

ArcSight Security Information and Event Management (SIEM) Platform and Integrated Products

The business world is increasingly digital and interconnected. Your processes, payments, and information are online, making business more responsive and flexible. However, this move to the digital world also has dramatically increased business risk.

Data breaches, identity theft, malware, hackers...we read about new problems every week. These risks occur because too many organizations can't see the big picture of their security and compliance status. A growing number of network devices – firewalls, desktops, web servers, VPNs, etc. – each generate data about potential problems. Taken together, these bits of data paint a picture of your risk profile. Is anyone watching the picture?

In many organizations, the answer is no. It's simply too hard to collect this information into a central location, analyze it, understand the results and take appropriate action.

ArcSight solves this problem with the ArcSight Security Information and Event Management (SIEM) Platform.

The ArcSight SIEM Platform is an integrated set of products for collecting, analyzing, and managing enterprise event information. These products can be purchased and deployed separately or together, depending on organization size and needs. They include software and appliances for:

- Event Collection
- Log Management
- Event Correlation
- Compliance Automation
- Identity Monitoring

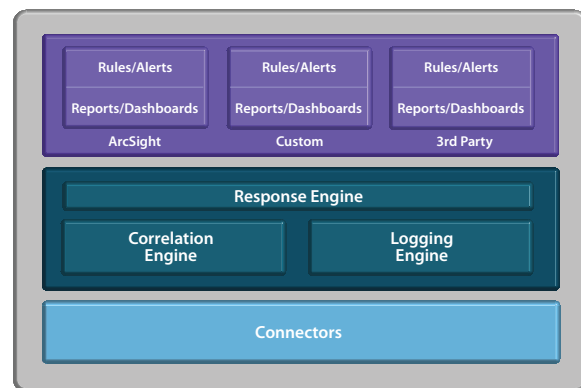
Forensics on the Fly

The ArcSight SIEM Platform is unique in its ability to provide "Forensics on the Fly" across a broad range of customer needs. Some organizations might only need historical reporting, others simple alerting or time and frequency threshold notification. Still others require complex multi-variable correlation and pattern matching. Across this spectrum, ArcSight provides different products that deliver summarized alerts and reports plus drill-down into the source events behind each alert or report.

Customers can deploy the appliance or software product that best fits their needs, while still retaining the ability to drill down and perform live forensics.

Integrated Set of Products

The ArcSight SIEM Platform is used across a wide variety of industries to manage and monitor security, business risk and compliance. The Platform includes products for event collection, real time event management, log management, automatic response and compliance reporting.



The ArcSight SIEM Platform

Event Collection

ArcSight connectors insulate your security and compliance analysis from your technology choices. By collecting logs in native device formats, then normalizing this data into a common format, ArcSight Connectors produce a single structure for searching, correlating and reporting on event information. As a result, your analysis platform is future-proofed against new network technologies. Swap out one vendor's firewall for another, and all of your correlation and compliance reports will continue to work as defined. Connectors are available as installable software, data center appliances, or small branch-office/store appliances.

ArcSight Connectors decouple an organization's ability to analyze risk from its network device decisions.

Log Management

ArcSight's log management product, ArcSight Logger, is a self-contained appliance for storing, managing and reporting against enterprise log data. A single appliance can effectively store up to 35 TB of log information, without the need for tuning or optimization. ArcSight Logger offers search and reporting, as well as alerting via email, SNMP or a web console.

Unlike other log management products, ArcSight Logger provides drill-down from alerts and reports to the source events behind the alert or report. As a result, even customers who require only simple alerting and reporting benefit from "Forensics on the Fly."



ArcSight Logger can be deployed on its own or in conjunction with ArcSight ESM and ArcSight Connectors.

The ArcSight PCI Logger includes all of the log management functionality described above, plus pre-built reports, rules, and alerts mapped directly to the PCI DSS requirements. This appliance can be deployed in a single-box configuration or with separate ArcSight Connectors, depending on customer needs.

ArcSight Logger provides a cost- and time-efficient way to store and manage enterprise logs for security and compliance purposes.

Event Correlation

ArcSight's market-leading real-time correlation product, ArcSight ESM, provides advanced analysis of log event data to discover potential threats before they spread.

Advanced Correlation

ESM uses a variety of sophisticated techniques to sift through millions of events to find the incidents that can have real business impact. Effective correlation is very important; poor correlation results in either missed threats or too many false positives and therefore, wasted time and money. ArcSight ESM provides "Forensics on the Fly" via real-time correlation across multiple systems and millions of events, with drill down from a complex alert to the events that caused it.

Automatic Response

When ArcSight ESM finds a potential problem via event correlation, the optional guided response engine, ArcSight Threat Response Manager (TRM) can provide administrators with workflow-driven advice for containing the problem. For example, if ArcSight ESM detects an employee potentially accessing records in an unauthorized way, ArcSight TRM can determine which Active Directory account to disable, which VPN session to disconnect, etc. and then guide an administrator through the proper steps.

ESM is available as configurable software or as an appliance (ArcSight ESM E7100), and can be deployed on its own or with ArcSight Logger and ArcSight Connectors. By using ESM and ArcSight Logger together, customers can find anomalies in real-time, and then compare those to historical data for more context.

ArcSight ESM makes organizations more effective and secure by filtering out the "noise" and focusing on the most important incidents.

Compliance Automation

ArcSight Compliance Insight Packages are an ideal way to jump start a compliance project or automate the monitoring of existing manual compliance controls. Installable on top of the ArcSight SIEM Platform, these Modules provide pre-packaged rules, reports, dashboard and alerts mapped to specific regulations. Through automation and best practices, ArcSight Compliance Insight Packages can dramatically cut the cost and effort of compliance.

Identity Monitoring

ArcSight IdentityView is a specialized solution designed to help organizations understand who is on the network, what data they are seeing, and which actions they are taking with that data. IdentityView leverages the user and role information stored in corporate directories and managed by Identity and Access Management systems. It correlates user activity with role and rights information to demonstrate that controls are working effectively. It also performs activity profiling to assist in identifying problem scenarios early. IdentityView enhances an organization's investment in identity management and increases security, visibility, and compliance.

About ArcSight

ArcSight (NASDAQ: ARST) is a leading global provider of compliance and security management solutions that protect enterprises and government agencies. ArcSight helps customers comply with corporate and regulatory policy, safeguard their assets and processes, and control risk. The ArcSight platform collects and correlates user activity and event data across the enterprise so that businesses can rapidly identify, prioritize, and respond to compliance violations, policy breaches, cybersecurity attacks and insider threats.