## EventTracker EDR

*Accelerate detection and remediation of advanced threats that can cause downtime and data breaches.*

Our managed SIEM/SOC service includes EDR (Endpoint Detection and Response) to protect your critical endpoints and servers from Zero-day attacks and mutating malware, all powered by an AAA-rated technology plus a 24/7 SOC staffed by security experts who augment your team.

<table>
<thead>
<tr>
<th>Enhance Visibility</th>
<th>Simplify Management</th>
<th>Rapidly Remediate</th>
<th>Augment Expertise</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Insight across network &amp; endpoints</td>
<td>- Managed service tracking internal and external threats</td>
<td>- Targeted remediation</td>
<td>- Easy to implement &amp; maintain</td>
</tr>
<tr>
<td>- Pinpoint unfolding attacks</td>
<td>- No performance impacts with lightweight sensor</td>
<td>- Forensic investigation</td>
<td>- 24/7 access to global security experts</td>
</tr>
<tr>
<td>- Minimize false positives to detect true threats</td>
<td>- Take immediate action per protection policies</td>
<td>- Stop unknown malware</td>
<td>- Actionable threat intelligence</td>
</tr>
<tr>
<td>- Single pane of glass when integrated with SIEM</td>
<td>- Single admin can manage over 10,000 systems</td>
<td>- Prevent lateral spread</td>
<td>- Recommend mitigation steps</td>
</tr>
<tr>
<td>- Identify adversary actions</td>
<td>- Block threats before damage occurs</td>
<td>- Integrated with &gt; 50 threat intelligence data sources</td>
<td>- Optimize for future threats</td>
</tr>
</tbody>
</table>

Stopping an attack early in the cyberattack lifecycle restricts adversary access, insights, and damage. EventTracker EDR provides comprehensive visibility to inspect the entire kill chain and help investigate the steps adversaries take.
Questions We Help You Address

- Have adversaries already installed malware and moved laterally in our network?
- Are employees and their risky behavior compromising organizational security?
- Do we have complete visibility across our network and endpoints 24/7?
- Has malware compromised our business?
- Are legacy devices putting us at risk?
- Are we protected from vulnerabilities before patching occurs?
- Are we using threat intelligence to reduce false positives and prioritize our finite resources?
- Is there a less complex approach to endpoint detection than my current EDR solution?
- Do we have the skills or time to identify and investigate advanced threats?
- Would a managed service augment our expertise and provide better time to value?
- Would integrated EDR + SIEM improve our visibility and coverage?

Features

- A 24/7 managed service without capital costs
- Early and rapid detection of advanced and mutating threats
- ISO 27001-certified Security Operations Center
- U.S. based data center
- Legacy system and unpatched device protection
- Easy-to-understand remediation recommendations
- Ongoing optimization meetings with an assigned EDR analyst
- Actionable Threat Intelligence that adds context to malicious behavior
- Blocks or disables suspicious networking and processes on endpoints
- Flexible management policies for endpoint protection and containment

Powered by a Trusted Security Platform

EDR is included with our manage SIEM/SOC service. It provides 24/7 advanced threat protection for key assets like servers and endpoints to quickly detect and efficiently recover from cyber attacks. Integrated EDR and SIEM enhance your security effectiveness.

EventTracker EDR earns an AAA rating from trusted security testing firm SE Labs for its excellent performance and handling of threats from cyber criminals, putting it in the highest class of endpoint security products. Learn more here: [https://selabs.uk/en/enterprise](https://selabs.uk/en/enterprise)

Sensor Specifications

Microsoft Windows (all)

- **Servers:** 2008, 2008 R2, 2012, 2012 R2, 2016 and 2019
- **Desktops:** 7, 8, 8.1, and 10