CCS Media

WatchGuard EPDR

Endpoint Protection Detection and Response

Organisational Cybersecurity Challenges

Endpoints are the primary target for most cyberattacks and as the technology infrastructure becomes more complex, organisations are struggling to find the expertise and resources necessary to monitor and manage endpoint security risks. So, what types of challenges are companies facing when adopting endpoint security solutions?

Alert fatigue:

Organisations receive thousands of weekly malware alerts, of which only 19% are considered trustworthy, and only 4% of which are ever investigated. Two-thirds of cybersecurity admins' time is dedicated to managing malware alerts.

Complexity:

Too many disconnected cybersecurity tools can be hard to manage for security professionals, due to the number of enabling technologies, the lack of in-house skills, and the time needed to identify threats.

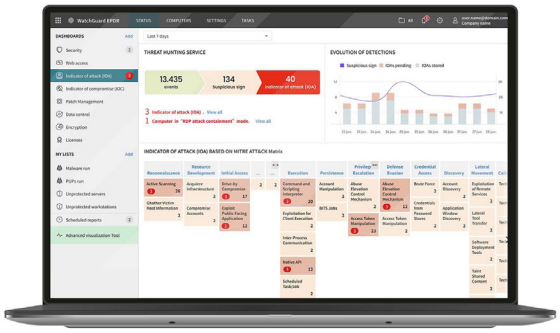
Poor performance:

Frequently endpoint security solutions require installation and management of multiple agents on each monitored computer, server and laptop, causing serious errors, poor performance and high resource consumption.

Traditional endpoint protection technologies focused on prevention are valid for known threats and malicious behaviors, but they are not enough against advanced cyber threats.

From Prevention To Response - Automated Endpoint Security

WatchGuard EPDR is an innovative cybersecurity solution for computers, laptops and servers, delivered from the Cloud. It automates the prevention, detection, containment and response to any advanced threat, zero day malware, ransomware, phishing, in-memory exploits, and fileless and malwareless attacks.



Unlike other solutions, it combines the widest range of endpoint protection technologies (EPP) with automated detection and response (EDR) capabilities. It also has two services, managed by WatchGuard experts, that are delivered as a feature of the solution:

- Zero-Trust Application Service: 100% classification of the applications
- Threat Hunting Service: detecting hackers and insiders

call: **01246 200 200** | email: **letstalk@ccsmedia.com** | visit our website at **ccsmedia.com**

CCS Media

WatchGuard EPDR integrates next-gen AV with innovative, adaptive protection and EDR technologies in a single solution, allowing IT pros to deal with advanced cyber threats:

Organisational Cybersecurity Challenges

- Personal or managed firewall (IDS)
- Device control
- Collective Intelligence and pre-execution heuristics
- Permanent multi-vector anti-malware & on-demand scan
- URL filtering, web browsing and anti-phishing
- Anti-tampering
- Automatic remediation and ability to rollback
- Recover encrypted files with shadow copies
- Vulnerability assessment

Advanced Security Technologies

- Continuous endpoint monitoring with EDR
- Cloud-based machine that learns to classify 100% of processes
- (APTs, ransomware, rootkits, etc.)
- Sandboxing in real environments
- Anti-exploit protection
- Network attack protection: prevent attacks exploiting vulnerabilities in Internet-exposed services
- Threat hunting: behavioral analysis and detection of indicators of attack (IoAs) to detect living off the land attacks (LotL)
- IoAs mapped to MITRE ATT&CK Framework
- Detection and prevention of RDP attacks
- Containment and remediation capabilities such as computer isolation and program blocking

Benefits

Simplifies & Maximises Security

Its automated services reduce the costs of expert personnel. There are no false alerts to manage, no time wasted on manual settings, and no responsibility is delegated.

Endpoint performance is not impacted since it is based on a single agent and Cloud-native architecture.

Easy to Use and Easy to Manage

Endpoint Security portfolio handles all needs of your endpoint protection in a remarkably simple way from a single web console.

Easy to set up. Cross-platform endpoint management from a single pane of glass.

Unique EDR Features

Twelve-month data retention and real-time physical sandboxing to avoid unnoticed hacker actions.

Zero-Trust Application Service - each process is classified based on the dynamic behavior of the process.
Threat Hunting Service - for detecting hackers and insiders.

call: **01246 200 200** | email: **letstalk@ccsmedia.com** | visit our website at **ccsmedia.com**

Zero-Trust Model: A Layered Protection

WatchGuard's Endpoint Security platform doesn't rely on just one single technology; we implement several together to reduce the opportunity for a threat actor to have success. Working in concert, these technologies utilise resources at the endpoint to minimise the risk of a breach.

Zero-Trust Model: A layered protection

Endpoint Layers:

Layer 1/ Signature Files and Heuristic Technologies

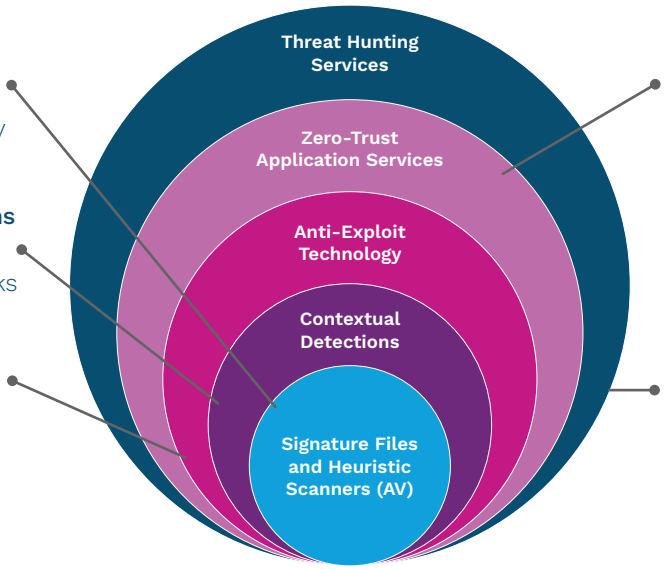
Effective, optimised technology to detect known attacks

Layer 2 / Contextual Detections

They enable us to detect malwareless and fileless attacks

Layer 3 / Anti-Exploit Technology

It enables us to detect fileless attacks designed to exploit vulnerabilities



Cloud-Native Layers:

Layer 4 / Zero-Trust Application Service

Provides detection if a previous layer is a breach, stops attacks on already infected computers and stops lateral movement attacks inside the network

Layer 5 / Threat Hunting Service

Detect compromised endpoints, early stage attacks, suspicious activities, and identify IoAs that minimize detection and response time (MTTD and MTTR).

Implement Powerful, Simplified Security With Watchguard's Unified Security Platform

WatchGuard's Unified Security Platform architecture is a single platform for elevating modern security delivery. Our platform approach helps you deliver powerful security services for every threat vector with increased scale and velocity while supporting operational efficiencies and greater profitability.

Comprehensive Security

A complete portfolio of endpoint, multi-factor authentication, and network security products and services for protecting environments, users, and devices.

Clarity & Control

Centralised security administration visibility, and advanced reporting via **WatchGuard Cloud.**

Operational Alignment

Simplified busiess operations with direct **API access,** a rich ecosystem of **out-of-the-box integrations**, and support for all payment and consumption models via **FlexPlay**.

Shared Knowledge

A full integrated platform for adopting a zero-trust security posture via WatchGuard's **Indentity Framework** and deploying a true XDR-based approach to threat detection and remediation via **ThreatSync®.**

Automation

WatchGuard's **Automation Core®** brings simplification and scale to every aspect of security consumption, delivery, and management.