EventTracker Essentials is a managed security service powered by enterprise technology yet packaged to deliver advanced threat protection 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

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 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 IP
- Anomalous login detection and blocking

High Risk Activity

- Windows audit log cleared
- Users added to domain admin or local admin group

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

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
- Unusual Windows interactive logon
- User account disabled
- User account added or deleted

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.