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.

<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>

Netsurion’s EventTracker Essentials solution is the single most important product we’ve launched in our company’s history. We feel that with this offering we are at the forefront of IT security. This allows us to provide the best protection possible for our clients, which is what this is all about.

“Vice President | Netsurion MSP Partner
**Alerts and Reports**

**Critical Threats**
- Terminate processes with blacklisted hash
- Terminate connections to low reputation IP addresses
- Potential breach from low reputation IP addresses
- Anomalous login detection and blocking
- Mapped to MITRE ATT&CK techniques

**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
- 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**
- Barracuda NG F-Series
- Cisco ASA
- Cisco Meraki
- Cisco Umbrella OpenDNS
- Fortinet
- Juniper Junos 11.4 onwards
- Microsoft Windows
- Microsoft Active Directory
- Microsoft 365
- Palo Alto Networks PanOS v 2.0 onwards
- SentinelOne
- 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.

The EventTracker platform is lab-approved by SC Media, the cybersecurity industry’s trusted publication and honored by MSSP Alert as a pioneer that specializes in comprehensive, outsourced cybersecurity services for MSPs and MSSPs.

**Sensor Specifications**
- Windows 7 and higher
- Windows Embedded POSReady