QUISTOR

An ITG Company

Managed Operational Security

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.

MOS Benefits

Patch Management - Trusted Approach

Recurring security patching follows a mutual pre-aligned schedule. Critical patches are applied ad hoc upon release and in alignment. Additionally, there's a guarantee of patch compatibility with applications within the scope of support.

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.

QUISTOR
An ITG Company

MOS Service Catalogue

Patch Management services

With the Security Patch Management services, the MOS team takes responsibility for prioritizing and applying the latest security patches, for systems and software in the scope of our support. This critical service helps protect the IT infrastructure from security vulnerabilities and cyber-attacks.

Security patching is critical in ensuring the safety and integrity of digital systems. By applying updates and fixes to software, operating systems, and devices, you can effectively address vulnerabilities and protect against potential cyber threats. This proactive approach reduces the risk of data breaches, unauthorized access, and system compromises. Security patching also helps enhance system performance and stability, ensuring your digital infrastructure operates smoothly.

Security Patch Management (continuous, recurring process)

- Windows Operating System (monthly / at chosen interval*).
- Linux Operating System (monthly / at chosen interval*).
- Oracle Weblogic Server / Fusion Middleware (quarterly*).
- Oracle Java (quarterly*).
- Oracle Database Client & Oracle Database (quarterly*).

*Ideal moment, but can also be patched at other intervals.

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.

EDR vs. traditional Antivirus (AV)

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

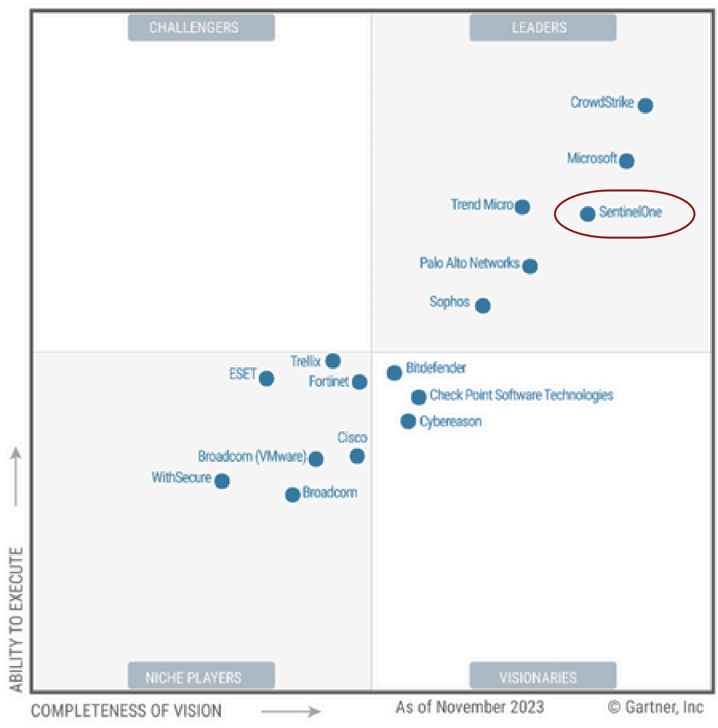
- Minimize costly downtime caused by threat incidents.
- Help increase employee productivity.
- Maintain device performance, lowering the distractions that eat into employee productivity.
- Rely on IT security professionals to manage your cybersecurity protocols.
- Mitigate the negative impact of ransomware attacks.

About SentinelOne

SentinelOne Endpoint Detection & Response (EDR) software

- 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.
- With EDR services consumed from MOS, we take care of Endpoint Detection & Response product implementation, licensing, and code current services. Additionally, 24x7 Managed EDR Services are provided.

Figure 1: Magic Quadrant for Endpoint Protection Platforms



In-Depth Visibility

Lighten Analyst Load

Automated Threat Resolution

Inside the EDR offering, the Managed Operational Security team provides two different options: EDR Complete and Managed EDR (MDR).

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.

Benefits

Protect your business from ransomware attacks

Increase employee productivity

Centralized Endpoint security via one console

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:

- Manage the solution; provide 24x7 EDR monitoring.
- Take care of incident triage and prioritization, ticketing, mitigations, and resolution of incidents.
- Open escalations for urgent matters only.
- Report per incident including a timeline.
- Integrate Security Reporting in existing periodical reports (Monthly or Quarterly).

Benefits

24x7x365 monitoring, triage, and prioritization

Ongoing engagement and reporting

Threat investigation, containment, and response

Threat hunting for latest threats and cybercrime

QUISTOR

An ITG Company

info@quistor.com

+31 164 213 300

www.quistor.com