EventTracker Essentials is a managed security service powered by enterprise technology yet packaged to deliver advanced threat protection with endpoint detection and response plus IT compliance to small- and medium-sized organizations that demand practical and cost-effective solutions.

**Network security and compliance orchestration powered by a unified SIEM platform and 24/7 SOC.**

<table>
<thead>
<tr>
<th>Log Management</th>
<th>Monitoring &amp; Alerts</th>
<th>Detection &amp; Response</th>
<th>Compliance Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure and centralized</td>
<td>Cloud-hosted SIEM</td>
<td>Critical alert outreach</td>
<td>PCI DSS compliance</td>
</tr>
<tr>
<td>400 day log archives</td>
<td>24/7 monitoring</td>
<td>Incident response help</td>
<td>GDPR compliance</td>
</tr>
<tr>
<td>Threat Dashboard</td>
<td>Daily security report</td>
<td>Host-based IDS</td>
<td>HIPAA compliance</td>
</tr>
<tr>
<td>Unlimited log management</td>
<td>File integrity monitoring</td>
<td>Automated threat remediation with EDR</td>
<td>NIST 800-171 compliance</td>
</tr>
</tbody>
</table>

"We’ve never seen a time-to-value in cybersecurity quite like what we’ve seen with EventTracker Essentials."

Jay Ryerse, CISSP | CTO, Security Products, Continuum
Alerts and Reports

Critical Threats
- Terminate processes with blacklisted hash
- Terminate connections to low reputation IPs
- Critical potential breach from low reputation IPs
- Anomalous login detection and blocking

High Risk Activity
- Windows audit log cleared
- Users added to domain admin or local admin group
- Lateral network movement

Suspicious Activity
- New TCP port started listening
- Active directory group policy change
- Admin remote logon success
- Administrative logon success
- External media inserted
- New Windows audit policy and account management activity
- New Windows software install activity
- New Windows user location affinity
- Unusual IP address activity
- User account disabled
- User account added or deleted
- Detect advanced threats

Supported Logs
- Microsoft Windows
- Microsoft Active Directory
- Microsoft Office 365
- Barracuda NG F-Series
- Cisco ASA
- Cisco Meraki
- Cyberoam
- Fortinet
- Palo Alto Networks PanOS v2.0 - 8.1
- Juniper Junos 11.4 onwards
- SonicWall UTM
- Sophos SG
- Sophos XG
- Untangle
- WatchGuard XTM
- Webroot SecureAnywhere

Powered by a Trusted SIEM Platform

EventTracker Essentials is delivered as a managed service to best-fit the security and compliance needs of SMBs.

EventTracker is lab-approved by SC Media, the cybersecurity industry’s trusted publication and has been included in the annual research report, Gartner Magic Quadrant for SIEM, for an astounding 11 consecutive years.

Sensor Specifications
- Windows 7 and higher
- Windows Embedded POSReady

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