Endpoint Security and Asset Management

www.zdlgroup.com

Data Sheet

Endpoint Detection and Response addresses the need for continuous monitoring and response to evolving threats.

Our endpoint solution enables the prevention of threats and the mitigation of risks with machine learning behavioural analysis, essential antivirus, exploit prevention, firewall, and web control. This required threat intelligence and other telemetry collected from your entire estate.

We also provide centralised management and data visualisation to highlight threat data so you can quickly harden your defences and make policy changes.

Real-time scanning, cloud analytics, application containment, and rollback remediation work together to limit the impact of suspicious files and zero-day malware. Manual detections and remediation are replaced by automatic analysis, containment and policies to halt threats before they spread, returning endpoints to a healthy state. EDR integration with threat intelligence assists with faster detection of activities, tactics, techniques and procedures identified as malicious.

Our automated and adaptable Endpoint Detection and Response (EDR) technology is easy to use and makes incident response as simple as one click. Automated AI-guided investigations equip analysts of any experience level and help speed threat triage.

ZDL GROUP

Monitor and collect activity data from endpoints which may indicate a threat

Analyse this data

Provide forensic and analysis tools to research identified threats

Automatically respond to threats

Our Solution:

- Provides better and stronger defence against malware from rapid analysis.
- Allows analysts to apply strategic incident response without a demanding administration overhead.
- Detects evasive zero-day threats in near real time by examining how they look and behave.
- Provides roll back remediation, automatically reversing malicious actions made by threats by returning them to their previous healthy state to keep your systems and users productive.
- Directly maps to Mitre ATT&CK Framework making it quicker to understand the techniques, tactics, and procedures of any given threat.
- Centralises management to provide greater visibility with the orchestrator console, simplifying operations, unifying security and reducing costs.
- Seamlessly integrates with existing tools within the threat hunting and intelligence ecosystem such as SIEM and Sandbox to provide a more mature and complete security posture.

ZDL GROUP

Delivering excellence in Cyber Security

At ZDL, we believe that effective risk management requires a holistic 360° approach. We take a comprehensive view of our clients' cyber security risks and provide quality services to address those risks.

Our approach to Total Security Management helps make our clients' infrastructure, applications and data more secure in the face of a continually evolving Threat Landscape. Our aim is to build a partnership with our clients, built on a mutual respect and understanding of each other's businesses.
We become a part of our clients' team, a valued partner; an intrinsic part of their business.

ZDL's 4 key service areas are designed to focus on our clients' cyber resilience journey. Our unique portfolio of services enables you to build an agile, responsive security infrastructure and strategy.

Our Services

Ethical Hacking

- Broad Security Review
- Red Teaming
- Security Audits
- Penetration Testing
- Cloud Security & Security Ops Testing
- Source Code Review/Coding Standards
- Social Engineering
- Physical Security

Training

- Security Awareness Programmes
- Secure Coding School for Developers
- Bespoke Senior Exec Security Training
- Runbook training/ Scenario Workshops
- Phishing & Resilience Programmes
- Physical Security Awareness
- Online Assessment / CBT Developer Training

Managed Services

- Supplier Evaluation Risk Management (VenDoor)
- Incident Response Preparedness
- Security Training for Developers - Annual Programme
- Managed Detection and Response (MDR)
- Virtual Information Security Manager
- OSINT/Threat Intelligence

Compliance

- Policy Review & Creation
- 360° Assessment
- PCI Remediation Support
- ISO/ NIST/EU GDPR Standards Agreement
- Business Continuity Management
- IR Management Review
- ISO Readiness Programmes
- Office365 Configuration Review

www.zdlgroup.com
London | Brighton | Manchester | USA

Contact Us ⟶