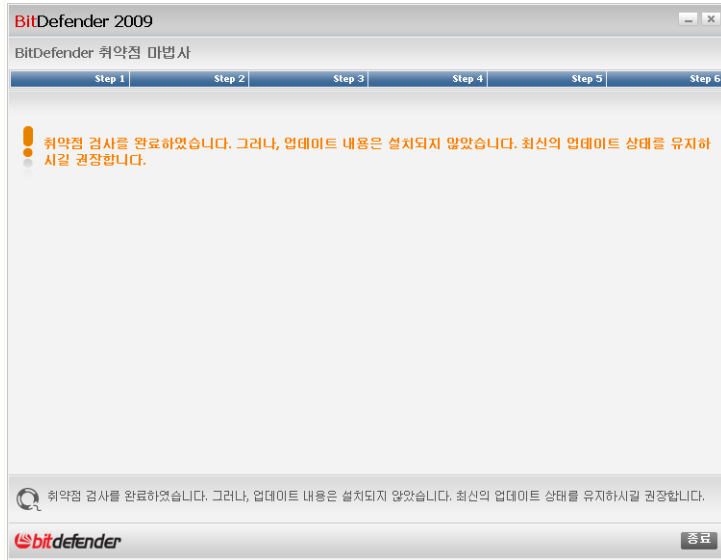
윈도 업데이트

현재 여러분 컴퓨터에 설치되어 있지 않은 중요한 윈도 업데이트들과 중요하지 않은 업데이트들의 목록이 보일 것입니다. 모든 사용할 수 있는 업데이트들을 설치하려면, 모든 시스템 업데이트 설치를 클릭하십시오.

다음을 클릭하십시오.



6/6 단계 - 보기 결과들



결과들

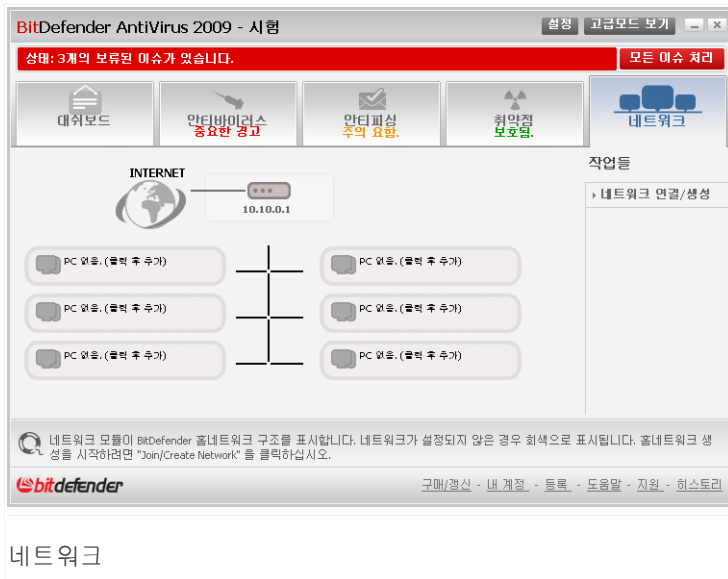
단기를 클릭하십시오.



10. 네트워크

네트워크 모듈은 여러분의 가정용 컴퓨터들에 설치된 비트디펜더 제품들을 한 대의 컴퓨터에서 관리할 수 있게 합니다.

네트워크 모듈로 들어가려면, 파일관리자 탭을 클릭하십시오.



여러분의 가정용 컴퓨터들에 설치된 비트디펜더 제품들을 관리하기 위해서는 다음 단계들을 따라야 합니다:

1. 여러분 컴퓨터의 비트디펜더 가정용 네트워크에 동참하십시오. 네트워크에 동참하려면 가정용 네트워크 관리를 위한 관리자 비밀번호 설정이 필요합니다.
2. 관리하기 원하는 각 컴퓨터로 가서 네트워크에 동참하십시오(비밀번호 설정).
3. 여러분 컴퓨터로 가서 여러분이 관리하기 원하는 컴퓨터들을 추가하십시오.



10.1. 작업들

처음에는, 하나의 버튼만 사용할 수 있습니다.

- 네트워크 동참/생성 - 네트워크 비밀번호를 설정해서 네트워크에 들어갈 수 있게 합니다.

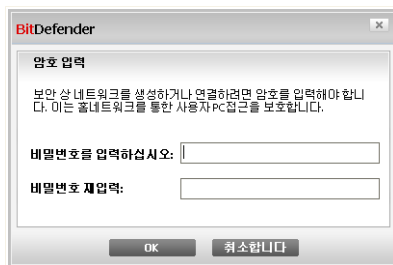
네트워크에 동참한 후, 몇몇 버튼들이 더 생길 것입니다.

- 네트워크 나가기 - 네트워크를 나갈 수 있게 합니다.
- 네트워크 관리 - 여러분의 네트워크에 컴퓨터를 추가할 수 있게 합니다.
- 모두 검사 - 모든 관리되는 컴퓨터들을 동시에 검사할 수 있게 합니다.
- 모두 업데이트하기는 모든 관리되는 컴퓨터들을 동시에 업데이트할 수 있게 합니다.
- 모두 등록하기는 여러분이 모든 관리되는 컴퓨터들을 동시에 등록할 수 있게 합니다.

10.1.1. 비트펜더 네트워크에 동참하기

비트펜더 가정용 네트워크에 동참하려면 이 단계들을 따르십시오:

1. 네트워크 동참/생성을 클릭하십시오. 여러분은 가정용 네트워크 관리 비밀번호를 설정하도록 요구받을 것입니다.



BitDefender

암호 입력

보안 상 네트워크를 생성하거나 연결하려면 암호를 입력해야 합니다. 이는 홈네트워크를 통한 사용자 PC접근을 보호합니다.

비밀번호를 입력하십시오:

비밀번호 재입력:

OK 취소합니다

비밀번호를 설정하십시오.

2. 각 편집칸에 동일한 비밀번호를 입력하십시오.
3. 확인을 클릭하십시오.



네트워크 지도에 컴퓨터 이름이 보일 것입니다.

10.1.2. 비트펜더 네트워크에 컴퓨터들을 추가하기

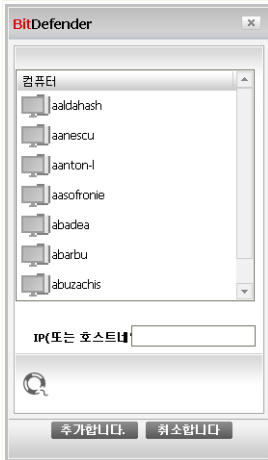
비트펜더 가정용 네트워크에 한 컴퓨터를 추가할 수 있기 전에, 여러분은 각 컴퓨터 상의 비트펜더 가정용 네트워크 관리 비밀번호를 설정해야 합니다.

비트펜더 가정용 네트워크에 어떤 컴퓨터를 추가하려면, 이 단계들을 따르십시오:

1. 네트워크 관리를 클릭하십시오. 여러분은 지역의 가정용 네트워크 관리비밀번호를 제공하도록 요구받을 것입니다.

비밀번호를 입력하십시오.

2. 가정용 관리비밀번호를 입력하고 OK를 클릭하십시오. 새로운 창이 나타날 것입니다.



컴퓨터를 추가하십시오.

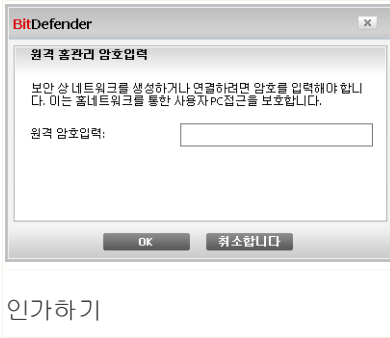
네트워크에 여러 컴퓨터들이 보일 것입니다. 아이콘의 의미는 다음과 같습니다:

-  어떤 비트펜더 제품도 설치되지 않은 온라인 컴퓨터를 가리킵니다.
-  비트펜더가 설치된 온라인 컴퓨터를 가리킵니다.
-  비트펜더가 설치된 오프라인 컴퓨터를 가리킵니다.

3. 다음 중 한 가지를 실행하십시오:

- 추가할 컴퓨터의 이름을 목록에서 선택하십시오.
- 추가할 컴퓨터의 IP주소 혹은 이름을 해당 칸에 입력하십시오.

4. 추가를 클릭하십시오. 여러분은 각 컴퓨터의 가정용 네트워크 관리 비밀번호를 입력하도록 요구받을 것입니다.



5. 각 컴퓨터 상에 설정된 가정용 네트워크 관리비밀번호를 입력하십시오.
6. 확인을 클릭하십시오. 만약 여러분이 바른 비밀번호를 제공했으면, 선택된 컴퓨터 이름이 네트워크 지도에 나타날 것입니다.



참고

여러분은 네트워크 지도에 다섯 대의 컴퓨터까지 추가할 수 있습니다.

10.1.3. 비트펜더 네트워크 관리하기

여러분이 비트펜더 가정용 네트워크를 성공적으로 생성했으면, 여러분은 한 대의 컴퓨터에서 모든 비트펜더 제품들을 관리할 수 있습니다.



네트워크 지도

만약 네트워크 지도에서 어떤 컴퓨터 위로 마우스 커서를 옮기면, 시스템 보안, 비트펜더 등록상태에 영향을 주는 문제들의 이름, IP주소, 번호 등 이에 대한 짧은 정보가 보일 것입니다.

만약 네트워크 지도에서 어떤 컴퓨터 이름을 오른쪽 클릭하면, 원격컴퓨터에서 작동할 수 있는 모든 관리 작업들이 보일 것입니다.

- 이 컴퓨터 등록하기
- 비밀번호 설정하기
- 검사작업 실행
- 이 컴퓨터에 관한 문제 고치기
- 이 컴퓨터의 이력을 보이기
- 지금 이 컴퓨터 상에서 업데이트 실행
- 프로필 적용
- 이 컴퓨터에 대한 시스템조정 실행



■ 이 컴퓨터를 이 네트워크의 업데이트 서버로 설정하십시오

특정 컴퓨터 상에서 작업을 실행하기 전에, 여러분은 지역의 가정용 관리 비밀번호를 제공하도록 요구받을 것입니다.

비밀번호를 입력하십시오.

가정용 관리비밀번호를 입력하고 OK를 클릭하십시오.



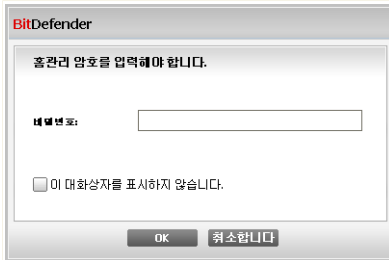
참고

만약 여러분이 몇몇 작업들을 실행할 계획이라면, 여러분은 이 세션에서 이 메시지 다시 보이지 않기를 선택하실 것입니다. 이 선택사항을 선택함으로써, 여러분은 현재 세션에서는 이 비밀번호를 다시 요구받지 않을 것입니다.

10.1.4. 모든 컴퓨터들 검사하기

모든 관리되는 컴퓨터들을 검사하려면 이 단계들을 따르십시오:

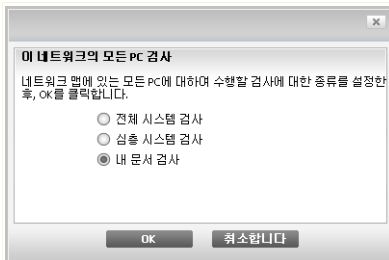
1. 모두 검사 여러분은 지역의 가정용 네트워크 관리비밀번호를 제공하도록 요구받을 것입니다.



비밀번호를 입력하십시오.

2. 검사유형을 선택하십시오.

- 전체 시스템검사 — 여러분 컴퓨터에 대한 전체검사를 시작합니다(자료보관소 제외).
- 심층검사 — 여러분 컴퓨터에 대한 전체검사를 시작합니다(자료보관소 포함).
- 내 문서 검사 — 여러분의 문서들과 설정들에 대한 빠른 검사를 시작합니다.



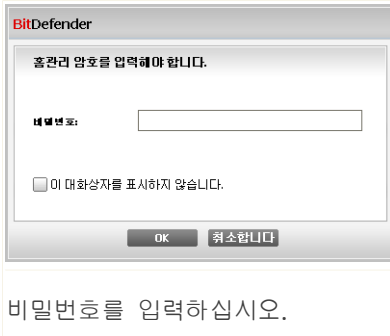
검사유형 선택

3. 확인을 클릭하십시오.

10.1.5. 모든 컴퓨터들 업데이트하기

모든 관리되는 컴퓨터들을 업데이트하려면, 이 단계들을 따르십시오:

1. 모두 업데이트를 클릭하십시오. 여러분은 지역의 가정용 네트워크 관리비밀번호를 제공하도록 요구받을 것입니다.



BitDefender

호환성 암호를 입력해야 합니다.

비밀번호:

☐ 이 대화상자를 표시하지 않습니다.

OK 취소합니다

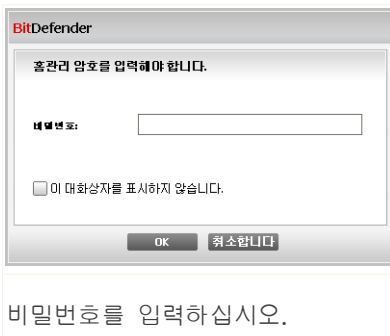
비밀번호를 입력하십시오.

2. 확인을 클릭하십시오.

10.1.6. 모든 컴퓨터 등록

모든 관리되는 컴퓨터들을 등록하려면, 이 단계들을 따르십시오:

1. 모두 등록을 클릭하십시오. 여러분은 지역의 가정용 네트워크 관리비밀번호를 제공하도록 요구받을 것입니다.



BitDefender

호환성 암호를 입력해야 합니다.

비밀번호:

☐ 이 대화상자를 표시하지 않습니다.

OK 취소합니다

비밀번호를 입력하십시오.

2. 여러분이 등록할 때 사용하기 원하시는 번호를 입력하십시오.



PC 등록

등록할 키를 입력하십시오.

라이선스 키 입력:

OK 취소합니다

모두 등록

3. 확인을 클릭하십시오.



11. 기본 설정들

기본설정모듈은 중요한 보안모듈들을 쉽게 가동 혹은 해제할 수 있는 곳입니다.
기본설정모듈로 들어가려면, 기본보기 상단의 설정을 클릭하십시오.



기본 설정들

사용할 수 있는 보안 모듈들은 몇몇 분류들로 나뉘어져 있습니다.

분류	설명
지역보안	여기는 실시간 파일 보호 혹은 자동 업데이트를 가동 / 해제할 수 있는 곳입니다.
온라인 보안	여기는 실시간 메일 및 웹 보호를 가동 / 해제할 수 있는 곳입니다.
일반설정들	여기는 게임모드, 랩탑모드, 비밀번호, 검사활동막대 등을 가동 / 해제할 수 있는 곳입니다.

카테고리를 열려면 “+” 표시되어 있는 상자를, 닫으려면 “-” 표시되어 있는 상자를 클릭하십시오.



11.1. 지역보안

여러분은 한 번의 클릭으로 보안모듈들을 가동/해제할 수 있습니다.

보안모듈	설명
실시간 바이러스차단 & 엡탐프로그램 차단 파일보호	실시간 파일보호는 여러분들 혹은 이 시스템에서 실행되는 어떤 응용소프트웨어가 접근할 때 모든 파일들이 검사되게 합니다.
자동업데이트	자동업데이트는 최신 비트펜더 제품 및 서명 파일들이 주기적으로 자동으로 설치되게 합니다.
자동 취약성 확인	자동취약성확인은 여러분 PC상의 중요한 소프트웨어들이 최신 업데이트되어 있게 합니다.

11.2. 온라인 보안

여러분은 한 번의 클릭으로 보안모듈들을 가동/해제할 수 있습니다.

보안모듈	설명
실시간 개인정보불법수집차단 웹 보호	실시간 웹 개인정보불법수집차단 보호는 개인정보불법수집 시도가 있는지 HTTP를 통해 내림받는 모든 파일들이 검사되게 합니다.
신분제어	신분제어는 어떤 특정 문자열이 있는지 모든 웹 및 메일 교통을 검사해서 기밀 데이터를 안전하게 하는데 도움을 줍니다.
메신저 암호화	만약 여러분의 메신저 연락처들에 비트펜더 2009가 설치되어 있다면, 야후! 메신저 및 윈도 라이브 메신저를 통한 모든 메신저 문자대화들이 암호화될 것입니다.

11.3. 일반설정들

여러분은 한 번의 클릭으로 보안관련 항목들을 가동/해제할 수 있습니다.



항목	설명
게임모드	게임모드는 게임이 진행되는 동안 시스템 성능에 미치는 영향을 최소화하도록 보호설정들을 임시로 변경합니다.
랩탑모드	랩탑모드는 여러분 랩탑배터리의 수명에 미치는 영향을 최소화하도록 보호설정들을 임시로 변경합니다.
설정 비밀번호	이는 오직 이 비밀번호를 아는 사람만 비트펜더 설정들을 변경할 수 있게 합니다.
비트펜더 소식	이 선택사양을 가동함으로써, 여러분은 비트펜더로부터 중요한 회사소식, 제품업데이트 혹은 새 보안위협들에 관한 정보를 받으실 것입니다.
제품들 통지 경고	이 선택사양을 가동함으로써, 여러분은 정보경고들을 받을 것입니다.
활동막대검사	검사활동막대는 비트펜더 검사활동 과정을 가리키는 작고 투명한 막대입니다. 녹색의 흐르는 선은 여러분의 지역 시스템 상의 검사활동을 보여줍니다. 빨간색의 흐르는 선은 여러분의 인터넷 연결 상의 검사활동을 보여줍니다.
시작 시 비트펜더 올리기	이 선택사양을 가동하면, 시작 시 비트펜더 사용자 인터페이스가 올려집니다. 이 선택사양은 보호수준에는 영향을 미치지 않습니다.
바이러스 보고서 보내기	이 선택사양을 가동하면, 분석을 위해 바이러스 검사보고들이 비트펜더 실험실로 보내집니다. 이 보고들에는 여러분의 성명이나 IP주소와 같은 어떤 기밀데이터도 포함되지 않으며 또한 그런 데이터가 상업목적으로 사용되지도 않을 것임을 숙지하시기 바랍니다.
출현탐지	이 선택사양을 가동함으로써, 바이러스 발생가능성과 관련된 보고서들이 분석을 위해 비트펜더 실험실로 보내집니다. 이 보고들에는 여러분의 성명이나 IP주소와 같은 어떤 기밀데이터도 포함되지 않으며 또한 그런 데이터가 상업목적으로 사용되지도 않을 것임을 숙지하시기 바랍니다.



12. 상태막대

쉽게 찾으실 수 있듯, 비트펜더 바이러스차단 2009 상단에 미결문제들의 수를 보이는 상태막대가 있습니다. 여러분 컴퓨터 보안에 대한 모든 위협들을 쉽게 제거하기 위해 모든 문제해결하기를 클릭하십시오. 보안상태창이 나타날 것입니다.

보안상태는 여러분 컴퓨터 상의 보안취약성들에 대한 체계적으로 구성되어 쉽게 관리할 수 있는 목록을 보여줍니다. 비트펜더 바이러스차단 2009는 어떤 문제가 여러분 컴퓨터 보안에 영향을 줄 수 있을 때마다 여러분에게 알려줄 것입니다.



상태막대

12.1. 지역보안

저희는 어떤 문제가 여러분의 컴퓨터 보안에 영향을 줄 수 있을 때마다 알려주는 것이 중요하다는 것을 알고 있습니다. 각 보안모듈들을 감시함으로써, 비트펜더 바이러스차단 2009는 언제 여러분이 여러분의 컴퓨터의 보안에 영향을 줄 수 있는 설정들을 할 수 있는지 뿐 아니라 여러분이 중요한 작업을 잊어버렸을 때도 여러분에게 알려줍니다.



지역보안에 관한 문제들은 매우 명시적인 문장으로 설명됩니다. 각 문장과 관련하여, 여러분 컴퓨터의 보안에 영향을 줄 수 있는 것이 있으면, 고치기라고 불리는 빨간 상태 버튼이 보일 것입니다. 그렇지 않을 경우, 녹색의 OK 상태버튼이 나타납니다.

문제	설명
실시간 파일보호가 가동되었습니다	여러분 혹은 이 시스템 상에 실행되고 있는 한 응용소프트웨어가 접근해서 모든 파일을 검사하게 합니다.
여러분은 오늘 악성 소프트웨어가 있는지 여러분의 컴퓨터를 검사했습니다	여러분 컴퓨터에 저장된 파일들에 악성소프트웨어가 없는지 확인하기 위해 되도록 빨리 주문형 검사를 실행하도록 권장합니다.
자동업데이트가 가동되었습니다	여러분의 비트펜더 제품에 대한 악성프로그램 서명들이 정기적으로 업데이트되도록 자동업데이트가 가동된 상태로 두십시오.
지금 업데이트하기	제품 및 악성프로그램 서명들의 업데이트가 실행 중입니다.

상태버튼들이 녹색일 때에는 여러분 시스템의 보안위험이 최소수준에 있습니다. 버튼들을 녹색으로 바꾸시려면, 이 단계들을 따르십시오:

1. 보안취약성들을 하나씩 고치려면 고치기 버튼들을 클릭하십시오.
2. 한 문제가 즉석에서 고쳐지지 않으면, 이 문제를 고치기 위해 마법사를 따르십시오.

어떤 문제를 감시에서 제외하기 원하실 경우, 예, 이 구성요소를 감시해 주세요 체크박스를 제거하기만 하면 됩니다.

12.2. 온라인 보안

온라인 보안 관련 문제들은 매우 명시적인 문장들로 설명되어 있습니다. 각 문장에서, 만약 여러분 컴퓨터의 보안에 영향을 줄 수 있는 것이 있는 경우, 고치기라고 불리는 빨간상태버튼이 보일 것입니다. 그렇지 않을 경우, 녹색의 OK 상태버튼이 나타납니다.



문제	설명
메신저에 대한 문자 대화 암호화가 가동되어 있습니다	여러분의 메신저 연락처들에게 비트펜더 2009가 설치되어 있으면, 야후!메신저 및 윈도우즈 라이브 메신저를 통한 모든 논의는 암호화될 것입니다. 여러분의 메신저 문자대화가 사생활보호를 받을 수 있도록 메신저에 대한 대화 암호화가 가동된 상태로 두도록 권장합니다.
파이어폭스 개인정보불법수집 차단 보호가 가동되어 있습니다	비트펜더는 여러분이 인터넷을 항해하시는 동안 개인정보불법수집 시도로부터 여러분을 보호합니다.
인터넷익스플로러 개인정보불법수집 차단 보호가 가동되어 있습니다	비트펜더는 여러분이 인터넷을 항해하시는 동안 개인정보불법수집 시도로부터 여러분을 보호합니다.

상태버튼들이 녹색일 때에는 여러분 시스템의 보안위험이 최소수준에 있습니다. 버튼들을 녹색으로 바꾸시려면, 이 단계들을 따르십시오:

1. 보안취약성들을 하나씩 고치려면 고치기 버튼들을 클릭하십시오.
2. 한 문제가 즉석에서 고쳐지지 않으면, 이 문제를 고치기 위해 마법사를 따르십시오.

어떤 문제를 감시에서 제외하기 원하실 경우, 예, 이 구성요소를 감시해 주세요 체크박스를 제거하기만 하면 됩니다.

12.3. 취약성 검사

취약성들과 관련된 문제들은 매우 명시적인 문장으로 설명되어 있습니다. 각 문장에서, 만약 여러분 컴퓨터의 보안에 영향을 주는 것이 있으면, 고치기라고 불리는 빨간 상태버튼이 보일 것입니다. 그렇지 않을 경우, 녹색의 OK 상태버튼이 나타납니다.

문제	설명
취약성 확인이 가동되어 있습니다.	여러분의 운영체계가 업데이트된 상태에 있으며 비밀번호가 취약하지 않게 하기 위해 마이크로소프트 윈도우즈 업데이트



문제	설명
	트, 마이크로소프트 윈도우 오피스 업데이트 및 마이크로소프트 윈도우 계정들의 비밀번호들을 감사합니다.
중요 마이크로소프트 업데이트들	사용할 수 있는 중요 마이크로소프트 업데이트들을 설치하십시오.
기타 마이크로소프트 업데이트들	사용할 수 있는 중요하지 않은 마이크로소프트 업데이트들을 설치하십시오.
윈도 자동 업데이트가 가동되어 있습니다	새 윈도우즈 보안 업데이트들이 나오는 즉시 그 업데이트들을 설치하십시오.
관리자 (강력한 비밀번호)	특정 사용자에게 대한 비밀번호의 유효성을 가리킵니다.

상태버튼들이 녹색일 때에는 여러분 시스템의 보안위험이 최소수준에 있습니다. 버튼을 녹색으로 바꾸시려면, 이 단계들을 따르십시오:

1. 보안취약성들을 하나씩 고치려면 고치기 버튼들을 클릭하십시오.
2. 한 문제가 즉석에서 고쳐지지 않으면, 이 문제를 고치기 위해 마법사를 따르십시오.

어떤 문제를 감시에서 제외하기 원하실 경우, 예, 이 구성요소를 감시해 주세요 체크박스를 제거하기만 하면 됩니다.



13. 등록

빗디펜더 바이러스차단 2009는 30일 시험기간이 주어집니다. 만약 빗디펜더 바이러스차단 2009를 등록하거나, 면허번호를 변경하거나 혹은 빗디펜더 계정을 생성하기 원하실 경우, 빗디펜더 창 하단에 위치한 등록하기 링크를 클릭하십시오. 등록마법사가 나타날 것입니다.

13.1. 1/1 단계 — 빗디펜더 바이러스차단 2009를 등록합니다.

BitDefender Antivirus 2009

등록 마법사

BitDefender 제품 등록을 하려면 다음의 지시 사항에 따라 주십시오.

현재 사용자 BitDefender 라이선스 키 상태: 시험

현재 BitDefender 라이선스 키: 704BE277EF7785580DF8

라이선스 키 잔여일: 30 일

라이선스 옵션

현재 키를 유지하시려면, 첫 번째 옵션을 선택하시기 바랍니다. 새로운 키를 추가하시려면, 두 번째 옵션을 선택하고, 하단의 난에 키를 입력하십시오.

☒ 현재 키를 계속 사용합니다.
 ☐ 제품을 신규 라이선스 키로 등록합니다.

라이선스 키 입력

라이선스 키 구매

라이선스 키를 구입하시려면, 하단의 링크를 클릭하십시오.

BitDefender 라이선스 키 옵션

사용자의 라이선스 키:

1) CD-Rom 라벨

2) 제품 등록 카드

3) 온라인 구입 이메일

귀하의 BitDefender 제품을 등록하시려면 본 페이지를 통해 이동하시기 바랍니다.

bitdefender

마침

취소합니다

등록

여러분은 빗디펜더 등록상태, 현재 면허 비밀번호 및 면허가 만기될 때까지 며칠이 남았는지를 볼 수 있습니다.

빗디펜더 바이러스차단 2009를 등록하려면:

등록

82



1. 새 비밀번호를 사용해 제품을 등록하기 원합니다를 선택하십시오.
2. 편집 필드에 면허번호를 입력하십시오.



참고

여러분의 면허번호를 다음에서 찾을 수 있습니다.

- CD라벨 위
- 제품등록카드 위
- 온라인 구매 이메일 내

빗디펜더 면허번호가 없으시면, 제시된 링크를 클릭해서 빗디펜더 온라인 매장에서 하나를 구입하십시오.

완료를 클릭하십시오.



14. 이력

빗디펜더 보안센터 창 하단의 이력 링크는 빗디펜더 이력 & 사건들이 있는 또다른 창을 엽니다. 이 창은 여러분에게 보안관련 사건들에 대한 개요를 제공합니다. 예를 들면, 여러분은 업데이트가 성공적으로 수행되었는지 혹은 여러분 컴퓨터 등에서 악성소프트웨어가 발견되었는지 쉽게 확인할 수 있습니다.

BitDefender Antivirus 2009

로그 & 이벤트 모듈

바이러스차단

조치 이름	취해진 조치	날짜와 시간
실시간 보호	가동 중	2009-02-02 오후 12:41:08
B-HAVE 검사도구	가동 중	2009-02-02 오후 12:41:08
실시간 보호	해제	2009-02-02 오후 12:40:58
실시간 보호	가동 중	2009-02-02 오후 12:38:35
실시간 보호	해제	2009-02-02 오후 12:35:29
실시간 보호	가동 중	2009-02-02 오후 12:26:50
실시간 보호	해제	2009-02-02 오후 12:26:50
실시간 보호	가동 중	2009-02-02 오후 12:26:17
실시간 보호	해제	2009-02-02 오후 12:26:08

사용자 작업

조치 이름	작업 이름	날짜와 시간
검사가 완료되었습니다	내문서	2009-02-02 오후 12:44:46
검사가 완료되었습니다	3543	2009-02-02 오후 12:37:38
검사가 완료되었습니다	3543	2009-02-02 오후 12:37:10
검사가 완료되었습니다	3543	2009-02-02 오후 12:36:44
검사가 완료되었습니다	3543	2009-02-02 오후 12:36:12
검사가 완료되었습니다	수동검사	2009-02-02 오후 12:33:36
검사가 취소되었습니다	마법사 검사 제외목록	2009-02-02 오후 12:31:19
검사가 취소되었습니다	내문서	2009-02-02 오후 12:29:46
검사가 취소되었습니다	빠른 시스템검사	2009-02-02 오후 12:29:37

BitDefender 사용자 인터페이스에서 제공하는 개별 옵션에 대한 설명을 위해서는 항위로 마우스 커서를 이동하십시오. 관련된 도움말 문장이 표시됩니다.

bitdefender 로그 삭제 리프래시 Ok

사건로그

여러분이 빗디펜더 이력 & 사건들을 여과하는데 도움을 주기 위해 왼쪽에 다음 분류들이 주어 습니다:

- 바이러스차단
- 개인정보보호제어
- 업데이트
- 네트워크



각 분류에 대해 여러 사건들이 있습니다. 각 사건에는 그 사건이 일어났을 때 비트디펜더가 이 사건에 관해 취한 조치, 및 날짜와 시간에 관한 정보가 있습니다. 목록에 나타난 특정 사건에 관해 더 많은 정보를 찾고 싶으실 경우, 그 사건을 더블 클릭하십시오.

오래된 로그들을 제거하려면 로그지우기를, 최신 로그가 나타나게 하려면 새로 고침을 클릭하십시오.



상세 관리



15. 일반사항

일반모듈은 비트펜더 활동 및 시스템에 관한 정보를 제공합니다. 여기서, 여러분은 비트펜더의 전반적 거동을 바꿀 수도 있습니다.

15.1. 계기반

제품활동통계 및 여러분의 등록상태를 보시려면, 상세보기 내의 일반사항>계기판으로 가십시오.

BitDefender AntiVirus 2009 - 시험 [기분모드 보기]

상태: 3개의 보류된 매수가 있습니다. [모든 매수 처리]

일반사항 | 설정들 | 시스템 정보

통계

검사 파일:	68110
치료 파일:	0
탐지된 감염된 파일들:	0
최근 검사:	절대 아님
다음검사:	절대 아님

개요

마지막 업데이트: 절대 아님

내 계정: testare.automata@mailinator.com

등록상태: 시험

~에 만료됨 [Progress Bar]

30 일

파일상태

네트워크 모듈이 BitDefender 홈 네트워크 구조를 표시합니다. (홈네트워크가 구성되지 않은 경우 회색으로 표시됩니다). 사용자 홈네트워크 생성을 시작하려면 '연결/생성 네트워크'를 클릭하십시오.

bitdefender 구매/경선 - 내 계정 - 등록 - 도움말 - 지원 - 히스토리

계기반

계기판은 다음과 같은 몇몇 영역들로 이루어져 있습니다:

- 통계 - 비트펜더 활동에 관한 중요한 정보를 보여줍니다.



- 개요 — 업데이트 상태, 여러분 계정상태, 등록 및 면허정보를 보여줍니다.
- 파일영역 — 비트펜더 악성소프트웨어차단에 의해 검사하는 대상들의 수의 추이를 가리킵니다. 막대의 높이는 그 시간 간격 동안의 교통의 강도를 가리킵니다.

15.1.1. 통계

만약 비트펜더 활동을 유심히 살피기 원하실 경우, 관찰을 시작할 좋은 곳은 통계 영역입니다. 여러분은 다음 항목들을 볼 수 있습니다:

항목	설명
검사한 파일들	여러분의 마지막 검사 시 악성소프트웨어가 있는지 확인한 파일 수를 가리킵니다.
치료된 파일들	여러분의 마지막 검사 시 감염되지 않았던 파일들의 수를 가리킵니다.
탐지된 바이러스들	여러분의 마지막 검사 시 여러분 시스템에서 찾아진 바이러스의 수를 가리킵니다.

15.1.2. 개요

여기는 업데이트 상태, 여러분의 계정 상태, 등록 및 면허정보에 관한 통계들의 요약 볼 수 있는 곳입니다.

항목	설명
최신 업데이트	여러분의 비트펜더 제품이 마지막으로 업데이트된 날짜를 가리킵니다. 시스템이 완전히 보호되도록 정기적으로 업데이트를 실행하십시오.
내 계정	여러분의 잃어버린 비트펜더 면허번호를 찾고 비트펜더 지원 및 기타 맞춤형 서비스들의 혜택을 얻기 위해 여러분의 온라인 계좌로 접속하는데 사용할 수 있는 이메일 주소를 가리킵니다.
등록	여러분의 면허번호 형태 및 상태를 가리킵니다. 여러분의 시스템을 안전하게 유지하려면 여러분 번호의 유효기간



항목	설명
유효기간:	이 지났을 때 비트펜더를 갱신 혹은 업데이트해야 합니다. 면허번호의 유효기간이 지날 때까지 남은 날 수를 가리킵니다.

15.2. 설정들

비트펜더에 대한 일반설정을 하고 그 설정을 관리하려면, 상세보기 내의 일반>설정들로 가십시오.

BitDefender AntiVirus 2009 - 시험

기본모드 보기

상태: 3개의 보류된 미슈가 있습니다.

모든 미슈 처리

대쉬보드

설정들

시스템 정보

일반사항

바이러스차단

개인정보 보호

위악점 분석

암호화

게임/노트북 모드

네트워크

업데이트

등록

일반 설정들

제품 설정에 패스워드 보안 활성화

☒ BitDefender 뉴스 포시(보안관련 정보)

☒ 팝업창(화면 고정) 보기

☒ 고급 보기에서 팝업을 표시합니다.
☐ 기본 보기에서 팝업을 표시합니다.

☒ 윈도우 시작시 BitDefender 로드

☒ 검사 활동 바 활성화(제품 활동에 대한 화면 그래프)

바이러스 보고서 설정

☒ 바이러스 리포트 전송

☒ BitDefender 출현 검지를 활성화시킵니다.

제품 설정에 대한 접근 차단용 암호를 설정합니다.

구매/경신 · 내 계정 · 등록 · 도움말 · 지원 · 히스토리

일반설정들



여기에서 BitDefender의 전반적 행동을 설정할 수 있습니다. BitDefender는 윈도우 시작 시 로드되어 태스크 바에서 최소화된 상태로 가동되도록 초기설정 되어 있습니다.

15.2.1. 일반설정들

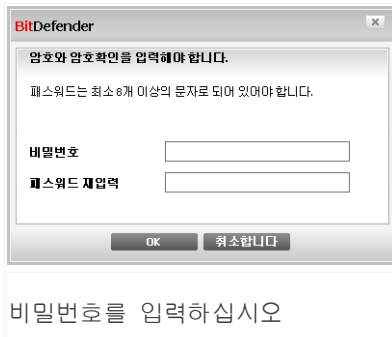
- 제품설정들에 대한 비밀번호 보호 가동 — 비트펜더 설정을 보호하기 위해 비밀번호 설정을 가동합니다.



참고

만약 여러분이 이 컴퓨터 사용에 대한 관리권을 가진 유일한 사람이 아니라면, 비밀번호를 사용해 여러분의 비트펜더 설정들을 보호하시기를 권장합니다.

이 선택사항을 선택하시면, 다음 창이 나타납니다:



BitDefender

암호와 암호확인을 입력해야 합니다.

패스워드는 최소 8개 이상의 문자로 되어 있어야 합니다.

비밀번호

패스워드 재입력

OK 취소합니다

비밀번호를 입력하십시오

비밀번호 칸에 비밀번호를 입력하고, 비밀번호 재입력 칸에 다시 입력한 후, OK를 클릭하십시오.

비밀번호를 설정했으면, 여러분은 비트펜더 설정을 변경하고자 할 때마다 이 비밀번호를 요구받을 것입니다. (있는 경우) 다른 시스템 관리자들도 비트펜더 설정들을 변경하려면 이 비밀번호를 제시해야 할 것입니다.



중요

패스워드를 분실한 경우, 사용자는 BitDefender 환경 설정 변경을 위해 제품을 교정해야 합니다.

- 비트펜더 소식보이기 (보안관련 통지들) — 가끔씩 비트펜더 서버에서 보낸 바이러스출현 관련 보안통지들을 보여줍니다.
- 팝업창 보이기 (즉석 공지들) — 제품상태에 관련된 팝업창들을 보여줍니다. 기본모드 보기 또는 고급모드 보기를 사용하는 경우에만 BitDefender 팝업을 설정할 수 있습니다.



- 윈도 시작 시 비트펜더 올리기 - 시스템 시작 시 자동으로 비트펜더를 올립니다. 이 선택사항의 사용을 권장합니다.
- (제품활동 그래프 상의) 검사활동막대 가동하기 - 여러분이 창들 안으로 로그인할 때마다 **검사활동막대**를 보여줍니다. 검사활동막대가 더 이상 보이지 않게 하기 원하실 경우 이 체크상자를 해제하십시오.



참고

이 선택사항은 현재 창 사용자 계정에 대해서만 설정될 수 있습니다.

15.2.2. 바이러스 보고서 설정들

- 바이러스 보고서 전송 - 사용자의 컴퓨터에서 확인된 바이러스에 관한 보고서를 BitDefender 연구소로 전송합니다. 이는 바이러스 출몰의 경로를 파악하는 데 도움이 됩니다.

보고서에는 사용자명, IP 주소 등과 같은 비밀 데이터는 포함되지 않으며, 상업적으로도 사용되지 않을 것입니다. 제공된 정보에는 단지 바이러스 명만이 포함될 것이며, 통계 보고서 작성을 위해서만 사용될 것입니다.

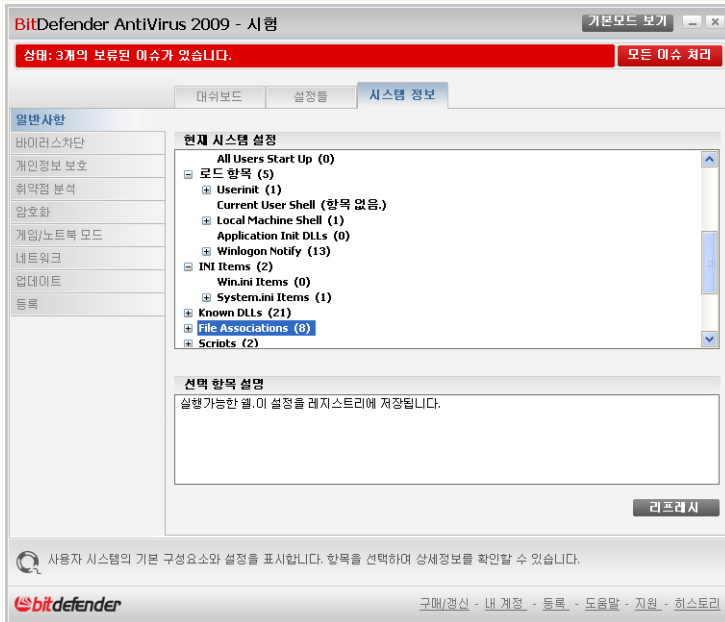
- 비트펜더 출현탐지 가동 - 비트펜더 연구소에 바이러스출현 관련 보고서들을 보냅니다.

보고서들에는 여러분의 성명, IP주소 등 기밀데이터는 포함되지 않을 것이며, 여러분 정보는 상업목적으로 사용되지 않을 것입니다. 제공되는 정보는 바이러스 가능성에 관한 정보만 포함되며 오직 새 바이러스 탐지 목적에만 사용됩니다.

15.3. 시스템 정보

비트펜더는 한 곳에서 시작시에 실행되도록 등록된 모든 시스템 설정과 응용소프트웨어들을 볼 수 있게 합니다. 이런 식으로 여러분은 시스템 감염가능성 뿐 아니라 시스템과 여기에 설치된 응용소프트웨어들의 활동을 감시할 수 있습니다.

시스템 정보를 얻으시려면, 상세 보기 내의 일반>시스템 정보로 가십시오.



시스템 정보

이 리스트에는 시스템 시작 시 로드되는 모든 항목과 다양한 어플리케이션에 의해 로드되는 항목이 포함됩니다.

다음의 세 가지 버튼을 사용할 수 있습니다:

- 복구 - 현재 파일상태를 기본값으로 변경합니다. 파일 연합 설정들에 대해서만 이용가능!
- 가기 - 선택된 항목이 있는 창을 엽니다(예, 레지스트리)



참고

선택된 항목에 따라, 가기 버튼이 나타나지 않을 수 있습니다.

- 새로고침 - 시스템 정보 영역을 다시 엽니다.



16. 바이러스차단

빗디펜더는 바이러스, 트로이목마, 염탐프로그램, 관리권 편취 프로그램 등 모든 종류의 악성소프트웨어로부터 여러분의 컴퓨터를 보호합니다. 빗디펜더가 제공하는 보호는 다음과 같이 두 분류로 나뉩니다:

- **실시간 보호** — 새 악성소프트웨어 위협들이 여러분의 시스템에 들어가지 못하도록 보호합니다. 예를 들면, 빗디펜더는 알려진 위협들은 없는지 찾기 위해 여러분이 어떤 워드 문서를 열 때에 이 문서를 검사하고, 어떤 이메일을 받을 때에 이메일도 합니다.



참고

실시간 보호는 또한 접속에 따른 검사라고도 불리며, 사용자들이 파일에 접근할 때 파일들을 검사합니다.

- **주문형 검사** — 시스템 내에 이미 존재하는 악성소프트웨어를 탐지 및 제거할 수 있게 합니다. 이것은 사용자가 실행하는 기본 검사로서, 빗디펜더가 검사할 드라이브, 폴더 혹은 파일을 여러분이 선택합니다. 빗디펜더는 그 대상을 주문식으로 검사합니다. 검사 작업들은 맞춤형 검사절차들을 생성할 수 있게 하며, 이 절차들은 주기적으로 실행되도록 예약할 수 있습니다.

16.1. 실시간 보호

빗디펜더는 ICQ, 넷미팅, 야후메신저 및 MSN메신저 등 인스턴트 메시지 소프트웨어 응용프로그램들을 통해 모든 파일, 이메일 메시지 및 통신을 검사하면서 연속적, 실시간 보호를 제공합니다. 빗디펜더 개인정보불법수집차단은 개인정보불법수집 가능성 있는 웹페이지들에 관해 여러분에게 경고를 줌으로써 여러분이 인터넷을 하는 동안 여러분의 개인정보노출을 방지합니다.

실시간 보호 및 빗디펜더 개인정보불법수집차단을 설정하려면, 상세보기 내의 바이러스 차단 >로 가십시오.



실시간 보호

여러분은 실시간 보호가 가동되었는지 혹은 해제되었는지 볼 수 있습니다. 만약 실시간 보호상태를 변경하기 원하실 경우, 해당 체크박스를 선택하십시오.



중요

여러분의 컴퓨터를 바이러스로부터 보호하기 원하실 경우, 실시간 보호를 가동해 두십시오.

빠른 시스템 검사를 시작하려면, 지금 검사를 클릭하십시오.

16.1.1. 보호수준 설정하기

여러분은 여러분의 보안필요성에 더 적합한 보호수준을 선택할 수 있습니다. 적합한 보호수준에 맞추기 위해 눈금을 따라 미끄럼설정자를 끌어당기십시오.

보호수준에는 다음과 같이 3단계의 수준이 있습니다:



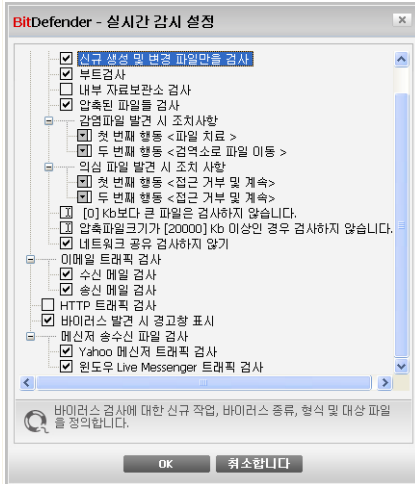
보호수준	설명
낮음	기본 보안필요성을 충족합니다. 자원소비수준이 매우 낮습니다. 프로그램들과 수신메일메시지들은 바이러스에 대해서만 검사됩니다. 전통적 서명 기반 검사 외에, 발견적 분석도 사용됩니다. 감염된 파일들에 취해진 조치들은 다음과 같습니다: 파일청소/접근거부
기본	표준보안을 제공합니다. 자원소비수준은 낮습니다. 바이러스 및 악성소프트웨어가 있는지 모든 파일과 수신&발신 메일메시지들을 검사합니다. 전통적 서명기반 검사 외에도, 발견적 분석도 사용됩니다. 감염된 파일들에 취한 조치들은 다음과 같습니다: 파일청소/접근거부
높음	높은 수준의 보안을 제공합니다. 자원소비수준은 보통입니다. 바이러스와 악성소프트웨어가 있는지 모든 파일, 수신&발신 메일메시지들 및 웹교통을 검사합니다. 전통적 서명기반 검사 외에, 발견적 분석도 사용됩니다. 감염된 파일들에 취해진 조치들은 다음과 같습니다: 파일청소/접근거부

기본 실시간 보호설정을 적용하려면, 기본 수준을 클릭하십시오.

16.1.2. 보호수준 맞추기

고급사용자들은 비트디펜더가 제공하는 검사설정들을 마음껏 활용하길 원할 것입니다. 검사기는 특정 악성소프트웨어 위협을 검색하거나 자료보관소를 건너뛰기 위해 오직 특정 파일확장자들만 검사하도록 설정할 수 있습니다. 이는 검사시간을 현격히 줄이고 검사하는 동안의 여러분의 컴퓨터의 반응성을 향상시킬 것입니다.

수준맞추기를 클릭해서 실시간 보호를 맞춤형으로 설정할 수 있습니다. 다음과 같은 창이 나타날 것입니다:



보호막 설정들

검사 선택사항들은 윈도 내에서의 탐색에 사용되는 메뉴들과 매우 비슷한 펼쳐지는 메뉴로 구성됩니다. 어떤 선택사항을 열려면 “+” 마크가 있는 상자를, 선택사항을 닫으려면, “-” 마크가 있는 상자를 클릭하십시오.



참고

“+” 마크가 있더라도 해당 옵션이 선택되지 않은 상태에서는 하위 옵션을 열어서 볼 수 없습니다. 하위 옵션을 보려면 해당 옵션을 선택하십시오.

- 접근 파일 및 P2P 전송 옵션 검사 — 인스턴트 메시지 프로그램 어플리케이션 (ICQ, NetMeeting, Yahoo 메신저, MSN 메신저)을 통한 통신 및 접근 파일을 검사합니다. 검사를 원하는 파일 종류를 선택하십시오.

옵션	설명
검사되는 파일들	종류에 관계 없이 모든 접근 파일이 검사될 것입니다.
모든 파일 검사	
프로그램 파일만 검사	실행 가능한 프로그램 파일에 대해서만 검사를 수행합니다. 즉, 이 옵션은 다음 확장자명



옵션		설명
		을 가진 파일들만 검사합니다: .exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml; .nws.
	지정된 확장자 사용자 검사	사용자가 지정한 확장자로 되어 있는 파일만 검사할 것입니다. 해당 확장자는 반드시 ";"로 구분되어야 합니다.
	위험한 소프트웨어 검사	위험한 소프트웨어가 있는지 검사합니다. 탐지된 파일들은 감염된 것으로 취급됩니다. 이 선택사항이 가동되면 광고 소프트웨어 구성요소들을 포함하는 소프트웨어의 작동이 멈출 것입니다. 이런 종류의 파일들을 검사대상에서 제외하려면 전화걸기과정 검사에서 건너뛰기를 선택하십시오.
부트섹터 검사		시스템 부팅 섹션을 검사합니다.
자료보관소 내부 검사		접근하는 자료보관소를 검사합니다. 이 옵션 사용으로 컴퓨터의 성능이 다소 저하될 수 있습니다.
압축된 실행파일 검사		모든 압축된 파일을 검사합니다.
첫째 조치		드롭다운메뉴에서 감염되었거나 의심스러운 파일들에 취할 첫 조치를 선택하십시오.
	억세스 및 진행 거부	감염된 파일이 검지된 경우, 해당 파일에 대한 접근이 거부될 것입니다.
	파일치료	감염된 파일들을 치료합니다.
	파일 삭제	감염된 파일들을 어떤 경고도 없이 즉시 삭제합니다.
	검역소로 이동	감염된 파일들을 검역소 안으로 옮깁니다.



옵션	설명
둘째 조치	첫째 조치가 실패할 경우, 드롭다운메뉴로부터 감염된 파일들에 취할 둘째 조치를 선택하십시오.
엑세스 및 진행 거부	감염된 파일이 검지된 경우, 해당 파일에 대한 접근이 거부될 것입니다.
파일 삭제	감염된 파일들을 어떤 경고도 없이 즉시 삭제합니다.
검역소로 이동	감염된 파일들을 검역소 안으로 옮깁니다.
[x] Kb보다 큰 파일들 검사안함	검사하려는 파일들의 최대크기를 입력합니다. 만약 크기가 0 Kb이면, 크기에 상관없이 모든 파일들을 검사합니다.
[2,000] Kb보다 큰 자료보관소 검사안함	검사하려는 데이터보관소의 최대크기를 킬로바이트(KB)로 입력하십시오. 크기에 상관없이 모든 자료보관소를 검사하려면, '0'을 입력하십시오.
네트워크공유 검사안함	만약 이 선택사항이 가동되었으면, 비트펜더는 네트워크 접근을 빠르게 할 수 있는 네트워크공유는 검사하지 않을 것입니다. 이 선택사항은 여러분이 속한 네트워크가 바이러스 방지 솔루션으로 보호되었을 때에만 가동하도록 권장합니다.

■ 메일교통 검사 - 메일교통을 검사합니다.

다음의 옵션을 사용할 수 있습니다.

옵션	설명
수신메일 검사	모든 수신메일 메시지들을 검사합니다.
송신메일 검사	모든 송신메일 메시지들을 검사합니다.

■ http 교통 검사 - http 교통을 검사합니다.

■ 바이러스가 발견되었을 때 경고를 표시합니다 - 파일 혹은 이메일 메시지에서 바이러스를 발견했을 때, 경고 창이 열립니다.



감염된 파일의 경우, 경고창에 바이러스명, 바이러스에 대한 경로, BitDefender에서 취하는 행동, 사용자가 추가 정보를 확인할 수 있는 BitDefender 사이트로의 링크가 포함됩니다. 감염된 이메일의 경우, 경고창에 송신자와 발신자에 관한 정보가 포함되게 될 것입니다.

의심파일이 검지되는 경우, 사용자는 경고창에서 마법사를 시작할 수 있으며, 경고창은 BitDefender 연구소에 추가 분석을 위해 파일을 전송하는 데 도움을 줄 것입니다. 사용자는 본 보고서와 관련된 정보를 수신할 이메일 주소를 기입할 수 있습니다.

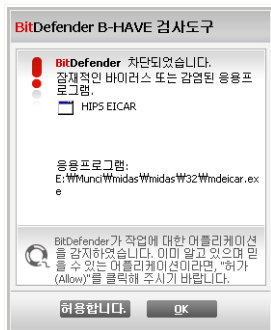
- 메신저로 송수신된 파일들을 검사합니다. 야후메신저 혹은 윈도우즈 라이브 메신저를 사용할 수신 혹은 발신하는 파일들을 검사하려면, 해당 체크상자들을 선택하십시오.

변경사항들을 저장하고 창을 닫으려면 OK를 클릭하십시오.

16.1.3. 거동검사기 설정

거동검사기는 서명이 아직 공개되지 않은 새 위협들에 대해 한 층의 보호를 제공합니다. 이것은 여러분 컴퓨터 상에 실행되고 있는 응용소프트웨어의 거동을 계속 감시 및 분석하며, 어떤 응용소프트웨어가 의심스러운 거동을 보이는지 여러분에게 경고합니다.

거동검사기는 어떤 응용소프트웨어가 잠재적 악성행동을 시도할 때마다 여러분에게 경고하고 여러분에게 조치를 요구합니다.

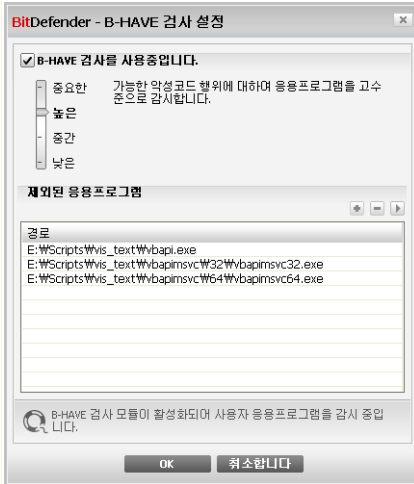


거동검사기 경고

탐지된 응용소프트웨어에 대해 잘 알고 신뢰하신다면, 허락을 클릭하십시오. 거동검사기는 더 이상 잠재적 악성행동에 대해 응용소프트웨어를 검사하지 않을 것입니다.

이 응용소프트웨어를 즉시 닫으려면, OK를 클릭하십시오.

거동검사기를 설정하려면, 검사기 설정을 클릭하십시오.



거동검사기 설정

거동검사기를 해제하기 원하시면, 거동검사기가 가동되어 있음 체크상자를 해제하십시오.



중요

알려지지 않은 바이러스로부터 보호받도록 거동검사기를 가동된 상태로 두십시오.

보호수준 설정하기

거동검사기보호수준은 새로운 실시간 보호수준을 설정할 때에 자동으로 바뀝니다. 기본설정이 마음에 들지 않으시면, 보호수준을 수동으로 설정할 수 있습니다.



참고

현재 실시간 보호수준을 바꾸시면, 거동검사기 보호수준도 그에 따라 바뀐다는 것을 기억하십시오.

여러분의 보안필요성에 가장 잘 맞는 보호수준으로 설정하기 위해 눈금을 따라 미끄럼막대를 끄십시오.



보호수준	설명
매우 높음	응용소프트웨어들은 잠재적 악성 행동들이 있는지 엄격하게 감시됩니다.
높음	응용소프트웨어들은 잠재적 악성행동들에 대해 강도높게 감시됩니다.
중간	응용소프트웨어들은 잠재적 악성행동들에 대해 적당하게 감시됩니다.
낮음	응용소프트웨어들은 잠재적 악성행동들에 대해 감시됩니다.

배제된 응용소프트웨어들 관리하기

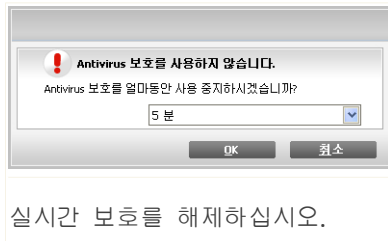
여러분은 거동검사가 특정 응용소프트웨어들은 확인하지 않도록 설정할 수 있습니다. 현재 거동검사가 확인하지 않은 응용소프트웨어들은 제외된 응용소프트웨어들 표에 나열됩니다.

제외된 응용소프트웨어들을 관리하려면, 표 상단에 있는 버튼들을 사용할 수 있습니다.

- ➕ Add — exclude a new application from scanning.
- ➖ Remove — remove an application from the list.
- ✎ Edit — edit an application path.

16.1.4. 실시간 보호 해제하기

실시간 보호 해제를 시도하면, 경고창이 나타날 것입니다.





실시간 보호를 얼마나 오래 해제상태에 둘지 메뉴에서 선택해서 여러분의 선택을 확인해야 합니다. 여러분은 실시간 보호를 5분, 15분 혹은 30분, 한 시간, 영구히 혹은 시스템이 재시작할 때까지 해제된 상태로 둘 수 있습니다.



주의

이것은 매우 중요한 보안문제입니다. 실시간 보호는 되도록 짧게 해제상태에 두도록 권장합니다. 만약 실시간 보호가 해제되어 있으면, 여러분은 악성소프트웨어 위협들로부터 보호되지 못할 것입니다.

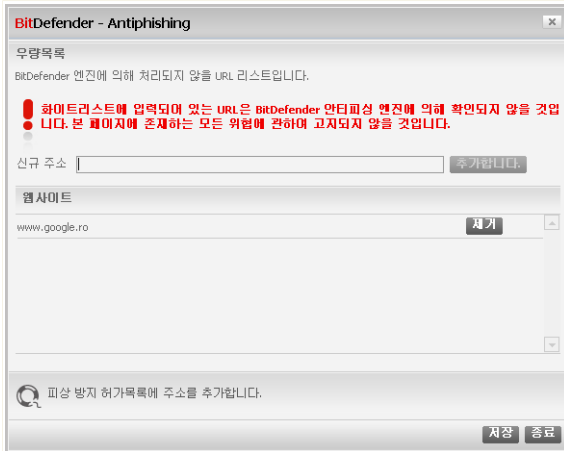
16.1.5. 개인정보불법수집차단 보호 설정

빗디펜더는 다음 대상에 대해 실시간 개인정보불법수집차단 보호를 제공합니다:

- 인터넷 익스플로러
- 모질라 파이어폭스
- 야후!메신저
- 윈도 라이브 (MSN) 메신저

여러분은 개인정보불법수집차단 보호를 완전히 혹은 특정 응용소프트웨어에 대해서만 해제하도록 선택할 수 있습니다.

여러분은 우량목록을 클릭해서 빗디펜더 개인정보불법수집차단 엔진들이 검사하지 말아야 할 한 무리의 웹사이트들을 설정 및 관리할 수 있습니다.



개인정보불법수집차단 우량목록

여러분은 비트펜더가 현재 개인정보불법수집 내용을 확인하지 않는 웹사이트들을 볼 수 있습니다.

우량목록에 어떤 새 웹사이트를 추가하려면, 새 주소 칸에 그 URL주소를 입력하고 추가를 클릭하십시오. 우량목록은 여러분이 완전히 신뢰하는 웹사이트들만 포함합니다. 예를 들면, 여러분이 현재 온라인으로 쇼핑하는 웹사이트들을 추가하십시오.



참고

여러분은 여러분의 웹브라우저에 통합된 비트펜더 개인정보불법수집차단 도구막대로부터 웹사이트들을 우량목록에 쉽게 추가할 수 있습니다.

우량목록에서 어떤 웹사이트를 제거하려면, 해당 제거 버튼을 클릭하십시오.

변경사항들을 저장하고 창을 닫으려면 닫기를 클릭하십시오.

16.2. 주문형 검사

BitDefender의 주요 목표는 바이러스가 없는 컴퓨터를 유지하는 것입니다. 새로운 바이러스를 컴퓨터에서 제거하고, 시스템에 복제되거나 다운로드되는 모든 신규



파일 및 이메일 메시지를 검사함으로써 1차적으로 그리고 주요하게 이루어지는 것입니다.

BitDefender를 설치하지 전에 시스템에 바이러스가 이미 존재하고 있을 위험이 있습니다. 때문에 BitDefender를 설치한 후, 컴퓨터에 존재하고 있는 바이러스를 검사하는 것이 좋습니다. 또한 자주 컴퓨터의 바이러스 존재 여부 검사를 시행하는 것이 좋습니다.

주문형 검사를 설정 및 시작하려면, 상세보기 내의 바이러스 차단>검사로 가십시오.

BitDefender AntiVirus 2009 - 시형

기본모드 보기

상태: 3개의 보류된 미수가 있습니다. 모든 미수 처리

보호막 바이러스 검사 제외됨 검역

일반사항
바이러스차단
개인정보 보호
위악질 분석
암호화
게임/노트북 모드
네트워크
업데이트
등록

시스템 작업

- 선택 시스템 검사
마지막 시행: 2009-02-02 12:27:01
- 전체 시스템 검사
마지막 시행: 절대 아님
- 빠른 시스템 검사
마지막 시행: 절대 아님
- 자동로그인 검사
마지막 시행: 2008-05-09 7:16:42

사용자 작업

- 내 문서
마지막 시행: 절대 아님

기타 작업

- 문맥 검사
- 장치감지

신규 작업 선택 작업

사용자 요구에 따른 신규 작업을 정의합니다.

구매/경신 · 내 계정 · 등록 · 도움말 · 지원 · 히스토리

작업들 검사

주문형 검사는 검사작업들에 기반합니다. 검사작업들은 검사 선택사항들과 검사하려는 대상들을 지정합니다. 기본값 작업들 혹은 여러분 나름의 검사작업들(사용자 정의된 작업들)을 실행함으로써 여러분이 원할 때마다 컴퓨터를 검사할 수 있습니다. 또한 정기적으로 혹은 작업에 방해가 되지 않도록 시스템이 공회전 중일 때 작업이 실행되도록 예약할 수 있습니다.



16.2.1. 작업들 검사

비트펜더에는 흔한 보안문제들을 다루는 기본적으로 생성된 몇몇 작업들이 있습니다. 여러분은 또한 여러분 나름대로 구성된 검사작업들을 만들 수도 있습니다.

각 작업에는 그 작업을 설정하고 검사결과를 볼 수 있게 하는 속성 창이 있습니다. 추가 정보는 “**검사작업들 설정하기**” (p. 108)를 참조하십시오.

검사 작업들에는 세 가지 분류가 있습니다.

■ **시스템작업들** - 기본시스템작업들의 목록을 담고 있습니다. 다음과 같은 작업들이 있습니다:

기본 작업	설명
심층 시스템검사	전체 시스템을 검사합니다. 기본 설정에서는, 바이러스, 염탐프로그램, 광고프로그램, 관리권 편취프로그램 등 여러분 시스템 보안을 위협하는 모든 형태의 악성프로그램이 있는지 검사합니다.
전체 시스템검사	자료보관소를 제외한 전체 시스템을 검사합니다. 기본 설정에서는, 바이러스, 염탐프로그램, 광고프로그램, 관리권 편취프로그램 등 여러분 시스템 보안을 위협하는 모든 형태의 악성프로그램이 있는지 검사합니다.
빠른 시스템검사	Windows, Program Files 및 All Users 폴더들을 검사합니다. 기본설정에서는, 관리권 편취프로그램을 제외한 모든 형태의 악성소프트웨어에 대해 검사하지만, 메모리, 레지스트리 혹은 쿠키는 검사하지 않습니다.
자동로그온 검사	어떤 사용자가 윈도우즈로 로그인 할 때에 실행되는 항목들을 검사합니다. 기본적으로, 자동로그온 검사를 사용하지 않습니다. 이 작업을 사용하려면, 마우스 오른쪽 버튼클릭 후, 예약을 선택한 후, 시스템 시작 시를 실행하십시오. 프로그램 시작 후, 얼마 후에 이 작업을 시작할 것 인지를 설정합니다.(분 단위)



참고

심층시스템검사와 전체시스템감사 작업들은 전체 시스템을 분석하기 때문에, 이런 검사는 제법 시간이 걸릴 수 있습니다. 따라서, 저희는 이런 작업들은 후 순위로 혹은 더 좋은 방법은 여러분 시스템이 공회전 중일 때 실행하도록 권장합니다.

■ 사용자 작업들 - 사용자 정의된 작업들을 담고 있습니다.

내 문서라고 불리는 어떤 작업이 제공됩니다. 이 작업을 사용해 중요한 현재 사용자 폴더들인, 내 문서, 바탕화면 및 시작을 검사하십시오. 이는 여러분의 문서들의 안전과, 안전한 작업공간 및 시작시 깨끄한 응용소프트웨어 실행을 보장합니다.

■ 여러 작업들 - 한 무리의 다양한 검사작업들을 포함합니다. 이 검사작업들은 이 창에서 실행될 수 없는 대체검사 형태들을 가리킵니다. 여러분은 오직 그 설정들을 수정하거나 검사보고서들을 볼 수만 있습니다.

각 작업의 오른쪽에 다음과 같은 세 버튼들이 있습니다:

■  예약 - 선택된 작업이 나중에 실행되도록 예약되었음을 가리킵니다. 이 버튼을 클릭해서, 속성 창, **예약관리**를 열면, 작업예약을 보고 수정도 할 수 있습니다.

■  삭제 - 선택된 작업을 제거합니다.



참고

시스템 작업들에 대해서는 사용될 수 없습니다. 시스템작업을 제거할 수 없습니다.

■  지금 검사하기 - 선택된 작업을 실행해서, **즉시 검사**를 시작합니다.

각 작업의 왼쪽에, 작업을 설정하고 검사로그를 볼 수 있게 하는 속성 버튼이 보일 것입니다.

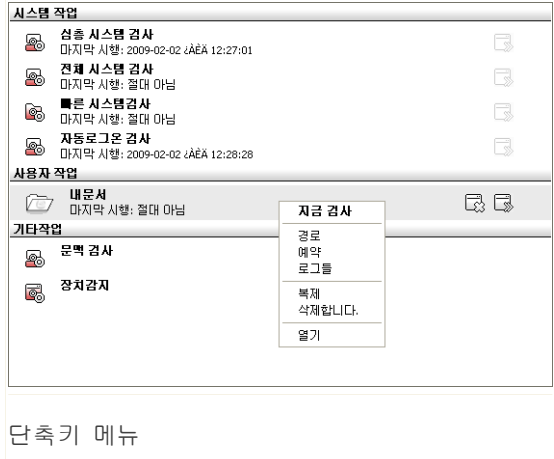


16.2.2. 단축키 메뉴 사용하기

각 작업에 대해 단축키 메뉴가 있습니다. 메뉴를 열려면 선택된 작업을 오른쪽 마우스 클릭하십시오.

다음 명령들은 단축키 메뉴에서 찾을 수 있습니다:

지금 검사하기 - 선택된 작업을 실행해서, 즉시 검사를 시작합니다.



- 경로 - 속성 창을 표시합니다. **경로** 탭에서 선택작업에 대한 검사대상을 변경할 수 있습니다.



참고

시스템작업들의 경우, 이 선택사항은 작업경로 보이기에 의해 교체되어 검사목표만 보입니다.

- 작업예약 - 속성 창, **예약관리** 탭을 열어서 선택된 작업을 예약할 수 있게 합니다.
- 로그 - 속성 창과 **로그** 탭을 엽니다. 여기에서 선택작업 실행 후 작성된 보고서를 확인할 수 있습니다.
- 복제 - 선택한 작업을 복제합니다. 작업 사본의 설정을 수정할 수 있기 때문에 이는 새 작업들을 생성할 때에 유용합니다.
- 삭제 - 선택된 작업을 삭제합니다.



참고

시스템 작업들에 대해서는 사용될 수 없습니다. 시스템작업을 제거할 수 없습니다.



■ 열기 - 속성 창을 엽니다. **Overview** 탭에서 선택된 작업의 설정을 수행할 수 있습니다.



참고

기타 작업 카테고리의 특정한 성격 때문에, 이 경우 로그와 열기 옵션만을 사용할 수 있습니다.

16.2.3. 검사작업 생성하기

검사작업을 생성하려면, 다음 방법들 중 한 가지를 사용하십시오:

- 기존 작업을 **복사**하고, 이름을 변경하고 속성 창에서 필요한 변경을 하십시오.
- 새 작업을 생성하고 설정하려면 새 작업을 클릭하십시오.

16.2.4. 검사작업들 설정하기

각 검사작업에는 검사선택사항들과 검사목표를 설정하고 작업을 예약하거나 보고서들을 볼 수 있는 각각의 속성 창이 있습니다. 이 창을 열려면, 작업 오른쪽에 위치한 열기 버튼을 클릭하거나 작업을 오른쪽 클릭 후 열기를 클릭하십시오.

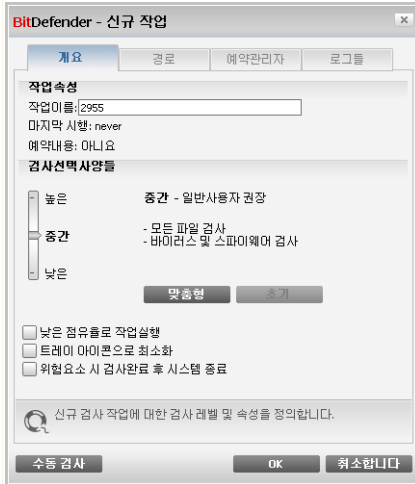


참고

로그보기와 로그 탭에 대한 추가 정보는, “**검사로그들 보기**” (p. 128)를 참조하십시오.

검사설정실행

특정 검사작업에 대한 검사선택사항들을 설정하려면, 그 작업을 오른쪽 클릭한 후 속성을 선택하십시오. 다음 창이 나타날 것입니다:



개요

여기서는 작업(이름, 마지막실행 및 예약상태)에 관한 정보를 보고 검사설정들을 실행할 수 있습니다.

검사수준 선택하기

여러분은 검사수준을 선택해서 쉽게 검사설정을 할 수 있습니다. 적합한 검사수준에 맞추기 위해 눈금을 따라 미끄럼설정자를 끌어당기십시오.

검사에는 다음과 같이 3 단계의 수준이 있습니다:

보호수준	설명
낮음	합리적 탐지효율을 제공합니다. 자원소비수준은 낮습니다. 바이러스가 있는지 프로그램들만 검사합니다. 전통적인 서명기반 검사 외에, 경험적 분석도 사용합니다.
중간	양호한 탐지효율을 제공합니다. 자원소비수준은 중간정도입니다. 바이러스 및 악성소프트웨어가 있는지 모든 파일들을 검사합니다. 기본적인 서명기반 검사 외에, 경험적인 분석도 사용합니다.



보호수준	설명
높음	높은 수준의 탐지효율을 제공합니다. 자원소비수준은 높습니다. 바이러스와 염탐프로그램이 있는지 모든 파일들과 자료보관소를 검사합니다. 기본적인 서명기반 검사 외에, 경험적 분석도 사용합니다.

검사과정에 대한 일련의 일반 선택사항들도 있습니다.

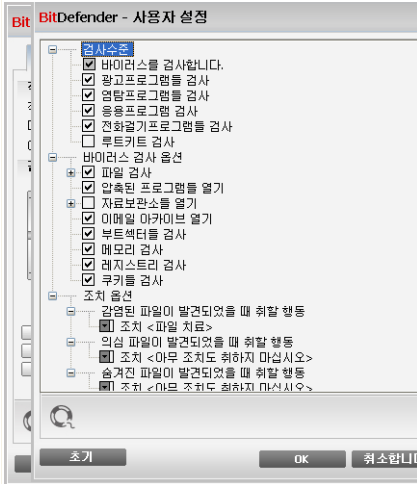
- 저 우선순위로 태스크 가동 . 검사과정의 우선순위를 낮춥니다. 사용자는 다른 프로그램을 사용하는데 지장을 받지 않고 검사를 수행할 수 있습니다. 반면 작업 소요 시간은 길어집니다.
- 시스템 트레이 시작에 대한 검사창 최소화 . 검사창을 **알림영역**으로 최소화시킵니다. 이 창을 열려면 비트펜더를 더블클릭하십시오.
- 아무 위협도 발견되지 않으면 검사완료 시 컴퓨터를 끕니다.

변경사항들을 저장하고 창을 닫으려면 OK를 클릭하십시오. 이 작업을 실행하려면, 그냥 검사를 클릭하시면 됩니다.

검사수준 맞추기

고급사용자들은 비트펜더가 제공하는 검사설정들을 마음껏 활용하길 원할 것입니다. 검사기는 특정 악성소프트웨어 위협을 검색하거나 자료보관소를 건너뛰기 위해 오직 특정 파일확장자들만 검사하도록 설정할 수 있습니다. 이는 검사시간을 현격히 줄이고 검사하는 동안의 여러분 컴퓨터의 반응성을 향상시킬 것입니다.

여러분 나름의 검사 선택사항들을 설정하려면 맞춤형을 클릭하십시오. 새 창이 나타날 것입니다.



검사설정

검사 선택사항들은 윈도우 내에서의 탐색에 사용되는 메뉴들과 매우 비슷한 펼쳐지는 메뉴로 구성됩니다. 어떤 선택사항을 열려면 “+” 마크가 있는 상자를, 선택사항을 닫으려면, “-” 마크가 있는 상자를 클릭하십시오.

이 검사선택사항들은 다음과 같이 3 분류로 나뉘어집니다:

- **검사수준.** 검사수준 분류에서 적합한 선택사항들을 선택해서 비트펜더가 검사하기 원하는 악성소프트웨어 유형을 지정하십시오.

옵션	설명
바이러스 검사	알려진 바이러스들을 검사합니다. 비트펜더는 불완전한 바이러스 개체들도 탐지하기 때문에, 여러분 시스템의 보안에 영향을 줄 수 있는 어떤 위협가능성도 모두 제거합니다.
광고프로그램 검사	광고프로그램 위협들을 검사합니다. 탐지된 파일들은 감염된 것으로 취급됩니다. 이 선택사항이 자동



옵션	설명
	되어 있으면 광고프로그램 요소를 포함하는 소프트웨어가 작동을 멈출 것입니다.
염탐프로그램 검사	알려진 염탐소프트웨어 위협들을 검사합니다. 탐지된 파일들은 감염된 것으로 취급됩니다.
응용소프트웨어 검사	악성 응용소프트웨어들을 숨기거나 다른 나쁜 목적을 위해 염탐도구로 사용될 수 있는 적법한 응용소프트웨어들을 검사합니다.
악성전화걸기프로그램 검사	고가 번호로 전화를 거는 프로그램들을 검사합니다. 탐지된 파일들은 감염된 것으로 취급됩니다. 이 선택사항이 가동되면 악성전화걸기프로그램 요소가 포함된 소프트웨어는 작동을 멈출 것입니다.
관리권편취 프로그램 검사	일반적으로 관리권 편취 프로그램으로 알려진 숨겨진 객체들(파일 및 과정)을 검사합니다.

■ 바이러스검사 선택사항. 바이러스검사 선택사항들 분류에서 적합한 선택사항들을 선택해서 검사하려는 객체들의 유형(파일형태 등)을 지정하십시오.

옵션	설명
파일 검사	모든 파일 검사 유형과 상관없이 모든 파일들을 검사합니다.
프로그램 파일만 검사	실행 가능한 프로그램 파일들만 검사합니다. 즉, 다음과 같은 확장자명을 가진 파일들만 검사합니다: exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; exe; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml; nws.
지정된 확장자 사용자 검사	사용자가 지정한 확장자로 되어 있는 파일만 검사할 것입니다. 해당 확장자는 반드시 ";"로 구분되어야 합니다.
압축된 프로그램 열기	압축된 파일 검사



옵션	설명
자료보관소 열기	자료보관소 내부를 검사합니다. 정리된 자료 파일들을 검사하면 검사하는데 걸리는 시간이 길어지고 더 많은 시스템 자원들을 필요로 합니다. 자료보관소 크기제한 칸을 클릭해서, 검사하려는 자료보관소의 최대크기를 킬로바이트(KB)로 입력할 수 있습니다.
메일 자료보관소 열기	메일 자료보관소 내부를 검사합니다.
부트 섹터 검사	시스템 부팅 섹션을 검사합니다.
검사메모리	메모리에 바이러스 및 기타 악성소프트웨어가 있는지 검사합니다.
레지스트리 검사	레지스트리 입력 사항을 검사합니다.
쿠키 검사	쿠키 파일들을 검사하십시오.

- 조치 선택사양: 조치 선택사양 분류 내의 선택사양들을 사용해, 탐지된 파일들의 각 분류에 대해 취할 조치를 지정하십시오.



참고

새 조치를 설정하려면, 현재 조치를 클릭하고 메뉴로부터 원하는 선택사양을 선택하십시오.

탐지된 감염된 파일들에 대해 취할 조치를 선택하십시오. 다음의 옵션을 사용할 수 있습니다.

행동	설명
조치 없음 (로그 객체들)	감염된 파일들에는 아무 조치도 취하지 않습니다. 이 파일들은 보고서 파일에 기록됩니다.
파일치료	탐지된 감염된 파일들로부터 악성소프트웨어 코드를 제거하십시오.
파일삭제	감염된 파일들을 어떤 경고도 없이 즉시 삭제합니다.



행동	설명
검역소로 이동	감염된 파일들을 검역소 안으로 옮깁니다. 감염된 파일들은 실행하거나 열 수 없습니다. 따라서 감염될 위험이 없어집니다.

탐지된 의심스러운 파일들에 대해 취할 조치를 선택하십시오. 다음의 옵션을 사용할 수 있습니다.

행동	설명
조치 없음 (로그 객체들)	의심스러운 파일들에 대해서는 아무 조치도 취해지지 않습니다. 이 파일들은 보고서 파일에 나타날 것입니다.
파일삭제	의심스러운 파일들을 아무 경고도 없이 즉시 삭제합니다.
검역소로 이동	의심스러운 파일들을 검역소 안으로 옮깁니다. 감염된 파일들은 실행하거나 열 수 없습니다. 따라서 감염될 위험이 없어집니다.



참고

경험적 분석에서 파일들이 의심스러운 것으로 탐지되었습니다. 이 파일들을 비트펜더 연구소로 보내시기를 권장합니다.

탐지된 숨겨진 객체들(관리권 편취)에 취할 조치를 선택하십시오. 다음의 옵션을 사용할 수 있습니다.

행동	설명
조치 없음 (로그 객체들)	숨겨진 파일들에 대해서는 아무 조치도 취해지지 않습니다. 이 파일들은 보고서 파일에 나타날 것입니다.
검역소로 이동	숨겨진 파일들을 검역소 안으로 옮깁니다. 감염된 파일들은 실행하거나 열 수 없습니다. 따라서 감염될 위험이 없어집니다.
보이게 하기	여러분이 숨겨진 파일들을 볼 수 있도록 숨겨진 파일들을 드러냅니다.



자료보관소 파일들 조치 선택사항들. 자료보관소 내 파일들에 대한 검사 및 취급은 제한을 받을 수 있습니다. 비밀번호로 보호된 자료보관소는 비밀번호를 제시하는 경우 외에는 검사할 수 없습니다. 자료보관소 양식(형태)에 따라, 비트펜더는 감염된 자료보관소 파일들을 치료, 격리 혹은 삭제할 수 없습니다. 자료보관소 파일들 조치 선택사항들 분류에서 적합한 선택사항들을 사용해, 탐지된 자료보관소 파일들에 대해 취할 조치들을 설정하십시오.

○탐지된 감염된 파일들에 대해 취할 조치를 선택하십시오. 다음의 옵션을 사용할 수 있습니다.

행동	설명
아무 조치도 안함	감염된 자료보관소 파일들의 기록은 검사로그 내에 두십시오. 검사 완료 후, 여러분은 이 파일들에 관한 정보를 보기 위해 검사로그를 열 수 있습니다.
파일치료	탐지된 감염된 파일들로부터 악성소프트웨어 코드를 제거하십시오. 감염된 파일이 특정메일 자료보관소에 있는 등 어떤 경우에는 치료가 실패할 수 있습니다.
파일삭제	아무 경고도 없이 디스크에서 감염된 파일들을 즉시 제거합니다.
검역소로 이동	감염된 파일들을 원래 위치에서 검역소 폴더 로 옮깁니다. 검역된 파일들은 실행하거나 열 수 없습니다. 따라서 감염될 위험이 없어집니다.

○탐지된 의심스러운 파일들에 대해 취할 조치를 선택하십시오. 다음의 옵션을 사용할 수 있습니다.

행동	설명
아무 조치도 안함	의심스러운 자료보관소 파일들의 기록은 검사로그 내에 두십시오. 검사 완료 후, 여러분은 이 파일들에 관한 정보를 보기 위해 검사로그를 열 수 있습니다.
파일삭제	의심스러운 파일들을 아무 경고도 없이 즉시 삭제합니다.



행동	설명
검역소로 이동	의심스러운 파일들을 검역소 안으로 옮깁니다. 검역된 파일들은 실행하거나 열 수 없습니다. 따라서 감염될 위험이 없어집니다.

○탐지된 비밀번호로 보호된 파일들에 대해 취할 조치를 선택하십시오. 다음의 옵션을 사용할 수 있습니다.

행동	설명
검사되지 않은 상태로 로그온	비밀번호로 보호된 파일들의 기록은 검사로그 내에 두십시오. 검사 완료 후, 여러분은 이 파일들에 관한 정보를 보기 위해 검사로그를 열 수 있습니다.
비밀번호 묻기	비밀번호로 보호된 파일이 탐지되었으면, 그 파일을 검사할 수 있도록 사용자에게 비밀번호를 제시하도록 알려십시오.



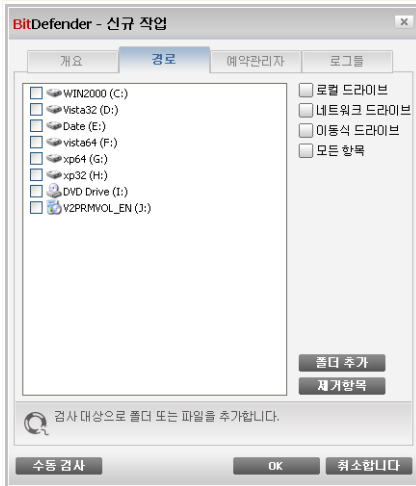
참고

탐지된 파일들을 무시하기로 선택하거나 선택한 조치가 실패하는 경우, 검사마법사에서 조치를 선택해야 할 것입니다.

기본값 버튼을 클릭하면 기본설정을 불러올 수 있습니다. 변경사항들을 저장하고 창을 닫으려면 OK를 클릭하십시오.

검사목표 설정하기

특정 사용자 작업의 검사 대상을 설정하려면, 태스크를 우클릭하고, 경로를 선택하십시오. 다음 창이 나타날 것입니다:



검사목표

이전에 추가된 파일들 혹은 폴더들 뿐 아니라 지역 네트워크 및 제거가능한 드라이브 목록이 보입니다. 그 작업 실행 시 모든 체크된 항목들이 검사될 것입니다.

이 항목에는 다음의 버튼이 포함되어 있습니다.

- 항목(들) 추가 — 검사하기 원하는 파일(들)/폴더(들)을 여러분이 선택할 수 있는 둘러보기 창을 엽니다.



참고

드래그 앤 드롭하여 파일/폴더를 리스트에 추가할 수 있습니다.

- 항목(들) 제거 — 검사할 객체들의 목록으로부터 이전에 선택된 파일(들) /폴더(들)을 제거합니다.



참고

나중에 추가된 파일/폴더만 삭제될 수 있습니다. 그러나 해당 파일은 자동적으로 BitDefender에 의해 "확인"되지 않습니다.



앞에서 설명한 버튼 이외에, 검사 위치를 빠르게 선택할 수 있도록 하는 일부 옵션이 있습니다.

- 지역 드라이브들 – 지역 드라이브들을 검사합니다.
- 네트워크 드라이브들 – 모든 네트워크 드라이브를 검사합니다.
- 제거가능 드라이브들 – 제거가능한 드라이브들을 검사합니다(CD-ROM, 플로피 디스크 장치).
- 모든 개체들 – 지역장치, 네트워크 혹은 제거가능장치에 상관없이 모든 드라이브들을 검사합니다.



참고

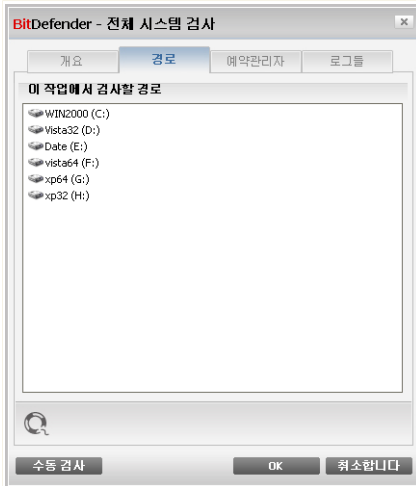
여러분의 컴퓨터 전체를 검사하고 싶으신 경우, 모든 개체에 해당하는 체크박스를 선택하십시오.

변경사항들을 저장하고 창을 닫으려면 OK를 클릭하십시오. 이 작업을 실행하려면, 그냥 검사를 클릭하시면 됩니다.

시스템 작업들의 검사목표 보기

시스템 작업들 분류에서는 검사작업들에 대한 검사목표를 수정할 수 없습니다. 여러분은 단지 그 검사목표를 볼 수만 있습니다.

어떤 특정 시스템 검사작업에 대한 검사목표를 보려면, 그 작업을 오른쪽 클릭하고 작업경로 보이기를 선택하십시오. 전체 시스템 검사를 하려면, 예를 들어 다음과 같은 창이 나타날 것입니다:



전체 시스템 검사에 대한 검사목표

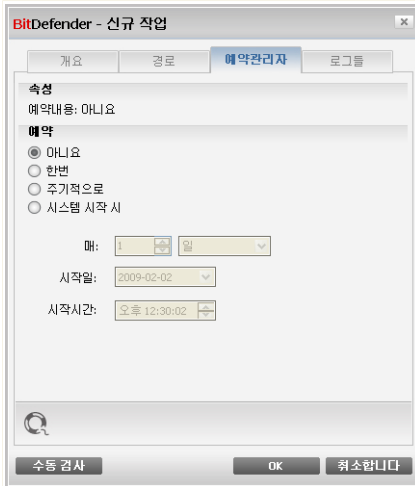
빠른 시스템 검사는 오직 Windows 및 Program Files 폴더들만 검사하지만 전체시스템검사 및 심층시스템검사는 모든 지역 드라이브들을 검사할 것입니다.

윈도우를 닫으려면 확인을 클릭하십시오. 작업을 실행하려면, 검사를 클릭하십시오.

검사작업 일정짜기

작업이 복잡한 경우, 검사과정이 제법 걸릴 수 있으며, 모든 다른 프로그램들을 닫는 것이 좋습니다. 그렇기 때문에 복잡한 작업은 여러분이 컴퓨터가 공회전 모드로 들어갔을 때 실행되도록 예약하는 것이 가장 좋습니다.

어떤 특정 작업에 대한 예약을 보거나 수정하려면, 그 작업을 오른쪽 클릭하고 작업예약을 선택하십시오. 다음 창이 나타날 것입니다:



예약관리

작업예약이 있으면 그 예약을 볼 수 있습니다.

어떤 작업에 대한 일정을 잘 때에 여러분은 다음 선택사항들 중 하나를 선택해야 합니다:

- **예약없음** - 사용자가 요청하는 경우에만 작업을 실행합니다.
- **한번만** - 어느 시기에 검사를 한번만 실행합니다. 시작날짜/시간 칸에 시작 날짜와 시간을 지정하십시오.
- **정기적으로** - 정기적으로, 정해진 시간 간격(시간, 일, 주, 월, 년)으로 정해진 일자와 시각에 검사를 시작합니다.
 검사를 어떤 주기마다 반복하게 하기 원하실 경우, 주기적으로를 선택하고, 이 과정의 주기를 나타내기 위해 주기 편집상자 내에 분/시간/주/월/년 수를 입력하십시오. 여러분은 또한 시작 날짜/시간 칸 내에 시작 날짜 및 시간을 지정할 수도 있습니다.
- **시스템 시작 시** - 어떤 사용자가 윈도우 안으로 로그인한 때로부터 지정된 수의 분이 지난 후에 검사를 시작합니다.



변경사항들을 저장하고 창을 닫으려면 OK를 클릭하십시오. 이 작업을 실행하려면, 그냥 검사를 클릭하시면 됩니다.

16.2.5. 검사객체들

어떤 검사과정을 시작하기 전에, 여러분은 비트펜더를 악성프로그램 서명에 대해 최신 업데이트된 상태에 두어야 합니다. 오래된 서명 데이터베이스를 사용해 여러분 컴퓨터를 검사하면 비트펜더가 마지막 업데이트 후 발견된 새 악성프로그램을 탐지하지 못할 수 있습니다. 마지막 업데이트가 언제 실행되었는지 확인하려면, 설정화면 내의 업데이트>업데이트를 클릭하십시오.



참고

BitDefender가 완벽한 검사를 할 수 있도록 사용자는 열려있는 모든 프로그램을 닫아야 할 필요가 있습니다. 특히 이메일 클라이언트(예. Outlook, Outlook Express, Eudora)는 꼭 닫아야 합니다.

검사방법들

비트펜더는 네 가지 형태의 주문형 검사를 제공합니다.

- **즉시 검사** - 시스템 / 사용자 작업들로부터 어떤 검사작업을 실행합니다.
- **마우스메뉴 검사** - 파일이나 폴더를 마우스 오른쪽 버튼으로 클릭하고, BitDefender 안티바이러스 2009를 선택합니다.
- **드래그 앤 드롭 검사** - 파일이나 폴더를 **검사 활동** 바에 드래그 앤 드롭합니다.
- **수동 검사** - 검사할 파일들 혹은 폴더들을 직접 선택하기 위해 비트펜더 수동 검사를 사용합니다.

즉시 검사

여러분의 컴퓨터 전체 혹은 그 일부에 대한 검사는 기본적으로 설정된 검사작업 혹은 여러분 나름의 검사작업으로 실행할 수 있습니다. 이런 검사를 '즉시 검사'라고 합니다.

어떤 검사작업을 실행하려면, 다음 방법들 중 한 방법을 사용하십시오:

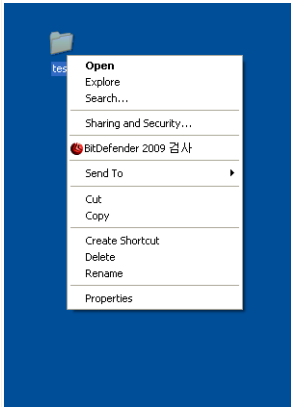
- 목록에서 원하는 검사작업을 더블클릭하십시오.
- 작업에 해당하는 지금 검사하기버튼을 클릭하십시오.
- 작업을 선택하고 그 다음 작업실행을 클릭하십시오.



빗디펜더 검사기가 나타나 검사를 시작할 것입니다. 추가 정보는 “빗디펜더 검사기” (p. 124)를 참조하십시오.

단축메뉴 검사

새 검사작업을 설정하지 않고 파일 혹은 폴더를 검사하려면, 단축메뉴를 사용할 수 있습니다. 이런 검사를 '단축메뉴검사'라고 합니다.



단축메뉴 검사

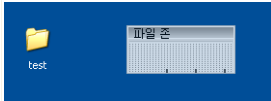
검사하기 원하시는 파일 혹은 폴더를 오른쪽 클릭하고, 빗디펜더 바이러스차단 2009를 선택하십시오.

빗디펜더 검사기가 나타나 검사를 시작할 것입니다. 추가 정보는 “빗디펜더 검사기” (p. 124)를 참조하십시오.

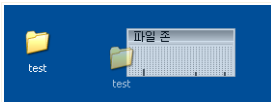
단축메뉴검사 작업의 속성창에 접근해서, 검사 선택 사양들을 수정하고 보고서 파일들을 볼 수 있습니다.

드래그 앤 드롭 검사

아래와 같이 검사하려는 파일 혹은 폴더를 집어서 검사활동막대 위에 놓으십시오.



파일 끌기



파일 놓기

빗디펜더 검사기가 나타나 검사를 시작할 것입니다. 추가 정보는 “**빗디펜더 검사기**” (p. 124)를 참조하십시오.

수동 검사

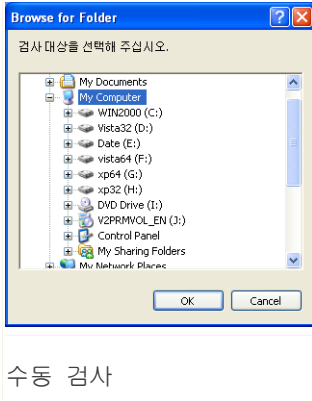
시작메뉴 내의 빗디펜더 프로그램 그룹에서 빗디펜더 수동검사 선택사항을 사용해 검사하려는 객체를 직접 선택합니다.



참고

수동검사는 원도가 안전모드에서 작동 중일때에도 실행할 수 있기 때문에 매우 유용합니다.

원도 시작메뉴에서 빗디펜더가 검사할 객체를 선택하려면, 시작 → 프로그램 → 빗디펜더 2009 → 빗디펜더 수동검사 경로를 따르십시오. 다음 창이 나타날 것입니다:



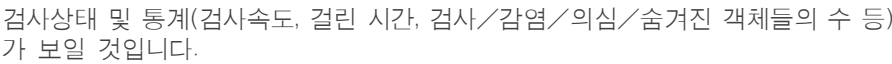
검사하려는 객체를 선택하고 OK를 클릭하십시오.
빗디펜더 검사기가 나타나 검사를 시작할 것입니다. 추가 정보는 “빗디펜더 검사기” (p. 124)를 참조하십시오.

빗디펜더 검사기

주문형 검사과정을 시작하시면, 빗디펜더검사기가 나타날 것입니다. 검사과정을 완성하기 위해 세 단계로 안내되는 절차를 따르십시오.

1/3 단계 — 검사

빗디펜더가 선택된 객체들을 검사하기 시작할 것입니다.



참고

검사의 복잡한 정도에 따라 검사과정이 제법 걸릴 수 있습니다.

검사와정을 잠시 멈추려면, 일시정지를 클릭하십시오. 검사를 계속하려면 계속을 클릭해야 합니다.

여러분은 [정지&예를 클릭해서](#) 언제든지 검사를 멈출 수 있습니다. 그러면 마법사의 가장 마지막 단계로 바로 가게 될 것입니다.

빗디펜더가 검사를 마칠 때까지 기다리십시오.

2/3 단계 - 조치들 선택

검사가 완료되면, 검사결과가 보이는 새 창이 나타날 것입니다.



여러분은 여러분 시스템에 영향을 주는 문제들의 수를 보실 수 있습니다.

감염시킨 악성프로그램에 따른 그룹별로 감염된 객체들이 나타납니다. 감염된 객체들에 대한 추가 정보를 찾으려면 위협에 해당하는 링크를 클릭하십시오.

여러분은 모든 문제들에 대해 취할 전반적 조치를 선택하거나 문제들의 각 그룹에 대한 조치들을 따로 선택할 수도 있습니다.

다음 선택사항들이 메뉴에 나타날 수 있습니다:

행동	설명
아무 조치도 취하지 않음	탐지된 파일들에 대해 아무 조치도 취해지지 않을 것입니다.
치료	감염된 파일들을 치료합니다.
삭제	탐지된 파일들을 삭제합니다.
드러내기	숨겨진 객체들을 보이게 합니다.



지정된 조치들을 적용하려면 계속을 클릭하십시오.

3/3 단계 - 보기결과들

빗디펜더가 문제들 고치기를 마치면, 검사결과들이 새 창에 나타날 것입니다.

BitDefender 2009

바이러스차단 검사 - 3/3 단계

결과들 요약	Step 1	Step 2	Step 3
해결된 항목:	1		
해결되지 않은 항목:	1		
암호 보호 항목:	0		
무시 항목:	0		
실제한 항목:	1		

1 파일이 정리될 수 없으므로, 귀하의 시스템 내에 바이러스가 존재합니다. 보다 자세한 사항은 www.bitdefender.com

검사 수행 중 완료할 수 없었던 항목수입니다.

bitdefender

로그 파일 보기 종료

요약

여러분은 결과들의 요약을 보실 수 있습니다. 검사로그를 보시려면 로그파일 보이기를 클릭하십시오.



중요

필요 시, 청소과정을 완료하도록 여러분의 시스템을 재시작하십시오.

창을 닫으려면 닫기를 클릭하십시오.

빗디펜더는 어떤 문제들은 해결하지 못합니다.

대부분의 경우 빗디펜더는 탐지한 감염된 파일들을 성공적으로 치료하거나 격리시킵니다. 그러나 해결할 수 없는 문제들도 있습니다.



그런 경우, 저희는 여러분이 www.bitdefender.com의 비트펜더 지원팀에 연락하시기를 권장드립니다. 저희 지원팀 요원들은 여러분이 겪고 계신 문제들을 해결하도록 여러분을 도울 것입니다.

비트펜더 탐지된 의심되는 파일들

의심스러운 파일들은 경험적 분석에 의해 서명이 아직 공개되지 않은 악성소프트웨어 감염가능성이 있는 것으로 탐지됩니다.

만약 검사 도중에 의심되는 파일들이 탐지되면, 여러분은 그 파일들을 비트펜더 연구소로 보내시도록 요구받으실 것입니다. 추가 분석을 위해 이 파일들을 비트펜더 연구소로 보내시려면 OK를 클릭하십시오.

16.2.6. 검사로그들 보기

작업 실행 후 검사결과들을 보려면, 작업을 마우스 오른쪽 클릭하고 로그를 선택하십시오. 다음 창이 나타날 것입니다:





여기서는 작업이 실행될 때마다 생성된 보고서 파일들을 보실 수 있습니다. 각 파일에 대해 여러분은 로그생성된 검사과정 상태, 검사가 실행된 날짜 및 시간, 그리고 검사결과들에 대한 요약에 관한 정보를 제공받으실 것입니다.

다음과 같은 두 버튼들을 사용하실 수 있습니다:

- 삭제 — 선택된 검사로그를 삭제합니다.
- 보이기 — 선택된 검사로그를 보입니다. 검사로그는 여러분의 기본웹브라우저에서 열릴 것입니다.



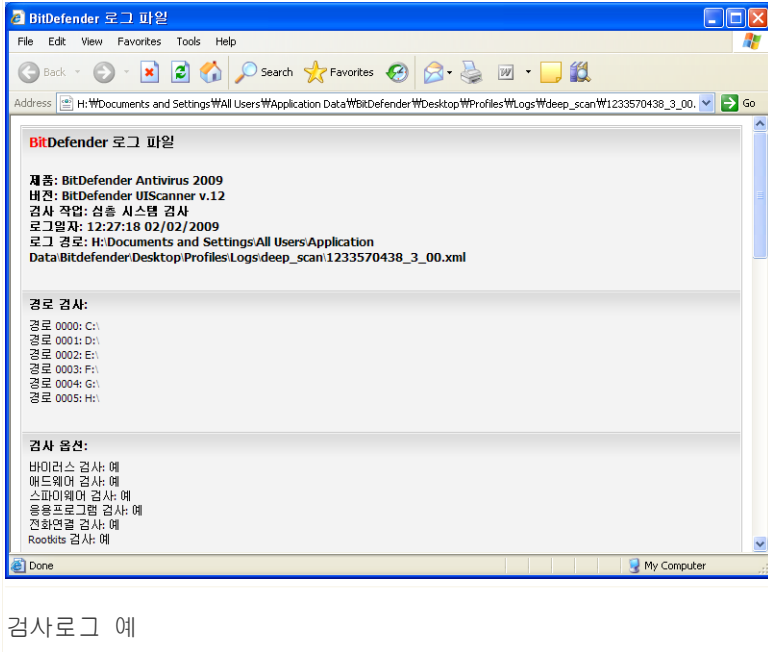
참고

또한, 어떤 파일을 보거나 삭제하려면, 그 파일을 오른쪽 클릭하고 단축메뉴로부터 해당 선택사항을 선택하십시오.

변경사항들을 저장하고 창을 닫으려면 OK를 클릭하십시오. 이 작업을 실행하려면, 그냥 검사를 클릭하시면 됩니다.

검사로그 예

다음 그림은 검사로그의 한 예를 보여줍니다:



검사로그에는 검사 선택사항들, 검사목표, 발견된 위협들 및 이 위협들에 대해 취해진 조치들과 같은 로그생성된 검사과정에 대한 상세정보가 포함됩니다.

16.3. 검사에서 제외된 객체들

검사에서 어떤 파일들을 제외해야할 경우도 있습니다. 예를 들면, 여러분은 실시간 검사에서 EICAR시험파일을 제외하거나 주문형검사서에서 .avi파일들을 제외하기 원하실 수 있을 것입니다.

비트펜더는 실시간 검사나 주문형 검사 혹은 둘 모두로부터 객체들을 제외시킬 수 있게 합니다. 이 기능은 검사시간을 줄이고 여러분 작업에 대한 간섭을 피하기 위한 것입니다.

검사에서는 다음과 같은 두 유형의 객체들을 제외할 수 있습니다:



- 경로들 - 지정된 경로에서 지시된 파일 혹은 폴더(그 안에 있는 모든 객체들 포함)가 검사에서 제외될 것입니다.
- 확장자들 - 특정 확장자들을 가진 모든 파일들이 검사에서 제외될 것입니다.



참고

실시간 검사에서 제외된 객체들은 여러분 혹은 응용소프트웨어에 의한 접근여부와 상관없이 검사되지 않을 것입니다.

검사에서 제외된 객체들을 보거나 관리하려면, 상세보기 내의 바이러스차단>예외들로 가십시오.

BitDefender AntiVirus 2009 - 시험

상태: 3개의 보류된 미슈가 있습니다. 모든 미슈 처리

보호막 바이러스 검사 **제외들** 검역

일반사항

바이러스차단 ☒ 예외적용을 사용합니다.

검사 제외 대상 파일들 및 폴더들	실시간	사용자 조작
c:\₩	예	예
확장자:		
*.zip (압축파일)	예	예

적용 취소

최근 변경을 적용합니다.

bitdefender

구매/갱신 - 내 계정 - 등록 - 도움말 - 지원 - 히스토리

예외들

여러분은 검사에서 제외된 객체들(파일, 폴더, 확장자)을 보실 수 있습니다. 각 객체에 대해 여러분은 실시간 검사나 주문형 검사 혹은 둘 모두로부터 제외되었는지 보실 수 있습니다.



참고

여기에 지정된 예외들은 단축메뉴검사에 적용되지 않습니다.

표에서 어떤 항목을 제거하려면, 그 항목을 선택하고  삭제 버튼을 클릭하십시오.

표에서 어떤 항목을 편집하려면, 그 항목을 선택하고  편집 버튼을 클릭하십시오. 새 창이 나타날 것입니다. 이 창에서 여러분은 필요에 따라 제외하려는 확장자나 경로 및 제외하기 원하시는 검사유형을 변경할 수 있습니다. 필요한 변경을 한 후 OK를 클릭하십시오.



참고

여러분은 또한 어떤 객체를 편집 혹은 삭제하기 위해 그 객체를 오른쪽 클릭해서 단축메뉴 상의 선택사항들을 사용할 수도 있습니다.

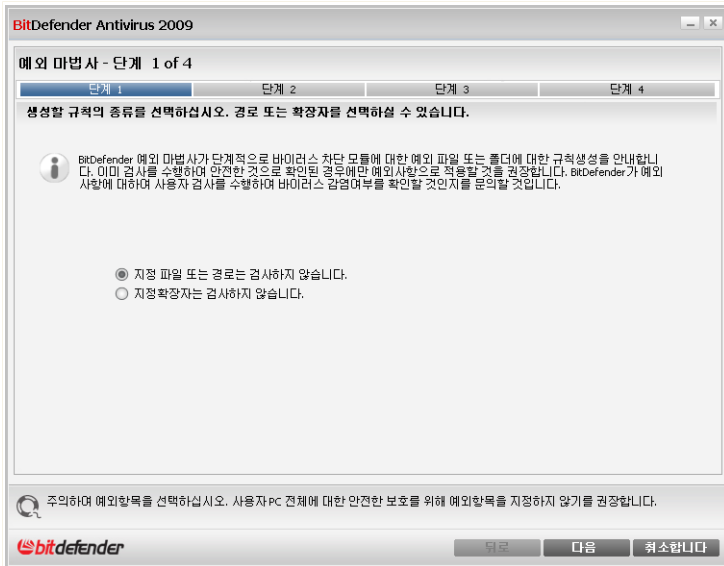
적용을 클릭해서 변경사항들을 저장하지 않았다면, 여러분은 버리기를 클릭해서 변경사항을 원위치시킬 수도 있습니다.

16.3.1. 검사에서 경로들 제외하기

검사에서 경로들을 제외하려면,  추가 버튼을 클릭하십시오. 이어서 설정방법사가 나타나서 검사에서 경로들을 제외하는 과정 동안 여러분을 안내할 것입니다.



1/4 단계 — 객체유형 선택



객체유형

검사에서 어떤 경로를 제외하는 선택사항을 선택하십시오.
다음을 클릭하십시오.



2/4 단계 - 제외할 경로 지정

제외되는 경로들

검사에서 제외할 경로를 지정하려면 다음 방법들 중 하나를 사용하십시오:

- 둘러보기를 클릭하고, 검사에서 제외하기 원하시는 파일 혹은 폴더를 선택하신 후, 추가를 클릭하십시오.
- 검사에서 제외하기 원하시는 경로를 편집 칸에 입력하신 후, 추가를 클릭하십시오.



참고

만약 제공된 경로가 존재하지 않으면 오류메시지가 나타날 것입니다. OK를 클릭 후, 경로가 유효한지 확인하십시오.

추가 시 표에 경로가 나타날 것입니다. 여러분은 원하시는 수만큼의 경로들을 추가할 수 있습니다.



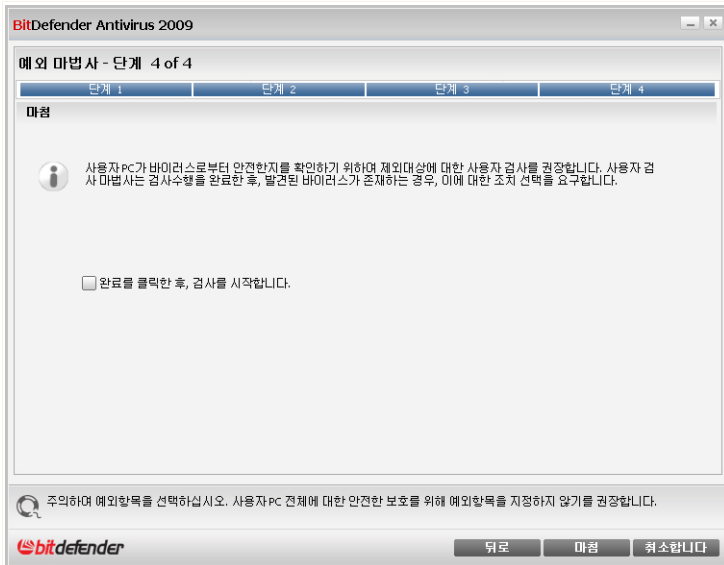
다음은 클릭하십시오.

3/4 단계 - 검사유형선택

다음은 클릭하십시오.



4/4 단계 — 검사 제외된 파일들



검사 제외된 파일들

검증이 되지 않았음을 확인하기 위해 지정된 경로들 내의 파일들을 검사하도록 권장합니다. 검사에서 제외하기 전에 이 파일들을 검사하려면, 체크박스를 선택하십시오.

완료를 클릭하십시오.

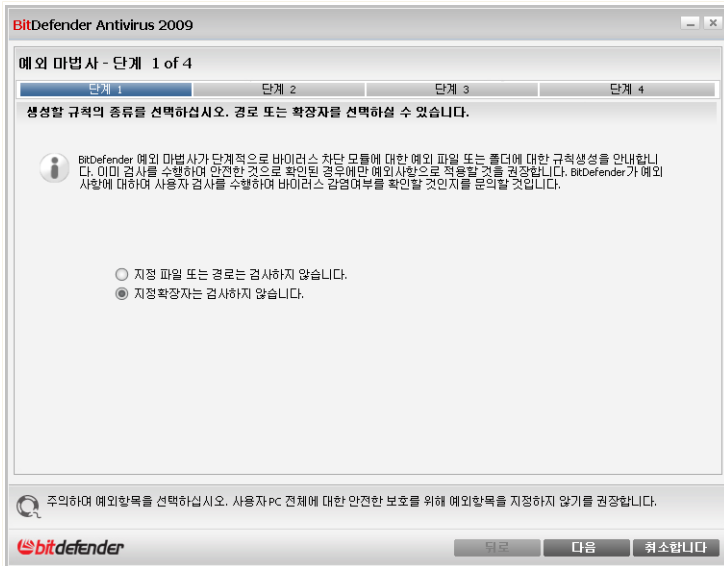
변경 사항을 저장하려면 적용을 클릭하십시오.

16.3.2. 검사에서 확장자명 제외하기

검사에서 확장자명을 제외하려면,  추가 버튼을 클릭하십시오. 설정마법사가 나타나, 검사에서 확장자명을 제외하는 과정으로 여러분을 안내할 것입니다.



1/4 단계 — 객체유형 선택

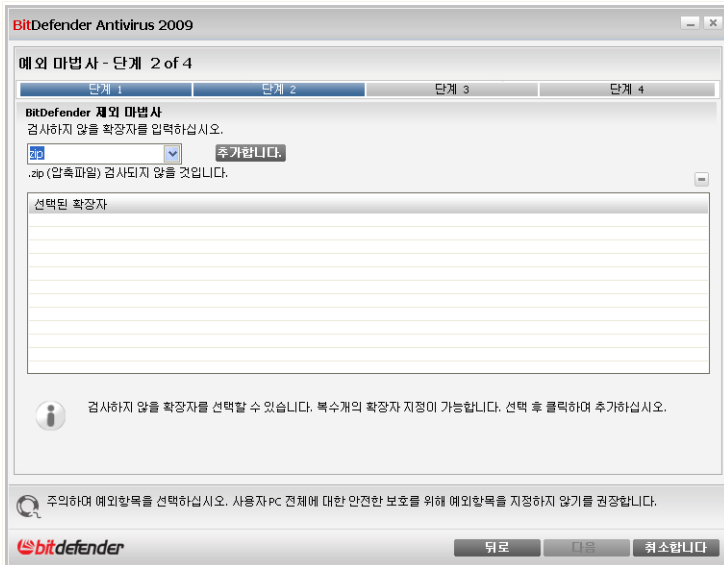


객체유형

검사에서 어떤 확장자명을 제외하는 선택사항을 선택하십시오.
다음을 클릭하십시오.



2/4 단계 - 제외되는 확장자명 지정하기



제외되는 확장자명들

검사에서의 확장자명 제외를 지정하려면, 다음 방법들 중 하나를 사용하십시오:

- 메뉴에서 검사에서 제외하기 원하시는 확장자명을 선택 후, 추가를 클릭하십시오.



참고

이 메뉴에는 여러분 컴퓨터에 등록된 모든 확장자명 목록이 포함됩니다. 어떤 확장자명을 선택하시면, 그에 대한 설명이 있는 경우 그 설명을 보실 수 있습니다.

- 검사에서 제외하기 원하시는 확장자명을 편집 칸에 입력하고, 추가를 클릭하십시오.

확장자명들을 추가함에 따라 그 확장자명들이 표에 나타날 것입니다. 여러분은 원하는 수만큼 확장자들을 추가하실 수 있습니다.



다음은 클릭하십시오.

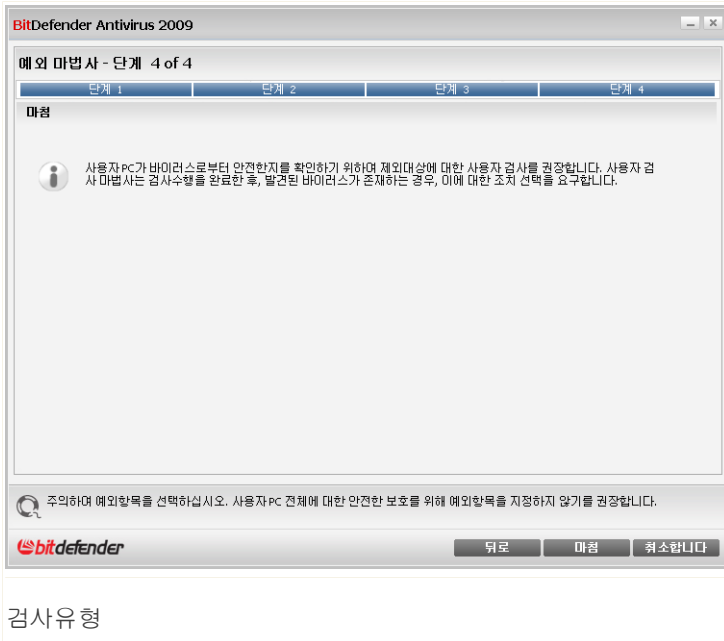
3/4 단계 - 검사유형선택

기본값으로, 선택된 확장자들은 실시간 검사 및 주문형 검사 모두에서 제외됩니다.
제외시기를 변경하시려면, 오른쪽 열을 클릭하신 후 목록에서 원하시는 선택사양
을 선택하십시오.

다음은 클릭하십시오.



4/4 단계 - 검사유형 선택



감염되지 않았음을 확인하기 위해 지정된 확장자명을 가진 파일들을 검사하도록 권장합니다.

완료를 클릭하십시오.

변경 사항을 저장하려면 적용을 클릭하십시오.

16.4. 검역소 영역

BitDefender는 검역소라고 하는 보안 지역에 감염 혹은 의심 파일을 격리시키는 기능을 제공합니다. 해당 파일을 검역소에 격리시킴으로써, 감염될 위험이 사라지고, 이와 함께 해당 파일을 추가 분석을 위해 BitDefender 연구소로 전송할 수 있습니다.



검역된 파일들을 보고 관리하고 검역설정을 하시려면, 상세보기 내의 바이러스차단>검역소로 가십시오.

BitDefender AntiVirus 2009 - 시형

상태: 4개의 보류된 미수가 있습니다. 모든 미수 처리

보호막 바이러스 검사 제외됨 **검역**

일반사항
바이러스차단
개인정보 보호
위악점 분석
암호화
게임/노트북 모드
네트워크
업데이트
등록

검역소 폴더

파일명	바이러스 이름	위치	전송
4.vir	EICAR-Test-File (not a virus)	H:\Documents...\Wav_testbed\W	아니요
3.vir	Win32.Parkit.C	H:\Documents...\Wav_testbed\W	아니요

설정들 전송 제거

치료실패 또는 제거실패된 파일에 대해서는 위험요소 차단을 위해 검역소로 이동합니다.

bitdefender 구매/경선 - 내 계정 - 등록 - 도움말 - 지원 - 히스토리

검역

검역소 영역은 검역소 폴더 내에 격리된 모든 파일들을 보여줍니다. 각 검역된 파일에 대해, 여러분은 파일이름, 탐지된 바이러스의 이름, 원래 위치 경로 및 제출 날짜를 보실 수 있습니다.



참고

검역소 내에 어떤 바이러스가 있더라도, 그 바이러스는 실행되거나 읽힐 수 없기 때문에 어떤 해도 끼칠 수 없습니다.

16.4.1. 검역된 파일들 관리하기

검역소에서 선택된 파일들을 삭제하려면, 제거 버튼을 클릭하십시오. 만약 어떤 선택된 파일을 원위치시키기 원하시면, 원위치를 클릭하십시오.

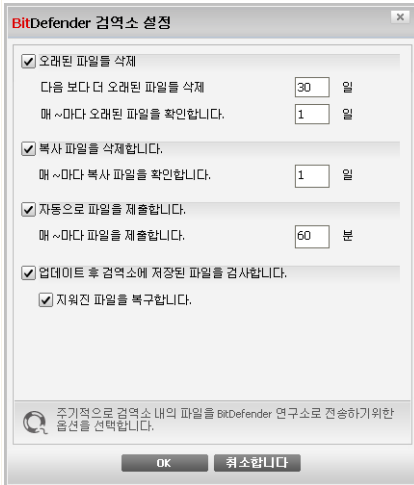


여러분은 보내기를 클릭해서, 검역소로부터 선택된 어떤 파일도 비트펜더 연구소로 보내실 수 있습니다.

단축메뉴. 단축메뉴가 있는데, 이 메뉴는 검역된 파일들을 쉽게 관리할 수 있게 합니다. 이전에 언급된 선택사항들과 같은 선택사항들이 있습니다. 여러분은 또한 검역소 영역을 새로 고침하기 위해 새로 고침을 선택할 수도 있습니다.

16.4.2. 검역소 설정

검역소 설정을 실행하려면, 설정들을 클릭하십시오. 새로운 창이 나타날 것입니다.



검역소 설정

검역소 설정들을 사용해, 여러분은 비트펜더가 자동으로 다음 조치들을 실행하도록 설정할 수 있습니다:

오래된 파일들을 삭제. 오래된 검역파일들을 자동으로 삭제하려면, 해당 선택사항을 체크표시 하십시오. 검역 파일들 삭제 주기와 비트펜더가 오래된 파일들을 확인해야할 주기를 지정하여야 합니다.



참고

기본적으로, BitDefender는 30일 이상 경고된 파일에 대하여 매일 검사를 수행하고 제거합니다.



복사본 삭제. 복사본 검역파일들을 자동으로 삭제하려면, 해당 선택사항을 체크 표시 하십시오. 여러분은 복사본을 찾기 위해 두 연속 확인들 사이의 날짜 수를 지정하셔야 합니다.



참고

기본값으로, 비트펜더는 복사본 검역된 파일들을 매일 확인할 것입니다.

자동으로 파일 제출. 검역된 파일들을 자동으로 제출하려면, 해당 선택사항을 체크 표시 하십시오. 여러분은 파일 제출 주기를 지정하셔야 합니다.



참고

기본값으로, 비트펜더는 매 60분마다 검역된 파일들을 자동으로 제출할 것입니다.

업데이트 후 검역된 파일들 검사. 매 업데이트 실행 후 검역된 파일들을 자동으로 검사하려면, 해당 선택사항을 체크 표시 하십시오. 깨끗한 파일 원위치시키키를 선택해서, 여러분은 치료된 파일들을 원래 위치로 자동으로 복귀시키도록 선택할 수 있습니다.

변경사항들을 저장하고 창을 닫으려면 OK를 클릭하십시오.



17. 개인정보보호제어

비트펜더는 얄탐프로그램이 활동하고 있을 수 있는 여러분 시스템 내 수십개의 잠재적 "선택점들"을 감시하고, 또한 여러분 시스템 및 소프트웨어에 취해진 변경 사항들을 확인합니다. 트로이 목마를 차단하고, 신용카드 등 여러분의 개인정보를 불법으로 여러분 컴퓨터에서 해커에게 보내려고 시도하는 해커들이 설치한 다른 도구들을 차단하는데 효과적입니다.

17.1. 개인정보제어상태

개인정보보호제어를 설정하고 그 활동에 관한 정보를 보려면, 상세보기 내의 개인정보보호>상태로 가십시오.

BitDefender AntiVirus 2009 - 시현

상태: 3개의 보류된 이슈가 있습니다. 모든 이슈 처리

일반사항
바이러스차단
개인정보 보호
위악점 분석
암호화
게임/노트북 모드
네트워크
업데이트
등록

☒ 개인정보 보호를 사용합니다.
개인정보 보호 컨트롤이 비활성화됩니다.

보호 수준

적극적
초기
허용적

허용적

- ID 제어를 사용하지 않습니다.
- 레지스트리 제어를 사용하지 않습니다.
- 쿠키 제어를 사용하지 않습니다.
- 스크립트 제어를 사용하지 않습니다.

사용자 수준 초기 수준

개인정보 제어 통계

차단된 ID 정보:	0
차단된 레지스트리:	0
차단된 쿠키:	0
차단된 스크립트:	0

개인정보 보호 모듈을 현재 사용하지 않습니다. 이 박스를 체크하여 사용하도록 설정하십시오. 사용자 데이터 보호를 위해 개인정보 보호 모듈을 항상 사용할 것을 권장합니다.

bitdefender 구매/경신 - 내 계정 - 등록 - 도움말 - 지원 - 히스토리

개인정보제어상태



여러분은 개인정보보호제어가 가동되어 있는지 해제되어 있는지를 볼 수 있습니다. 개인정보보호제어상태를 변경하시려면, 해당 체크박스를 해제 혹은 선택하십시오.



중요

데이터 유출 방지와 개인 정보 보호를 위해서는 개인 정보 보호 컨트롤을 활성화시켜 두십시오.

개인정보보호제어는 다음과 같은 중요한 보호제어들을 사용해 여러분의 컴퓨터를 보호합니다:

- **신분제어** — 여러분이 **신분** 질에서 생성한 규칙들에 따라 모든 송신 웹(HTTP), 이메일(SMTP) 및 메신저 교통을 여과해서 여러분의 기밀 데이터를 보호합니다.
- **레지스트리 제어** — 윈도우 시작 시에 실행되도록 어떤 프로그램이 레지스트리 등록을 변경하려고 시도할 때마다 여러분에게 허가를 요청합니다.
- **쿠키 제어** — 어떤 새 웹사이트가 쿠키를 설정하려고 시도할 때마다 여러분에게 허가를 요청합니다.
- **스크립트 제어** — 어떤 웹사이트가 어떤 스크립트 혹은 기타 활성컨텐츠를 활성화하도록 시도할 때마다 여러분에게 허가를 요청합니다.

이 절 하단에, 여러분은 개인정보보호 제어통계를 보실 수 있습니다.

17.1.1. 보호수준 설정하기

여러분은 여러분의 보안필요성에 더 적합한 보호수준을 선택할 수 있습니다. 적합한 보호수준에 맞추기 위해 눈금을 따라 미끄럼설정자를 끌어당기십시오.

보호수준에는 다음과 같이 3단계의 수준이 있습니다:

보호수준	설명
낮음	레지스트리 제어만 가동되어 있습니다.
기본	레지스트리 제어 및 신분제어가 가동되어 있습니다.
높음	등록제어, 신분제어 및 스크립트제어가 가동되어 있습니다.

여러분은 수준맞춤설정을 클릭해서, 보호수준을 맞춤형으로 설정하실 수 있습니다. 다음에 나타날 창에서, 여러분이 가동하기 원하시는 보호제어들을 선택하고, OK를 클릭하십시오.



미끄럼설정자를 기본값 수준에 두려면, 기본값 수준을 클릭하십시오.

17.2. 신분제어

기밀 데이터를 안전하게 유지하는 것은 우리 모두가 마주치는 중요한 문제입니다. 데이터 도난은 인터넷통신의 발달과 함께 커졌으며, 사람들의 개인정보유출을 야기하는 방법들도 더 교묘해져가고 있습니다.

여러분의 이메일 주소든 혹은 여러분의 신용카드번호이든, 악의적인 의도를 가진 이들의 손에 들어가면, 그런 정보유출은 여러분에게 해가 될 수 있습니다. 여러분은 악성광고메시지들의 괴롭힘을 받거나 여러분의 은행계좌가 비어있는 것을 보고 놀랄 수도 있습니다.

신분제어는 여러분이 온라인에 있는 동안 민감한 데이터 분실로부터 여러분을 보호해 줍니다. 여러분이 생성하는 규칙들에 따라, 신분제어는 여러분의 컴퓨터가 특정 문자열들(예를 들면, 여러분의 신용카드번호)찾게 함으로써, 웹, 이메일 그리고 메신저 교통을 탐색합니다. 만약 찾는 문자열이 있으면, 각 웹페이지, 이메일 및 메신저가 차단됩니다.

여러분은 여러분의 전화번호 혹은 이메일 주소에서부터 여러분의 은행계좌번호에 이르기까지 여러분이 개인적 혹은 기밀이라 여길 수 있는 어떤 정보이든 그에 대한 보호규칙들을 생성할 수 있습니다. 다른 윈도우 사용자 계정으로 로그인 하는 사용자들이 자신 나름의 신분보호 규칙들을 설정하고 사용할 수 있도록 다중 사용자 지원이 제공됩니다. 여러분이 생성하는 규칙들은 여러분이 여러분의 윈도우 사용자 계정으로 로그인할 때에만 적용 및 접속됩니다.

왜 여러분은 신분제어를 사용해야 하는가?

■ 신분제어는 키보드를 통한 엽탐프로그램을 차단하는데 매우 유용합니다. 이런 종류의 악성프로그램들은 여러분의 키보드 사용을 기록하고 그 기록을 인터넷을 통해 악의를 가진 이들(해커)에게 보냅니다. 해커는 은행계좌번호 및 비밀번호 등 훔친 데이터로부터 민감한 정보들을 찾아, 개인적 이익을 얻는데 그 정보들을 사용할 수 있습니다.

그런 응용소프트웨어가 바이러스차단 탐지를 피하기 위해 가동 중이라고 가정할 경우, 여러분이 적합한 신분보호규칙들을 생성했다면 훔친 데이터를 이메일, 웹 혹은 메신저를 통해 보낼 수 없습니다.

■ 신분제어는 여러분을 **개인정보불법수집** 시도로부터 보호할 수 있습니다. 가장 흔한 개인정보불법수집 시도들은 여러분이 여러분 개인정보를 허위 웹페이지에 제출하도록 속이는 사취 이메일을 사용합니다.



만약 적합한 신분보호규칙들을 설정해 두었다면, 각 웹페이지에 대한 예외를 명시적으로 정의해 둔 경우 외에는 여러분은 여러분의 신용카드번호 등 개인정보를 내놓을 수 없습니다.

BitDefender AntiVirus 2009 - 시형

가본모드 보기

상태: 3개의 보류된 매수가 있습니다. 모든 매수 처리

상태 ID 레지스터 쿠키 스크립트

일반사항
바이러스 차단
개인정보 보호
위악점 분석
암호화
게임/노트북 모드
네트워크
업데이트
등록

☒ 개인정보 보호
차단된 총 시도: 0

규칙명 규칙 ... H... Sntp 계... 잔액 단어 사례 대조 설명

예외들

네트워크 모듈이 BitDefender 홈 네트워크 구조를 표시합니다.(홈네트워크가 구성되지 않은 경우 회색으로 표시됩니다). 사용자 홈 네트워크 생성을 시작하려면 '연결/생성' 네트워크를 클릭하십시오.

bitdefender

구매/경신 - 내 계정 - 등록 - 도움말 - 지원 - 히스토리



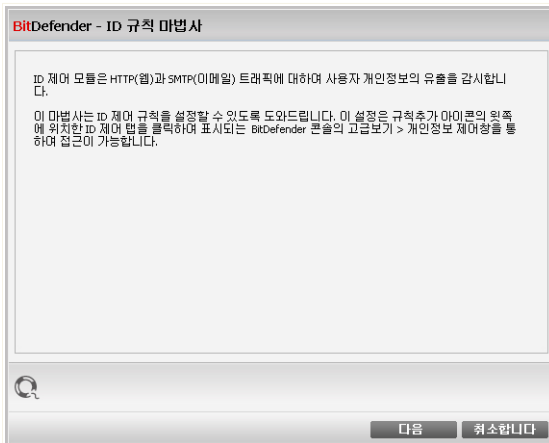
만약 여러분이 신분제어를 사용하기 원하시면, 이 절차들을 따르십시오:

1. 신분제어 체크박스를 선택하십시오.
2. 여러분의 민감한 데이터를 보호하기 위한 규칙들을 만드십시오. 추가 정보는, “신분규칙들 생성하기” (p. 148)를 참조하십시오.
3. 필요한 경우, 여러분이 만든 규칙들에 대한 구체적 예외를 정의하십시오. 추가 정보는, “예외 정의” (p. 151)를 참조하십시오.

17.2.1. 신분규칙들 생성하기

신분보호규칙을 생성하려면,  추가 버튼을 클릭한 후, 설정마법사를 따르십시오.

1/4 단계 — 환영 창



환영 창

다음을 클릭하십시오.



2/4 단계 - 규칙 유형 및 데이터 설정

BitDefender - ID 규칙 마법사

규칙명

규칙 종류

신용 카드

규칙 데이터

개인 정보는 암호화되며, 사용자 이외에는 어느 누구도 사용할 수 없습니다. 추가 보안을 위해서, 보호하고자 하는 정보의 부분을 입력하십시오. (예, john.doe@example.com이라는 이메일 주소에 대한 트래픽 필터링을 원한다면, 대상 문자열에 "john"을 추가해 주십시오.)

규칙 이름을 입력하십시오.

뒤로

다음

취소합니다

규칙 유형 및 데이터 설정

여러분은 다음 매개변수들을 설정해야 합니다:

- **규칙 이름** - 이 편집칸에 규칙 이름을 입력하십시오.
- **규칙유형** - 주소, 이름, 신용카드, 비밀번호, 사회보장번호, 등 규칙유형을 선택합니다.
- **규칙데이터** - 이 편집칸 내에 여러분이 보호하기 원하시는 데이터를 입력하십시오. 예를 들면, 만약 여러분이 여러분의 신용카드번호를 보호하기 원하신다면, 이 번호의 전부 혹은 일부를 여기에 입력하십시오.

참고

만약 여러분이 세 글자 미만을 입력할 경우, 데이터를 확인하도록 여러분에게 알릴 것입니다. 메시지들 및 웹페이지들이 잘못 차단되는 경우를 피하기 위해 저희는 최소 세 글자 이상 입력하도록 권장합니다.

여러분이 입력하는 모든 데이터는 암호화됩니다. 안전성을 높이려면, 보호하기 원하는 모든 데이터를 입력하지는 마십시오.

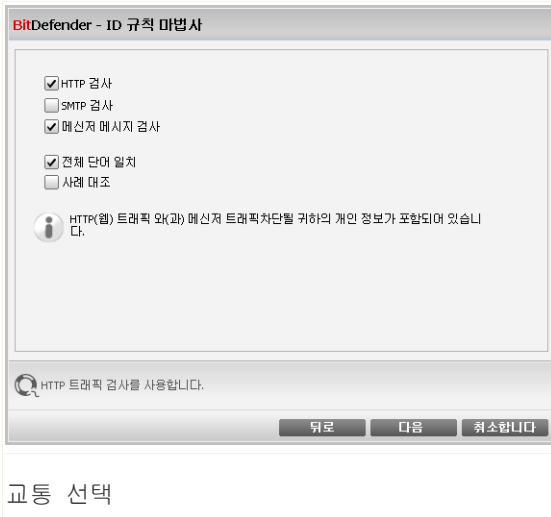
다음을 클릭하십시오.

개인정보보호제어

149



3/4 단계 - 교통 선택



여러분이 비트펜더가 검사하기 원하시는 교통의 유형을 선택하십시오. 다음의 옵션을 사용할 수 있습니다.

- HTTP검사 - HTTP(웹) 교통을 검사하고 규칙데이터에 맞는 송신데이터를 차단합니다.
- SMTP검사 - SMTP(메일)교통을 검사하고 규칙데이터를 담은 송신이메일메시지들을 차단합니다.
- 메신저 검사 - 메신저 교통을 검사하고 규칙데이터를 담은 송신문자대화 메시지들을 차단합니다.

여러분은 규칙데이터가 전체 단어들에 맞거나 규칙데이터와 탐색된 문자열이 맞는 경우에만 규칙을 적용하도록 선택할 수 있습니다.

다음을 클릭하십시오.



4/4 단계 - 규칙설명

BitDefender - ID 규칙 마법사

규칙 설명

이 규칙에 대한 설명을 입력합니다. 설명은 사용자나 다른 관리자가 어떠한 정보가 차단되었는지를 보다 쉽게 확인하는 데 도움이 됩니다.

현재 규칙의 설명을 입력합니다.

뒤로 마침 취소합니다

규칙 설명

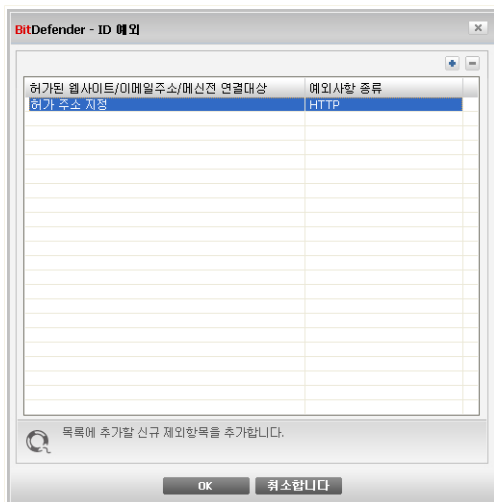
규칙에 대한 짧은 설명을 편집 칸 내에 입력하십시오. 차단된 데이터(문자열)은 규칙에 접근할 때 보통 텍스트에 나타나지 않기 때문에, 설명은 여러분이 그 데이터를 쉽게 찾을 수 있도록 되어야 합니다.

완료 버튼을 클릭하십시오. 규칙은 표에 나타날 것입니다.

17.2.2. 예외 정의

특정신분규칙들에 대한 예외들을 지정할 필요가 있는 경우들이 있습니다. 여러분이 여러분의 신용카드번호가 HTTP(웹)으로 보내지는 것을 방지하는 규칙을 만드는 경우를 생각해 봅시다. 웹에서 여러분의 계정으로부터 여러분 신용카드번호가 제출될 때마다 각 페이지는 차단됩니다. 예를 들어, 만약 여러분이 어떤 온라인 매장(여러분이 안전하다는 것을 알고 있는)에서 신발류를 구입하기 원한다면, 여러분은 각 규칙에 대한 예외를 지정해야 할 것입니다.

예외를 관리할 수 있는 창을 열려면, 예외들을 클릭하십시오.



예외들

예외를 추가하려면, 이 단계들을 따르십시오:

1. 새 항목을 표에 추가하려면 추가를 클릭하십시오.
2. 허용된 주소 지정을 더블클릭하고, 여러분이 예외로 추가하기 원하시는 웹사이트, 이메일 주소 혹은 메신저 연락정보를 제공하십시오.
3. 형태 선택하기를 더블클릭한 후 메뉴로부터 이전에 입력한 주소 형태에 해당하는 선택사항을 선택하십시오.
 - 만약 여러분이 웹주소를 지정했다면, HTTP를 선택하십시오.
 - 만약 여러분이 이메일 주소를 지정했다면, SMTP를 선택하십시오.
 - 만약 메신저 연락정보를 지정하신 경우, 메신저를 선택하십시오.

목록에서 어떤 예외를 제거하려면, 그 예외를 선택한 후 제거를 클릭하십시오.
변경 사항을 저장하려면 확인을 클릭하십시오.

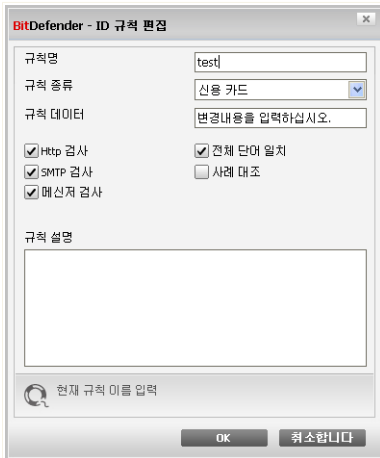
17.2.3. 규칙들 관리하기

여러분은 지금까지 생성된 규칙들이 표에 나열된 것을 볼 수 있습니다.



어떤 규칙을 삭제하려면, 그 규칙을 선택 후, 삭제 버튼을 클릭하십시오.

어떤 규칙을 편집하기 원하실 경우, 그 규칙을 선택하고 편집 버튼을 클릭하십시오. 새 창이 나타날 것입니다.



여기서 여러분은 규칙의 이름, 설명 및 매개 변수들(유형, 데이터 및 교통)을 변경할 수 있습니다. 변경사항들을 저장하려면 OK를 클릭하십시오.

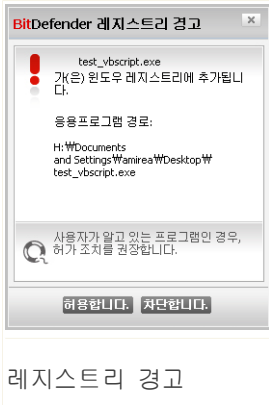
규칙 편집

17.3. 레지스트리 컨트롤

윈도우 운영 체제에서 가장 중요한 부분을 레지스트리라고 합니다. 레지스트리는 윈도우가 윈도우 설정, 설치된 프로그램, 사용자 정보 등을 유지하는 장소입니다.

또한 레지스트리는 윈도우가 시작될 때 자동적으로 시작되어야 하는 프로그램 지정에 사용되기도 합니다. 바이러스는 종종 사용자가 컴퓨터를 켤 때 자동적으로 프로그램이 실행될 수 있도록 하기 위해 레지스트리를 사용합니다.

레지스트리 제어는 윈도우 레지스트리를 감시하는 눈과 같습니다. 이 제어는 트로이안 목마와 같은 해킹프로그램을 감시하는데 유용합니다. 윈도우의 시작 프로그램으로 등록하기 위해 레지스트리를 수정하려는 시도가 발생하면 사용자에게 즉시 경고합니다.



레지스트리 경고

여러분은 윈도우 레지스트리를 수정하려고 시도하고 있는 프로그램을 볼 수 있습니다.

만약 여러분이 그 프로그램이 의심스럽게 보인다면, 그 프로그램이 윈도우 레지스트리를 수정하지 못하도록 차단을 클릭하십시오. 그렇지 않다면, 수정을 허락하도록 허락을 클릭하십시오.

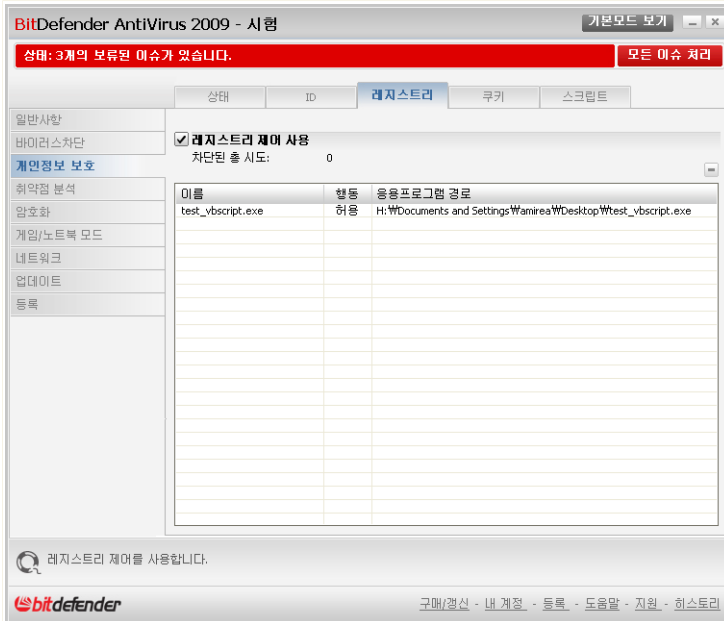
여러분의 응답에 따라, 한 규칙이 생성되어 규칙 표에 나열될 것입니다. 이 프로그램이 어떤 레지스트리 항목을 수정하려고 시도할 때마다 동일한 조치가 적용됩니다.



참고

BitDefender는 일반적으로 사용자가 컴퓨터를 다시 시작한 이후에 가동될 필요가 있는 새로운 프로그램을 설치할 때 경고를 하게 됩니다. 대부분의 경우에서 이러한 프로그램은 적법하고 신뢰할 수 있는 것입니다.

레지스트리 제어를 설정하려면, 상세보기 내의 개인정보보호 제어>레지스트리로 가십시오.



레지스트리 컨트롤

여러분은 지금까지 생성된 규칙들이 표에 나열된 것을 볼 수 있습니다. 어떤 규칙을 삭제하려면, 그 규칙을 선택 후, 삭제 버튼을 클릭하십시오.

17.4. Cookie 컨트롤

쿠키는 인터넷 상에서 널리 사용되고 있습니다. 이것은 사용자의 컴퓨터에 작은 파일을 저장합니다. 웹사이트들은 사용자 정보를 추적하기 위한 방법으로 쿠키를 생성합니다.

쿠키는 일반적으로 사용자를 보다 편안하게 만들기 위한 것입니다. 예를 들어, 쿠키 파일은 웹사이트가 사용자명과 기호를 기억하도록 하는 데 도움을 줄 수 있고, 이로써 사용자가 매번 입력을 하지 않아도 되게 합니다.



그러나 또한 쿠키 파일은 사용자의 인터넷 사용 패턴을 추적함으로써 개인 정보에 위협을 주는 데 사용될 수도 있습니다.

쿠키 컨트롤 도움말입니다. 활성화 되어 있을 때 쿠키 컨트롤이 새로운 웹 사이트의 쿠키 파일이 설치될 때마다 사용자의 허가를 요청합니다.



쿠키 경고

쿠키 파일 전송을 시도하는 응용소프트웨어의 이름과 원격지 주소를 확인할 수 있습니다.

답변 기억하기 옵션을 체크하고, 예나 아니오 를 클릭하면, 규칙이 생성되고, 적용되며, 표에 개재될 것입니다. 사용자는 동일 사이트에 연결할 때 이에 관한 고지를 받지 않게 될 것입니다.

이것은 신뢰할 수 있는 사이트와 그렇지 않은 사이트를 구별하는데 도움이 됩니다.



참고

오늘날 인터넷에서 사용하는 쿠키 파일의 수가 엄청나기 때문에 쿠키 컨트롤은 처음에는 상당히 귀찮을 수 있습니다. 처음에는 사용자의 컴퓨터에 쿠키 파일 설치를 시도하는 사이트에 관하여 상당히 많은 질문을 할 것입니다. 사용자가 적절한 사이트를 규칙 리스트에 추가하는 순간, 인터넷 서핑은 예전만큼 편안해질 것입니다.

쿠키제어를 설정하려면, 상세보기 내의 개인정보제어>쿠키로 가십시오.



규칙들은 우선 순위별로 나열됩니다. 즉 맨 위의 규칙이 가장 중요하다는 의미입니다. 규칙 우선순위를 바꾸려면, 규칙들을 드래그 앤 드롭으로 옮기십시오.

어떤 규칙을 수동으로 추가하려면,  추가 버튼을 클릭하고, 설정 창에서 규칙 매개변수들을 설정하십시오.



17.4.1. 설정 창

어떤 규칙을 편집하거나 수동으로 추가할 때, 설정창이 나타날 것입니다.

주소, 조치 및 지침 선택

여러분은 다음 매개변수들을 설정할 수 있습니다:

- 도메인 주소 — 규칙이 적용되어야 하는 도메인에 입력하십시오.
- 행동 — 규칙의 행동을 선택하십시오.

행동	설명
허용	해당 도메인 내의 쿠키가 시행될 것입니다.
거부	해당 도메인 내의 쿠키가 시행되지 않을 것입니다.

- 방향 — 트래픽 방향을 선택합니다.

형태	설명
발신	이 규칙은 연결된 사이트로 재전송되는 쿠키 파일에만 적용됩니다.



형태	설명
수신	이 규칙은 연결된 사이트에어 수신되는 쿠키 파일에만 적용됩니다.
모두	송/수신 트래픽 모두에 적용합니다.



참고

사용자는 쿠키 파일을 받아들이는 수 있지만, 거부 행동 및 발신 방향을 설정함으로써, 해당 파일을 리턴시키지는 못합니다.

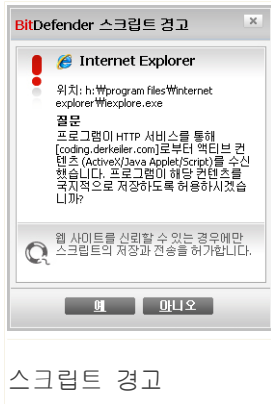
완료를 클릭하십시오.

17.5. 스크립트 컨트롤

스크립트이며, 쌍방향 웹 페이지에 사용되는 **ActiveX 컨트롤**이나 **자바 애플릿**과 같은 기타 코드는 유해한 영향을 미칠 수 있도록 프로그래밍 될 수 있습니다. 예를 들어 ActiveX는 사용자의 데이터에 전체적인 접근권을 가지고, 사용자의 컴퓨터에서 데이터를 읽고, 정보를 삭제하며, 패스워드를 포착하고, 사용자가 온라인 상에 있을 때 메시지를 엿볼 수 있습니다. 사용자는 완전히 알고 신뢰하는 사이트에서만 액티브 콘텐츠를 수락하여야 합니다.

BitDefender는 사용자가 해당 요소를 가동시키거나, 시행을 차단하도록 선택할 수 있게 합니다.

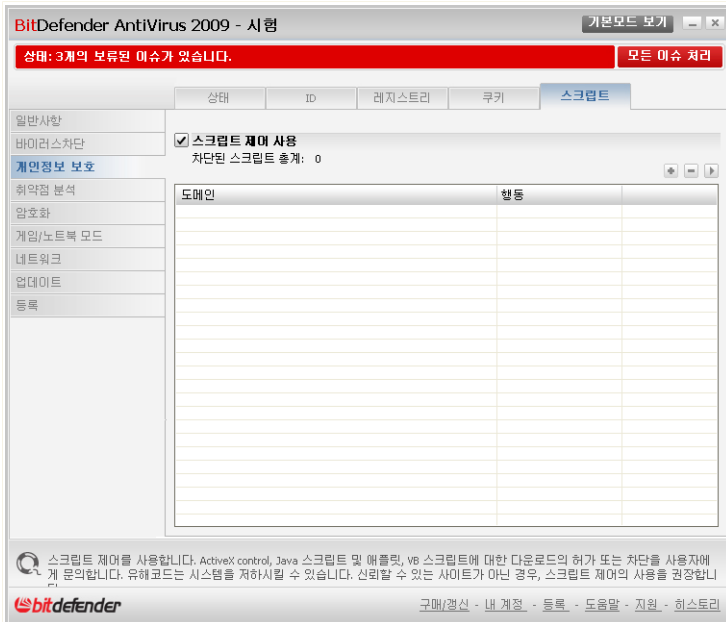
스크립트 컨트롤을 이용하여 신뢰하는 사이트와 그렇지 않은 사이트를 지정할 것입니다. BitDefender는 웹 사이트가 스크립트나 기타 액티브 콘텐츠를 활성화시키려고 시도할 때마다, 사용자의 허가를 요청할 것입니다.



여러분은 자원의 이름을 볼 수 있습니다.

답변 기억하기 옵션을 체크하고, 예나 아니오를 클릭하면, 규칙이 생성되고, 적용되며, 표에 개재될 것입니다. 사용자는 동일 사이트에서 사용자에게 액티브 콘텐츠를 전송할 때 이에 관한 고지를 받지 않게 될 것입니다.

스크립트 제어를 설정하려면, 상세보기 내의 개인정보보호 제어>스크립트로 가십시오.



스크립트 컨트롤

여러분은 지금까지 생성된 규칙들이 표에 나열된 것을 볼 수 있습니다.



중요

규칙들은 우선 순위별로 나열됩니다. 즉 맨 위의 규칙이 가장 중요하다는 의미입니다. 규칙 우선순위를 바꾸려면, 규칙들을 드래그 앤 드롭으로 옮기십시오.

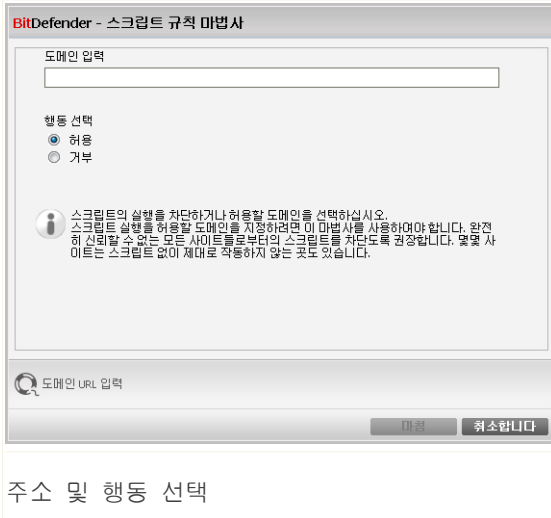
어떤 규칙을 삭제하려면, 그 규칙을 선택 후, 삭제 버튼을 클릭하십시오. 규칙 매개변수들을 바꾸려면, 설정 창에서 규칙을 더블클릭해서 원하는 대로 바꾸십시오.

어떤 규칙을 수동으로 생성하려면, 추가 버튼을 클릭하고, 설정 창 내에서 규칙 매개변수들을 설정하십시오.



17.5.1. 설정 창

어떤 규칙을 편집하거나 수동으로 추가할 때, 설정창이 나타날 것입니다.



BitDefender - 스크립트 규칙 마법사

도메인 입력

행동 선택

☒ 허용
☐ 거부

스크립트의 실행을 차단하거나 허용할 도메인을 선택하십시오.
스크립트 실행을 허용할 도메인을 지정하려면 이 마법사를 사용해야 합니다. 완전
히 신뢰할 수 없는 모든 사이트로부터의 스크립트를 차단하도록 권장합니다. 몇몇 사
이트는 스크립트 없이 제대로 작동하지 않는 곳도 있습니다.

도메인 URL 입력

마침 취소합니다

주소 및 행동 선택

여러분은 다음 매개변수들을 설정할 수 있습니다:

- 도메인 주소 — 규칙이 적용되어야 하는 도메인에 입력하십시오.
- 행동 — 규칙의 행동을 선택하십시오.

행동	설명
허용	해당 영역의 스크립트가 실행될 것입니다.
거부	해당 영역의 스크립트가 실행되지 않을 것입니다.

완료를 클릭하십시오.



18. 메신저 암호화

기본값으로, 비트펜더는 여러분의 모든 메신저 문자대화 세션들을 다음과 같은 가정에 따라 암호화합니다:

- 여러분의 문자대화상대는 대화에 사용되는 메신저 응용소프트웨어에 맞도록 가동된 메신저 암호화를 지원하는 비트펜더 버전을 사용합니다.
- 여러분과 여러분의 문자대화상대는 야후 메신저 혹은 윈도 라이브(MSN) 메신저를 사용합니다.



중요

문자대화상대가 Meebo 혹은 야후 메신저 혹은 MSN을 지원하는 다른 대화 응용 소프트웨어와 같은 웹기반 대화 응용소프트웨어를 사용하는 경우, 비트펜더는 대화를 암호화하지 않을 것입니다.

메신저 암호화를 설정하려면, 상세보기 내의 암호화>메신저 암호화로 가십시오.



참고

여러분은 문자대화 창으로부터 비트펜더 도구막대를 사용해 메신저 암호화를 쉽게 설정할 수 있습니다. 추가 정보는, “메신저로의 통합” (p. 36)를 참조하십시오.



메신저 암호화

기본값으로, 메신저 암호화는 야후메신저 및 윈도 라이브 메신저 모두에 대해 자동됩니다. 여러분은 특정 문자대화프로그램에 대해서만 혹은 전체에 대해 메신저 암호화를 해제하도록 선택할 수 있습니다.

다음과 같은 두 사양이 제시되어 있습니다:

- 암호화 배제 - 사용자 ID들 및 암호화가 해제된 관련 메신저 프로그램을 나열합니다. 목록에서 어떤 연락처를 제거하려면, [제거] 버튼을 클릭하십시오.
- 현재 연결 - 현재 메신저 연결들(사용자 ID 및 관련 메신저 프로그램) 및 암호화여부를 나열합니다. 다음과 같은 이유로 연결이 암호화되지 않을 수 있습니다:

여러분이 각 연락처에 대한 암호화를 명시적으로 해제했습니다.

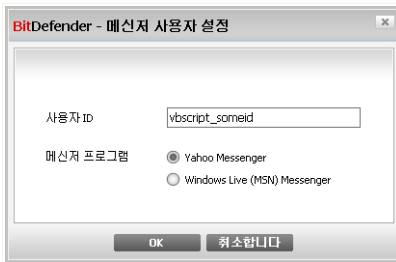


여러분의 연락처에 메신저 암호화를 지원하는 비트펜더 버전이 설치되어 있지 않습니다.

18.1. 특정 사용자에게 대한 암호화 해제

특정 사용자에게 대한 암호화를 해제하려면, 다음 단계들을 따르십시오:

1. 설정창을 열기 위해  추가 버튼을 클릭하십시오.



연락처 추가하기

2. 편집 칸에 여러분 연락처의 사용자 ID를 입력하십시오.
3. 연락처와 관련된 메신저 프로그램을 선택하십시오.
4. 확인을 클릭하십시오.



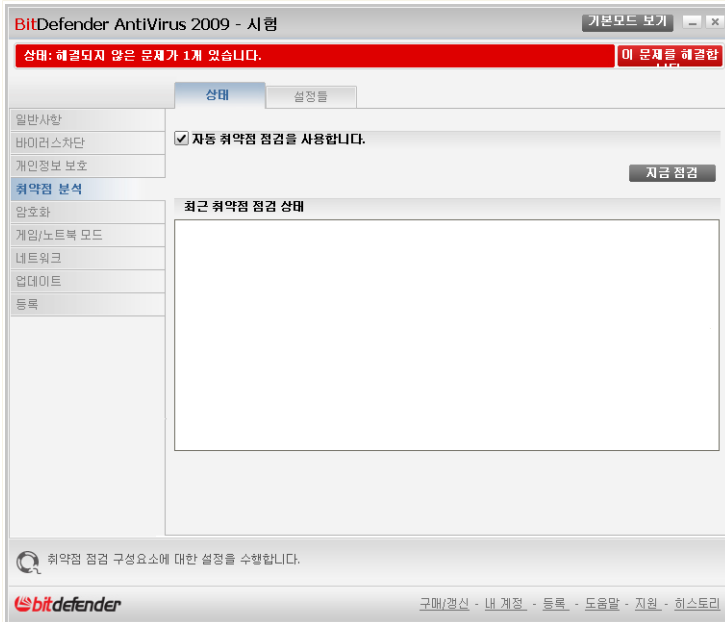
19. 취약성

여러분 컴퓨터를 악의적인 사람들과 프로그램들로부터 보호하기 위한 중요한 단계는 운영체제와 여러분이 일상적으로 사용하는 프로그램들이 최신 업데이트된 상태로 있게 하는 것입니다. 더욱이, 여러분 컴퓨터에 허가없이 물리적으로 접근하는 것을 막기 위해서는 각 윈도우 사용자 계정에 대해 강력한 비밀번호들(쉽게 추측할 수 없는 비밀번호들)이 설정되어야 합니다.

빗디펜더는 여러분 시스템의 취약성여부를 정기적으로 확인하고, 현존하는 문제들에 대해 여러분에게 알려드립니다.

19.1. 상태

자동취약성 확인을 설정하거나 취약성확인을 실행하려면, 상세보기 내의 취약성> 상태로 가십시오.



취약성 상태

최근 취약점 점검을 통해 발견된 이슈에 대한 정보를 제공합니다. 각각의 취약점에 대하여 조치할 내역에 대한 정보를 표시합니다. None 을 선택하는 경우, 발견된 항목을 더이상 취약점으로 분류하지 않습니다.



중요

시스템 혹은 프로그램의 취약성들에 대해 자동으로 통지를 받으시려면, 자동 취약성 확인을 가동된 상태로 두십시오.

19.1.1. 취약점 조치하기

지정된 취약점을 조치하기 위해서, 해당 항목을 더블클릭하고 이슈에 따라서 다음을 진행합니다:



- 윈도우 업데이트가 사용가능한 경우, 모든 시스템 업데이트 설치 를 클릭하여 업데이트합니다.
- 응용프로그램 업데이트가 존재하는 경우, 해당 응용프로그램에서 제공하는 홈페이지 링크를 클릭하여 최신 업데이트를 설치합니다.
- 윈도우 사용자 계정암호가 취약한 경우, 사용자에게 다음 로그인 시도 시 암호를 강제로 변경하도록 합니다.

지금 점검 을 클릭하여 단계별로 취약점을 조치하도록 합니다.

1/6 단계 — 확인하려는 취약성들을 선택하십시오.

BitDefender 2009

BitDefender 취약점 마법사

Step 1

Step 2

Step 3

Step 4

Step 5

Step 6

작업 선택

마법사가 뒤떨어진 어플리케이션과 취약한 패스워드를 가진 윈도우 계정을 확인하기 위한 단계로 귀하를 안내할 것입니다. 취약성을 확인할 항목을 아래의 리스트에서 선택하십시오.

- ☒ 윈도우 중요 업데이트 확인
- ☒ 윈도우 선택 업데이트 확인
- ☒ 응용프로그램 업데이트 확인
- ☒ 윈도우 계정 암호 확인

이 상자를 선택하여 BitDefender가 귀하의 윈도우 운영체제가 마이크로소프트 최신 보안 업데이트 사항을 적용하였는지를 확인하도록 하십시오.

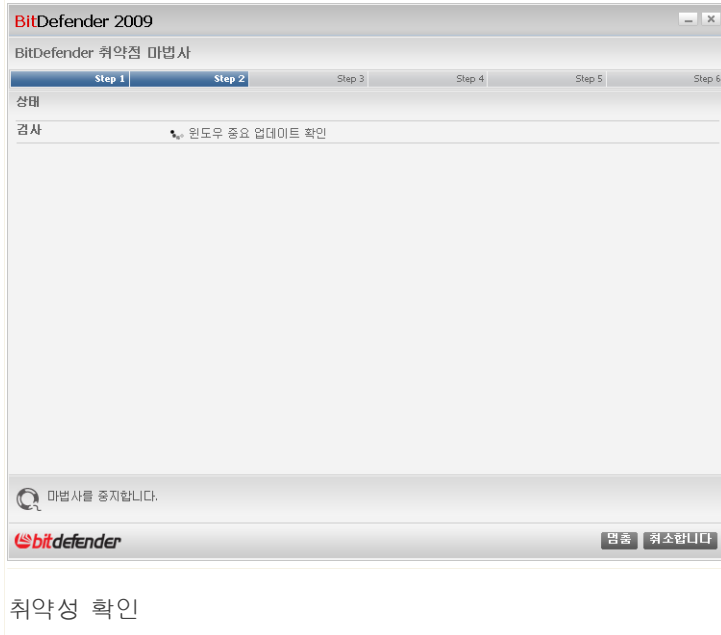
다음 취소합니다

취약성들

선택된 취약성들에 대해 시스템을 확인하려면 다음을 클릭하십시오.



2/6 단계 - 취약성 확인하기



비트펜더가 취약성 확인을 마칠 때까지 기다리십시오.



3/6 단계 — 약한 비밀번호 변경

BitDefender 2009

BitDefender 취약점 마법사

Step 1

Step 2

Step 3

Step 4

Step 5

Step 6

윈도우 업데이트

윈도우 중요 업데이트 확인

Security Update for Windows XP (KB901190)

MSXML 6.0 RTM Security Update (925673)

Security Update for Windows XP (KB943485)

Security Update for Windows XP (KB946026)

Security Update for Windows XP (KB943055)

Update for Office 2003 (KB907417)

Security Update for Windows XP (KB945553)

Microsoft .NET Framework 1.1 Service Pack 1

Security Update for Windows XP (KB950749)

Update for Windows XP (KB932823)

Office 2003 Service Pack 3 (SP3)

Security Update for Windows XP (KB950762)

Security Update for Windows XP (KB951376)

Security Update for Windows XP (KB951698)

Security Update for Windows XP (KB951748)

모든 시스템 업데이트를 설치합니다.

이것은 중요한 혹은 중요하지 않은 윈도우 어플리케이션 업데이트 리스트입니다.

다음 취소합니다

사용자 비밀번호들

여러분 컴퓨터 상에 설정된 윈도우즈 사용자 계정들의 목록과 그 비밀번호들이 제공하는 보호 수준을 보여줍니다.

약한 비밀번호를 변경하려면 고치기를 클릭하십시오. 새로운 창이 나타날 것입니다.



비밀번호 변경

다음 이 문제를 고치는 방법을 선택하십시오:

- 다음 로그인 시 사용자가 비밀번호를 고치도록 요구하십시오. 비트펜더는 사용자가 다음에 윈도우로 로그인할 때에 비밀번호를 바꾸도록 사용자에게 요구할 것입니다.
- 사용자 비밀번호 변경. 여러분은 편집 칸에 새 비밀번호를 입력해야 합니다.



참고

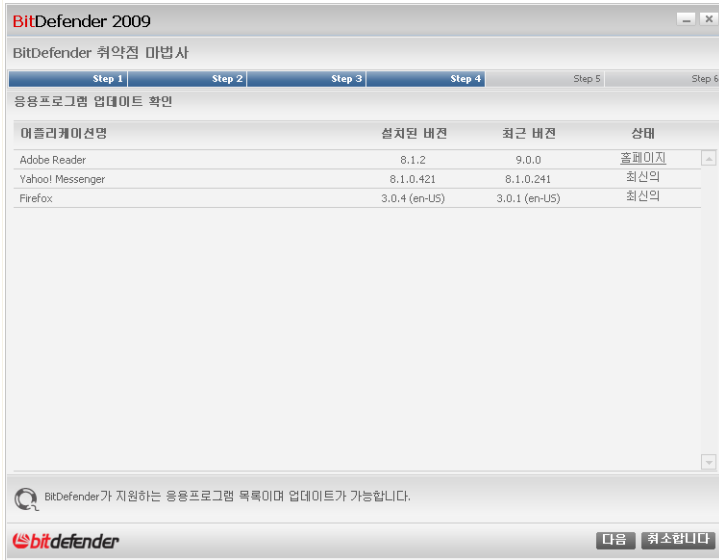
비밀번호를 튼튼하게 하기 위해 대문자와 소문자, 숫자와 #, \$ 혹은 @ 등 특수 문자들의 조합을 사용하십시오.

비밀번호를 변경하려면, OK를 클릭하십시오.

다음은 클릭하십시오.



4/6 단계 - 응용소프트웨어 업데이트



응용소프트웨어들

여러분은 비트펜더가 확인한 응용소프트웨어들의 목록과 업데이트 상황을 볼 수 있습니다. 약 어떤 응용소프트웨어가 최신업데이트되어 있지 않으면, 제공된 링크를 클릭해서 최신버전을 내림받으십시오.

다음을 클릭하십시오.



5/6 단계 - 윈도 업데이트



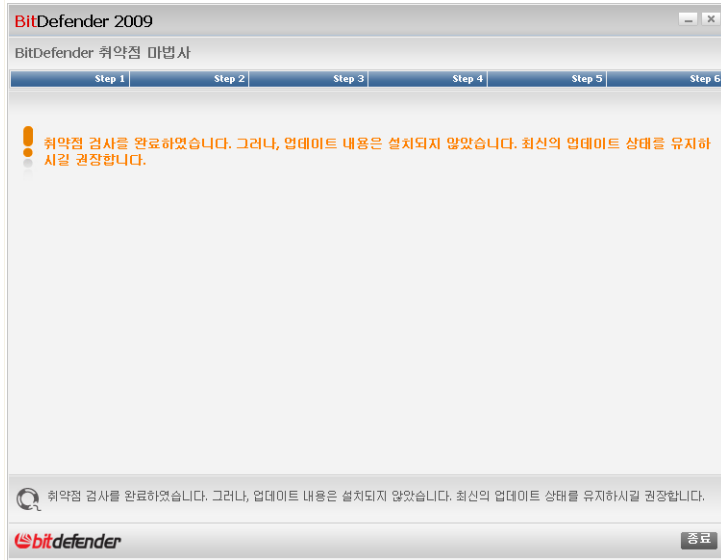
윈도 업데이트

현재 여러분 컴퓨터에 설치되어 있지 않은 중요한 윈도 업데이트들과 중요하지 않은 업데이트들의 목록이 보일 것입니다. 모든 사용할 수 있는 업데이트들을 설치하려면, 모든 시스템 업데이트 설치를 클릭하십시오.

다음을 클릭하십시오.



6/6 단계 - 보기 결과들



결과들

단기를 클릭하십시오.

19.2. 설정들

자동취약성확인을 설정하려면, 상세보기 내의 취약성>설정들로 가십시오.



여러분이 주기적으로 확인하기 원하시는 시스템 취약성들에 해당하는 체크박스들을 선택하십시오.

- 매우 중요한 윈도 업데이트들
- 정기적 윈도 업데이트들
- 약한 비밀번호들
- 프로그램 업데이트



참고

특정 취약성에 해당하는 체크박스를 해제하면, 비트펜더는 더 이상 여러분에게 관련 문제들을 알려드리지 않을 것입니다.



20. 게임 / 랩탑 모드

게임 / 랩탑 모드 모듈은 여러분이 비트펜더의 특수한 작동모드들을 설정할 수 있게 합니다.

- **게임 모드**는 여러분이 휴식 중일 때 자원소비를 최소화하기 위해 제품설정들을 임시로 수정합니다.
- **랩탑 모드**는 배터리 전력을 아끼기 위해 랩탑이 배터리로 작동 중일 때에는 예약된 작업들이 실행되지 못하게 합니다.

20.1. 게임모드

게임 모드는 시스템 성능에 대한 영향을 최소화하기 위해 보호설정들을 임시로 수정합니다. 게임모드 동안 다음 설정들이 적용됩니다:

- 모든 비트펜더 경고들과 팝업창들이 해제되었습니다.
- 비트펜더 실시간 보호수준이 허용에 맞춰져 있습니다.
- 기본값에 따라 업데이트들이 실행되지 않습니다.



참고

이 설정을 변경하려면, **업데이트>설정들**로 가서 게임모드가 켜져 있으면 업데이트 하지 마십시오 체크박스를 해제하십시오.

- 예약된 검사작업들은 기본값에 따라 해제되어 있습니다.

기본값으로, 비트펜더는 여러분이 알려진 게임들에 대한 비트펜더의 목록으로부터 게임을 시작하거나 어떤 프로그램이 전체 화면으로 될 때 자동으로 게임모드로 들어갑니다. 여러분은 기본값이 Ctrl+Alt+Shift+G 단축키를 사용해 수동으로 게임모드로 들어갈 수 있습니다. 게임을 마쳤으면 게임모드를 나가도록 강력히 권장합니다(같은 기본값 Ctrl+Alt+Shift+G를 사용할 수 있습니다).



참고

게임모드에 있는 동안,  비트펜더 아이콘 위에 G 문자가 보일 것입니다.

게임모드를 설정하려면, 상세보기 내의 게임/노트북 모드>게임모드로 이동합니다.



게임모드

이 영역 상단에, 게임모드 상태를 볼 수 있습니다. 현재 상태를 변경하려면 게임 모드 들어가기 혹은 게임모드 나가기를 클릭할 수 있습니다.

20.1.1. 자동게임모드 설정

자동게임모드는 어떤 게임이 탐지되었을 때 비트펜더가 자동으로 게임모드로 들어갈 수 있게 합니다. 여러분은 다음 선택사항들을 설정할 수 있습니다:

- 비트펜더가 제공한 게임들의 기본값 목록 - 알려진 게임들에 대한 비트펜더 목록으로부터 어떤 게임을 시작할 때 자동으로 게임모드로 들어갑니다. 이 목록을 보려면, 게임들 관리를 클릭하고, 그 다음 허가된 게임들 보기를 클릭하십시오.
- 전체화면으로 있을 때 게임모드 들어가기 - 어떤 응용프로그램이 전체화면으로 갈 때 자동으로 게임모드로 들어갑니다.



- 응용프로그램을 게임목록에 추가 - 여러분이 전체화면을 나갈 때 새 응용프로그램을 게임목록에 추가하도록 알립니다. 어떤 새 응용프로그램을 게임목록에 추가함으로써, 여러분이 다음에 그 응용프로그램을 시작할 때 비트펜더가 자동으로 게임모드로 들어갈 것입니다.

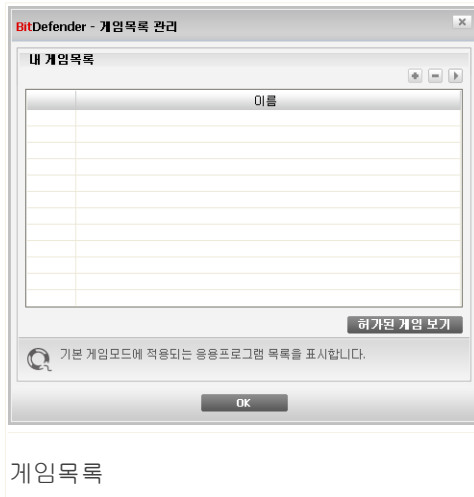


참고

비트펜더가 자동으로 게임모드로 들어가는 것을 원치 않으실 경우, 자동게임모드 체크박스를 해제하십시오.

20.1.2. 게임목록 관리

어떤 응용프로그램을 게임목록에서 시작하면 비트펜더는 자동으로 게임모드로 들어갑니다. 게임목록을 보고 관리하려면, 게임들 관리를 클릭하십시오. 새로운 창이 나타날 것입니다.



다음과 같을 때 새 응용프로그램들이 자동으로 목록에 추가됩니다:

- 비트펜더의 알려진 게임목록에서 어떤 게임을 시작할 때. 이 목록을 보시려면, 허가된 게임들 보기를 클릭하십시오.
- 전체화면을 나갈 후, 여러분이 프롬프트 창에서 그 응용프로그램을 게임목록에 추가할 때.



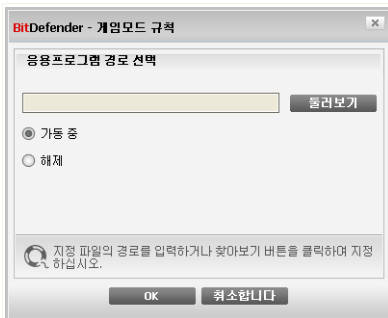
목록에서 어떤 특정 응용프로그램에 대한 자동게임모드를 해제하려면, 해당 체크박스를 해제하십시오. 웹브라우저와 동영상재생기와 같이 전체화면이 되는 정상 응용프로그램들에 대한 자동게임모드를 해제해야 합니다.

게임목록을 관리하려면, 표 상단에 위치한 다음과 같은 버튼들을 사용할 수 있습니다:

- ➕ 추가 - 게임목록에 새로운 응용프로그램을 추가합니다.
- - 제거 - 게임목록에서 응용프로그램을 제거합니다.
- ➡ 수정 - 게임목록의 응용프로그램 정보를 수정합니다.

게임 추가 혹은 편집

게임목록에서 어떤 항목을 추가 혹은 편집할 때 다음 창이 나타날 것입니다:



게임추가

응용프로그램을 선택하거나 편집 칸에 응용프로그램으로의 전체경로를 입력하려면 둘러보기를 클릭하십시오.

선택된 응용프로그램이 시작되었을 때 자동으로 게임모드로 들어가기를 원하지 않을 때에는 해제를 선택하십시오.

항목을 게임목록에 추가하려면 OK를 클릭하십시오.

20.1.3. 게임모드 설정

예약된 작업들에 대한 거동을 설정하려면 다음 선택사항들을 사용하십시오:



- 작업 검사 - 게임모드에 있는 동안에는 예약된 작업들이 실행되지 못하게 합니다. 여러분은 다음 선택사항들 중 하나를 선택할 수 있습니다:

옵션	설명
작업건너뛰기	예약된 작업을 절대로 실행하지 마십시오.
작업연기	여러분이 게임모드를 나간 직후 예약된 작업을 실행하십시오.

20.1.4. 게임모드 단축키 바꾸기

여러분은 기본값이 Ctrl+Alt+Shift+G 단축키를 사용해 수동으로 게임모드로 들어갈 수 있습니다. 단축키를 변경하기 원하실 경우, 이 단계들을 따르십시오:

1. 고급설정들을 클릭하십시오. 새로운 창이 나타날 것입니다.



고급설정들

2. 단축키 사용하기선택사항 아래에서 다음과 같은 방법으로 원하는 단축키를 설정하십시오:

- 다음 중 하나를 클릭해서, 여러분이 사용하기 원하시는 수정키들을 선택하십시오: 제어키 (Ctrl), 시프트 키 (Shift) 혹은 알트 키 (Alt)
- 편집 칸에서, 여러분이 사용하기 원하시는 일반적인 키에 해당하는 문자를 입력하십시오.



예를 들면, Ctrl+Alt+D 단축키를 사용하기 원하실 경우, 여러분은 오직 Ctrl와 Alt 만 체크하고 D를 입력해야 합니다.

3. 변경 사항을 저장하려면 확인을 클릭하십시오.



참고

단축키 사용 옆의 체크표시를 제거하면 단축키 기능이 해제될 것입니다.

20.2. 랩탑 모드

랩탑모드는 랩탑 및 노트북 사용자들을 위해 특별히 고안되었습니다. 이 모드의 목적은 이 장치들이 배터리로 작동 중일 때 비트디펜더의 전력소모영향을 최소화하는 것입니다.

랩탑모드에 있는 동안에는 기본값에 따라 예약된 작업들이 실행되지 않습니다.

비트디펜더는 여러분의 랩탑이 언제 배터리 전원으로 전환했는지를 탐지하고, 자동으로 랩탑모드로 들어갑니다. 마찬가지로, 비트디펜더는 랩탑이 더 이상 배터리로 작동하고 있지 않다는 것을 탐지할 때 자동으로 랩탑모드를 나갑니다.

노트북모드를 설정하려면, 고급보기의 게임/노트북모드>노트북모드로 이동합니다.



여러분은 랩탑모드가 가동되었는지를 볼 수 있습니다. 만약 랩탑모드가 가동되어 있으면, 비트펜더는 랩탑이 배터리로 작동 중일 때 설정을 적용할 것입니다.

20.2.1. 랩탑모드 설정

예약된 작업들에 대한 거동을 설정하려면 다음 선택사항들을 사용하십시오:

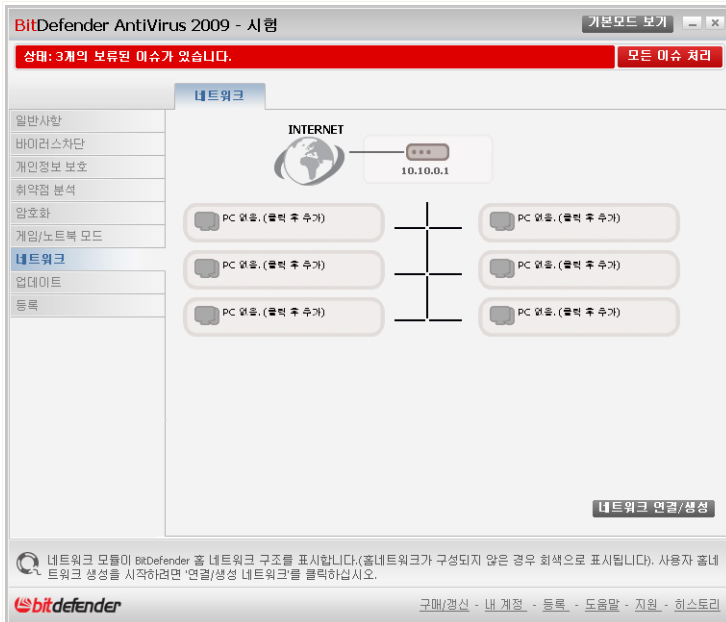
- 검사 작업 - 노트북모드에 있는 동안에는 예약된 검사작업들이 실행되지 못하게 합니다. 여러분은 다음 선택사항들 중 하나를 선택할 수 있습니다:

옵션	설명
작업건너뛰기	예약된 작업을 절대로 실행하지 마십시오.
작업연기	랩탑모드를 나간 직후 예약된 작업을 실행하십시오.



21. 네트워크

네트워크 모듈은 여러분의 가정용 컴퓨터들에 설치된 비트디펜더 제품들을 한 대의 컴퓨터에서 관리할 수 있게 합니다.



네트워크 지도

여러분의 가정용 컴퓨터들에 설치된 비트디펜더 제품들을 관리하기 위해서는 다음 단계들을 따라야 합니다:

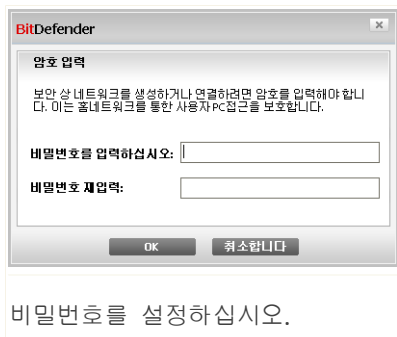
1. 여러분 컴퓨터의 비트디펜더 가정용 네트워크에 동참하십시오. 네트워크에 동참하려면 가정용 네트워크 관리를 위한 관리자 비밀번호 설정이 필요합니다.
2. 관리하기 원하는 각 컴퓨터로 가서 네트워크에 동참하십시오(비밀번호 설정).
3. 여러분 컴퓨터로 가서 여러분이 관리하기 원하는 컴퓨터들을 추가하십시오.



21.1. 비트펜더 네트워크에 동참하기

비트펜더 가정용 네트워크에 동참하려면 이 단계들을 따르십시오:

1. 네트워크 동참/생성을 클릭하십시오. 여러분은 가정용 네트워크 관리 비밀번호를 설정하도록 요구받을 것입니다.



비밀번호를 설정하십시오.

보안 상 네트워크를 생성하거나 연결하려면 암호를 입력해야 합니다. 이는 홈네트워크를 통한 사용자 PC 접근을 보호합니다.

비밀번호를 입력하십시오:

비밀번호 재입력:

OK 취소합니다

2. 각 편집칸에 동일한 비밀번호를 입력하십시오.
3. 확인을 클릭하십시오.

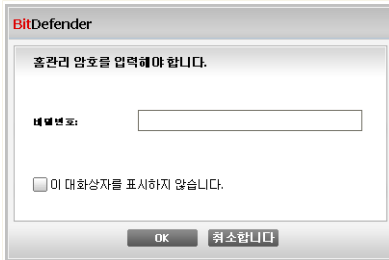
네트워크 지도에 컴퓨터이름이 보일 것입니다.

21.2. 비트펜더 네트워크에 컴퓨터들을 추가하기

비트펜더 가정용 네트워크에 한 컴퓨터를 추가할 수 있기 전에, 여러분은 각 컴퓨터 상의 비트펜더 가정용 네트워크 관리 비밀번호를 설정해야 합니다.

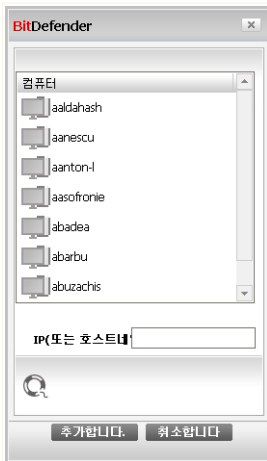
비트펜더 가정용 네트워크에 어떤 컴퓨터를 추가하려면, 이 단계들을 따르십시오:

1. 네트워크 관리를 클릭하십시오. 여러분은 지역의 가정용 네트워크 관리비밀번호를 제공하도록 요구받을 것입니다.



비밀번호를 입력하십시오.

- 가정용 관리비밀번호를 입력하고 OK를 클릭하십시오. 새로운 창이 나타날 것입니다.



컴퓨터를 추가하십시오.

네트워크에 여러 컴퓨터들이 보일 것입니다. 아이콘의 의미는 다음과 같습니다:

-  어떤 비트펜더 제품도 설치되지 않은 온라인 컴퓨터를 가리킵니다.
-  비트펜더가 설치된 온라인 컴퓨터를 가리킵니다.



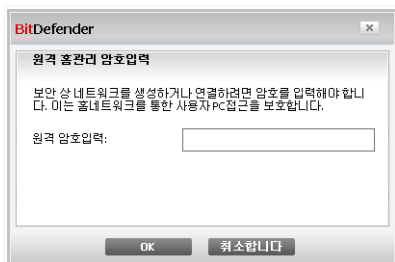
■  비트펜더가 설치된 오프라인 컴퓨터를 가리킵니다.

3. 다음 중 한 가지를 실행하십시오:

■ 추가할 컴퓨터의 이름을 목록에서 선택하십시오.

■ 추가할 컴퓨터의 IP주소 혹은 이름을 해당 칸에 입력하십시오.

4. 추가를 클릭하십시오. 여러분은 각 컴퓨터의 가정용 네트워크 관리 비밀번호를 입력하도록 요구받을 것입니다.



인가하기

5. 각 컴퓨터 상에 설정된 가정용 네트워크 관리비밀번호를 입력하십시오.

6. 확인을 클릭하십시오. 만약 여러분이 바른 비밀번호를 제공했으면, 선택된 컴퓨터 이름이 네트워크 지도에 나타날 것입니다.



참고

여러분은 네트워크 지도에 다섯 대의 컴퓨터까지 추가할 수 있습니다.

21.3. 비트펜더 네트워크 관리하기

여러분이 비트펜더 가정용 네트워크를 성공적으로 생성했으면, 여러분은 한 대의 컴퓨터에서 모든 비트펜더 제품들을 관리할 수 있습니다.



네트워크 지도

만약 네트워크 지도에서 어떤 컴퓨터 위로 마우스 커서를 옮기면, 시스템 보안, 비트펜더 등록상태에 영향을 주는 문제들의 이름, IP주소, 번호 등 이에 대한 짧은 정보가 보일 것입니다.

만약 네트워크 지도에서 어떤 컴퓨터 이름을 오른쪽 클릭하면, 원격컴퓨터에서 작동할 수 있는 모든 관리 작업들이 보일 것입니다.

- 이 컴퓨터 등록하기
- 비밀번호 설정하기
- 검사작업 실행
- 이 컴퓨터에 관한 문제 고치기
- 이 컴퓨터의 이력을 보이기
- 지금 이 컴퓨터 상에서 업데이트 실행

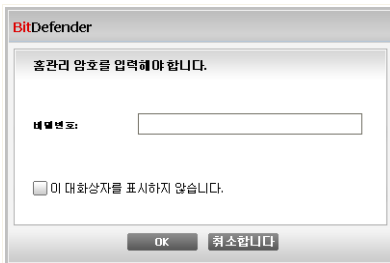


■프로필 적용

■이 컴퓨터에 대한 시스템조정 실행

■이 컴퓨터를 이 네트워크의 업데이트 서버로 설정하십시오

특정 컴퓨터 상에서 작업을 실행하기 전에, 여러분은 지역의 가정용 관리 비밀번호를 제공하도록 요구받을 것입니다.



비밀번호를 입력하십시오.

가정용 관리비밀번호를 입력하고 OK를 클릭하십시오.



참고

만약 여러분이 몇몇 작업들을 실행할 계획이라면, 여러분은 이 세션에서 이 메시지 다시 보이지 않기를 선택하실 것입니다. 이 선택사항을 선택함으로써, 여러분은 현재 세션에서는 이 비밀번호를 다시 요구받지 않을 것입니다.



22. 업데이트

악성프로그램은 매일 찾아지게 마련입니다. 이는 비트펜더를 늘 최신 악성소프트웨어 서명된 상태로 두어야 하는 중요한 이유입니다.

광대역 혹은 DSL로 인터넷에 연결되어 있으면, 비트펜더는 자체적으로 실행할 것입니다. 기본적으로, 비트펜더는 여러분이 컴퓨터를 켜 때와 그 후 매 시간 업데이트를 확인합니다.

만약 어떤 업데이트가 탐지되었다면, **자동업데이트설정들**에 따라 여러분이 업데이트를 확인하도록 요구를 받거나 업데이트가 자동으로 실행될 것입니다.

업데이트 과정은 업데이트되는 파일이 점진적으로 교체되는 방식으로 이루어집니다. 이런 식으로, 업데이트과정은 제품의 작동에 영향을 미치지 않을 것이고, 동시에 어떤 취약성도 배제될 것입니다.

다음의 방법에 따라 업데이트를 진행합니다.

- **바이러스 방지 엔진 업데이트** - 새로운 위험요소가 나타나면 바이러스 서명을 포함하는 파일을 업데이트하여 지속적인 보호를 받아야 합니다. 이러한 형식의 업데이트를 바이러스 정의 업데이트라고 합니다.
- **염탐소프트웨어 엔진 업데이트** - 새로운 염탐소프트웨어 서명을 데이터베이스에 추가합니다. 이 업데이트 형식을 염탐소프트웨어 방지 업데이트라고 합니다.
- **제품 업그레이드** - 제품의 새 버전이 출시될 때, 제품의 성능 향상을 위해 새로운 특징과 검사 기술이 도입됩니다. 이러한 업데이트 종류는 제품 업데이트라고 합니다.

22.1. 자동 업데이트

업데이트관련 정보를 보고 자동업데이트를 실행하려면, 상세보기 내의 업데이트> 업데이트로 가십시오.



BitDefender AntiVirus 2009 - 시험

상태: 3개의 보류된 미슈가 있습니다. 모든 미슈 처리

업데이트 설정

☒ 자동 업데이트가 활성화됩니다.

마지막 확인 2009-02-02 12:43:39
마지막 업데이트 절대 아님 [지금 업데이트](#)

안티바이러스 서명 속성

바이러스 서명 2624271
엔진 버전 7.23394 [바이러스 서명 보기](#)

다운로드 상태

업데이트가 취소되었습니다. 검사 프로세스를 중지합니다. 다시 시도하십시오.

파일: 0 % 0 kb
총 업데이트 0 % 0 kb

BitDefender 제품이 정상적으로 바이러스 시그니처를 업데이트하도록 유지하려면 자동 업데이트 사용을 유지하기 바랍니다.

VBApi Info Window

자동 업데이트

여기서 마지막 실행된 업데이트(성공적이었는지 오류가 일어났는지)에 관한 정보 뿐 아니라 업데이트 마지막 확인 및 업데이트 마지막 실행 시기도 볼 수 있습니다. 또한, 현재 엔진버전 및 서명번호에 관한 정보도 나타납니다.

업데이트 도중 이 부분을 열면, 내림받기 상태가 보일 것입니다.



중요

최신 위협들로부터 보호받으려면, 자동업데이트를 가동된 상태로 두십시오.

바이러스목록 보이기를 클릭해서 여러분의 비트펜더의 악성프로그램 서명들을 얻을 수 있습니다. 구할 수 있는 모든 서명들을 담은 HTML파일이 생성되어 웹브라우저에 열릴 것입니다. 특정 악성프로그램 서명이 있는지 데이터베이스를 검색하거나 온라인 비트펜더 서명데이터베이스로 가기 위해 비트펜더 바이러스목록을 클릭할 수 있습니다.



22.1.1. 업데이트 요청

자동업데이트는 지금업데이트하기를 클릭해서 언제든지 할 수 있습니다. 이런 업데이트는 또한 사용자 요청 업데이트라고도 알려져 있습니다.

업데이트 모듈이 비트펜더 업데이트 서버에 연결되어 어떤 업데이트가 있는지 확인할 것입니다. 만약 어떤 업데이트가 탐지되면, **수동업데이트설정** 절 안에 설정된 선택사항들에 따라, 업데이트를 묻거나 업데이트가 자동으로 실행될 것입니다.



중요

업데이트 완료 후에 재 시작을 요청하는 경우가 있습니다. 이 때는 가능한 빨리 컴퓨터를 재시작하시기 바랍니다.

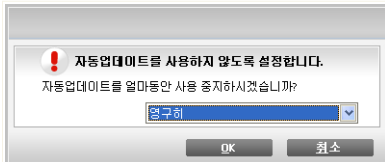


참고

전화선으로 인터넷에 연결되어 있다면, 사용자 요청을 통해 비트펜더를 정기적으로 업데이트하시기를 권장합니다.

22.1.2. 자동업데이트 해제하기

자동업데이트를 해제하려면, 경고창이 나타날 것입니다.



자동업데이트 해제

자동업데이트를 얼마나 오랫동안 해제해 둘지 메뉴에서 선택해야 합니다. 자동업데이트는 5, 15 혹은 30분, 영구적으로 혹은 시스템이 재시작할 때까지 해제된 상태로 둘 수 있습니다.



주의

이는 매우 중요한 보안문제입니다. 저희는 업데이트를 되도록 해제된 상태에 두지 않도록 권장합니다. 만약 비트펜더가 정기적으로 업데이트되지 않으면, 최신 위협들로부터 여러분을 보호하지 않을 것입니다.



22.2. 업데이트 설정들

로컬 컴퓨터에서 인터넷을 통해 직접적으로 혹은 프록시 서버를 통해 업데이트가 시행될 수 있습니다. 기본적으로, 비트디펜더는 매시간 인터넷으로 업데이트를 확인해서, 여러분에게 경고하지 않고 구할 수 있는 업데이트를 설치할 것입니다.

업데이트를 설정하고 프록시를 관리하려면, 상세보기 내의 업데이트>설정들로 가십시오.

BitDefender AntiVirus 2009 - 시험 [기본모드 보기]

상태: 3개의 보류된 미수가 있습니다. [모든 미수 처리]

업데이트 설정들

업데이트 위치 설정
 우선 업데이트 위치 설정: ☐ 프록시 사용
 대체 업데이트 위치 설정: ☐ 프록시 사용

자동 업데이트 설정
 시간 간격: 시간
 업데이트 확인:
☐ 사일런트 업데이트
☒ 업데이트 다운로드 전 요청
☐ 업데이트 설치 전 요청

수동 업데이트 설정
☐ 사일런트 업데이트
☒ 업데이트 다운로드 전 요청

고급 설정
☐ 요청 대신 재시작을 기다립니다.
☒ 검사가 진행 중인 경우, 업데이트를 하지 않습니다.
☒ 게임모드 상태에서는 업데이트 하지 않습니다.

[적용] [초기] [프록시 관리]

BitDefender 사용자 인터페이스에서 제공하는 개별 옵션에 대한 설명을 위해서는 창위로 마우스 커서를 이동하십시오. 관련된 도움말 문장이 표시됩니다.

VBApi Info Window

업데이트 설정들

업데이트 설정들은 4 분류로 나뉘어집니다(업데이트위치설정, 자동업데이트설정, 수동업데이트설정 및 고급설정). 각 분류는 별도로 설명됩니다.



22.2.1. 업데이트위치 설정

업데이트위치를 설정하려면, 업데이트위치설정 분류에서 선택사양들을 사용하십시오.



참고

이 설정들은 오직 비트펜더 악성프로그램 서명들을 지역적으로 저장하는 지역네트워크에 연결되어 있거나 프록시서버를 통해 인터넷에 연결될 때에만 설정하십시오.

더 신뢰성이 있고 빠른 업데이트를 위해서는, 다음과 같이 두 업데이트 위치를 설정할 수 있습니다: 1차 업데이트 위치 및 대체 업데이트 위치. 기본적으로, 이 위치들은 <http://upgrade.bitdefender.com>에 같이 설정되어 있습니다.

업데이트 위치들 중 하나를 수정하려면, 수정하기 원하는 위치에 해당하는 URL 칸 안에 지역 미러 URL을 입력하십시오.



참고

지역미러를 이용할 수 없게 될 때를 위한 고장안전계획의 일환으로서 지역미러를 1차 업데이트위치로 설정하고 대체 업데이트위치는 변경되지 않은 상태로 두도록 권장합니다.

회사가 프록시서버를 사용해 인터넷에 연결하는 경우, 프록시를 설정하기 위해 프록시 사용을 체크한 후 프록시 관리를 클릭하십시오. 추가 정보는 “[프록시 관리](#)” (p. 194)를 참조하십시오.

22.2.2. 자동업데이트 설정

비트펜더가 자동으로 실행하는 업데이트과정을 설정하려면, 자동업데이트설정 분류 내의 선택사양들을 사용하십시오.

시간간격 칸 내에 업데이트 연속2회 확인 간 시간을 지정할 수 있습니다. 기본적으로, 업데이트 시간간격은 1시간으로 맞춰져 있습니다.

자동업데이트과정 실행방법을 지정하려면, 다음 선택사양들 중 하나를 선택하십시오:

- 사일런트 업데이트 — BitDefender가 업데이트를 자동 다운로드 및 설치합니다.
- 업데이트 내림받기 전 알림 — 업데이트가 있을 때마다, 업데이트를 내림받기 전에 여러분에게 알릴 것입니다.
- 업데이트 설치 전 알림 — 업데이트를 내림받았을 때마다 업데이트 설치 전에 여러분에게 알릴 것입니다.



22.2.3. 수동업데이트 설정

수동업데이트(사용자 요청에 의한 업데이트) 방법을 지정하려면, 수동업데이트 설정 분류 내의 다음 선택사항들 중 하나를 선택하십시오:

- **조용한 업데이트** - 수동업데이트가 사용자 관여 없이 배경에서 자동으로 실행될 것입니다.
- **업데이트 내림받기 전 알림** - 업데이트가 있을 때마다, 업데이트를 내림받기 전에 여러분에게 알릴 것입니다.

22.2.4. 고급설정

비트펜더 업데이트 과정이 여러분 작업에 방해를 하지 않게 하려면, 고급설정 분류 내의 다음 선택사항들을 설정하십시오:

- **요청 대신 재시작을 기다립니다** - 업데이트를 위해 재시작을 해야 하는 경우, 시스템이 재시작될 때까지는 예전 파일을 계속 사용할 것입니다. 사용자는 재시작 요청을 받지 않을 것이며, 이렇게 BitDefender 업데이트 프로세스가 사용자의 업무에 지장을 주지 않을 것입니다.
- **검사가 진행 중인 경우, 업데이트를 하지 않습니다** - 검사가 진행 중인 경우, BitDefender는 업데이트를 하지 않을 것입니다. 이러한 방식으로 BitDefender 업데이트 프로세스가 검사 태스크에 지장을 주지 않을 것입니다.



참고

검사 진행 중 BitDefender가 업데이트 된다면, 검사 프로세스가 중지될 것입니다.

- **게임모드가 켜져 있을 때 업데이트 하지 않기** - 만약 게임모드가 켜져 있으면 비트펜더는 업데이트하지 않을 것입니다. 이런 식으로, 여러분은 게임 중 시스템에 대한 제품의 영향을 최소화할 수 있습니다.

22.2.5. 프록시 관리

만약 여러분 회사가 프록시 서버를 사용해 인터넷에 연결하면, 여러분은 비트펜더가 자체적으로 업데이트하도록 프록시 설정을 지정해야 합니다. 그렇지 않을 경우, 비트펜더는 제품을 설치한 관리자 혹은 현재 사용자 기본브라우저의 프록시 설정을 사용할 것입니다.



참고

프록시설정들은 컴퓨터 관리권한이 있는 사용자들 혹은 파워유저(제품설정에 대한 비밀번호를 아는 사용자)만 할 수 있습니다.

프록시설정들을 관리하려면, 프록시 관리를 클릭하십시오. 프록시 관리자 창이 나타날 것입니다.

프록시 설정

관리자 프록시 설정(설치 시 검지된 것)

주소: 포트: 사용자이름:
암호:

현재 사용자 프록시 설정 (기본 브라우저에서)

주소: 포트: 사용자이름:
암호:

사용자의 프록시 설정을 구성합니다.

주소: 포트: 사용자이름:
암호:

☐ 관리자 프록시 설정을 변경합니다.

OK 취소합니다

프록시 관리자

프록시 설정에는 다음과 같이 세 가지가 있습니다:

- 관리자 프록시 설정(설치 시 탐지됨) — 설치 중에 관리자의 계정에서 탐지되고 여러분이 그 계정에 로그인 된 경우에만 설정할 수 있는 프록시 설정들입니다. 만약 이 프록시 서버가 사용자이름과 비밀번호를 요구할 경우, 여러분은 해당 칸에 그 정보를 입력해야 합니다.
- 현재 사용자 프록시 설정들(기본브라우저에서) — 기본 브라우저에서 나온, 현재 사용자의 프록시 설정들입니다. 만약 프록시 서버가 사용자이름과 비밀번호를 요구하는 경우, 해당 칸에 그 정보를 입력해야 합니다.



참고

지원되는 웹브라우저들은 인터넷 익스플로러, 모질라 파이어폭스 및 오페라입니다. 만약 기본적으로 다른 브라우저를 사용할 경우, 비트펜더는 현재 사용자의 프록시 설정들을 얻지 못할 것입니다.

■ 여러분 나름의 프록시 설정들 — 여러분이 관리자로 로그인되었을 때 여러분이 설정할 수 있는 프록시 설정들입니다.

다음 설정들을 지정해야 합니다:

주소 — 프록시 서버 IP를 입력합니다.

포트 — 비트펜더가 프록시 서버에 연결하기 위해 사용하는 포트를 입력합니다.

사용자이름 — 프록시가 인정하는 사용자이름을 입력합니다.

비밀번호 — 이전에 지정된 사용자의 유효한 비밀번호를 입력합니다.

인터넷 연결을 시도할 때, 비트펜더가 연결하게 될 때까지 각 프록시 설정들이 한번씩 시도됩니다.

우선, 인터넷에 연결하기 위해 여러분 나름의 프록시 설정들을 담은 설정이 사용될 것입니다. 만약 이 설정으로 연결되지 않으면, 다음에는 설치 시에 탐지된 프록시 설정들이 시도될 것입니다. 마지막으로, 만약 그 설정들을 사용해서도 연결되지 않으면, 인터넷 연결을 위해 현재 사용자의 프록시 설정들이 기본브라우저에서 인출되어 사용될 것입니다.

변경사항들을 저장하고 창을 닫으려면 OK를 클릭하십시오.

변경 사항을 적용하려면 적용을 클릭하고, 초기 설정을 불러오려면 디폴트를 클릭하십시오.



23. 등록

여러분 비트펜더 제품 및 등록상태에 관한 전체 정보를 찾으시려면, 상세보기 내의 등록으로 가십시오.

BitDefender AntiVirus 2009 - 시험

상태: 3개의 보류된 예수가 있습니다. 모든 이슈 처리

등록

일반사항
바이러스차단
개인정보 보호
취약점 분석
암호화
게임/노트북 모드
네트워크
업데이트

제품 정보
BitDefender Antivirus 2009
버전: 12.0.11.4

등록 정보
estare.automata@mailinator.com에 등록되었습니다.
30 후에 만료됩니다.
라이선스 키: 704BE27EF7785580DF8

조치들
개인 생성
지금 등록

사용자의 BitDefender 제품, 라이선스 종류, 유효기간 및 라이선스 키에 대한 상세정보를 확인할 수 있습니다.

bitdefender 구매/결산 · 내 계정 · 등록 · 도움말 · 지원 · 히스토리

등록

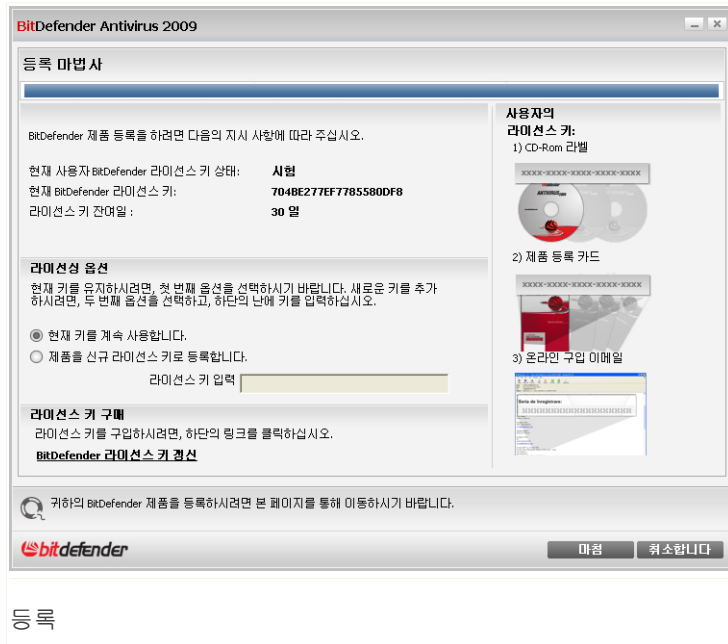
이 절에는 다음 정보가 나타납니다:

- 제품정보: 비트펜더 제품 및 버전.
- 등록정보: 여러분의 비트펜더 계정(설정된 경우)으로 로그인하는데 사용되는 이메일주소, 현재 사용면허번호 및 사용면허만료까지 남은 날수



23.1. 비트디펜더 바이러스차단 2009 등록하기

제품등록창을 열려면 지금등록하기를 클릭하십시오.



BitDefender Antivirus 2009

등록 마법사

BitDefender 제품 등록을 하려면 다음의 지시 사항에 따라 주십시오.

현재 사용자 BitDefender 라이선스 키 상태: **시험**
 현재 BitDefender 라이선스 키: **704BE277EF7785S80DF8**
 라이선스 키 잔여일: **30 일**

라이선스 옵션

현재 키를 유지하려면, 첫 번째 옵션을 선택하시기 바랍니다. 새로운 키를 추가 하려면, 두 번째 옵션을 선택하고, 하단의 난제 키를 입력하십시오.

☒ 현재 키를 계속 사용합니다.
☐ 제품을 신규 라이선스 키로 등록합니다.

라이선스 키 입력:

라이선스 키 구매

라이선스 키를 구입하려면, 하단의 링크를 클릭하십시오.
BitDefender 라이선스 키 검색

사용자의 라이선스 키:
 1) CD-Rom 라벨
 2) 제품 등록 카드
 3) 온라인 구입 이메일

귀하의 BitDefender 제품을 등록하시려면 본 페이지를 통해 이동하시기 바랍니다.

bitdefender

등록

마침 취소합니다

여러분은 비트디펜더 등록상태, 현재 면허 비밀번호 및 면허가 만기될 때까지 며칠이 남았는지를 볼 수 있습니다.

비트디펜더 바이러스차단 2009를 등록하려면:

1. 새 비밀번호를 사용해 제품을 등록하기 원합니다를 선택하십시오.
2. 편집 필드에 면허번호를 입력하십시오.



참고

여러분의 면허번호를 다음에서 찾을 수 있습니다.



- CD라벨 위
- 제품등록카드 위
- 온라인 구매 이메일 내

빗디펜더 면허번호가 없으시면, 제시된 링크를 클릭해서 빗디펜더 온라인 매장에서 하나를 구입하십시오.

완료를 클릭하십시오.

23.2. 빗디펜더 계정 만들기

등록절차의 일부분으로써 BitDefender 계정을 반드시 생성해야 합니다. BitDefender 계정을 통하여, 업데이트, 무료고객지원 및 특별제안과 판매행사정보를 수령할 수 있습니다. 만약 빗디펜더 면허 비밀번호를 잃어버릴 경우, <http://myaccount.bitdefender.com>에서 여러분 계정으로 들어가 다시 찾을 수 있습니다.



중요

BitDefender를 설치한 후 15일 이내에 사용자는 계정을 생성해야 합니다.(등록 시 30일로 연장됩니다.) 그렇지 않으면, BitDefender가 더이상 업데이트되지 않습니다.

만약 아직 빗디펜더 계정을 만들지 않았으면, 계정 만들기를 클릭해서 계정등록창을 여십시오.



BitDefender Antivirus 2009

계정 생성

내 계정 등록

사용제품 및 바이러스 엔진, 바이러스 시그니처를 최신의 상태로 유지하기 위해서는 제품을 등록하고 BitDefender 계정을 생성하시기 바랍니다. 최신상태 유지를 통하여 사용자 시스템을 안전하게 보호할 수 있습니다. 등록에 대한 자세한 정보는 BitDefender 고객센터에 문의하시기 바랍니다. <http://www.bitdefenderkorea.com>

☒ **현존 BitDefender 계정에 서명**

이메일 주소:

비밀번호:

비밀번호를 잊어버리셨습니까?

☐ 나중에 등록합니다.

☐ **새로운 BitDefender 계정 만들기**

이메일 주소:

암호(6-16문자):

암호확인:

이름:

성:

국가:

☒ BitDefender의 모든 소식을 알려주세요.
☐ 가장 중요한 메시지만 전송하십시오.
☐ 아무런 메시지도 보내지 않습니다.

파일

마침 **취소합니다**

계정만들기

지금 비트펜더 계정을 만들기 원하지 않으시면, 등록건너뛰기를 선택 후, 마치를 클릭하십시오. 그렇지 않으면, 여러분의 현재 상황에 따라 진행하십시오.

- “저는 비트펜더 계정이 없습니다.” (p. 200)
- “이미 비트펜더 계정을 가지고 있습니다.” (p. 201)

저는 비트펜더 계정이 없습니다.

비트펜더 계정을 만들려면, 새 비트펜더 계정 만들기를 선택해서 필요한 정보를 제공하십시오. 여러분이 여기서 제공하시는 데이터는 기밀정보로 유지될 것입니다.

- 이메일 주소 - 사용자 메일주소를 입력하십시오.
- 비밀번호 - 여러분 비트펜더 계정의 비밀번호를 입력하십시오. 비밀번호는 최소 여섯 자리 글자가 되어야 합니다.



■비밀번호 재입력 — 이전 비밀번호를 다시 입력하십시오.

■이름 — 여러분의 이름을 입력하십시오.

■성 — 여러분의 성을 입력하십시오.

■국가 — 여러분의 거주국가를 선택하십시오.



참고

제공된 이메일 주소와 비밀번호를 사용해 <http://myaccount.bitdefender.com>에서 여러분 계정으로 들어가십시오.

계정을 성공적으로 만들기 위해, 여러분은 우선 여러분의 이메일 주소를 활성화해야 합니다. 여러분의 이메일 주소를 확인하고 비트펜더 등록서비스에서 여러분에게 보낸 이메일의 지침들을 따르십시오.

또한, 비트펜더는 여러분 계정의 이메일 주소를 사용해 여러분에게 특별제안 및 판매행사에 관한 정보를 보낼 수 있습니다. 다음 선택사항들 중 하나를 선택하십시오:

■비트펜더로부터의 모든 메시지들을 보내주세요

■가장 중요한 메시지만 보내주세요

■아무 메시지도 보내지 말아주세요

완료를 클릭하십시오.

이미 비트펜더 계정을 가지고 있습니다.

비트펜더는 여러분 컴퓨터에 여러분이 이전에 등록한 비트펜더 계정이 있는지 자동으로 탐지합니다. 이 경우, 여러분 계정 비밀번호를 알려주십시오.

만약 여러분이 활성화된 계정이 이미 있지만 비트펜더가 그것을 탐지하지 못하는 경우, 기존 비트펜더 계정으로 들어가십시오를 선택한 후 여러분 계정의 이메일주소와 비밀번호를 입력하십시오.

여러분의 비밀번호를 잊어버리신 경우, 비밀번호 분실을 클릭 후, 지침들을 따르십시오.

또한, 비트펜더는 여러분 계정의 이메일 주소를 사용해 여러분에게 특별제안 및 판매행사에 관한 정보를 보낼 수 있습니다. 다음 선택사항들 중 하나를 선택하십시오:

■비트펜더로부터의 모든 메시지들을 보내주세요



BitDefender Antivirus 2009

- 가장 중요한 메시지만 보내주세요
- 아무 메시지도 보내지 말아주세요

완료를 클릭하십시오.



도움말 얻기



24. 지원

우수한 제품공급자로서, 비트펜더는 고객들에게 타의 추종을 불허하는 빠르고 정확한 지원을 제공하려고 노력합니다. 지원센터(아래 주소로 연락)는 계속해서 최신 위협들을 해결해 나갑니다. 여기는 여러분의 모든 질문들을 시의적절하게 답변하는 곳입니다.

비트펜더에서는, 가장 합리적 가격으로 가장 뛰어난 제품들을 공급함으로써 고객들의 시간과 비용을 줄이기 위한 헌신은 늘 저희의 최우선과제였습니다. 더욱이, 저희는 저희사업의 성공은 고객지원을 위한 원활한 의사소통과 두드러진 노력에 근거한다고 믿고 있습니다.

지원이 필요하신 경우 언제든지 support@bitdefender.com로 지원을 요청하시기 바랍니다. 조속한 답변을 위해, 이메일에 여러분의 비트펜더 제품 및 여러분 시스템에 관해 원하시는 만큼 상세히 적으시고, 문제를 되도록 정확히 적어서 문의하십시오.

24.1. 비트펜더 지식창고

비트펜더 지식 창고는 비트펜더 제품에 대한 온라인 정보 저장소입니다. 이는 바이러스 방어/비트펜더 솔루션 관리와 관련된 보다 일반적인 이해를 돕는 내용과 다른 많은 컬럼들과 비트펜더 지원 및 개발팀이 수행하는 기술 지원 및 버그수정의 결과에 대해 쉽게 접근할 수 있는 리포트 형태로 저장됩니다.

비트펜더 지식 창고는 일반인에게 공개되며 무료로 검색 가능합니다. 비트펜더 지식 창고는 사용자가 필요로 하는 기술 지식 및 깊이 있는 정보를 제공하는 추가적인 정보 제공 방안입니다. 비트펜더 고객으로부터 접수된 정보나 버그 리포트에 대한 요청들은 비트펜더 지식 창고 내의 버그수정 리포트, 차선 안이 될 수 있는 방안서, 제품 도움말 을 보충할 수 있는 항목과 같은 데이터로부터 해결책이 찾아 집니다.

비트펜더 지식 창고는 웹사이트 <http://kb.bitdefender.com>을 통해 언제든지 확인 가능합니다.



24.2. 도움말 요청

24.2.1. 웹 자가서비스로 가기

질문이 있으십니까? 저희 보안전문가들이 24/7 전화, 이메일 혹은 문자대화로 추가비용없이 도와드릴 수 있습니다.

아래 링크들을 따르십시오:

영어

<http://www.bitdefender.com/site/KnowledgeBase/>

독일어

<http://www.bitdefender.com/de/KnowledgeBase/>

프랑스어

<http://www.bitdefender.com/fr/KnowledgeBase/>

로마니아어

<http://www.bitdefender.com/ro/KnowledgeBase/>

스페인어

<http://www.bitdefender.com/es/KnowledgeBase/>

24.2.2. 지원티켓 열기

지원티켓을 열고 이메일을 통해 도움말을 받으려면, 이 링크들 중 하나를 따르십시오:

영어: <http://www.bitdefender.com/site/Main/contact/1/>

독일어: <http://www.bitdefender.de/site/Main/contact/1/>

프랑스어: <http://www.bitdefender.fr/site/Main/contact/1/>

로마니아어: <http://www.bitdefender.ro/site/Main/contact/1/>



스페인어: <http://www.bitdefender.es/site/Main/contact/1/>

24.3. 연락정보

원활한 의사소통은 사업성공의 핵심입니다. 지난 10년 동안, 비트펜더 회사는 저희 고객들과 동반자들의 기대를 넘도록 더 나은 의사소통을 위해 노력하여 뛰어난 명성을 이룩했습니다. 어떤 질문이라도 있으시면, 주저없이 저희에게 연락주시십시오.

24.3.1. 웹주소

판매부: sales@bitdefender.com
기술지원: support@bitdefender.com
문서화: documentation@bitdefender.com
동반자 프로그램: partners@bitdefender.com
마케팅: marketing@bitdefender.com
언론: pr@bitdefender.com
구직: jobs@bitdefender.com
바이러스 보고: virus__submission@bitdefender.com
염탐소프트웨어 보고: spam__submission@bitdefender.com
남용보고: abuse@bitdefender.com
제품 웹사이트: <http://www.bitdefender.com>
제품FTP자료보관소: <ftp://ftp.bitdefender.com/pub>
지역판매처들: http://www.bitdefender.com/partner__list
비트펜더 지식창고: <http://kb.bitdefender.com>

24.3.2. 지점들

비트펜더 사무실들은 영업 및 일반 문제들 모두에 관해 자신들의 영업지역에 관한 어떤 문의에도 응할 준비가 되어 있습니다. 각 주소들 및 연락처들은 아래에 나열되어 있습니다.

미국

비트펜더 주식회사
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
전화: 1-954-776-6262



BitDefender Antivirus 2009

웹: <http://www.bitdefender.com>

기술지원 (등록된 사용자에게 한함):

■ 이메일: support@bitdefender.com

■ 전화(무료):

미국: 1-888-868-1876

캐나다: 1-866-947-1873

고객서비스(등록된 사용자에게 한함):

■ 이메일: customerservice@bitdefender.com

■ 전화(무료):

미국: 1-888-868-1876

캐나다: 1-866-947-1873

독일

빗디펜더 GmbH

Airport Office Center

Robert-Bosch-Straße 2

59439 Holzwickede

Deutschland

Hotline: +49 2301 91 84 555

Technische Beratung: support@bitdefender.de

Vertrieb: vertrieb@bitdefender.de

Web: <http://www.bitdefender.de>

영국 및 아일랜드

Business Centre 10 Queen Street

Newcastle, Staffordshire

ST5 1ED

Tel: +44 (0) 8451-305096

이메일: info@bitdefender.com

판매: sales@bitdefender.com

웹: <http://www.bitdefender.co.uk>

기술지원: support@bitdefender.com



스페인

Constelaci n Negocial, S.L
C/ Balmes 195, 2a planta, 08006
Barcelona
기술 지원: soporte@bitdefender-es.com
판매: comercial@bitdefender-es.com
전화번호: +34 932189615
팩스: +34 932179128
제품 웹사이트: <http://www.bitdefender-es.com>

로마니아

BITDEFENDER
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
기술지원: support@bitdefender.com
판매: sales@bitdefender.com
Tel: +40 21 3001226; +40 21 3001227; +40 21 3001228; +40 21 3001229
Fax: +40 21 2641799
제품 웹사이트: <http://www.bitdefender.com>



BitDefender Antivirus 2009

응급복구 CD



25. 개요

빗디펜더 바이러스차단 2009에는 여러분의 운영체제가 시작하기 전에 모든 존재하는 하드드라이브를 검사 및 치료할 수 있는 부팅되는 CD (빗디펜더 응급복구 CD)가 있습니다.

응급 복구 CD는 사용자의 운영체제가 바이러스에 의해 작업이 불가능한 시점에 사용해야 합니다. 사용자가 바이러스차단을 사용하지 않는 경우 바이러스 감염이 일어납니다.

바이러스 정의는 응급복구 CD로 시작할 때마다 자동으로 업데이트됩니다.

빗디펜더 응급복구 CD는 리눅스 보안솔루션용 최신 빗디펜더를 GNU/리눅스 라이브 CD에 통합하여, 기존 하드드라이브들(윈도 NTFS파티션 포함)을 검사 및 치료할 수 있는 데스크탑용 바이러스차단 기능을 제공하는 빗디펜더에 의해 재 마스터된 크노픽스 판입니다. 아울러, 빗디펜더 응급복구 CD는 윈도가 뜨지 않을 때 여러분의 귀중한 데이터를 복구하는데 사용할 수 있습니다.



참고

빗디펜더 응급복구 CD는 다음 위치에서 내림받을 수 있습니다:
http://download.bitdefender.com/rescue_cd/

25.1. 시스템 요건들

빗디펜더 응급복구 CD를 부트시키기 전에, 우선 여러분 시스템이 다음 요건들을 충족하는지 확인해야 합니다:

CPU 유형

최소 : x86 호환, 166 MHz 권장 : i686(펜티엄 프로)이상의 프로세서, 800MHz 이상.

메모리

최소 512 MB 램 메모리 (1 GB 권장)

CD-ROM

빗디펜더 응급복구 CD는 시디롬에서 실행됩니다. 따라서, 시스템은 시디롬으로 부팅될 수 있어야 합니다.



인터넷 연결

비트펜더 응급복구 CD는 인터넷연결없이도 실행되지만, 업데이트 질차는 어떤 프록시 서버를 통해서라도 능동 HTTP 링크를 필요로 합니다. 따라서, 최신 위협으로부터의 보호를 위해, 인터넷 연결은 필수입니다.

그래픽 해상도

표준 SVGA 호환 그래픽카드

25.2. 포함된 소프트웨어

비트펜더 응급복구 CD에는 다음과 같은 소프트웨어 패키지가 포함되어 있습니다.

Xedit

이것은 텍스트 파일 편집기입니다.

Vim

이 패키지는 문법 강조, GUI 등을 포함하는 강력한 텍스트 파일 편집기입니다. 추가 정보는, [vim 홈페이지](#)를 참조하십시오.

Xcalc

이 패키지는 계산기입니다.

RoxFiler

록스파일러는 빠르고 강력한 그래픽 파일관리기입니다.

추가 정보는, [록스파일러 홈페이지](#)를 참조하십시오.

MidnightCommander

GNU미드나잇 커맨더는 텍스트모드 파일 관리기입니다.

추가 정보는, [MC 홈페이지](#)를 참조하십시오.

Pstree

Pstree는 실행과정을 보여줍니다.

Top

탑은 리눅스 작업들을 보여줍니다.

Xkill

엑스킬은 X자원들을 이용해 클라이언트를 죽입니다.

Partition Image

파티션 이미지는 여러분이 EXT2, Reiserfs, NTFS, HPFS, FAT16, 및 FAT32 파일 시스템 포맷으로 된 파티션들을 이미지 파일로 저장하는 것을 돕니다. 이 프로그램은 백업용으로 유용합니다.



추가 정보는, [파티미지 홈페이지](#)를 참조하십시오.

GtkRecover

Gtk리커버는 콘솔 프로그램 리커버의 GTK버전입니다. 이 프로그램은 어떤 파일을 복구하는 것을 돕니다.

추가 정보는, [Gtk리커버 홈페이지](#)를 참조하십시오.

ChkRootKit

Chk루트키트는 컴퓨터 관리권 편취 프로그램이 있는지 검사하는 것을 돕습니다.

추가 정보는, [Chk루트키트 홈페이지](#)를 참조하십시오.

Nessus Network Scanner

네수스는 리눅스, 솔라리스, FreeBSD 및 맥킨토시 OS X용 원격 보안검사기입니다.

추가 정보는 [네수스 홈페이지](#)를 참조하십시오.

lptraf

입트라프는 IP네트워크 감시 소프트웨어입니다.

추가 정보는, [이프트라프 홈페이지](#)를 참조하십시오.

lftop

이프탑은 어떤 인터페이스의 대역사용을 보여줍니다.

추가 정보는, [이프톱 홈페이지](#)를 참조하십시오.

MTR

MTR은 네트워크 진단도구입니다.

추가 정보는, [MTR 홈페이지](#)를 참조하십시오.

PPPStatus

PPP스테이터스는 송수신 TCP/IP교통에 관한 통계를 보여줍니다.

추가 정보는, [PPP스테이터스 홈페이지](#)를 참조하십시오.

Wavemon

웨이브몬은 무선네트워크장치를 위한 감시 응용프로그램입니다.

추가 정보는, [웨이브몬 홈페이지](#)를 참조하십시오.

USBView

USB뷰는 USB버스에 연결된 장치들에 관한 정보를 보여줍니다.

추가 정보는, [USB뷰 홈페이지](#)를 참조하십시오.



Pppconfig

PPP컴피그는 PPP연결 자동 전화걸기를 돕습니다.

DSL/PPPoE

DSL/PPP오이는 PPPoE(ADSL) 연결을 설정합니다.

i810rotate

i810로테이트는 i810스위치(1)을 사용하는 i810 하드웨어 상의 비디오 출력을 전환합니다.

추가 정보는, [i810로테이트 홈페이지](#)를 참조하십시오.

Mutt

무트는 강력한 텍스트 기반 MIME메일 클라이언트입니다.

추가 정보는, [무트 홈페이지](#)를 참조하십시오.

Mozilla Firefox

모질라 파이어폭스는 잘 알려진 웹브라우저입니다.

추가 정보는, [모질라 파이어폭스 홈페이지](#)를 참조하십시오.

Elinks

엘링크는 텍스트모드 웹브라우저입니다.

추가 정보는 [엘링크스 홈페이지](#)를 참조하십시오.



26. 비트펜더 응급복구 CD 사용법

이 장은 비트펜더 응급복구 CD를 시작하고 멈추고, 데이터를 윈도우 PC에서 이동용 저장장치로 저장할 뿐 아니라 여러분 컴퓨터에 악성프로그램이 있는지를 검사하는 방법에 관한 정보를 담습니다. 그뿐 아니라, CD에 있는 응용소프트웨어를 사용해, 여러분은 이 책에서 모두 설명할 수 없는 많은 작업들을 할 수 있습니다.

26.1. 비트펜더 응급복구 CD 시작하기

CD로 부팅하기 위해 사용자 컴퓨터의 BIOS를 조정합니다. 드라이브에 CD를 넣고 컴퓨터를 재 부팅 합니다. 사용자의 컴퓨터가 CD로 부팅되도록 합니다.

다음 화면이 나타날 때까지 기다린 후, 화면에 나타는 지시들을 따라 비트펜더 응급복구 CD를 시작하십시오.



참고

사용할 수 있는 목록에서 응급복구 CD에 대해 사용하기 원하는 언어를 선택하십시오.



부트 스플래시 화면



부트될 때, 바이러스 서명 업데이트가 자동으로 이루어질 것입니다. 이 과정은 시간이 제법 걸릴 수 있습니다.

부트과정이 마치면 다음 바탕화면이 보일 것입니다. 여러분은 비트펜더 응급복구 CD를 사용해 이제 시작할 수 있습니다.



바탕화면

26.2. 비트펜더 응급복구 CD메م추기

BitDefender 응급복구 CD 단축메뉴(오른쪽 클릭으로 엽니다)로부터 종료를 선택하거나 단말기에서 멈춤 명령을 통해 컴퓨터를 안전하게 종료할 수 있습니다.



"EXIT"선택 시 화면



비트펜더 응급복구 CD가 성공적으로 모든 프로그램들을 닫았으면, 다음 이미지와 같은 화면이 나타날 것입니다. 여러분 하드드라이브에서 부트하기 위해 CD를 제거할 수 있습니다. 이제 여러분 컴퓨터를 끄거나 재부팅시킬 수 있습니다.

```
X Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Killing processes with signal 15: (init) (aufs) (aufs) (aufs) (aufs)
(ald) (hald-addon-acpi) (hald-addon-keyb) (ksoftirqd/0) (logsave) (inetd)
(s/0) (khelper) (kthread) (ata/0) (ata_aux) (kseriod) (kpsmoused) (ksuspend)
(aio/0) Done.
Waiting for processes to finish.....
Killing processes with signal 9: (init) (aufs) (aufs) (aufs) (aufs)
(kblockd/0) (kacpid) (knopix-halt) (events/0) (khelper) (kthread) (ata/0)
(d) (khsbpkt) (pdflush) (pdflush) (kswapd0) (aio/0) Done.
Waiting for processes to finish.....
Syncing/Unmounting filesystems: /sys/fs/fuse/connections /UNIONFS/lib/init
Turning off swap... Done.
Unmounting remaining file systems.
rootfs unmounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return [auto 2 minutes].
```

종료 되기 전에 이 메시지를 표시하고 대기합니다.

26.3. 어떻게 바이러스를 검사하나요?

부트과정이 마치면 마법사가 나타나, 여러분이 컴퓨터를 검사할 수 있게 할 것입니다. 여러분이 하실 일은 시작 버튼을 클릭하는 것입니다.



참고

만약 여러분 화면해상도가 충분히 높지 않으면, 여러분은 텍스트모드로 검사를 시작하도록 요구받을 것입니다.

검사과정을 완성하기 위해 세 단계로 안내되는 절차를 따르십시오.

1. 검사상태 및 통계(검사속도, 걸린 시간, 검사/감염/의심/숨겨진 객체들의 수 등)가 보일 것입니다.



참고

검사의 복잡한 정도에 따라 검사과정이 제법 걸릴 수 있습니다.

2. 여러분은 여러분 시스템에 영향을 주는 문제들의 수를 보실 수 있습니다.



문제들은 그룹별로 나타납니다. 그룹을 열려면 “+” 박스를, 그룹을 닫으려면 “-” 박스를 클릭하십시오.

문제들의 각 그룹에 대해 취할 전반적 조치를 선택하거나 각 문제에 대한 개별 조치를 선택할 수도 있습니다.

3. 여러분은 결과들의 요약을 보실 수 있습니다.

어떤 디렉토리만 검사하기 원하시면, 다음을 따르십시오:

폴더를 탐색하고 파일이나 폴더에서 오른쪽 마우스 버튼을 클릭하여 Send to 를 선택합니다. 그 다음에BitDefender Scanner를 선택합니다.

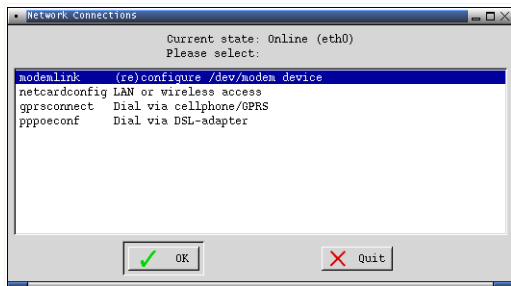
터미널에서 root 권한으로 아래의 명령을 실행할 수도 있습니다. BitDefender Antivirus Scanner 는 지정한 파일이나 폴더를 검사할 수 있습니다.

```
# bdscan /path/to/scan/
```

26.4. 인터넷 연결은 어떻게 설정할 것인가?

DHCP가 동작하는 네트워크에서는 사용자가 이더넷 네트워크 카드를 보유하고 있다면 인터넷 연결은 이미 구성되어 있을 것입니다. 수동으로 구성하려면 다음의 절차를 따르십시오.

1. 바탕화면 상의 네트워크연결 단축키를 더블클릭하십시오. 다음 창이 나타날 것입니다.



네트워크 연결들



2. 여러분이 사용하고 있는 연결유형을 선택하고 OK를 클릭하십시오.

연결	설명
모뎀링크	모뎀 및 전화선을 사용해 인터넷에 접속할 때에는 이 연결유형을 선택하십시오.
넷카드 설정	LAN을 사용해 인터넷에 접속할 때에는 이 연결유형을 선택하십시오. 이 유형은 무선연결에도 적합합니다.
gprs연결	GPRS(일반패킷라디오서비스) 프로토콜을 사용해 이동전화 네트워크를 통해 인터넷에 접속할 때에는 이 연결유형을 선택하십시오. 물론, 이동전화 대신 GPRS모뎀을 사용할 수도 있습니다.
pppoeconf	DSL모뎀을 사용해 인터넷에 접속할 때에는 이 연결유형을 선택하십시오.

3. 화면상의 지시들을 따르십시오. 어느 것을 선택해야 할지 모를 때에는, 여러분 시스템 혹은 네트워크 관리자에게 문의하십시오.



중요

여러분은 위에 언급된 선택사항들을 선택해서만 모뎀을 가동할 수 있음을 유의하십시오. 네트워크 설정을 하려면 이 단계들을 따르십시오:

1. 바탕화면에서 오른쪽 클릭하십시오. 비트펜더 응급복구 CD 단축메뉴가 나타날 것입니다.
2. 단말기(루트)를 선택하십시오.
3. 다음 명령들을 입력하십시오:

```
# pppconfig
```

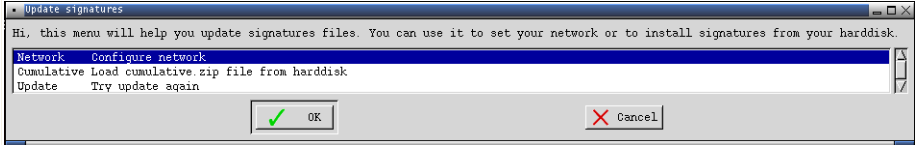
4. 화면상의 지시들을 따르십시오. 어느 것을 선택해야 할지 모를 때에는, 여러분 시스템 혹은 네트워크 관리자에게 문의하십시오.

26.5. 어떻게 비트펜더를 업데이트하나요?

부트 시, 바이러스 서명 업데이트가 자동으로 이루어집니다. 그러나, 이 단계를 건너뛰었다면, 여기에 비트펜더 업데이트 방법이 있습니다.



1. 바탕화면 상의 업데이트 서명 단축키를 더블클릭하십시오. 다음 창이 나타날 것입니다.



서명들 업데이트

2. 다음 중 한 가지를 실행하십시오:
 - 여러분 컴퓨터를 둘러보기하고 cumulative.zip 파일을 올려서 여러분 하드디스크에 이미 저장된 서명들을 설치하기 위해 누적을 선택하십시오.
 - 즉시 인터넷에 접속해 최신 바이러스 서명들을 내림받으려면, 업데이트를 선택하십시오.
3. 확인을 클릭하십시오.

26.5.1. 어떻게 프록시를 통해 비트펜더를 업데이트 할 수 있나요?

여러분 컴퓨터와 인터넷 사이에 프록시 서버가 있으면, 바이러스 서명들을 업데이트하기 위해 일부 설정을 실행해야 할 수 있습니다.

프록시를 통해 비트펜더를 업데이트하려면, 다음 단계들을 따르십시오:

1. 바탕화면에서 오른쪽 클릭하십시오. 비트펜더 응급복구 CD 단축메뉴가 나타날 것입니다.
2. 단말기(루트)를 선택하십시오.
3. 다음 명령을 입력하십시오: `cd /ramdisk/BitDefender-scanner/etc`
4. 다음 명령을 입력하십시오: GNU미드나이트를 사용해 이 파일을 편집하려면 `mcedit bdscan.conf`
5. 다음 줄에서 다음과 같이 코멘트를 삭제하십시오: `#HttpProxy =` (# 기호를 제거), 및 프록시 서버의 도메인, 사용자이름, 비밀번호 및 서버포트를 지정합니다. 예를 들면, 각 줄은 다음과 같이 되어야 합니다:

`HttpProxy = myuser:mypassword@proxy.company.com:8080`

6. F2를 눌러서 현재 파일을 저장하고, 저장을 확인 후, F10을 눌러 파일을 닫으십시오.



7. 다음 명령을 입력하십시오. bdsan 업데이트

26.6. 어떻게 내 데이터를 저장하나요?

어떤 알려지지 않은 문제들로 인해 여러분의 윈도 PC를 시작할 수 없다고 가정합니다. 동시에, 여러분은 여러분 컴퓨터로부터 어떤 중요한 정보를 가져와야 하는 절박한 상황에 있습니다. 이런 상황에서 비트펜더 응급복구 CD가 유용합니다.

여러분 데이터를 컴퓨터에서 USB메모리스틱 등 이동저장장치로 저장하려면 이 단계들을 따르십시오:

1. 비트펜더 응급복구 CD를 CD드라이브로 넣고, 메모리스틱을 USB드라이브 안으로 넣은 후 컴퓨터를 재시작하십시오.



참고

메모리스틱을 나중에 꽂을 경우, 다음 단계들을 따라 이동용 장치를 장착해야 합니다:

- a. 바탕화면 상의 단말기 에뮬레이터 단축키를 더블클릭하십시오.
- b. 다음 명령들을 입력하십시오:

```
# mount /media/sdb1
```

여러분 컴퓨터 설정에 따라 sdb1 대신 sda1가 될 수 있음을 유의하십시오.

2. 비트펜더 응급복구 CD가 부팅을 마칠 까지 기다리십시오. 다음 창이 나타날 것입니다.



바탕화면

3. 여러분이 저장하기 원하는 데이터가 있는 파티션을 더블클릭하십시오(예, [sda3]).



참고

빗디펜더 응급복구 CD를 사용해 작동할 때에는, 리눅스형 파티션 이름들이 나타날 것입니다. 따라서, [sda1]는 (C:) 윈도우형 파티션, [sda3]는 (F:), 그리고 [sdb1]는 메모리스틱에 해당할 것입니다.



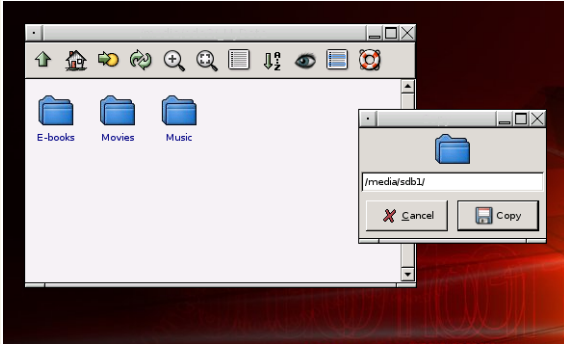
중요

만약 컴퓨터가 바르게 켜지지 않았다면, 일부 파티션들이 자동으로 장착되지 않았을 것입니다. 파티션을 장착하려면, 다음 단계들을 따르십시오.

- a. 바탕화면 상의 단말기 에뮬레이터 단축키를 더블클릭하십시오.
- b. 다음 명령들을 입력하십시오:

```
# mount /media/partition_name
```

4. 폴더를 둘러보기 해서 원하는 디렉토리를 여십시오. 예를 들면, Movies, Music 및 E-books 하부디렉토리들을 포함하는 MyData를 열 수 있습니다.
5. 원하는 디렉토리를 마우스 오른쪽 버튼으로 클릭해서 복사를 선택하십시오. 다음 창이 나타날 것입니다.



데이터 저장

6. `/media/sdb1/`를 해당 텍스트상자 안으로 입력하고, 복사를 클릭하십시오.
여러분 컴퓨터 설정에 따라 `sdb1` 대신 `sda1`가 될 수 있음을 유의하십시오.



용어집

ActiveX

ActiveX는 작성 프로그램의 모델이며, 다른 프로그램과 운영 체제가 ActiveX을 부를 수 있습니다. ActiveX 기술은 마이크로소프트 인터넷 익스플로러가 정적인 페이지라기보다는 컴퓨터 프로그램 같이 보이고, 그렇게 행동하는 웹 페이지와 쌍방향 통신을 하는 데 사용되는 것입니다. ActiveX를 사용하여, 사용자는 질문을 던지거나, 답변을 하고, 누르기 버튼을 이용하며, 웹 페이지와 기타 방식으로 상호 작용을 하게 됩니다. ActiveX 컨트롤은 종종 비주얼 베이직을 이용하여 작성됩니다.

ActiveX은 보안 컨트롤이 완전히 부재한 것으로 유명합니다. 컴퓨터 보안 전문가들은 인터넷에서 ActiveX를 사용하지 않을 것을 권장합니다.

광고프로그램들

애드웨어는 종종 사용자가 애드웨어를 수락할 것에 동의하는 동안 무료로 제공되는 호스트어플리케이션과 연동됩니다. 애드웨어 어플리케이션이 일반적으로 사용자가 어플리케이션의 목적을 명시한 라이선스 계약을 체결한 다음에 설치되는 관계로, 공격 행위는 일어나지 않습니다.

그러나 팝업 광고는 성가신 것이 될 수 있으며, 때로는 시스템 성능을 저하시키기도 합니다. 또한 일부 애드웨어가 수집한 정보는 라이선스 계약 규정을 완벽하게 인지하지 못한 사용자의 개인정보와 관련된 문제를 일으키기도 합니다.

아카이브

백업된 파일을 담고 있는 디스크나 테이프, 디렉토리.

압축 형식으로 하나 이상의 파일을 담고 있는 파일.

백도어

작성자 혹은 관리자가 마련해 높은 시스템 보안 상의 허점. 이러한 허점을 만 들어지는 동기가 언제나 악의가 있는 것은 아닙니다. 예를 들어 일부 운영 체제는 현장 서비스 기술자 혹은 판매인의 관리 프로그래머가 사용할 목적의 우선적인 계정이 있는 제품이 출시되고 있습니다.

부트 섹터

개별 디스크 시작 시, 디스크 아키텍처(섹터 크기, 클러스터 크기 등)을 식별하는 섹터. 디스크를 시작하는 경우, 부트 섹터에는 운영체제를 불러오는 프로그램이 포함되어 있습니다.



부트 바이러스

고정 디스크 혹은 플로피 디스크의 부트 섹터를 감염시키는 바이러스. 부트 섹터 바이러스를 담고 있는 감염된 디스켓을 이용한 부팅 시도는 메모리에서 바이러스를 활동하게 만들 위험이 있습니다. 디스켓을 이용하여 시스템을 부팅할 때마다, 사용자는 메모리 내에서 활동하는 바이러스를 가지게 될 것입니다.

브라우저

웹 브라우저용 바로가기로써 웹 페이지를 위치시키고 표시하는 데 사용되는 소프트웨어 어플리케이션. 가장 유명한 두 브라우저는 넷스케이프 네비게이터와 마이크로소프트 인터넷 익스플로러입니다. 이 두 브라우저 모두 그래픽을 기반으로 하는 것으로써, 이는 텍스트와 마찬가지로 그래픽을 디스플레이할 수 있음을 의미합니다. 또한 최신 브라우저는 해당 포맷에 필요한 플러그인을 요청함으로써 사운드와 영상과 같은 멀티미디어 정보를 표현해 낼 수 있습니다.

명령 행

명령행 인터페이스에서 사용자는 명령어를 사용하여 화면에서 직접 명령을 입력합니다.

쿠키

인터넷 산업에서 쿠키 파일은 사용자의 온라인 기호와 흥미 사창을 추적하기 위해 광고인들이 분석하고 사용할 수 있는 개인 컴퓨터에 관한 정보를 담고 있는 작은 파일로 설명됩니다. 이러한 부문에서 쿠키 파일 기술은 여전히 발전을 거듭하고 있으며, 그 목적은 사용자가 관심을 보인 대상에 대하여 직접 광고를 하는 것이다. 쿠키 파일은 많은 이들에게 양날검과 같은데, 이는 한편으로는 쿠키 파일이 사용자가 관심을 보이는 광고만을 보여주는 효과적이고 적절한 도구이지만, 다른 한편으로는 쿠키 파일이 사용자가 무엇을 클릭했는지를 "tracking"하고 "following"하는 데 사용되기 때문입니다. 이렇게 이해할 수 있는 것은 프라이버시에 관한 문제가 존재하고, 많은 이들이 자신이 "SKU 숫자" (다들 알고 있듯이, 슈퍼마켓 계산대에서 스캔을 하는 상품의 뒷면에 부착된 바코드)와 같이 보여진다고 생각하고 있기 때문입니다. 이러한 관점이 과도한 것일 수는 있지만, 일부 경우에는 이러한 관점이 정확하기도 합니다.

디스크 드라이브

디스크에서 데이터를 읽거나 데이터를 저장하는 기계장치입니다.

한 하드디스크 드라이브가 하드디스크들을 읽고 씁니다.

한 플로피 드라이브가 플로피 디스크들에 접근합니다.



디스크 드라이브들은 내장(컴퓨터 내에 장착) 혹은 외장(컴퓨터로 연결된 별도의 상자 내에 장착)될 수 있습니다.

내림받기

주변 자원에서 외부 기기로 데이터 복사(일반적으로 전체 파일). 이 용어는 종종 온라인 서비스에서 사용자의 컴퓨터로 파일을 복사하는 프로세스를 설명하는 데 사용됩니다. 다운로드를 네트워크 파일 서버에서 네트워크 내의 컴퓨터로 파일을 복사해 오는 것을 말합니다.

이메일

전자 메일. 로컬 네트워크나 글로벌 네트워크를 통해 컴퓨터에 메시지를 전송하는 서비스.

사건로그

프로그램에 의해 검지된 행동. 상황이라는 것은 마우스 버튼을 클릭하거나 키를 누르는 것과 같은 사용자의 행동이나, 메모리 초과 등과 같이 시스템에서 발생하는 일일 수 있다.

긍정오류

검사가 파일이 실제로 감염되어 있지 않음에도, 감염된 것으로 식별할 때 발생합니다.

파일명 확장

최종점에 따라 파일명 비율은 파일에 저장된 데이터의 종류를 명시합니다.

Unix, VMS, MS-DOS와 같은 많은 운영 체제가 파일명 확장자를 사용하고 있습니다. 이러한 확장자는 하나에서 세 개까지의 문자로 되어 있습니다. (일부 예전 운영체제는 세 개 이상의 문자를 지원하지 않습니다.) 설명하자면, "c"는 C 소스코드이고, "ps"는 PostScript, "txt"는 임의 텍스트 파일 확장자입니다.

경험적

새로운 바이러스를 식별하는 규칙 기반 방법. 이러한 검사 방법은 특정한 바이러스 서명에 의존하지 않습니다. 휴리스틱 검사의 장점은, 이것이 현존 바이러스의 새로운 변형에 의해 혼란을 겪지 않는다는 점입니다. 그러나 때로는 정상 프로그램내의 의심스러운 코드를 보고할 수도 있으며, 이를 "긍정 오류"라고 합니다.

IP

인터넷 프로토콜 TCP/IP 프로토콜 내의 프로토콜로써, IP 주소, 루팅, IP 패킷 분할 및 조합을 담당합니다.



자바 애플릿

웹 페이지 작동을 위해서만 작성된 자바 프로그램. 웹 페이지에서 애플릿을 사용하려면, 애플릿이 사용할 수 있는 애플릿명과 크기(길이 및 넓이, 픽셀 단위)를 지정해야 합니다. 웹 페이지에 접근할 때, 브라우저는 서버에서 애플릿을 다운로드 받아서 이를 클라이언트에서 실행시킵니다. 어플리케이션과 달리, 애플릿은 확실한 보안 프로토콜의 관리를 받습니다.

예를 들어 클라이언트에 애플릿이 작동되는 경우라고 해도, 해당 애플릿은 클라이언트 컴퓨터에서 데이터를 읽어오거나, 데이터를 쓸 수 없습니다. 또한 애플릿은 더 제한을 받기 때문에, 애플릿이 제공된 동일한 도메인에서만 데이터를 쓰고, 읽을 수 있습니다.

매크로 바이러스

문서에 삽입된 매크로로써 암호화된 컴퓨터 바이러스의 일종. Microsoft Word와 Excel과 같은 많은 어플리케이션이 강력한 매크로 언어를 지원합니다.

이러한 어플리케이션은 사용자가 문서에 매크로를 끼워 넣고, 문서가 열릴 때마다 매크로를 실행시킬 수 있도록 합니다.

메일 클라이언트

이메일 클라이언트는 이메일을 송수신할 수 있는 어플리케이션입니다.

메모리

컴퓨터 내부 저장 공간. 텀 메모리(term memory)는 칩의 형태로 되어 있는 데이터 저장을 확인하며, 단어 저장은 테이프나 디스크에 존재하는 메모리를 사용합니다. 모든 컴퓨터에는 특정 규모의 물리적 메모리가 존재하며, 일반적으로 이를 메인 메모리 혹은 RAM이라고 합니다.

비경험적

이러한 검사 방법은 특정 바이러스 서명에 의존하고 있습니다. 비휴리스틱 검사의 장점은 바이러스일지도 모르는 것에 의해 혼란이 생기지 않고, 잘못된 경고를 보내지 않는다는 것입니다.

압축된 프로그램들

압축 형태의 파일. 많은 운영체제와 어플리케이션에는 파일에 압축이 가능하여 메모리를 차지하는 공간을 줄일 수 있는 명령이 포함되어 있습니다. 예를 들어 10개의 연속 스페이스 문자가 담겨 있는 텍스트파일을 생각해 보십시오. 정상적으로 이 텍스트를 저장하려면 10바이트가 필요합니다.

그러나 파일을 압축하는 프로그램은 교체된 스페이스 수에 따른 스페이스 문자열에 의해 스페이스 문자를 교체하게 됩니다. 이러한 경우, 10개의 스페이스 문자에는 2바이트만 소비됩니다. 이것은 단지 압축 기술의 하나일 뿐이며, 그 외에도 여러 가지 기술이 존재합니다.



경로

컴퓨터내의 파일의 정확한 방향. 이러한 방향은 일반적으로 위에서 아래로 향하는 서열적인 파일 시스템으로 설명된다.

두 컴퓨터간의 통신 채널과 같이 두 지점간의 루트.

개인정보불법수집(phishing)

이메일을 발송하여 사용자들에게 거짓으로 적법한 기업이라고 주장하며, 사용자의 ID를 훔치기 위해 사용될 개인 정보를 제공하도록 하는 사기 행동. 적법한 기관에서 이미 보유하고 있는 패스워드와 신용카드 번호, 사회보장번호, 은행 계좌번호 등과 같은 개인 정보 업데이트를 요청하는 웹 사이트를 방문하는 사용자에게 전송되는 이메일. 그러나 해당 웹 사이트는 가짜이며 사용자의 정보를 훔칠 목적으로만 만들어진 것입니다.

다형 바이러스

파일이 감염될 때마다 그 형태가 변하는 바이러스. 일관성있는 패턴이 없는 관계로, 이러한 바이러스를 확인하는 것은 쉽지 않습니다.

포트

어떤 장치를 연결할 수 있는 컴퓨터 상의 인터페이스. 개인용 컴퓨터에는 다양한 형태의 포트들이 있습니다. 내부적으로는, 디스크 드라이브, 디스플레이 화면 및 키보드를 연결하기 위한 몇 개의 포트들이 있습니다. 외부적으로는, 개인용 컴퓨터들에는 모뎀, 프린터기, 마우스 및 기타 주변기기들을 연결하기 위한 포트들이 있습니다.

TCP/IP와 UDP 네트워크를 접속하기 위한 논리 커넥션에서 종단점을 말합니다. 포트 번호는 그것이 어떤 유형의 포트인지 명시됩니다. 예를 들면, PORT 80번은 은 HTTP 교통을 위해 사용됩니다.

파일 보고서

발생된 행동이 열거되어 있는 파일. BitDefender는 경로 검사, 폴더, 검사된 아카이브와 폴더 수, 얼마나 많은 의미 및 감염 파일이 발견되었는지에 대한 보고서 파일을 유지합니다.

관리권 편취 프로그램

관리권편취프로그램(rootkit)은 어떤 시스템에 대한 관리자 수준의 접근을 제공하는 일군의 소프트웨어 도구들입니다. 이 용어는 처음에 유닉스 운영체제들에 사용되었다가, 나중에 침입자들에게 관리자 권한을 제공하여 시스템 관리자들이 침입자들을 보지 못하게 하기 위해 침입자들이 자신들의 존재를 숨길 수 있게 한 재편집된 도구들을 가리켰습니다.



관리권 편취 프로그램들의 주된 역할은 과정, 파일, 로그인 및 로그를 숨기는 것입니다. 이 프로그램들은 또한 적합한 소프트웨어를 동원하는 경우 단말기, 네트워크 연결 혹은 주변기기들로부터 데이터를 가로챌 수도 있습니다.

관리권 편취 프로그램들은 본질적으로 악성 프로그램입니다. 예를 들면, 시스템들 그리고 심지어 응용프로그램마저도 관리권 편취 프로그램을 사용해 결정적으로 중요한 파일들을 숨깁니다. 그러나 이 프로그램들은 대개 악성프로그램을 감추거나 시스템 내의 침입자의 존재를 숨기는데 사용됩니다. 악성프로그램들과 결합하여, 관리권 편취 프로그램들은 시스템의 완결성 및 보안에 심각한 위협을 가합니다. 이 프로그램들은 교통을 감시하고 시스템으로 진입을 위한 뒷문을 만들고, 파일과 로그를 변경하고 탐지를 피합니다.

스크립트

다름 매크로 혹은 배치 파일에 관한 용어. 스크립트는 사용자의 개입 없이 시행될 수 있는 명령 리스트입니다.

무차별광고메일

쓰레기 메일로 불리기도하는 무차별살포광고메일(스팸)은 일반적으로 수신을 원하지 않는 모든 메일을 의미합니다.

염탐프로그램(스파이웨어)

간첩(spy)과 소프트웨어의 합성어로, 본래는 어떤 사람이나 조직에 관한 정보를 수집하는 데 도움을 주는 기술을 뜻했습니다. 광고나 마케팅을 목적으로 배포하는 것이 대부분이어서 광고성 프로그램(adware)이라고도 불립니다. 그러나 최근에는 다른 사람의 컴퓨터에 몰래 숨어들어가 있다가 중요한 개인정보를 빼가는 프로그램을 지칭하게 되었습니다.

염탐프로그램들은 사용자들이 다른 소프트웨어를 설치할 때에 자신도 모르는 사이에 함께 설치하게 된다는 점에서 트로이 목마와 비슷합니다. 염탐프로그램의 희생자가 되는 흔한 경로는 오늘날 많은 사람들이 사용하는 피투피 파일교환 내림받기를 통해서입니다.

윤리나 프라이버시와 관련된 문제와는 별도로, 스파이웨어는 컴퓨터 메모리 리소스를 이용하고, 사용자로부터 정보를 훔쳐내어 사용자의 인터넷 연결을 통해 스파이웨어 홈으로 정보를 전송합니다. 스파이웨어가 메모리와 시스템 리소스를 사용하기 때문에, 기본적으로 가동되는 어플리케이션이 시스템을 깨뜨리고, 일반적인 시스템 불안정 문제가 나타날 수 있습니다.

시작 항목들

본 폴더에 포함되어 있는 모든 파일은 컴퓨터 시작 시 열릴 것입니다. 예를 들어 시작 화면과 컴퓨터 첫 시작 시 나타나는 사운드 파일, 일정표, 어플리



케이션 프로그램 등이 시작 항목일 수 있습니다. 또한 파일 자체가 아닌 폴더 내에 위치한 파일의 바로가기 아이콘이 있을 수 있습니다.

시스템 트레이

윈도우 95와 함께 도입된 시스템 트레이는 윈도우 태스크바에 있으며(일반적으로 시계 옆 하단), 여기에는 팩스와 프린터, 모델, 볼륨 등과 같은 시스템 기능에 쉽게 접근할 수 있도록 하는 작은 아이콘이 포함되어 있습니다. 해당 아이콘을 더블클릭하거나 우클릭하면, 세부 사항과 컨트롤의 확인 및 접근이 가능합니다.

TCP/IP

TCP/IP 다양한 하드웨어 아키텍처와 다양한 운영체제를 가진 상호 연결된 컴퓨터 네트워크에서 통신 할 수 있도록 하는 인터넷에서 널리 이용되는 네트워크 프로토콜입니다. TCP/IP에는 컴퓨터가 통신하는 방법 및 네트워크 연결, 트래픽 루팅 등의 방법 표준이 포함되어 있습니다.

트로이 목마

[트로이 목마]프로그램이 트로이 목마와 같은 역할을 하여 파일을 훔치거나 변경함으로써 프로그램에 결함을 가져오게 할 수 있습니다.

이 용어는 호머의 일리아드에서 유래한 것으로서, 이 작품에서 그리스인들은 트로이인들에게 평화의 상징으로써 거대한 목마를 선물합니다. 그러나 트로이인들이 목마를 성안으로 들여온 후, 그리스 병사들이 목마에서 빠져나와 성문을 열어, 그리스인이 밀려들어가 트로이를 점령할 수 있도록 합니다.

업데이트

동일한 제품의 예전 버전을 교체하기 위해 만들어진 새로운 버전의 소프트웨어 혹은 하드웨어 제품. 또한 업데이트용 설치 루틴은 종종 옛 버전이 컴퓨터에 이미 설치되어 있는지를 확인하며, 제품이 설치되어 있지 않은 경우 사용자는 업데이트를 할 수 없습니다.

BitDefender는 자체적인 업데이트 모듈을 보유하고 있으며, 이 모듈은 사용자가 업데이트를 수동으로 확인하거나 자동적으로 제품을 업데이트 할 수 있도록 하는 것을 가능케 합니다.

바이러스

사용자의 의지에 반하여 사용자가 알지 못하는 사이 컴퓨터에 로드된 프로그램이나 코드. 대부분의 바이러스는 자체적으로 복제가 가능합니다. 모든 컴퓨터 바이러스는 인간이 만든 것입니다. 자체적으로 반복 복사가 가능한 단순한 바이러스는 만들기가 상대적으로 쉽습니다. 이러한 단순한 바이러스 조차도 위험요소를 가지고 있는데, 그것은 이러한 바이러스가 빠르게 모든 사용 가능한 메모리를 사용하고, 시스템을 멈추게 만들기 때문입니다. 더욱 위험한 바



이러스 종류는 자체적으로 네트워크에 퍼지고 보안 시스템을 빠져나가는 것입니다.

바이러스 정의

안티바이러스 프로그램이 바이러스를 검지하고 삭제하기 위해 사용하는 바이러스의 2진법적 패턴.

웜바이러스

자체적으로 네트워크 내에서 확산되며, 자체적으로 복사되는 프로그램입니다. 이 프로그램은 다른 프로그램에 자체적으로 첨부되지 못합니다.