

**Logging in Depth**

EventTracker is a complete Security Information and Event Management (SIEM) solution that combines real-time Log Management (Search, Correlation, Analytics, Reporting, USB tracking, Automatic Remediation) with powerful network traffic monitoring, policy-based Configuration Assessment and File and Registry Integrity monitoring in one turnkey software package. EventTracker enables compliance with a wide variety of regulatory standards, protects critical systems from both traditional and emerging security threats and helps improve service levels and availability.

**Event Log Collection**

EventTracker provides automatic, unattended consolidation of millions of events in a secure environment in real-time from a variety of sources – including Windows, UNIX/Linux, Syslog, z/OS, Solaris BSM and SNMP devices.

- Agent Optional - Supports either agent or agent-less setup, or a combination
- Guaranteed, encrypted (FIPS-140 compliant) transmission of events between agents and console
- Prioritized event delivery
- High speed direct log archiver supports non real-time log import
- Highly scalable collection-point architecture – supports multiple virtual collection points on a single machine as well as collection points on multiple machines for unparalleled scalability.

**Centralized Event Log Monitoring**

The advanced, central web console puts the security manager, event log monitor, event log reporting and analytics engine at your fingertips. Instantly display events from all systems on a centralized console and customize views using multiple dashlets and rule based filtering.

- Alert console combines vulnerability, asset value and threat data to prioritized events based on criticality
- Real-time notifications via RSS, text message, SNMP or email
- Event Filtering
- Log File and Application Monitoring
- User Tracking and USB device monitoring
- Indexed, high speed Log Search
- Network Connection and Device Monitoring
- Network Traffic Monitoring
- Process and Service Monitoring
- System Monitoring
- Centralized Security Policy Editor
- Automatic remediation – block USB access, terminate process, execute custom script etc

**Event Consolidation**

- Centralized, secure and compressed event storage
- Archive compressed (over 90% compression) events in a tamper proof store, with on-line storage limited only by disk space.

**Event Correlation**

- Correlate events from multiple servers and domains for faster decision making and greater security.
  - Example: Generate an alert condition when you have 100 logon failures in five minutes in all domain controllers.
- Search out-of-box correlation rules to detect the most common and critical security conditions.
- Create customized correlation rules and actions.
- Search user defined pattern(s) of events or sequence(s) of events in real-time.

**Activity Monitoring**

- Automatically monitor any system variable for first seen or unusual patterns of activity
  - Example: Record first time execution of any new process or alert on abnormal usage patterns in areas as user logons or network activity
- Continuous auto-learning for baselining with, user-configurable thresholding

**Event Analysis and Forensics**

- Ability to quickly and easily search through terabytes of log data to pinpoint critical events behind security and operational incidents; Google-like search interface
- Ability to search and scan events using single and multiple strings within an Event description, freeform keywords, phrases, operators, wildcard characters

- Supports Pearl Compatible Regular Expression (PCRE)
- Over 500 predefined rules to search the most common conditions

**Reporting**

- Over 2000 summary and detail templates for security, compliance and operations
- Compliance templates for SOX 404, PCI-DSS, HIPAA, GLBA, FISMA, FFEIC, NISPOM, BASEL II, FDCC
- Report templates include Active Directory, security related events, login-logoff events, application related events, domain admin activity, password reset, account lock out, security profile changes, logon failures, system performance, software maintenance activities, trend analysis
- Ability to generate customized reports
- Generate reports automatically according to schedule or on-demand
- Report delivery via email and/or notification via RSS

**Change Monitoring**

- Monitor and alert on critical Windows applications, services, registry entries or files
- Compare snapshots with a master configuration or for change over time
- Restore to previous working configuration
- Automatically generate change reports

**Configuration Assessment**

- Certified SCAP-based configuration assessment
- Monitor for FDCC or DISA STIG compliance

**IP Traffic Monitoring**

- Collect and analyze netflow information
- Supports netflow versions 5 and 9

**Key Enterprise Features**

- Group systems based on business or management units
- Monitor and create reports based on groups and organization
- Manage and distribute configuration to groups of systems or to all systems
- Quick and easy upgrade of new version to all systems in both domain-based and domain-less Network configurations
- Hierarchical event and security monitoring with support for multiple consoles and event stores
  - Example : Headquarters based consoles monitor systems from all offices but a branch office console monitor only systems in that branch
- Forward events to trouble ticketing system or SNMP manager(s) such as HP OpenView, Tivoli, Unicenter

**EventTracker Framework**

- Support for Windows domain-based and domain-less Network configurations
  - Domain Windows Explorer – Domain-wide file explorer; ability to change file audit on any system within the domain; ability to change file permission from any system within the domain; ability to copy files from one system to any system; ability to find file in any/all systems within a domain; ability to start the performance monitor on any system.
  - Domain-Less Topologies – Seamlessly configures and monitors systems outside an Active Directory or NT domain. Apply configurations, upgrades, change the settings, restart services, and monitor security and configuration.
- Active Directory (AD) – Organizational Units (OUs) Administrator Console – Reliably deploy (install, remove, upgrade, configure) agents to monitored systems from a central console. Actions can be restricted to user-defined groups.
- Automatically backs up and clears the windows event logs when needed

**Installation**

- Rapid installation of EventTracker Console (next->next->done); monitor events instantly
- Quick provisioning and installation of EventTracker Agent(s) from the central console on Windows systems within the domain in strict compliance with defined security policy
- Centralized installation of EventTracker Agent on Windows systems outside the domain