

Product Brief: ArcSight Logger

Combat Cybercrime, Demonstrate Regulatory Compliance and Streamline IT Operations

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, fine-grained access controls and automated retention policies
- **Powerful analytics:** High performance interactive searches across all data formats (both structured and unstructured), comprehensive reporting and real-time alerting engine with pre-packaged cybercrime, compliance and IT operations content
- **Cost-effective solution:** Capture, store and search up to 42TB of effective log data per appliance, enough for years of reporting

ArcSight Logger delivers industry-leading, cost-effective management of any type of log data, to protect private and public organizations of any size.

The Need for a Comprehensive Log Management Solution

With more data, transactions, and users online, governments and businesses across the globe are increasingly vulnerable to fraud, theft and breaches due to hackers, malware and malicious insiders. Within a year, data theft and breaches from cybercrime, have resulted in a global loss of one trillion dollars worth of intellectual property and expenditures. This growing risk of cybercrime has in turn triggered a wave of regulatory oversight. Today, even a mid-sized business may be subject to the cost and effort of complying with numerous mandates such as Sarbanes-Oxley, HIPAA, FISMA, GLBA, PCI, BASEL II, NERC, international data privacy laws and many more.

Logs provide an audit trail which can be analyzed to detect and investigate a cybercrime, streamline regulatory audits and improve IT operations. However, to address today's sophisticated and evolving cybersecurity threats, commercial log management solutions are necessary to enable complete collection, efficient storage and fast, intuitive analysis of any structured or unstructured event data.



ArcSight Logger: World-Class Log Management Solution

Traditional log management solutions have failed to simultaneously meet the needs of security, compliance and IT operations teams. They either focus only on structured data for security analysis or only on unstructured data for IT operations. ArcSight Logger unifies reporting, alerting, searching and analysis across any type of enterprise information making it unique in its ability to collect and analyze massive amounts of data generated by modern networks.

ArcSight Logger aids in:

- **Combating cybercrime** by allowing unified analysis across all types of data for simpler and faster forensic investigations;
- **Demonstrating regulatory compliance** through audit quality data collection and storage, pre-packaged reporting and efficient storage of years of regulated data; and
- **Streamlining IT operations** by enabling faster, better and easier investigation of all types of operations data required for change management, network management and application management.

Complete Collection

ArcSight Logger supports collection of raw or unstructured logs from any syslog or file-based log source and also leverages the vast library of ArcSight Connectors that collect from over 275+ distinct log generating sources. Additionally, the ArcSight FlexConnector framework extends log collection capabilities to

custom sources and in-house applications that are required for regulatory compliance and forensic investigations. ArcSight Connectors can be deployed as software or as appliances in data centers and regional or branch offices for secure and reliable collection. ArcSight Connectors also offer bandwidth controls, log traffic prioritization, local caching and other measures to minimize data loss or impact on business critical traffic.

Forensics on the Fly

ArcSight Logger provides role-based or personalized dashboards that combine relevant reports into a single console. From these summary dashboards, users can drill into specific reports and simulate audit workflow. ArcSight Logger reports leverage a common event format and do not require familiarity with source-specific log formats. This avoids the need for device- or vendor-specific analysis. Interesting results in reports can be further analyzed using a simple Google-like search interface to investigate any structured or unstructured log data. In turn, the search patterns can be converted into real-time alerts to ensure that subsequent matches lead to immediate 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. This is where unstructured search and fast performance play a key role as analysis might lead to data which is either very old or does not follow a particular format. This logical flow across different forms of analysis eliminates the need to build new content at each stage of an investigation.

Performance Without Compromise

Most log management tools support fast log analysis 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 42TB of logs or execute searches at over millions of events per second for both structured and unstructured data.

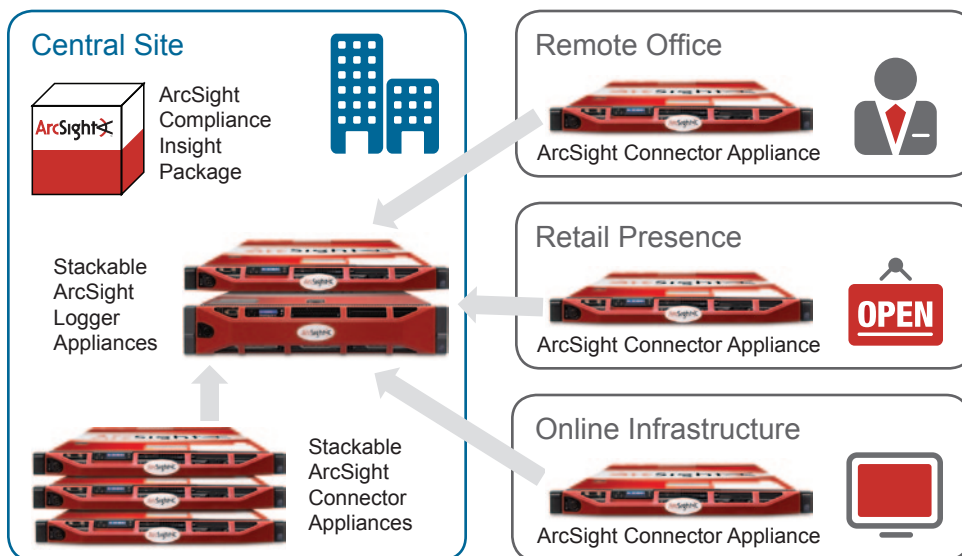
Flexible Storage

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 off-board, log data is efficiently compressed at a ratio of up to 10:1. Role-based access controls protect both system and event data. Additionally, multiple retention policies can be created based on regulation, source type or IP address. Once defined, retention policies are automatically enforced, with no manual clean-up effort required.

Pre-packaged Content

ArcSight Logger is shipped with system content that can be used for cybersecurity, compliance and IT operations 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.

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



Small to Enterprise Scalability

The addition of ArcSight Logger appliances to any deployment will linearly scale collection and analysis performance as well as onboard capacity. 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 enterprise-wide log data is always available.

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

The use of logs in compliance audits and litigation requires organizations to demonstrate the integrity and availability of log data both in transit and at rest. Several audit quality controls are built into ArcSight Logger. ArcSight Connectors provide local caching at remote sites which mitigates the impact of a connectivity loss to the data center. ArcSight Logger also supports automated failover from ArcSight Connectors at the remote location to a secondary, centralized ArcSight Logger destination.

Logs are reliably transmitted and stored to ensure that critical events 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. Most government organizations require very specific standards for security and interoperability. ArcSight Logger delivers on those requirements by supporting both FIPS and CAC.

Complement Your SIEM Investment

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. ArcSight Logger 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 and is packaged with ArcSight Express.

The integration allows ArcSight Logger to flexibly forward security events to ArcSight ESM and ArcSight Express for real-time, cross-device correlation, visualization and threat detection. In turn, ArcSight ESM and ArcSight Express can send correlated alerts back to ArcSight Logger for search and archival using a simple click of a mouse. ArcSight is unique in offering a tightly integrated platform for both log management and SIEM which leverages a common collection infrastructure to ensure a low TCO and high ROI.

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

© 2009 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.
 ARST-PB001-102509-12