AutoXDR Managed Service

autodata

Free up your resources and respond to security incidents 24/7 with a fully managed and automated XDR service

What is XDR? How does it differ from standard EPP?

XDR encompasses different tools within an agent. EPPs are purely deployed on the endpoint to detect and stop signature-based attacks. XDR acts across different security layers to continuously monitor and rapidly detect threats from a wider range of sources across the organisation, such as cloud-based applications, network traffic, and user behaviour.

Why Managed XDR?

Organisations are commonly overwhelmed by the volume of security alerts and are struggling to hire and retain skilled cyber-security talent. Managed XDR resolves these issues by consolidating tooling via a best-in-class automated platform backed by a fully managed detection and response service.

AutoXDR Benefits

- END-TO-END PROTECTION
- NATIVE RESPONSE AUTOMATION
- EASY TO USE & FAST TO DEPLOY
- COMPLETE VISIBILITY
- EFFECTIVE TCO/ROI
- 24/7 PEACE OF MIND

bsi ISO/IEC 27001 Information Security Management CERTIFIED

CYBER ESSENTIALS CERTIFIED PLUS

The current approach to threat protection requires an expensive, multi-product security stack that can only be operated by a sizeable and skilled security team. This approach is critically flawed. It leaves your internal IT resources drained, exhausted, blinded, and exposed. Even if your company could afford this approach, why would you?

XDR: the New Approach to Security

Over the years, threats have become more sophisticated. Malware and ransomware are no longer just a standard file-encryption piece. Attackers are now infiltrating cryptographic systems and it has become much harder for legacy security products to detect these types of attacks. Integrating several disparate solutions has also been difficult and often prohibitively expensive.

The new guard of XDR platforms **can** detect these newer attack intrusions. Perhaps the biggest improvement has been a significant reduction in the number of false positives being generated, thus avoiding alert fatigue.

AutoXDR powered by Cynet is a managed alternative ranked as a top performer by the MITRE Engenuity ATT&CK Enterprise Evaluation due to its **100% detection, visibility, analytic coverage and real-time detection** scores, all with ZERO configuration changes. With a proactive 24/7 MDR team continuously monitoring your environment, providing expert assistance and guidance, AutoXDR is considerably more cost-effective than hiring even just one single cyber-security professional internally.

AutoXDR: the All-in-One Cyber-Security Platform

AutoXDR provides all the prevention, detection, correlation, investigation, and response you need, all backed by a 24/7 MDR service without the associated cost and complexity. Automate your day-to-day cyber-security operations with:

- **Automated Investigation:** automated root cause and impact analysis
- **Automated Remediation**: eliminate malicious presence, activity, infrastructure
- **Custom Playbooks:** procedures, tools, who to involve during security incidents
- **Threat Detection:** EDR, NDR, UEBA, Deception, Sandbox, TI
- **EPP:** Next Generation AV, Device Control, Critical Resource Protection
- **SaaS & Cloud Security:** CSPM, SSPM
- **IT Security Operations:** IT Hygiene, Asset Inventory, Vulnerability Management
- **CLM:** automatically collect the highest-priority data to uncover threats
- **Event Correlation:** collect and correlate alert and activity data into actionable incidents, providing SIEM-like capabilities
- **Forensics:** investigate, remediate, orchestrate and automate IR workflows