DATASHEET | SOC

WATCHGUARD ADVANCED EPDR

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 necessary to monitor and manage endpoint security risks. So, what types of challenges are security teams facing when adopting endpoint security solutions?

- **Ever-evolving sophisticated threats:** Efficient proactive security practices can mean the difference between a minor security operation or being a victim. These practices range from reducing the attack surface to uncovering emerging threats before an actual compromise.
- **Alert fatigue, lack of efficiency:** Security teams receive thousands of weekly alerts, of which only 19% are considered trustworthy, and only 4% of which are ever investigated. Two-thirds of security teams' time is dedicated to managing alerts. Security automation increases their efficiency.
- **Poor performance:** Endpoint security solutions require frequent installation and management of multiple agents on each monitored computer, server, and laptop, causing serious errors, poor performance and high resource consumption.

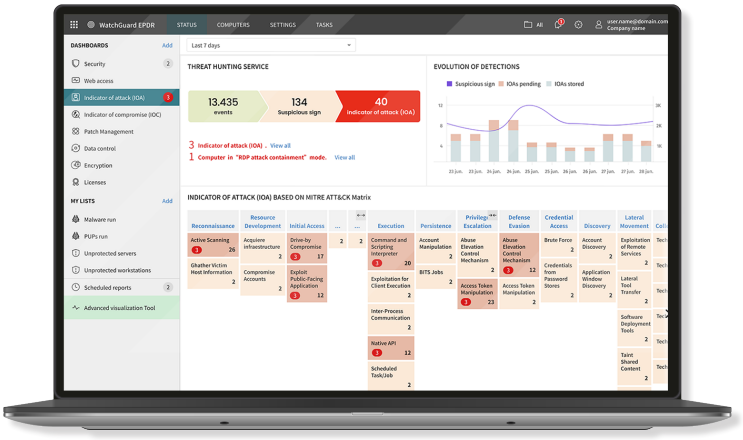
Traditional endpoint protection technologies focused on prevention are valid for known threats and malicious behaviours, but they are not enough against unknown sophisticated cyber threats. From common compromise vectors to new threats, attackers are always looking for ways to escape IT notice, evade defense measures and exploit emerging weaknesses.

COMPLETE PROACTIVE CYBERSECURITY AGAINST EVER-EVOLVING THREATS

WatchGuard Advanced 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, inside and outside the corporate network.

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



WatchGuard Advanced EPDR integrates traditional endpoint technologies with EDR technologies in a single solution, allowing security teams to deal with advanced cyber threats.

Traditional Preventive Technologies

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

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
- Threat hunting, with behavioural analytics to detect LotL (living-off-the-land techniques)
- Indicators of attack mapped to MITRE ATT&CK Framework
- Detection and prevention of RDP attacks
- Containment and remediation capabilities such as computer isolation and programme blocking by hash or name
- STIX 2.0 indicators of attack (IoCs)
- Enhanced security policies enable hardened endpoints from the execution of common attack techniques

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.
- No management infrastructure to install, configure or maintain.
- Endpoint performance is not impacted since it is based on a lightweight agent and Cloud-native architecture.
- It reduces security risk by denying the execution of common LotL techniques.

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.
- It provides a clean and intuitive user interface design that can be quickly mastered.
- Centralised management of IoCs search on all endpoints.

Automated EDR Features

- Detects and blocks hacking techniques, tactics and procedures, and malicious in-memory activity (exploits) before they can cause damage.
- Resolution and response: forensic information is used to thoroughly investigate each attack attempt, and tools to mitigate its effects (disinfection).
- Traceability of each action: actionable visibility into the attacker and their activity, facilitating forensic investigation.

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 utilize resources at the endpoint to minimize the risk of a breach.

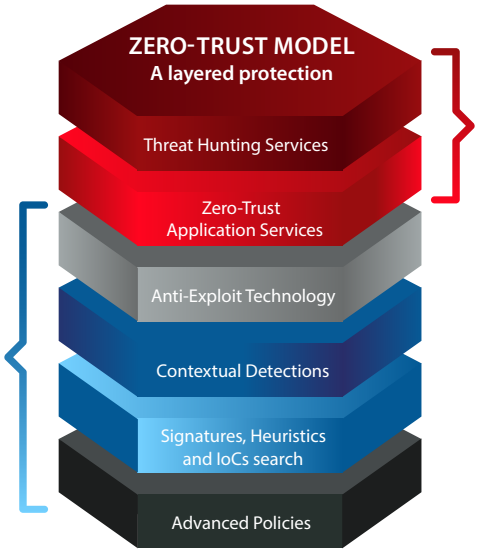
ENDPOINT LAYERS:

Layer 1/ / Enhanced Security Policies
Detect or block the execution of common attack techniques

Layer 2 / Signature Files, Heuristic Technologies and IoC Search
Effective, optimised technology to detect known attacks

Layer 3 / Contextual Detections
They enable us to detect malwareless and fileless attacks

Layer 4 / Anti-Exploit Technology
It enables us to detect fileless attacks designed to exploit vulnerabilities



CLOUD-NATIVE LAYERS

Layer 5 / Zero-Trust Application Service
Classifies 100% of processes before they run, denying any execution until it is certified as trusted

Layer 6 / Threat Hunting Service
It enables us to detect compromised endpoints, early stage attacks, suspicious activities, and detection of IoAs

Enhanced Security Policies enable security pros to supervise or harden endpoints from the execution of suspicious scripts and common attack techniques utilised by sophisticated threats (PowerShell, unknown scripts, documents with macros, etc.)

Signature files and heuristic technologies, known as traditional endpoint protection (EPP), make up a next-generation antivirus technology layer that is proven effective against many common, low-level threats, and malicious URL blocking.

IoC Search capability enables security teams to quickly hunt for recently disclosed incidents as well as find impacted endpoints in a forensic analysis. Different types of indicators are supported – MD5/SHA256, filename/path, domain/IPv6/IPv4 and Yara rules.

Contextual detection is very effective against script-based attacks, attacks using goodware OS tools such as PowerShell, WMI, etc., web browser vulnerabilities and other commonly targeted applications such as Java, Adobe, and more.

Anti-exploit technology searches for and detects anomalous behaviour. It is mission-critical on unpatched/waiting-to-be-patched endpoints, and on endpoints with operating systems that are no longer supported.

Zero-Trust Application Service classifies 100% of processes, by default denying any execution until it is certified as trusted. No need to manually classify threats or delegate them to security admins.

Threat Hunting Service is based on a set of hunting rules created by cybersecurity specialists that are automatically processed against all data gathered from telemetry, identifying indicators of attack (IoAs) that minimise detection and response time (MTTD and MTTR).

Supported platforms and systems requirements of WatchGuard's Endpoint Security platform:

Supported operating systems: Windows (Intel & ARM), macOS (Intel & ARM), Linux, iOS and Android.

Support to legacy systems starting in Windows XP SP3 and Server 2003.

EDR capabilities are available on Windows, macOS, and Linux, with Windows being the platform that provides all the capabilities in their entirety.

List of compatible browsers: Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge and Opera.

PHONE +27 21 683 3899 EMAIL sales@dolos.africa WEB www.dolos.africa

DOLOS - SECURITY EXCELLENCE