



## Introduction

Security On-Demand's Log Management On-Demand service raises the bar for compliance reporting, log analysis, risk management and real-time event correlation. Our service offering lowers the cost of ownership, product learning curve and implementation time, while increasing the usability and satisfaction that clients have in operating a simple to use, straightforward, low-cost solution.

## “Security-as-a-Service” Cloud Approach

Security On-Demand utilizes a “software-as-a-service” cloud approach which delivers immediate value at a lower cost compared to procuring, integrating, and operating technology “in-house”.

Some of the key advantages to this approach include lower cost of ownership, reduced integration time, Best Practices Implementation, pre-tuned device parameters (less customization), and no staff learning curve or expensive training required. We also provide your IT department security operations support that improves IT efficiency via a structured process for alert triage and 24x7 monitoring coverage that extends and expands your IT department's resources.

## Solution

Our Log Management On-Demand solution offering includes the following components

- ... **Log Collection**—Agentless collection, normalization, aggregation & correlation of data
- ... **Monitoring & Correlation**—24x7 Monitoring of all event data and correlated alerts
- ... **3rd Party Log/Collector Support**—Supports existing log collection devices already owned
- ... **Custom Audit Log Monitoring**—Can monitor proprietary audit logs from applications
- ... **Compliance**—Fully addresses regulatory compliance requirements for SOX, PCI, HIPAA, etc.
- ... **File Integrity Monitoring**—Can provide optional functionality with file change monitoring
- ... **Reports & Analysis**—Offers multiple canned reports, ad hoc query, and log analysis tools

## Key Features

- ... **Log Centralization**—Saves time & money, simplifies searches & reporting by consolidating all data into a single database repository
- ... **Device Support**—Supports virtually any type of Host (Server/PC), Network, or Security Device (WMI, syslog, or custom) without the installation of agents
- ... **Custom Audit Log Support**—Can read and monitor proprietary log formats, audit trails, database files, and application logs
- ... **Non-Repudiation**—Eliminates risk that logs may be altered by an insider or an attacker since all logs are copied into a secure database and stored off-site
- ... **No Licenses or Hardware Required**—Cost of all licenses & maintenance are included in service
- ... **Pay-as-you-grow Subscription Model**—Use only what you need, reduce or add coverage any time you make a change to your network without a small fortune invested in software licenses
- ... **Ease of Integration**—No more integration headaches and long integration cycles, the system is pre-built and pre-optimized with Best Practice configurations for most devices & systems
- ... **Lower Cost of Ownership**—Compared with IT training costs and cost of maintaining internally

## Audit & Compliance Logs

There is no need to worry about providing reports and documentation to support audits and satisfy regulators when your logs and compliance reports are provided by our 24x7 monitored, Log Management On-Demand Service.

Our solution enables IT Managers, compliance officers, auditors, network engineers, security professionals and forensic analysts to examine, process and analyze correlated log data immediately, and in-real time as data is being collected.



Regulation	Section	Required?
Payment Card Industry Data Security Standard (PCI-DSS)	Section 10: “Retain audit trail history for at least one year”, plus Sections 11 & 12	Yes
Health Insurance Portability & Accountability Act (HIPAA)	NIST Pub 800-66, Section 164 105(c)(1): “Retain required documentation of policies, procedures, actions, activities, or assessments required by the HIPAA security rule for 6 years”	Yes
Sarbanes-Oxley (SOX)	Section 103: “Prepare and maintain for a period of not less than 7 years, audit work papers and other information related to any audit report in sufficient detail to support the conclusions reached in such report”	Yes
Gramm-Leech-Bliley Act (GLBA) & FFIEC Guidelines	Requires logging of all access to personal information (by a person or user to view, read, write, or delete)	Yes

## Log Collection vs. Correlation

Most log management products collect and aggregate logs, but do not provide real-time analysis and alert correlation. For those solutions that do provide this capability, there is enormous complexity, management overhead, learning curve, and lengthy tuning periods that increase the costs and extend the time for return on investment.

Our service extends beyond what log collection systems can do by immediately detecting and escalating a security event that is worthy of further analysis. Security On-Demand provides true business risk and compliance analysis that is integrated into a security dashboard which present risk data in real-time, while integrating security operations and compliance management functions into a fully unified and integrated threat management system.

## Technology & Architecture

Our technology takes advantage of Best of Breed vendor technology at it's core while providing a proprietary and integrated and customized Security dashboard for the client. As part of this integration, we have created our own patent pending log event triage system that incorporates ITIL based workflow for alert processing and coordinated incident response.

### Key Technological Advantages include:

- ... Our solution offers an innovative risk-based model instead of a rules-based correlation approach
- ... Each alert that we detect computes a risk score. Risk = Threat x Vulnerability x Asset Value
- ... The risk score is based on underlying factors and algorithms that evaluate the frequency of events, severity, threat potential, and other factors.
- ... High performance database that can track and store thousands of events per second and millions of events per day without any impact on performance.
- ... User-defined compliance analyses using real-time data for instant, on-demand, intra-period, and ad hoc compliance reporting.
- ... Business intelligence Dashboard provides instant awareness of security metrics, critical information, summary data and presentation of security metrics that allow "drill downs" via various charts, graphs and tables that provide rich information of integrated alert and event data.
- ... Analysis tools that link security operations and vulnerability management with forensic data, which eases audit compliance by combining analyses in a single system.
- ... Data collection *without* the use of client agents that can also log audit data from databases and proprietary apps.



## Compliance with PCI

We meet all of the PCI mandated Log collection and monitoring requirements, in sections 10, 11, & 12 including:

Section	PCI Requirement
10.2	Implementation of, and access to audit trails, changes made within applications that affect application or system security
10.3	Audit Trail log entries that contain user, time/date, event identity, event origination, success & failure system component, etc.
10.5	Centralizing & Preserving Audit Trails
10.6	Daily Log Review & Monitoring
10.7	1 Year Audit trail history, Minimum of 3 Months On-line

