

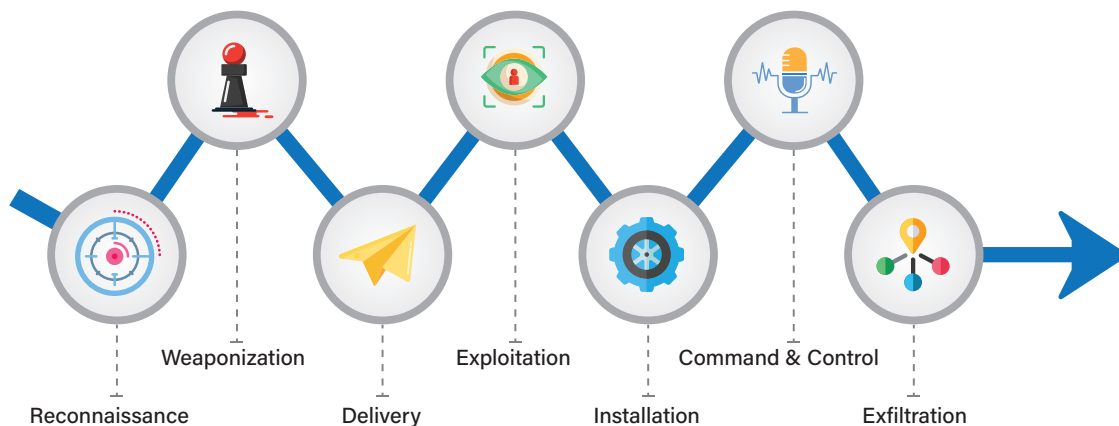
EventTracker EDR

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

EventTracker EDR is a co-managed service that protects 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 malware and network security experts who augment your team.

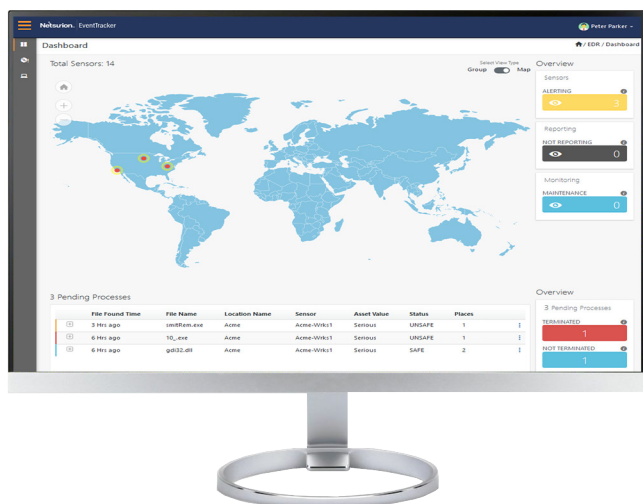
Enhance Visibility	Simplify Management	Rapidly Remediate	Augment Expertise
<ul style="list-style-type: none"> Insight across network & endpoints Pinpoint unfolding attacks Minimize false positives to detect true threats Single pane of glass when integrated with SIEM Identify adversary actions 	<ul style="list-style-type: none"> Managed service tracking internal and external threats No performance impacts with lightweight sensor Take immediate action per protection policies Single admin can manage over 10,000 systems Block threats before damage occurs 	<ul style="list-style-type: none"> Targeted remediation Forensic investigation Stop unknown malware Prevent lateral spread Integrated with > 50 threat intelligence data sources 	<ul style="list-style-type: none"> Easy to implement & maintain 24/7 access to global security experts Actionable threat intelligence Recommend mitigation steps Optimize for future threats

Stopping an attack early in the cyberattack lifecycle restricts adversary access, insights, and damage. EventTracker EDR provides visibility to inspect the entire kill chain and help investigate the steps adversaries take within an organization.



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?
- Am I prepared for future threats as adversaries evolve?



Sensor Specifications

Microsoft Windows (all)

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

Features

- A 24/7 managed service without capital costs
- Early and rapid detection of advanced and mutating threats
- ISO 27001-certified Security Operations Center
- US-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

EventTracker EDR is a 24/7 managed service that provides advanced threat protection for critical assets like endpoints and servers to quickly detect and efficiently recover from cyberattacks. Integrating your EDR solution with our co-managed SIEM platform takes a leap forward in cybersecurity 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>



Recognized for 11 consecutive years on the Gartner Magic Quadrant for SIEM.