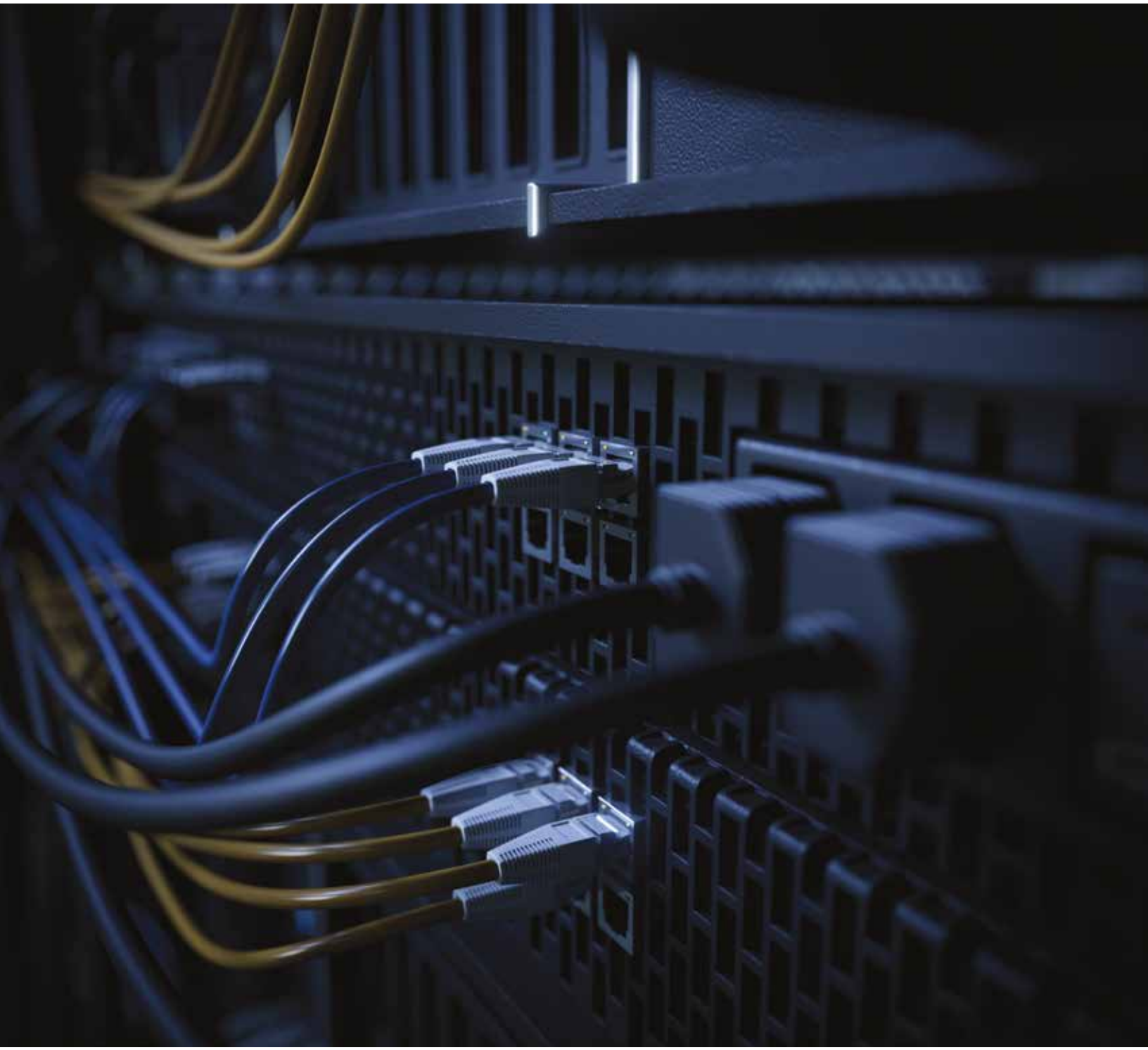
Canon
CANON SOLUTIONS AMERICA

EVENTSENTRY



SECURITY INFORMATION EVENT MANAGEMENT

Intelligent Threat Mitigation

SMART CHANGE STARTS HERE.

CANON SEE IMPOSSIBLE

KNOW WHEN YOU NEED TO ACT.

Delivering meaningful insight into your network data.

Executive Summary

EventSentry is a powerful monitoring solution that provides your IT team with actionable network data that helps drive intelligent IT decisions—in real time. Reliable, secure, scalable, and easily deployed, EventSentry will help enhance the performance of your network while helping you in your compliance efforts. Help save time, prevent disasters, and reduce TCO with a cost-effective monitoring solution. New users are up and running in minutes and can easily adapt the solution to suit their needs—with amazing customer service at their fingertips.

Supporting IT

Give your IT and security teams the toolset they need to help your organization to remain in compliance with standards and regulations such as ISO / IEC 27001, SOC 2 audits, HIPAA, PCI-DSS, SOX and more. Once analyzed, the data that is aggregated can help to support operational project planning efforts to enhance security policies and infrastructure updates to protect your business.

- Software/Hardware inventory
- Detect Hardware and software issues
- Easily integrate with 3rd party help desk software
- Monitoring 3rd party software
- Fully customizable dashboards

- Detect network security violations
- FIM and access tracking
- In-depth Active Directory monitoring
- Compliance templates

- Performance trends
- Disk space trends
- Forensic analysis

Key Features

- Correlate and monitor event logs and log files in real time as well as monitor performance, disk space, services, processes, and much more on both physical and virtual (cloud) servers and workstations.
- Track processes, console and network logons, file access, account management events, and even policy change events to help with compliance with PCI, SOX, HIPAA, CJIS and others.
- Visualize data with insightful dashboards and a powerful job and reporting feature. Reporting supports granular authentication and sophisticated log searching.
- Supports reliable, secure (TLS) and compressed data transmission over insecure media with the new collector service.
- Extend core functionality with the application scheduler feature, which integrates existing or new scripts into the monitoring environment.

Monitoring Coverage

NETWORK	SERVERS, WORKSTATIONS & DEVICES	LOGS
• SNMP Traps • Active Directory • NetFlow • ARP	• Services and Processes • File Integrity Performance (FIM) • NTP • Scheduled Tasks • Audit Policies	• EVENT LOGS • Logs • Syslogs
• Change Tracking • User Management • Group Policy Changes • Threats • Bandwidth • New Devices • Spoofing	• Digital Signature • Entropy • Windows • SNMP	• Raw Events • Normalization • Structured • Non-Structured • Integration • Consolidation

Dashboard

The EventSentry dashboard provides real-time monitoring of normalized activity log data, providing security and IT workers a single pane of glass that can enable them to react quickly and effectively to anomalies and suspicious events.

imageRUNNER ADVANCE SIEM Integration

All newly released imageRUNNER ADVANCE Third Generation III devices now offer the ability to automatically generate syslogs directly into Event Sentry and other popular SIEM products. This creates yet another critical component in the cybersecurity segment of the Canon Solutions America defense in-depth 5 pillar security strategy.

AVAILABLE LOGS:

- User Authentication Log
- Job Log
- Transmission Log
- Mail Box Operation Log
- Mail Box Authentication Log
- Advance Box Save Log
- Advance Box Operation Log
- Import / Export All Log
- Network Authentication Log
- Machine Management Log
- Audit Log Management Log

Key Benefits

- A SIEM is a critical and pivotal element in any defense-in-depth security strategy
- EventSentry enables IT and security personnel to make intelligent decisions in real time
- Aggregates security data from across your entire organization
- Helps security teams detect and respond to security incidents
- EventSentry can create compliance and regulatory reports
- EventSentry is simple, scalable and easy to deploy
- Ultimately, EventSentry can help to prevent disasters from happening

Features Overview

EVENT LOG MONITORING & CORRELATION

Real-time event log monitoring and correlation which supports advanced features such as thresholds, recurring events, timers, insertion strings, and more.

COMPLIANCE TRACKING

Track file access activity, processes and console logons, successful or failed network logons, account management, and more to help with PCI, HIPAA, CJIS, SOX, and other compliance requirements.

LOG FILE MONITORING & CORRELATION

Monitors and correlates any log file (e.g. IIS, DHCP, Backup, Firewall) in real time and sends alerts upon matching text. Create custom views for delimited log files in the web-based reporting.

PERFORMANCE MONITORING

Monitors any Windows performance or SNMP counter and supports smart alerts as well as long-term data collection. Includes smart features such as leak detection and self-learning.

EXTENSIVE INVENTORY

Inventories installed software and patches as well as hardware information, including VM inventory (VMWare© and Hyper-V©). Shows warranty status on Dell©, HP© and IBM© servers as well as physical switch port mappings.

DISK SPACE MONITORING

Receive alerts based on absolute or percentage limits on drivers or folders. View and predict disk space usage with intuitive charts. Shows the 250 largest files on volumes to speed up disk space cleanup efforts.

NETWORK TIME SYNCHRONIZATION

Verifies and optionally synchronizes the local system time with one or more remote Network Time Protocol (NTP) servers based on RFC 1769 and RFC 1305.

PROCESS, SERVICE, AND SCHEDULED TASKS

Proactively monitors services, scheduled tasks and stand-alone processes. Failed processes and services can be restarted automatically.

SECURITY

Enhance your network security with real-time security log monitoring, file integrity monitoring, and service monitoring, as well as ARP monitoring which detects new devices plugged into the network.

NOTIFICATIONS

EventSentry includes 16 different notification types including: SMTP Email, Syslog, SNMP Traps, HTTP(S), Jabber (IM), database, SNPP, RSS, text file, network, processes, reboot, service control, desktop, and more.

LIGHTWEIGHT MONITORING

Our agents monitor your hosts without affecting the performance of the monitored hosts, while also helping minimize network bandwidth usage. EventSentry is also an economical solution that fits most budgets.

CENTRAL COLLECTOR SERVICE

A central collector service supports data collection over insecure mediums (e.g. Internet) through strong TLS encryption. Also supports local caching and compression.

WEB REPORTING

Next-generation web reporting with dashboards, granular access control, flexible reporting, jobs engine, and extensive visualization tools. Extensive API to access data from 3rd party software. Works with all major browsers and mobile devices.

HEARTBEAT MONITORING

Centrally monitors the uptime of hosts and TCP services and provides availability stats.

SYSLOG/SNMP/ARP DAEMON

Collects Syslog messages and SNMP traps (v1-v3) centrally from Unix/Linux hosts and/or network devices. Alerts matching configured rulesets can be dispatched in real time.

UPTIME MONITORING

Continuously logs the current uptime as well as the uptime history across reboots. Helps identify problematic servers that are rebooted too often and also records the longest uptime.

CANON SOLUTIONS AMERICA

1-800-815-4000 CSA.CANON.COM/SECURITY

4/19-364-3266