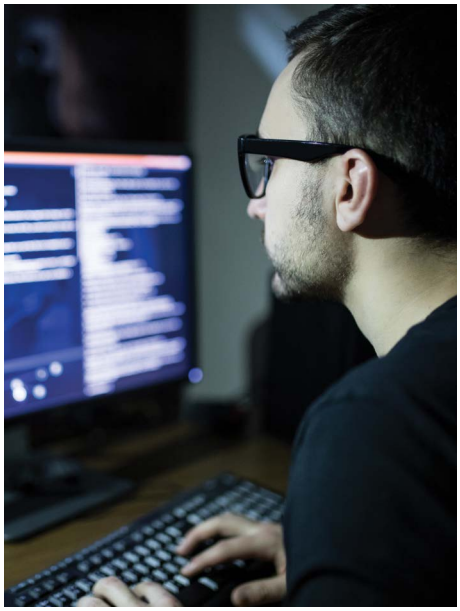
Product Flyer

Security



ArcSight SecureData Add-on for ADP Enabling Privacy Compliance

Today's privacy mandates, such as GDPR (Article 32), call for increased use of encryption of personal data. ArcSight delivers a global-scale SIEM solution for ingesting and processing high volumes of event data, including personal data. To provide confidence that event data is not exposed without authorization, ArcSight supports Voltage SecureData with Format-Preserving Encryption (FPE) at the point of data ingestion. ArcSight SecureData Add-on for ADP increases enterprise data protection in flight and at rest, while enabling usability for analytics.

ArcSight SecureData Add-on for ADP at a Glance:

- **Data privacy compliance made simple:**
  De-identifies sensitive classes of event data to accelerate compliance with today's regulatory mandates, such as GDPR and beyond, for a unified approach
- **Safe, open analytics:**
  Enables controlled data access for threat analytics by ensuring persistent protection of sensitive data from the source
- **Breach protection and risk reduction:**
  Neutralizes the impact of data breach by applying FPE, which maintains data usability for analytics, but renders data useless when exfiltrated for unauthorized use

ADP Delivers Threat Intelligence That Includes Regulated Data

The ArcSight Data Platform (ADP) Event Broker and ADP SmartConnectors ingest data from wide-ranging sources, with coverage of more than 400 source types. ADP collects data from mobile phones and devices, data centers, applications, cloud services, call logs, web data, laptops, servers, and more—and enriches it in real-time to give analysts organized information for interpretation and action.

This massive data flow potentially includes personal data relevant today that is subject to data privacy regulations such as GDPR, the New York State Department of Financial Services (23 NYCRR 500), California Consumer Privacy Act (CCPA2018)—and the host of industry, state, and international data protection mandates focused on protection of consumer information.

ADP architecture enables data to be used by nearly any system *(see Figure 1 on the following page)*, including existing data lakes, analytics tools, and other technologies. As a result, threat intelligence and valuable business information can be mined from massive data sets involving systems activity, transactions, and interactions between users and systems. ADP delivers normalized and enriched data at scale, enabling businesses to reduce risk through fast threat detection and response with ArcSight ESM, and to gain business insights from analysis of security data when using Logger and Investigate.

With the increasingly stringent approach taken by regulatory bodies toward protecting personal data from security breach, what's needed is a way to de-identify data in line with privacy regulations, while supporting the volume and scale of data flow, and opening access to data for threat analytics.

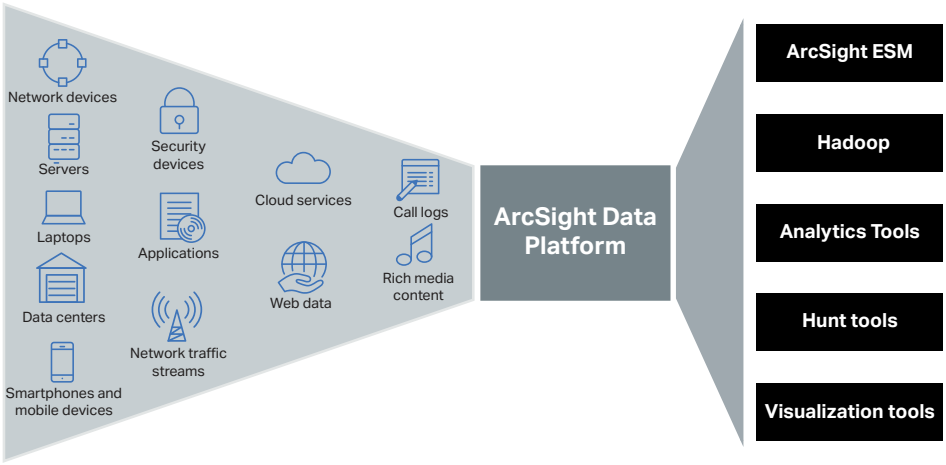


Figure 1. Data from everywhere to anywhere

Innovative Data Protection Enables Privacy Compliance for GDPR and Beyond

The GDPR sets a bar for protection of personal data, recommending pseudonymization and encryption as mechanisms that can be used to enable privacy compliance. Pseudonymization enables data de-identification by substituting surrogate data, which can be used in business processes and later reversed when authorized.

Data masking is a useful technique for de-identifying sensitive data, but traditional data masking techniques tend to be irreversible. Specific masking techniques may or may not be accepted by auditors and assessors, affecting whether they truly meet compliance requirements and provide safe harbor in the event of a breach.

Voltage Format-Preserving Encryption (FPE) is based on next-generation data masking technologies, and is the technology used in the SecureData Add-on. FPE uses NIST-standard FF1 mode AES (Advanced Encryption Standard) to replace sensitive data elements with usable—yet de-identified—equivalents that retain their format, behavior, and meaning. Protection is applied at the data field level and access policy persists with the data itself. Policy controlled secure reversibility enables data to be selectively re-identified in trusted systems that need live data.

FPE is the leading, standards-based, industry-vetted method of pseudonymization that de-identifies sensitive classes of event data in line with regulatory mandates, addressing audit requirements and simplifying compliance with a single, integrated approach. The ArcSight SecureData Add-on for ADP encrypts sensitive data on ingestion, and protects it for privacy compliance persistently: as it travels through the enterprise and in threat analytics—without the need for frequent decryption.

Safe, Open Threat Analytics

Enterprises are concerned about exposure of sensitive and regulated data. But most data protection techniques run counter to the needs of the business, which require faster, more comprehensive analytics at scale. Traditional encryption methods, such as CBC-mode AES (Cipher Block Chaining mode Advanced Encryption Standard) have enormous impact on data structures, schema, and applications. Many data masking transformations create duplicates and destroy referential integrity, causing join operations on data base tables to map improperly and reducing the ability to perform analytics on the data. But options are not limited to either accepting the risk of exposure or locking down access to threat analytics.

ArcSight SecureData Add-on for ADP enables FPE at the point of data ingestion with ADP SmartConnectors, automatically applying data protection to the pre-configured fields in the normalized security events created from the raw data. FPE preserves data value and referential integrity across distributed data sets. This means applications, analytic processes, and databases use the protected data without alteration, even across distributed systems, platforms, and tools. Encryption keys are derived on-the-fly, eliminating the need to maintain a key database, and enabling high-volume, real-time threat data ingestion with ADP.

Breach Protection and Risk Reduction for Threat Data

Data breaches are increasing in frequency and severity, with 5,207 breaches recorded in 2017—the highest number yet—and over 7.8 billion records exposed, a 24.2% increase over the prior year*.

In response, data protection mandates are increasingly challenging global businesses with stringent rules for data breach disclosure, mandatory encryption of the most sensitive categories of personal data, and harsh penalties for non-compliance. Threat intelligence—SEIM data—contains sensitive information and is therefore vulnerable to data breach and subject to enterprise data protection policies.

* *Risk Based Security's* 2017 Data Breach QuickView Report

Today's transformation of the digital enterprise demands enhanced security for users, data, and applications. From compliance to cybersecurity, current business and technology trends require sophisticated solutions to safeguard enterprises. ArcSight Data Platform transforms data chaos into security insight—now with data-centric protection included for data privacy compliance, safe analytics, breach protection, and risk reduction.

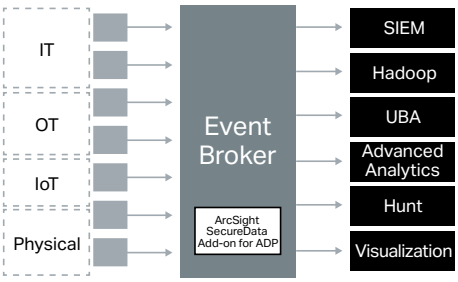
Contact us at:
www.microfocus.com

Outdated security models that do not maintain usability, relying instead upon controlling access to authorized parties, are no longer sufficient. If threat data containing personal information is exfiltrated through cyber-attack, but is protected by FPE, it will be unusable by the thieves. Moreover, breach of data protected by FPE can be considered a 'safe breach'. GDPR waives the requirement for breach notification if the data stolen is encrypted (Article 34).

By protecting threat data itself, ArcSight SecureData Add-on for ADP neutralizes the impacts of data breach, including requirements for breach disclosure, and avoids related brand damage and loss of customer trust.

ArcSight SecureData Add-on to ADP for Simplified Deployment

Micro Focus® offers the ArcSight SecureData Add-on for ADP to enable comprehensive data protection at the point of data collection, extending to systems where normalized security events data are shared. It uses Voltage FPE technology to provide end-to-end encryption for enterprise security data collected and enriched by ADP, limiting exposure of sensitive information and thus lowering risk in environments vulnerable to data breach.



Open N:M Architecture

Figure 2.

The SecureData Add-on updates ADP SmartConnectors to add Voltage protection during the data ingestion and normalization flow. The SecureData Virtual Appliance provided with the solution offers transparent, scalable, automated key management for authorized users and applications. Enterprises may deploy as many SecureData appliances as desired to achieve high-availability deployment and high-volume scale.

ArcSight Management Center (ArcMC) deploys the required software updates for the Connectors, making updating existing environments simple. Additionally, administrators can use ArcMC to configure the role-based security of Logger for data re-identification processes used during security incidents and investigations to limit data exposure risks.

ArcSight Connectors can apply FPE as needed for data masking, as close to the source as possible—a data security best practice—protecting sensitive data at rest, in motion, and in use.

Protect What Matters Most

ArcSight SecureData Add-on for ADP delivers a highly-effective solution to ensure data privacy. It answers questions such as how sensitive data can be protected in use, even in untrusted environments such as data lakes; how to reduce the overall risk profile of the enterprise; and—in the event of a data breach—whether the organization is ready to report a breach within the timelines required by privacy mandates such as GDPR. ArcSight ADP provides industry-leading methods to automatically detect the early stages of attacks and effectively stop data breaches as they happen. And now with the availability of the SecureData Add-on for ADP, enterprises can adopt proven, standards-based Voltage FPE to protect sensitive data at rest, in motion, and in use to reduce the risk of unauthorized data exposure, enable privacy compliance, and neutralize breach impact.

161-000201-001 | M | 09/18 | © 2018 Micro Focus or one of its affiliates. Micro Focus and the Micro Focus logo, among others, are trademarks or registered trademarks of Micro Focus or its subsidiaries or affiliated companies in the United Kingdom, United States and other countries. All other marks are the property of their respective owners.