



Solution Brief: ArcSight Log Management Suite

Collect and Manage Avalanche of Event Logs

The ArcSight Log Management Suite delivers universal audit quality log collection and role based analysis portals for IT operations, security and compliance.

Highlights

- Scalable, distributed collection and centralized storage architecture in a range of deployment options
- Audit quality collection of all logs from any commercial or custom source
- Personalized, role-based dashboards with drill down reporting and real time alerting

The Need for a Log Management Solution

Regulatory compliance mandates including PCI, Sarbanes Oxley, HIPAA, and FISMA have imposed overwhelming requirements on organizations to collect, store, and analyze tremendous volumes of log data across their entire infrastructure—from physical, network and security devices to hosts, databases and applications—for extended durations and at increasingly granular levels. Log data can also provide visibility into network, system and application health and availability; support security operations; and streamline network troubleshooting. Despite these mandates and clear benefits of log management, organizations struggle with the numerous challenges associated with existing log management solutions:

- Massive and growing log volumes
- Unsupported custom and legacy log generating sources
- Bandwidth contentions between logs and transactional traffic
- Lack of audit and litigation quality log data
- Growing cost of long term log storage
- High cost of meeting audit reporting requirements
- Lack of scalability in log management infrastructure
- Lack of easy-to-use reporting and analysis capabilities

ArcSight Log Management Suite: The Ideal Solution for Log Management Needs

To address the growing need for collection, storage and analysis of enterprise-wide log data, the ArcSight Log Management Suite is delivered in a range of turnkey, stackable appliances that support high performance audit quality collection of all logs from all sources into a highly compressed but easily searchable enterprise log repository.

The ArcSight Log Management Suite offers a cost-effective distributed collection and centralized storage architecture that scales linearly and delivers unmatched price/performance to lower compliance, security and IT operational costs. With its powerful log analysis, real-time alerting, personalized role based portal and out-of-the-box collection support for over 180 commercial event-generating sources and any custom or legacy database or application; the ArcSight Log Management Suite greatly simplifies forensic analysis, compliance audits and organizational reporting, while eliminating inefficient, error-prone manual procedures.

The ArcSight Log Management Suite is tightly integrated into the broader ArcSight product suite for advanced correlation or can also function as a standalone solution for log management.

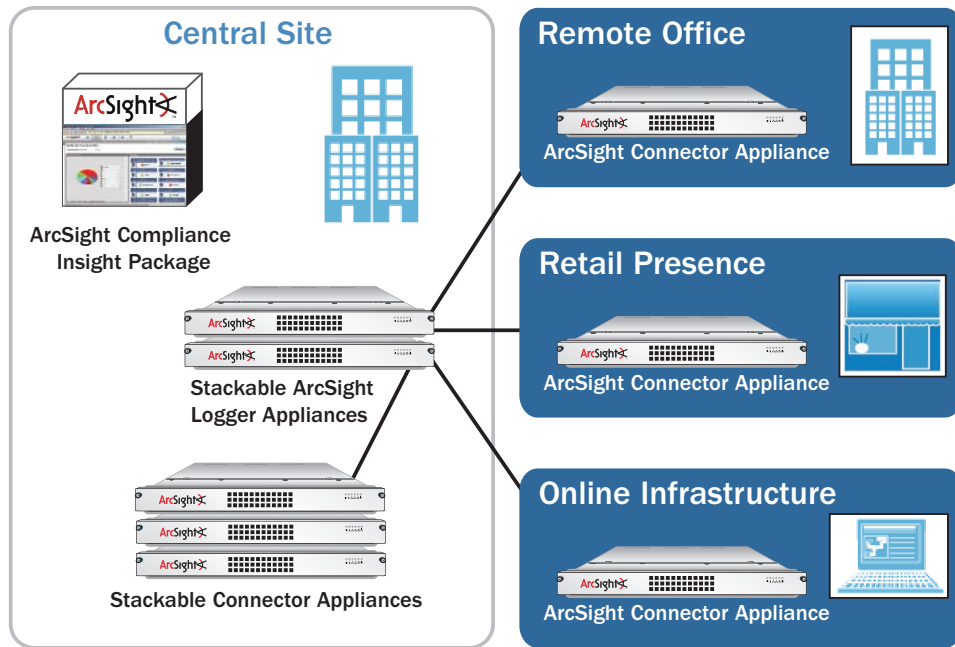


Figure 1: The ArcSight Log Management Suite supports several deployment options optimized both for small businesses as well as large, heterogeneous and widely distributed environments.

Components of the ArcSight Log Management Suite

The ArcSight Log Management Suite supports multiple deployment options and is optimized for both small as well as large, heterogeneous and widely distributed businesses.

Key components include:

- **ArcSight Logger.** Appliances that provide advanced high performance log collection, cost effective archival and powerful personalized analysis.
- **ArcSight Connectors.** The industry's broadest and deepest software or appliance-based event collection support spanning the entire IT infrastructure, including custom sources, in-house applications and physical access points.
- **ArcSight Compliance Insight Packages.** Prepackaged reports, alerts and dashboards mapped to the needs of regulations or industry mandates and audit best practices to automate audit reporting requirements.

In the deployment scenario shown in Figure 1, the organization has a major remote office in addition to its corporate data center. Both locations have local IT staff and the remote location generates a significant amount of logs which are frequently analyzed by the local IT helpdesk and security teams. ArcSight Logger is deployed in both locations to provide localized storage and to minimize unnecessary network traffic. Auditors who less frequently need to analyze logs corporate-wide can use distributed querying across locations for a global perspective. Other

smaller retail and e-commerce infrastructure locations are equipped with the ArcSight Connector Appliances which provide audit quality log collection and secure, reliable transfer of logs to the corporate data center. This is just one of many possible deployment scenarios.

Next-generation Log Management Platform Scalable Architecture

The ArcSight Log Management Suite uniquely supports a cost effective distributed collection and centralized storage and management architecture that ensures audit and litigation quality of all data as well as transaction assurance. Both ArcSight Logger and ArcSight Connectors are available in a range of appliance models that can scale from small business needs to large, distributed, heterogeneous networks. These stackable appliances allow organizations to easily scale collection and analysis performance as well as onboard capacity linearly. Large organizations with multiple administrative domains or managed security service providers can choose to deploy multiple ArcSight Logger appliances in a hierarchical or peer-to-peer manner to extend capacity and performance as needed. Since multiple ArcSight Logger appliances operate as an array, a universal view into corporate wide log data remains available.

Universal Event Collection

ArcSight Logger supports collection of raw logs directly from any syslog or file-based log generating source and also leverages the vast library of ArcSight Connectors that collect from over 180 distinct log generating sources.



ArcSight Connectors pre-process and optimize logs for analysis. Additionally, the ArcSight FlexConnector framework extends log collection capabilities to custom sources and in-house applications that are required for regulatory compliance.

High-Performance Collection

At the high end, ArcSight Logger captures raw logs at sustained rates in excess of 100,000 events per second per appliance. Performance can be linearly scaled through the addition of ArcSight Logger appliances which operate as an array of peers. Across the ArcSight Logger appliance family, a range of collection performance options are available to optimally address the needs of both large and small organizations.

Transaction Assurance

Remote locations are often connected to corporate data centers over low bandwidth links which must be shared by log traffic and transactional data. The ArcSight Log Management Suite provides several measures to ensure that business critical transactional traffic is always prioritized. In addition to compressing all log data, a specific amount of bandwidth can be allocated to log traffic. Within the bandwidth allocated to logs, high severity log events that must be analyzed in real time can be prioritized. If peak business hours require dedicated use of bandwidth for transactional data, logs can be cached locally and batched to the central repository during off hours.

Minimal Footprint at Remote Sites

The ArcSight Connector appliances allow highly-distributed organizations to cost-effectively and easily manage audit-quality event collection by offering an energy efficient 1U appliance for remote collection. Once deployed, these appliances can be configured, updated, upgraded and administered en masse from the central location over a web interface. In locations where no additional rack space is available, ArcSight Connectors can also be deployed on non-critical hosts that have spare computing capacity. Regardless of deployment form factor, collection is agentless and does not require placement on the end device or log generating source.

Storage Flexibility

The ArcSight Logger appliance family can store up to 15TB of uncompressed logs per appliance which can be scaled linearly through the addition of more appliances. In addition to bundled onboard storage, ArcSight Logger appliances support external storage, both as a primary data store and as an archival destination. Regardless of whether the storage is onboard or off-board, log data is always efficiently compressed at a ratio of up to 10:1. Organizations can define multiple retention policies based on regulations they are subject to or in accordance with internal standards. Log data can be flexibly assigned to these policies based on

source type or IP address. Once defined, retention policies are automatically enforced, eliminating the need for manual data disposition or clean-up efforts.

Audit Quality Log Data

The use of logs in compliance audits and litigation requires organizations be able to demonstrate the integrity and availability of log data both in transit and at rest. Even a few missing or compromised log events can lead to inaccurate audit results or may create doubt around the validity of audit reports.

Several audit quality controls are built into the ArcSight Log Management Suite. ArcSight Connectors provide local caching at remote sites which mitigates the impact of a connectivity loss between remote offices and central log aggregation points that would otherwise lead to a loss of critical event data that may be the missing link in an audit or investigation. The ArcSight Log Management suite also supports automated failover from ArcSight Connectors at the remote location to a secondary centralized ArcSight Logger destination in the event that the primary destination is unavailable. Logs are transmitted and stored reliably - to ensure that critical events (such as logs that indicate compliance violations) are not dropped or lost due to saturated transmissions links, lack of buffers at the source, or unreliable transport protocols. Integrity checks are enforced in accordance with the NIST 800-92 Log Management standard and ArcSight supports raw data collection across all devices. Granular role-based access controls protect both system objects and event data.

Powerful Analysis

The ArcSight Log Management suite delivers a powerful combination of historical and real time analysis options ranging from personalized dashboards and comprehensive interactive reporting to high speed searches and intelligent alerting. Users are presented with visually appealing, interactive and personalized dashboards that combine relevant and related reports into a single role-based view. From these aggregate dashboard views, users can drill into specific report elements to simulate audit workflow and investigate policy violations or anomalies. Interesting results in reports can be further analyzed using a web based search interface to conduct rapid ad hoc audit investigations for root cause analysis. In turn, the search patterns can be converted into real-time alerts to ensure that subsequent incidents and pattern matches lead to real time notification as the incidents and violations occur.

All content can be built using a unique device-independent taxonomy that allows end users to easily and intuitively navigate through log data without familiarity with source-specific log syntax. This abstracted and intuitive taxonomy also eliminates content explosion and device or vendor specific analysis.



Pre-packaged Solutions

Dashboards, reports, search filters and alerts are available out-of-the-box to address common compliance, operational and security monitoring needs. In addition, solution packages mapped to specific regulations and mandates such as PCI are also available. These pre-packaged solutions enable organizations to continually monitor their compliance status and automate compliance audits based on established best practices while also saving on internal research and development costs.

Complement Your SIEM Investment

Log management and SIEM solutions are part of a continuum of value extraction from logs for reporting, real time monitoring and remediation. Organizations expect synergy across these investments and ArcSight is unique in offering a tightly integrated platform for both log management and SIEM.

The ArcSight Log Management Suite can complement any SIEM investment to provide a cost effective long term log repository. More specifically, it integrates bi-directionally with the market-leading SIEM offering—ArcSight ESM. The integration allows ArcSight Logger to flexibly forward relevant security events to ArcSight ESM for real-time, cross-device correlation, visualization and threat detection. In turn, ArcSight ESM can send correlated alerts back to ArcSight Logger for search and archival. Both investments leverage a common collection infrastructure built on ArcSight Connector technology.

About ArcSight

ArcSight is a leading provider of security and compliance solutions that intelligently identify and mitigate business risk and deliver a centralized view of enterprise-wide events across heterogeneous infrastructures. This real time and historic view into external attacks, insider threats and regulatory compliance provides enterprises, MSSPs and government agencies with the intelligence and response capabilities required to effectively protect and manage their networks and their businesses.



ArcSight, Inc.

5 Results Way, Cupertino, CA 95014, USA
www.arcsight.com
email: info@arcsight.com

Corporate Headquarters: 408 864 2600
EMEA Headquarters: +44 870 351 6510
Asia Pac Headquarters: 852 2166 8302

© 2007 ArcSight, Inc. All rights reserved. ArcSight and the ArcSight logo are trademarks of ArcSight, Inc. All other product and company names may be trademarks or registered trademarks of their respective owners. 11/07