Datasheet

MyCyberIQ
STAY AWARE. STAY SMART. STAY SECURE.

EDR Cloud

Advanced Endpoint Detection and Response

Cyber-criminals are growing ever more sophisticated and today's advanced attacks are increasingly difficult to detect. Using techniques that individually look like routine behavior, an attacker may access your infrastructure and remain undetected for months, significantly increasing the risk of a costly data breach. When your existing endpoint security doesn't provide the advanced attack detection and response required – adding EDR Cloud quickly and effectively strengthens your security operations.

EDR Cloud monitors your network to uncover suspicious activity early and provides the tools you need to fight off cyber-attacks. By integrating our award-winning machine-learning, cloud-scanning and sandbox analyzer to it can detect activity that evades traditional endpoint prevention mechanisms. It provides full visibility on the techniques, tactics and procedures (TTPs) being used in active attacks while providing comprehensive search capabilities for specific indicators of compromise (IoCs), MITRE ATT&CK techniques and other artifacts to discover early-stage attacks.

EDR Cloud provides innovative and easy-to-understand visualizations with rich context and threat intelligence that help IT staff understand attack paths and identify gaps in protection. These visualizations streamline the investigation and response, easing the burden on IT staff. The sandbox analyzer enables staff to automatically execute suspicious payloads in a contained, virtual environment to isolate and neutralize suspicious files. EDR Cloud capabilities protect organizations against advanced threats, while enabling proactive threat hunting and root-cause analysis.

How does EDR Cloud help?

- **Advanced attack detection and response.** Monitors your network to uncover suspicious activity early and provides the tools to enable you to fight-off cyber-attacks.
- **Bridge the security skills gap.** Enables teams to respond efficiently with automated alert prioritization and one click response.
- **Reduce organization risk.** Continuously analyses your infrastructure to identify risk across hundreds of factors. Helps to mitigate user, network and OS risks.
- **Minimize operational burden.** Cloud-delivered and low maintenance, agents are easily toe deploy and integrate into your existing security architecture and is fully compatible with your endpoint antivirus solution.

At-a-Glance

EDR Cloud detects advanced threats including fileless attacks, ransomware, and other zero-day threats in real-time. It's threat analytics and cloud-based event collector continuously monitor endpoints and prioritizes security events into a list of incidents for investigation and response. EDR provides innovative and easy-to-understand visualizations with rich context and threat intelligence that help IT staff understand attack paths and identify gaps in protection. These visualizations streamline the investigation and response, easing the burden on IT staff.

Key Benefits

- Industry-leading detection – Enhanced threat detection and visibility that enables the strengths of XDR for protecting endpoints. Comprehensive search capabilities for specific indicators of compromise (IoCs), MITRE ATT&CK techniques, and other artifacts to discover early-stage attacks.
- Focused Investigation and Response – Organizational-level incident visualizations enable you to respond efficiently, limit the lateral spread, and stop ongoing attacks.
- Maximum Efficiency – Our easy-to-deploy, low overhead agent ensures maximum efficiency and protection, with minimal effort. For a fully managed solution, easily upgrade to Managed Detection and Response (MDR).

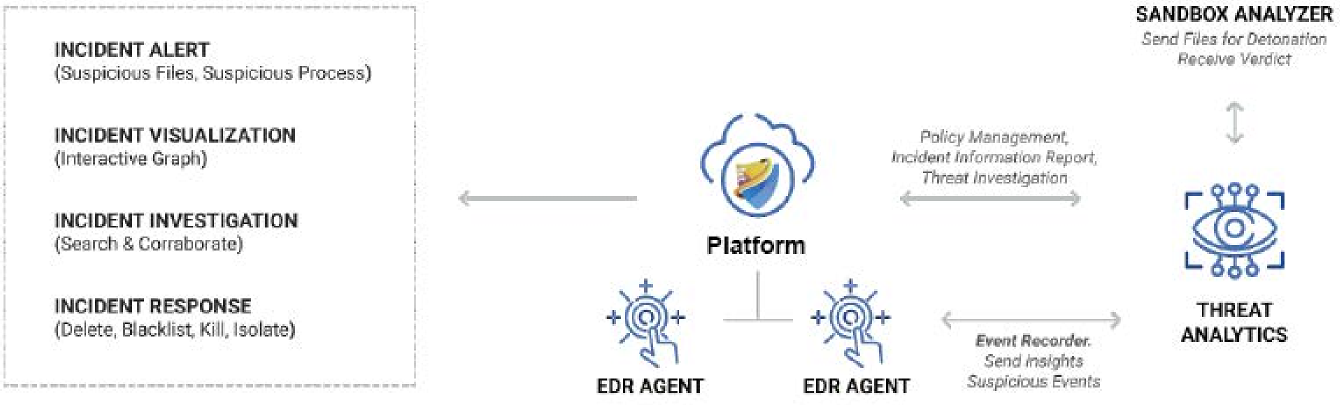
"EDR capabilities provide us with detailed reporting on how processes were affected across the entire incident chain. That saves us an immense amount of time on investigating since the manual work is eliminated."

Sascha Neuhaus,
IT Security Officer, Louis

Innovation for Efficiency and Effectiveness

Our cross-endpoint correlation technology takes threat detection and visibility to a new level by applying XDR capabilities for detecting advanced attacks involving multiple endpoints in hybrid infrastructures (workstations, servers, or containers; running various OS). It extends EDR visibility, analytics and event correlation capabilities beyond the boundaries of a single endpoint, to enable security teams to deal more effectively with complex cyber-attacks involving multiple endpoints. This cross-endpoint correlation technology combines the granularity and rich security context of EDR with the infrastructure-wide analytics of Extended Detection and Response (XDR). By providing threat visualizations at the organizational level, XDR helps organizations focus investigations and respond more effectively.

How it Works



EDR Cloud is a cloud-based solution built upon the XDR platform. Each EDR agent deployed on your organization's endpoints has an event recorder that continuously monitors the endpoint and securely sends insights and suspicious event details to the centralized Control Center. In the Control Center, the cross-endpoint correlation engine collects and distills endpoint events and generates prioritized, organizational-level views of security incidents, enabling administrators to quickly investigate and respond effectively to threats.