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.

**Log Management**
- Secure and centralized
- 400 day log archives
- Threat Dashboard
- Unlimited log management

**Monitoring & Alerts**
- Cloud-hosted SIEM
- 24/7 monitoring
- Daily security report
- File integrity monitoring

**Detection & Response**
- Critical alert outreach
- Incident response help
- Host-based IDS
- Automated threat remediation with EDR

**Compliance Reports**
- PCI DSS compliance
- GDPR compliance
- HIPAA compliance
- NIST 800-171 compliance

---

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

Jay R., CTO, Continuum
**Alerts and Reports**

**Critical Threats**
- Terminate processes with blacklisted hash
- Terminate connections to low reputation IP addresses
- Critical potential breach from low reputation IPs
- 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
- 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.

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

---


netsurion.com/eventtracker

©2020 Netsurion, LLC