OX IT Solutions Ltd

# EPDR
# Endpoint Detection & Response

WatchGuard

## ORGANISATIONAL CYBERSECURITY CHALLENGES

Endpoints are the primary target for most cyberattacks and as the technology infrastructure becomes more complex, organizations 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?

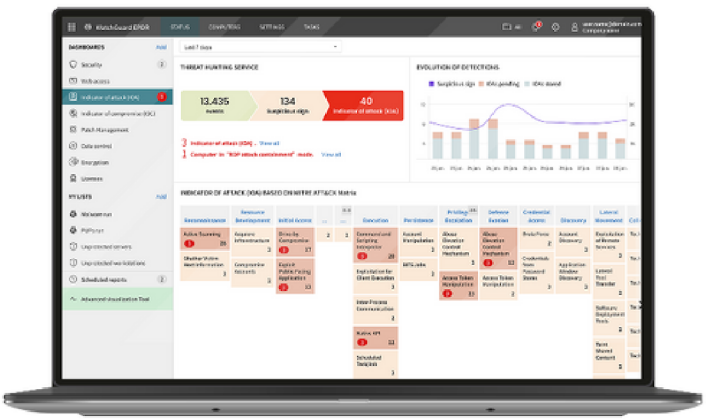
- **Alert fatigue**
  - Organisations receive thousands of weekly malware alerts, of which only 19% are considered trustworthy, and only 4% of which are ever investigated. Two-thirds of cybersecurity admins' time is dedicated to managing malware alerts.
- **Complexity**
  - Too many disconnected cybersecurity 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 behaviours, but they are not enough against advanced 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.

## 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, 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 EPDR integrates traditional endpoint technologies with innovative, adaptive protection and EDR technologies in a single solution, allowing IT pros 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, including behavioural analysis and detection of IoAs (indicators of attack) to detect LotL (living off the land attacks)
- Indicators of attack mapped to MITRE ATT&CK Framework
- Detection and prevention of RDP attacks
- Containment and remediation capabilities such as computer isolation and program blocking by hash or name

OX IT Solutions Ltd

# EPDR
# Endpoint Detection & Response

WatchGuard

## BENEFITS

### Simplifies & Maximizes 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.

### 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 obvious user interface design that can be quickly mastered.

### Automated EDR Features

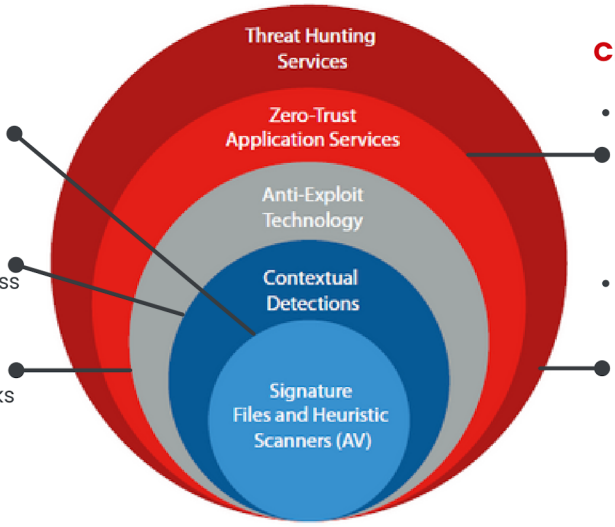
- Detects and blocks hacking techniques, tactics and procedures, and malicious in-memory activity (exploits) before it can cause damage.
- Resolution and response: forensic information to thoroughly investigate each attack attempt, and tools to mitigate its effects (disinfection).
- Traceability of each 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 utilise resources at the endpoint to minimize the risk of a breach.

### ENDPOINT LAYERS:

- **Layer 1/ Signature Files and Heuristic Technologies**
  - Effective, optimized 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**
  - It enables us to detect compromised endpoints, early stage attacks, suspicious activities, and detection of IoAs

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.

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 behavior. 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.

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

**Supported platforms and systems requirements of Watchguard EPDR**

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.

www.oxitsolutions.co.uk sales@oxitsolutions.co.uk 01865 594930

OX IT Solutions Ltd

powered by WatchGuard

# WatchGuard Cloud

- Connect in real time to deploy tasks to thousands of devices in seconds
- Manage all WatchGuard-branded products from a single console
- View devices across endpoint platforms including Windows, Linux, macOS, iOS and Android

## THE WATCHGUARD PORTFOLIO

### Network Security

WatchGuard Network Security solutions are designed from the ground up to be easy to deploy, use, and manage – in addition to providing the strongest security possible. Our unique approach to network security focuses on bringing best-in-class, enterprise-grade security to any organization, regardless of size or technical expertise.

### Multi-Factor Authentication

WatchGuard AuthPoint® is the right solution to address the password driven security gap with multi-factor authentication on an easy-to-use Cloud platform. WatchGuard's unique approach adds the "mobile phone DNA" as an identifying factor to ensure that only the correct individual is granted access to sensitive networks and Cloud applications.

### Secure Cloud Wi-Fi

WatchGuard's Secure Wi-Fi Solution, a true game-changer in today's market, is engineered to provide a safe, protected airspace for Wi-Fi environments, while eliminating administrative headaches and greatly reducing costs. With expansive engagement tools and visibility into business analytics, it delivers the competitive advantage businesses need to succeed.

### Endpoint Security

WatchGuard Network Security solutions are designed from the ground up to be easy to deploy, use, and manage – in addition to providing the strongest security possible. Our unique approach to network security focuses on bringing best-in-class, enterprise-grade security to any organization, regardless of size or technical expertise.

## Find out more

**For additional details, talk to OX IT Solutions. We're an authorised WatchGuard Gold partner.**

www.oxitsolutions.co.uk

01865 594930

sales@oxitsolutions.co.uk

## About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, endpoint security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by over 18,000 security resellers and service providers to protect more than 250,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for midmarket businesses and distributed enterprises. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Pacific, and Latin America. To learn more, visit WatchGuard.com.