# BITDEFENDER SECURITY FOR SAMBA

## SCHUTZ PLATTFORMÜBERGREIFENDER NETZWERKRESSOURCEN

Samba-Datei-Server werden in vielen großen, heterogenen Netzwerken als Ressourcen verwendet, da sie eine günstige Suite von Dienstprogrammen mitbringen und Interoperabilität zwischen Linux/UNIX- und Windows-basierten Arbeitsstationen und Servern ermöglichen. Samba bietet per SMB/CIFS-Protokoll sichere, stabile und schnelle Datei- und Druckerdienste für verschiedenste Plattformen einschließlich sämtlicher Versionen von DOS, Windows, OS/2 und Linux.

Samba ist eine wichtige Komponente, die Linux-/UNIX-Arbeitsstationen und -Server nahtlos in Active Directory-Umgebungen von Microsoft integriert. Aufgrund dieser Integrationsfunktion in die Windows-Umgebung kann Samba schnell zum Überträger von Schad-Software werden, die auf die Windows-Plattform abzielt.

Die kritischen Dienste, die von Datei-Servern im Netzwerk bereitgestellt werden, beinhalten:

- Web-Server (Apache)
- Datei- und Drucker-Server (Samba)
- Remotezugriffs-/VPN-Server
- DNS-Server

Samba-Datei-Server können die folgenden Sicherheitsrisiken verbreiten:

- Schad-Code über gemeinsame Dateien
- Infizierte komprimierte Archive
- Viren, Trojaner und Rootkits
- Würmer und Spyware

Auf Samba Shares gespeicherte Dateien können stets andere Systeme mit unerwünschter Spyware, Adware, mit Trojanern und Viren infizieren. Auch Würmer können sich in Netzwerken ausbreiten und Server unbemerkt infizieren. Besteht kein Schutz, fallen die entsprechenden kritischen Netzwerkdienste aus und stehen den Benutzern nicht zur Verfügung. Die Produktivität des Unternehmens wird so empfindlich beeinträchtigt.

## SICHERE SAMBA-DATEI-SERVER MIT BITDEFENDER

Unternehmen können ihre Samba-Datei-Server vor Angriffen schützen, indem Sie die Fähigkeit von BitDefender nutzen, Dateien auf Schad-Software hin zu prüfen, die Einhaltung der Sicherheitsrichtlinien des Unternehmens zu gewährleisten und sensible Daten vor einer Verbreitung außerhalb des Unternehmens zu schützen.

BitDefender Security for Samba ermöglicht Unternehmen den Schutz ihrer Samba-Netzwerkfreigaben auf Linux-, FreeBSD- und Solaris-Systemen vor Viren und Spyware. Security for Samba wird zentral innerhalb des Netzwerks eingesetzt und gewartet. Plattformübergreifend werden Datenstrukturen und Dateispeicher auf Malware geprüft und vor Virusinfektionen geschützt.

## HAUPTMERKMALE UND -VORTEILE

- Preisgekrönte Virenerkennung, Bereinigung und Quarantäne
- Minimiert Ausfallzeiten sowie Risiken von Malware-Infektionen des Netzwerks, indem gemeinsame Dateien geprüft werden, um den Echtzeitschutz vor Schad-Software zu garantieren
- Erlaubt flexible Planung von On-Demand- oder Immediate-Execution-Prüfungen
- Infizierte und verdächtige Dateien werden zur Risikominimierung in Quarantäne verschoben
- Ermöglicht über eine zentrale Management-Konsole Remote-Konfigurationen von einem beliebigen Unternehmens-Computer aus
- Erfüllt den File System Hierarchy Standard (FHS) und arbeitet ausschließlich nicht-intrusiv
- Kann mit jedem Samba Build betrieben werden und ist dank des integrierten Open-Source-VFS-Moduls mit allen Versionen kompatibel
- Kompatibel mit allen gängigen UNIX-basierten Plattformen durch rpm-, deb- und generische .tar.run-Pakete

Bitdefender

## ERWEITERTE FUNKTIONEN

- Integration mit dem BitDefender Management Server
- Zentrales Dashboard mit Bereitstellungsstatus und Alarmschwellen
- Sichere Unterbringung verdächtiger Dateien in Quarantäne mit optionaler Funktion für eine Wiederherstellung am Ursprungsort
- Anpassbare E-Mail-Benachrichtigungen oder SNMP-Warnungen bei Aktivität: Anzahl geprüfter, desinfizierter, gelöschter, infizierter oder gefilterter Dateien

## BITDEFENDER TECHNOLOGIEN

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.

## UMFASSENDER SCHUTZ

BitDefender Security for Samba File Servers ist nur ein Element einer umfassenden Suite von Lösungen, die End-to-End-Schutz 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

**Betriebssystem:**

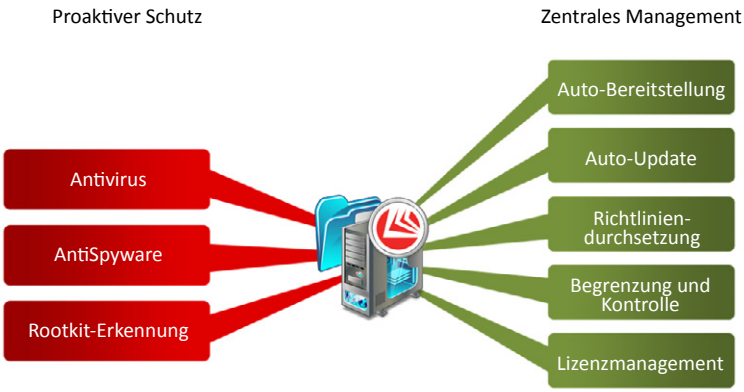
- Linux, FreeBSD, Solaris
- Linux Kernel 2.6.18 oder höher
- glibc 2.3.1 oder höher und libstdc++ von gcc4 oder höher

**Samba:**

- Version 3.0 oder höher

**Unterstützte Distributionen:**

- Debian GNU/Linux 3.1 oder höher
- Fedora Core 1 oder höher
- FreeBSD: 5.4-RELEASE (oder höher, mit compat5x)
- Mandrake/Mandriva 9.1 oder höher
- Novell SuSE Linux Enterprise Server 9, Linux 8.2 oder höher
- OpenSolaris 2008 oder 2009 (x86-Plattform)
- Oracle Linux 5 oder höher
- RedHat Enterprise Linux 3, Linux 9 oder höher
- Slackware 9.x oder höher
- Solaris 9 oder 10 (x86-Plattform)




BitDefender Security for Samba File Server bietet proaktiven Schutz und ein zentrales Management

## INNOVATIVE PROAKTIVE ERKENNUNG

Die preisgekrönten Prüf-Engines von BitDefender sind für Samba-Datei-Server-Umgebungen optimiert und wurden von führenden Zertifizierungsbehörden wie ICSA Labs, Virus Bulletin und West Coast Labs wegen ihres unschlagbaren proaktiven Schutzes vor Malware ausgezeichnet. BitDefender bietet mehrfachen Schutz durch hochentwickelte Technik;

**Antivirus –** Zusätzlich zur signaturbasierten Erkennung bietet BitDefender auch heuristische Erkennungsmethoden, die einen virtuellen „Computer im Computer" simulieren und hier alle Dateien und Software auf schädliches Verhalten hin überprüfen. Diese Technik liefert weniger falsch positive Ergebnisse und hat deutlich bessere Erkennungsraten bei Zero-Day- und unbekannten Bedrohungen.

**Antispyware –** BitDefender spürt bekannte Spy- und Adware über Dateiprüfmethoden auf, um Infektionen mit Spyware und damit verbundene Risiken von Datenlecks nach außen zu unterbinden.

**Trojaner und Rootkits –** Diese wurden 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.

## GRANULARE PRÜFUNGSKONFIGURATION UND -VERWALTUNG

BitDefender Security for Samba bietet Prüfmethoden On-Access, On-Demand und nach Plan, um Schad-Software aufzuspüren und die Integrität der Datei-Repositorys zu sichern. Verdächtige Dateien werden in Quarantänebereichen isoliert. 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

BitDefender Security for Samba File Servers ermöglicht die Integration mit den Sicherheits-Dashboards des Management Servers und schafft für Administratoren so eine unternehmensweite Transparenz der Netzwerkressourcen und der gesamten Sicherheitslage. 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

Bitdefender