Symantec™ Endpoint Protection 12.1.5 Datenblatt

Datenblatt: Endgerätesicherheit

Übersicht

Malware hat sich von groß angelegten, massiven Angriffen hin zum Einschluss gezielter Attacken und andauernder moderner Bedrohungen entwickelt, die nicht allein durch Virenschutz gestoppt werden können. Es ist Zeit, mehr zu unternehmen. Die einzigartige Fähigkeit von Symantec, intelligente Sicherheit zu bieten, nutzt das kollektive Wissen des weltgrößten Global Intelligence Network (GIN), das Daten von Millionen Nutzern und Sensoren sammelt. Die einzigartige Insight™ Technologie in Symantec™ Endpoint Protection ist von GIN abgeleitet – sie blockiert wechselnde Bedrohungen und ermöglicht schnellere Scanzeiten, indem sie die Reputation einer Datei analysiert. Währenddessen stoppt SONAR™ Technologie neu auftretende Bedrohungen, in dem sie das Dateiverhalten in Echtzeit überwacht. Mit einem einzigen Hochleistungs-Agenten, der intelligente Sicherheitstechnologien mit starkem Antivirenschutz und Policy Lockdown integriert, ermöglicht es Ihnen Symantec™ Endpoint Protection 12.1.5, sich aufs Geschäft zu konzentrieren, ohne Kompromisse bei Sicherheit und Leistung einzugehen.

Einzigartige Sicherheit

Stoppt gezielte Attacken und andauernde moderne Bedrohungen mit intelligenter Sicherheit und geschichtetem Schutz, der über Virenschutz hinausgeht.

- Nutzt das weltgrößte Global Intelligence Network (GIN), bestehend aus Hunderten Millionen von Sensoren, die Daten in unsere proaktiven Schutztechnologien einspeisen.
- Abgeleitet von GIN ist die einzigartige Insight™ Technologie: Sie ermittelt die Dateireputation, indem sie die wichtigsten Dateieigenschaften analysiert – etwa, wie oft die Datei heruntergeladen wurde, wie lange sie dort gespeichert war und von wo sie heruntergeladen wird. Diese Informationen ermöglichen es uns, mehr Bedrohungen zu blockieren und neue, sich ändernde Malware abzuwehren.
- SONAR™ Technologie, ebenfalls von GIN abgeleitet, überwacht das Verhalten von Anwendungen in Echtzeit und stoppt gezielte Angriffe sowie neu auftretende Bedrohungen.
- Network Threat Protection analysiert Datenströme, die auf dem Gerät eines Nutzers ankommen, über Netzwerkverbindungen und blockiert Bedrohungen, bevor sie das System treffen können.
- Symantec™ Endpoint Protection ermittelt und entfernt mehr Bedrohungen als alle anderen Lösungen dieser Klasse[1]. Im Dennis Labs Real World A/V Test hat sie mehrfach die Bewertung AAA erhalten, die bestmögliche Note.

Überragende Leistung

Performance, die so schnell ist, dass die Nutzer sie nicht einmal bemerken.

- Die in Endpoint Protection enthaltene Symantec Insight™ Technologie spart bis zu 70 Prozent der Scanzeit im Vergleich zu herkömmlichen Lösungen, indem sie die Dateireputation präzise feststellt – auf diese Weise werden nur gefährdete Dateien gescannt.
- Ermöglicht es Hardware dank verringertem Einfluss auf das System, schneller zu arbeiten und länger zu halten.
- Reduziert die Netzwerkbelastung, indem sie flexible Kontrolle über eine Reihe von Verbindungen und Bandbreiten bietet.
- Übertrifft alle Produkte ihrer Klasse in Scan-Geschwindigkeit und Gesamtleistung[2].

1 AV-TEST, Product Review, Corporate Solutions for Windows 7, July/August 2013.
2 PassMark Software, “Enterprise Endpoint Security Performance Benchmarks”, 2014.

Smarteres Management

Eine einzige Management-Konsole für physische und virtuelle Plattformen mit granularer Richtlinienkontrolle.

- Enthält intelligente Sicherheitstechnologien und Policy Lockdown-Funktionen in einem einzigen Hochleistungs-Agenten mit einer einzigen Management-Konsole für PC, Mac, Linux und virtuelle Maschinen.
- Bietet granulare Richtlinienkontrolle mit der Flexibilität, Richtlinien je nach Nutzern und ihrem Standort anzupassen.
- Unterstützt entfernte Verteilung und Client Management sowohl für PC als auch für Mac – das erleichtert es, entfernte Endpunkte auf dem neuesten Stand zu halten.
- Erweitert herkömmliches Reporting, indem es eine mehrdimensionale Analyse und robustes grafisches Reporting in einem einfach bedienbaren Dashboard integriert.
- Group Update Provider reduziert den Netzwerk-Aufwand und senkt den Zeitaufwand für Updates, indem ein Client einfach Updates an einen anderen sendet. So werden effektivere Updates an entfernten Standorten möglich.

5 Schutzschichten

Symantec™ Endpoint Protection 12.1.5 bietet **5 Schutzschichten** 1) Netzwerk 2) Datei 3) Reputation 4) Verhalten und 5) Reparatur:

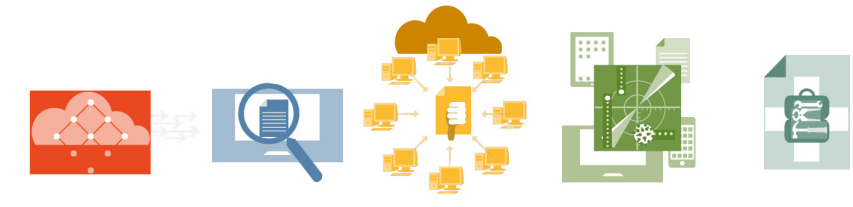
1) Netzwerk: Der Symantec Schutz vor Netzwerkbedrohungen umfasst *Vantage* Technologie, die ankommende Daten analysiert und Bedrohungen blockiert, während sie durch das Netzwerk wandern, bevor sie das System treffen können. Eine regelbasierte Firewall und Browserschutz sind ebenfalls inbegriffen, um vor webbasierten Angriffen zu schützen.

2) Datei: Signaturbasierter Virenschutz sucht nach Malware und löscht sie auf einem System, um vor Viren, Würmern, Trojanern, Spyware, Bots, Adware und Rootkits zu schützen.

3) Reputation: Das einzigartige Insight *von Symantec™* korreliert mehrere Milliarden Verlinkungen zwischen Nutzern, Dateien und Websites, um schnell wechselnde Bedrohungen aufzudecken. Durch Analyse wichtiger Dateieigenschaften kann Insight™ präzise erkennen, ob eine Datei gutwillig ist, und jeder Datei eine Reputationsbewertung zuweisen. Das bedeutet wirkungsvollen Schutz gegen gezielte Angriffe und reduziert zugleich den Scan-Aufwand um bis zu 70%.

4) Verhalten: SONAR™ nutzt künstliche Intelligenz, um vor neuen Bedrohungen zu schützen. Es stoppt wirkungsvoll neue und unbekannte Bedrohungen, indem es in Echtzeit nahezu 1.400 Datei-Verhaltensmuster überwacht, während sie ablaufen, um das Dateirisiko zu bestimmen.

5) Reparatur: Power Eraser™ scannt aggressiv infizierte Endpunkte, um die andauernden modernen Bedrohungen zu lokalisieren und hartnäckige Malware zu entfernen. Remote Support ermöglicht es dem Administrator, den Power Eraser-Scanvorgang zu starten und die Infektion rechnerfern von der Symantec™ Endpoint Protection Management-Konsole aus zu beseitigen.



Firewall und Schutz vor Eingriffen
Netzwerk
Blockiert Malware, bevor sie sich in Ihrem Gerät ausbreitet und den Traffic kontrolliert

Virenschutz
Datei
Scannt und löscht Malware, die auf einem System ankommt

Insight
Reputation
Bestimmt die Sicherheit von Dateien und Websites, indem es das Wissen der Community nutzt

Sonar
Verhaltensmuster
Überwacht und blockiert Programme, die ein verdächtiges Verhalten aufweisen

Power eraser
Reparatur
Aggressive Behebung von schwer entfernbaren Infektionen

Erweiterte Richtlinien-Kontrollfunktionen

Zusätzlich zu den grundlegenden Schutztechnologien bietet Symantec™ Endpoint Protection 12.1.5 auch granulare Richtlinienkontrollen, einschließlich:

1) System Lockdown: Verbessert den Schutz für geschäftskritische Systeme, indem es nur die Ausführung von Anwendungen aus der weißen Liste (die als gutwillig bekannt sind) erlaubt, oder Anwendungen aus der schwarzen Liste (die als böswillig bekannt sind) an der Ausführung hindert.

2) Application and Device Control: Hilft, interne und externe Sicherheitsverstöße zu verhindern, indem es das Anwendungsverhalten überwacht sowie Dateizugriffe, Registry-Zugriffe, erlaubte Prozesse und Geräte, auf die Informationen geschrieben werden dürfen, kontrolliert.

3) Host Integrity Checking & Policy Enforcement: Ermöglicht es Nutzern, auf ihren Endgeräten Scripts auszuführen, um Compliance zu verifizieren und zu berichten; Quarantäne und Überwachung des Datenaustauschs sperren und isolieren ein nicht konformes oder infiziertes System.

4) Location Awareness: Ermittelt automatisch, von welchem Ort aus ein System Verbindung aufnimmt, wie etwa von einem Hotel, Hotspot, WLAN oder VPN, und passt die Sicherheit so an, dass der beste Schutz für die Umgebung geboten wird.

System Lockdown

Sorgen Sie durch fortschrittliches Whitelisting und Blacklisting für die straffe Kontrolle von Anwendungen

Application Control

Überwachen und kontrollieren Sie das Verhalten von Anwendungen

Device Control

Beschränken und erlauben Sie den Zugriff auf die Hardware, die benutzt werden darf

Host Integrity

Stellt sicher, dass Endpunkte geschützt und regelkonform sind

Virtual Optimization

Symantec™ Endpoint Protection schützt ihre virtuelle High-Density-Umgebung, während sie zugleich die Leistung auf höherem Niveau hält als bei agentenlosen Lösungen sowie die Sichtbarkeit der End-to-end-Sicherheit bietet.

1) VMware vShield Integration: Ermöglicht höhere VM-Dichte und reduziert den Einsatz von I/O und CPU.

2) Virtual image exception: Setzt Dateien von einer virtuellen Maschine auf die weiße Liste, um das Scannen zu optimieren.

3) Resource leveling: Randomisiert den Scan und aktualisiert Zeitpläne, um Störungen des Ressourceneinsatzes zu vermeiden.

4) Shared Insight™ cache: Scannt Dateien einmal, tauscht die Ergebnisse zwischen den Clients aus und dedupliziert das Dateiscannen, um Bandbreite und Wartezeit zu reduzieren.

5) Virtual client tagging: Erkennt und berichtet automatisch, ob der Client in einer virtuellen Umgebung läuft – das macht es leichter, unterschiedliche Richtlinien für virtuelle Maschinen zu erstellen.

6) Offline image scanning: Findet Bedrohungen in Offline-Bildern von virtuellen Maschinen.

7) Scan-Drosselung für die Virtualisierung: Ermittelt die Festplattenauslastung und reduziert die Scan-Geschwindigkeit, um Nutzungsstörungen zu vermeiden.

Systemanforderungen für Client Workstation und Server*

Windows Betriebssysteme

- Windows XP (32-bit, SP2 oder höher; 64-bit)
- Windows XP Embedded (SP2 oder höher)
- Windows Vista (32-bit, 64-bit)
- Windows 7 (32-bit, 64-bit)
- Windows 7 Embedded
- Windows 8 (32-bit, 64-bit)
- Windows Server 2003 (32-bit, 64-bit, R2 oder SP1 oder höher)
- Windows Server 2008 (32-bit, 64-bit, einschließlich R2)
- Windows Server 2012 (32-bit, einschließlich R2)
- Windows Small Business Server 2011 (64-bit)
- Windows Essential Business Server 2008 (64-bit)

Macintosh Betriebssysteme

- MAC OS X 10.6.8, 10.7, 10.8, 10.9
- MAC OS X Server 10.6, 10.7, 10.8, 10.9

Linux Betriebssysteme (32-bit- und 64-bit-Versionen)

- Red Hat Enterprise Linux
- SuSE Linux Enterprise (Server/Desktop-PC)
- Novell Open Enterprise Server
- Oracle Linux
- VMWare ESX
- Ubuntu
- Debian
- Fedora

Virtuelle Umgebungen

- vSphere Server (ESXi)
- Microsoft Hyper-V
- Citrix XenServer, XenDesktop, XenApp

Hardware-Anforderungen

- 1 GHz CPU oder höher
- 512 MB RAM (1 GB empfohlen)
- 850 MB freier Speicherplatz auf der Festplatte

Managersystem-Anforderungen

Windows Betriebssysteme

- Windows 7
- Windows XP (32-bit, SP3 oder höher; 64-bit, SP2 oder höher)
- Windows Server 2003 (32-bit, 64-bit, R2 oder SP1 oder höher)
- Windows Server 2008 (32-bit, 64-bit, einschließlich R2)
- Windows Small Business Server 2008 (64-bit)
- Windows Small Business Server 2011 (64-bit)
- Windows Essential Business Server 2008 (64-bit)
- Windows Server 2012 (64-bit, einschließlich R2)

Hardware

- 1 GHz CPU oder höher
- 1 GB of RAM (2 GB empfohlen)
- 16 GB oder mehr freier Speicherplatz auf der Festplatte

Webbrowser

- Microsoft Internet Explorer
- Mozilla Firefox

Datenbank

Eingebettete Datenbank inklusive, oder wählen Sie aus den folgenden:

- SQL Server 2005, SP4 oder höher
- SQL Server 2008 und R2
- SQL Server 2012
- SQL Server 2014