MICRO FOCUS

Data Sheet
Security

ArcSight Data Platform

This open platform transforms data chaos into security insight.

Product Highlights

In the year 20161, 98% of companies were victims of cyberattacks. Threat to organizations from cyberattacks is increasing each year and the estimated cost is as high as $74 million annually[1].

Security data underpins the modern security operations environment. The increasing number of disparate sources of data and data formats make it nearly impossible to build a single data architecture to meet all your needs. The amount of data we create and copy annually doubles every two years, and will reach 44 zettabytes by 2020[2]. With exponential increases in data volume and velocity, from IoT, Physical, OT, and IT, the Security Operations Center (SOC) struggles to ingest and process the tsunami of data required for threat detection. Limitations in data access and critical systems connectivity cause major delays and costs. Making matters worse, more than 209,000 cybersecurity positions went unfilled in 2015 in the United States alone, and job postings were up 74 percent from 2010 to 2015[3].

The SOC must fundamentally restructure itself to adapt to increased volumes, a rapidly changing threat landscape, and the lack of skilled security resources.

Micro Focus® ArcSight Data Platform (ADP) offers a future-ready data solution that enriches data in real time and supports open standards

1 *Ponemon Institute—2016 Cost of Cyber Crime Study & the Risk of Business Innovation*
2 *IDC—The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things*
3 *U.S. Bureau of Labor Statistics report*

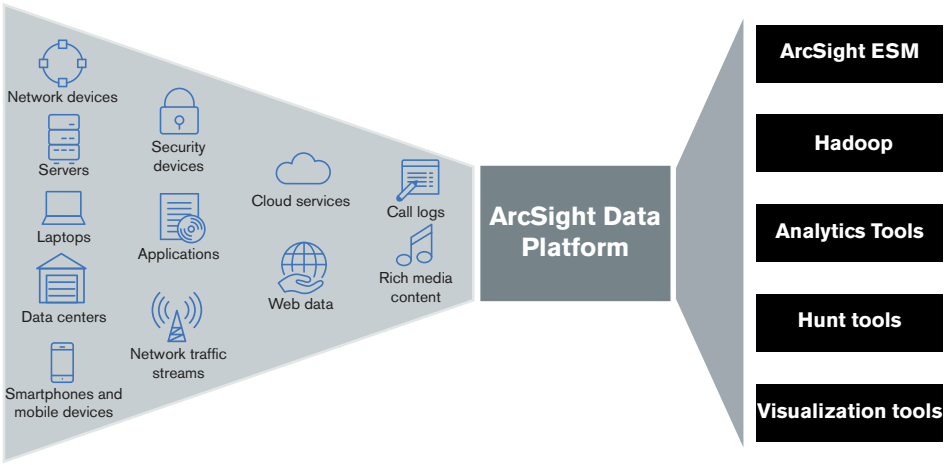

Figure 1. Data from everywhere to anywhere: Open Architecture

Key Capabilities

- Event Broker, built with Apache Kafka, ingests data from any source and sends it anywhere
- Real-time data enrichment adds security context to raw data, making it instantly usable
- 400+ out of box connectors collect data from all source types
- Centralized management console provides an end to end picture of your security environment
- 'Guest data' feature allows using Event Broker message bus for all IT needs

Key Benefits

- Expand data visibility to reduce risk of attack, reputational damage
- Reduce risk through faster threat detection and response
- Efficiently utilize skilled security resources
- Capitalize on investment by utilizing data for Hadoop and analytics tools
- Reduce cost and complexity of extracting and distributing data to multiple destinations

for better threat detection. Using security data connectors, ADP collects data and enriches it in real-time to give analysts organized information that can be acted upon instantly. With an intelligent Event Broker, built on a foundation of Apache Kafka, ArcSight Data Platform can ingest and broker data from any source, anywhere, seamlessly.

Features and Benefits

Unleash the Power to Scale through Variety and Velocity

With over 400 out-of-box security data connectors and a custom connector creation tool, ADP allows you to collect data from all types of data sources. New data sources and version updates are now supported faster with new parsers released every 4 weeks. Syslog Connector in Event Broker helps enterprises scale more easily while reducing network traffic. Token-based tool for building parsers improves consistency and reduces the time to build new connectors from days to hours and from hours to minutes. The intelligent Event Broker extracts data at a high speed of 1 million events per second and helps broker data to multiple destinations seamlessly.

Management of increasing disparate data sources is tedious. ADP comes with ArcSight Management Centre, which provides intuitive visuals and metrics. An end-to-end view of all your devices, connectors and destinations aids identifying issues instantly and reduces time to fix them. The management console makes management of SOC resources easier than ever and saves time by introducing the Instant Connector Deployment feature and by helping you perform actions on hundreds of nodes at one time, effortlessly.

ArcSight Data Platform (ADP) simplifies security operations and reduces risk of attack by allowing you to expand your security operations coverage. It optimizes the collection and management of large volumes and variety of data, at high velocity.

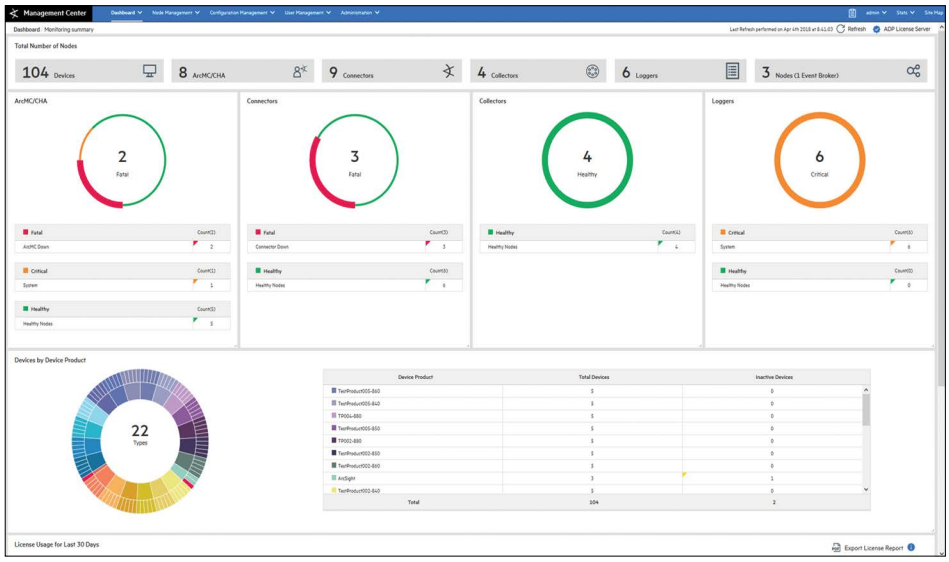

Figure 2. ADP centralized management console—dashboards

Deliver Insight with Real-Time Security Context

ArcSight Data Platform enriches raw data in real-time to give analysts organized information that can be acted upon instantly. ADP's Smart Connectors normalize, categorize and enrich data during ingestion to add ArcSight's security expertise developed over years. The data

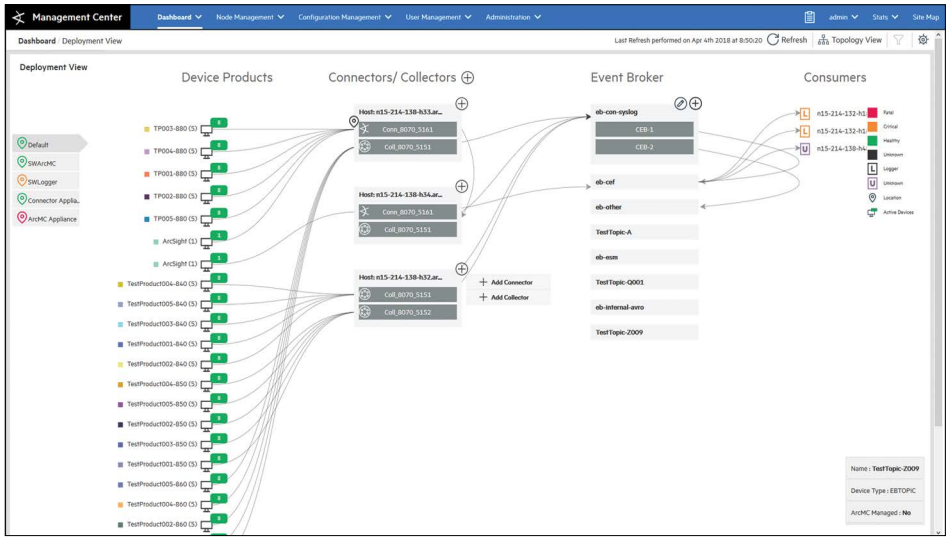

Figure 3. ADP centralized management console—end to end monitoring

is therefore already structured and organized, enabling faster and accurate investigation and event correlation to aid threat detection.

To meet compliance requirements as well as to prevent data manipulation by cyber-attacks, it is important to ensure reliability and integrity of data. ADP delivers encrypted and compressed logs, which keeps data safe from interception, alteration, and deletion. All the data in motion is secured by transport layer security (TLS).

Capitalize with Open Architecture

With increasing sources and far higher volumes moving to multiple destinations for real-time analytics and archival, N:1 architectures are an impediment to the growth and needs of Security Operations. ArcSight Data Platform comes with the Event Broker, an Apache Kafka based message bus, which provides an N:M architecture that can ingest data from all sources and broker it to multiple destinations. This allows you to open up your security environment and utilize the data collected over your existing data lakes, analytics tools, and other technologies. Thus, increasing the return on your investment by utilizing captured data over multiple use cases, future-proofing your security operations.

The open architecture gives you the flexibility to choose how you store, search, and analyze data, and employ the best of breed technologies that your business demands.

Maximize returns on your investment by using ADP's Kafka based message bus for your IT data needs. ADP also offers advanced HA capabilities through Event Broker Kafka replication

In conclusion, ArcSight Data Platform offers a future-ready data solution that enriches data in real time and supports open standards for better threat detection. Its open architecture message bus allows you to connect your existing N:M architecture that can ingest data from all sources and broker it to multiple destinations. This allows you to open up your security environment and utilize the data collected over your existing data lakes, analytics tools, and other technologies. Thus, increasing the return on your investment by utilizing captured data over multiple use cases, future-proofing your security operations, data lakes, analytics tools, and other security technologies directly into the SOC, thus enabling you to send data from anywhere to anywhere. ADP scales with your enterprise and adds meaning to data to that analysts can act upon organized information instantly.

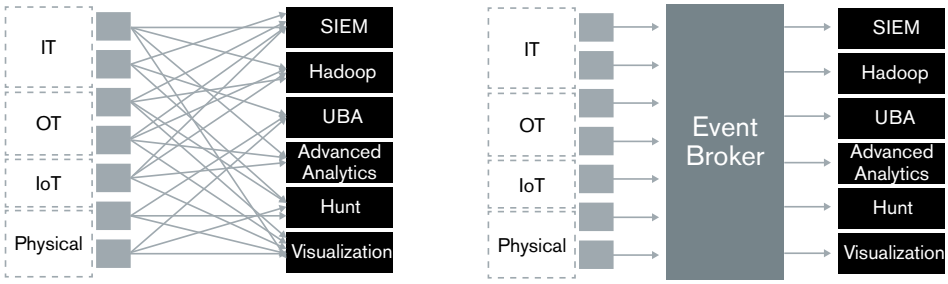

Figure 4. Intelligent message bus architecture

Learn More At
www.microfocus.com/adp

Contact us at:
www.microfocus.com

Like what you read? Share it.