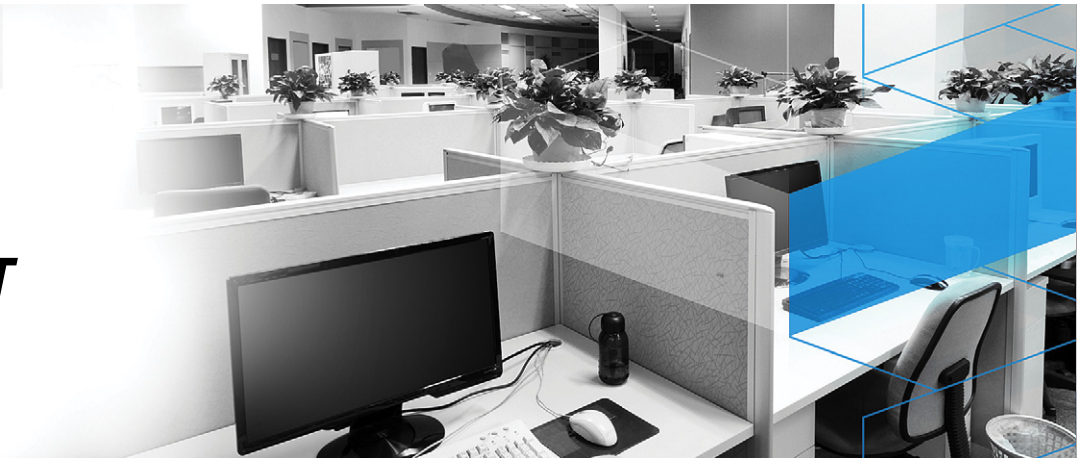
BITDEFENDER CLIENT SICHERHEIT



DAS FUNDAMENT DER UNTERNEHMENSSICHERHEIT

Die Sicherheitsanforderungen neuer oder bestehender Unternehmen sollten unabhängig von der Unternehmensgröße dieselben sein. Der Schutz des geistigen Unternehmenseigentums und der Kundendaten gehört zu jeder guten Geschäftspraxis, doch die Auswirkungen von Virusinfektionen beeinträchtigen die wirtschaftliche Effizienz von Unternehmen und können zu Produktivitätseinbußen der Mitarbeiter führen. Dieser Produktivitätsverlust kann nicht nur das Wachstum kleiner Unternehmen hemmen, sondern sie komplett handlungsunfähig machen.

ANTIVIRUS REICHT NICHT AUS

Bedrohungen werden ständig weiterentwickelt, um die Sicherheitskontrollen Ihres Unternehmens zu umgehen. Antivirus-Schutz ist zwar die Grundlage jeder guten Sicherheitspolitik, reicht aber nicht mehr aus, um Ihre Arbeitskraft vor den Risiken durch Schad-Software zu schützen. Bedrohungen, die signifikante Geschäftsunterbrechungen verursachen, können u. a. folgende sein:

Viren: Übertragung durch Infektion ausführbarer Dateien, versteckt in komprimierten Archiven oder als Makros innerhalb legitimer Dokumente. Virenschäden können in Dateilöschungen bestehen, in Datenverschlüsselungen, Löschungen der Festplatte etc.

Adware/Spyware: Spyware ist fast genauso störend und gefährlich wie Viren und kann zudem schwierig zu identifizieren und zu entfernen sein. Die unerwünschte Weitergabe von Personen- und Unternehmensdaten ist eine der Hauptgefahren, zudem sind Leistungseinbußen bei den Arbeitsplatzrechnern, Installationen unerwünschter Software und die heimliche Umleitung von Browser-Aktivitäten möglich. Schwer infizierte Systeme können eine komplette Neuinstallation erfordern und zahlreiche IT-Stunden sowie Ressourcen verschlingen.

Würmer: Ein selbstreplizierendes Programm, das sich innerhalb des Netzwerks ausbreitet, die Leistung beeinträchtigt und Systeme infiziert, indem es System- und Anwendungsschwachstellen ausnutzt. Payloads können Dateien löschen oder installieren, verschlüsseln, Dokumente per E-Mail versenden, Backdoor-Programme Endgeräte in „Zombies“ verwandeln und Trojaner einschleusen.

Trojaner und Rootkits: Trojaner und Rootkits täuschen vor, legitime Programme zu sein, wurden jedoch entwickelt, um den Fernzugriff auf Computer-Systeme zu ermöglichen. Sobald ein Trojaner oder ein Rootkit installiert ist, hat der Angreifer die Möglichkeit, aus der Ferne auf das System zuzugreifen. Dies führt häufig zu Datendiebstahl. Es kann ein aufwendiger Prozess sein, solche Bedrohungen manuell aufzuspüren und unschädlich zu machen. Oft ist eine komplette Neuinstallation des Systems erforderlich, wenn die Bedrohungen nicht vollständig entfernt wurden.

E-Mail-Spam und Phishing: Unerwünschte kommerzielle E-Mail-Werbung ist mehr als nur ein Ärgernis. Spam nimmt zu viel Zeit der Mitarbeiter in Anspruch, wenn er nicht gut verwaltet wird. Manche Spam- oder Phishing-Attacken enthalten Malware in Dateianhängen, deren Ausführung zu internen Schäden führt, oder Links zu Websites, die persönliche Informationen verlangen. Phishing bedient sich ähnlicher Techniken, führt den Benutzer allerdings zu scheinbar legitimen Websites, um an persönliche Informationen wie Kreditkarten- oder Kontodaten zu gelangen bzw. Keylogger in das System einzuschleusen, die sensible Unternehmensdaten sammeln.

Die Auswirkungen von Malware können in schwerwiegenden Unterbrechungen sämtlicher Arbeitsprozesse eines Unternehmens bestehen. Die IT-Abteilung ist jedoch der Bereich, der die Nachwirkungen am deutlichsten zu spüren bekommt. IT-Administratoren, die mit sich rasch verbreitenden Würmern oder Viren und einer Vielzahl infizierter Systeme konfrontiert waren, wissen, wie zeitintensiv und aufwendig die Gegenmaßnahmen sein können. Leider haben solche Gegenmaßnahmen Priorität gegenüber anderen IT-Projekten, um Datenverluste und Ausfallzeiten bei der Arbeitskraft so schnell wie möglich einzudämmen.

HAUPTMERKMALE UND -VORTEILE

- Preisgekrönte Virenerkennung, Bereinigung und Quarantäne
- Erlaubt flexible Planung von On-Demand- oder Immediate-Execution-Prüfungen zur aktuellen Einschätzung von Infektionen
- Optimierte Prüfmethoden mit Datei-Fingerprinting bei jeder Benutzersitzung und Neuprüfungen bei Erstellung neuer Sitzungen, bei Updates oder Infektionen des Systems
- Infizierte und verdächtige Dateien werden in Quarantäne verschoben, um Infektionsrisiken zu minimieren und sichere Analysen durchführen zu können.
- Richtlinienbasierte Konfiguration und Verwaltung
- Persönlicher Firewall-Schutz für remote und mobil angebundene Mitarbeiter
- Scan von Wechseldatenträgern und Zugriffssteuerungsregeln
- Spam-Schutz auf Systemebene mit fortlaufend aktualisierten schwarzen und seißen Listen sowie einer Bayesschen Lern-Engine zur Identifikation neuen Spams, den traditionelle Filter nicht aufhalten
- Anpassbare Inhaltsfilter erkennen sensible Informationen, und minimieren so die Gefahr unerwünschter Weitergabe von Daten
- Erhöhte Sicherheit durch Profile mit eingeschränkten Zugriffsrechten und passwortgeschützter Deinstallation
- Senken Sie Ressourcenkosten und -aufwand einer Vielzahl zu verwaltender Clients, indem Sie eine zentrale Management-Konsole verwenden
- Ermöglicht die Remote-Konfiguration, -Prüfung, -Installation und -Anwendungsentfernung von jedem Client- und Serversystem des Netzwerks

Bitdefender

BITDEFENDER TECHNOLOGIEN

AVC BitDefender Active Virus Control ist eine innovative, proaktive Erkennungstechnik, die mithilfe hochentwickelter heuristischer Methoden neue potenzielle Bedrohungen in Echtzeit erkennt. Sie überwacht jedes Programm, das auf Ihrem Computer läuft, und überprüft es auf verdächtige Aktivitäten. Wenn genügend solcher Aktivitäten beobachtet werden, wird das entsprechende Programm als schädlich eingestuft.

b-have Sämtliche Lösungen von BitDefender beinhalten B-HAVE, eine zum Patent angemeldete Technologie, die das Verhalten potenziell schädlicher Codes in einem virtuellen Computer analysiert, falsch positive Ergebnisse eliminiert und die Erkennungsraten neuer bzw. unbekannter Schad-Software signifikant erhöht.

NeuNet Um neuen Spam besser in den Griff zu bekommen, hat das BitDefender Lab den leistungsstarken Spamfilter NeuNet geschaffen. NeuNet wird im Antispam-Labor mithilfe einer Vielzahl von Spam-Nachrichten trainiert und lernt so, neuen Spam anhand von Ähnlichkeiten mit den bereits untersuchten Nachrichten zu erkennen.

SYSTEMANFORDERUNGEN

Die Client Security-Lösung von BitDefender bietet zentrale Verwaltung auf der Server-Seite und Endpunkt-Sicherheit auf der Client-Seite. Die Client-Seite umfasst zwei Elemente: BitDefender Business Client zum Schutz und zur Steuerung von Windows-Endpunkten und BitDefender Management Agent für die zentrale Verwaltung. Die Elemente der Client-Seite werden über die zentrale Verwaltungsplattform von BitDefender installiert.

BitDefender Business Client und Management Agent

Intel Pentium kompatibler Prozessor

- 500 MHz für Windows 2000
- 800 MHz für Windows XP
- 1 GHz für Windows Vista, Windows 7

Arbeitsspeicher:

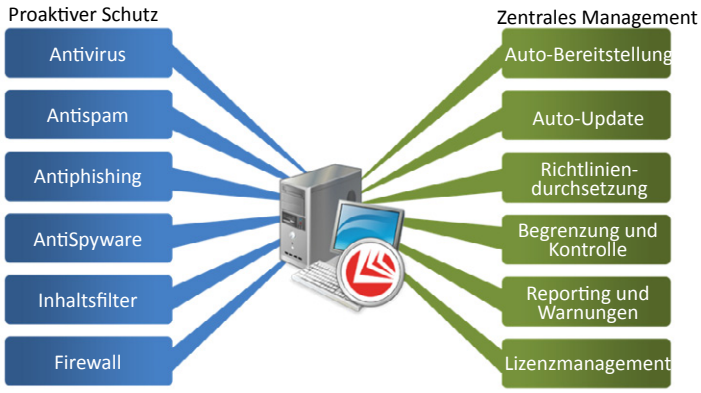
- 512 MB für Windows 2000, Windows XP
- 1 GB für Windows Vista, Windows 7

Minimaler freier Festplattenspeicher:

- 300 MB (400 MB für die Installation)

Betriebssystem:

- **Business Client und Management Agent** für Windows 7, Windows Vista SP1, Windows XP (SP2), Windows Home Server, Windows 2000 Professional (SP4 Rollup 1 v2)
- **Management Agent** auch für Windows 2008/2008 SBS/2008 R2, Windows Server 2003 (SP2), Windows 2000 Server (SP4 Rollup 1 v2), Mac OS X 10.4.6 oder höher, Linux 2.4.x oder 2.6.x mit glibc 2.3.1 oder höher und libstdc++5 von gcc 3.2.2 oder höher



BitDefender Client Security bietet Schutz und Client Management-Funktionalität auf verschiedenen Ebenen

INNOVATIVE PROAKTIVE ERKENNUNG

Die preisgekrönten Prüf-Engines von BitDefender wurden von führenden Zertifizierungsbehörden wie ICSA Labs, Virus Bulletin und West Coast Labs wegen ihres unschlagbaren proaktiven Schutzes vor Malware anerkannt. BitDefender bietet mehrere innovative Schutzebenen.

BitDefender Client Security bietet mehrfachen Schutz durch hochentwickelte Technik: Antivirus, Antispam, Antispyware, Antiphishing, Inhaltsfilter, Trojaner-/Rootkit-Erkennung und eine umfangreiche persönliche Firewall. Sämtliche Elemente sind aus der Ferne konfigurierbar, darunter auch weitreichende Sicherheitsregeln zur Steuerung des Nutzerzugriffs auf Wechseldatenträger, lokale Anwendungen oder Zeitbeschränkungen für den Internet-Zugang.

GRANULARE PRÜFUNGSKONFIGURATION UND -VERWALTUNG

BitDefender Client Security bietet verschiedene Prüfmethodologien, um Schad-Software aufzuspüren und die Integrität von Laptops und Arbeitsstationen des Netzwerks zu schützen. Verschiedene Prüfoptionen helfen bei der Aufrechterhaltung der Systemintegrität und minimieren Beeinträchtigungen des Benutzererlebnisses.

On-Access Echtzeitprüf-Engines zum Aufspüren von Viren in Echtzeit, wenn ein Benutzer einer Dokumentenbibliothek oder -liste ein Dokument hinzufügt bzw. ein Dokument daraus abruft.

On-Demand Prüfungen erlauben geplante System-Prüfungen ausserhalb der Spitzenzeiten, ohne die Gesamtleistung oder Verfügbarkeit des Systems zu beeinträchtigen.

Konfiguration der planmäßigen Prüfung bietet konfigurierbare Ereignisplanung für On-Demand-Prüfungen und Update-Aufgaben, so dass während der Kernbetriebszeiten mögliche Serverbeeinträchtigungen oder Systemunterbrechungen minimiert werden.

Quarantäne für infizierte oder verdächtige Dateien dient der Isolation von verdächtige Dateien in Quarantänebereichen. Diese Dateien können gereinigt werden, zu Auswertungszwecken in Quarantäne verbleiben, nach erfolgreicher Validierung am Ursprungsort wiederhergestellt oder zur Einschätzung direkt ins BitDefender Antivirus Lab gesendet werden.

INTEGRATION MIT DER CENTRAL MANAGEMENT-PLATTFORM VON BITDEFENDER

Zahlreiche Arbeitsstationen lassen sich schnell und einfach über die zentrale Management-Plattform von BitDefender verwalten, so dass IT-Administratoren von unternehmensweiter Transparenz der Bedrohungen durch Malware sowie von der Möglichkeit profitieren, ihre Netzwerkressourcen proaktiv zu schützen. Der BitDefender Management Server bietet einen zentralen Punkt für Remote-Installation, -Konfiguration und -Reporting sämtlicher BitDefender-Produkte auf den Clients, Servern und Gateways des Unternehmens. Administratoren werden mit Hilfe des umfassenden Warnmeldungsmoduls über Prüfleistung, Infektionen und Update-Aufgaben informiert.

vb 100 VIRUS virusbtn.com

Compatible with Windows 7

Bitdefender