CyberRes

Article

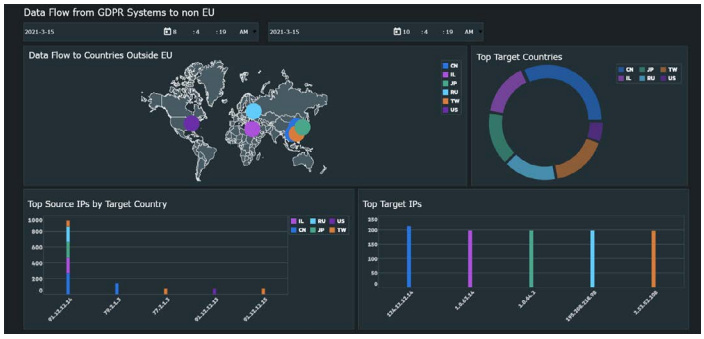
ArcSight's Latest and Greatest

New Features of ArcSight 2021.1 Release

ArcSight 2021.1: Integrated SaaS for Elevated Security

General Availability—ArcSight 2021.1 release

We are excited to announce the general availability of our Micro Focus ArcSight 2021.1 release! With new offerings to facilitate usability, ease and flexibility of deployment, this marks an important chapter in ArcSight's elevation of security operations. The introduction of our unified compliance, search and storage solution, tightly integrated with our behavioral analytics and advanced threat hunting solution, **now offered as SaaS**, represents ArcSight's commitment to simplicity and flexibility of deployment. In short, this release delivers on our promise to make SecOps more **simple**, **open**, and **intelligent**.



Introducing ArcSight Recon SaaS—ArcSight Recon SaaS plays a pivotal role in the delivery of ArcSight's layered analytics, adding high-volume storage and faster search and threat hunting without the drawbacks normally associated with complex storage architectures, hardware investments and maintenance of on-premises solutions. When used in combination with ArcSight Intelligence SaaS, the unified insights and output of ArcSight's SaaS portfolio offering is nothing short of staggering. We are thrilled to offer this new SaaS deployment model, which is a key component of ArcSight's strategy moving forward.

In addition to ArcSight Recon SaaS, on-premises deployments of ArcSight Recon now deliver several notable advancements for the ArcSight portfolio in this release. In order to give an enjoyable experience that more accurately replicates the capabilities users can expect of our full storage and threat hunting solution, **a free trial is now available** for the on-premises deployment model that includes ArcSight's Transformation Hub and several SmartConnectors. ArcSight Recon version 1.2 also brings the ability for users to access and search data located within existing ArcSight Logger deployments. ArcSight Logger users can now augment their existing setup with the addition of ArcSight Recon.

As part of our mission to elevate security operations, ArcSight 2021.1 offers more cloud-native integrations with AWS and Azure, and new SmartConnectors that monitor Google Cloud environments. SmartConnectors and FlexConnectors are available to help you quickly ingest pre-parsed, reliable and actionable data from these popular environments. As organizations have become more reliant on external cloud-data sources for their day-to-day operations, ArcSight has built robust integrations to help monitor and secure your ever-extending security perimeter.

Detect zero-day attacks—ArcSight has a long history of partnering with complementary technology providers for the betterment of security operations and is excited about our recent partner integration with Polyverse. With the integration of Polyverse Zerotect, ArcSight can now detect zero-day attacks, in real-time as they happen, by observing system events such as segmentation faults, core dumps, application crashes, etc., Zerotect can interpret disparate events and identify patterns that indicate an attack in progress. For more information, please watch the demonstration or learn more about the integration on the ArcSight Marketplace.

On April 20th, 2021, MITRE Engenuity released the results from the 2020 ATT&CK Round 3 evaluations, focusedon the Carbanak and FIN7 techniques. ArcSight is proud to have participated in this evaluation as one of only 3 SIEM vendors, and the only pure-SIEM vendor. As a direct result, ArcSight has developed actionable content for Carbanak and FIN7 that benefits all ArcSight users. While this evaluation is not directly tied to the ArcSight 2021.1 release, the resulting content is now available. For more information about ArcSight ESM's results, click here.

ArcSight 2021.1 features new releases of ArcSight Recon SaaS, ArcSight ESM 7.5, ArcSight Intelligence 6.3, ArcSight Fusion 1.3, ArcSight Recon 1.2, ArcSight SOAR 3.1, Transformation Hub 3.5, ArcMC 3.0, ArcSight SmartConnectors 8.2, and ArcSight Logger 7.2. The key features and improvements of our first ArcSight 2021 release are listed below. Please refer to the individual release notes (cited in this document) for more complete information.

ArcSight Platform

Key Highlights

- **SaaS deployment of ArcSight Recon** offers the storage, search and compliance capabilities of ArcSight Recon hosted as SaaS
- **Recon search** of Logger event data is now enabled
- **New Google Cloud SmartConnector** for native Google Cloud Logging support
- New Microsoft Azure SmartConnector for native Microsoft 365 Defender support
- **AWS Security Hub SmartConnector** now supports AWS Cloud Front service
- **New Polyverse** Zerotect FlexConnector for industry-leading polymorphic and zero-day detection capabilities
- **New content** for Carbanak and FIN7 developed during the MITRE Engenuity Evaluations
- **Containerized deployment of ArcMC** within ArcSight Fusion simplifies the deployment of ArcMC with the containerized ArcSight Platform
- **Performance improvements** allow you to configure SmartConnectors to send events to Transformation Hub with greater data reliability guarantees (Leader ACK ON) without sacrificing throughput rates
- **FIPS mode** enabled by default on fresh installations
- **New widgets** for monitoring database health
- **New documentation site** for a comprehensive reference of ArcSight Connectors
- **Updated libraries** for RHEL and CentOS, Azul Java, Apache Tomcat

ArcSight ESM 7.5

Key Highlights

- **Integration with Full Armor**, a leader in enterprise policy management, enables SOCs to use Active Directory users and groups to manage their ArcSight ESM user/group membership
- **Currency updates** to Java and OS
- **FIPS mode** enabled by default on fresh installations
- **Performance improvements** to cloud-hosted deployments and more
- **Stability improvements** and security enhancements

ArcSight Fusion 1.3

Key Highlights

- **Complete integration** of ArcSight SOAR, ArcMC, and ESM's ArcSight Command Center (ACC) web console into Fusion further centralizes the ArcSight experience
- **FIPS mode supported** and set as default on fresh installations
- **New widgets** for monitoring database health

ArcSight Recon 1.2

Key Highlights

- **Recon search** of Logger event data is now enabled
- **Cloud-native deployment in Azure, AWS** to bring flexible deployment options and decrease hardware requirements
- **Scheduled searches** to save time for searching, analyzing and threat hunting
- **Pixel perfect reports and interactive dashboards**; create, edit, publish and visualize desired reports to increase the visibility across the whole security landscape
- **100+ Out of the box report/dashboards** covering MITRE ATT&CK, Cloud, Monitoring, OWASP
- **Import and export** of reports, dashboards and related content to simplify sharing and reviewing
- **Data modeler** to provide an integrated view and understanding of all the data available in customer's environment
- **Supported external data sources** including Text/Excel/Directory, Elastic search, JDBC, REST JSON/XML
- **Ready built compliance packages** covering GDPR, PCI, IT-GOV to ease the burden security compliance requirements
- Recon Free Trial is now available. Recon Free trial duration is 90 days.

ArcSight Recon SaaS

(To be released within 60 days)*

Key Highlights

- **User-friendly search** displays grid or message views and a time-based histogram
- **Search time horizon expression** dynamically derives search time horizon from user defined expression
- **Syntax highlighting** for improved search command readability
- **Raw message view** allows analysts to inspect original, unformatted event logs
- **Event detail panel** allows detail inspection for selected event
- **Unified platform** enables routing, filtering and storage for all ArcSight products
- **Outlier detection** visualizes deviations from baseline host behavior metrics
- **Data Quality Dashboard** displays detailed information about the gap between Device Receipt Time from the raw event versus the time when the event was persisted
- **User preferences** for search parameters, display formats and limits
- **Independent retention periods per storage group for up to 10 groups**, allows sets of logs to be retained for different periods and improves search performance
- **Pixel perfect reports and interactive dashboards**; create, edit, publish and visualize desired reports to increase the visibility across the whole security landscape
- **100+ Out of the box report/dashboards** covering MITRE ATT&CK, Cloud, Monitoring, OWASP
- **Import and export** of reports, dashboards and related content to simplify sharing and reviewing
- **Data modeler** to provide an integrated view and understanding of all the data available in customer's environment
- **Ready built compliance packages** covering GDPR, PCI, IT-GOV to ease the burden security compliance requirements

*Referring to (to be released within 60 days)—Footnote 1: MicroFocus Confidential—"Roadmaps are subject to change and are therefore not a commitment to deliver a software product, code or functionality or to meet any specific timetable"

ArcSight SOAR 3.1

Key Highlights

- **ArcSight Intelligence** customers are now entitled to use SOAR without an extra license or no additional cost
- **Non-auto-pass ESM licenses** is supported with ArcSight SOAR 3.1. Customers using ESM version 6.11 and upgrade versions can implement SOAR as a native capability
- **15+ Out of the Box Playbooks** to help the customers implement and customize pre-built automation and orchestration playbooks to speed up incident response processes
- **(FIPS) Information Processing Standard** is supported. SOAR runs FIPS-enabled mode by default
- **MISP Threat Sharing Integration** to provide both threat intelligence sharing and enrichment for artifacts capabilities
- **MITRE ATT&CK integration** to provide analyst to use the database of techniques brought by MITRE framework to display the attack details and run playbooks based on MITRE ATT&CK ID

ArcSight Intelligence 6.3

Key Highlights

- **Custom model support and custom anomaly templates** to enable organizations to define new models for unique use cases and adapt event alert messages to customer preferences
- **Cloud-native deployment in AWS and Azure** to support customers' cloud-based deployments and reduce their need for capital expenditure on storage equipment
- **Policy-based data retention** to support automatic, policy-based purging of event, anomaly, and entity risk data on a scheduled basis
- **Analytics performance improvements** to minimize customer and SaaS resource requirements and reduce time required for analytics runs

ArcSight Transformation Hub 3.5

Key Highlights

- **Updated libraries** for RHEL and CentOS, Azul Java, PostgreSQL, Apache Kafka Client, and the Confluent Platform

Watch our on-demand webinar ArcSight SaaS: Integrated Threat Hunting and Behavioral Analytics where ArcSight Director of Product Management Michael Mychalczuk presents our key SaaS strategy of ArcSight moving forward, as well as outlining the exciting roadmap currently in development for the upcoming year. For more information regarding the recent changes to ArcSight's portfolio, watch our new Advancing with ArcSight video.

ArcSight Management Center 3.0

Key Highlights

- **New containerized deployment** of ArcMC within ArcSight Fusion performs simplified installation and configuration
- **Integration into Fusion UI** launches ArcMC (Fusion version) with single sign-on access and consolidated group/user/role management
- **Updated libraries** for RHEL and CentOS, Azul Java, Apache Tomcat

ArcSight SmartConnectors 8.2

Key Highlights

- **Performance improvements** allow you to configure SmartConnectors to send events to Transformation Hub with greater data reliability guarantees (Leader ACK ON) without sacrificing throughput rate
- **New Google Cloud SmartConnector** for native Google Cloud Logging support
- **New Microsoft Azure SmartConnector** for native Microsoft 365 Defender support
- **AWS Security Hub SmartConnector** now supports AWS Cloud Front service
- **New Polyverse Zerotect FlexConnector** for industry-leading polymorphic and zero-day detection capabilities
- **New documentation site** for a comprehensive reference of ArcSight Connectors

ArcSight Logger 7.2

Key Highlights

- **MySQL upgrade** to 5.7.21 for enhanced security
- **Enhanced Search UI** improves peer search, saved results and response time
- **Recon search** of Logger event data is now enabled
- **One-step upgrade** from any supported version (v6.6 and above) to v7.2

ArcSight Documentation

Release Notes

- ArcSight ESM 7.5
- ArcSight Intelligence 6.3
- ArcSight Recon 1.2
- ArcSight SOAR 3.1
- ArcSight Fusion 1.3
- Transformation Hub 3.5
- ArcSight Management Center 3.0
- ArcSight SmartConnectors 8.2
- ArcSight Logger 7.2

Is Your ArcSight Version up to Date?

Product Name	Newest Version
ArcSight ESM	7.5
ArcSight Intelligence	6.3
ArcSight Recon	1.2
ArcSight SOAR	3.1
ArcSight Fusion	1.3
ArcSight Logger	7.2
Transformation Hub	3.5
ArcSight Management Center	3.0
ArcSight SmartConnectors	8.2

Learn more at
www.arcsight.com

Contact us at **CyberRes.com**

Like what you read? Share it.

CyberRes
A Micro Focus line of business