OpenText Core Endpoint Protection

Hochwirksamer Echtzeitschutz für Benutzer überall

Vorteile

- Vollständiges Remote-Endpoint-Management und -Kontrolle
- Hochgradig automatisierter, kostengünstiger Betrieb
- Problemlose Bereitstellung
- Überlegene Wirksamkeit gegen Zero-Day-Bedrohungen
- Speziell entwickelte Lösungen für Managed Service Provider und kleine und mittelständische Unternehmen

Unternehmen jeder Größe sind ständigen Angriffen ausgesetzt. Angesichts der Vielfalt, des Umfangs und der Geschwindigkeit der Angriffe ist es wichtiger denn je, Malware, Ransomware, Phishing, Cryptomining und andere schädliche Angriffe auf Ihre Benutzer und Systeme zu stoppen.

OpenText Core Endpoint Protection löst diese Probleme und mehr mit einer preisgekrönten, intuitiven Verwaltungskonsole. Mit über 40 Integrationen von Drittanbietern, einer RESTful-API sowie vollständig automatisierter Erkennung, Prävention und Behebung von Endpunktbedrohungen bietet OpenText umfassenden Endpunktschutz als Ergänzung zur Cyber-Resilienz-Strategie eines Unternehmens. OpenText nutzt die Leistungsfähigkeit von Cloud Computing und Machine Learning in Echtzeit, um die Endgeräteabwehr jedes Systems kontinuierlich zu überwachen und an die spezifischen Bedrohungen anzupassen, von denen Endbenutzer oder Systeme bedroht sind.

Ein proaktiver, vorausschauender und mehrschichtiger Sicherheitsansatz

OpenText Core Endpoint Protection basiert auf der BrightCloud Threat Intelligence-Plattform von OpenText. Die Plattform kombiniert das Beste aus künstlicher Intelligenz und maschinellem Lernen, um Unternehmen bei der Bekämpfung der sich schnell verändernden Bedrohungslandschaft zu unterstützen. Mehr als 140 Netzwerk-, Sicherheits- und Technologieanbieter vertrauen auf BrightCloud.

Dank dieser erstklassigen Bedrohungsinformationen bietet der Schutz von OpenText mit mehreren Schutzschilden Echtzeit-Verhaltensanalysen, Kernsystem-, Webbedrohungs-, Identitäts-, Phishing-, Umgehungs- und Offline-Schutzmaßnahmen zur Erkennung, Prävention und Abwehr komplexer Angriffe. Die patentierte OpenText Evasion Shield-Technologie erkennt, blockiert und behebt (Quarantäne) schwer zu erkennende Skriptangriffe, unabhängig davon, ob diese dateibasiert, dateilos, verschleiert oder verschlüsselt sind. Außerdem verhindert sie mit ihrem Script Shield die Ausführung bösartiger Verhaltensweisen in PowerShell, JavaScript und VBScript.

Überwachen, protokollieren und isolieren Sie Infektionen – auch wenn ein Endgerät offline ist

Im Gegensatz zu herkömmlichen Ansätzen, bei denen nur eine einzige Möglichkeit besteht, eine Bedrohung zu erkennen und zu stoppen, funktioniert der Schutz der nächsten Generation von OpenText in drei Stufen:

1. Er verhindert vorausschauend, dass Malware in das System eindringt. Anschließend schützt er vor der Ausführung von Malware und unbekannten Dateien, die verdächtiges Verhalten zeigen.
2. Der Schutz von OpenText überwacht die Aktivitäten der Datei und protokolliert sie, bis sie ordnungsgemäß klassifiziert werden kann, falls eine zuvor unbekannte Datei (z. B. eine potenzielle Infektion) ausgeführt wird.
3. Alle Änderungen an lokalen Laufwerken werden automatisch auf den Zustand vor der Infektion zurückgesetzt, wenn die Datei als Bedrohung eingestuft wird.

Diese mehrstufige Strategie ist nicht nur wirksamer gegen moderne Bedrohungen, sondern reduziert auch die Wahrscheinlichkeit von Fehlalarmen. Es müssen keine Signaturen oder Definitionen aktualisiert werden, da die Bedrohungsprävention in Echtzeit über die Cloud erfolgt. Die Updates des OpenText-Agenten erfolgen automatisch, dauern in der Regel drei Sekunden und sind für den Benutzer vollständig transparent.

Infektionswarnungen und -behebungen erfolgen automatisch, während regelmäßige Berichte hinsichtlich Inhalt, Zeitpunkt und Verbreitung geplant werden. Unsere cloudbasierte Verwaltungskonsole bietet Ihnen Transparenz und Kontrolle über alle Geräte, auf denen der OpenText-Agent installiert ist. Sie können mehrere Standorte und Standorte verwalten und leistungsstarke Remote-Agent-Befehle nutzen. Ein wesentlicher Vorteil unseres cloudbasierten Ansatzes besteht darin, dass die intensive Verarbeitung der Malware-Erkennung und -Analyse in der Cloud erfolgt.

Verbesserte Ausfallsicherheit durch intuitive, automatisierte Cybersicherheit

OpenText-Lösungen unterstützen Ihr Unternehmen dabei, cyberresilient zu bleiben. OpenText-Lösungen helfen Ihnen, Bedrohungen durch schnelle Erkennung, Reaktion und Datenwiederherstellung zu verhindern und sich davor zu schützen. Außerdem unterstützen sie Ihr Unternehmen dabei, sich an veränderte Vorschriften anzupassen und diese einzuhalten.

OpenText Core Endpoint Protection bietet erweiterten Schutz vor den ständig zunehmenden und sich weiterentwickelnden modernen Angriffen. Dank der automatisierten Endpunktsicherheit benötigen Sie keine dedizierten IT-Sicherheitsressourcen oder Experten mehr, um die digitale Fitness Ihres Unternehmens sicherzustellen. Dies bedeutet weniger Infektionen und sicherheitsrelevante Vorfälle – ganz zu schweigen von weniger Reparaturfällen und Produktivitätsverlusten.

Unterstützung der Sicherheitsbeauftragten mit fortschrittlichen Richtlinien

OpenText bietet die wesentlichen Tools, die die Cybersicherheit von Unternehmen erheblich verbessern. Unsere Tools schützen und unterstützen Sicherheitsbeauftragte mit umsetzbaren Erkenntnissen und flexiblen Reaktionsoptionen. Zu unseren neuesten Funktionen gehören:

- **Isolierung von Geräten:** Im Falle einer Bedrohung ist es von entscheidender Bedeutung, deren Ausbreitung im Netzwerk zu verhindern. Mit unserer Geräteisolierungsfunktion können Sie betroffene Geräte schnell isolieren, die Ausbreitung von Malware stoppen und gleichzeitig die wichtige Kommunikation aufrechterhalten. Diese Funktion ist für die schnelle Eindämmung und Untersuchung von Bedrohungen sowie für den Schutz der Integrität Ihres Netzwerks von entscheidender Bedeutung.
- **Prozessbaum-Visualisierung:** Für eine effektive Cybersicherheit ist es entscheidend, das „Wie“ und „Wo“ einer Bedrohung zu verstehen. Mit der Prozessbaum-Visualisierung erhalten Verteidiger forensische Einblicke in Systeme. Mit dieser Funktion können Sie die Ursprünge und Pfade von Prozessen verfolgen und erhalten so einen klaren Überblick über potenzielle Bedrohungen.

Diese schlanken, aber leistungsstarken Erweiterungen Ihres Sicherheitstoolkits sind wesentliche Komponenten, die Ihnen dabei helfen können, die Anforderungen Ihrer Cyberversicherung zu erfüllen. Sie stehen für das Engagement von OpenText, Lösungen anzubieten, die Schutz bieten, ohne unnötige Komplexität zu verursachen oder Ihre Abläufe zu verlangsamen.

OpenText Cybersecurity bietet umfassende Sicherheitslösungen für Unternehmen und Partner jeder Größe. Von Prävention, Erkennung und Reaktion bis hin zu Wiederherstellung, Untersuchung und Compliance: Unsere einheitliche End-to-End-Plattform unterstützt Kunden dabei, mit einem ganzheitlichen Sicherheitsportfolio ihre Cyberresilienz zu verbessern. Basierend auf praxisbezogenen Erkenntnissen aus unseren kontextrelevanten Echtzeitinformationen zu Cyberrisiken profitieren Kunden von OpenText Cybersecurity von hochwirksamen Produkten, Einhaltung aller Compliance-Vorschriften und einer einfachen Sicherheitslösung, die sie bei der Verwaltung von Unternehmensrisiken unterstützt.

ELOVADE

Kontaktdaten für Deutschland & Österreich:
ELOVADE Deutschland GmbH
security@elovade.com
DE: +49 6441 67118 842
elovade.com/opentext-cybersecurity
AT: +43 820 0010 36

Kontaktdaten für die Schweiz:
ELOVADE Swiss AG
sales@elovade.ch
CH: +41 55 552 27 92
elovade.ch/opentext-cybersecurity