Netsurion | EventTracker

GPG13 Solution Brief

www.netsurion.com/eventtracker

GPG13

About Netsurion

Netsurion powers secure and agile networks for highly distributed and small-to-medium enterprises and the IT providers that serve them. In such environments, the convergence of threat protection and network management are driving the need for greater interoperability between the NOC (network operations center) and the SOC (security operations center) as well as solutions that fuse technology and service to achieve optimal results. To this end, Netsurion has converged purpose-built network hardware, innovative security software, and flexible managed services.

Netsurion's SD-Branch solution, BranchSDO, is a comprehensive network management and security solution consisting of SD-WAN, next-gen security, cellular, Wi-Fi, and PCI DSS compliance tools and support. At the heart of the solution is the CXD, Netsurion's SD-WAN edge appliance.

Netsurion's Security Operations solution, EventTracker, delivers advanced threat protection and compliance benefits in a variety of deployment options: a SIEM platform, a co-managed SIEM service with 24/7 SOC, and a managed SIEM for MSPs.

GPG13 Compliance Overview

Deploying a good Protective Monitoring regime, as detailed within Good Practice Guide 13 (GPG13) and its 12 Protective Monitoring Controls (PMC), enables departments and agencies of Her Majesty's Government (HMG) to meet a number of mandatory requirements. These mandatory requirements are issued by the U.K. Cabinet Office as part of the Security Policy Framework, and focus on achieving proportionate risk managed approaches to allow HMG businesses to function effectively, safely and securely. Protective monitoring, also known as GPG13, encompasses people, business processes and technology to improve company risk profiles. Protective monitoring provides visibility and understanding of who is accessing an organizations sensitive data. The goal is to ensure a level of operational insight for organizations to see how their IT systems are being used or abused by internal or external agents.

By implementing the controls detailed in GPG13, HMG's departments and agencies will achieve enhanced confidentiality, integrity and availability of IT systems, impacting business sustainability and reputation. The use of EventTracker's GPG13 reporting pack provides valuable security guidance for organizations in all industry sectors to improve risk profiles.

Protective Monitoring

The policy is not reproduced here and public sector bodies should obtain it from the CESG. However, in summary, the logging requirements regarding user access to your network and systems include recording the following events:

- Unauthorized application access (where applicable)
- File access attempts to protectively marked information (e.g. RESTRICTED data).
- Unsuccessful login / logout
- Successful login / logout
- Privileged system changes (e.g. account management, policy changes, device configuration)

Logs should be kept for at least 6 months. This may include the use of backup tapes, but logs should be easily available for use as part of your incident response policy, as well as help with an investigation. In practice, this may need a system which maintains logs that are readily recoverable from any archive.

EventTracker Provides a Full View of the Entire IT Infrastructure

EventTracker SIEM improves security, helps organizations demonstrate compliance, and increases operational efficiency. EventTracker SIEM enables your organization to be more aware of potential security risks and internal/external threats. It provides you with the ability to respond to a security incident with comprehensive data and forensic tools for analysis. The time required to investigate and mitigate security incidents can be greatly reduced, minimizing potential exposure and costs.

SIEMphonic is our managed services offering that enhances the value of EventTracker implementations. Our expert staff can assume responsibility for some or all EventTracker SIEM-related tasks, including system management, incident reviews, daily/weekly log reviews, configuration assessments, and audit support. We augment your IT Security team, allowing you to focus on your priorities by leveraging our expertise, discipline and efficiency.

Scalable, Log Collection and Processing with Notifications based on Criticality

EventTracker SIEM provides automatic consolidation of thousands, or even millions of audit events, to meet the needs of any size organization. The inbound log data is identified by EventTracker's built-in Knowledge Base, which contains log definitions for thousands of types of log events, and automatically identifies which events are critical to security standard.

EventTracker SIEM provides real-time and batch aggregation of all system, event and audit logs from your firewalls, IDS/IPS, network devices, Windows, Linux/Unix, VMware ESX, Citrix, databases, MS Exchange web servers, EHRs and more.

Ease of Deployment and Scalability

EventTracker SIEM is available on premises or as a highly scalable cloud-based SIEM and Log Management solution. It offers several deployment options to meet the needs of organizations with a few dozen systems or those with thousands of systems spread across multiple locations. EventTracker Cloud is available as an AMI on Amazon EC2, Microsoft Azure or your cloud infrastructure provider of choice. It supports multi-tenant implementations for MSSP organizations serving the needs of smaller customers.

GPG13 Compliance Requirements

Requirements	EventTracker Solution	EventTracker Reports	EventTracker Alerts
PMC-1 Accurate Time Stamps	EventTracker provides accurate, consistent and independent time synchronization across all collected accounting data, and detects abnormal patterns, such as time adjustment, both back and forward.	Yes	Yes
PMC-2 Recording of Business Traffic Crossing a Boundary	EventTracker analyzes network events and combines accounting data from other boundary devices to establish a record of all cross-boundary imports and exports. Raw accounting data is checked against applicable policy in real time, and alerts and reports are generated if any policy breaches or other malicious activities are detected.	Yes	Yes
PMC-3 Recording Relating to Suspicious Activity at The Boundary	EventTracker analyzes the behavior of boundary traffic and immediately identifies any suspicious or unusual traffic. Alerts are generated and distributed in real time, and all raw data is made available for data mining and forensic analysis.	Yes	Yes
PMC-4 Recording on Internal Workstation, Server or Device status	Workstation, server and other device accounting data is collected and analyzed by EventTracker in real time. EventTracker automatically detects when suspicious activity occurs, such as configuration changes; privileged access and unauthorized escalation; unexpected system and application restart; software installation and patch failures; removable media insertion and removal; sensitive file access and more.	Yes	Yes
PMC-5 Recording Relating to Suspicious Internal Network Activity	EventTracker constantly monitors the behavior of users, networks, machines and applications. Alerts are generated in real-time, whenever any suspicious activity is detected, to indicate an external breach has occurred or an insider is acting maliciously.	Yes	Yes
PMC-6 Recording Relating to Network Connections	All connections made to a network are analyzed by EventTracker including wireless, VPN and dial up. EventTracker automatically detects and alerts on any suspicious activity, such as attempt to gain access or wireless network hacking attempts.	Yes	Yes
PMC-7 Recording on Session Activity by User and Workstation	EventTracker monitors user activity across the network, including data access and communications. EventTracker ensures that any security policy breaches or suspicious patterns of behavior are identified and alerted on in real time. The raw accounting data is also available in EventTracker for reporting and ad-hoc analysis purpose.	Yes	Yes
PMC-8 Recording on Data Backup Status	EventTracker monitors Accounting data related to the status and operation of backup and restore process. EventTracker can identify and generate alerts if an error in the backup and restore process occurs, such as failure to complete a backup/ restore, data corruption or deletion.	Yes	Yes

Requirements	EventTracker Solution	EventTracker Reports	EventTracker Alerts
PMC-9 Alerting Critical Events	EventTracker categorizes and prioritizes all the alerts it generates based on risk. Alerts can be viewed centrally via the EventTracker console using the dashboard view.	Yes	Yes
PMC-10 Reporting on The Status of the Audit System	EventTracker enables all aspects of the audit process – from data collection to viewing, alerting and reporting – to be independently tracked and audited.	Yes	Yes
PMC-11 Production of Sanitized and Statistical Management Reports	EventTracker ships with hundreds of compliance and security status and management reports, for example number of failed logons, number and type of intruders detected, average time to resolve the security incident, etc. The reporting function is highly configurable – existing reports can be amended or new ones written simply through the interface.	Yes	Yes
PMC-12 Providing a Legal Framework for Protective Monitoring Activities	EventTracker is deployed and configured in accordance with the guidance recommended as a part of the overall risk management process. Throughout the accounting data collection process, EventTracker ensures that all data is collected and analyzed for forensic validity.	Yes	Yes