DATENBLATT

ADVANCED EPDR FÜR LINUX

BEDROHUNGEN VON LINUX FERNHALTEN

Das Linux-System macht bereits 15 bis 20 % des Servermarktes aus und wird in ca. 40 % der Website-Server eingesetzt. Seine Präsenz in Unternehmensinfrastrukturen nimmt weiter zu, während Cyberangriffe auf diese Systeme immer häufiger und schwerwiegender werden. Daher ist der Schutz von Linux-basierten Servern und Workstations für Unternehmen von entscheidender Bedeutung.

WatchGuard Advanced EPDR vereinfacht die Sicherheitspraktiken für Linux-Systeme, indem es eine zentrale Verwaltung der gesamten Endpoint-Sicherheit und den vollständigen Schutz von Unternehmen jeder Größe, Branche oder Komplexität ermöglicht.

Die Sicherheits- und Verwaltungsfunktionen von WatchGuard Advanced EPDR für Linux wurden von Grund auf neu entwickelt und ausschließlich für Linux optimiert. Sie basieren auf Funktionen, die speziell auf Linux ausgerichtet sind, um die Anforderungen von Sicherheitsteams zu erfüllen, von Leistung bis hin zu Prävention, Erkennung und automatisierter Reaktion auf Bedrohungen.

Der einzelne **ressourcensparende Agent** von WatchGuard Advanced EPDR unterstützt die meisten Linux-Distributionen bei minimalem **Ressourcenverbrauch, wodurch die Auswirkungen auf das System selbst reduziert werden.**

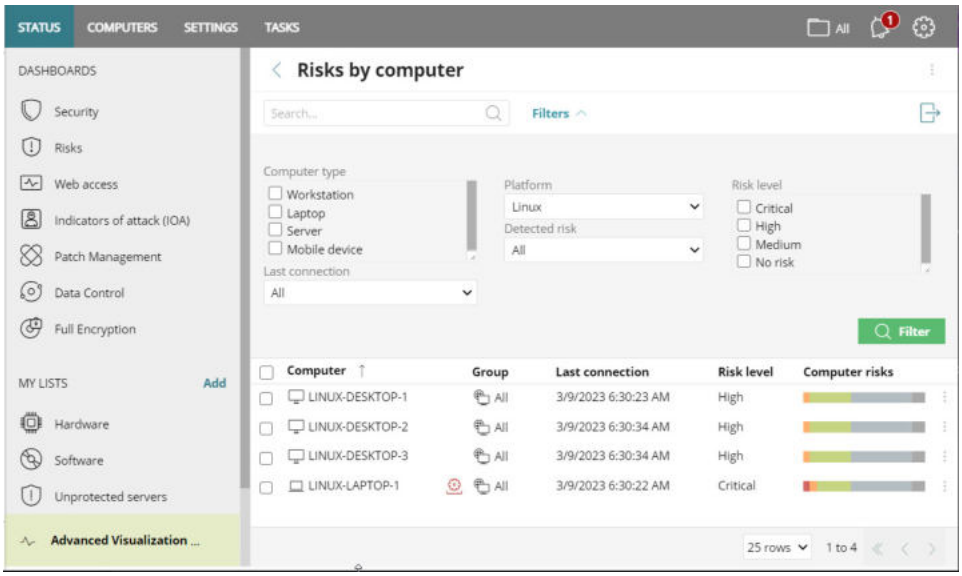

Abbildung 1. WatchGuard Advanced EPDR zentralisiert und verstärkt die Sicherheit aller Endpoints, einschließlich Linux OS.

Cyberkriminelle haben das Linux-Betriebssystem ins Visier genommen

Es gibt zwei Arten von Angriffen auf Linux-Endpoints, über die sich Unternehmen am meisten Sorgen machen sollten:

Ransomware-Angriffe auf virtuelle Maschinen

Ransomware hat sich zu einer der Haupteinnahmequellen für cyberkriminelle Gruppierungen entwickelt. Sie gehen nicht nur wahllos gegen Windows-Rechner vor, sondern haben auch damit begonnen, Strategien zur Verschlüsselung von Linux-basierten Installationen zu entwickeln, da dieses Betriebssystem am häufigsten auf firmeneigenen und Cloud-Servern eingesetzt wird

Cryptojacking

Unter Cryptojacking versteht man das Hacken von Systemen, um unter Ausnutzung der Ressourcen eines Rechners Kryptowährungen zu schürfen. Dies ist einer der am weitesten verbreiteten Cyberangriffe auf Linux-Systeme. Er ermöglicht es Angreifern, sich direkte Vorteile zu verschaffen, und kann von Opfern relativ unbemerkt bleiben, die sich erst Sorgen machen, wenn der Leistungsverlust ihrer Rechner offensichtlich wird.

WatchGuard Advanced EPDR bietet – ohne die Notwendigkeit einer kostspieligen Infrastruktur – zentrale Verwaltungs- und erweiterte Sicherheitsfunktionen, die die folgenden Vorteile mit sich bringen.

Betriebliche Effizienz:

- Zentrale Verwaltung – Benutzerfreundlichkeit in gemischten IT-Umgebungen: Windows, Linux, macOS, Android und iOS
- Flexible Bereitstellung: Unterstützung auch befestigter oder isolierter Umgebungen unter Nutzung der „No-Deps“ -Version und nativer Proxy-Funktionen
- Kontinuierliche Risikobewertung unter Berücksichtigung des Endpoint-Sicherheitsstatus
- Einzel- oder Gruppen-Sicherheitseinstellungen von Workstations, Servern und Kunden für MSPs
- E-Mail-Benachrichtigungen im Fall einer Infektion und bei Entdeckung ungeschützter Endpoints
- Hardware- und Software-Bestandsführung
- Hohe Leistung – speziell entwickelt, um Auswirkungen auf andere Programme und die allgemeine Leistung des Systems zu minimieren

Überlegener Schutz vor und Erkennung von Zero-Day- und Ransomware-Angriffen:

- Vorbeugender Virenschutz (Antivirus, AV) gegen bekannte Malware durch Auswertung des minutengenauen cloudbasierten Bedrohungswissens von WatchGuard, Collective Intelligence (CI)
- Die CI von WatchGuard wird automatisch aus mehreren Informationsquellen für Bedrohungen angereichert. Eine Quelle ist der Zero-Trust Application Service von WatchGuard, der von Millionen geschützter Endpoints auf der ganzen Welt mit Daten versorgt wird.
- Kontextbasierte Erkennung von Angriffen ohne Malware
- Threat Hunting Service, der automatisch Angriffsindikatoren (Indicators of Attack, IoAs) im Zusammenhang mit Living-off-the-Land(LotL)-Techniken erkennt
- Dem MITRE ATT&CK-Framework zugeordnete IoAs
- Automatisierte Eindämmung und Abhilfe durch Entfernen von Malware
- Untersuchungsbereich für IoAs und verdächtiges Verhalten
- Zugriff auf angereicherte Telemetrie, bei der MITRE ATT&CK-Taktiken und -Techniken verdächtigen Ereignissen zugeordnet werden

Verkürzte Reaktionszeit:

- Automatisierte Entfernung von Malware
- On-Demand- und geplante Scans über die zentrale cloudbasierte Konsole
- On-Demand-Neustart von Computern
- Remote Shell zur Verwaltung von Prozessen und Diensten, Dateiübertragungen, Befehlszeilentools, Dump-Abrufen, pcap und mehr

REDUZIERUNG DER ANGRIFFSFLÄCHE VON ORGANISATIONEN. SCHUTZ VON LINUX-SERVERN UND -WORKSTATIONS

Unterstützte Systeme und Distributionen innerhalb der Endpoint-Sicherheitsplattform für Linux:

WatchGuard Advanced EPDR

Linux-Systemanforderungen

Unterstützte Linux-Distributionen

[i] Laut Fortune Business Insights, https://www.fortunebusinessinsights.com/server-operating-system-market-106601, hat Linux einen Marktanteil von 21,8 % bei den Server-Betriebsumgebungen, und basierend auf W3techs wird Linux von 38,8 % aller Websites verwendet: https://w3techs.com/technologies/comparison/os-linux,os-windows

[ii] https://www.watchguard.com/wgrd-resource-center/feature-brief/zero-trust-application

VERTRIEB USA +1.800.734.9905 E-MAIL strategic.accounts@watchguard.com INTERNET www.watchguard.com/de WatchGuard Technologies, Inc.