Trend Micro™

ServerProtect™ for Microsoft™ Windows™/Novell™ NetWare™

Einfacher und wirksamer Malware-Schutz für Server auf Enterprise-Ebene

Unternehmensserver können einen anfälligen, zentralen Punkt für den Informationsaustausch darstellen. Selbst innerhalb des Netzwerks können Benutzer oder Anwendungen ohne ausreichenden Schutz infizierte Dateien unbeabsichtigt auf den Server laden. Durch Zugriff auf diese Dateien kann sich die Malware auf weitere Systeme ausbreiten. Zudem verfügen Großunternehmen über hunderte bis tausende von Einzelservern, die überwacht, konfiguriert und gewartet werden müssen. Noch wichtiger ist jedoch, dass die heutigen raffinierten Angriffe auf mehrere Punkte im Netzwerk abzielen und unbemerkt Schäden hinterlassen und das Risiko einer erneuten Infektion bedeuten können.

Trend Micro™ ServerProtect™ bietet den branchenweit zuverlässigsten Schutz vor Viren, Spyware und Rootkits. Gleichzeitig vereinfacht und automatisiert es Sicherheitsvorgänge auf Servern. ServerProtect durchsucht und entdeckt Malware in Echtzeit und umfasst Säuberungsfunktionen, um bösartigen Code zu entfernen und Systemschäden zu beheben. Der Administrator kann den Malware-Schutz über eine zentrale Management-Konsole auf allen Servern eines Unternehmens durchsetzen, verwalten und aktualisieren. Mit dieser robusten Lösung können Unternehmen das gesamte Server-Dateisystem einschließlich komprimierter Archive schützen, Viren-Pattern zur Entfernung von nicht erkannten Viren verteilen und den Säuberungsvorgang automatisieren, um Probleme zu beheben, die durch Vireninfektionen ausgelöst wurden. Kosten und Aufwand bei einer Vireninfektion werden damit deutlich gesenkt.

DIE WICHTIGSTEN FUNKTIONEN

Zuverlässiger und wirksamer Malware-Schutz

- Mehrfach ausgezeichnete Scan-Engine-Technologie mit einer langjährigen Erfolgsgeschichte im Bereich Malware-Schutz
- Kombination von Technologien, die zur wirksamen Malware-Erkennung auf Regeln und auf der Erkennung von Pattern basieren
- Neue APIs zur besseren Erkennung und Beseitigung von Spyware und Rootkits
- Schutz von internen Kommunikationskanälen zur Vermeidung von Malware-bedingten Unterbrechungen
- Malware-Support rund um die Uhr durch weltweite TrendLabs℠ Forschungs- und Support-Zentren

Optimaler Schutz durch automatische Suche

- Individuelle Anpassung je nach Aufgabe, um bestimmte Anforderungen hinsichtlich des Arbeitsablaufs für Echtzeitsuchen, bedarfsgesteuerte Suchen, zeitgesteuerte Suchen, Verteilung, Protokollierung und Statistiken zu erfüllen
- Aufteilen zeitgesteuerter Suchen, um häufig genutzte Verzeichnisse mit einer anderen Häufigkeit zu durchsuchen als selten verwendete Verzeichnisse
- Geringere Beeinträchtigung von Ressourcen durch Analyse des Datenverkehrs und Erstellung benutzerdefinierter RTS-Richtlinien (Release Time for Research) für unterschiedliche Tageszeiten

Zentrale Installation und Verwaltung

- Vereinfachte Erstverteilung und kontinuierliche Verwaltung aller wichtigen Windows und NetWare Server
- Zentrale Verwaltung der Systemüberwachung, Software-Updates, Konfigurationsänderungen und Ereignisbenachrichtigungen über eine Remote-Konsole
- Zentrale Steuerung mehrerer ServerProtect Information Server und Installation von Produkt-Updates auf allen Servern über eine einzige Konsole
- Gleichzeitige Installation von Programmen und Updates auf Servern und Überwachung des Serverstatus in Echtzeit
- Zentrale Verwaltung von Sicherheitsstrategien, die im gesamten Multisite-Netzwerk installiert werden

Sofortiger Schutz und Säuberungsfunktionen

- Entfernen von Malware-Überresten von allen Servern durch automatisierte Säuberung und Reparatur, um das Risiko einer erneuten Infektion zu minimieren
- Suchen und Beseitigen von Malware in komprimierten Archiven zur Vermeidung unnötiger Dekomprimierung
- Erkennen von Sicherheitslücken durch die Ausführung der Schwachstellensuchfunktion (erhältlich auf Anfrage)

SOFTWARE

Bedrohungsschutz

- Viren
- Spyware
- Rootkits

Geschützte Punkte

- Microsoft Server
- Novell NetWare Server

ENTSCHEIDENDE VORTEILE

- Zuverlässiger und wirksamer Malware-Schutz
- Zentrale Installation und Verwaltung
- Einfache Administration und Richtliniendurchsetzung für alle Server
- Plattformübergreifender Schutz des heterogenen Netzwerks sorgt für eine Produktunterstützung auf Enterprise-Ebene
- Vireneindämmungsfunktion verhindert die Ausbreitung von Malware

ServerProtect™ kann so konfiguriert werden, dass Updates der Viren-Pattern-Dateien und der Scan Engine automatisch heruntergeladen und anschließend auf bestimmte Server verteilt werden. Die Lösung nutzt einen inkrementellen Update-Mechanismus, so dass die angegebenen Server nur die neuen Viren-Pattern-Dateien herunterladen, die seit der letzten Version hinzugefügt wurden. Dies reduziert die für den Download benötigte Zeit und schont die Bandbreite.

ServerProtect verwendet eine dreistufige Architektur: die Management-Konsole, den Information Server und den Normal Server. Ein Normal Server kann jeder Server im Netzwerk sein, auf dem ServerProtect installiert ist, z. B. ein File- oder FTP-Server. Die Management-Konsole wird für die Konfiguration dedizierter Information Server genutzt, die dann die Normal Server steuern.

MINDESTSYSTEMVORAUSSETZUNGEN

Microsoft™ Windows™

Betriebssysteme

- Windows Server 2008 Standard/Enterprise/Storage/Datacenter/Web (x32 & x64 ohne Hyper-V)
- Windows Server 2008 Core Standard/Enterprise/Datacenter/Web (x32 & x64)
- Windows Server 2008 Hyper-V Standard/Enterprise/Storage/Datacenter (x64)
- Windows Server 2003 Standard/Enterprise/Storage Edition (SP1 oder SP2 oder R2– x32 & x64)
- Microsoft Windows 2000 Standard/Advanced mit SP4

Normal Server (Antiviren-Server) und Information Server

- Intel Pentium IV 2,5 GHz oder Intel 3,0 GHz EM64T oder AMD Athlon 2,0 GHz 64 Bit oder vergleichbarer Prozessor
- 1 GB Arbeitsspeicher (512 MB für Windows Server 2003 Standard/Enterprise und Windows 2000); 500 MB Festplattenspeicher

Novell™ NetWare™

Novell Netware 6.5 Patch 7 oder Patch 8 (Open Enterprise Server 2)

- PC der Server-Klasse mit einem Pentium IV oder AMD Athlon Prozessor
- 512 MB Arbeitsspeicher; 500 MB Festplattenspeicher

Webbasierte Management-Konsole

Betriebssysteme

- Windows Server 2008 Standard/Enterprise/Storage/Datacenter/Web (x32 & x64 ohne Hyper-V)
- Windows Server 2008 Core Standard/Enterprise/Datacenter/Web (x32 & x64)
- Windows Server 2008 Hyper-V Standard/Enterprise/Storage/Datacenter (x64)
- Windows Server 2003 Standard/Enterprise/Storage Edition (SP1 oder SP2 oder R2 – x32 & x64)
- Windows 2000 Standard/Advanced/Professional mit SP4
- Windows XP Home/Professional
- Windows Vista Home/Business/Ultimate

Verwaltungsserver

- Intel Pentium IV 2,5 GHz oder Intel 3,0 GHz EM64T oder AMD Athlon 2,0 GHz 64 Bit oder vergleichbarer Prozessor
- 1 GB Arbeitsspeicher (512 MB für Windows Server 2003 Standard/Enterprise und Windows 2000); 500 MB Festplattenspeicher

Virtualisierungsunterstützung

- VMware™ ESX Server 3.5 oder ESXi (ESX Server Edition)
- VMware Server 2 (Server Edition)

ZUSÄTZLICHE PRODUKTE ZUM SCHUTZ VON SERVERN

- ServerProtect for Linux
- ServerProtect for EMC Celerra
- ServerProtect for NetApp
- Deep Security

ERGÄNZENDE PRODUKTE UND SERVICES

- OfficeScan™ Client-Server Suite
- Trend Micro Endpoint Security Platform
- InterScan™ Messaging Security Lösungen
- InterScan™ Web Security Lösungen
- Trend Micro™ Premium Support Services

www.trendmicro.com