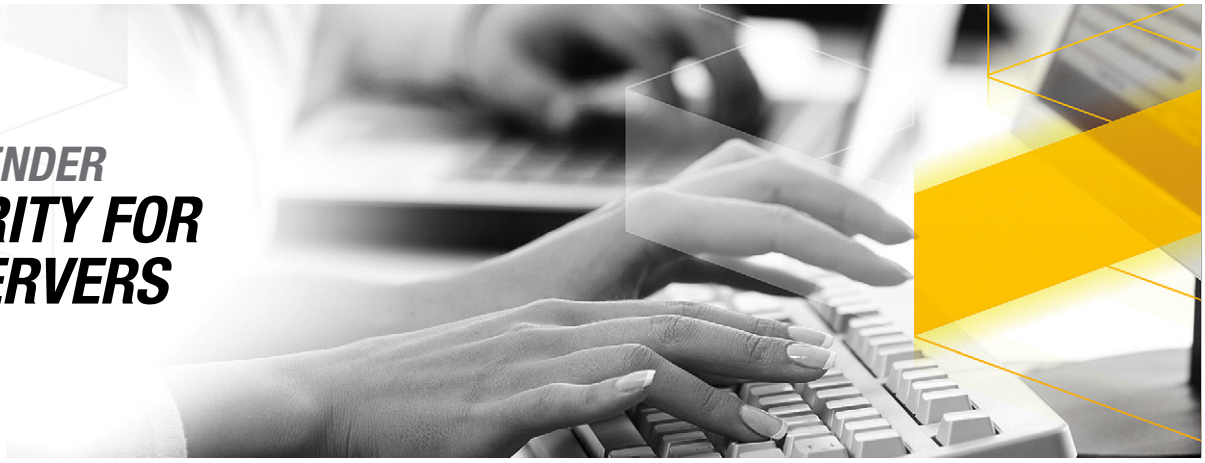


# BITDEFENDER SECURITY FOR ISA SERVERS

## INTERNET-GATEWAYS – DIE ERSTE VERTEIDIGUNGSLINIE

Heute gewähren Unternehmen dem Großteil ihrer Mitarbeiter gemeinsamen Zugriff auf das Internet. Webbasierte Proxy-Dienste können bei der Verwaltung der Bandbreitenauslastung helfen und den Datenverkehr mit lokalen Zwischenspeichern stabilisieren. Der Webzugriff zu persönlichen und geschäftlichen Informationszwecken steigert das Volumen des Internet-Datenverkehrs beträchtlich – und damit auch das Bedrohungsrisiko. Unternehmen mit Internet-Gatewaylösungen wie Microsoft® Internet Security and Acceleration (ISA) Server profitieren von schnelleren Internet-Reaktionszeiten und den grundlegenden Firewall-Funktionen, die eine erste Verteidigungslinie darstellen.

## SCHUTZ FÜR INTERNET-GATEWAYS

Unternehmen, die Gateways für den Internet-Zugriff einsetzen, profitieren von der Sicherheit der zusätzlichen Firewall. Doch der Schutz ist aufgrund der statischen Firewall-Regeln und mangelnder Transparenz der Pakete, die das Gateway passieren, begrenzt. Daher kann ein solcher Schutz vor Schad-Software, die das Unternehmensnetzwerk über nicht überwachte Anwendungen oder aufgrund mangelhafter Prüfung von Inhalten unterwandert, nicht verhindern, dass eine Infektion gegebenenfalls enorme Kosten und Zeitaufwand verursacht.

Webbasierte Dienste können Sicherheitsrisiken bergen, darunter:

- Websites und heruntergeladene Dateien, die mit Schad-Software infiziert sind
- das Herunterladen infizierter E-Mail-Anhänge von Online-E-Mail-Diensten
- das Hoch- oder Herunterladen infizierter Dateien über einen FTP-Dienst
- Infektionen, die sich in einem zugeordneten Netzlaufwerk ausbreiten

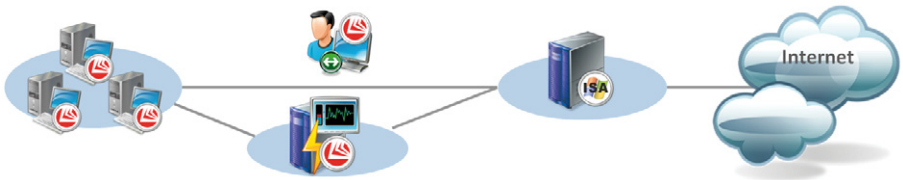
Gateways stellen einen zentralen Durchgangspunkt für internetbasierte Inhalte dar und helfen Unternehmen, Richtlinien für den ein- und ausgehenden Datenverkehr zu implementieren. Um die Sicherheit und Überlebensfähigkeit von ISA-Serverinstallationen zu optimieren, ohne dabei Leistung und Reaktionszeiten geschäftskritischer Prozesse zu beeinträchtigen, bedarf es zusätzlicher Lösungen, die die operative Effizienz sicherstellen.

## SICHERE INTERNET-GATEWAYS MIT BITDEFENDER

BitDefender Security for ISA Servers ermöglicht Unternehmen, ihre Microsoft® ISA Server zu schützen, bestimmte Arten von Websites zu blockieren und heruntergeladene Dateien sowie E-Mail-Anhänge von Internet-E-Mail-Diensten zu prüfen. Dies erleichtert die Einhaltung der Sicherheitsrichtlinien und die dauerhafte Kontrolle sensibler Daten, die vor einer Verbreitung außerhalb des Unternehmens geschützt werden müssen.

## HAUPTMERKMALE UND -VORTEILE

- Preisgekrönte Virenerkennung, Bereinigung und Quarantäne
- Minimierte Ausfallzeiten des Netzwerks für mehr operative Effizienz
- Reduzierte Sicherheitsrisiken und Aufwendungen für Ressourcen, gesteigerte Produktivität
- Browser-freundliche Technologie zur Prüfung und Übertragung großer Dateien in kleinen Blöcken
- Pflegeleichte, stichwortbasierte schwarze Listen für Webseiten und FTP-Server und weiße Listen für sichere Webseiten
- Prüft den Datenverkehr und bietet Echtzeitschutz zur Minimierung des Ausbreitungsrisikos von Malware im Netzwerk
- Integration mit Firewall-Regeln und Web-Caching von Microsoft über das Virus Scanning Interface (ISAPI) von Microsoft zur Optimierung und Beschleunigung des Prüfprozesses
- Reports zu Virenaktivitäten, Prüfstatistiken und Internet-Datenverkehrsvolumen
- Konfigurierbare Aktionen lösen bei verschiedenen Ereignissen E-Mail-Warnungen und andere Maßnahmen aus
- Unterstützt hohe Auslastungen durch multiple ISA-Server in Array-Konfiguration zum Ausgleich der Arbeitslast
- Ermöglicht über eine zentrale Management-Konsole Remote-Konfigurationen von einem beliebigen Unternehmens-Computer aus




BitDefender Security for ISA Servers prüft ein- und ausgehenden Datenverkehr mit Internet- und FTP-Diensten auf Basis bestimmter Prüf- und Filterregeln, die sich über den zentralen Management Server konfigurieren lassen.

Bitdefender

## 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.

## AUTOMATISCHE UPDATES

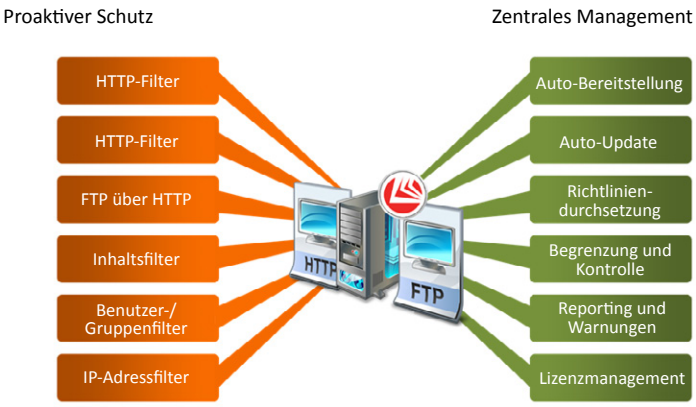
BitDefender Security for ISA Servers bietet stündliche, intelligente Aktualisierung der Virusdefinitionen, damit Ihr Microsoft® ISA Server konstant und zuverlässig gegen die neuesten Bedrohungen geschützt ist.

## UMFASSENDER SCHUTZ

BitDefender Security for ISA Servers ist nur ein Element 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

- Windows Server 2003 mit SP1, Windows Server 2003 R2
- Windows Server 2008, Windows Server 2008 R2
- Microsoft ISA Server 2000/2004/2006 Standard Edition
- Microsoft ISA Server 2004/2006 Enterprise Edition
- Internet Explorer Version 6.0 oder höher




BitDefender Security for ISA Servers bietet preisgekrönte Virenerkennungs-, Verwaltungs- und Reportingfunktionen, um einen sicheren unternehmensweiten Zugriff auf Informationen zu gewährleisten.

## MEHRERE PRÜF- UND FILTERLEVEL

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 Prüf- und Filtertechnologien auf mehreren Ebenen, um Schad-Software aufzuspüren und vertrauliche Daten zu schützen:

**Web-Datenverkehr (http)**– Die Prüf-Engine spürt Viren und Malware in Echtzeit auf, während der Benutzer Websites aufruft und auf E-Mail-Dienste oder andere webbasierte Anwendungen zugreift.

**FTP-Upload/-Download**– Die Prüffunktionen spüren Viren und Malware in Echtzeit auf, sobald Benutzer Dateien über File Transfer Protocol (FTP) hoch- oder herunterladen.

**Inhaltsfilterung** – Inhaltsfilter erkennen vordefinierte Informationen wie Kreditkarten- oder Namen von Kundendatenbanken etc. und dass sie den Kontrollbereich des Unternehmens verlassen. Die Inhaltsfilterung verwendet auf Web- oder FTP-Serveradresse, Schlüsselbegriffen und Inhaltsgröße basierende, anpassbare Beschränkungen.

**Schwarze und weiße Listen**– Dienen der Blockierung von Webseiten auf Basis von Stichworten bzw. der Auflistung bekannter, sicherer Webseiten.

**Nutzungsrichtlinien**– Diese Richtlinien ermöglichen flexible Einschränkungen innerhalb des Unternehmensnetzwerks auf Basis von IP-Adressbereichen, Inhaltsarten oder Protokollen.

## SCHUTZ IN EIN- UND AUSGANGSRICHTUNG

- Preisgekrönte Virenerkennung, Bereinigung und Quarantäne
- Integration mit Firewall-Regeln und Web-Caching von Microsoft über das Virus Scanning Interface (ISAPI) von Microsoft zur Optimierung und Beschleunigung des Prüfprozesses
- Prüft Dateien und Web-Inhalte und bietet so Echtzeitschutz zur Minimierung des Ausbreitungsrisikos von Malware im Netzwerk
- Pflegeleichte, stichwortbasierte schwarze Listen für Webseiten und FTP-Server und weiße Listen für sichere Webseiten

## OPTIMIERUNG, MANAGEMENT UND REPORTING

- Reduziert den Verwaltungsaufwand durch zentrales Benachrichtigungs-Management über die Integration von BitDefender-Warnungen mit dem Warnmeldungsmodul von ISA-Servern
- Unterstützt ISA-Server-Installationen in Array-Konfiguration zum Ausgleich der Arbeitslast in Umgebungen mit hohen Datenverkehrsauslastungen
- Browser-freundliche Technologie zur Prüfung und Übertragung großer Dateien in kleinen Blöcken
- Reports zu Virenaktivitäten, Prüfstatistiken und Internet-Datenverkehrsvolumen
- Konfigurierbare Aktionen lösen bei verschiedenen Ereignissen E-Mail-Warnungen und andere Maßnahmen aus

Bitdefender