IBM Software

Die ideale Lösung für Endpunktmanagement

Erhöhte Transparenz und verbesserte Steuerung für unzählige verteilte Endpunkte

IBM

Die Verwaltung Tausender IT-Endpunkte, einschließlich Workstations, Servern und mobiler Roaminggeräte wie Laptops, Smart Phones und Tablet-Computer, stellt IT-Abteilungen vor eine enorme Herausforderung. Mit herkömmlichen Verwaltungsmethoden kann sogar die Beantwortung einfacher Fragen, etwa „Wie viele mobile Laptops stehen zur Verfügung?“, „Unter welchen Betriebssystemversionen laufen unsere Desktopsysteme?“ oder „Befinden sich unsere Patches auf dem aktuellen Stand?“, mehrere Tage in Anspruch nehmen – wobei die ermittelten Antworten fehlerhaft und unvollständig sind.

Im Rahmen ihrer Bemühungen, redundante und nicht funktionsfähige Management-Tools zu konsolidieren und außer Betrieb zu nehmen, die Sicherheit und Compliance zu optimieren sowie Kosten und IT-Arbeitslast zu reduzieren, ermitteln daher zahlreiche Unternehmen Möglichkeiten, wie sich die komplexen Anforderungen beim Endpunktmanagement durch eine Automatisierung der IT-Vorgänge und Sicherheitsverfahren einhalten lassen.

Unternehmen sind an einer transparenten Endpunktinfrastruktur interessiert, damit sie Einblicke in Anforderungen, Diskrepanzen und zu verbessernde Bereiche erhalten. Eine schnelle und einfache Implementierung neuer Software, Software-Updates und kritischer Sicherheitskorrekturen, eine kontinuierliche und nachweisliche Einhaltung neuer branchenspezifischer und behördlicher Verordnungen sowie der Schutz einer immer größeren und häufig gefährdeten und für Angriffe und Sicherheitsrisiken anfälligen Umgebung – dies sind die Aspekte, auf die Unternehmen Wert legen.

In einer Welt zahlreicher verschiedener, fragmentierter Technologien und Einzellösungen benötigen Unternehmen einen einheitlichen Ansatz zur Unterstützung des Endpunktmanagements über heterogene Geräte und Betriebssysteme hinweg. Worauf es ankommt, sind kurze Implementierungs- und Wertschöpfungszeiten. Ebenso erforderlich ist eine offene Architektur zur Anpassung und Erstellung unternehmensspezifischer Richtlinien ohne aufwendige Programmierung und Scripterstellung. Und wenn die Umgebung Bedrohungen ausgesetzt ist, zählen schließlich flexible und echtzeitorientierte Transparenz in Endpunkte, Schutz, schnelle Korrekturen sowie Berichtsfunktionen.

Eine effektive Lösung für das Endpunktmanagement wird diesen Zielvorgaben gerecht. Über eine zentrale, anwenderfreundliche grafische Benutzerschnittstelle bietet sie unkomplizierte Verwaltungsprozesse, eine optimierte Endpunktsteuerung und zentrale Sichten. Diese Managementfunktionen stehen für eine beliebige Anzahl physischer und virtueller Endpunkte bereit, von Servern über Desktop-PCs, Laptops, Smart Phones und Tablet-Computer bis hin zu speziellen Endgeräten wie POS-Systemen, Bankautomaten oder Self-Service-Kiosksystemen.

Die Verwaltung von Endpunkten ist ausschlaggebend bei der effektiven Bereitstellung sicherer, stabiler IT-Services rund um die Uhr für Kunden, Mitarbeiter, Geschäftspartner, Behörden, Investoren und sonstige Beteiligte. Angesichts der umfassenden Zugänglichkeit moderner IT-Infrastrukturen ändern Unternehmen die Verwaltung von Endpunkten, Prozessen und Daten. Eine Endpunktmanagementlösung kann zu einem grundlegenden Wandel bei den IT-Funktionen führen – von Back-End-Operationen bis zu wichtigen Services, die maßgeblich zum geschäftlichen Erfolg, zur Einhaltung interner Sicherheitsrichtlinien und zu einer effektiven Prozessabwicklung beitragen.

Endpunktmanagement – erste Schritte

In diesem Leitfaden für Käufer werden die Merkmale und Funktionen einer effektiven Endpunktmanagementlösung vorgestellt:

- Erkennung von Endpunkten, Inventarisierung und Nutzungsanalyse
- Patch-Management und Verteilung von Endpunktsoftware
- Sicherheit und Compliance
- Verwaltung mobiler Endgeräte
- Umweltverträgliche IT-Nutzung („Green IT“)
- Architektur des Managementsystems

Dieser Leitfaden informiert über die Vorteile der einzelnen Funktionen und enthält Prüflisten, anhand derer die Käufer beurteilen können, ob die Lösung eines bestimmten Anbieters den Anforderungen all dieser Bereiche wirksam Rechnung trägt. Darüber hinaus sind Attribute und Leistungsmerkmale aufgelistet, die das Produkt eines ausgewählten Anbieters aufweisen sollte, damit sämtliche Anforderungen bezüglich des Endpunktmanagements erfüllt werden können.

Erkennung von Endpunkten, Inventarisierung und Nutzungsanalyse

Die Erfassung von Informationen zu Endpunkten sollte mehr als eine in bestimmten Abständen durchgeführte „Momentaufnahmenermittlung“ von Zahlen umfassen. Vielmehr sollte dynamisch und nahezu in Echtzeit Auskunft über Veränderungen in der Infrastruktur gegeben werden. Eine zeitnahe und standortunabhängige Transparenz und Steuerung machen es dabei möglich, rasch sämtliche IP-adressierbaren Endgeräte im Unternehmen sowie die darauf installierten Anwendungen zu ermitteln.

Die optimale Lösung bietet Drilldown-Analysen zur Ermittlung von Details zu weitverzweigten Infrastrukturen mit unzähligen Endpunkten. So stehen schnell aggregierte Statistiken und Nutzungsinformationen zur Verfügung. Sie sorgt für kontinuierliche transparente Einblicke in alle Endpunkte, so auch in mobile Endgeräte, die außerhalb des Unternehmensnetzwerks für Roaming eingesetzt werden. Ferner besticht die Lösung durch die Möglichkeit zur Verwaltung neu ermittelter Endpunkte sowie durch minimale Auswirkungen auf Netzwerkoperationen. Die genannten Vorgänge sollten hierbei so echtzeitorientiert wie möglich erfolgen.

Erkennung von Endpunkten, Inventarisierung und Nutzungsanalyse

Die Lösung sollte folgende Merkmale aufweisen:	**IBM**	**Andere**
Umfasst eine dezentrale Sucharchitektur sowohl mit als auch ohne Agenten zur Geräteerkennung mit geringen Auswirkungen und kurzer Latenzzeit sowie zur gründlichen Prüfung und zur Berichterstellung	✓	
Ermittelt neben Computerendpunkten rasch alle IP-adressierbaren Geräte einschließlich Netzwerkeinheiten und Peripheriegeräten wie Druckern, Scannern, Routern und Switches	✓	
Erkennt nicht dokumentierte Endpunkte innerhalb der Umgebung und ermittelt verdächtige zerstörerische Geräte	✓	
Ermöglicht echtzeitnahe Berichterstellung zu in Verwendung befindlichen offenen Ports und Services	✓	
Bietet Funktionen für zentrale Erkennung und Bestandsverwaltung	✓	
Unterstützt Ad-hoc-Abfragen an Endpunkte – z. B. Abrufen der Seriennummern aller Computermonitore – und gibt innerhalb von Minuten und mit minimalen Auswirkungen konkrete Ergebnisse aus	✓	
Erreicht Endpunkte unabhängig von ihrem Standort und Netzwerkstatus (verbunden/nicht verbunden) und hält auch für Endpunkte, die nicht durchgehend mit dem Netzwerk verbunden sind, Bestandsdaten auf dem aktuellen Stand	✓	
Stellt präzise, umfassende und detaillierte Bestandsdaten bereit, die sämtliche Hardware-, Konfigurations- und Softwareeigenschaften umfassen	✓	
Unterstützt unmittelbares Durchsuchen und Bearbeiten eines Softwareidentifikationskatalogs, der mehr als 100.000 Kennungen enthält, und wird entsprechend den jeweiligen Änderungen in der Softwarebranche aktualisiert	✓	
Ermöglicht einfache, assistentenbasierte Anpassung des Softwareidentifikationskatalogs zur Überwachung unternehmenseigener und proprietärer Anwendungen	✓	
Stellt ausführliche Informationen zu den an Endpunkten ermittelten Softwareanbietern, Titeln und Anwendungen zur Verfügung	✓	
Umfasst Messung von Softwaredaten zur Aggregierung von Protokollstatistiken und Nutzungsinformationen	✓	
Korreliert Informationen zu Softwarenutzung mit Lizenzinformationen für sofortige, präzise und automatisierte Lizenzanpassungen, sodass nicht konforme Instanzen ermittelt werden, und markiert die Instanzen anschließend, damit sie entfernt werden	✓	
Stellt umfassende Assetdaten für Berichterstellung und Integration in andere Unternehmenssysteme bereit, die eine korrekte, aktuelle Inventarisierung erfordern (z. B. Service-Desk, Asset-Management-System, Inventarisierungswarehouse, CMDBs (Configuration Management Databases))	✓	
Erleichtert Implementierung und Verwendung anhand von Software-Asset-Management-Funktionen für den Einstieg und anhand der Möglichkeit zur Einführung hoch entwickelter Lösungen	✓	
Bietet nahtlose Integration in Sicherheits- und Compliance-Management von Endpunkten	✓	
Unterstützt die Auswertung der Nutzung physischer und auch virtueller Software, einschließlich virtueller Microsoft® App-V-Anwendungen	✓	

Patch-Management und Verteilung von Endpunktsoftware

Immer komplexere Infrastrukturen, die zunehmende Verbreitung von Management-Tools und eine Überlastung der IT-Mitarbeiter können der Verwaltung einer schnell steigenden Anzahl an Endgeräten und Plattformen im Weg stehen. Unternehmen benötigen eine umfassende, einheitliche Managementlösung. Auf diese Weise können sie die Anzahl, Ineffizienz und Ausgaben in Zusammenhang mit unzähligen unterschiedlichen Toolsets verringern und gleichzeitig echtzeitorientierte Transparenz und Steuerung bereitstellen. Mithilfe einer derartigen Lösung lassen sich Prozesse optimieren, indem diese in einem einzelnen Managementvorgang zusammengefasst werden. Parallel dazu werden Kosten und Risiken minimiert und Verwaltungsabläufe effektiv gestaltet.

Eine effektive Lösung ermöglicht eine richtlinienbasierte Installation von Sicherheitsupdates und Softwarepaketen, Überprüfungen innerhalb eines geschlossenen Systems sowie Softwareverteilungen auf mehreren Plattformen über einen zentralen Zugangspunkt. Die Implementierung kritischer Betriebssystem- und Software-Patches erfolgt über dieselbe Managementkonsole, sodass Systemadministratoren problemlos den Soll-Status verwalteter Endpunkte aufrechterhalten können. Hinzu kommen eine Verkürzung der für Inbetriebnahme von Betriebssystemen und für Migration von Benutzerprofilen notwendigen Zeiträume, eine Begrenzung der Risiken in Bezug auf nicht kompatible Konfigurationen, eine Minimierung der Auswirkungen auf Endbenutzer sowie eine Vereinfachung der Implementierung neuer Workstations, Laptops, Server und mobiler Endgeräte.

Patch-Management

Die Lösung sollte folgende Merkmale aufweisen:	**IBM**	**Andere**
Ermöglicht automatisches Patch-Management von einer zentralen Managementkonsole aus	✓	
Verwaltet automatisch Patches für unterschiedliche Betriebssysteme, einschließlich Microsoft Windows®, UNIX®, Linux® und Mac OS®, sowie für Smart Phones und Tablet-Computer über eine zentrale Konsole und einen zentralen Server	✓	
Verwaltet automatisch Patches für Anwendungen von zahlreichen verschiedenen Anbietern, einschließlich Microsoft, Apple®, Adobe®, Mozilla® und Java™	✓	
Minimiert Sicherheits- und Compliancerisiken durch Verkürzung von Patchzyklen von Wochen auf Tage oder Stunden	✓	
Ermöglicht Patch-Management für Endpunkte unabhängig von ihrem Netzwerkstatus (verbunden oder nicht verbunden), einschließlich mit dem Internet verbundener Geräte im Roamingbetrieb	✓	
Bietet auch in Netzwerken mit geringer Bandbreite oder in global verteilten Netzwerken konsistente Funktionen	✓	
Erhöht die Erfolgsquote bei der erstmaligen Durchführung von Programmkorrekturen auf bis zu 95 bis 99 Prozent (zuvor in der Regel 60 bis 75 Prozent) und bestätigt den Erfolg eines Patches	✓	
Minimiert den Arbeitsaufwand in Zusammenhang mit dem Patch-Management durch Bereitstellung vorab getesteter und standardisierter Patchrichtlinien, die dem zuständigen Administrator automatisch zur Verfügung gestellt werden	✓	
Ermöglicht Zusammenfassung von Patches zu einer einzelnen Implementierungstask, wobei bei Bedarf Abhängigkeiten automatisch aufgelöst werden	✓	
Lädt nur die für die einzelnen Endpunkte jeweils relevanten Patches herunter und wendet sie an	✓	
Ermöglicht Systemadministratoren die schnelle Erstellung und Implementierung angepasster Patches	✓	
Erhöht die Transparenz in die Patch-Compliance anhand flexibler, grafischer Echtzeitüberwachung und Berichterstellung	✓	

Patch-Management

Die Lösung sollte folgende Merkmale aufweisen:	**IBM**	**Andere**
Stellt Informationen zum Patchstatus bereit (z. B. Patch erforderlich, Patch anstehend oder wird durchgeführt, Patch erfolgreich installiert, Patchinstallation fehlgeschlagen)	✓	
Stellt Informationen dazu bereit, welche Patches wann und von wem implementiert wurden	✓	
Gleicht automatisch die Endpunktcompliance mit festgelegten Richtlinien, z. B. verbindlichen Patch-Levels, ab	✓	
Erkennt und behebt Probleme an Stellen, an denen ein zuvor installiertes Patch rückgängig gemacht oder überschrieben wurde; ermöglicht automatische erneute Anwendung nicht installierter Patches	✓	
Ermöglicht Bereitstellung von Patches als „Angebote“ für Benutzer mit oder ohne obligatorische Implementierungszeitpunkte zur Minimierung von Unterbrechungen	✓	
Ermöglicht Zusammenfassung und schnelle Installation von Patches während definierter Änderungszeitfenster	✓	
Ermöglicht optionales Unterdrücken und verzögertes/terminiertes erneutes Aufrufen von Patchdialogfenstern	✓	

Unternehmen sind heutzutage dezentraler strukturiert als je zuvor. Das bedeutet, IT-Management-Tasks wie die Verteilung und Verwaltung von Softwareendpunkten wird extrem komplex.

Diese Unternehmen benötigen leistungsfähige Funktionen zur schnellen und zuverlässigen Bereitstellung und Verwaltung von an sämtlichen Endpunkten ausgeführten geschäftskritischen Anwendungen.

Verteilung von Endpunktsoftware

Die Lösung sollte folgende Merkmale aufweisen:	**IBM**	**Andere**
Ermöglicht Verwaltung der Softwareverteilungen auf mehreren Plattformen über einen zentralen, einheitlichen Steuerungspunkt	✓	
Unterstützt die richtlinien- und computergruppenbasierte Installation neuer und aktualisierter Softwarepakete über verteilte Umgebungen hinweg	✓	
Bietet Überprüfung von Softwareinstallationen/-deinstallationen innerhalb eines geschlossenen Systems	✓	
Unterstützt Self-Service-Funktionen für Benutzer für Bereitstellung und Entfernung berechtigter Anwendungen und Softwarepakete	✓	
Unterstützt lokale Vorabzwischenspeicherung von Softwarepaketen zur Steigerung der Zuverlässigkeit von Installationen	✓	
Vermeidet Duplizierung von Dateien zur Softwareverteilung	✓	
Unterstützt Softwareverteilungsrichtlinien zur Benutzerüberwachung	✓	
Stellt einfache, leistungsfähige Anpassungsfunktionen für präzise Steuerung und Implementierung von Softwarepaketen bereit	✓	

Verteilung von Endpunktsoftware

Die Lösung sollte folgende Merkmale aufweisen:	**IBM**	**Andere**
Minimiert die Auswirkungen auf das Netzwerk anhand richtlinienbasierter statischer und dynamischer Bandbreitenregulierung über sämtliche Betriebssystemplattformen hinweg, einschließlich der Möglichkeit zur Regulierung der tatsächlich verfügbaren Bandbreite für Netzwerkverbindungen	✓	
Verwaltet zur effizienten Ausführung unterschiedlicher Paketkonfigurationen Konfigurationsdateien wie MST- (Microsoft Software Transform) und MSP-Dateien (Microsoft Software Patch) getrennt von zentralen Softwarekomponenten	✓	
Ist mit gängigen Softwareverteilungstools und Paketformaten kompatibel	✓	
Unterstützt die Implementierung von Betriebssystemen nach dem Bare-Metal-Prinzip für neue Workstations, Laptops und Server im gesamten Netzwerk und unterstützt Betriebssystemmigrationen und -aktualisierungen für vorhandene Endpunkte	✓	
Nutzt die zentrale Endpunktmanagementinfrastruktur für Betriebssystemmigrationen, sodass die Kosten für die Verwaltung einer eigenständigen für die Betriebssystemimplementierung eingerichteten Infrastruktur wegfallen	✓	
Verkürzt Implementierungs- und Migrationszeiten anhand voll automatisierter Vorgänge wie Wake-up-Unterstützung und Terminierung von Implementierungen	✓	
Implementiert hardwareunabhängige Images auf Maschinen verschiedener Hardwareanbieter und fügt bei Bedarf geeignete Gerätetreiber hinzu	✓	
Ermöglicht Inplace-Migration von Benutzerprofilen und -daten	✓	
Implementiert Betriebssysteme im Kontext von Sicherheitsreferenzen und Anforderungen bezüglich der Bereitstellung von Konfigurationen und führt abschließende Programmkorrekturen durch, damit Systeme unmittelbar verwendbar sind	✓	
Bietet plattformübergreifende Remotesteuerung und Fehlerbehebung	✓	
Stellt Administratoren echtzeitorientierte Endpunktdaten anhand von Ferndiagnosefunktionen bereit, mit denen sich Anrufe beim Help-Desk sowie die Fehlerbeseitigung einfacher und besser abwickeln lassen	✓	
Passt spezifische Aktionen an die entsprechenden exakten Endpunktkonfigurations- oder Benutzertypen an	✓	
Bietet ferne Erkennung und Analyse von an Endpunkten installierten Anwendungen	✓	
Ermöglicht Administratoren die Erstellung von rollenbasiertem Zugriff zur Unterstützung verschiedener benutzerspezifischer Aufgabenbereiche und zur Erfüllung unterschiedlicher Anforderungen von Geschäftsbereichen	✓	
Vereinfacht und operationalisiert Sicherheit durch Einbindung von Sicherheitsverfahren und Complianceinitiativen in den IT-Betrieb	✓	

Sicherheit und Compliance

Die groß angelegten Umgebungen der heutigen Zeit sind häufig nicht klar strukturiert, sodass Endpunkte eine äußerst hohe Anfälligkeit gegenüber Angriffen aufweisen. Doch dies ist noch nicht alles: Die Zeiträume zwischen den Angriffen und auch zwischen dem Auftreten neuer Sicherheitslücken werden immer kürzer – und zwar so kurz, dass die meisten aktuellen Tools nicht mehr Schritt halten können. Kann ein Unternehmen Schwachstellen schnell genug erkennen und beheben, damit die Server, PCs und sonstigen Endpunkte vor Attacken geschützt sind?

Während die Mehrheit der Unternehmen den Fokus auf den Schutz der Benutzer gegen die Bedrohung eingehender Malware und Viren setzt, müssen sich immer mehr von ihnen auch Gedanken um die Absicherung mobiler Benutzer und damit um den Schutz vertraulicher Daten vor internen Bedrohungen machen. Nicht alle Datenschutzverstöße entspringen bösen Absichten: Benutzer kopieren routinemäßig sensible Informationen auf Geräte wie USB-Laufwerke, Speicherkarten, cloudbasierte Synchronisierungsservices und mobile Endgeräte. Zahlreiche Mitarbeiter arbeiten mittlerweile von Laptops aus, die regelmäßig inklusive darauf befindlicher schutzwürdiger Daten aus dem Büro transportiert werden.

In Anbetracht dieser Herausforderungen benötigen Unternehmen eine Lösung zur Vermeidung von Datenverlusten, die sich ohne großen Aufwand als Bestandteil der auf die Endpunkte abgestimmten vorhandenen Sicherheitsinfrastruktur implementieren lässt. Es sollte sich hierbei um ein einheitliches Tool handeln, mit dem nicht nur Sicherheitsbedrohungen und die damit verbundenen Risiken behoben, sondern auch die Kosten, die Komplexität und die Arbeitsbelastung der Mitarbeiter kontrolliert und die Compliancevorgaben eingehalten werden können. Eine derartige Lösung bietet die Möglichkeit, sowohl Endpunkte zu schützen als auch die Einhaltung interner Sicherheitsrichtlinien zu gewährleisten.

Sicherheit von Endpunkten

Die Lösung sollte folgende Merkmale aufweisen:	**IBM**	**Andere**
Verwaltet die Konfiguration physischer und virtueller Endpunkte unabhängig von Standort, Betriebssystem, installierten Anwendungen oder Verbindung (einschließlich kabelgebundener Computer oder zeitweise verbundener mobiler Endgeräte)	✓	
Führt Korrekturen an Endpunkten entsprechend Compliancereferenzen durch und setzt anschließend unabhängig von der Netzwerkverbindung kontinuierlich Konfigurationsrichtlinien durch	✓	
Bietet präzise, echtzeitorientierte Transparenz in sowie kontinuierliche Durchsetzung von Sicherheitskonfigurationen und -patches über eine zentrale Managementkonsole	✓	
Ermöglicht echtzeitorientierte Reaktionen auf Zero-Day-Attacken anhand von Ad-hoc-Korrekturen innerhalb eines geschlossenen Systems, sodass Administratoren schnell und einfach angepasste Korrekturrichtlinien erstellen und diese innerhalb von Stunden im gesamten Unternehmen implementieren können, wobei es nicht darauf ankommt, ob Endpunkte mit dem Netzwerk verbunden sind oder nicht	✓	
Enthält ein umfassendes Spektrum technischer und auf bewährten Verfahren basierter Steuerelemente, die durch die Erkennung und Durchsetzung von Sicherheitskonfigurationen zur Einhaltung von Sicherheitsbestimmungen beitragen	✓	
Unterstützt das Security Content Automation Protocol (SCAP)	✓	
Verwendet vordefinierte, sofort einsatzfähige Richtliniendefinitionen, die auf dem OVAL-Standard (Open Vulnerability and Assessment Language) basieren und die Bewertung verwalteter Endpunkte im Hinblick auf bekannte Sicherheitslücken ermöglichen	✓	
Reagiert auf vom SANS Institute veröffentlichte Alerts zu Schwachstellen und Sicherheitsrisiken	✓	
Ordnet Sicherheitslücken Branchenstandards zu und stellt so CVE- (Common Vulnerabilities and Exposures) und CVSS-Referenzen und -Links (Common Vulnerability Scoring System) zur National Vulnerability Database (NVD) bereit	✓	

Sicherheit von Endpunkten

Die Lösung sollte folgende Merkmale aufweisen:	**IBM**	**Andere**
Stellt sofort einsatzfähige Prüflisten mit über 5.000 standardmäßigen Konfigurationseinstellungen bereit, die Branchenstandards für Windows, UNIX und Linux zugeordnet sind	✓	
Automatisiert und vereinfacht die Erstellung von auf technische Steuerelemente zugeschnittenen Compliance-berichten für Sarbanes-Oxley, HIPAA, UK Financial Services Act und sonstige Vorschriften	✓	
Bietet sofort einsatzfähige Best Practices gemäß den US-amerikanischen FDCC- (Federal Desktop Core Configuration) und USGCB-Bestimmungen (United States Government Configuration Baseline)	✓	
Bietet sofort einsatzfähige Best Practices gemäß den Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs)	✓	
Ermittelt und beseitigt bekannte Sicherheitslücken anhand automatisierter Richtliniendurchsetzung oder manueller Implementierung	✓	
Ermöglicht reibungslose Integration in zusammengehörige Technologien wie Help-Desk-Systeme, Asset-Management-Systeme, CMDBs und SIEM-Systeme (Security Information and Event Management, Sicherheitsinformations- und Ereignismanagement)	✓	
Gibt Alarmnachrichten zur schnellen Ermittlung zerstörerischer oder fehlerhaft konfigurierter Endpunkte aus und ergreift Maßnahmen zur Korrektur oder Entfernung	✓	
Verlagert automatisch nicht den Vorschriften entsprechende Endpunkte in isolierte Netzwerkbereiche und verwaltet sie während des gesamten Korrekturvorgangs	✓	
Stellt Assistenten zur Definition angepasster Richtlinien sowie zur zugehörigen Berichterstellung und Durchsetzung bereit	✓	
Ist vom National Institute of Standards and Technology (NIST) sowohl für Bewertung als auch Fehlerbehebung zertifiziert	✓	
Ermöglicht schnelle Anpassung mit minimalen Codezeilen anhand einer benutzerfreundlichen Anwendungs-programmierschnittstelle, die durch Verwendung der gleichen Sprache Unterstützung für verschiedene Plattformen bietet	✓	
Stellt einen zentralen Hub für sämtliche Tools zur Automatisierung des Systemmanagements bereit, sodass Administratoren die ihnen vertrauten Tools verwenden können (d. h. Erstellung von Shell-Scripts in UNIX, Verarbeitung von Stapeldateien in Windows, Einsatz von Scripts in Apple usw.)	✓	
Unterstützt Qualifikationsstufen von Administratoren von Einsteigern (assistentenbasierte Scripterstellung ohne erforderliche Kenntnis der Toolsprache) bis zu Experten (extrem flexibles Anpassungs-Know-how)	✓	
Bietet nahtlose Integration in das Betriebsmanagement von Endpunkten über den gesamten Lebenszyklus hinweg	✓	

Es ist üblich, dass ein Unternehmen Complianceinformationen zu einer bestimmten Plattform oder einem bestimmten Endpunkttyp, zu einem Unternehmensbereich oder einer geografischen Region oder auch zu einer spezifischen behördlichen oder Governance-vorgabe für sämtliche Endpunkte anfordert. Die Bereitstellung der gewünschten Angaben setzt umfassende Berichtsfunktionen voraus, mit denen auf Basis von Warehouseanalysen und Assetdaten schnell und zeitgerecht benutzerfreundliche Berichte und Sichten erstellt werden.

Berichte und Analysen

Die Lösung sollte folgende Merkmale aufweisen:	**IBM**	**Andere**
Erfasst und archiviert Ergebnisse automatisierter Sicherheitsprüfungen zur einfachen Ermittlung von Konfigurationsproblemen und zur Dokumentation von Compliancestufen in Zusammenhang mit der IT-Sicherheit	✓	
Stellt Analysefunktionen bereit, die die Durchsetzung der unternehmensinternen technischen und konfigurationsspezifischen Richtlinien unterstützen, indem der Fortschritt überwacht, dokumentiert und protokolliert und der Erfolg von Sicherheitsinitiativen bestimmt wird	✓	
Stellt Langzeitberichte zur Bestimmung des Fortschritts im Hinblick auf die Einhaltung von Vorschriften bereit	✓	
Stellt aussagekräftige Echtzeit- sowie Langzeitberichte zu Zustand und Sicherheit von Endpunkten bereit, die im Rahmen der Fehlerbehebung bei nicht konformen Endpunkten und der Bestätigung durchgeführter Korrekturen Verwendung finden	✓	
Stellt Dashboards zur Übersicht und Rollups für Führungskräfte bereit, anhand derer die Einhaltung von Sicherheitsbestimmungen und die Problemstellungen im bisherigen langfristigen Verlauf dargestellt werden, und bietet die Möglichkeit zum detaillierten Abfragen von Informationen	✓	
Stellt fundierte und durch Korrekturverfahren (z. B. spezifische Patches) konsolidierte Berichte anstatt einer langen Liste sich überschneidender und oftmals redundanter Schwachstellen bereit	✓	
Ermittelt und verwaltet Ausnahmen und Abweichungen von Richtlinien und erstellt zugehörige Berichte	✓	
Stellt umfassende Berichte zur Verwaltung von IT-Richtlinienprüfungen, einschließlich Richtlinienkonformität und Verlauf, sowiecomputer- und computergruppenspezifische Berichte und Abweichungsberichte bereit	✓	
Ermöglicht die Erstellung flexibler, bedarfsgerechter Ad-hoc-Abfragen und -Berichte	✓	
Bietet flexible Berichte, einschließlich Berichtsfilter (z. B. Langzeitcompliance, Computermetadaten, Prüflistenmetadaten usw.), Verwaltung von Berichtsspalten, Ist-Werte vs. Soll-Werte, Berichtsexporte, gespeicherter Berichte u. v. m.	✓	
Ermöglicht Benutzern die einfache Erstellung angepasster Prüflisten in Minutenschnelle durch Kombination im Produktumfang enthaltener Best Practices mit angepassten Prüfungen	✓	
Stellt anhand hoch entwickelter Berichterstellung Trends und Analysen von Konfigurationscompliance und Sicherheitsänderungen im bisherigen langfristigen Verlauf dar	✓	
Basiert Analysen auf Infrastruktursichten, die sich auf vielfältige Weise definieren lassen, von einem einzelnen Gerät über Gerätegruppen bis hin zur gesamten Infrastruktur	✓	

Berichte und Analysen

Die Lösung sollte folgende Merkmale aufweisen:	**IBM**	**Andere**
Umfasst ein separates Data-Warehouse zur Sicherheitsanalyse für die Speicherung von Langzeitcompliancedaten	✓	
Bietet eine ganzheitliche Sicht der Richtlinienkonformität und der Schwachstellen (Zusammenfassung in einem einzelnen Bericht oder einer zentralen Onlinesicht)	✓	
Unterstützt Prüfanforderungen durch Bereitstellung von Sichten zu Langzeitstatus vs. aktuellem Status	✓	
Unterstützt einen Berichterstellungsserver für Prüfer mit Lesezugriff und Zugriff auf ausgewählte Informationen	✓	
Schränkt anhand von Benutzerberechtigungen und -rollen Zugriff auf Endpunkte und Berichte ein	✓	
Verwendet für das Endpunktmanagement dieselbe Konsole, Architektur und denselben Agenten wie IT-Operationen	✓	

Vor Kurzem vorgefallene Datenschutzverstöße machen deutlich, wie dringend notwendig es ist, vertrauliche Daten gegen unbeabsichtigten oder aber vorsätzlichen Missbrauch und Verlust zu schützen. Angesichts dieser Herausforderungen benötigen Unternehmen eine leistungsstarke Lösung zum Schutz von Endpunkten und zur Vermeidung von Datenverlusten, die sich mühelos in die vorhandene Endpunktmanagementinfrastruktur integrieren lässt. So können die Hindernisse bei der Implementierung wirksamer Datenschutzmechanismen effektiv beseitigt werden. Eine einheitliche auf die Endpunkte zugeschnittene Sicherheitsinfrastruktur trägt zu einer Vereinfachung komplexer Strukturen und zu einer Reduzierung des zeitlichen und finanziellen Verwaltungsaufwands bei.

Schutz von Endpunkten

Die Lösung sollte folgende Merkmale aufweisen:	**IBM**	**Andere**
Bietet ein konsolidiertes, einheitliches Konzept zur Bereitstellung und Verwaltung von Virenschutz-, Spywareschutz-, Firewall- und Verschlüsselungsservices für führende Produkte verschiedener Anbieter, z. B. Symantec®, McAfee®, Trend Micro®, Microsoft und Sophos®	✓	
Überwacht den Systemstatus, damit gewährleistet ist, dass für den Schutz von Endpunkten eingesetzte Clients kontinuierlich ausgeführt und dass Virensignaturen aktualisiert werden	✓	
Erleichtert die Migration von Endpunkten von einer Sicherheitslösung auf eine andere anhand von Software-deinstallationen und -neuinstallationen per Mausklick	✓	
Nutzt Prüfungen innerhalb eines geschlossenen Systems, damit sichergestellt ist, dass Sicherheitseinstellungen angewendet und durchgesetzt wurden und dass Aktualisierungen und sonstige Änderungen abgeschlossen sind; bietet internetfähige Prüfung für Endpunkte, die nicht mit dem Netzwerk verbunden sind	✓	
Verhindert den Benutzerzugriff (entweder in Form eigener Aktionen oder aufgrund verdeckter, automatisierter Abläufe, die von auf dem Computer befindlicher Malware ausgeführt werden) auf zerstörerische Websites	✓	

Schutz von Endpunkten

Die Lösung sollte folgende Merkmale aufweisen:	**IBM**	**Andere**
Verwendet cloudbasierte Webreputationstechnologie, mit der täglich dynamisch Millionen einzelner Webseiten klassifiziert werden, damit Schutz vor webbasierter Malware einschließlich Web 2.0-Bedrohungen und vor auf Datendiebstahl ausgelegter Malware besteht	✓	
Schützt Endpunkte gegen Viren, Trojanische Pferde, Computerwürmer, Spyware, Rootkits, neue Malwarevarianten und zerstörerische Websites	✓	
Ermittelt und entfernt vollständig erkannte Spyware, einschließlich verdeckter Rootkits und restlicher Komponenten	✓	
Stellt eine voll integrierte Virenschutz- und Firewalllösung mit zentraler Konsole und Infrastruktur für das Endpunktmanagement bereit und vermeidet somit die Kosten und Komplexität, die die Verwaltung einer eigenständigen Infrastruktur zur Implementierung von Virenschutz- und Firewallprodukten mit sich bringt	✓	
Stellt integrierte Funktionen zur Vermeidung von Datenverlusten über eine zentrale Konsolen- und Agenteninfrastruktur bereit	✓	
Umfasst Funktionen zur Vermeidung von Datenverlusten für die Sicherung von Daten auf allen Geräten, für die Durchsetzung von Sicherheitsrichtlinien, sodass Benutzer für ihre Jobs auf vertrauliche Daten zugreifen, diese jedoch nicht unsachgemäß verwenden oder verlieren können, und für die vereinfachte Einhaltung von Datenschutzverordnungen	✓	
Schützt vor unsachgemäßer Nutzung von Daten anhand von Schlüsselwörtern, regulären Ausdrücken und konfigurierbaren Regeln, mit denen spezifische Formatierungen oder sogar Codes (z. B. Java-Code) ermittelt und entsprechende Reaktionen durchgeführt werden können	✓	
Umfasst vordefinierte Vorlagen, die für die Ermittlung und Steuerung von Daten je nach bestimmten Regelungen, z. B. GLBA, HIPAA, PCI-DSS, SB-1386, PCI und US PII, konzipiert sind	✓	
Bietet mehrkanalige Überwachung und Durchsetzung, sodass die Genehmigung verweigert oder erteilt werden kann, zu welchem Zeitpunkt Daten an verschiedene Vertriebskanäle (u. a. E-Mail, Zwischenablage, FTP, HTTP, HTTPS, SMB, IM, Webmail) kopiert und gesendet werden dürfen; bietet Überwachung physischer Kanäle, z. B. Datenbrenner, Verschlüsselung, Peer-to-Peer-Anwendungen, austauschbare Speichergeräte usw.	✓	
Ermöglicht konfigurierbare Antwortaktionen von der Blockierung von Aktionen und Ausgabe von Warnungen an den Endbenutzer bis zur automatisierten Benachrichtigung von Administratoren	✓	
Überwacht und steuert physische Ports an Endpunkten und bietet die Möglichkeit zur Aktivierung oder Deaktivierung dieser Ports entsprechend dem Gerätetyp und den kontextsensitiven Sucheinschränkungen	✓	
Umfasst differenzierte Gerätesteuerung zur Beschränkung des Zugriffs durch austauschbare USB-Speichereinheiten nach Anbieter, Modell und Seriennummer des jeweiligen Geräts	✓	

Verwaltung mobiler Endgeräte

Millionen von Menschen besitzen leistungsstarke Smart Phones und Tablet-Computer und auch der berufliche Einsatz dieser Geräte nimmt rapide zu. Diese mobilen Endpunkte verhelfen Mitarbeiter zu noch nie da gewesener Flexibilität und eröffnen dadurch wiederum eine neue Dimension der Produktivität. Doch im Gegensatz zu herkömmlichen Endpunkten, die IT-Abteilungen seit Jahren verwalten, zeichnen sich mobile Endgeräteplattformen durch spezifische Managementanforderungen aus, die von bisherigen entsprechenden Voraussetzungen abweichen. Da IT-Abteilungen diese Geräte nicht mit den vorhandenen Technologien und Infrastrukturen verwalten können, müssen sie oftmals mühsam nach Mitteln und Wegen zur effizienten und sicheren Verwendung mobiler Endgeräte am Arbeitsplatz suchen.

Anstatt eine separate Managementinfrastruktur und zugehörige Prozesse ausschließlich für mobile Endgeräte zu implementieren, empfiehlt sich der Einsatz einer für einheitliches Endpunktmanagement konzipierten Einzellösung. Diese bietet hochwertige Anwendungs- und Sicherheitsverwaltung für alle Typen von Endpunkten und kommt den spezifischen Anforderungen mobiler Endgeräte nach. Die ideale einheitliche Managementplattform überzeugt durch Schutz und Verwaltung von herkömmlichen Endpunkten sowie von Smart Phones und Tablet-Computern.

Verwaltung mobiler Endgeräte

Die Lösung sollte folgende Merkmale aufweisen:	**IBM**	**Andere**
Nutzt eine zentrale Infrastruktur zur Bereitstellung einheitlicher Verwaltung und Sicherheit für sämtliche Typen von Unternehmensendpunkten, einschließlich Smart Phones, Tablet-Computern, Desktopsystemen, Laptops und Servern	✓	
Ermöglicht umfassende Konfiguration und Durchsetzung von Geräteeinstellungen, einschließlich Kennwort- und Verschlüsselungsrichtlinien, E-Mail, VPN, LDAP, Wi-Fi, Kamera und sonstiger Einstellungen	✓	
Schützt Unternehmensdaten durch Durchführung vollständiger oder teilweiser Bereinigungen, wenn Geräte verloren gehen, gestohlen oder stillgelegt werden	✓	
Bietet flexibles Sichern und Verwalten von Geräten durch eine Kombination aus E-Mail- und agentenbasiertem Management unter Berücksichtigung des nativen Geräteaspekts	✓	
Unterstütz die kontinuierliche Einhaltung von Vorschriften durch die Ermittlung nicht konformer Geräte und durch die automatische Durchführung von Korrekturmaßnahmen, z. B. Verweigern des E-Mail-Zugriffs, Löschen von Profilen oder Entfernen des VPN-Zugriffs (virtuelles privates Netzwerk)	✓	

Verwaltung mobiler Endgeräte		
Die Lösung sollte folgende Merkmale aufweisen:	**IBM**	**Andere**
Bietet vollständiges Anwendungsmanagement durch Erstellung von Berichten zu installierten Anwendungen, durch Ermittlung von mit Sperrvermerken versehenen Anwendungen und durch die Möglichkeit zur Verteilung von Anwendungen über einen entsprechenden unternehmensinternen Vertrieb	✓	
Bietet auf Großunternehmen zugeschnittene Anwendungsprogrammierschnittstellen für die Integration mobiler Endgeräte und herkömmlicher Endpunktdaten in andere Unternehmenssysteme, z. B. Service-Desks und CMDBs	✓	
Ermöglicht die Verwaltung über das Unternehmensnetzwerk, auf OTA-Basis (Over the Air, per Funkschnittstelle) oder über das Internet	✓	
Stellt Self-Service-Funktionen für Benutzer bereit	✓	
Erfasst und speichert detaillierte Gerätedaten, einschließlich Bestandsdaten wie Gerätemodell und Seriennummer, Nutzungsdaten wie letzte Verbindungszeit, Hardwareinformationen wie Firmware- und Speicherdaten sowie Betriebssystemversion, Positionsdaten, Netzwerkdaten und Daten zu installierten Anwendungen und Zertifikaten	✓	
Erkennt Rootgeräte oder auch Geräte ohne Nutzungsbeschränkungen	✓	
Ermöglicht Administratoren das Verteilen, Installieren, Widerrufen, Entfernen und Zurückgeben von Status von Zertifikaten anderer Anbieter	✓	

Umweltverträgliche IT-Nutzung („Green IT“)

Neben integrierten Stromsparfunktionen verfügen die meisten Endpunkte über Steuerelemente, mit denen zahlreiche Endbenutzer vertraut sind. Doch die Erzielung messbarer Ergebnisse bei der Energieersparnis hängt in den seltensten Fällen nur von den Endbenutzern ab. Größere Wirkung zeigt ein zentrales Management. Ideale Lösungen ermöglichen eine Senkung des Strombedarfs und eine Vermeidung von Unterbrechungen, wobei die erforderlichen Steuerelemente über eine zentrale, einheitliche Konsole bereitstehen.

Anhand einer derartigen Lösung können IT-Abteilungen sowohl infrastrukturweit gültige Einsparungsrichtlinien einführen als auch bei Bedarf differenziert Energiemanagementrichtlinien auf einen einzelnen Computer anwenden. Durch die Kombination aus Stromversorgungsmanagement und remote ausführbaren Wake-up-Funktionen lassen sich die bisweilen widersprüchlichen Anforderungen der Verwaltung (in der Regel vorzugsweise häufiges Ausschalten von Systemen für maximale Energieeinsparung) und der IT (durchgehender Systembetrieb auch außerhalb der Arbeitszeit zur einfachen Durchführung von Patches und Aktualisierungen in diesen Zeiträumen) in Einklang bringen.

Umweltverträgliche IT-Nutzung („Green IT“)

Die Lösung sollte folgende Merkmale aufweisen:	**IBM**	**Andere**
Ermöglicht die Verwaltung von Energieeinstellungen über einen zentralen Server und eine zentrale Konsole für alle Endpunkte, an denen Windows- und Mac-Betriebssysteme ausgeführt werden	✓	
Stellt sofort nutzbare Funktionen zur Beseitigung gängiger Probleme beim Energiemanagement, z. B. PC Insomnia (PC wird nicht in Standby-Modus versetzt) und PC Narcolepsy (PC kehrt nicht aus Standby-Modus zurück), bereit	✓	
Bietet die zur bedarfsorientierten Anwendung von Richtlinien auf einen einzelnen Computer notwendige Differenziertheit	✓	
Ermöglicht Administratoren die Zuordnung verschiedener Energieverbrauchsmesswerte zu Systemen auf Basis erkannter Merkmale	✓	
Stellt differenzierte Steuerelemente für Hibernation-, Standby- und für Optionen zum Speichern von Daten vor dem Herunterfahren bereit	✓	
Bietet Endbenutzern ein Anmeldungsmodell, bei dem sie ihre Energieprofile aus verschiedenen vom Administrator definierten Stromkonfigurationsoptionen auswählen können	✓	
Bindet Endbenutzer über eine clientseitige Dashboardsicht in ihren individuellen Stromverbrauch und in die entsprechenden Einsparungen in Energiesparinitiativen ein	✓	
Ermöglicht die Erstellung von „Was-wäre-wenn“-Energieverbrauchsszenarios und stellt Umweltverträglichkeitsberichte bereit, damit die Beteiligung an Energiesparinitiativen gefördert wird	✓	
Ermittelt fehlerhaft konfigurierte Energieprofile und korrigiert diese automatisch	✓	
Terminiert Ruhe- und Hibernationsmodi von Computern, sodass eine begrenzte Anzahl an PCs ausreichend funktionsfähig ist und somit Wake-up-Nachrichten empfangen oder an andere Computer, die sich in noch inaktiveren Modi befinden, übermitteln kann	✓	
Sichert Benutzerdaten, indem Dokumente automatisch vor dem Herunterfahren oder vor dem Einleiten eines Ruhe-/Standby-Modus gespeichert werden	✓	
Terminiert Wake on LAN (WoL), damit Endpunkte vor Beginn eines Arbeitstags aktiviert oder planmäßige Wartungsarbeiten, einschließlich Supporttätigkeiten für Aktivierung ferner Benutzer, durchgeführt werden können	✓	
Bietet Erstellung grafischer Berichte zu Energieverbrauch und -einsparungen insgesamt und bietet die Möglichkeit zum Export von Berichtsdaten an Microsoft Excel für weitere Auswertung	✓	

Architektur des Managementsystems

In den meisten verteilten Umgebungen steigen die Gesamtanzahl an Endpunkten sowie die Anzahl der verschiedenen Endpunkttypen, darüber hinaus werden Netzwerke zunehmend komplex. Endpunkttransparenz und -steuerung sind häufig unzureichend und Serviceziele können nicht leicht eingehalten werden. Folglich ist es schwierig, einen präzisen und umfassenden zentralen verlässlichen Datenbestand für die Umgebung zu erstellen und anschließend zur Verwaltung dieser unzähligen Endpunkte darauf zurückzugreifen. Die Lösung für dieses Problem besteht in Technologien zur unternehmensweiten Konsolidierung und Vereinfachung zentraler Management-Services.

Indem an jedem Endpunkt ein intelligenter Agent platziert wird, können Funktionen wie kontinuierliche automatische Bewertung und Richtliniendurchsetzung durchgeführt werden. Anders als bei herkömmlichen Client/Server-Architekturen, die Anweisungen von einem zentralen Steuerpunkt empfangen, werden von einem intelligenten Agenten Aktionen autonom eingeleitet. Dabei werden Nachrichten vorgeschaltet an den zentralen Verwaltungsserver gesendet und Patches, Konfigurationen und sonstige Informationen bedarfsorientiert zur Einhaltung einer relevanten Richtlinie auf den betreffenden Endpunkt angewendet.

Bei diesem Konzept einer zentralen Infrastruktur erfolgt die Entscheidungsfindung an den Endpunkten. Die Folgen sind verkürzte Aktualisierungszyklen, erhöhte Erfolgsquoten bei der Bereitstellung, eine gesteigerte Benutzerproduktivität sowie geringere Anforderungen an die IT- und Help-Desk-Mitarbeiter.

Architektur des Managementsystems

Die Lösung sollte folgende Merkmale aufweisen:	**IBM**	**Andere**
Konsolidiert IT-Operationen und IT-Sicherheitsfunktionen zu einer zentralen Sicht, einem zentralen Bereitstellungsmodell und einem zentralen Softwareangebot	✓	
Bewertet und korrigiert Probleme anhand eines zentralen, vielseitigen, intelligenten Agenten	✓	
Bietet kontinuierliche automatische Bewertung von Endpunkten sowie echtzeitorientierte Richtliniendurchsetzung	✓	
Beansprucht in der Regel weniger als zehn MB des Endpunktspeichers	✓	
Erfordert durchschnittlich weniger als zwei Prozent der CPU-Auslastung und stellt somit sicher, dass die Leistung an den Endpunkten nicht beeinträchtigt ist	✓	
Ermöglicht automatische Bewertung und Durchsetzung von Richtlinien unabhängig davon, ob der Endpunkt mit dem Unternehmensnetzwerk verbunden ist oder nicht	✓	

Architektur des Managementsystems

Die Lösung sollte folgende Merkmale aufweisen:	**IBM**	**Andere**
Stellt lokale Ressourcen sowie auf Richtlinien basierende, dynamische Steuerelemente zur Regulierung der Belegung der Netzwerkbandbreite bereit	✓	
Verwendet eine veröffentlichte Befehlssprache, sodass Kunden, Geschäftspartner und Entwickler angepasste Richtlinien und Services für verwaltete Endpunkte erstellen können	✓	
Bietet echtzeitorientierte Transparenz in alle Endpunkte, einschließlich Desktopsystemen, Laptops, Servern, mobiler Endgeräte, POS-Systemen, Bankautomaten und Self-Service-Kiosksystemen	✓	
Stellt eine benutzerfreundliche grafische Benutzerschnittstelle sowie eine erweiterte Befehlszeilen- und eine Anwendungsprogrammierschnittstelle bereit	✓	
Unterstützt bis zu 250.000 Endpunkte von einem zentralen Management-Server aus	✓	
Verwaltet mobile Endpunkte unabhängig von ihrem Netzwerkstatus (verbunden/nicht verbunden)	✓	
Verwaltet heterogene Plattformen (Microsoft Windows-, UNIX-, Linux- und Mac-Betriebssysteme, die auf physischen oder virtuellen Maschinen ausgeführt werden) sowie Smart Phones und Tablet-Computer	✓	
Nutzt dieselbe Infrastruktur und dieselben Ressourcen zur Bereitstellung integrierter Remotesteuerung für vereinfachte und optimierte Abwicklung von Anrufen beim Help-Desk sowie von Fehlerbeseitigungsmaßnahmen	✓	
Nutzt vorhandene Server oder Workstations zur Bereitstellung von Inhalten wie Softwareinstallationsprogrammen und Patches, sodass weniger Management-Server erforderlich sind, Pakete konstant schnell bereitgestellt werden und der Datenaustausch im Netzwerk minimiert wird	✓	
Ermöglicht die Konfiguration eines beliebigen Agenten als Relay-Agent – oder Zwischenspeicheragent – zwischen anderen Agenten und der zentralen Managementkonsole, wobei sich optional Richtlinien und Inhalte speichern und dadurch Netzwerklasten reduzieren lassen	✓	
Stellt Softwarelösungen anderer Anbieter bereit, die auf Basis der EAL 3 Common Criteria zertifiziert sind	✓	
Steuert den Zugriff anhand von Benutzerberechtigungen und -rollen zur Einschränkung des Zugriffs auf Endpunkte, Berichte und auf die Managementkonsole	✓	
Bietet eine kurze Installationszeit, wobei vollständige Implementierungen auch für die größten Unternehmen innerhalb von Stunden oder Tagen anstatt Wochen oder Monaten abgeschlossen sind	✓	

Architektur des Managementsystems

Die Lösung sollte folgende Merkmale aufweisen:	**IBM**	**Andere**
Ermöglicht durch eine lokale Implementierung des intelligenten Agenten die Verwaltung neu ermittelter Endpunkte in Minutenschnelle	✓	
Nutzt dieselbe Infrastruktur für alle Endpunktmanagementfunktionen, sodass sich Herausforderungen der heutigen Zeit ohne Probleme bewältigen und weitere Endpunktmanagementfunktionen bei steigenden Unternehmensanforderungen reibungslos hinzufügen lassen	✓	
Aktualisiert sich eigenständig unter Verwendung der eigenen Infrastruktur und ermöglicht Produktupgrades und -updates innerhalb von Minuten anstatt Wochen oder gar Monaten	✓	
Minimiert durch integrierte Produkt- und Inhaltsaktualisierungen den zur Aufrechterhaltung des aktuellen Implementierungsstatus erforderlichen Aufwand	✓	
Lässt sich in ein umfassendes Managementportfolio integrieren, sodass echtzeitorientierte Transparenz, zentrale Steuerung und erweiterte Funktionalität für die gesamte IT-Infrastruktur sichergestellt sind	✓	
Bietet Unterstützung in der Landessprache für Italienisch, Deutsch, Französisch, Spanisch, Japanisch, vereinfachtes Chinesisch, traditionelles Chinesisch, Portugiesisch, Koreanisch und Englisch	✓	

Auswahl des geeigneten Anbieters für Endpunktmanagement

Der ausgewählte Anbieter sollte alle Anforderungen hinsichtlich des Endpunktmanagements erfüllen können. Im Idealfall geht er sogar bei der Implementierung der Lösung zur Hand. Bevor die Entscheidung für einen Anbieter fällt, sollten folgende Fragen gestellt werden:

Unterstützt die Technologie des Anbieters die Unternehmensziele? Ratsam sind Anbieter, deren Lösungen an den Unternehmenszielen ausgerichtet werden können. Bieten die Lösungen Effizienzsteigerungen, kurze Implementierungszeiten für Geschäftsservices, Kostensenkungen, optimierte Compliance und kurze Markteinführungszeiten?

Stellt der Anbieter nur einen Teil oder die Gesamtlösung bereit?
Bietet ein Anbieter eine Lösung, die lediglich auf eine bestimmte Umgebungs- oder Endpunktanforderung ausgelegt ist, entstehen womöglich isolierte Verwaltungssilos. Die für die Lösung aufzubringenden Kosten und der notwendige Zeitaufwand zur Verwaltung verschiedener Provider können bei Beteiligung mehrerer Anbieter drastisch ansteigen. Ratsam sind Anbieter, die ein vollständiges Portfolio für das Endpunktmanagement zur Verfügung stellen.

Inwieweit ist der Anbieter weltweit vertreten?
Unternehmen mit internationalen Niederlassungen sollten einen Anbieter auswählen, der weltweit vertreten ist und über bewährte Erfahrungen auf internationaler Ebene verfügt. Ratsam sind Anbieter, die die Unternehmensniederlassungen im Ausland mit ihren eigenen lokalen Ressourcen unterstützen können.

Wird die Lösung von einer erfahrenen Unterstützungsorganisation betreut, die das spezielle und vielfältige Know-how aufweist, auf dessen Basis sie im Bedarfsfall verlässlich zur Seite stehen kann?
Der Provider sollte äußerst reaktionsfähige und effektive Kundenunterstützung bieten. Ratsam sind Anbieter mit einer bewährten Unterstützungsorganisation, damit Softwareinvestitionen maximal ausgeschöpft werden können.

Wie zukunftsfähig sind die Stabilität und Leistungsfähigkeit des Anbieters vor dem Hintergrund der modernen Wirtschaftswelt?
Auf hart umkämpften Märkten spielen Stabilität und Entwicklungsfähigkeit des Anbieters eine wesentliche Rolle. Ratsam sind Anbieter, die sich bereits seit Langem in der Branche etabliert haben und eine solide, zukunftsorientierte Strategie sowie die Ressourcen aufweisen, damit sie in wirtschaftlich schwierigen Zeiten ihr Fortbestehen sichern können.

Kann der Anbieter strategisch konzipierte und technisch erstklassige Produkte bereitstellen?
Beim Vergleich unterschiedlicher Lösungen kommt es auf technische Exzellenz (optimal abgestimmtes Funktionsspektrum, intelligenter Aufbau der Lösungsarchitektur, Unterstützung für Branchenstandards) an.

Einheitliche Lösungen für erfolgreiches Endpunktmanagement

Bei der Bewertung von Lösungen im Hinblick auf die Erreichbarkeit von Zielvorgaben wird deutlich, dass IBM nicht nur eine herausragende Software zur Endpunktverwaltung, sondern auch ein leistungsstarkes Sicherheitsportfolio mit vielfältigen Produkten und Integrationsmöglichkeiten bietet. IBM Lösungen sorgen für transparente Einblicke in die Endpunktumgebungen von Unternehmen. Sie erleichtern die Kontrolle von Verwaltungs-, Sicherheits- und Compliancekosten. Überdies lassen sich heterogene Endpunkt-, Betriebssystem- und Anwendungsinfrastrukturen unkompliziert verwalten.

Die Aussage, dass nur verwaltet werden kann, was sichtbar ist, gilt für das Endpunktmanagement ebenso wie für andere Bereiche. Dank der funktionsübergreifenden und einheitlichen Transparenz und Steuerungsoptionen beim IBM Endpunktmanagement können IT-Silos aufgelöst werden, die eine effektive und zeitgerechte Verwaltung von Endpunkten verhindern. Durch die Automatisierung und Konsolidierung von Tasks in Kombination mit intelligenten Agenten, die fortlaufend und asynchron die Bewertung und Durchsetzung von Richtlinien steuern, erübrigt sich eine komplexe Management-Server-Infrastruktur.

Anhand der schnellen und präzisen Durchführung von Änderungen in der gesamten Infrastruktur verhilft die Lösung IBM Endpoint Manager zu einer erheblichen Reduzierung von unzulänglichen Verwaltungsfunktionen und Sicherheitslücken. Auf der Grundlage der BigFix®-Technologie trägt diese Lösung durch schnelle und exakte Durchsetzung endpunktrelevanter Richtlinien und durch Anwendung von Korrekturmaßnahmen dazu bei, die Sicherheitsrisiken, Verwaltungskosten und die Komplexität beim Management zu begrenzen. Die Strategie sieht nur einen Agenten, eine zentrale Konsole und einen einzelnen Management-Server vor. Auf diese Weise lässt sich die Zuverlässigkeit erhöhen und die Implementierungszeit verkürzen. Möglich machen dies Funktionen wie Patch-Management, Konfigurationsverwaltung und Endpunkterkennung. Außerdem kann dieses Modell durch eine Steigerung der Effizienz von Geschäftsabläufen, durch eine Konsolidierung der Managementinfrastruktur und durch eine Optimierung der IT-Produktivität zu einem höheren ROI (Return-on-Investment, Kapitalrendite) führen.

Mit dem IBM Endpoint Manager-Konzept mit nur einem Agenten können Unternehmen des Weiteren ihre vorhandenen Ressourcen optimal nutzen. Da der Management-Server der Lösung vom Agenten immer auf dem aktuellen Stand gehalten wird, sind keine langwierigen Suchläufe oder Abfragen erforderlich und keine Probleme mit heruntergefahrenen Systemen oder Systemen im Roamingbetrieb außerhalb des Unternehmensnetzwerks zu befürchten. Durch den völlig autonomen Betrieb des Agenten in Kombination mit der Transparenz, die die zentrale Konsole bietet, können Administratoren alle Ereignisse im gesamten Netzwerk sehen.

IBM Endpoint Manager ist Teil des umfassenden Portfolios an Sicherheits- und Managementlösungen, mit dem Unternehmen die Probleme bezüglich verteilter Infrastrukturen lösen können. Bei den instrumentierten, vernetzten und intelligenten IT-Prozessen, die in unserer intelligenten Welt von heute dominieren, tragen IBM Sicherheits- und Managementlösungen dazu bei, Echtzeittransparenz, zentrale Steuerung und erweiterte Automation für die gesamte IT-Infrastruktur und deren weltweit verteilte Endpunkte sicherzustellen.

Weitere Informationen

Wenn Sie mehr über IBM Endpoint Manager erfahren möchten, wenden Sie sich an den zuständigen IBM Ansprechpartner oder IBM Business Partner oder besuchen Sie uns unter: **ibm.com**/tivoli/endpoint

Informationen zu Tivoli Software von IBM

Tivoli Software von IBM unterstützt Unternehmen dabei, ihre IT-Ressourcen, Aufgaben und Prozesse effizient und effektiv zu verwalten, damit sie den sich stetig wandelnden Geschäftsanforderungen gerecht werden. Sie ermöglicht ein flexibles und reaktionsfähiges IT-Service-Management und eine Kostensenkung. Das Tivoli Portfolio umfasst Software für Sicherheit, Compliance, Speicherung, Leistung, Verfügbarkeit, Konfiguration, Prozesse und IT-Lifecycle-Management und basiert auf erstklassigen IBM Angeboten in den Bereichen Services, Support und Forschung.

Finanzierungslösungen von IBM Global Financing bieten Möglichkeiten wie ein effektives Cash-Management, den Schutz vor überalterter Technologie, die Senkung der Gesamtbetriebskosten und einen höheren ROI. Zudem helfen unsere Global Asset Recovery Services dabei, durch neue energieeffizientere Lösungen auch dem Umweltschutz Rechnung zu tragen. Weitere Informationen zu IBM Global Financing finden Sie unter: **ibm.com**/financing

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

Bitte der Wiederverwertung zuführen

Jeder Kunde ist für die Einhaltung der geltenden Gesetze und Verordnungen selbst verantwortlich. Es obliegt allein dem Kunden, sich von kompetenter juristischer Stelle zu Inhalt und Einhaltung aller relevanten Gesetze und gesetzlichen Bestimmungen beraten zu lassen, die sich auf seine Geschäftstätigkeit und alle Maßnahmen auswirken können, die er im Hinblick auf die Einhaltung solcher Bestimmungen durchführen muss. IBM erteilt keine Rechtsberatung und gibt keine Garantie bezüglich der Konformität von IBM Produkten oder Services mit jeglichen relevanten Gesetzen und Verordnungen.

TIO14008-DEDE-01