IBM Tivoli Endpoint Manager for Security and Compliance

Lösung für das zentrale Management der Endgerätesicherheit im gesamten Unternehmen

Highlights

- Bereitstellung aktueller Informationen und zentrale Steuerung über eine einzige Managementkonsole
- Nutzung eines einzelnen, vielseitigen, intelligenten Agenten, der Probleme einschätzt und beseitigt, um kontinuierliche Sicherheit und Compliance zu gewährleisten
- Verwaltung Hunderttausender von physischen und virtuellen Endgeräten, unabhängig von deren Standort, Verbindungstyp oder Status
- Automatisches Management von Patches für mehrere Betriebssysteme und Anwendungen

Die Zahl der Endgeräte und der Sicherheitsrisiken, denen sie ausgesetzt sind, wächst heute so schnell wie nie zuvor. Deshalb bietet IBM Tivoli Endpoint Manager for Security and Compliance eine Lösung für die Bereitstellung einheitlicher Informationen in Echtzeit und die Durchsetzung von Richtlinien, um Ihre komplexe und in hohem Maße verteilte Umgebung zu schützen.

Tivoli Endpoint Manager for Security and Compliance ist dafür ausgelegt, die Sicherheit von Endgeräten im gesamten Unternehmen zu gewährleisten. Die Lösung hilft Ihrem Unternehmen, sowohl seine Endgeräte zu schützen als auch den zuständigen Aufsichtsbehörden gegenüber nachzuweisen, dass es die geltenden Compliance-Bestimmungen einhält. Diese Lösung, die einfach zu managen und schnell zu implementieren ist, unterstützt die Sicherheit in einer Umgebung, die eine Vielzahl verschiedenster Endgeräte umfassen kann – von Servern über Desktop-PCs und mobil eingesetzte Laptops mit Internetzugang bis zu spezialisierten Geräten wie Kassensystemen, Bankautomaten und Self-Service-Kiosken.

Tivoli Endpoint Manager for Security and Compliance kann die Kosten und Komplexität des IT-Managements reduzieren und gleichzeitig die Flexibilität des Unternehmens steigern, die Problembehebung beschleunigen und die Genauigkeit erhöhen. Da die Lösung nur geringe Auswirkungen auf den laufenden Betrieb der Endgeräte hat, sorgt sie für höhere Produktivität und eine verbesserte Benutzererfahrung. Durch die konstante Durchsetzung von Richtlinien, wann immer Endgeräte mobil eingesetzt werden, trägt Tivoli Endpoint Manager for Security and Compliance dazu bei, das Risiko zu senken und die Transparenz bei Audits zu erhöhen, um kontinuierliche Compliance zu erreichen.

Erfüllung der Sicherheitsanforderungen im gesamten Unternehmen

Tivoli Endpoint Manager for Security and Compliance ist eine Lösung für die Bewältigung von Sicherheitsproblemen im Zusammenhang mit Desktop- und verteilten Umgebungen. Das Produkt vereint Funktionen für das Management und den Schutz von Endgeräten in einer einzigen Lösung und trägt so dazu bei, kontinuierliche Sicherheit und Compliance sicherzustellen. Beispielsweise kann die Lösung Sicherheitslücken deutlich schneller beseitigen, indem Software-Patches in nur wenigen Minuten eingespielt werden. Außerdem kann die Lösung die Lücke zwischen verschiedenen Abteilungen überbrücken, z. B. zwischen den Abteilungen, die für die Festlegung und Umsetzung einer Strategie und Richtlinie verantwortlich sind, Abteilungen für das Management von Geräten in Echtzeit und Abteilungen für die Erstellung von Berichten zu Sicherheits- und Compliance-Fragen.

Tivoli Endpoint Manager for Security and Compliance bietet Folgendes:

- Bereitstellung akkurater, präziser und aktueller Informationen zur Erkennung und kontinuierlichen Durchsetzung von Sicherheitskonfigurationen und Patches
- Zentrales Management von Produkten für Malware- und Firewallschutz verschiedener Anbieter
- Bereitstellung sofort einsatzfähiger bewährter Verfahren (Best Practices), die den US-FDCC-Bestimmungen (Federal Desktop Configuration Control) und den Defence Information Systems Agency Security Technical Implementation Guides (DISA STIGs) entsprechen
- Unterstützung des Security Content Automation Protocol (SCAP); Tivoli Endpoint Manager ist das erste Produkt, das vom National Institute of Standards and Technology (NIST) sowohl für die Einschätzung als auch die Behebung von Sicherheitsproblemen zertifiziert wurde
- Sichere Übertragung von Endgeräteanweisungen, nachgewiesen durch die Zertifizierungen gemäß NIAP CCEVS EAL3 und FIPS 104-2 Level 2
- Unterstützung des OVAL-Standards (Open Vulnerability and Assessment Language), um offene und öffentlich zugängliche Sicherheitsinhalte zu fördern
- Erhalt der vom SANS Institute veröffentlichten Warnmeldungen bezüglich Schwachstellen und Sicherheitsrisiken und Einleitung geeigneter Abhilfemaßnahmen
- Anzeige von Trends und Analysen zu Änderungen an Sicherheitskonfigurationen durch erweiterte Berichtsfunktionen

Zusätzliche Funktionen, die für alle Produkte der Tivoli Endpoint Manager-Produktfamilie auf der Basis von BigFix-Technologie verfügbar sind, ermöglichen Folgendes:

- Erkennung von Endgeräten, von denen Unternehmen möglicherweise gar nicht wussten, dass sie sich in ihrer Umgebung befinden – in einigen Fällen konnten so bis zu 30 Prozent mehr Endgeräte identifiziert werden
- Bereitstellung einer einzigen Konsole für Management-, Konfigurations-, Analyse- und Sicherheitsfunktionen zur Vereinfachung des Betriebs
- Anwendung gezielter Maßnahmen auf eine bestimmte Art von Endgerätekonfiguration oder einen bestimmten Benutzertyp unter Verwendung praktisch jeder Hardware- oder Softwareeigenschaft
- Nutzung einer einheitlichen Managementinfrastruktur zur Koordination des IT-, Sicherheits-, Desktop- und Serverbetriebs
- Erreichbarkeit von Endgeräten unabhängig vom Standort, Verbindungstyp oder Status mit umfassenden Managementfunktionen für alle wichtigen Betriebssysteme, Anwendungen anderer Anbieter und richtlinienbasierte Patches

Tivoli Endpoint Manager for Security and Compliance ermöglicht automatisierte, in hohem Maße zielgenaue Prozesse, die die nötige Kontrolle, Transparenz und Schnelligkeit für die Umsetzung von Änderungen und den Nachweis der Compliance bieten. Sicherheitsprobleme, z. B. Risiken durch Malware und Viren, können durch Funktionen für ein rasches Patch-Management schnell behoben werden.

Eine breite Palette an leistungsfähigen Sicherheitsfunktionen

Tivoli Endpoint Manager for Security and Compliance enthält die im Folgenden aufgeführten Schlüsselfunktionen und bietet Ihnen zudem die Möglichkeit, bei Bedarf auf einfache Weise weitere ausgewählte Funktionen hinzuzufügen, ohne dass zusätzliche Infrastruktur- oder Implementierungskosten anfallen.

Patch-Management

Das Patch-Management beinhaltet umfassende Funktionen für die Bereitstellung von Patches für Microsoft® Windows®, UNIX®, Linux® und Mac OS und für Anwendungen von Anbietern wie Adobe, Mozilla, Apple und Java™ für verteilte Endgeräte – unabhängig von deren Standort, Verbindungstyp

oder Status. Ein einziger Management-Server kann bis zu 250.000 Endgeräte unterstützen. Damit lässt sich die für das Einspielen von Patches benötigte Zeit verkürzen, ohne Verlust von Endgerätefunktionalität, selbst über Netzwerke mit geringer Bandbreite oder global verteilte Netzwerke. Echtzeitreports liefern Informationen dazu, welche Patches wann und von wem implementiert wurden, sowie eine automatische Bestätigung, dass Patches eingespielt wurden. Damit steht eine vollständige, in sich geschlossene Lösung für den Patch-Prozess zur Verfügung.

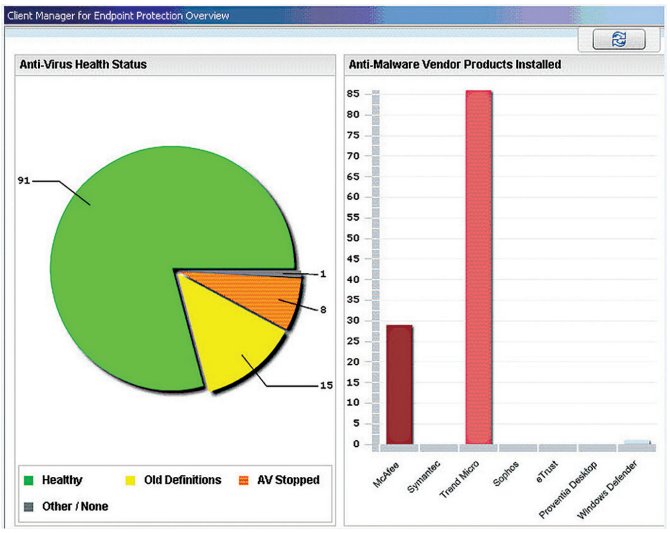
Sicherheitskonfigurationsmanagement

Die Sicherheitskonfigurationsfunktionen der Lösung, die vom NIST zertifiziert wurden, stellen eine umfassende Bibliothek mit technischen Steuerungen bereit, die Sie durch die Erkennung und Durchsetzung von Sicherheitskonfigurationen bei der Einhaltung von Compliance-Bestimmungen unterstützen. Diese Richtlinienbibliotheken unterstützen die kontinuierliche Durchsetzung von Konfigurationsgrundlagen (Configuration Baselines). Sie entdecken, behandeln und bestätigen die Behandlung von Richtlinienverstößen bei Endgeräten in Echtzeit für alle Endgeräte.

Dieses Feature liefert aussagefähige Informationen zum Status und zur Sicherheit von Endgeräten, unabhängig von deren Standort, Betriebssystem oder Verbindung (berücksichtigt werden sowohl fest verkabelte Computer als auch sporadisch mit einem Netzwerk verbundene mobile Laptops) und unabhängig von den installierten Anwendungen. Das Feature trägt dazu bei, den Compliance-Lifecycle zu konsolidieren und zu vereinheitlichen, und reduziert so den Zeitaufwand für die Konfiguration von Endgeräten und die Behebung von Sicherheitsproblemen.

Schwachstellenmanagement

Das Schwachstellenmanagement erlaubt Ihnen die Erkennung, Einschätzung und Beseitigung von Schwachstellen, bevor sie sich auf die Endgeräte auswirken können. Das Feature prüft Systeme im Hinblick auf standardisierte OVAL-Schwachstellendefinitionen und meldet Richtlinienverstöße in Echtzeit. Daraus ergeben sich größere Transparenz und volle Integration bei jedem Schritt im gesamten Workflow aus Erkennung, Einschätzung, Behebung und Dokumentation von Schwachstellen.



Die von Tivoli Endpoint Manager for Security and Compliance bereitgestellten Reports helfen Unternehmen, die Probleme, die die Effektivität ihrer Sicherheits- und Compliance-Maßnahmen beeinträchtigen, zu visualisieren.

Die IT-Mitarbeiter können – entweder mittels automatisierter oder manueller Maßnahmen – bekannte Schwachstellen bei Endgeräten erkennen und beseitigen. Durch Verwendung eines einzigen Tools, das Schwachstellen sowohl erkennt als auch beseitigt, können Administratoren die Schnelligkeit und Genauigkeit erhöhen und die Zyklen für die Implementierung von Patches, Software-Updates und Fixes für Schwachstellen verkürzen. Zudem können Administratoren das Sicherheitsmanagement auf mobile Clients, sowohl im Netzwerk als auch außerhalb, ausweiten. Sie können Warnmeldungen konfigurieren, um nicht autorisierte Assets schnell zu erkennen, und Maßnahmen ergreifen, um sie zu lokalisieren und zu entfernen oder anderweitig Abhilfe zu schaffen.

Asset-Erkennung

Mit Tivoli Endpoint Manager for Security and Compliance hat die Asset-Erkennung nichts mehr mit „Erbsenzählerei“ zu tun. Stattdessen schafft die Lösung ein dynamisches Lagebild der sich ändernden Bedingungen in der Infrastruktur. Die Fähigkeit, häufige Scans des gesamten Netzwerks durchzuführen, sorgt für umfassende Transparenz und Kontrolle. Dadurch wird sichergestellt, dass Unternehmen alle IP-adressierbaren Geräte – darunter virtuelle Maschinen, Netzwerkgeräte und Peripheriegeräte wie Drucker, Scanner, Router und Switches zusätzlich zu Computerendgeräten – schnell und mit nur minimalen Auswirkungen auf das Netzwerk identifizieren können. Dank dieser Funktion haben Unternehmen stets Einblick in alle Endgeräte, einschließlich mobiler Laptops und Notebooks, die außerhalb des Unternehmensnetzwerks eingesetzt werden.

Management von Produkten für die Endgerätesicherheit verschiedener Anbieter

Dieses Feature bietet Administratoren einen zentralen Steuerungspunkt für das Management von Sicherheitssoftware von Anbietern wie Computer Associates, McAfee, Sophos, Symantec und Trend Micro. Mit dieser zentralisierten Managementfunktion können Unternehmen die Skalierbarkeit, Schnelligkeit und Zuverlässigkeit von Sicherheitslösungen verbessern. Das Feature überwacht den Systemstatus, um sicherzustellen, dass Clients für die Endgerätesicherheit stets in Betrieb sind und Virusdefinitionen aktualisiert werden. Es bietet jedoch nicht nur eine einheitliche Sicht unterschiedlicher Technologien, sondern vereinfacht auch die Migration von Endgeräten von einer Lösung auf eine andere, da die Software einfach per Mausklick deinstalliert und neu installiert werden kann. Die in sich geschlossene Verifizierung stellt sicher, dass Updates und andere Änderungen durchgeführt werden – auch auf Endgeräten, die nicht mit dem Netzwerk verbunden sind. Dies wird durch eine Verifizierungsmethode über das Internet erreicht.

Automatische Netzwerkquarantäne

Tivoli Endpoint Manager for Security and Compliance prüft Endgeräte automatisch im Hinblick auf erforderliche Compliance-Konfigurationen – und wenn ein Endgerät nicht mit diesen konform ist, kann die Lösung das Endgerät so konfigurieren, dass es in Netzwerkquarantäne bleibt, bis die Konformität erreicht wird. Während der Quarantäne erhält der Tivoli Endpoint Manager-Server Managementzugriff auf das Endgerät, aber sämtliche sonstigen Zugriffsmöglichkeiten sind deaktiviert.

Anti-Malware- und Web-Reputation-Service (optionales Zusatzfeature)

Die enge Integration mit dem Core Protection Module (CPM) von Trend Micro bietet Features zum Schutz von Endgeräten vor Viren, Trojanern, Würmern, Spyware, Rootkits, neuen Malware-Varianten und schädlichen Websites. Durch die Abfrage von Echtzeitinformationen in der Cloud kann die Notwendigkeit von Definitionsdateien auf dem Endgerät praktisch ganz vermieden werden. Die Web-Reputation-Technologie hindert Benutzer daran, auf schädliche Websites zuzugreifen – ob gewollt oder unabsichtlich durch versteckte, automatisierte Aktionen, die von Malware ausgeführt werden.

Die Tivoli Endpoint Manager-Produktfamilie

Sie können Tools weiter konsolidieren, die Zahl der Endgeräteagenten reduzieren und Ihre Managementkosten senken, indem Sie Ihre Investitionen in Tivoli Endpoint Manager for Security and Compliance ausweiten und weitere Komponenten der Tivoli Endpoint Management-Produktfamilie hinzufügen. Da alle Funktionen über dieselbe Konsole, denselben Management-Server und denselben Endgeräteagenten gesteuert werden, können weitere Services auf einfache Weise hinzugefügt werden. Es muss lediglich der Lizenzschlüssel geändert werden.

- **Tivoli Endpoint Manager for Power Management** – Diese Option erlaubt die Durchsetzung von Richtlinien für Energieeinsparungen im gesamten Unternehmen, wobei sie die nötige Granularität bietet, um Richtlinien nur auf einen einzelnen Computer anzuwenden.
- **Tivoli Endpoint Manager for Lifecycle Management** – Diese umfassende und leistungsfähige Lösung wird der heutigen Konvergenz von IT-Funktionen gerecht, da sie Einblick in den Status von Systemendgeräten in Echtzeit bietet und Administratoren erweiterte Funktionalität für das Management dieser Endgeräte bereitstellt.

Tivoli Endpoint Manager: Auf der Basis von BigFix-Technologie

Die Grundlage aller Funktionen von Tivoli Endpoint Manager bildet ein spezieller Ansatz auf der Basis einer einzigen Infrastruktur, der die Entscheidungsfindung an die Endgeräte auslagert. Dieser Ansatz bietet enorme Vorteile für die gesamte Lösungsfamilie, unter anderem durch folgende Features:

- **Ein intelligenter Agent** – Tivoli Endpoint Manager nutzt eine herausragende Methode, bei der ein intelligenter Agent auf jedem Endgerät eingesetzt wird. Dieser einzelne Agent füllt mehrere Funktionen aus, darunter die kontinuierliche Selbstprüfung und Richtliniendurchsetzung, hat jedoch nur minimale Auswirkungen auf die Systemleistung. Im Gegensatz zu traditionellen Client-Server-Architekturen, die auf Anweisungen von einem zentralen Steuerungspunkt warten, initiiert dieser Agent Maßnahmen auf intelligente Weise. Er sendet Nachrichten an den zentralen Management-Server und ruft Patches, Konfigurationen oder weitere Informationen von diesem Server ab und verteilt sie an das Endgerät, sofern notwendig, um eine relevante Richtlinie einzuhalten. Aufgrund der Intelligenz und Schnelligkeit des Agenten kennt der zentrale Management-Server stets den Compliance- und Änderungsstatus von Endgeräten. Dadurch ist die schnelle Erstellung aktueller Compliance-Berichte möglich.
- **Reporting** – Die zentrale, einheitliche Konsole, die in Tivoli Endpoint Manager integriert ist, sorgt für ein hohes Maß an Transparenz, unter anderem dank der echtzeitorientierten und kontinuierlichen Berichterstellung und Analyse durch die intelligenten Agenten auf den Endgeräten des Unternehmens.
- **Relay-Funktionalität** – Dank der einfachen und skalierbaren Architektur von Tivoli Endpoint Manager kann jeder Agent als Relay zwischen anderen Agenten und der Konsole konfiguriert werden. Diese Relay-Funktion bietet die Möglichkeit, vorhandene Server oder Workstations für die Übertragung von Paketen über das Netzwerk einzusetzen, wodurch weniger Server benötigt werden.
- **IBM Fixlet-Nachrichten** – Die Fixlet Relevance Language ist eine veröffentlichte Befehlssprache, mit der Kunden, Geschäftspartner und Entwickler benutzerdefinierte Richtlinien und Services für die von Tivoli Endpoint Manager-Lösungen gesteuerten Endgeräte erstellen können.

Ausweitung der Tivoli-Stärken auf die Sicherheit

Tivoli Endpoint Manager for Security and Compliance ist Teil des umfassenden Portfolios an IBM Sicherheitslösungen, die Ihnen helfen, Sicherheitsprobleme im gesamten Unternehmen zu bewältigen. IBM Sicherheitslösungen unterstützen die digitalisierten, vernetzten und intelligenten IT-Abläufe eines smarteren Planeten. Sie bieten Informationen in Echtzeit, Funktionen für die zentralisierte Steuerung und verbesserte Sicherheit für die gesamte IT-Infrastruktur, einschließlich der global verteilten Endgeräte.

Tivoli Endpoint Manager-Produktfamilie auf einen Blick

Servervoraussetzungen:

- Microsoft SQL Server 2005/2008
- Microsoft Windows Server 2003/2008/2008 R2

Konsolenvoraussetzungen:

- Microsoft Windows XP/2003/Vista/2008/2008 R2/7

Unterstützte Plattformen für den Agenten:

- Microsoft Windows, einschließlich XP, 2000, 2003, Vista, 2008, 2008 R2, 7, CE, Mobile, XP Embedded und Embedded Point-of-Sale
- Mac OS X
- Solaris
- IBM AIX
- Linux auf IBM System z
- HP-UX
- VMware ESX Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise
- Oracle Enterprise Linux
- CentOS Linux
- Debian Linux
- Ubuntu Linux

Weitere Informationen

Wenn Sie mehr über IBM Tivoli Endpoint Manager for Security and Compliance erfahren möchten, wenden Sie sich bitte an Ihren IBM Vertriebsbeauftragten oder IBM Business Partner oder besuchen Sie die folgende Website: **ibm.com**/tivoli/endpoint

Tivoli-Software von IBM

Tivoli-Software von IBM unterstützt Unternehmen durch das effiziente und effektive Management von IT-Ressourcen, Aufgaben und Prozessen dabei, dynamischen Geschäftsanforderungen gerecht zu werden, ein flexibles und reaktionsfähiges IT-Service-Management zu erreichen und gleichzeitig die Kosten zu senken. Das Tivoli-Portfolio umfasst Software für das Management von Sicherheit, Compliance, Speicher, Performance, Verfügbarkeit, Konfigurationen, Betrieb und IT-Lebenszyklus und wird von erstklassigen IBM Service- und Supportangeboten sowie der IBM Forschung unterstützt.

IBM leistet keine rechtliche Beratung oder Beratung bei Fragen der Buchführung und Rechnungsprüfung. IBM gewährleistet und garantiert nicht, dass seine Produkte oder sonstigen Leistungen die Einhaltung bestimmter Rechtsvorschriften sicherstellen. Der Kunde ist für die Einhaltung anwendbarer Sicherheitsvorschriften und sonstiger Vorschriften des nationalen und internationalen Rechts verantwortlich.

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustrasse 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

Tivoli software

TID14075-DEDE-00