Product Brief: ArcSight Logger

Simplifying Log Collection, Storage and Analysis

ArcSight Logger is a turnkey appliance for collection, efficient storage, and high-performance search and reporting of all enterprise log data.

Highlights:

- Comprehensive log aggregation: Raw log data as well as optimized out-of-the-box collection for over 275+ distinct sources
- Audit-quality log repository: Secure collection and storage, integrity checks, granular access controls and automated retention policies
- Powerful analytics: Comprehensive reporting and real-time alerting engine with prepackaged regulatory content

ArcSight™

The Need for a Robust Log Management Solution

Compliance, security and IT operations teams recognize the value in collecting, archiving, and analyzing log data to deliver visibility into risk posture, compliance and audit automation, rapid threat detection and improved service level agreements. To address these use cases, any log management investment must support event collection from a large variety of sources, ranging from network and security devices to databases and homegrown applications.

In addition to broad device support and high-performance log aggregation, compliance and forensics use cases also mandate audit-quality log collection and storage. Only collecting logs at the source of origin can guarantee end-to-end security, reliability and availability of collected events. This requires a turnkey, scalable log management solution that can easily be rolled out and managed across hundreds or even thousands of locations to ensure complete collection of all enterprise event data.

Once collected, log data needs to be retained for varying periods, often multiple years, as dictated by regulations such as SOX, PCI, FISMA, HIPAA and GLBA or existing corporate retention policies. A cost-effective log storage strategy is therefore paramount. Log collection infrastructure must offer store and forward capabilities to a centralized location where data is compressed and stored securely, but is readily accessible for analysis.

Beyond aggregation and efficient storage of logs, a complete log management solution must support high-performance analysis without compromising collection rates or storage efficiency. To comprehensively

address these use cases, the aggregated log data must be accessible through an intuitive interface with drill down navigation across terabytes of log data.

ArcSight Logger: The Solution for Log Management Needs

To address the growing need for collection, storage and analysis of enterprise-wide log data, ArcSight Logger is delivered in a range of turnkey, stackable appliances that support high-performance collection of logs from any source into a highly compressed yet accessible and self-managing log data repository. With a powerful reporting and alerting engine, ArcSight Logger functions both as a standalone appliance for log management as well as a strong complement to deployments of ArcSight ESM and the broader ArcSight platform.

Comprehensive Log Aggregation

ArcSight Logger supports collection from any raw syslog or file-based log source.

Through the library of ArcSight Connectors, log collection is available for over 275+ event sources right out of the box. The ArcSight FlexConnector framework extends collection capabilities to in-house applications.

With the flexibility of software or appliance-based deployments, ArcSight Connectors provide a scalable collection option for remote locations across the enterprise. In addition to providing a secure and reliable connection to the ArcSight Logger data store, ArcSight Connectors also offer bandwidth controls, log traffic prioritization, local caching, and failover across ArcSight Logger appliances.

Performance Without Compromise

So far, log management tools have delivered high-speed analysis only by compromising collection rates and storage efficiency or by requiring more hardware. ArcSight Logger is uniquely architected to minimize that tradeoff, thus enabling a single ArcSight Logger appliance to capture raw logs at rates of up to 100,000 events per second, compress and store up to 35TB of logs, or execute searches at over 3 million events per second.

Efficient and Flexible Storage

In addition to RAID-enabled onboard storage, ArcSight Logger can also leverage an existing SAN investment as the log data store. Regardless of whether the storage is onboard or offboard, log data is always efficiently compressed at a ratio of up to 10:1.

Scalability

The addition of ArcSight Logger appliances to any deployment will scale collection and analysis performance as well as onboard capacity linearly. As such, large organizations with multiple administrative domains or managed security service providers (MSSPs) 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.

Figure 1:"Forensics on the Fly." From dashboards to reports and from alerts to base events, "forensics on the fly" enables rapid and intuitive analysis.

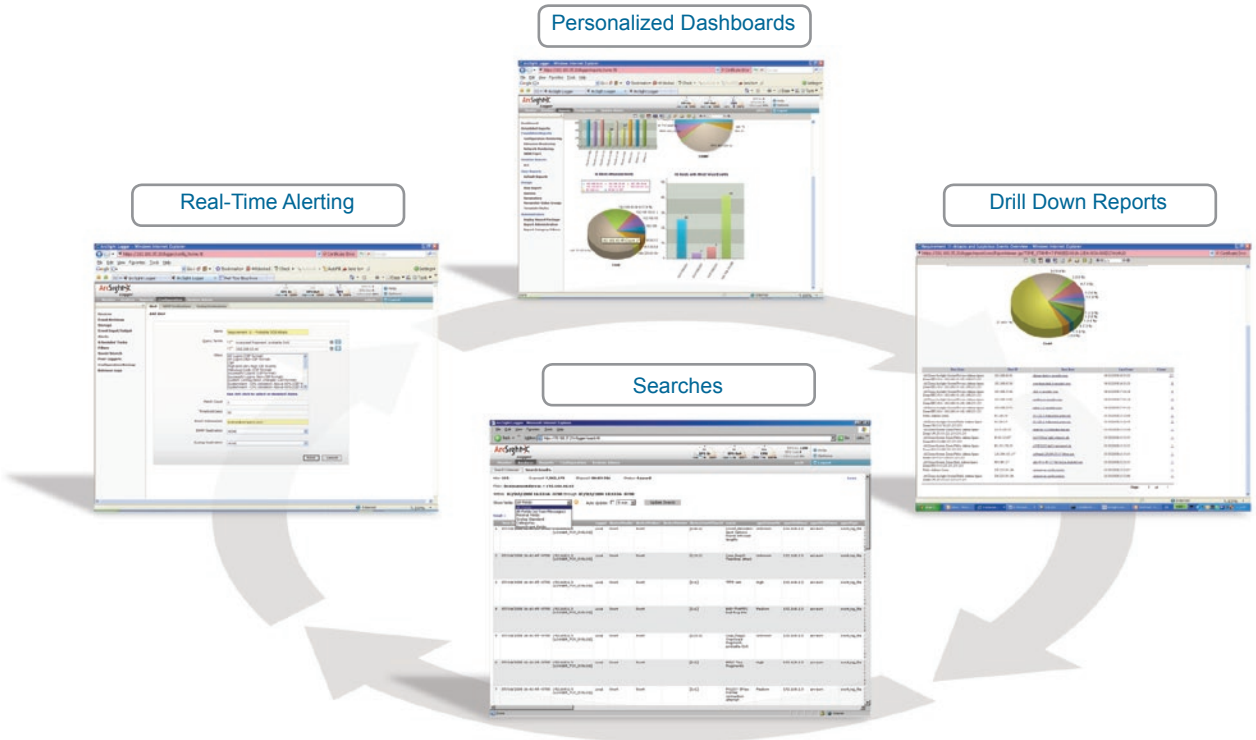
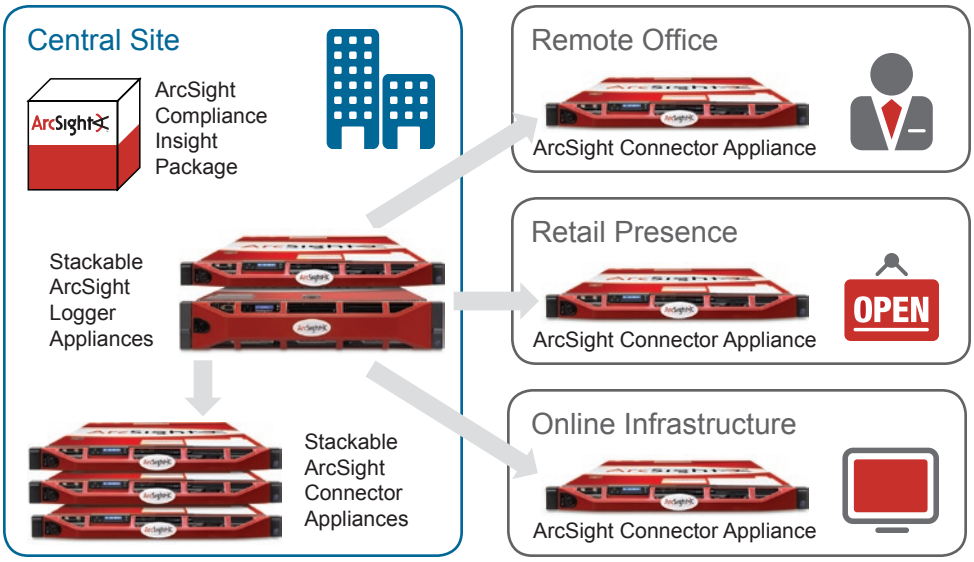


Figure 2: ArcSight Logger supports several deployment options optimized both for small businesses as well as large, heterogeneous and widely-distributed environments.



Personalized Analysis Portal

Users are presented with interactive and personalized dashboards that combine relevant reports into a single role-based view. From these aggregate dashboard views, users can drill into reports and simulate audit workflow. Interesting results in reports can be further analyzed using a simple Google-like search interface for interactive investigations. In turn, the search patterns can be converted into real-time alerts to ensure that subsequent matches lead to real-time notification within the ArcSight Logger console or via SMTP, SNMP or syslog. Finally, users can directly drill from the alert to underlying base events that triggered the alert for root-cause analysis. Collectively, this navigation path from dashboards down to base events enables “forensics on the fly” and eliminates the need to build new content at each stage of an investigation.

All content leverages a common event format that allows end users to build reports and searches without familiarity with source-specific log syntax. This also avoids the need for device- or vendor-specific analysis.

Ease of Deployment and Management

Log management is seamless with the hardened and energy efficient appliance and unique storage architecture of ArcSight Logger. No database administration expertise is required and a 100 percent web-based administration GUI simplifies deployment and ongoing management without the need to install client software.

Specialized configurations, such as ArcSight PCI Logger, offer an all-in-one appliance for collection, storage and pre-packaged analysis that is ideal for small merchants to get their PCI initiative kick started with minimal effort.

Audit-Quality Log Data

Numerous audit and litigation best practices have been incorporated into ArcSight Logger. Raw log data collected from across the enterprise is subject to integrity checks as received, using the NIST 800-92 (log management standard) approved SHA-1 hashing algorithm. Role-based access controls protect both system and event data.

Automated Retention Policies

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 and IP address. Retention policies are automatically enforced and no manual clean-up effort is required.

Pre-Packaged Content

ArcSight Logger is shipped with system content that can be used for security and compliance monitoring. Additional content specific to regulations like PCI and SOX are available as add-on solution packages and are mapped to well-known standards such as NIST 800-53, ISO-17799 and SANS.

ArcSight Platform Integration

Log management and security information and event management (SIEM) solutions both extract value from the same underlying data. As such, organizations expect synergy across these investments and ArcSight is unique in offering a tightly integrated platform for both.

ArcSight Logger integrates bi-directionally with the market-leading ArcSight SIEM offering, ArcSight ESM. The integration allows ArcSight Logger to flexibly forward 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 can leverage a common collection infrastructure built on ArcSight Connector technology.

ArcSight Logger Appliance Family Specifications

Model	L3200 & L3200-PCI	L7200-SAN	L7200s	L7200x
Management	Web browser, CLI			
Supported Sources	Raw syslog (TCP/UDP), raw file-based logs (FTP, SCP, SFTP) Analysis optimized collection for 275+ commercial products FlexConnector framework for legacy event sources ArcSight Common Event Format (CEF), ArcSight ESM			
OS	Oracle Enterprise Linux 4, 64-bit			
Compression	Up to 10:1			
Devices	200	Unrestricted	500	Unrestricted
Max EPS	2,000	75,000	5,000	100,000
CPU	1 x Intel Xeon E5504 Quad Core 2.0 GHz	2 x Intel Xeon E5504 Quad Core 2.0 GHz		
RAM	12GB	24GB		
Storage	2 x 1TB - RAID 1	External - SAN	6 x 1TB - RAID 5	
Chassis	1U	2U		
Power	480W - Non-Redundant 100-240 VAC	2 x 870W - Redundant 90-264 VAC		
Ethernet Interfaces	2 x 10/100/1000	4 x 10/100/1000		
Host Bus Adapter	N/A	Emulex LPe 11002	N/A	
Dimensions (DxWxH)	24.7” x 17.1” x 1.7”	26.8” x 17.4” x 3.4”		

Actual performance will depend on factors specific to a user’s environment.

About ArcSight:

ArcSight (NASDAQ: ARST) is a leading global provider of security and compliance management solutions that protect businesses and government agencies. ArcSight identifies, assesses, and mitigates both internal and external cyberthreats and risks across the organization for activities associated with critical assets and processes. With the market-leading ArcSight SIEM platform, organizations can proactively safeguard their assets, comply with corporate and regulatory policy and control the risks associated with cybertheft, cyberfraud, cyberwarfare and cyberespionage. For more information, visit www.arcsight.com.

ArcSight, Inc.
5 Results Way, Cupertino, CA 95014, USA
www.arcsight.com info@arcsight.com

Corporate Headquarters: 1-888-415-ARST
EMEA Headquarters: +44 870 351 6510
Asia Pac Headquarters: 852 2166 8302

ARST-PB001-083109-07