Top 5 Reasons to Choose ArcSight

This document covers the top 5 reasons why your organization should choose the ArcSight product line for your security operations solution. From real-time correlation to active community involvement, the ArcSight platform has what your organization needs to monitor real-time security information, identify potential threats, and minimize exposure.

---

1. **Top Correlation Engine.** ArcSight Enterprise Security Manager (ESM) by OpenText™ offers real-time threat detection and response, allowing you to see and stop threats as they occur. Unlike other SIEM solutions, ArcSight ESM can plow through mountains of incoming event logs almost instantly because it was built to handle data from large organizations. ArcSight ESM analyzes information from all of your data sources and provides the highest level of enterprise security for your company. It is extremely customizable, allowing users to create their own company-specific rulesets that will trigger instant alerts. ArcSight ESM enables both simple and complex automated responses that can be triggered on-demand or by specific alerts. In addition to this, ArcSight ESM integrates with leading SOAR and digital workflow solutions such as ServiceNow and ATAR Labs.

2. **Threat Intelligence.** ArcSight Interset by OpenText™ keeps your company secure with the most up-to-date threat intelligence available. ArcSight ESM has automated integrations with MITRE ATT&CK and MISP CIRCL, and it also has partner integrations with companies like Anomali, Ixia, and LookingGlass that can equip your company with the most up-to-date protections available. Micro Focus has made it easier for companies to assess their overall security posture by incorporating the MITRE ATT&CK Framework into ArcSight ESM and Logger reports and dashboards. Learn how ArcSight Interset works together to protect your company.

3. **Integration of UEBA.** Incorporating Interset for User Behavioral and Entity Analytics (UEBA) is a vital part of boosting ArcSight Interset security capabilities moving forward. With UEBA, your organization can get valuable, actionable insights about user activity within the first 30 days. Unlike other UEBA offerings in the market today, Interset's analytical capabilities are powered by its unsupervised machine learning and advanced mathematical models to deliver more intelligent insights—before damage is done. This extensible approach combined with an intuitive interface, allows you to detect, investigate, and respond to the threats that matter in your organization with more accuracy and efficiency. It informs you what normal user behavior looks like in your company, and instantly identifies and alerts you to the abnormal. There is no need to spend time creating rulesets because Interset does the work for you. UEBA allows your company to sift through the flood of daily alerts and prioritize the few that need attention NOW.

Are you using the most updated version of the ArcSight product line? Here are some of the capabilities you can utilize when you upgrade to the latest release:

ArcSight ESM

- Global ID
- Out-of-box content
- Stronger integration with ServiceNow
- MISP CIRCL integration
- MITRE ATT&CK dashboard

ArcSight Logger

- Machine-learning packages
- MITRE ATT&CK reports
- Demo videos
- GIS lookup

ArcSight Security Open Data Platform

- New SmartConnectors
- Container-based deployment
- Enhanced cloud connector support

“Through the ArcSight Marketplace and Activate framework, we benefit from security rule-sets, dashboards, and reports developed by Micro Focus [now part of OpenText] SOC experts and the ArcSight Community. It has hugely enriched and enhanced our security operations and response times.”

Majeed Behzadi
Executive Manager, Group Information Security Management and IT Infrastructure Design
Kuwait Finance House

Connect with Us
www.CyberRes.com

4. **Open, Efficient and Scalable Data Platform.** ArcSight implements the Security Open Data Platform (SODP) by OpenText™ to collect, organize, enrich and distribute security data. Collecting data from all your data sources in Common Event Format (CEF) allows your analysts to use the data quickly and easily. ArcSight SODP partner integrations allow you to leverage existing security solutions, increase your ROI, and lets you expand your security coverage at will. ArcSight SODP open infrastructure lets you use what you already have while gaining the benefits of organized and centralized data.

5. **Extensive Community Support.** ArcSight has thousands of users in the ArcSight community, with massive community-driven support. Chances are good that if you have a question, someone has already answered it within the community. If not, our support team is happy to give you the necessary assistance ASAP. In the ArcSight Marketplace, you can choose from hundreds of ArcSight-verified apps and community-created content packages. If you feel particularly industrious, you can build and monetize your own ArcSight packages within the ArcSight Marketplace.

Learn more at
www.microfocus.com/en-us/products/security-operations/overview

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

769-000007-001 | O | 09/23 |