ManageEngine
Endpoint Central

Datenblatt

Komplettes Endpoint Management – über ein einziges Interface

Aktuelle Herausforderungen

Die Arbeitsweise von Unternehmen hat sich durch die rapide steigende Anzahl und Vielfalt der verwendeten Endgeräte signifikant verändert. Vor diesem Hintergrund suchen immer mehr Unternehmen nach einer Unified-Endpoint-Management- & -Security(UEMS)- Lösung, mit der sich die breite Palette an Firmengeräten über eine einzige Software-Plattform verwalten und kontrollieren lässt – von Servern und Desktops über Laptops bis hin zu Smartphones und Tablets.

Die Lösung

Endpoint Central ist eine umfangreiche UEMS-Lösung, mit der IT-Abteilungen Server, Desktops und mobile Geräte über eine einzige Benutzeroberfläche verwalten können. Wiederkehrende Aufgaben bei der Verwaltung von Desktops und mobilen Geräten können von Anfang bis Ende automatisiert werden. Das hilft Unternehmen, ihre IT-Infrastrukturkosten zu senken, die betriebliche Effizienz und Produktivität zu verbessern sowie Schwachstellen, Insider-Bedrohungen und Datenverluste im Netzwerk zu reduzieren.

Mit Endpoint Central können Sie

- regelmäßige Aktivitäten beim Endgeräte-Management automatisieren
- Konfigurationen für Betriebssysteme und Anwendungen in Ihrem gesamten Netzwerk standardisieren
- Endgeräte vor einer Vielzahl von Bedrohungen schützen
- alltägliche IT-Probleme beheben
- Audits zu Ihren IT-Assets erstellen

Highlights

Unterstützte Betriebssysteme

Linux
macOS
ChromeOS
Windows
iOS
Android
Windows Phone
tvOS

Ausgezeichnet von

IDC
Forrester
Gartner
PUR 2025 Professional User Rating

Über **17 Jahre** Erfahrung im Endpoint Management

Mehr als **25.000** Kunden vertrauen auf Endpoint Central

Derzeit werden **20 Mio.** Endpoints mit Endpoint Central verwaltet

Unterstützung von **20** Sprachen

In **190** Ländern im Einsatz

Kostenlose Verwaltung von bis zu 25 Endpoints

Patch Management

- Automatisieren Sie das Patch Management für über 1.000 Windows-, Mac-, Linux- und Drittanbieter-Anwendungen.
- Lassen Sie fehlende Patches von Endpoint Central proaktiv aufspüren und bereitstellen.
- Testen und genehmigen Sie Patches vor der Bereitstellung, um Sicherheitsrisiken zu minimieren.
- Verteilen Sie kritische Zero-Day-Patches.
- Deaktivieren Sie automatische Aktualisierungen und lehnen Sie Patches je nach Bedarf ab.
- Erhalten Sie Berichte über den Zustand des Systems sowie über die Anfälligkeit der Systeme.

Software Deployment

- Installieren oder deinstallieren Sie MSI- und EXE-basierte Anwendungen.
- Planen Sie die Bereitstellung von Software und legen Sie fest, welche Aktivitäten vor und nach der Bereitstellung durchgeführt werden sollen.
- Erlauben Sie Anwendern, Software über das Self-Service-Portal selbst zu installieren.
- Nutzen Sie über 10.000 vordefinierte Vorlagen für die Bereitstellung von Anwendungen.
- Erstellen Sie ein Repository mit Software-Paketen und verwenden Sie diese beliebig oft zur Installation oder Deinstallation.
- Installieren Sie Software als bestimmter Benutzer, indem Sie die Option „Ausführen als“' verwenden.

Vulnerability Management

- Verbessern Sie Ihre Sicherheitslage mit integriertem Threat- und Vulnerability-Management, indem Sie Schwachstellen sofort erkennen und beheben.
- Erhöhen Sie die Sicherheit durch den Einsatz von Sicherheitsrichtlinien und die Beseitigung von Systemfehlkonfigurationen.
- Nutzen Sie die exklusive Partnerschaft von ManageEngine mit dem Centre for Internet Security (CIS), um die Compliance mit den CIS-Benchmarks sicherzustellen.
- Identifizieren Sie Zero-Day-Schwachstellen und mindern Sie diese mit vorgefertigten, getesteten Skripten ab.
- Überwachen und deinstallieren Sie High-Risk-Software, wie End-of-Life-, Remote-Desktop-Sharing- und Peer-to-Peer-Software, um sich vor unbefugten Datenzugriffen zu schützen.
- Überprüfen Sie aktive Ports, um Anomalien zu entdecken.

Asset Management

- Überwachen Sie die gesamte Hardware und Software in Ihrem Netzwerk live.
- Stellen Sie Compliance bei den Software-Lizenzen sicher.
- Blockieren Sie ausführbare Dateien und deinstallieren Sie verbotene Software.
- Analysieren Sie Software-Nutzungsstatistiken und reduzieren Sie die Kosten für ungenutzte Software durch Software-Metering.
- Lassen Sie sich bei bestimmten Ereignissen benachrichtigen, z. B. wenn neue oder verbotene Software erkannt wird oder eine Unterlizenzierung die Compliance gefährdet.
- Behalten Sie den Überblick mit über 20 vordefinierten Berichten für Hardware, Software, Inventar und Lizenz-Compliance.

Mobile Application Management

- Erstellen Sie Ihr eigenes App-Repository, das nur von der IT-Abteilung genehmigte interne und kommerzielle Apps enthält.
- Installieren, aktualisieren und entfernen Sie Unternehmens-Apps im Hintergrund von Geräten, verwalten Sie App-Lizenzen und konfigurieren Sie App-Berechtigungen.
- Stellen Sie sicher, dass auf den Geräten nur vertrauenswürdige Unternehmens-Apps ausgeführt werden, setzen Sie bösartige/nicht-sichere Apps auf eine schwarze Liste und verhindern Sie, dass Benutzer Unternehmens-Apps deinstallieren.

System-Tools

- Überwachen und analysieren Sie remote verwaltete Systeme, indem Sie sich Details zu den darauf laufenden Tasks und Prozessen anzeigen lassen.
- Booten Sie einen Rechner mit Wake-on-LAN aus der Ferne oder planen Sie das Hochfahren.
- Veröffentlichen Sie Ankündigungen unternehmensweit oder nur für Techniker.
- Planen Sie die Defragmentierung, Überprüfung und Bereinigung von Festplatten für lokale oder entfernte Workstations.

Anwendungskontrolle

- Erkennen Sie alle installierten Anwendungen und ausführbaren Dateien und kategorisieren Sie sie auf der Grundlage ihrer digitalen Signaturen als vom Unternehmen genehmigt oder nicht genehmigt.
- Regulieren Sie den Grad an Flexibilität, indem Sie mehrere Modi zur effizienten Einrichtung einer Zero-Trust-Umgebung nutzen.
- Kontrollieren Sie Anwendungen problemlos, indem Sie Anwendern die Möglichkeit geben, den Zugriff auf Anwendungen zu beantragen.
- Verfolgen Sie einen Zero-Trust-Ansatz, indem Sie den „Strict Mode“ aktivieren, um auch nicht verwaltete Anwendungen automatisch zu verbieten.

Data Leakage Prevention

- Überwachen und regulieren Sie Datenbewegungen in Ihrem Unternehmen von einer zentralen Benutzeroberfläche aus, um Insider-Angriffe und Datenverluste zu verhindern.
- Scannen und kategorisieren Sie unternehmenskritische Daten entsprechend den Compliance- und Regulierungsstandards.
- Regulieren Sie Datenübertragungsversuche über Cloud-Uploads, E-Mail-Austausch, Drucker und andere Peripheriegeräte.
- Erhalten Sie sofortige Warnmeldungen bei Verstößen gegen Richtlinien und korrigieren Sie falsch positive Ereignisse.

Browser Security

- Sperren Sie Unternehmens-Browser und härten Sie die Browser-Einstellungen, um Browser-basierte Angriffe zu verhindern.
- Verschaffen Sie sich einen umfassenden Überblick über die verschiedenen Browser, die in Ihrem Netzwerk verwendet werden.
- Setzen Sie Browser-Sicherheitskonfigurationen wie STIG- und CIS-Compliance durch.
- Sorgen Sie für ein sicheres Brower-Erlebnis, indem Sie schädliche Plug-Ins erkennen und entfernen.
- Lassen Sie freigegebene Websites zu und blockieren Sie unerwünschte Webanwendungen, um die Produktivität und Sicherheit zu erhöhen.

Mobile Device Management

- Automatisieren Sie die Registrierung und Authentifizierung von mehreren BYOD- und Unternehmensgeräten auf einmal.
- Kontrollieren Sie Betriebssystem-Updates und beheben Sie Probleme auf mobilen Geräten.
- Verschaffen Sie sich durch vorkonfigurierte und anpassbare Berichte einen vollständigen Überblick über die mobilen Endgeräte Ihres Unternehmens.

Mobile Security Management

- Konfigurieren Sie Sicherheitsrichtlinien für WLAN, VPN, E-Mail etc. und setzen Sie diese für Ihr Unternehmen durch.
- Verhindern Sie unbefugte Zugriffe auf geschäftliche E-Mails und sorgen Sie für eine sichere Bereitstellung, Speicherung und Darstellung von Inhalten.
- Erzwingen Sie eine Verschlüsselung auf Geräteebene und trennen Sie persönliche und unternehmenseigene Arbeitsbereiche auf BYOD-Geräten. Spüren Sie verlegte Geräte auf, sperren Sie diese und löschen Sie die darauf befindlichen Daten.

Konfigurationen

- Standardisieren Sie Desktop-, Computer-, Anwendungs- und Sicherheitseinstellungen mithilfe von Basiskonfigurationen.
- Nutzen Sie die über 40 Konfigurationen für Benutzer und Computer oder erstellen Sie eigene Vorlagen für häufig verwendete Konfigurationen.
- Wählen Sie aus über 180 Skripten im Script Repository.
- Schränken Sie die Nutzung von USB-Geräten (z. B. Drucker, CD-Laufwerke, externe Geräte, Bluetooth-Geräte, Modems und andere Peripheriegeräte) im Netzwerk sowohl auf Benutzer- als auch auf Computerebene ein.
- Sorgen Sie für ein effektives Energiemanagement, indem Sie Energieschemata anwenden, inaktive Computer abschalten und sich Berichte über die Systembetriebszeit anzeigen lassen.
- Konfigurieren Sie Browser-, Firewall- und Sicherheitsrichtlinien und kontrollieren Sie den Zugriff auf Dateien, Ordner und die Registry mit Hilfe der Zugriffsrechteverwaltung.
- Konfigurieren Sie Warnungen für in Kürze ablaufende Passwörter und geringen Speicherplatz auf dem System.

Kontrolle von Peripheriegeräten

- Regulieren und beschränken Sie effektiv den Zugang zu mehr als 15 Arten von Peripheriegeräten von einer zentralen Benutzeroberfläche aus – mit automatischer Erkennung aktiver Ports.
- Schützen Sie unternehmenskritische Daten durch rollenbasierte Dateizugriffs- und -übertragungskontrollen mit Limits für die Dateiübertragung.
- Gewähren Sie bestimmten Endpoints temporären Zugriff auf Peripheriegeräte für einen bestimmten Zeitraum.
- Handeln Sie proaktiv, indem Sie Daten an einem sicheren Ort spiegeln, wenn USB-Geräte auf Ihre kritischen Unternehmensdaten zugreifen, und verhindern Sie so Datenverluste.
- Halten Sie die Compliance-Standards für Geräte ein, indem Sie Datenverluste durch Peripheriegeräte verhindern, und verschaffen Sie sich einen Überblick durch umfassende Audit-Berichte für Geräte.

Berichte

- Nutzen Sie über 200 sofort einsatzbereite Active-Directory-Berichte über Benutzer, Computer, Gruppen, Organisationseinheiten (OUs) und Domänen.
- Senken Sie Ihre Stromkosten durch effektives Energiemanagement und lassen Sie sich Berichte zur Systembetriebszeit anzeigen.
- Erhalten Sie aktuelle Details zur Benutzeranmeldung mit den Benutzeranmeldeberichten.
- Erstellen Sie Berichte zu Patches, Konfigurationen und Ereignissen für Audits.

Endpoint Privilege Management

- Beseitigen Sie unnötige Admin-Rechte und führen Sie geschäftskritische Anwendungen mit eingeschränkten Rechten aus, um Angriffe zu verhindern, die auf einer Ausweitung von Zugriffsrechten oder der Kompromittierung von Zugangsdaten basieren.
- Befolgen Sie das Least-Privilege-Modell, ohne die Produktivität zu beeinträchtigen, indem Sie anwendungsspezifische Berechtigungserweiterungen aktivieren.
- Bewältigen Sie vorübergehende Anforderungen von Anwendern, indem Sie einen temporären privilegierten Zugriff auf Anwendungen ermöglichen, der nach einem bestimmten Zeitraum automatisch wieder entzogen wird.

Anti-Ransomware

- Erhöhte Endpoint-Sicherheit durch reaktiven Schutz vor Ransomware.
- Die mehrfach patentierte und durch maschinelles Lernen unterstützte Verhaltensanalyse erkennt sofort jede Ransomware, die versucht, in Ihr Netzwerk einzudringen.
- Erhalten Sie eine detaillierte Analyse aller Eindringversuche.
- Stellen Sie Daten bei Bedarf mit einem Klick durch patentierte manipulationssichere Backup-Techniken wieder her.

** Hinweis: Anti-Ransomware befindet sich derzeit in der Early-Access-Phase.*

Fernsteuerung

- Erfüllen Sie mit der sicheren Remote Control verschiedene Compliance-Vorschriften wie HIPAA, PCI DSS etc.
- Beheben Sie Probleme mit Remote-Desktops nahtlos und bei Bedarf durch die Zusammenarbeit mehrerer Benutzer – auch im Homeoffice.
- Nutzen Sie die integrierten Video-, Anruf- und Chatfunktionen sowie die Optionen für die Dateiübertragung zwischen Rechnern.
- Zeichnen Sie Fernsteuerungssitzungen zu Audit-Zwecken auf.
- Sperren Sie die Tastaturen und Mäuse von Endanwendern und verdunkeln Sie deren Bildschirme, um die Vertraulichkeit während Remote-Control-Sitzungen zu gewährleisten.
- Profitieren Sie von den Vorteilen der 128-Bit-AES-Verschlüsselungsprotokolle bei Fernsteuerungsvorgängen.

OS-Bereitstellung

- Erstellen Sie mit intelligenten Online- und Offline-Imaging-Techniken automatisch das Image eines Computers.
- Speichern Sie diese Images in einem zentralen Repository und stellen Sie Betriebssysteme bei Bedarf auch von unterwegs bereit.
- Passen Sie die erfassten Images mit Hilfe von Bereitstellungsvorlagen für verschiedene Rollen und Abteilungen in Ihrem Unternehmen an.
- Sorgen Sie für eine problemlose Bereitstellung auf verschiedenen Hardware-Typen.
- Führen Sie nach der Bereitstellung diverse Aktivitäten aus, wie die Installation von Anwendungen, die Konfiguration von Computereinstellungen und vieles mehr.

BitLocker-Management

- Sichern Sie die Daten Ihrer Computer, indem Sie die Verschlüsselung für ausgewählte Laufwerke oder gesamte Festplatten automatisieren.
- Identifizieren Sie Computer, auf denen ein TPM installiert ist, um die PIN-Sicherheit in Verbindung mit einer Passphrase-Authentifizierung zu erhöhen.
- Stellen Sie bei defekter Hardware die Daten eines Computers mit dem Wiederherstellungsschlüssel wieder her und setzen Sie das Passwort für Computer zurück, die aus dem Netzwerk entfernt wurden.
- Setzen Sie Richtlinien zur Datenverschlüsselung ein und halten Sie sich an Datenschutzrichtlinien wie FISMA, HIPAA und PCI-DSS.

Next-Gen Antivirus

- Verstärken Sie den Schutz vor neuen Bedrohungen durch KI-unterstützte Malware-Erkennung in Echtzeit.
- Umfassende forensische Untersuchung von Incidents mit detaillierten Berichten, die sich an den MITRE TTPs (Tactics, Techniques, and Procedures) orientieren.
- Detaillierte Einblicke in Angriffsmethoden, Pfade und Kill-Chain-Analysen.
- Reagieren Sie umgehend auf Angriffe, um diese schnell zu neutralisieren – inklusive Ransomware-Schutz.
- Gewährleisten Sie die Geschäftskontinuität durch eine Bedrohungsabwehr, die den Betrieb Ihres Netzwerks nur minimal unterbricht.
- Stellen Sie kompromittierte Dateien mit wenigen Klicks in ihrem ursprünglichen Zustand wieder her.

** Hinweis: Next-Gen Antivirus befindet sich derzeit in der Early-Access-Phase.*

Kontakt

Weitere Informationen

www.manageengine.de/endpointcentral

Ihr ManageEngine-Partner:

MicroNova AG
Unterfeldring 6, D-85256 Vierkirchen
Tel.: +49 8139 9300-456
E-Mail: sales-ManageEngine@micronova.de
Support: www.manageengine.de/support

© 2024 Zoho Corp. All rights reserved.

ManageEngine