White Paper

Analytics and Big Data

Why an Open Architecture Is Vital to Security Operations

MICRO FOCUS

Table of Contents

page

Open Architecture Data Platforms Deliver 1
Micro Focus ADP Open Architecture Approach 3
Better Security and Business Outcomes 6
Future-Ready Security Data Solution 8

If organizations don't stay ahead of the big data problem, they will face significant visibility gaps, misinterpretation of threats, mismanagement of collected machine data, security data overload, delays in threat detection, and threats that simply go undetected.

The Internet of Things (IoT), operational technology, cloud, and new applications continue to drive the exponential growth of data that intelligent security operations centers (SOCs) must ingest and analyze to keep their organizations secure. This continued data explosion pushes security and data tools to their technological limits. The ongoing increases and disparate nature of big data sources make it difficult to collect, clean, analyze, and manage the distribution of security data in a unified manner.

As SOCs mature and become more intelligent, they need solutions that can efficiently distribute vast amounts of actionable data to analytics tools and data lakes. If organizations don't stay ahead of the big data problem, they will face significant visibility gaps, misinterpretation of threats, mismanagement of collected machine data, security data overload, delays in threat detection, and threats that simply go undetected. Studies already indicate that 82 percent of SOCs are not at the optimal maturity level needed to help limit risk and protect business operations*.

A driving catalyst for this security data problem is that many organizations adopt multiple point solutions to solve a variety of unique problems. This complicates data sharing and creates architectural chaos with several one-to-many relationships, where each individual data source has to feed multiple analytic tools and applications. When you multiply all your different data sources by all your consumer applications, tools, and data lakes, you end up with a management and administration tsunami that can drown your SOC personnel in mundane maintenance tasks. Even when built with best-of-breed solutions, this creates operational complexities and inefficiencies that obstruct organizations' most determined security management and analysis efforts.

An open architecture message bus solution reduces data chaos by collecting data once and by making clean, security data available for consumption by any technology. This reduces complexity and cost associated with data distribution, while transforming your several one-to-many source to destination relationships to a streamlined and unified many-to-one-to-many relationship. Such an open architecture simplifies your ability to manage your security data, allows you to scale up and scale down your applications as needed, and enables you to maximize operational efficiency and analysis of your data streams in a way that dramatically strengthens your overall security posture and speed of response.

Open Architecture Data Platforms Deliver

One of the biggest strengths of an open architecture security data platform is its ability to provide standard methods and a common language for interaction between all of your different data sources and your downstream tools, applications, and data lakes. This can make it very easy to add new sources and allow the data from those sources to be quickly consumed and analyzed by your existing security tools. Likewise, it also lets you quickly bring on new downstream applications and analytical engines that can immediately take advantage of your existing data sources. All your different solutions and tools no longer work in isolation, but rather operate in cooperation.

** 2017 State of Security Operations report*

Flexibly Manage Data Sources, Streams, and Destinations

Data is essential for Intelligent SOCs to get the necessary visibility into potential threats. But it's not easy dealing with the operational and management complexities associated with a growing number of data sources and downstream destinations as you pursue multiple security use cases.

Modern Intelligent SOCs need an open architecture approach that can stream data through a centralized message bus with the ability to aggregate and standardize data so it can be easily consumed by any destination. This creates a scalable and easy to manage many-to-one-to-many model of data producers and consumers. With the right solution, you'll be able to more easily broaden and diversify your ecosystem of tools. You'll be able to ensure that the right data goes to the right places at the right time, giving your security analyst access to the data required to investigate different use cases and hunt for bad actors in your environment.

Simplify and Bring Under Control Data Chaos, Complexity, and Costs

Continued increases in data volume, variety, and velocity means more chaos, complexity, and costs for an organization's SOC. This creates data silos and impairs visibility into and usefulness of valuable security data. Your skilled security resources waste more valuable time and effort performing tedious management tasks, while facing a never-ending battle to keep your systems running smoothly.

A centralized open architecture data platform can help you eliminate data silos that thwart accurate threat analysis. To put an end to data chaos, complexity, and high cost of clean-up and distribution, you need to complement your open architecture approach with a centralized management tool that can give you visibility into your data sources and their destinations. This should include what type and how much data needs to move through your different data flow configurations, and what the health of your varying data flows are at any given time. It will make it easier and faster to connect and configure new best-of-breed technologies. It can help you reduce and better manage your computing resources and network loads. You gain the ability to simplify manageability at scale, while optimizing your time and skilled resources more effectively.

Gain More Complete and Accurate Security Analysis and Visibility

Consistent, accurate threat detection requires the ability to analyze data from all sources. When you're dealing with raw data that isn't immediately usable because it isn't yet normalized, it can significantly delay and complicate your ability to analyze data and detect threats. This can also occur when you have data sets from different systems with non-standard formats that can't be consumed by your downstream applications. Such scenarios create gaps in your analysis and visibility, which allows threats to go undetected.

You can easily solve these problems with an open architecture data platform that in real-time can automatically normalize all incoming data from disparate sources into the industry standard Common Event Format (CEF). Such a platform allows you to collect data once and make it instantly usable and available to any desired destinations. The right open security solution should also help enrich data in real-time to improve threat detection, hunting, and analysis with speed at enterprise scale.

Continued increases in data volume, variety, and velocity means more chaos, complexity, and costs for an organization's SOC. This creates data silos and impairs visibility into and usefulness of valuable security data.

Collect, enrich, and share. That's the open architecture approach Micro Focus takes with its ArcSight Data Platform (ADP).

Utilize Security Resources Efficiently

Connecting multiple data sources to multiple downstream consuming technologies, creates multiple point-to-point connections that can result in duplication of data traffic and wasted network and computing resources. Open architecture platforms that can simplify the relationships between your data sources and subscribing consumers, can automatically reduce computing loads and network traffic, just like they can reduce network complexity and improve manageability. Additionally, they can give you the control you need to route only relevant data to the right destinations, which reduces data overload and increases the ROI of those downstream systems.

Micro Focus ADP Open Architecture Approach

Collect, enrich, and share. That's the open architecture approach Micro Focus® takes with its ArcSight Data Platform (ADP). It removes the complexity and chaos from big data security by making it easy for your SOC to share enriched security data with your data lakes, analytics tools and other best-of-breed security solutions. It enriches raw data in real-time to let your analysts act instantly on all critical security information. It expands visibility by aggregating large volumes and variety of security data at high velocity.

The key elements that make ADP the right open architecture solution for your intelligent SOC include the following:

- Normalized, enriched data
- Many-to-one-to-many message bus
- Simplified management for enterprise scale

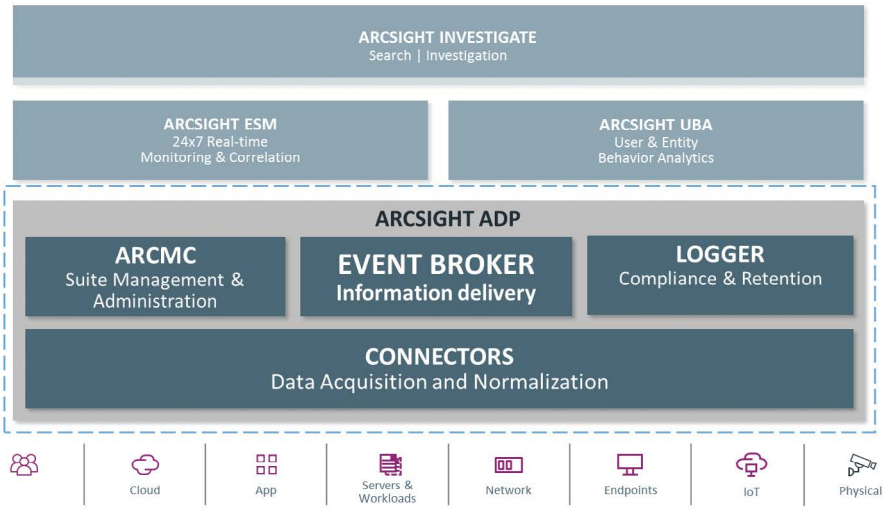

Figure 1. ArcSight Security Operations Solution

Normalized, Enriched Data

ADP includes over 400 prebuilt SmartConnectors that normalize, categorize, and enrich raw data in real-time with security context. It transforms data into standard CEF nomenclature to make it instantly usable for analytics and other use cases. Prebuilt connectors together with a Quick Flex tool to create new connectors, makes it easy to onboard new data sources with minimal manual intervention. Additionally, routing structured data reduces load on consumer applications.

SmartConnectors make adding new data sources a breeze. From the ArcSight Management Center console, you simply choose the connector for your new source, it remotely deploys, and in minutes it begins publishing actionable security data. That eliminates the need for expertise in connector deployment or configuration. ADP enables you to onboard new sources quickly, collect high volumes of data at high velocity, and manage enterprise deployments at scale.

Many-to-One-to-Many Message Bus

At the heart of ADP is Event Broker, a scalable message bus that ingests data from multiple sources and then brokers that data to multiple destinations in a way that reduces network complexity and improves manageability. Built on Apache Kafka, Event Broker takes advantage of the powerful capabilities inherent to the open source distributed streaming platform, including publishing and subscribing to streams of records through resilient and redundant messaging pipelines, storing those streams of records in a fault-tolerant manner, and processing the streams in real-time as they occur.

Built on Apache Kafka, Event Broker takes advantage of the powerful capabilities inherent to the open source distributed streaming platform, including publishing and subscribing to streams of records through resilient and redundant messaging pipelines, storing those streams of records in a fault-tolerant manner, and processing the streams in real-time as they occur.

The ADP Event broker builds on Apache Kafka further with monitoring, centralized and local management, and container-based deployment that utilizes Docker and Kubernetes technologies. Designed to handle thousands of clients at hundreds of megabytes per second, ADP distributes data at scale within its high availability, server cluster environment. Event Broker has been further fine-tuned with FIPS 140-2 security hardening, event filtering and routing of CEF messages, a CEF to AVRO format transformation engine, and ready-to-go producer and consumer topics.

With its capability to use guaranteed message delivery, Event Broker uses connectors to receive normalized and enriched security information from all your data sources. It seamlessly brokers ready-to-analyze data to multiple destinations that you can easily plug in to meet your growing security needs, including Hadoop and other data lakes, analytics tools, hunt tools, visualization tools, and other best-of-breed technologies. To ensure data persistence, Event Broker stores record streams in message topics that can be configured with their own retention policies. This allows your security operations (SecOps) teams to easily plug in new tools or workflows needed by their SecOps practices.

Event Broker lets you easily and quickly configure data flows, making it simple to expand your data consumption. Since data flows are standardized with CEFs, you can easily adjust routing of security events to the exact needs of your downstream systems, without requiring deep expertise. And because Event Broker makes it easy to filter, aggregate and route the right data to the right downstream tools, it reduces

As an enterprise-grade management platform, ArcSight Management Center gives you intuitive single pane of glass administration with complete visibility into the health of your security event stream ecosystem.

the data filtering that those downstream tools need to do, reducing your overall computing resource needs and the cost of running your third-party applications.

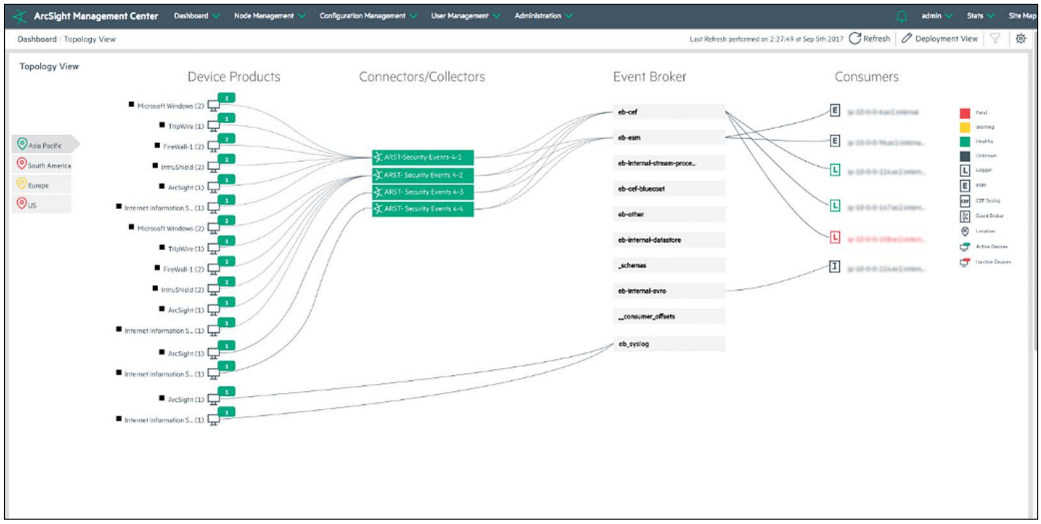

Figure 2. ArcSight Management Center—end-to-end monitoring

Additionally, the data resiliency and high availability built into Event Broker cluster foundation technologies ensures that you don't experience loss of valuable security data or interruptions in data acquisition due to network failures, network spikes, or maintenance windows. Its topic replication provides uninterrupted event streams to your target applications. If network outages or maintenance downtime happen, Event Broker holds onto events so they will be available to applications once they're back online.

Simplified Management for Enterprise Scale

As an enterprise-grade management platform, ArcSight Management Center gives you intuitive single pane of glass administration with complete visibility into the health of your security event stream ecosystem. Security architects can quickly visualize and understand the layout of their security data streams, making it easy to make sure the right data is served to the right tools. You can quickly deploy, configure, monitor, and update connectors to speed up on-boarding of new data sources and to facilitate the detection of new threats. Its Instant Connector Deployment feature lets you remotely deploy connectors on host machines from a central administrative user interface with little effort.

Its management console gives you end-to-end visibility into Event Broker and the health of your data streams, devices, connectors, and destinations with visual metrics and drill-down details on the status of individual components. It enables you to instantly identify potential problems throughout your data ecosystem and reduce the time needed to resolve them, including the ability to quickly and easily adjust data flows as needed.

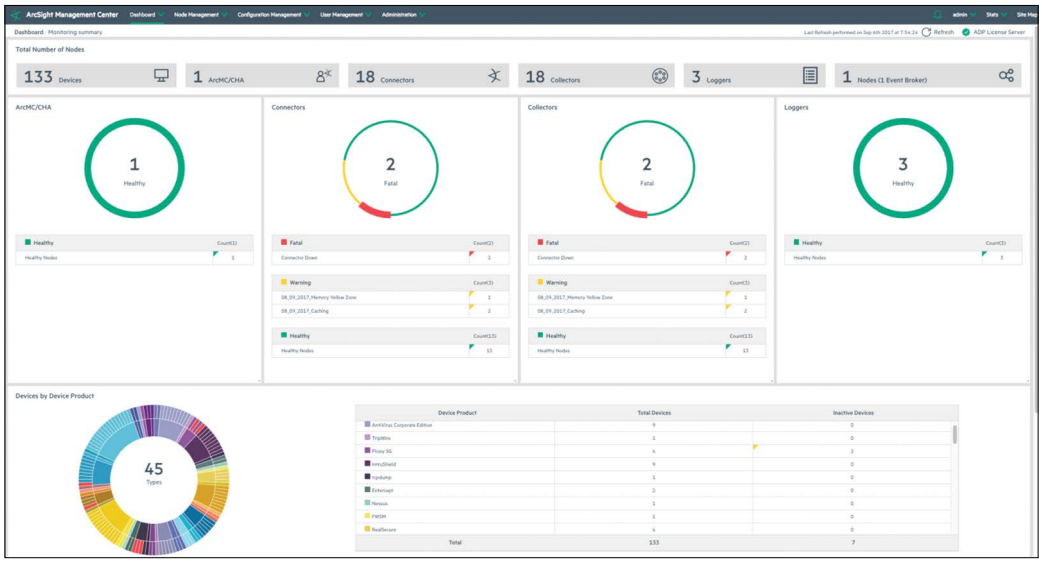

Figure 3. Simplified centralized graphical interface

ADP empowers you to use and optimize the best security applications, services, and tools needed to strengthen your security posture.

ADP simplifies SOC management, while giving security operations enterprise scalability. Its ability to ingest high volumes of data at 1 million events per second combined with being able to seamlessly broker data from any source to any new application allows you to scale at the rate your business demands. At the same time, it enables you to optimize your operations and get the most value from your skilled resources, including empowering them to be more efficient.

Better Security and Business Outcomes

The open architecture approach employed by Micro Focus ADP enables you to enjoy better security and business outcomes, allowing you to:

- Strengthen your security posture
- Reduce costs and complexity
- Increase the ROI of consumer systems

Strengthening Your Security Posture

ADP empowers you to use and optimize the best security applications, services, and tools needed to strengthen your security posture. It elevates your threat detection capabilities with the ability to transform raw data in real-time to normalized, categorized and enriched data that analysts can act on instantly.

ADP also optimizes your collection and management of large volumes and data varieties at high velocity so you can expand your security operations coverage and reduce your risk of attack.

The manner in which ADP structures and adds security context to data, speeds up threat detection by enabling consistent and accurate event correlation and investigation across diverse sets of data and data sources. You get the visibility into events and use cases you need, as well as the data persistence needed to ensure that no critical data is ever missed.

ADP also optimizes your collection and management of large volumes and data varieties at high velocity so you can expand your security operations coverage and reduce your risk of attack. The speed and ease at which you can onboard new data, services, and applications, as well as make data stream adjustments, helps you to identify and respond to new threats faster. You can easily take down analytical applications, adjust them, and re-connect them again without worry of losing any data. That enhances your ability to take advantage of more complex analytical models and quickly track new security use cases. No matter the size and expertise of your SOC, ADP can simplify, speed up, and optimize your big data security management and analysis. Plus, as your security maturity level rises, you can take even greater advantage of the security gains ADP has to offer.

Reducing Your Costs and Complexity

The open nature of ADP and the way it simplifies your operations and management at scale can considerably reduce your costs and complexity. With faster implementation speeds and dynamic creation of new data streams, you substantially decrease the time spent on-boarding services, and configuring and adjusting data flows. Simplicity of management means you spend less time and effort maintaining all your different systems, which reduces the cost of running them. The open environment and standardized integrations reduce the amount of training and expertise you need to manage your infrastructure. You enjoy greater operational efficiencies with streamlined data flows, lower network loads, greater data resiliency, and higher data availability.

Increasing the ROI of Your Consumer Systems

With its open architecture, ADP allows you to get more out of your legacy and existing systems. The ability to send clean, enriched data from anywhere to anywhere allows your applications to leverage new data sources and reduces computing resources needed to clean raw data. Additionally, routing the right data to the right consumer reduces cost of ingestion on your best of breed technologies. You can now utilize clean, valuable security data for new use cases and analytics models that used to be out of reach. These all combine to dramatically increase the value of all your existing security and IT investments.

For example, an international security provider, operating sixteen SOCs worldwide uses ADP to forward only relevant security data to its IT operations management solution. With its ability to handle 3 million security events per second, ADP has significantly expanded the security provider's end-to-end visibility, elevated its operations maturity, and increased its accuracy and effectiveness in reducing false positives.

Future-Ready Security Data Solution

ArcSight Data Platform provides a future-ready security solution that helps you address the challenges of exponentially increasing data and the need to employ new technologies to stay ahead of a rapidly changing threat landscape. Its open architecture message bus allows you to connect your existing data lakes, analytics tools, and other security technologies directly into your SOC, thus enabling you to send clean data from anywhere to anywhere. It lets you seamlessly scale with new data sources and consumer technologies to improve visibility and address continued growth. It helps you improve your speed and accuracy of threat detection and analysis by enriching your security data in real-time with security context, allowing your analysts to act upon organized information instantly. It lets you get the most out of your chosen security technologies and solutions, increasing your return on investment and enhancing your ability to detect bad actors.

To learn more about how the open architecture of ADP can elevate your SOC's ability to detect and respond to threats, attend our workshop [insert workshop details] and visit **microfocus.com/adp**.

Learn More At
microfocus.com/adp

ArcSight Data Platform provides a future-ready security solution that helps you address the challenges of exponentially increasing data and the need to employ new technologies to stay ahead of a rapidly changing threat landscape.

Additional contact information and office locations:
www.microfocus.com

www.microfocus.com