DATENBLATT

WatchGuard Endpoint Security-Produkte: Funktionen je nach Plattform

	WINDOWS (INTEL & ARM)	LINUX	MAC OS (INTEL & ARM)	ANDROID	iOS
ALLGEMEIN					
Webkonsole	■	■	■	■	■
Informationen in Dashboards	■	■	■	■	■
Filterbasierte Computer-Organisation	■	■	■	■	■
Gruppenbasierte Computer-Organisation	■	■	■	■	■
In der lokalen Konsole unterstützte Sprachen	11	11	11	16	10
LISTEN UND BERICHTE					
Häufigkeit, mit der Informationen zu Malware, PUPs und gesperrten Programmen an den Server gesendet werden	1 Min.	10 Min.	10 Min.	Sofort nach Abschluss des Scanvorgangs	–
Häufigkeit, mit der sonstige erkannte Probleme an den Server gesendet werden	15 Min.	15 Min.	15 Min.	Sofort nach Abschluss des Scanvorgangs	15 Min.
Liste der erkannten Probleme	■	■	■	■	■
Berichte für die Unternehmensleitung	■	■	■	■	■
Geplante Berichte für die Unternehmensleitung	■	■	■	■	■
SCHUTZ					
Manipulationsschutz	■				
Anti-Phishing	■		■		■
Dauerhafter Echtzeit-Virenschutz	■	■	■	■	
Kontextuelle Erkennung	■	■			
Netzwerkangriffsschutz	■				
Anti-Exploit	■*				
Zero-Trust Application Service (Hardening & Lock)	■				
Ständige Risikoüberwachung der Endpoints	■	■	■	■	■
Schattenkopien	■				
Decoy-Dateien	■				
Firewall	■				
URL-Filterung	■		■		■
Gerätesteuerung	■				
Suche nach STIX IOCs und YARA-Regeln	■				
Erweiterte Sicherheitsrichtlinien zur Verringerung der Angriffsfläche	■				
Diebstahlschutz				■	■

	WINDOWS (INTEL & ARM)	LINUX	MAC OS (INTEL & ARM)	ANDROID	iOS
ERKENNUNG					
Erkennung gefährdeter Treiber	■				
Erkennung von Codeinjektionen in laufenden Prozessen	■				
Threat Hunting Service: MITRE ATT&CK zugeordnete nicht-deterministische IoAs mit kontextueller Telemetrie	■				
ZeroTrust Application Service zur Klassifizierung aller nicht vertrauenswürdigen ausführbaren Dateien im System, um potenziell bösartige Anwendungen zu erkennen	■				
IoAs und Untersuchungsbereich für verdächtiges Verhalten	■	■	■		
Zugang zu angereicherter Telemetrie, bei denen MITRE ATT&CK-Taktiken und -Techniken verdächtigen Ereignissen zugeordnet werden	■	■	■		
Tiefgehende Dateianalyse	■				
Verbose-Modus für Angriffssimulation	■				
ANTWORT VON DER WEBKONSOLE					
On-Demand-Scans	■	■	■	■	–
Geplante Scans	■	■	■	■	–
Computerneustart	■	■	■		
Computerisolierung	■	■	■		
Remote Shell zur Verwaltung von Prozessen und Diensten, Dateiübertragungen, Befehlszeilentools, Dump-Abruf, pcap und anderen	■	■	■		
INFORMATIONEN ZU HARDWARE UND SOFTWARE					
Hardware	■	■	■	■	■
Software	■	■	■	■	■
Protokoll der Softwareänderungen	■	■	■	■	■
Informationen über installierte Betriebssystem-Patches	■				
Schwachstellenanalyse	■	■	■		
EINSTELLUNGEN					
Sicherheitseinstellungen für Workstations und Server	■	■	■	–	–
Passwörter zur Deinstallation des Schutzes und zur Ergreifung lokaler Maßnahmen	■				
Sicherheit für die Durchsetzung des Netzwerkzugriffs (erfordert Firebox)	■		■	■	
Durchsetzung des Netzwerkzugriffs auf WLAN über Access Points	■		■		
Sicherheit für VPN-Verbindungen (erfordert Firebox)	■		■	■	
Sicherer Zugang zum WLAN-Netzwerk über Access Points	■		■		
Sicherer Zugriff auf Endpoints von anderen Geräten aus	■				
Möglichkeit zur Festlegung mehrerer Proxys	■	■	■	–	–
Möglichkeit des Einsatzes als WatchGuard Proxy	■			–	–
Möglichkeit zur Nutzung des WatchGuard Proxys	■	■	■	–	–
Möglichkeit des Einsatzes als Repository/Cache	■			–	–
Möglichkeit zur Nutzung des Repository/Cache	■	■	■	–	–
Möglichkeit, Verbindungen von nicht autorisierten Endpoints zu blockieren	■				
Entdeckung ungeschützter Computer	■				
E-Mail-Warnmeldungen bei einer Infektion	■	■	■	■	■
E-Mail-Warnmeldungen bei der Entdeckung ungeschützter Computer	■	■	■	■	■

** Die Funktion steht unter Windows (Intel) und teilweise unter Windows (ARM) zur Verfügung.*

	WINDOWS (INTEL & ARM)	LINUX	MAC OS (INTEL & ARM)	ANDROID	iOS
REMOTE-AKTIONEN VON DER WEBKONSOLE					
Echtzeitaktionen	■	■	■	■	■
Ferninstallation des Agenten	■				
Möglichkeit zur erneuten Installation von Agent und Schutz	■				
Autorisierte Software nach Hash oder Programmeigenschaften	■				
Programmsperre nach Hash und Programmname	■				
UPDATES UND UPGRADES					
Signaturupdates	■	■	■	■	–
Schutzupgrades	■	■	■	■	–
Möglichkeit zur Planung von Schutzupgrades	■	■	■	Google Play	App Store
MODULE					
WatchGuard Advanced Reporting Tool	■	■	■		
WatchGuard Patch Management	■	■	■		
WatchGuard Data Control	■				
WatchGuard Full Encryption	■		■		
WatchGuard SIEMFeeder	■	■	■		
WATCHGUARD CLOUD					
Mehrstufige und mandantenfähige produktübergreifende Verwaltung	■	■	■	■	■
Zentrale Administration, umfassende Transparenz, Dashboard und Berichterstellung	■	■	■	■	■

Als Teil der Unified Security Platform-Architektur von WatchGuard bieten WatchGuard EPDR und Advanced EPDR folgende Plattformfunktionen:

THREATSYNC-XDR					
Produktübergreifende Korrelation und Erkennung von Sicherheitsdaten (Netzwerk- und Endpoint-Sicherheit)	■	■	■		
Score-basierte IOAs und Bedrohungspriorisierung	■	■	■		
Aktion zum Prozessabbruch	■				
Löschung und Wiederherstellung verdächtiger Programme	■				
Isolation und Isolationsstopp	■				
Automatisierte Antwortrichtlinien	■	■	■		

BETRIEBSSYSTEM

Kompatibilität des Betriebssystems für Endpoint-Sicherheitsfunktionen
Installationsvoraussetzungen
Browserkompatibilität

■ Funktionen in WatchGuard EPDR und WatchGuard Advanced EPDR
■ Funktionen exklusiv in WatchGuard Advanced EPDR

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 INTERNATIONALER VERTRIEB: +1.206.613.0895 WEB: www.watchguard.com/de WatchGuard Technologies, Inc.