Netsurion™
Powering Secure and Agile Networks

Security Executive Insights

Maximizing Endpoint Security

EDR Integrated with SIEM and Backed by a Managed Service is Key

Battle for the Endpoint

There are many more endpoints than fortified servers in the data center, and they are staffed by non-technical users who present softer targets for today's attacker. Attacks are continuously sprayed at every endpoint and if any one of them is successful then lateral movement is next. The traditional defense at the endpoint has been signature-based anti-virus which has proven inadequate in the current threat landscape. Aside from efficacy, there is also the problem of visibility, of detecting the kill chain, and of course the pervasive shortage of skilled staff required to administer such solutions. This leads to teams being reactive and resorting to re-imaging the endpoint as the first and only remediation. Endpoint Detection and Response (EDR) technology was initially conceived to address the post-breach visibility requirement but has evolved to provide top quality prevention as well.

Optimize EDR Effectiveness

The SOC analyst requires more advanced monitoring and analytics to gain visibility into complex and layered indicators of compromise. EventTracker EDR is designed to let the analyst quickly detect and efficiently respond to, and recover from, cyberattacks. EventTracker EDR is naturally much more effective when integrated with our EventTracker SIEM solution - enabling the business to index and aggregate systems and log data including data from endpoints. Once centralized, EventTracker EDR telemetry is used to correlate data and sharpen contextual visibility into attacks that span multiple endpoints and networks.

Better together.

SIEM

- Network-wide visibility
- Centralized log management
- Intrusion detection
- Single-pane-of-glass for SOC

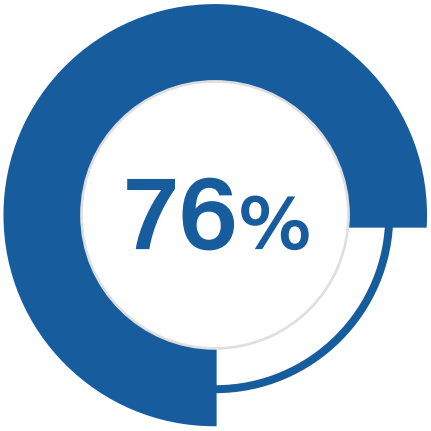
EDR

- Contextual visibility
- Behavior analysis
- Targeted remediation
- Forensic investigation

Technology Integration is Half the Battle

A defense-in-depth strategy is predicated on integration of various security technologies. When SIEM and EDR are together on one integrated platform, are integrated, the capabilities of the security team take a leap forward in cybersecurity effectiveness. The other elephant in the room is the global cybersecurity skill shortage which makes getting the promised value out of the technology very difficult.

An optimal balance between control, cost and effectiveness results from the selection of a co-managed SIEM and EDR provider who can deliver a 24/7 security operations center (SOC).



Report SIEM resulted in a reduction of security breaches

Source: "2019 SIEM Report, Cybersecurity Insiders."

Key Insights

Security executives should consider maximizing the "convergence" of their cybersecurity technology and employing managed services that are best suited to augment existing staff to bring about optimal security and compliance results.

A SIEM platform should be right-sized for organization needs and integrate threat intelligence and critical capabilities such as intrusion detection, vulnerability assessment, and even threat deception.

An EDR platform should leverage the visibility of the SIEM, provide an actionable easy-to-use interface, and leverage machine learning for effective remediation and automation.

Integrated SIEM and EDR provides consolidated visibility and threat detection with accelerated time to value.

Co-Managed SIEM Operationalizes EDR

Co-management is on the rise and expected to continue to grow as organizations have discovered that self-managing a robust SIEM and bolt-on EDR platform is too expensive, arduous to maintain, and is difficult to staff for constant monitoring. Effective security management is the result of a good collaboration between an external SOC that delivers actionable intelligence to optimize an internal IT team's effectiveness.

It is essential that endpoint security solutions help reduce false positives by scanning and collecting artifacts from endpoints as well as third-party tools like security information and event management (SIEM) and intrusion detection systems. Naturally, if the SIEM, EDR, and SOC are fully integrated, organizations stands a better chance of quickly operationalizing their cybersecurity strategy.

EventTracker EDR

EventTracker EDR is natively built into the EventTracker SIEM platform. It combines application safelisting, heuristic network and process monitoring functions to ensure that only approved programs, applications, and processes that meet your endpoint security policies can operate. All others are blocked from doing any damage. Combining endpoint and network behavior observations across the entire network, as a managed service, is especially effective against known and unknown attacks such as Zero-day and evolving threats. Early detection reduces dwell time and the risk of lateral movement. Threat intelligence sharing promotes a learn-once-defend-everywhere paradigm. Superior post breach visibility is enabled via a centralized management console with EventTracker SIEM, which supports advanced querying capabilities for the security analyst.

Enabling comprehensive visibility on all endpoints enables early detection of an attacker's progression through the kill-chain that may start low-and-slow but evolve to escalation of privileged access on servers that compromises your entire organization. Visibility into each step that a malicious actor takes is the difference between rapid detection and response or becoming a statistic with an average breach detection of 197 days according to the Ponemon Institute. As a fully managed capability, EventTracker EDR detects emerging and mutating threats 24/7 and reduces your attack surface to respond quickly before damage escalates.

Features

- A 24/7 managed service without capital expenses
- Early and rapid detection of advanced and mutating threats
- ISO 27001-certified Security Operations Center (SOC)
- One sensor, one console, consolidated reporting
- Legacy system and unpatched device protection
- Easy-to-understand remediation recommendations and reports
- 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 your endpoints
- Flexible management policies for endpoint protection and containment

EDR AAA Rated by SE Labs	"Systems protected by the EventTracker endpoint agent were exposed to a mixture of targeted attacks using well-established techniques and public web-based threats that were found to be live on the internet at the time of the test. EventTracker EDR was effective at handling general threats from cybercriminals, and preventing targeted attacks in all cases." **SE Labs**
SOC ISO 27001 Certified	"We have had a great experience with Netsurion. Overall, I like the real-time alerts, centralized log management, and visibility into security threats. We could not manage our Risk without the EventTracker SOC augmenting our staff." **Current Customer, CISO in Higher Education**
SIEM An SC Media Awarded Platform	"EventTracker is a great SIEM solution that provides continuous support. Implementation is easy as they provide hands-on support and have many integration guides. Our EventTracker SOC team is very responsive at protecting us." **Current Customer, Law Firm**

Powering Secure and Agile Networks

www.netsurion.com/eventtracker