DATENBLATT

WatchGuard Endpoint Security Basic

Moderner EDR-Schutz. Kein Stress.

Heutzutage ist es für Unternehmen von entscheidender Bedeutung, über einen starken Endpoint-Schutz zu verfügen. Herkömmliche Antiviren-Tools reichen nicht mehr aus, um moderne Cyberangriffe zu stoppen, doch viele EDR-Plattformen (Advanced Endpoint Detection and Response) sind komplex, ressourcenintensiv und schwer zu verwalten.

WatchGuard Endpoint Security Basic ändert dies durch die Bereitstellung eines modernen, KI-gestützten EDR-Schutzes mit minimalem Verwaltungsaufwand. Die Lösung wurde für Unternehmen entwickelt, die zuverlässigen Schutz mit geringer Komplexität benötigen, und kombiniert Verhaltenserkennung, Schutz vor Ransomware und Reduzierung der Angriffsfläche in einer leichten, cloudverwalteten Lösung.

Mit automatisierter Klassifizierung, einer geringen Anzahl an Warnmeldungen und zentralisiertem Cloud-Management schützt Endpoint Security Basic Anwender, Geräte und Daten, ohne dass ein ständiges Tuning oder dedizierte Sicherheitsexpertise erforderlich sind.

Starker Schutz ohne Komplexität

WatchGuard ist sich bewusst, dass viele Unternehmen einfach einen zuverlässigen Schutz benötigen, der Anwender und Geräte schützt, ohne dass ein dediziertes Sicherheitsteam erforderlich ist.

Endpoint Security Basic wurde für Unternehmen entwickelt, die einen starken Schutz ohne Betriebsaufwand benötigen, und kombiniert intelligente Malware-Prävention, Schutz vor Ransomware und Kontrolle der Angriffsfläche in einer leichten, cloudverwalteten Lösung. Mit Sicherheitsüberwachung in Echtzeit und geringem Betriebsaufwand stoppt die Lösung Angriffe frühzeitig ohne ständiges Tuning oder manuelles Eingreifen.

Endpoint Security Basic bietet modernen Endpoint-Schutz mit KI-gesteuerten Präventionstechnologien, die Malware, Ransomware, bösartige Skripte und neue Bedrohungen sowie dateilose Angriffe und Living-off-the-Land-Techniken automatisch erkennen und blockieren. Integrierter Anti-Phishing-Schutz, Gerätesteuerung und URL Filtering tragen dazu bei, gängige Angriffspunkte zu reduzieren, bevor sich Bedrohungen durchsetzen können.

Da die Lösung über eine zentrale, cloudnative Plattform bereitgestellt wird, können Teams problemlos Richtlinien bereitstellen, die Sicherheit überwachen und den Schutz über alle Endpoints hinweg von einer einzigen Konsole aus verwalten. Das Ergebnis ist ein zuverlässiger Schutz, der Bedrohungen frühzeitig stoppt und gleichzeitig den Betriebsaufwand gering hält.

Endpoint Security Basic umfasst moderne Präventions- und Erkennungsfunktionen, die entwickelt wurden, um Angriffe frühzeitig zu stoppen.

Reduzierung der Angriffsfläche

- Anpassbares Dashboard mit Risiken für Endpoints
- Erkennung nicht verwalteter Endpoints
- Schwachstellenanalyse

Integrierte Präventionstechnologien

- Firewall, IDS und Gerätekontrolle
- Schutz für mehrere Angriffsvektoren (Web, E-Mail, Netzwerk, Geräte)
- Kollektive Intelligenz
- KI-gestützte Erkennung, die bösartige Installationsprogramme und Skripte identifiziert und blockiert
- Anti-Phishingschutz
- Scans zur Malware-Erkennung und on-Demand Scans
- URL Filtering und Webbrowsing

Funktionen für Erkennung und Reaktion

- Ständige Überwachung von Endpoints
- KI-gestützte Erkennung
- Kontextbasierte Verhaltenserkennung
- Blockiert automatisch Versuche, Schwachstellen in aktiven Prozessen auf dem Gerät auszunutzen
- Risikoüberwachung für Endpoints
- Integration von ThreatSync (XDR) für Transparenz
- Automatisierte Erstellung des Verlaufs von Vorfällen
- Wiederherstellung verschlüsselter Dateien (Schattenkopien)

Zuverlässiger Schutz. Leiser Betrieb.

Sicherheit mit dem Set-It-and-Forget-It-Ansatz

Endpoint Security Basic wurde entwickelt, um leise im Hintergrund zu arbeiten. Die KI-gestützte Klassifizierung analysiert automatisch die Aktivität und bestimmt, ob sie sicher oder bösartig ist, wodurch die Notwendigkeit einer ständigen Feinabstimmung oder Untersuchung entfällt.

Dieser Quiet-by-Design-Ansatz reduziert die Alarmermüdung und den Betriebsaufwand erheblich, sodass Teams einen starken Schutz aufrechterhalten können, ohne Zeit für die laufende Überwachung aufwenden zu müssen.

Zentrale Gerätesteuerung

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

Risikoüberwachung für Endpoints

Verwalten und überwachen Sie ungeschützte Endpoints, 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.

Schutz vor Malware and Ransomware

Endpoint Security Basic analysiert Verhaltensweisen und Hacking-Techniken, um bekannte und unbekannte Malware, einschließlich Ransomware, Trojanern und Phishing, zu erkennen und zu blockieren.

Echtzeit-Monitoring 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.

Integrierte Reduzierung der Angriffsfläche

Viele erfolgreiche Sicherheitsverletzungen beginnen mit nicht gepatchten Schwachstellen, nicht autorisierten Anwendungen oder unsicherem Webzugriff.

Endpoint Security Basic trägt dazu bei, diese Risiken durch integrierte Schwachstellenbewertungen, Gerätesteuerung und URL Filtering-Richtlinien zu reduzieren, die die Exposition gegenüber gängigen Angriffstechniken proaktiv begrenzen.

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.

Cloudnative Einfachheit

Endpoint Security Basic wird über die cloudnative Management-Plattform von WatchGuard verwaltet und bietet zentralisierte Richtlinien, Dashboards und Berichte über alle Endpoints hinweg.
Diese einheitliche Konsole vereinfacht den Betrieb, reduziert den Verwaltungsaufwand und ermöglicht es Unternehmen, Mitarbeiter überall zu schützen.

Informationen zu WatchGuard

WatchGuard Technologies ist ein weltweit führendes Unternehmen für einheitliche Cybersicherheit, das speziell für Managed Service Provider (MSPs) entwickelt wurde. Seit mehr als 30 Jahren definiert WatchGuard, wie MSPs Sicherheit in großem Maßstab bereitstellen, und entwickelt kontinuierlich Innovationen, um jeder größeren Veränderung in der Bedrohungslandschaft einen Schritt voraus zu sein. Die KI-gestützte Unified Security Platform® von WatchGuard bietet an Zero-Trust-Prinzipien ausgerichteten Netzwerk-, Endpoint- und Identitätsschutz in einer einzigen, integrierten Plattform, die es MSPs ermöglicht, die betriebliche Komplexität zu reduzieren, Sicherheitsergebnisse zu verbessern und ihr Geschäft effizienter auszubauen. WatchGuard genießt das Vertrauen von mehr als 25.000 MSPs, die weltweit über 1,5 Millionen Kunden schützen, und ermöglicht es Partnern, starke, messbare Sicherheitsergebnisse für Kunden auf der ganzen Welt zu liefern. Weitere Informationen finden Sie unter WatchGuard.com/de.

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49-206-596-1001 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB: www.watchguard.com/de
WatchGuard Technologies, Inc.