

# BITDEFENDER ZENTRALES MANAGEMENT



## ZENTRALES MANAGEMENT DER UNTERNEHMENS SICHERHEIT

Zu den größten Herausforderungen heutiger IT-Abteilungen gehören Kontrollierbarkeit und Transparenz der gesamten Sicherheitslage des Unternehmens. Leider verfügen viele Unternehmen aus Kostengründen nicht über eigene Ressourcen zur Entwicklung und Verwaltung geeigneter Netzwerksicherheitsstrategien. Kleine und mittelständische Betriebe unterliegen oft strikten Budgetbeschränkungen, und IT-Aufgaben werden von Mitarbeitern in Doppelrollen erledigt. Diese mangelnde Priorisierung erschwert die Implementierung eines effektiven Sicherheitsprogramms bei den meisten kleinen und mittelständischen Unternehmen.

Wenn ein Unternehmen wächst, steigern neue Mitarbeiter, Systeme und Anwendungen zur Umsetzung neuer Geschäftsiniciativen auch oft die Gesamtzahl der Angriffsvektoren, die von Schad-Software zur Infiltration des Unternehmensnetzwerks ausgenutzt werden. Um proaktiv tätig zu werden, müssen IT-Abteilungen Kontrollen implementieren und so die Auswirkungen von schädlichen Anwendungen, Software und Internet-Ressourcen – beispielsweise Web-2.0-Anwendungen – begrenzen, die das Unternehmen weiteren Angriffsrisiken aussetzen.

## SICHERHEITSLÖSUNGEN FÜR ENDGERÄTE REICHEN NICHT AUS

Antivirs-Schutz auf den Laptops und Arbeitsplätzen des Unternehmens ist zwar die Grundlage jeder guten Sicherheitspolitik, reicht aber nicht mehr aus, um Ihre Arbeitskraft vor den Risiken durch Schad-Software zu schützen. Malware wird ständig weiterentwickelt, um die implementierten Sicherheitslösungen zu umgehen, und kann sich rasant ausbreiten, wenn sie nicht von ausgleichenden Kontrollmaßnahmen aufgespürt wird. Daher wurden die Antimalware-Lösungen von BitDefender über den eigentlichen Virenschutz hinaus entwickelt und bieten eine Lösung, die proaktiv einen Schutz auf nicht verwalteten Arbeitsstationen und Servern installiert, unautorisierte Anwendungen remote erkennt und entfernt und auch Systemeinstellungen remote vornehmen kann. So lassen sich die Folgen von Malware-Infektionen des Netzwerks minimieren.

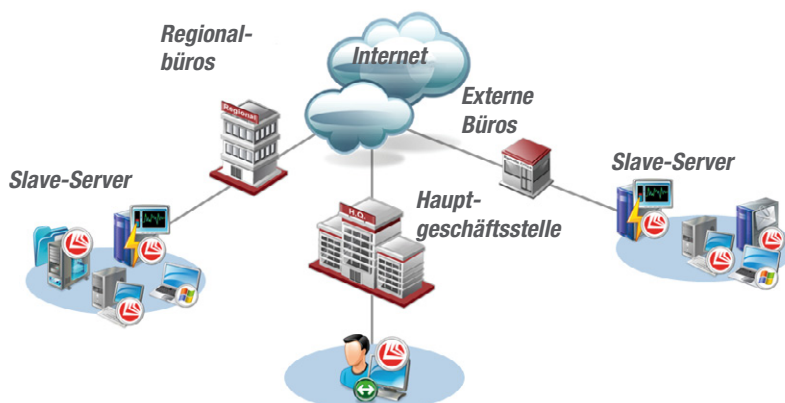
## SICHERHEIT FÜR IHR UNTERNEHMEN MIT BITDEFENDER

Die zentrale Management Console von BitDefender ist eine einheitliche Verwaltungsplattform für die Remote-Installation, -Konfiguration und -Auswertung sämtlicher BitDefender-Produkte auf den Clients, Servern und Gateways des Netzwerks. BitDefender Centralized Management umfasst:

- Netzwerkweite Transparenz sämtlicher Ereignisse im Zusammenhang mit Malware für IT-Administratoren
- Proaktive Prüfung von Hard- und Software-Einrichtungen des Netzwerks
- Remotekonfiguration und -verwaltung von Client- und Serversystemeinstellungen
- Reporting von Ereignissen im Zusammenhang mit Malware zur Identifikation von Infektionsraten und Trends
- Tools zur Messung der Wirksamkeit des Anti-Malware-Sicherheitsprogramms des Unternehmens

## HAUPTMERKMALE UND -VORTEILE

- Reduzierte Ressourcenkosten und weniger Verwaltungsaufwand bei mehreren Endgeräten und Servern
- On-Demand-Problemkonsolidierung mit One-Click-Lösung
- Ermöglicht die Remote-Konfiguration, -Prüfung, -Installation und -Anwendungsentfernung von jedem Endgerät und Serversystem des Netzwerks
- Netzwerkprüfungsdaten für datenbankbasierte Inventar- und Änderungsberichte können automatisch erhoben werden
- Netzwerkerkennung von Endgeräten ohne Installationen von Antivirenlösungen, Remote-Installationen von Client Security
- Konfigurierbare Sicherheitsrichtlinien mit Vorlagen zur Unterstützung der Richtlinien-durchsetzung
- Vereinfachte Netzwerkverwaltung durch assistentengesteuerte Netzwerk-Tasks
- Integration mit Active Directory ermöglicht die Nutzung vorhandener Windows-Domänenstrukturen und Gruppenrichtlinien
- Ermöglicht über eine zentrale Management-Konsole Remote-Konfigurationen von einem beliebigen Unternehmens-Computer aus
- Skalierbare Master-Slave-Architektur zur Verwaltung von Gateways, Servern und Endgeräten an physisch getrennten Orten



## ENDGERÄTEPRÜFUNG UND VERWALTUNGSSKRIPTS

Der BitDefender Management Server verwendet die Skriptsprache Windows Management Instrumentation (WMI) für die Prüfung und Verwaltung von Endgeräten und Servern. Zur Automatisierung der Fernverwaltung sind über 30 vordefinierte WMI-Skriptvorlagen enthalten; beenden Sie Anwendungen und Prozesse, installieren und deinstallieren Sie Software, starten Sie Arbeitsstationen oder fahren Sie sie herunter, aktivieren oder deaktivieren Sie Autoruns und greifen Sie auf USB-Wechselmedien zu.

## UMFASSENDE SCHUTZ

BitDefender Centralized Management ist das Hauptelement einer umfassenden Suite von Lösungen, die durchgängigen Netzwerkschutz vom Gateway bis zum Desktop bieten. Die proaktiven Multi-Plattform-Produkte erkennen und stoppen Viren, Spyware, Adware und Trojaner, die die Integrität Ihres Netzwerks bedrohen.

## SYSTEMANFORDERUNGEN

Die zentrale Management-Lösung von BitDefender umfasst drei Hauptkomponenten: Management Server als zentrales Management-Backend für alle BitDefender-Lösungen, Management Console als Benutzeroberfläche, Update Server als Download- und Verteilungsplattform der Produkt- und Virendefinitions-Updates.

### *BitDefender Management Server, Management Console und Update Server*

#### Minimal erforderlicher Prozessor:

- Intel Pentium 1 GHz (2 GHz empfohlen)

#### Minimaler RAM-Speicher:

- 512MB (2GB empfohlen)

#### Minimaler freier Festplattenspeicher:

- 1,5 GB  
(2,5 GB empfohlen), 3 GB bei Upgrades

#### Betriebssystem:

- Windows 2000 Professional SP4
- Windows 2000 Server, SP4
- Windows XP SP2
- Windows Server 2003 SP2
- Windows Vista
- Windows Server 2008
- Windows Server 2008 R2
- Windows Small Business Server (SBS) 2008
- Windows 7

#### Datenbank:

- Microsoft SQL Server 2005, 2008 oder Microsoft SQL Express Edition (enthalten)

#### Die Management Console unterstützt die folgenden

##### Browser:

- Internet Explorer 7 (oder höher)
- Internet Explorer 6 (Windows 2000)



Die Konsole von BitDefender verwaltet Gateways, Endgeräte und kritische Server von einem zentralen Punkt aus

## TRANSPARENZ UND FERNVERWALTUNGSFUNKTIONEN

Die BitDefender Management Console ist einfach in Installation und Verwaltung und kombiniert die Transparenz der aktuellen Sicherheitslage eines Unternehmens mit der Remotekonfiguration von Endgeräten und Richtlinien-durchsetzung über eine zentrale Oberfläche. Die Management Console fasst Informationen über Bedrohungen sowie über den Systemstatus sämtlicher verwalteter Windows-, Mac- und UNIX-basierter Arbeitsstationen bzw. Server des Unternehmensnetzwerks zusammen. Systemereignisse bei Endgeräten und kritische Probleme werden rasch identifiziert und per „One Click“-Problemlösung behoben – bei minimalem Verwaltungsaufwand und extrem geringen Reaktionszeiten.



Die UNIX-basierten Lösungen von BitDefender verwenden eine separate, webbasierte Fernverwaltungsoberfläche für BitDefender Security for Mail Servers bzw. für BitDefender Security for Samba File Servers. In Ergänzung zu der webbasierten Fernverwaltungsoberfläche ist für fortgeschrittene Benutzer auch eine Befehlszeilenschnittstelle verfügbar, falls eine Standardschnittstelle zur Verwaltung der Netzwerkinfrastruktur bevorzugt wird.

## MASTER/SLAVE-ARCHITEKTUR DES MANAGEMENT SERVERS

Die zentrale Synchronisation von Richtlinien, Produkten und Updates wird über einen Master Management Server unternehmensweit gesteuert. Dies ermöglicht die zentrale und intelligente Verteilung von Updates innerhalb des lokalen oder fernverwalteten Netzwerks über den Einsatz eines lokalen Slave Management Servers. Die Architektur stellt sicher, dass die Updates den lokalen Ressourcen zur Verfügung stehen, um die Netzwerkauslastung zu optimieren.

## AKTUALISIERUNG NACH PLAN ODER AUTOMATISCH

BitDefender Management Server ermöglicht die intelligente Verteilung neuer Virendefinitionen und Produktaktualisierungen von einem zentralen Punkt aus. Die Aktualisierungen können entweder bei Verfügbarkeit automatisch stündlich vorgenommen werden oder nach Plan stattfinden, um dabei Spitzenzeiten zu vermeiden und Leistungsabfälle sowie Beeinträchtigungen des Netzwerks zu minimieren.

## VERWALTETE SICHERHEITSRICHTLINIEN AUF EINER WINDOWS BASIERTEN DOMÄNE STRUKTUR

Dank Integration mit Active Directory können die Unternehmen ihre vorhandenen Windows-Domänenstrukturen und Gruppenrichtlinien nutzen. Sicherheitsrichtlinien lassen sich direkt umsetzen, indem Benutzer oder Benutzergruppen aus dem Active Directory gewählt werden, anstatt Gruppen von Arbeitsstationen im Management Server zu verwalten. Der BitDefender Management Server erkennt nicht verwaltete Arbeitsstationen, um sie einfach identifizieren zu können. Dann lassen sie sich entweder durch automatisierte Remote-Bereitstellung verwalten, oder ausgewählte Arbeitsstationen werden von den allgemeinen Sicherheitsrichtlinien ausgenommen.