

Endpoint Detection and Response (EDR) Service

Managed Operational Security

As part of Quistor's Managed Services, the Managed Operational Security (MOS) department is responsible for mitigating technical risks associated with your company's security vulnerabilities. The MOS team protects valuable assets through security patching, vulnerability assessments, incident handling, and 3rd party security product implementation, ensuring that all systems are fortified against security threats.

Benefits



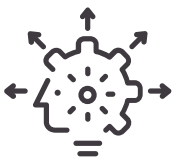
Clear Reporting

MOS reports are meticulously designed to meet auditing requirements and compliancy standards. Security statistics are seamlessly integrated into existing monthly and quarterly reports. Furthermore, vulnerability assessments provide valuable insights into your system's security posture.



Dedicated Team of Experts

Our team comprises dedicated consultants with technical application and cyber security knowledge. They ensure correct patch levels, prioritize patches effectively, and conduct thorough testing. Their expertise extends to 3rd party security products, tailored precisely to your needs.



EDR for Peace of Mind

Our AI-based Endpoint Detection & Response (EDR) software offers robust remediation capabilities. Rest easy knowing that 24x7 Managed EDR support is also available.

The Quistor's Managed Operational Security team offers the best solution for your IT security and business continuity: Endpoint Detection and Response (EDR).

Endpoint Detection and Response (EDR) services

Endpoint Detection and Response (EDR) protection platforms provide the facility to deploy agents or sensors to manage endpoints including PCs, servers, laptops, virtual machines in the cloud, and other devices. These are designed to prevent a range of threats, known and unknown malware, in order to provide protection from such risks; in addition, they provide the ability to investigate and remediate any incidents that evade protection controls.

The core functionalities of an endpoint protection platform include:

- Prevention and protection against security threats, including malware that uses file-based and fileless exploits.
- The ability to apply control (allow/block) to software, scripts and processes.
- The ability to detect and prevent threats using behavioral analysis of device activity, application and user data.
- Facilities to investigate incidents further and/or obtain guidance for remediation when exploits evade protection controls.

How it works

Detection

Threat incidents are identified by AI-based detection engines available in the EDR solution.

Investigation

Analysts classify the threat incidents based on AI/ML, threat intelligence and forensics, and their own expertise.

Analysis

Analysts interpret and document all console incidents and provide you with key insights.

Resolution

Analysts mitigate and resolve threat incidents, and escalate them to you proactively as needed.

EDR vs. traditional Antivirus (AV)

Security used to be simple for businesses, as it could be solved with an installed anti-virus (AV) solution, trained employees not to click on unknown links, and software kept up to date. Nevertheless, now companies need to fortify against new, advanced, real-time threats that can get around traditional antivirus solutions. Endpoint Detection and Response (EDR) offers more guarantees to prevent these potential security issues from occurring.

Endpoint Detection and Response	Anti-Virus Solutions
Gain freedom from ransomware by rolling back devices to their pre-infected state.	Can't roll back to a pre-infected state, increasing your ransomware risks.
Use artificial intelligence (AI) to detect and prevent both current and emerging threats, with continual updates to the platform.	Use signatures to identify threats, meaning capabilities lag behind cyber-attackers' latest strategies.
Configure automated system remediation for fast threat incident response.	Manually gather information / investigate the health of the endpoint and remediate any misconfigurations or unwanted system changes.
Monitor processes before, during, and after execution, to prevent new threats from slipping in.	Fly blind during execution, creating an entry point for new threats from savvy attackers.
Monitor your systems in real-time.	Rely on daily or weekly scans, increasing your risks.
Keeps device performance fast with continual monitoring.	Can slow down your device performance with longscans.

EDR Benefits

- Minimize costly downtime caused by security incidents.
- Help increase employee productivity.
- Rely on IT security professionals to manage your cybersecurity.
- Mitigate the negative impact of ransomware attacks.

About SentinelOne

SentinelOne Endpoint Detection & Response (EDR) software

The Quistor Managed Operational Security (MOS) team has decided to provide the Endpoint-Detection-Response (EDR) Solution SentinelOne.

This offers both the EDR Complete service and, combined with Managed 24x7 SoC Services, Managed EDR (MDR).

- AI-based EDR software including powerful remediation capabilities.
- Product implementation, Licensing & Code-current services.
- Streamlined Alerting and Security Reporting.
- Automated system remediation for fast threat incident response.
- 24x7 Managed EDR as an additional service.

Figure 1: Magic Quadrant for Endpoint Protection Platforms



In-Depth
Visibility



Lighten
Analyst Load



Automated Threat
Resolution

Which options does Quistor MOS provide?

EDR Complete

We deploy the SentinelOne Complete software on your systems that delivers a combination of proactive surveillance of traffic behavior in combination with powerful remediation and rollback capabilities should something go wrong. We implement, fine-tune, and maintain the product to keep it up to date.

Customers will be provided with access to the cloud-based console to manage the solution and take care of incidents.

EDR Complete - Benefits



Protect your business from ransomware attacks

Gain peace of mind by using EDR to roll back any and all devices to their pre-threat state. Simply click and restore infected machines to full productivity, no matter which strain of ransomware is holding them hostage.



Increase employee productivity

Eliminate threats that outwit traditional AV solutions and maintain faster device performance, creating fewer distractions that eat into employee productivity.



Centralized Endpoint security via one console

Access the cloud-based console to manage the product and treat incidents.

Managed EDR (MDR)

Just like EDR Complete, the SentinelOne Complete software is deployed in Managed EDR and offers the same benefits. However, MDR also includes some additional advantages.



24x7x365 monitoring, triage, and prioritization

- Analysts monitor your endpoints day and night.
- They triage and prioritize threat events detected by EDR, based on your unique program needs.
- They add human context, reducing alert fatigue.



Threat investigation, containment, and response

- Analysts investigate, interpret context-rich threat storylines, and add notes on all threat events in the EDR console.
- Four-hour threat response SLA.



Ongoing engagement and reporting

- Analysts proactively notify you of any malicious or suspicious activity.
- Reports on threat activity, mitigation actions, and false positive rates. Can also be scheduled to be sent out at regular intervals.
- They will open escalations for urgent matters only.



Threat hunting for latest threats and cybercrime

- Threat hunting activities can be performed using the EDR Complete license which provides the advanced Threat Hunting feature.
- Analysts perform proactive threat hunting for attacker techniques.
- They provide threat bulletins and alerts if/when threats are detected.
- The security experts performing threat hunting belong to SentinelOne's Watchtower team.

QUISTOR

An **ITG** Company



info@quistor.com



+31 164 213 300



www.quistor.com