ArcSight Logger to ArcSight SaaS Log Management and Compliance Transition Evaluation Guide

This transition evaluation guide focuses on the value and business benefits of transitioning from your Logger environment to ArcSight SaaS for Log Management and Compliance.

It covers the reasons why you should transition to ArcSight SaaS now; a guide for you to evaluate whether ArcSight SaaS addresses the broad use cases you care about; how Logger and ArcSight SaaS compare in their ability to address these use cases; and how to contact a CyberRes representative to find out whether you qualify for six months of **free** support for your Logger environment whilst you migrate to ArcSight SaaS.

Why Transition from Logger to ArcSight SaaS?

- **Lower** the total-cost-of ownership of your log management and compliance platform
- **Eliminate** version lag. Benefit from the latest ArcSight SaaS capabilities as they come online
- **Accelerate** investigations—up to 5X faster search speeds
- **Reduce** analyst fatigue with a natural language-like interface designed for investigation ease-of-use
- **Avoid** capability deficit—Logger, although supported, will no longer receive feature upgrades

A key value of not only ArcSight SaaS but SaaS in general is the lower total cost of ownership. IDG conducted an online quantitative survey among 300 U.S.-based IT and security leaders across all industries. When asked the following question, "Assuming you could change your SIEM solution tomorrow, which outcomes would you most like to realize?", the top three answers were 1) lower staffing costs 2) lower OpEx and 3) shorten deployment time.

Key Features:

- Automatically saved search criteria
- A unified analytics-based platform
- Intuitive natural language-like search (CyPL)
- Search engine-like autocompletion
- Lookup Lists to examine large sets of data
- Scheduled searches
- Raw message view to inspect original, unformatted event logs
- Data integrity check
- Event detail panel allows detailed inspection for selected events
- Independent retention periods for up to ten storage groups
- 100+ out-of-the-box reports and dashboards covering Cloud, OWASP and more.
- Add-on compliance packages covering GDPR, PCI, SOX, and IT-GOV
- Outlier detection visualizes deviations from baseline metrics

Key Business Benefits:

- Lower total-cost-of-ownership
- Significantly reduce the time-cost-effort of maintaining your log management environment
- Redirect your precious IT Security resources to higher value-add tasks
- Reduce analyst fatigue with fast search capabilities and saved searches
- Accelerate analyst onboarding with user-friendly querying
- Version currency: consume ArcSight SaaS' latest capabilities as they come online
- Increased version update frequency

"... we found out that when you move from on-prem to cloud, the overhead and administration and regularly refreshing the technology is pretty much mitigated ..."

Head of Architecture, Security, and Privacy
for a digital media services company

Irrespective of the scale of your infrastructure, whether large, medium, or small, transitioning from your Logger environment to ArcSight SaaS will help you solve four key issues:

- **Cost:** architecting, installing, configuring, tuning, maintaining, patching, upgrading, backing up and implementing a robust disaster recovery plan for your Logger environment is a significant, and regular, outlay for your organization
- **Time:** upgrading your Logger environment involves the assignment of dedicated resources involving testing, maintenance windows, roll-back preparation, and other tasks. This impedes time-to-value or results in postponing Logger upgrades by months, or even years. This delay results in your SOC not being able to take advantage of the latest solution capabilities or potentially running unsupported hardware and software
- **Change:** any changes to your Logger environment must be planned and authorized by a group of decision makers, for example a Change Advisory Board. This is a cumbersome and complex process.
- **Effort:** IT Security staff, instead of focusing on high value-add tasks, are dedicating their energy to manual, repetitive, time-intensive, patching, upgrading and maintenance processes.

I Am Interested. What Is the Next Step? Should I Transition Now?

Are these the use cases that you care about? Are these the capabilities you need to support your use cases? Do you want to lower TCO, speed up your investigation times, accelerate analyst onboarding, reduce analyst fatigue and be always version current? If the answer to these questions is 'Yes', then select 'Book a Meeting' and talk to a CyberRes representative to find out whether you qualify for six months of free support for your Logger environment whilst you migrate to ArcSight SaaS.

What Is ArcSight SaaS Log Management and Compliance?

ArcSight SaaS Log Management and Compliance is a comprehensive, intuitive, and accessible analytics solution that eases compliance burdens and accelerates and supports investigations and threat hunting for security professionals, processing billions of events quickly, making them available for search, visualization, and reporting.

ArcSight SaaS collects log event data from any source and its columnar database responds to queries faster than traditional databases, enabling it to investigate millions of events quickly and efficiently. Storing clean, structured, and normalized data in one centralized location accelerates investigations and improves the quality of results.

Are These the Use Cases That You Care About? If Yes, Then Book a Meeting Here

Use Case: You Want to...	ArcSight SaaS Enables You to...	Which Benefits Your Business by...
Eliminate the FTE time, effort and cost dedicated to patching, upgrading, tuning, and backing up your Logger environment	Transfer the burden of managing your Logger environment to the SaaS center-of-excellence with associated SLA/SLOs	Reducing TCO costs, shifting capital expenditure to Opex expenditure, and reassigning your IT Security staff to more value-add initiatives
A pricing model that is predictable	Predict future costs by building in inflation/currency protection and a cost model that does not charge you for short term spikes in EPS levels	Enabling you to budget for your log management and compliance needs with the assurance that costs will not fluctuate during the term period
Continue to ingest, store, and retain log event data	Easily redirect your existing Smart Connector framework to forward log events to our SaaS storage locations	Introducing a transition process that is low-cost and low-risk
Improve the way you search, analyze, and visualize both short- and long-term log event data	Analyze data at faster speeds with an easy-to-use, natural language-like, autocompletion-based UI built on a robust analytics-based columnar database	Accelerating investigation time and analyst onboarding as well as reducing analyst fatigue, resulting in the increased retention of your cyber security workforce
Visualize compliance data and produce pixel-perfect reports for both internal and external auditors and regulators	Leverage 100+ dashboards out of the box and integrate add-on compliance packages allowing you to visualize and report on data related to PCI, GDPR, SOX and ITGOV	Ensuring that you are audit-ready at any time
Introduce or increase the scope of your threat hunting activities	Engage in pro-active threat hunting supported by a platform that has been designed to ease the investigation process with easy-to-use querying (CyPL), automatically saved searches and search engine-like autocompletion	Easing and accelerating the transition from Logger to ArcSight SaaS by providing a more analyst-friendly, intuitive, faster, and easier-to-query search platform to maximize efficiency and expedite time-to-productivity

How Does ArcSight SaaS Support My Use Case Requirements Compared to Logger?

Use Case Requirement	Logger	ArcSight SaaS
Ingest and store log event data	**Yes.** Normalized and enriched event data is collected using the Smart Connector framework and stored on-premise or in the Cloud	**Yes**. Onboarding to SaaS is fast as it simply involves re-directing the Smart Connectors to store the event data in your SaaS tenant
Long term retention of log event data	**Yes.** Once a threshold is met however, customers must offload archive files from Logger to a separate storage location	**Yes.** There are no physical limits regarding data retention. The retention period is only constrained by the length of service of the contract
Search and analyze short- and long-term log event data	**Yes.** However, depending on the data volume, data distribution, server load and query complexity customers have reported delays in retrieving search results	**Yes.** Internal CyberRes testing has shown that the majority of search queries in ArcSight SaaS are twice as fast as Logger, and for certain queries five times as fast
Intuitive, natural language-like searching with autocompletion in order to accelerate the onboarding of threat hunters	**No.** Querying in Logger requires a steeper learning curve resulting in longer time-to-productivity	**Yes.** ArcSight SaaS is designed to ease the threat hunting process with easy-to-use, natural language-like querying (CyPL), automatically saved searches and autocompletion
Visualize data in the form of dashboards	**Yes.**	**Yes.**
Ongoing version currency	**No.** Customers will still receive ongoing support, fixes, and patches for ArcSight Logger. However, going forward, CyberRes will no longer dedicate R&D resources to releasing Logger feature updates	**Yes.** Consuming ArcSight's log management and compliance platform as a SaaS service ensures that customers are always able to take advantage of the latest capabilities as soon as they are released
Increased version cadency	**No.** Logger will be supported but will not receive feature upgrades going forward	**Yes.** In fact, ArcSight SaaS Log Management and Compliance will release new capabilities more frequently than the on-premise version, ArcSight Recon
Free SOAR option	**No.** The purchase of ArcSight Logger does not qualify the customer for a free SOAR license	**Yes.** SOAR is included with the base ArcSight SaaS platform along with advanced authentication; the unified storage platform; and reporting & dashboards
Reporting for compliance purposes	**Yes.**	**Yes.**

ArcSight SaaS provides a no-hassle security experience by eliminating the cost of buying, installing, and managing servers and simplifying and empowering security operations. The up-front costs are minimal when switching to SaaS with little to no maintenance costs. The ArcSight team manages all the servers, hardware, and maintenance on behalf of the customer to eliminate security infrastructure concerns. With auto-updates, customers can run on the latest and greatest versions and benefit from the capability improvements immediately.

Simple	The set-up process is low-cost, low-risk and straightforward. Simply re-point the ArcSight Smart Connectors to store the event data in your SaaS tenant.
Reliable	The SaaS center-of-excellence provides 24/7 monitoring with 99.9% uptime and disaster recovery built in. CyberRes has twenty years of experience in delivering SaaS. For example, Fortify-on-demand has been serving our customers since 2011. The SaaS COE is ISO27001 certified, and we have 700+ deployments in Europe, the Americas and Asia.
Predictable pricing	The pricing model reduces volatility as we do not penalize you if you experience a short-term surge in EPS consumption. We also provide a 3-year price lock removing currency or inflation risks.

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

Book a Meeting

Book a meeting to find out whether you qualify for 6-months of concurrent support. Concurrent support a.k.a. parallel support provides you with the assurance and peace of mind that CyberRes will continue to provide support for your Logger *and* SaaS environments for six months during the migration process, at no additional cost.

If you are not able to store security event data in the Cloud for governance reasons, then this is the perfect time to transition to our next-generation on-premise log management and compliance technology. **ArcSight Recon** provides faster search speeds, more ease-of-use, easier querying for your analysts, out-of-the-box dashboards, and reports, and much more. Free trial.

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 20 years of experience with some of the largest, most complex SOCs in the world make CyberRes uniquely qualified to help you achieve greater security posture and operational excellence.

Learn more at **www.microfocus.com/en-us/cyberres/saas/secops**

CyberRes
A Micro Focus Line of Business