

BITDEFENDER INTEGRIERTE NETZWERKSICHERHEIT, PRÜFUNGEN UND SYSTEMWARTUNG

PROAKTIVE SYSTEMWARTUNG ERHÖHT DIE NETZWERKSICHERHEIT

Von IT-Abteilungen wird erwartet, dass sie trotz knapper Ressourcen effektiv arbeiten, was ihnen wenig Gelegenheit gibt, proaktive Maßnahmen zum Schutz vor chronischen Bedrohungen einzuführen. Kleine und mittelständische Unternehmen müssen oft mit einem extrem eingeschränkten Budget arbeiten, und IT-Aufgaben werden sehr häufig von Mitarbeitern übernommen, die noch andere Aufgaben haben. Diese Umstände machen es den Unternehmen schwer, Sicherheitslösungen und Tools zur automatischen Systemprüfung und -wartung zu implementieren, die manuelle Routineaufgaben automatisieren, die Netzwerksicherheit erhöhen oder die Einhaltung von IT-Richtlinien erleichtern könnten.

MEHR SICHERHEIT UND PRODUKTIVITÄT DURCH AUTOMATISIERUNG

Wenn ein Unternehmen wächst, wächst auch die Zahl der Mitarbeiter, Systeme und Office-Anwendungen, wodurch das firmeneigene Netzwerk immer komplexer wird. Jeder zusätzliche PC, Laptop oder Server muss von der IT-Abteilung erfasst und verwaltet werden, was sowohl das Netzwerk-Management als auch die Darstellung der tatsächlichen Abläufe erschwert. Um proaktiv und effektiv arbeiten zu können, muss eine IT-Abteilung dafür sorgen, dass ihr einfache und effiziente Werkzeuge zur Verfügung stehen, mit denen manuelle Routineaufgaben automatisiert werden können. Diese Werkzeuge sollten auch die Übersicht über die für das Tagesgeschäft nötigen Geräte und Anwendungen erleichtern. Durch automatisierte Abläufe können viele Sicherheitslücken schnell erkannt werden: unberechtigte Tätigkeit von Schadsoftware; unbekannte Geräte, auf denen Dienste laufen, die weitere Sicherheitsrisiken wie die Verbreitung von Viren, Infektion durch Schadsoftware oder unerwünschte Weitergabe von Daten bergen, und vieles mehr.

RISIKOMINIMIERUNG IN DER NETZWERKVERWALTUNG

Die Business Security-Lösungen von BitDefender lassen sich leicht installieren und verwalten. Sie erhöhen die Transparenz der unternehmensinternen Netzwerk-Sicherheitsarchitektur und die Effizienz wichtiger Aufgaben im IT-Management. Das zentrale Management fasst traditionelle unternehmenseigene Anti-Malware-Funktionen durch zentrale, assistentengesteuerte Netzwerk-Tools zusammen. Dies erleichtert die gleichzeitige Fernkonfiguration mehrerer Windows-basierter PCs und Server im gesamten Netzwerk sowie deren Prüfung.

Integrated Network Security, Audit und System Management erlauben es Unternehmen:

- Die Netzwerkverwaltung vereinfachen und den manuellen Berichtsaufwand reduzieren
- Netzwerkprüfungsdaten für datenbankbasierte Inventar- und Änderungsberichte können automatisch erhoben werden
- Sicherstellen der Konformität von Softwarelizenzen und unerlaubte Software ausfindig machen
- Vermeiden von Mehraufwand für das Verwalten von separaten Inventarsystemen und Agenten für Endpoints
- Veraltete oder unterdimensionierte Hardware/ Software über die Suchfunktion leicht ausfindig machen

HAUPTMERKMALE UND VORTEILE

- Kosten für Ressourcen und Mehraufwendungen werden durch effizientere IT-Management-Tasks gesenkt
- Automatisiertes Sammeln von Daten des Netzwerkaudits für Datenbank gesteuerte Inventar- und Änderungsreportings
- Die Netzwerksicherheit wird erhöht und das Einhalten von Richtlinien erleichtert
- Vermeiden von Mehraufwand für das Verwalten von separaten Inventarsystemen und Agenten für Endpoints
- Assistentengesteuerte Netzwerk-Aufgaben vereinfachen die Netzwerkverwaltung
- Die Remote-Konfiguration, -Softwareinstallation und -Aktualisierung an Windows-Endpunkten wird automatisiert
- Lokalisieren von nicht autorisierten Anwendungen und Prozessen und automatisches Entfernen aus dem Netzwerk
- Es wird sichergestellt, dass die im Netzwerk installierte Software mit den vorhandenen Lizenzen übereinstimmt
- Hardware/ Software, die nicht die Minimalanforderungen des Netzwerks erfüllt, wird zuverlässig identifiziert
- Manuelle Berichterstattung wird durch vorgefertigte und selbsterstellte Berichtsvorlagen vereinfacht



NETZWERKPRÜFUNG UND SYSTEMWARTUNG

Der BitDefender Management Server verwendet die Skriptsprache Windows Management Instrumentation (WMI) für die Prüfung und Verwaltung von Endgeräten und Servern. Zur Automatisierung der Fernverwaltung sind über 30 vordefinierte WMI-Skriptvorlagen enthalten; beenden Sie Anwendungen und Prozesse, installieren und deinstallieren Sie Software, starten Sie Arbeitsstationen oder fahren Sie sie herunter, aktivieren oder deaktivieren Sie Autoruns und greifen Sie auf USB-Wechselmedien zu.

SYSTEMANFORDERUNGEN

Die BitDefender Centralized Management-Lösung umfasst den Management Server als zentrales Management-Backend für alle BitDefender-Lösungen, die Management Console als Benutzeroberfläche, und den Management Agent für die Verwaltung der Endpunkte.

BitDefender Management Server, Management Console und Update Server

Mindestanforderung Prozessor:

- Intel Pentium 1 GHz (2 GHz empfohlen)

Minimaler RAM-Speicher:

- 512MB (2GB empfohlen)

Minimaler freier Festplattenspeicher:

- 1,5 GB
(2,5 GB empfohlen), 3 GB bei Upgrades

Betriebssystem:

- Windows 2000 Professional SP4
- Windows 2000 Server, SP4
- Windows XP SP2
- Windows Server 2003 SP2
- Windows Vista
- Windows Server 2008
- Windows Server 2008 R2
- Windows Small Business Server (SBS) 2008
- Windows 7

Datenbank:

- Microsoft SQL Server 2005, 2008 oder Microsoft SQL Express Edition (enthalten)

Die Management Console unterstützt die folgenden Browser:

- Internet Explorer 7 (oder höher)
- Internet Explorer 6 (Windows 2000)



Mit den Netzwerk-Tools von BitDefender können von einer zentralen Stelle aus Fernwartung und Fernprüfung am Firmennetzwerk vorgenommen werden

NETZWERKPRÜFUNGEN ERLEICHTERN DAS EINHALTEN VON RICHTLINIEN UND DAS VERFOLGEN VON ÄNDERUNGEN

Viele Unternehmen mögen nicht über die nötigen Ressourcen verfügen, um in spezielle Asset-Management-Anwendungen zu investieren. Sie müssen jedoch aus finanziellen, gesetzlichen und betrieblichen Gründen den Überblick über ihre installierte Software behalten. BitDefender Management Server kann hierbei helfen. Die Lösung kann so konfiguriert werden, dass sie täglich zu einem festgelegten Zeitpunkt Daten zu im Netzwerk vorhandenen Systemen sammelt. Prüfberichte stellen der IT-Abteilung stets aktuelle Informationen über gegenwärtiges und vergangenes Inventar zur Verfügung, die für interne wie externe Prüfungen herangezogen werden können.

Im Netzwerk-Prüfassistenten gibt es vier Standard-Berichtformate:

Snapshot Report Wizard, zur Darstellung der aktuellen Software- und Hardware-Konfigurationen

Assistent für Vergleichsberichte, für den Vergleich installierter Software zu zwei verschiedenen Zeitpunkten

Historical Report Wizard, zur Anzeige von Details zu installierter Software während eines bestimmten Zeitraums

Selbsterstellte Berichte, zur Darstellung von Informationen zu CPU, Festplatten, Betriebssystem, Hauptplatine oder Software

Informationen zu Software und Hardware jedes Windows-PCs und -Servers sind stets abrufbereit und Berichte über vergangene Änderungen an den Systemen machen den Verlauf von Software-Installationen und Deinstallationen im Netzwerk über einen bestimmten Zeitraum nachvollziehbar, sobald ein Ausgangszeitpunkt definiert wurde. Berichte über alle üblichen Parameter können ebenfalls erstellt werden: Art und Geschwindigkeit der CPU; Festplatten, Dateisystem und freier Speicherplatz; Betriebssystem und installierte Service Packs; Hersteller, Seriennummer und Version der Hauptplatine; Größe und Ort der virtuellen Auslagerungsdatei; physischer Speicher; Namen und Versionen installierter Software (z. B. Microsoft Office oder Outlook).

NETZWERKFERNWARTUNG LEICHT GEMACHT

Mit dem BitDefender Management Server schafft eine IT-Abteilung mehr in kürzerer Zeit. Hierbei helfen Netzwerk-Fernwartungsaufgaben, die über 30 Skriptvorlagen für Windows Management Instrumentation (WMI) zur Verfügung stellen. Ein Assistent führt Schritt für Schritt durch die Konfiguration aller nötigen Parameter. Dabei können diese Aufgaben für einzelne Computer oder Gruppen von Computern im Netzwerk sofort oder zu einem festgelegten Zeitpunkt durchgeführt werden.

Die Netzwerk-Aufgaben können per Fernzugriff installierte Anwendungen, laufende Prozesse oder Dienste oder den Windows-Update-Prozess verwalten sowie Zugriff auf lokale USB-Speichermedien steuern. Diese Konfigurationsänderungen können automatisch gleichzeitig auf mehrere Windows-Systeme im Netzwerk angewendet werden, was IT-Mitarbeitern mehr Zeit für wichtigere und weniger triviale Aufgaben gibt.

UMFASSENDE SCHUTZ

BitDefender Centralized Management ist das Hauptelement 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.