

Trend Micro™

# InterScan™ Web Security Suite 3.1 for Linux

Umfassender Schutz vor Internet-Bedrohungen am Gateway

Cyber-Kriminelle nutzen jede Möglichkeit, um mit Hilfe komplexer Internet-Bedrohungen die Schutzvorrichtungen Ihres Unternehmens zu umgehen und sich unrechtmäßig zu bereichern. Ziel dieser allgegenwärtigen, profitgesteuerten Internet-Bedrohungen ist es, in Computer einzudringen, weitere Komponenten herunterzuladen und sich dann schnell an das jeweilige System anzupassen, um herkömmlichen Suchmethoden zu entgehen. Ohne wirkungsvollen Schutz am Internet-Gateway können Internet-Bedrohungen ungehindert in Ihr Netzwerk eindringen, Kundendaten entwenden, die Produktivität beeinträchtigen und Ihren Umsatz schwächen.

InterScan™ Web Security Suite schützt dynamisch vor webbasierten Angriffen am Internet-Gateway durch integrierte Bedrohungsabwehr. Diese hochperformante Software-Lösung ergänzt mehrfach ausgezeichneten Spyware- und Virenschutz durch eine neue Web-Reputation-Funktion. Diese erkennt und blockiert Internet-Bedrohungen, indem sie die Integrität der Quelle überprüft. Die InterScan Web Security Suite durchsucht auch den Inhalt und Fluss des HTTP- und FTP-Verkehrs. Auf Clients und Servern entdeckte Spyware wird automatisch, ohne Einsatz eines Agenten entfernt. Mit einer hoch skalierbaren Plattform und zentraler Verwaltung zur einfachen Administration arbeitet die InterScan Web Security Suite mit der Endpunkt-, Messaging- und Netzwerksicherheit zusammen und bietet dadurch vollständigen Schutz vor Internet-Bedrohungen.

## DIE WICHTIGSTEN FUNKTIONEN

### Web Reputation

- Sperrt den Zugriff auf verdächtige Domains und schützt dadurch vor Zero-Day-Angriffen
- Führt umfangreiche Bewertungen von Websites durch, ohne dass Datenbank-Updates erforderlich sind
- Bietet höchsten Benutzerkomfort durch hochperformante Echtzeitfilter
- Erweitert den Schutz auf Computer außerhalb des Netzwerks mit durchgängigem Internet-basierten Design

### Mehrfach ausgezeichneter Schutz vor Viren und Spyware

- Schützt HTTP- und FTP-Verkehr vor neuen und aufkommenden Bedrohungen
- Schützt vor dem Weiterleiten ausspionierter Daten und stoppt Spyware-Downloads
- Verhindert das Tunneln von Malware über nicht-HTTP-basierte Protokolle, wie Instant Messaging
- Blockiert den Zugriff auf böartige Spyware- und bekannte Phishing-Websites

### Automatische Säuberung (optional)

- Löst bei verdächtiger Webaktivität automatisch die Trend Micro™ Damage Cleanup Services aus
- Entfernt Bedrohungen von infizierten Clients und Servern ohne Einsatz eines Agenten
- Reduziert Kosten für die Schadensbeseitigung, minimiert den Administrationsaufwand und ermöglicht eine schnellere Wiederaufnahme der Produktivität

### Flexibler URL- und Applet-Filter (Advanced Version)

- Filtert URLs in Echtzeit durch den Abgleich mit flexiblen Richtlinien und einer umfassenden Spyware-Datenbank
- Kombiniert Web Reputation und Webseiten-Kategorisierung, um sicheren Zugriff zu gewährleisten
- Überprüft und analysiert ActiveX-Steuerelemente und Java-Applets, um den unbemerkten Download gefährlicher Dateien zu verhindern
- Verringert die Gefahr von Haftungsansprüchen durch die Überwachung des Zugriffs von Mitarbeitern auf unangemessene Websites

### Einfache Installation und Verwaltung bei reduziertem Risiko und geringeren Gesamtkosten

- Zentrale Verwaltung über Trend Micro Control Manager™, eine webbasierte Konsole mit Zugriff von jedem Punkt im Netzwerk
- Protokolliert Malware-Aktivitäten und bietet eine aktuelle Übersicht des Sicherheitszustands und der Bedrohungsabwehr im System
- Ermöglicht ausgewählten Benutzern die Überwachung des Systems und die Erstellung von Echtzeit- oder zeitgesteuerten Berichten
- Unterstützt SNMP, LDAP und Active Directory™, erhöht die Integration und senkt die Gesamtkosten

## SOFTWARE

### Geschützte Punkte

- Internet-Gateway

### Schutzumfang

- Komplexe Bedrohungen
- Viren und Würmer
- Internet-Bedrohungen
- Bots
- Spyware und Keylogger
- Böartiger mobiler Code
- Rootkits
- Phishing
- Content-Bedrohungen

## ENTSCHEIDENDE VORTEILE

- Blockiert den Zugriff auf böartige Websites durch die branchenweit umfassendste Web Reputation
- Stoppt Spyware und andere Internet-Bedrohungen am Gateway
- Vereinfacht die Verwaltung bei geringeren Kosten
- Verbessert die Mitarbeiterproduktivität durch URL-Filter
- Optimiert das Internet-Erlebnis durch hochperformante Suchfunktionen

## PIONIER IM BEREICH GATEWAY-SICHERHEIT

Trend Micro war einer der ersten Anbieter von Gateway-Sicherheitslösungen und baut seither seine Position als Marktführer kontinuierlich aus, beispielsweise durch die Kombination von Virenschutz und Schutz vor anderen Bedrohungen. Die Trend Micro Gateway-Sicherheitsprodukte werden von TrendLabs<sup>SM</sup> unterstützt, einem globalen Netzwerk von Antiviren-Zentren, das rund um die Uhr Bedrohungen überwacht und Präventionsstrategien entwickelt. Die genauen Echtzeitdaten von TrendLabs ermöglichen wirksame und zeitgenaue Sicherheitsmaßnahmen zur Erkennung, Prävention und Abwehr von Angriffen.

Die InterScan Web Security Suite schützt Ihr Gateway vor Internet-Bedrohungen und anderer Malware, um ungestörten Betriebsablauf zu gewährleisten, die Systemleistung zu verbessern und das Marken-Image zu bewahren.

GESCHÜTZTE PUNKTE			
Schutz		Standard	Advanced
<b>Web Reputation</b>	Sperrt den Zugriff auf bössartige Websites durch Bewertungen der Vertrauenswürdigkeit	✓	✓
<b>Virenschutz</b>	Sperrt Malware, wie z. B. Zero-Day-Angriffe	✓	✓
<b>Anti-Spyware</b>	Entdeckt und verhindert den Download von Spyware	✓	✓
<b>Integrierte Damage Cleanup Services</b>	Entfernt automatisch Spyware- und Malware-Dateien	✓	✓
<b>URL-Filter</b>	Verhindert das Surfen auf Websites, die nicht den Unternehmensrichtlinien entsprechen		✓
<b>Java-Applet- und ActiveX-Sicherheit</b>	Schützt vor unbemerkten Installationen durch Analyse des mobilen Codes		✓

## SYSTEMVORAUSSETZUNGEN

- RedHat Enterprise Linux AS 4 oder EL AP 5; Novell SUSE Linux Enterprise Edition 9 oder 10
- Server mit mindestens Intel Pentium™ 4 (2,4 GHz) oder entsprechendem Prozessor
- Mindestens 2 GB RAM
- Mindestens 4 GB Festplattenspeicher für URL-Filtermodul, Datenbank und Protokolldateien.
- Microsoft™ Internet Explorer 6.0 oder Firefox Mozilla 1.5 für Zugriff auf webbasierte Administrationskonsole
- Datenbank: Postgres v7.4.13 (im Umfang enthalten) oder die neuere 7.4.x-Version (bei separater Installation)
- ICAP 1.0-kompatibler Cache-Server (optional)
  - Cisco™ ICAP Server (CE Version 5.1.3, b15) oder
  - NetApp™ NetCache™ Release 6.0.1 oder
  - BlueCoat Systems™ SGOS 5.x
- Directory Server Integration (optional)
  - Microsoft Active Directory 2000 und 2003
  - Linux OpenLDAP Directory 2.2.16
  - Sun™ Java System Directory Server 5.2 (früher: Sun ONE Directory Server)
- Unterstützt Damage Cleanup Services 3.0\*
- Unterstützt Trend Micro Control Manager 3.0 SP6 und 3.5 mit aktuellen Hotfixes\*

## Trend Micro™ Enterprise Protection Strategy

Trend Micro™ Enterprise Protection Strategy bietet einen umfassenden, mehrschichtigen Ansatz zur Netzwerksicherheit. Die Produkte und Services von Trend Micro™ werden unterstützt von TrendLabs<sup>SM</sup>, einem globalen Netzwerk von Forschungszentren, das rund um die Uhr Bedrohungen überwacht und Präventionsstrategien entwickelt.



## WEITERE PRODUKTE

- InterScan™ Web Security Appliance

## ERGÄNZENDE PRODUKTE

- Zentrale Verwaltung
  - Trend Micro Control Manager
- Produkte zur Messaging-Sicherheit
  - InterScan™ Messaging Security Suite
  - InterScan™ Messaging Security Appliance
  - InterScan™ Messaging Hosted Security
- Endpunktsicherheit
  - OfficeScan Client/Server Edition
- Sicherheitsservices
  - Damage Cleanup Services



\*Eine vollständige Liste der Systemvoraussetzungen für optionale Produkte und Services finden Sie unter <http://de.trendmicro.com>

©2008 by Trend Micro Incorporated. Alle Rechte vorbehalten. Trend Micro, das T-Ball Logo, Trend Micro Control Manager, InterScan und TrendLabs sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Firmen- und/oder Produktnamen sind Marken oder eingetragene Marken ihrer jeweiligen Eigentümer. Die in diesem Dokument enthaltenen Informationen können sich ohne vorherige Ankündigung ändern. [DS12\_IWSS31\_071219DE]