Endpoint Management und -Security – über eine Oberfläche

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, Tablets und IoT-Geräten.

Die Lösung

Endpoint Central ist eine umfangreiche Endpoint-Management- und -Security-Lösung, mit der IT-Abteilungen Server, Desktops und mobile Geräte über eine einzige Benutzeroberfläche verwalten können. Die Lösung automatisiert wiederkehrende Aufgaben bei der Verwaltung von Endgeräten über deren gesamten Lebenszyklus. Das senkt IT-Kosten und erhöht die betriebliche Effizienz und Produktivität. Integrierte Sicherheitsfunktionen helfen Unternehmen dabei, Schwachstellen, Datenverluste und Browser-basierte Bedrohungen zu reduzieren. Zusätzliche Funktionen für das Enduser Experience Management ermöglichen es IT-Teams, die Performance aus Anwendersicht zu überwachen und Probleme proaktiv zu beheben.

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
- die digitale Benutzererfahrung überwachen und proaktiv verbessern

Highlights

Unterstützte Betriebssysteme

Linux
macOS
ChromeOS
Windows
iOS
Android
Windows Phone
tvOS

Ausgezeichnet von

IDC
FORRESTER®
Gartner
PUR 2026 Professional User Rating

Über **20 Jahre** Erfahrung im Endpoint Management

Mehr als **31.000** Kunden vertrauen auf Endpoint Central

Derzeit werden **26 Mio.** Endpoints mit Endpoint Central verwaltet

Unterstützung von **20** Sprachen

In **190** Ländern im Einsatz

Kostenlose Verwaltung von bis zu 25 Endpoints

Patch Management

- Automatisiertes Patch Management für über 1.000 Windows-, Mac-, Linux- und Drittanbieter-Anwendungen
- Proaktives Erkennen und Bereitstellen fehlender Patches
- Testen und Genehmigen von Patches vor der Verteilung zur Minimierung von Sicherheitsrisiken
- Verteilung kritischer Zero-Day-Patches
- Deaktivieren automatischer Updates und gezieltes Ablehnen einzelner Patches
- Berichte zum Systemzustand und zu Sicherheitsanfälligkeiten

Vulnerability Management

- Verbesserte Sicherheitslage durch integriertes Threat- und Vulnerability-Management mit sofortiger Erkennung und Behebung von Schwachstellen
- Erhöhung der Sicherheit durch Sicherheitsrichtlinien und die Beseitigung von Systemfehlkonfigurationen
- Sicherstellung der CIS-Compliance durch exklusive Partnerschaft mit dem Centre for Internet Security (CIS)
- Erkennung von Zero-Day-Schwachstellen und Risikominimierung mit vorgefertigten, getesteten Skripten
- Überwachung und Deinstallation von High-Risk-Software (z. B. End-of-Life-, Remote-Desktop-Sharing- und Peer-to-Peer-Software)
- Prüfung aktiver Ports zur Erkennung von Anomalien

Asset Management

- Live-Überwachung der gesamten Hardware und Software im Netzwerk
- Sicherstellung der Software-Lizenz-Compliance
- Blockieren ausführbarer Dateien und Deinstallation verbotener Software
- Analyse von Software-Nutzungsstatistiken und Reduzierung von Kosten für ungenutzte Software durch Software-Metering
- Ereignisbasierte Benachrichtigungen, z. B. bei neuer oder verbotener Software oder einer Unterlizenzierung
- Über 20 vordefinierte Berichte zu Hardware, Software, Inventar und Lizenz-Compliance

Mobile Application Management

- Erstellung eines eigenen App-Repositorys mit ausschließlich von der IT genehmigten internen und kommerziellen Apps
- Hintergrundinstallation, -aktualisierung und -entfernung von Unternehmens-Apps, inklusive Lizenzverwaltung und vorkonfgurierten App-Berechtigungen
- Ausführung ausschließlich vertrauenswürdiger Unternehmens-Apps, Blacklisting unsicherer Apps und Schutz vor App-Deinstallation

Software Deployment

- Installation und Deinstallation von MSI- und EXE-Anwendungen
- Softwarebereitstellungen planen sowie Ausführung von definierten Aktivitäten vor und nach der Bereitstellung
- Self-Service-Portal zur eigenständigen Softwareinstallation durch Anwender
- Über 10.000 Vorlagen für die Anwendungsbereitstellung
- Zentrales Repository mit Software-Paketen erstellen und diese beliebig oft zur Installation oder Deinstallation verwenden
- Installation von Software als bestimmter Benutzer mit der Option „Ausführen als“

System-Tools

- Überwachung und Analyse remote verwalteter Systeme inkl. laufender Tasks und Prozesse
- Rechner mit Wake-on-LAN aus der Ferne starten oder zeitgesteuert hochfahren
- Ankündigungen unternehmensweit oder nur für Techniker veröffentlichen
- Geplante Defragmentierung, Überprüfung und Bereinigung von Festplatten auf lokalen oder entfernten Workstations

Mobile Device Management

- Automatisierte Registrierung und Authentifizierung von mehreren BYOD- und Unternehmensgeräten auf einmal
- Kontrolle von Betriebssystem-Updates und Fehlerbehebung auf mobilen Endgeräten
- Vorkonfigurierte und anpassbare Berichte für vollständigen Überblick über mobile Geräte

Anwendungskontrolle

- Erkennung aller installierten Anwendungen und ausführbaren Dateien sowie Kategorisierung anhand digitaler Signaturen als genehmigt oder nicht genehmigt
- Flexible Steuerung mit mehreren Modi für effiziente Umsetzung einer Zero-Trust-Umgebung
- Einfache Anwendungskontrolle mit der Möglichkeit für Anwender, Zugriff auf Anwendungen zu beantragen
- Durchsetzung eines Zero-Trust-Ansatzes durch Aktivierung des „Strict Mode“, der nicht verwaltete Anwendungen automatisch verbietet

Browser Security

- Sperren von Unternehmens-Browsern und Härtung der Browser-Einstellungen zum Schutz vor Angriffen
- Zentraler Überblick über alle im Netzwerk eingesetzten Browser
- Durchsetzung von Browser-Sicherheitskonfigurationen wie STIG- und CIS-Compliance
- Erkennung und Entfernung schädlicher Plug-ins für ein sicheres Browser-Erlebnis
- Zulassen freigegebener Websites und Blockieren unerwünschter Webanwendungen zur Steigerung von Sicherheit und Produktivität

Mobile Security Management

- Konfiguration und Durchsetzung von Sicherheitsrichtlinien für WLAN, VPN, E-Mail und weitere mobile Dienste
- Schutz geschäftlicher E-Mails vor unbefugten Zugriffen sowie sichere Bereitstellung, Speicherung und Darstellung von Inhalten
- Verschlüsselung auf Geräteebene; Trennung persönlicher und geschäftlicher Arbeitsbereiche auf BYOD-Geräten; Ortung, Sperrung und Löschung von Daten auf verlorenen Geräten

Berichte

- Über 200 sofort einsatzbereite Active-Directory-Berichte zu Benutzern, Computern, Gruppen, Organisationseinheiten (OUs) und Domänen
- Energie- und Systembetriebszeitberichte zur Reduzierung von Stromkosten
- Detaillierte Benutzeranmeldeberichte mit aktuellen Login-Informationen
- Auditfähige Berichte zu Patches, Konfigurationen und Ereignissen

Konfigurationen

- Standardisierung von Desktop-, Computer-, Anwendungs- und Sicherheitseinstellungen über Basiskonfigurationen
- Über 40 Konfigurationen für Benutzer und Computer oder Erstellung eigener Vorlagen für häufig verwendete Konfigurationen
- Zugriff auf über 180 Skripte im Script Repository
- Einschränkung von USB-Geräten (z. B. Drucker, CD-Laufwerke, externe Geräte, Bluetooth-Geräte und andere Peripheriegeräte) im Netzwerk auf Benutzer- und Computerebene
- Effektives Energiemanagement durch Energieschemata, automatisches Abschalten inaktiver Computer und Berichte zur Systembetriebszeit
- Browser-, Firewall- und Sicherheitsrichtlinien sowie Zugriffskontrolle auf Dateien, Ordner und Registry
- Konfiguration von Warnungen für in Kürze ablaufende Passwörter oder geringen Speicherplatz

Kontrolle von Peripheriegeräten

- Zugriff auf über 15 Arten von Peripheriegeräten zentral steuern und einschränken, inklusive automatischer Erkennung aktiver Ports
- Rollenbasierte Datei- und Datenübertragungskontrollen mit definierten Übertragungslimits zum Schutz unternehmens-kritischer Daten
- Temporärer Zugriff auf Peripheriegeräte für ausgewählte Endgeräte
- Proaktive Datensicherung beim Zugriff von USB-Geräten auf kritische Unternehmensdaten durch Datenspiegelung an einem sicheren Ort
- Einhaltung von Compliance-Vorgaben sowie umfassende Audit-Berichte für Geräte

Endpoint Privilege Management

- Entfernung unnötiger Admin-Rechte und Ausführung geschäftskritischer Anwendungen mit eingeschränkten Rechten helfen, Angriffe durch Privilegienausweitung oder kompromittierte Zugangsdaten zu verhindern
- Umsetzung des Least-Privilege-Prinzips ohne Produktivitätseinbußen durch anwendungsspezifische Berechtigungserweiterungen
- Temporärer privilegierter Zugriff auf Anwendungen mit automatischem Entzug nach einem definierten Zeitraum

Anti-Ransomware

- Erhöhte Endpoint-Sicherheit durch reaktiven Schutz vor Ransomware
- Mehrfach patentierte und durch maschinelles Lernen unterstützte Verhaltensanalyse zur sofortigen Erkennung von Ransomware-Angriffen
- Detaillierte Analyse aller erkannten Eindringversuche
- Wiederherstellung von Daten mit einem Klick durch patentierte, manipulationssichere Backup-Technologien

Fernsteuerung

- Sichere Remote-Control-Sitzungen zur Einhaltung von Compliance-Vorgaben wie HIPAA, PCI DSS etc.
- Nahtlose Fehlerbehebung auf Remote-Desktops, auch durch Zusammenarbeit mehrerer Benutzer
- Integrierte Video-, Anruf- und Chatfunktionen sowie Dateiübertragung zwischen Systemen
- Aufzeichnung von Fernsteuerungssitzungen für Audit-Zwecke
- Sperren von Tastaturen und Maus sowie Bildschirmverdunkelung bei Remote-Control-Sitzungen zur Wahrung der Vertraulichkeit
- 128-Bit-AES-Verschlüsselung für sichere Fernsteuerungs-vorgänge

OS-Bereitstellung

- Automatisierte Erstellung von Betriebssystem-Images mit intelligenten Online- und Offline-Imaging-Techniken
- Zentrales Image-Repository für flexible Bereitstellung von Betriebssystemen – bei Bedarf auch von unterwegs
- Anpassung von Images für unterschiedliche Rollen und Abteilungen über Bereitstellungsvorlagen
- Problemlose Bereitstellung auf verschiedenen Hardware-Typen
- Automatisierte Ausführung von Post-Deployment-Aktivitäten wie die Installation von Anwendungen oder die Konfiguration von Computereinstellungen

Data Leakage Prevention

- Zentrale Überwachung und Steuerung von Datenbewegungen, um Insider-Angriffe und Datenverluste zu verhindern
- Scannen und Kategorisieren unternehmenskritischer Daten gemäß Compliance- und Branchenstandards
- Kontrolle von Datenübertragungsversuchen über Cloud-Uploads, E-Mail, Drucker und andere Peripheriegeräte
- Echtzeit-Warnmeldungen bei Verstößen gegen Richtlinien und Korrektur falsch positiver Ereignisse

Digital Employee Experience (DEX)*

- Kontinuierliche Überwachung von Endgeräten mit Echtzeit-Telemetrie (z. B. CPU, Arbeitsspeicher, Festplatte, Akku, Garantie, GPU und Anwendungsabstürze)
- Proaktive Erkennung und Priorisierung von Problemen durch konfigurierbare Warnmeldungen, Schweregrad-Kennzeichnung und intelligente Gruppierung von Alerts
- Schnelle Ursachenanalyse durch Einbeziehung relevanter Kontextdaten, die Ausfälle mit Geräte- und App-Versionen, Modellen, Diensten usw. verknüpfen
- Automatisierte Problembehebung in großem Maßstab mit vorgefertigten Skripten, Workflows und No-Code-Builder für unbeaufsichtigte oder zustimmungsbasierte Korrekturen
- Verbesserung der Endpoint-Performance mithilfe gerätespezifischer Experience-Scores, Trend-Dashboards und Vergleichen mit Referenzwerten
- Vorkonfigurierte Aktionsbibliothek mit Datensammlern, Skripten und Workflows für unternehmensspezifische Aktionen

** Als Add-on erhältlich*

BitLocker Management

- Automatisierte Verschlüsselung ausgewählter Laufwerke oder kompletter Festplatten zum Schutz von Computerdaten
- Erkennung von Computern mit TPM und Erhöhung der PIN-Sicherheit durch Kombination mit Passphrase-Authentifizierung
- Wiederherstellung von Daten bei Hardware-Defekten über Wiederherstellungsschlüssel sowie Zurücksetzen von Passwörtern für entfernte Computer
- Durchsetzung von Verschlüsselungsrichtlinien und Unterstützung von Compliance-Vorgaben wie FISMA, HIPAA und PCI DSS

Next-Gen Antivirus

- Schutz vor neuen Bedrohungen durch KI-unterstützte Malware-Erkennung in Echtzeit
- Umfassende forensische Analyse 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
- Umgehende Reaktion auf Angriffe, um diese schnell zu neutralisieren – inklusive Ransomware-Schutz
- Gewährleistung der Geschäftskontinuität durch eine Bedrohungsabwehr, die den Netzwerkbetrieb nur minimal unterbricht
- Wiederherstellung kompromittierter Dateien mit wenigen Klicks

Kontakt

Weitere Informationen

www.manageengine.de/endpointcentral

Ihr ManageEngine-Partner:

MicroNova
Technology Intelligence

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

ManageEngine