MICRO FOCUS

Data Sheet
Security

ArcSight Logger

Unify collection, storage, and analysis of machine data for security intelligence. Micro Focus® ArcSight Logger is an industry-leading data collection solution that can simultaneously address cyber-security, compliance, and IT Operations log management needs, as your enterprise grows.

Product Highlights

With the rise of cyber-security threats, centralized machine data logs quickly became an important source of intelligence. Today, effective log management plays an important role in achieving insightful security analysis.

ArcSight Logger is a comprehensive log management solution that eases compliance burdens and enables faster forensic investigation for security professionals, by unifying and storing machine data logs from across their organizations, and by facilitating rapid search and reporting on that data. ArcSight Logger plays an important role in ArcSight's mission to deliver powerful layered analytics and establish foundational Security Operations.

Logger enables organizations to collect data logs from over 480 sources, and store their logs in a clean, normalized format for years, thanks to its impressive, cost-effective compression ratio. Not only can Logger ingest and store millions (even billions) of events per day, but it can help security professionals use that data to efficiently uncover anomalies and conduct rapid forensic investigations through simplified searching and customizable dashboards.

Logger comes with built-in content, dashboards, and reports that facilitate non-stop security compliance. Content packages are also available to facilitate compliance with PCI, SOX, HIPAA, and more. This will ease the burden of audits and reduce the time it takes you to show that you're in compliance with relevant regulatory requirements.

Overall, ArcSight Logger offers organizations a solution to facilitate simplified data collection, storage, compliance, and search.

Key Benefits

Comprehensive Data Collection

ArcSight Logger collects machine data at ingest rates of terabytes of data per day from any source (including logs, clickstreams, sensors, stream network traffic, security devices, Web servers, custom applications, social media, and cloud services). It enables you to search, monitor, and analyze the data to gain valuable security intelligence across your entire organization.

ArcSight Logger at a Glance:

- Capture variety, volume, and velocity of information necessary to detect security breaches
- Set up, upgrade, and maintain with just a few clicks
- Cost-effectively store and search on Terabytes of data with rapid distributed peer searching

Flexible Deployment Architecture

ArcSight Logger can be configured as a cluster providing load-balanced collection, with search queries distributed across the platform. It can be installed on a Linux system , a VMware Virtual Machine (VM), as an appliance, and in the cloud (AWS and Azure). ArcSight Logger can leverage local drives or an existing

Figure 1. ArcSight Logger Dashboard

"ArcSight Logger has allowed us to achieve compliance with PCI requirements very quickly and helped us monitor our network for anomalies so we can stay on top of emerging threats."

SECURITY OFFICER
Fortune 500 Financial Services Company

Contact us at:
www.microfocus.com

Like what you read? Share it.

SAN investment as the primary datastore. Regardless of whether the storage is onboard or off-board, data is efficiently compressed to reduce the storage and maintenance costs.

It utilizes Common Event Format (CEF), an extensible, text-based, high-performance format so that data can be easily collected and aggregated for analysis by an enterprise management system, such as ArcSight ESM, ArcSight Investigate, Interset UEBA, or any third-party application that provides event orchestration, automation, correlation, prioritization, analysis of security events, or all of the above.

Secure and Reliable Data Collection

ArcSight Logger Software can deliver encrypted, compressed logs, keeping data safe from interception, alteration, and deletion, for both data at rest and in motion. With a SecureData add-on (Voltage), Logger supports::

- Secure Encryption on Logger appliances to encrypt your sensitive data at rest (while stored). It also supports TLS and SSL encryption protocols to secure data in motion.
- Security administration and user/group role definitions. Administrators can set access rights on reports and report categories based on user role and group permissions. They can also encrypt specific data columns and selectively grant decryption rights.
- Format Preserving Encryption (FPE), which keeps your data from being exposed without authorization. It protects your data at rest, in motion, and in use.
- Federal Information Processing Standard 140-2 (FIPS 140-2).

Ultra-Fast Investigation and Forensics

When seconds mean the difference between a successful or thwarted attack, obtaining the right information at the right time is critical. ArcSight Logger enables ultra-fast investigation of indexed data via a simple search interface. Interesting search patterns can easily be converted into real-time alerts.

Logger also speeds up your investigation with machine-learning data science content. Use pre-built content or develop your own data science algorithms using python scripts.

ArcSight Logger provides ad hoc searching of billions of events in less than 10 seconds over years of data, which allows you to identify breaches and conduct detailed breach analysis.

Non-Stop Compliance

ArcSight Logger comes with built-in content that can be used for cyber security, compliance, application security, and IT operations monitoring. Additional compliance content packages for PCI, ITGOV, HIPAA, NERC, and Sarbanes-Oxley (SOX) are available as add-on options and are mapped to well-known standards, including National Institute of Standards and Technology (NIST) 800–53, ISO-17799, and SANS.

Easy to Deploy and Manage

ArcSight Logger can be configured, managed, and monitored through ArcSight's Management Center, a centralized, a centralized management console, allowing you to connect to data easily and with just a few clicks. It can be configured, managed, and upgraded easily even in large deployments, allowing you to focus on your use cases and not the tool itself.

Key Features

- Comprehensive data collection
- Flexible deployment architecture
- Secure and reliable
- Ultra-fast search and investigation
- Non-stop compliance
- Easy to deploy and manage
- Machine-learning data science content

Why ArcSight?

The ArcSight next-gen SIEM platform is scalable and powerful. It is a comprehensive solution developed for security professionals by security experts. It takes a holistic approach to security intelligence, uniquely unifying Big Data collection, network, user and endpoint monitoring and forensics with advanced security analytics technologies, including hunt, investigation, and UEBA solutions. It provides real-time threat detection and response, compliance automation and assurance, and IT operational intelligence to provide a powerful layered analytics approach that enables the self-defending enterprise.

While many vendors claim to provide a robust SIEM solution, the ArcSight team has the security expertise, experience, and leadership that few vendors can match.

Our next-gen solution, proven methodologies, and 18+ years of experience with some of the largest, most complex SOCs in the world make Micro Focus uniquely qualified to help you achieve greater security posture and operational excellence.

Learn more about log management at
www.microfocus.com/arcsightlogger