opentext™

Datenblatt

ZENworks Endpoint Security Management

Schützen Sie Ihre anfälligsten IT-Assets über eine zentrale Konsole: Dank unserer richtlinienbasierten Lösung mit Standorterkennungsfunktion können Sie auf allen PCs den Schutz vor Malware-Bedrohungen und die Sicherheit von Daten gewährleisten, die Weitergabe von und den Zugriff auf Informationen kontrollieren sowie den Status von Endgeräten überwachen und aufrechterhalten.

Produkthighlights

Dank OpenText ZENworks Endpoint Security Management profitieren Sie von umfassender, richtlinienbasierter Kontrolle über sämtliche Windows-Desktop-PCs und Mobilgeräte und haben zum Beispiel die Möglichkeit, die Sicherheitskonfigurationen abhängig von Rolle und Standort eines Benutzers zu ändern. Durch die Erstellung und Verwaltung von Richtlinien von einer zentralen Konsole aus ermöglicht OpenText ZENworks die Implementierung und Durchsetzung streng kontrollierter und überaus anpassungsfähiger Sicherheitsrichtlinien, wobei kein Eingriff seitens der Endbenutzer erforderlich ist. ZENworks Endpoint Security Management beinhaltet zudem nicht nur zuverlässige Client Self Defence-Funktionen, die dafür sorgen, dass Sicherheitsrichtlinien nicht umgangen werden, sondern auch eine komplette Suite mit Überwachungs-, Benachrichtigungs-, Reporting- und Auditing-Tools.

Hauptvorteile

ZENworks Endpoint Security Management bietet Ihrem Unternehmen zahlreiche Vorteile:

- Ihre anfälligsten IT-Assets, die mobilen PCs in der Peripherie Ihres Unternehmens, werden durch umfassende, zentralisierte Sicherheit geschützt.
- Da Endbenutzer nicht mehr für das Konfigurieren und Verwalten der Sicherheitseinstellungen und -lösungen auf ihren eigenen Geräten verantwortlich sind, können sie produktiver arbeiten.
- Die verschiedenen Komponenten der Endgerätesicherheit werden auf allen PCs Ihres Unternehmens von einer zentralen Konsole aus verwaltet.
- Richtlinien und Beschränkungen der Endgerätesicherheit können benutzer-, standort- und geräteabhängig angepasst werden.
- Nie wieder schlaflose Nächte, denn die Kontrolle über das Definieren, Durchsetzen und Aufrechterhalten der Sicherheit von Endgeräten ruht in den Händen Ihrer Sicherheitsexperten und fällt nicht mehr in die Zuständigkeit unerfahrener Benutzer.
- Im Zusammenspiel mit der OpenText ZENworks Suite lassen sich über eine einheitliche Konsole für das Konfigurations-, Patch-, Asset- und Endpoint Security Management sowohl der Lebenszyklus als auch die Sicherheit von Endgeräten verwalten (wobei es möglich ist, die Konsole als virtuelle Appliance bereitzustellen).

Hauptfunktionen

Schutz vor Malware-Bedrohung

ZENworks Endpoint Security Antimalware schützt Windows-Desktops, Server und mobile PCs gegen bekannte und unbekannte (Zero-Day-)Malware-Angriffe. Dies umfasst:

- Anti-Malware-Engine-Technologien, die durch mehrere Erkennungsprozesse einen mehrschichtigen Sicherheitsansatz bieten. Herkömmliche signaturbasierte Erkennung schützt gegen bekannte Angriffe, generische Erkennung schützt gegen bekannte Bedrohungsvarianten und ausgefeilte heuristische Analysen schützen gegen unbekannte Zero-Day-Angriffe.
- Malware-Erkennung in Echtzeit beim Kopieren, Verschieben, Öffnen oder Ausführen von Dateien.

Systemanforderungen

Genaue Angaben zum Produkt und zu den Systemanforderungen erhalten Sie unter: **www.microfocus.com/de-de/products/zenworks/specs**

- Scannen von lokalen und Netzlaufwerkstandorten zu geplanten Zeiten oder beim manuellen Start.
- Scannen von Wechseldatenträgern beim Wechselvorgang.
- Desinfizierung, Quarantäne oder Löschung infizierter und verdächtiger Dateien.
- Konfiguration des gesamten Malware-Schutzverhaltens von Endgeräten über die zentrale Verwaltungskonsole.
- Überwachung des Malware-Status von Geräten und Erkennung von Bedrohungen über Dashboards in der zentralen Verwaltungskonsole.

Sicherheit von USB- und Storage-Geräten

ZENworks Endpoint Security Management wartet mit zuverlässigen Funktionen auf, die die ordnungsgemäße Verwendung von Wechseldatenträgern gewährleisten. Dies umfasst:

- Schutz vor Datendiebstahl: Beinhaltet die Möglichkeit, Wechseldatenträger jeglicher Art (einschließlich USB-, WPD-, Disketten-, CD-/DVD- und ZIP-Laufwerke, MP3-Player und Flash-Speicher, SCSI- und PCMCIA-Karten) zu aktivieren oder deaktivieren bzw. als schreibgeschützt zu definieren.
- Erstellung detaillierter Positivlisten: Ermöglicht Administratoren die Kontrolle über die Verwendung von USB- und WPD-Geräten.
- Vermeidung nicht prüfbarer Transaktionen: Unterbindet die Verwendung lokaler Storage-Geräte, auf die Dateien kopiert werden können, ohne dass dies im Audit-Protokoll festgehalten wird.
- Kontrollen für optische Schreibeinheiten (DVD/CD) und Diskettenlaufwerke: Hiermit kann der Zugriff zugelassen oder unterbunden bzw. nur schreibgeschützter Zugriff erlaubt werden.
- AutoPlay-/AutoRun-Steuerung: zentralisierte Kontrolle der AutoPlay- und AutoRun-Funktionen im gesamten Unternehmen.

Datenverschlüsselung

Mit ZENworks Endpoint Security Management können Sie Wechseldatenträger und Ordner auf Festplatten auf allen Endgeräten verschlüsseln. Dies umfasst:

- Verschlüsselung mit nativen Microsoft-Technologien anstelle von zusätzlichen Verschlüsselungstreibern: Bei der Verschlüsselung von Wechseldatenträgern kommt BitLocker zum Einsatz, bei Ordnern auf Festplatten das Encrypting File System (EFS).
- Zentrale Schlüsselverwaltung für die Wiederherstellung verschlüsselter Dateien durch den Administrator.
- Authentifizierung für Wechseldatenträger, mit der verschlüsselte Wechseldatenträger auf allen Geräten oder nur auf von ZENworks verwalteten Geräten entsperrt werden können.
- Optionale Authentifizierung für Ordner auf Festplatten, bei der nach der Windows-Anmeldung ein zweites Passwort eingegeben werden muss, bevor auf verschlüsselte Ordner zugegriffen werden kann.

Wireless Security

Mit ZENworks Endpoint Security Management haben Sie die Kontrolle darüber, wo, wann und wie die Benutzer auf Drahtlosnetzwerke zugreifen. Dies umfasst:

- Wi-Fi-Management: Erstellung von Positiv- und Negativlisten für drahtlose Zugriffspunkte und Implementierung von Richtlinien, die in bestimmten Situationen die Wi-Fi-Kommunikation deaktivieren oder unterbinden.
- Wi-Fi-Sicherheitskontrollen: Beschränkung der Wi-Fi-Verbindungen auf drahtlose Zugriffspunkte, die die erforderlichen Verschlüsselungsstandards erfüllen.
- Wi-Fi-Adapter-Sperre: Endgeräte können ausschließlich über vom Unternehmen genehmigte Wi-Fi-Adapter auf drahtlose Zugriffspunkte zugreifen.

Port-Kontrolle

ZENworks Endpoint Security Management bietet nicht nur Wi-Fi-Sicherheit, sondern auch umfassenden Schutz für alle anderen Arten von drahtgebundenen und drahtlosen Port- und Kommunikationsgeräten, darunter LAN, USB, 1394 (Firewire), serielle und parallele Ports, Modems sowie Bluetooth- und Infrarot-Verbindungen (IrDA).

VPN-Durchsetzung

Um die Sicherheit zu erhöhen, wenn Geräte eine Verbindung zu offenen Netzwerken herstellen oder von einem externen Standort aus auf Ihr internes Netzwerk zugreifen müssen, bietet ZENworks Endpoint Security Management die Möglichkeit der VPN-Durchsetzung. Neben der Gewährleistung einer sicheren Verbindung über VPN bietet diese Funktion Schutz vor „Evil Twin"-Angriffen und unterbindet risikobehaftetes Endnutzerverhalten wie Split-Tunneling.

Anwendungskontrolle

Die Anwendungskontrolle von ZENworks Endpoint Security Management ermöglicht Ihnen die präzise, richtlinienbasierte Kontrolle aller Anwendungen, die auf den Endgeräten ausgeführt werden. Dies umfasst:

- Negativlisten für Anwendungen: Schädliche oder unerwünschte Anwendungen werden gesperrt.

Stets das Neueste erfahren

- Standortbasierte Anwendungskontrolle: Hiermit können Sie abhängig vom Sicherheitsstatus des Benutzerstandorts die Ausführung bestimmter Anwendungen erlauben oder unterbinden und den Zugriff aufs Netzwerk blockieren.
- Prüfen der Virenschutz- und Spyware-Integrität: Hiermit wird die ordnungsgemäße Ausführung aller Sicherheitsanwendungen überprüft. Nicht-konforme Geräte werden in Quarantäne verschoben, und es werden entsprechende Gegenmaßnahmen eingeleitet.

Erweiterter Firewall-Schutz

Im Gegensatz zu herkömmlichen Firewalls auf Anwendungsebene oder auf der Basis von Hook-Treibern befindet sich ZENworks Endpoint Security Management in der NDIS-Schicht (Network Driver Interface Specification) der einzelnen Netzwerkschnittstellenkarten (NICs). Dies gewährleistet umfassende Sicherheit, sobald Daten auf einen PC übertragen werden. ZENworks Endpoint Security Management umfasst die folgenden besonderen Firewall-Funktionen:

- Stateful-Firewall: Es werden ausschließlich erwünschte Daten auf das Gerät übertragen.
- Regeln für TCP-/UDP-Ports sowie Zugriffssteuerungslisten (ACLs): Ermöglichen die umfassende Verwaltung und Steuerung des Firewall-Verhaltens auf bestimmten Geräten.
- Standortbasierte Steuerung des Firewall-Verhaltens: Abhängig von der relativen Sicherheit des Gerätestandorts werden automatisch unterschiedliche Port-Regeln und Zugriffssteuerungslisten angewendet.
- Zentralisierte, richtlinienbasierte Kontrolle: Firewall-Einstellungen können nicht von Endbenutzern oder unbefugten Administratoren deaktiviert oder umgangen werden.
- Echte Quarantäne-Funktionen: Selbst wenn die Sicherheitsintegrität eines PCs gefährdet ist, bleibt Ihr Netzwerk geschützt.

opentext™