ArcSight for Security Compliance

Your security operations center has plenty to deal with, keeping up with compliance regulations shouldn't add to the workload. ArcSight can reduce the pain of reporting, maintain compliance standards, and monitor your security environment.

ArcSight Compliance at a Glance
What sets Arcsight apart from other solutions?

Simple

ArcSight makes life simpler for professionals. Pre-built content and automation make the process straightforward and easily replicated.

Built for Security

ArcSight is meant for security. It facilitates near-instant alerts and maintains the highest standards for logging and compliance.

Comprehensive Monitoring

ArcSight's Security Open Data Platform ingests hundreds of different data types. It tracks the location of logs, time stored, and other relevant information.

Lou have a business to run, and the last thing you want to worry about is data compliance regulations. Whether you're dealing with an upcoming audit or just trying to manage security data, compliance is often painful and tedious. You don't have time to fill out reports and compile information every time documentation is needed. You need to monitor your security environment, protect your valuable data, and move on to more important things.

ArcSight has just the solution for easier, continuous compliance. ArcSight reduces the pain and complexity of reporting with automated, customizable reports and dashboards. Pre-built content makes compliance simpler, and saves time for your analysts for HIPAA, PCI, GDPR, or one of many other compliance standards. With automated creation and distribution of reports, your key stakeholders will always be in the loop.

You can view your security landscape with hundreds of ArcSight's connectors for up-to-date and continuous monitoring. Extensive and robust partner integrations, along with ArcSight's open architecture will help you get the most out of your existing solutions and centralize all your security insights.

ArcSight goes above and beyond simple compliance reporting by documenting event log locations, time stored, and providing detailed processes for handling security threats. Unlike other solutions, ArcSight was built specifically for security, which means it maintains the highest standards for logging and compliance. Reduce the pain and complexity of compliance, protect and monitor your data, and move on to more important things with the help of ArcSight.

Features and Benefits

Format Preserving Encryption: (FPE) keeps your data from being exposed without authorization. It protects your data at rest, in motion, and in use.

Customizable Dashboards: ArcSight's dashboards provide a unified view of your security landscape by bringing highly interactive reports onto a single screen. It's easy to drag and drop your desired security information to your dashboard, with widget displays of the reports you choose. You can organize, resize and format your dashboard to make sure you always know the health of your security.

Adaptable Reports: With ArcSight's reports, you can create intuitive smart reports to increase your visibility of the security of your network. You can automate your reports to run in the background, and export them in a variety of formats.

Distribution: After making your own customized reports with ArcSight, you can simultaneously email, upload and publish the reports as needed. You can also schedule your reports to be automatically generated and delivered to your peers and stakeholders, to multiple recipients at once.

Content for Compliance: Security compliance has become a huge burden for enterprises. ArcSight helps ease that burden by offering built-in content to facilitate regulatory and

Contact us at **CyberRes.com**
Like what you read? Share it.

compliance requirements including PCI, SOX, GDPR, CCPA, HIPAA, and more. Its built-in reports and dashboards will cut down the time required to document your compliance, and will enable you be "audit ready" at all times.

Process for Threat Response: With ArcSight, you can automate and track your threat response. Build playbooks simply by dragging and dropping components on a visual flow builder and setting parameters. For complex and/or repetitive business logic, it is even possible to add 'automation bits', a piece of code that can be saved and reused as a component in different flows. With an incident timeline, you'll see a full trail of events and actions associated with the incident, whether performed through automation or through manual action by the analyst team. After deploying, configuring and utilizing ArcSight, you will gain defense agility, accountability, and cost reduction needed for comprehensive threat response.

Monitored Digital Ecosystem: You can't stop a threat you can't see. That's why having centralized security log management is a SecOps best practice, and is integral to achieving company-wide security event visibility. ArcSight takes this role seriously. It can ingest terabytes of data per day from any source and gives you visibility into all your data

Hundreds of Connectors: Through ArcSight's Connectors, you can collect, normalize, aggregate, and enrich data from over 480 different data source types. The structured approach to data enables you to efficiently search, monitor, and analyze the data to gain valuable security intelligence across your entire organization.

Open Architecture: An open architecture gives you greater interoperability for increased coverage. With out-of-the-box connector support for hundreds of data sources, and a custom connector creation tool, you can collect data from all types of data sources. Extensive and robust partner integrations allow you to leverage existing security solutions, increase your ROI, and lets you expand your security coverage at will. ArcSight's open infrastructure lets you use what you already have, while gaining the benefits of organized and centralized data.

Learn more at
www.microfocus.com/en-us/cyberres/secops/arcsight-recon