

# WATCHGUARD EPP

Starke Endpoint Protection-Plattform



## HERAUSFORDERUNGEN BEI DER CYBERSICHERHEIT

Bei den kontinuierlichen Bemühungen, Ihr Unternehmen zu schützen, stellen Endpoints ein beliebtes Angriffsziel für Cyberkriminelle dar. Daher ist es wichtiger als je zuvor, alle Endpoints zu schützen und zu überwachen, an denen sensible Daten verarbeitet werden und die mit Systemen innerhalb und außerhalb des Unternehmensnetzwerks verbunden sind.

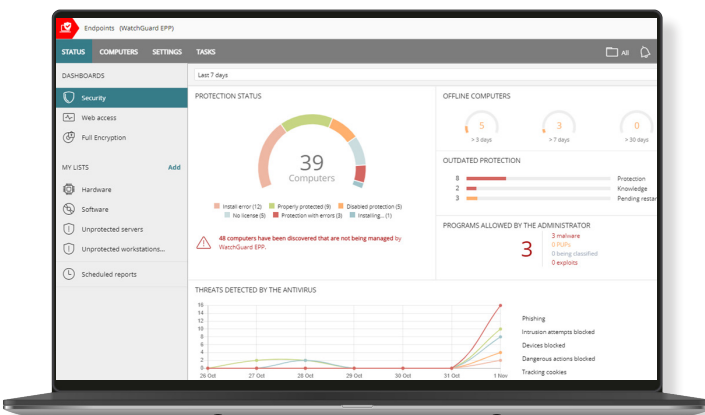
Letztes Jahr wurden tagtäglich mehr als 350.000 neue Schadprogramme registriert. Hacker konzentrieren sich auf anfällige Endpoints, auf denen Unternehmen ihre wertvollsten Ressourcen speichern. Warum? Wie so oft lautet auch hier die Antwort: wirtschaftlicher Gewinn. Malware und Ransomware zählen zu den am häufigsten auftretenden Sicherheitsbedrohungen, obwohl die direkten Kosten paradoxerweise nicht das Hauptproblem sind. Das größte Problem sind die Ausfallzeiten, die dadurch verursacht werden. Daher werden Unternehmen dazu gezwungen, Maßnahmen zu ergreifen, um die Sicherheit zu erhöhen.

## SCHÜTZEN SIE IHR UNTERNEHMEN VOR MALWARE UND RANSOMWARE

Da Unternehmen immer neuen Arten von Malware und anderen Bedrohungen ausgesetzt sind, müssen sie ihr Sicherheitskonzept überarbeiten und neue Ansätze umsetzen, um die Auswirkungen möglicher Angriffe zu verringern.

WatchGuard EPP ist eine effektive cloudnative Sicherheitslösung, die den Virenschutz der nächsten Generation für all Ihre Desktop-PCs, Laptops und Server mit Windows, MacOS und Linux sowie für die führenden Virtualisierungssysteme iOS- und Android-Geräte zentralisiert.

Er beinhaltet verschiedene EPP-Technologien, um Malware, Ransomware und die neuesten Bedrohungen abzuwehren. Eine dieser Technologien prüft WatchGuard Threat Intelligence in Echtzeit. Dabei handelt es sich um ein riesiges Repository, das die neuesten Algorithmen für maschinelles Lernen nutzt, um Angriffe schneller zu erkennen.



## VORTEILE

### Sicherheit für verschiedene Plattformen

- Schutz vor unbekanntem, komplexen Bedrohungen: erkennt und wehrt Malware, Trojaner, Phishing und Ransomware ab.
- Automatische Analyse und Virenentfernung auf Computern. Verhaltensanalyse, um bekannte und unbekannte Malware zu erkennen.
- Plattformübergreifende Sicherheit: Windows-Systeme, Linux, macOS, iOS, Android und virtuelle Umgebungen (VMware, Virtual PC, MS Hyper-V, Citrix). Verwaltung von Lizenzen, die zu einer persistenten und nicht-persistenten Virtualisierungsinfrastruktur (VDI) gehören.

### Einfache Verwaltung

- Wartungsfreundlich: zum Hosten der Lösung ist keine spezifische Infrastruktur erforderlich und die IT-Abteilung kann sich auf wichtigere Aufgaben konzentrieren.
- Einfache Bereitstellung: verschiedene Bereitstellungsmethoden, automatische Deinstallation von Konkurrenzprodukten, um die schnelle Migration von Lösungen von Drittanbietern zu vereinfachen.
- Lernfähig: intuitive, einfache, webbasierte Verwaltungsschnittstelle, bei der oft genutzte Optionen mit einem Klick zur Verfügung stehen.

### Kompromisslos leistungsfähig

- Netzwerk-, Speicher- und CPU-Nutzung des Agents sind sehr gering, da alle Abläufe in der Cloud stattfinden.
- WatchGuard EPP erfordert keine Installation. Die schlanke Anwendung wirkt sich nicht auf die Endpoint-Leistung aus. Sie vereinfacht die Sicherheitsverwaltung und erhöht die betriebliche Effizienz.

## ZENTRALE GERÄTESICHERHEIT

Zentrale Verwaltung aller Sicherheits- und Produkt-Updates für alle Workstations und Server im Unternehmensnetzwerk. Verwalten Sie den Schutz von Windows-, Linux-, macOS-, iOS- und Android-Geräten über eine zentrale, webbasierte Verwaltungskonsole.

## SCHUTZ VOR MALWARE UND RANSOMWARE

WatchGuard EPP analysiert Verhalten und Hacking-Techniken, um sowohl bekannte als auch unbekannte Malware, Ransomware, Trojaner und Phishing zu erkennen und zu stoppen.

## ERWEITERTE DESINFEKTION

Im Falle einer Sicherheitsverletzung können Unternehmen mit WatchGuard EPP betroffene Computer schnell in einen Zustand vor der Verletzung zurückversetzen, wobei fortschrittliche Tools für Desinfektion und Quarantäne genutzt werden, um verdächtige und gelöschte Elemente zu speichern.

Zudem haben Administratoren die Möglichkeit, Workstations und Server remote neu zu starten, um sicherzustellen, dass die neuesten Produkt-Updates installiert sind.

## ECHTZEIT-ÜBERWACHUNG UND BERICHTE

Die detaillierte Überwachung der Sicherheitsumgebung erfolgt über ein umfassendes Dashboard und übersichtliche Grafiken.

Es werden automatisch Berichte zum Schutzstatus, zur Erkennung und unsachgemäßen Nutzung von Geräten generiert und bereitgestellt.

## DETAILLIERTE KONFIGURATION VON PROFILEN

Sie haben die Möglichkeit, spezifische Schutzrichtlinien für verschiedene Anwenderprofile festzulegen, damit für jede Anwendergruppe die beste Richtlinie verwendet wird.



## ZENTRALE GERÄTESTEUERUNG

Stoppen Sie Malware und Datenlecks, indem Sie Gerätekategorien sperren (Flash-Laufwerke, USB-Modems, Webcams, DVD/CD usw.), Geräte zu einer Whitelist hinzufügen oder Berechtigungen für Lesezugriff, Schreibzugriff oder Lese- und Schreibzugriff festlegen.

## SCHNELLE, FLEXIBLE INSTALLATION

Stellen Sie den Schutz per E-Mail mithilfe einer Download-URL bereit oder nutzen Sie das Distributionstool der Lösung, um den Schutz auf ausgewählten Endpoints umzusetzen. Das MSI-Installationsprogramm ist mit den Tools von Drittanbietern kompatibel (z. B. Active Directory, Tivoli, SMS usw.).

## MALWARE FREEZER

Malware Freezer verschiebt Malware für sieben Tage in Quarantäne und im Falle eines False Positive wird die betroffene Datei automatisch wieder im System hergestellt.

## RISK-MONITORING FÜR ENDPOINTS

Verwalten und überwachen Sie ungeschützte Endpoints, Angriffsindikatoren, fehlerhafte Sicherheitskonfigurationen, Schwachstellen im Betriebssystem und in der Software von Drittanbietern sowie fehlende Patches, um Ihr Netzwerk proaktiv zu schützen, bevor es zu einer Sicherheitsverletzung kommt.

## SCHWACHSTELLENANALYSE

Die Schwachstellenanalyse ist ein kritischer Prozess, der IT-Teams dabei unterstützt, Sicherheitslücken und Schwachstellen in Anwendungen und Systemen zu identifizieren, zu bewerten und zu priorisieren. Verstehen und identifizieren Sie potenzielle Bedrohungen und ergreifen Sie proaktive Maßnahmen, um sie zu entschärfen, bevor Sie von Angreifern ausgenutzt werden.

## BEHEBUNG VON RANSOMWARE UND WIEDERHERSTELLUNG

Um zu verhindern, dass korruptierte Systeme wiederhergestellt werden, versuchen Angreifer nicht nur Dateien zu verschlüsseln, sondern auch von Administratoren erstellte Sicherungs- und VSS-Dateien zu löschen und Dienste zu deaktivieren, die bei der Wiederherstellung unterstützen sollen.

Die Funktion für Schattenkopien nutzt die Technologie des Betriebssystems und schützt diese Dateien mit unserer Technologie für den Schutz vor Manipulation. So können Benutzer Daten nach einem Ransomware-Angriff wiederherstellen.

IT-Experten verwenden die Schattenkopien, um Dateien nach einem kritischen Systemausfall wiederherzustellen, allerdings eignet sich diese Technologie auch hervorragend zur Wiederherstellung von Dateien, die durch Ransomware verschlüsselt wurden.

### Unterstützte Plattformen und Systemanforderungen von Watchguard EPP

Unterstützte Betriebssysteme: [Windows](#), [macOS \(Catalina oder höher\)](#) und [Linux \(RedHat, CentOS und SUSE\)](#).

Liste kompatibler Browser: [Google Chrome](#), [Google Chrome](#), [Mozilla Firefox](#), [Microsoft Edge](#) und [Safari](#).