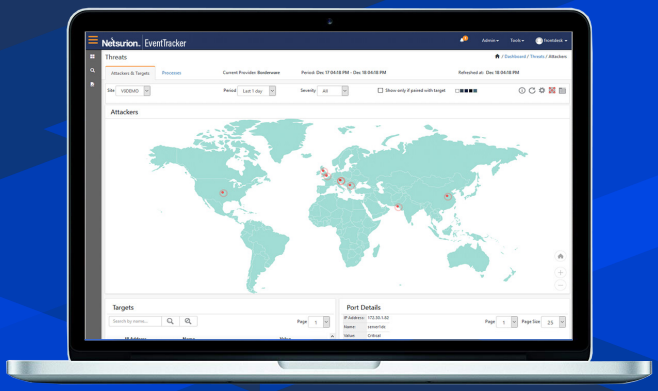
Netsurion™
Powering Secure and Agile Networks



EventTracker Security Center

One platform for all critical SIEM capabilities

Overview

Security Center is a comprehensive platform for real-time security monitoring, advanced threat detection and response, and audit-ready compliance. It identifies security threats, malware, unusual behavior and suspicious network traffic, and notifies you when you're under attack.

Whether your organization has 25 servers or 2,500, EventTracker Security Center can help by improving log analysis, awareness, detection, and incident response across all of your servers, workstations, network devices, locations, and teams.

Security Center monitors for anomalies and suspicious network activities and responds with built-in response rules to block or terminate harmful activities. Integrated threat intelligence provides curated data on bad actors, locations, and IP addresses across the globe, and alerts on unknown processes or low reputation endpoints interacting with assets inside the network. Security Center helps reduce false positives with refined internal whitelisting and correlation of unknown processes.

Simplify the audit process and reduce audit times by up to 90% using EventTracker Security Center's built-in compliance monitoring and reporting options. Detailed reports minimize the time and effort to determine potential gaps in compliance requirements and address them efficiently, empowering customers to easily maintain compliance.

Pricing

EventTracker Security Center is available by annual or perpetual license, with pricing to fit any budget. EventTracker Security Center is also available as a cloud-hosted solution deployed in our Tier 1 data center.

Features

Monitor

- Anti-virus
- Applications
- Behavior
- CPU/Disk/Memory Threshold
- Custom applications
- Databases
- File/folder access
- IDS/IPS
- Mobile devices
- Network devices
- Pre-defined policy templates
- Routers
- Servers/Workstations
- USB and CD/DVD
- Virtual infrastructure

Supported Log File Formats

- Windows EVT/EVTX
- SYSLOG (TCP/UDP)
- SNMP V1/V2/V3
- CHECKPOINT OPSEC LEA
- VMware API
- VULNERABILITY SCANNERS
- XML
- IIS/IIS W3C/IIS MSID
- TEXT FILE
- JSON
- MULTILINE
- LOG4J

Features

Automatic Remediation

- Configure automatic remediation using scripting, PowerShell, Visual Basic, and others
- Take immediate, predefined action on correlated events that meet serious or critical thresholds, or that occur after hours
- Detect data and audit changes with File Integrity Monitoring (FIM)

Behavior Analysis and Correlation

- Quickly detect and address changes in system and user behaviors
- Automatic baseline learning or flexible rules definitions determine your thresholds for alerting on anomalies
- Real-time processing and correlation for complete picture of what's new and different

Endpoint Threat Detection and Response

- Monitor and block removable media inserts and file copying
- Monitor and terminate suspicious processes
- Monitor and terminate connections to bad reputed IPs

Threat Intelligence

- Integrate threat intelligence from STIX/TAXII-compliant providers like ISACs, ISAOs, and other commercial providers
- Pre-configured integration with trusted open source providers
- Integrate with internal honeypots
- Reduce false-positives and detect hidden threats

Incident Handler's Casebook

- An Electronic Casebook, based on SANS Incident Handlers Guidebook
- Record/flag interesting incidents, reports to enable IT teams to collaborate efficiently

Reporting

- Over 2,200 pre-defined security and compliance reports
- Comprehensive support for PCI-DSS, HIPAA, ISO 27001, NIST 800-171, DoD RMG, GDPR, and more
- Easy to use wizard to provide custom definitions, filtering, grouping, and delivery options

Real-Time Alerting

- Rule-based alerts with dashboard updates and email notifications
- Incident Response Management: acknowledge, annotate, forward
- Pre-configured alerts for hundreds of security and operational conditions
- Detecting and blocking anomalous logins

Search and Forensic Analysis

- Logs are indexed to Elasticsearch using an extensible Common Indexing Model
- Flexible UI allows drill down, pivot, and include/exclude, export.
- Time slicing, trending and hundreds of pre-built common search queries using Lucene

Secure Log Storage

- Optimized, high performance Event Vault with no DBMS license required
- Archives are tamper evident with SHA-1 checksum
- Over 90% compression for efficient long-term log archiving

Dashboards

- Drillable dashboards to visualize important data
- Customizable dashlets for any user or need
- Easily scale views for small screens or SOC displays

Options Available

- Scale up and down with Collection Points reporting to a Master
- EventTracker Honeynet enables an enterprise to add a deception network layer to its cybersecurity defenses
- Flow analysis supports sFlow, NetFlow, etc.
- Host based Intrusion Detection via snort

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

Netsurion™
Powering Secure and Agile Networks

netsurion.com/eventtracker