opentext™ | Cybersecurity

Data Sheet

ArcSight Security Open Data Platform

Unlocking and sustaining the value of your ArcSight solution

Product Highlights

The chance of a company experiencing a data breach within the next two years is now 29.6%[1]. Threats to organizations from cyberattacks are increasing each year and the estimated damages are expected to exceed $6 trillion annually by 2021[2].

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[3]. 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.

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

ArcSight Security Open Data Platform (SODP) by OpenText offers a future-ready data solution that enriches data in real time and supports open standards for better threat detection. Using security data connectors, SODP collects data and enriches it in real-time to give analysts organized information that can be acted upon instantly. With an intelligent Transformation Hub, built on a foundation of Apache Kafka, ArcSight Security Open Data Platform can ingest and broker data from any source, anywhere, seamlessly.

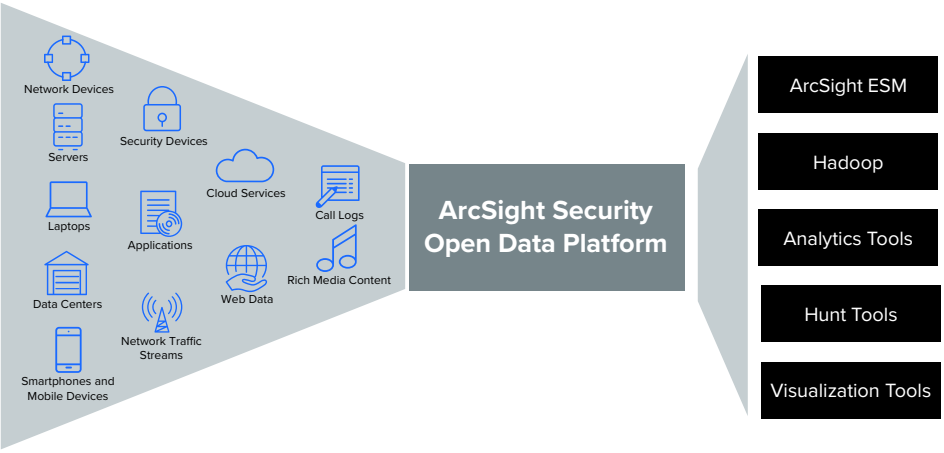

Figure 1. Data from everywhere to anywhere: Open Architecture

Key Capabilities

- Transformation Hub, 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
- 480+ 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 Transformation Hub 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

1. Ponemon Institute—Cost of a Data Breach Report 2019
2. CSO online: Top 5 cybersecurity facts, figures and statistics for 2018
3. IDC—The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things

Features and Benefits

Unleash the Power to Scale through Variety and Velocity

With over 480 out-of-box security data connectors and a custom connector creation tool, ArcSight SODP 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 Transformation Hub helps enterprises scale more easily while reducing network traffic. A 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 Transformation Hub extracts data at hundreds of thousands of events per second (EPS) and helps broker data to multiple destinations seamlessly.

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

ArcSight Security Open Data Platform (SODP) 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 varieties of data, at high velocity.

Deliver Insight with Real-Time Security Context

ArcSight Security Open Data Platform enriches raw data in real-time to give analysts organized information that can be acted upon instantly. ArcSight SODP Smart Connectors normalize, categorize and enrich data during ingestion to add OpenText's security expertise developed over years. The data is therefore already structured and organized, enabling faster and accurate investigation and event correlation to aid threat detection.

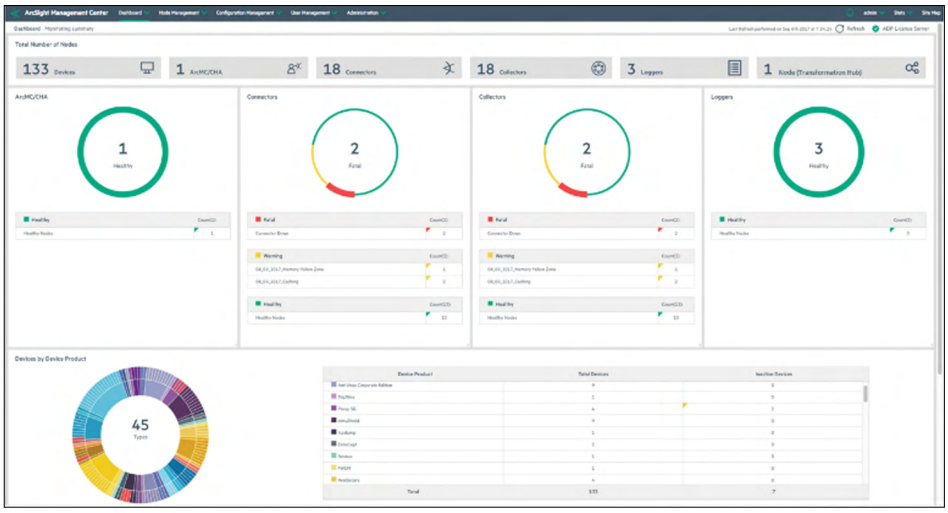

Figure 2. SODP centralized management console—dashboards

To meet compliance requirements as well as to prevent data manipulation by cyber-attacks, it is important to ensure reliability and integrity of data. ArcSight SODP 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).

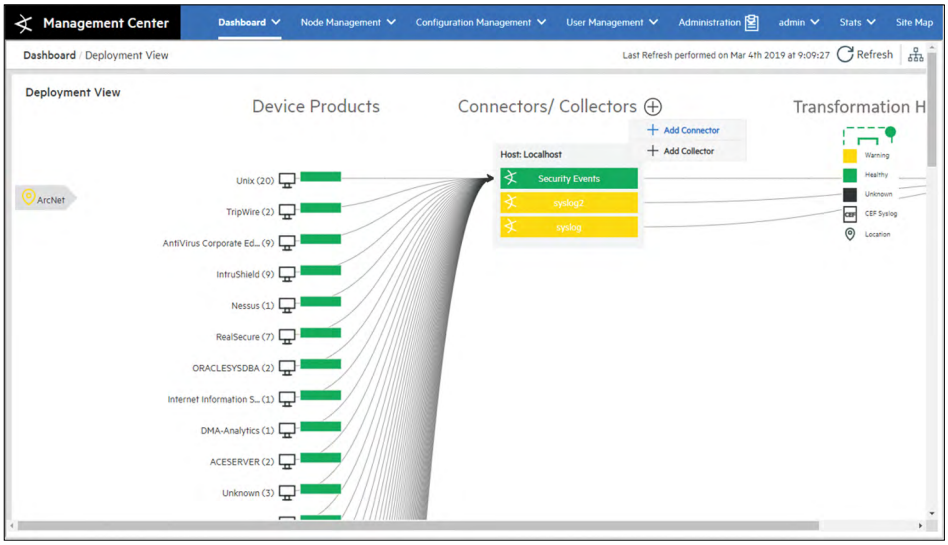

Figure 3. ArcSight SODP centralized management console—end to end monitoring

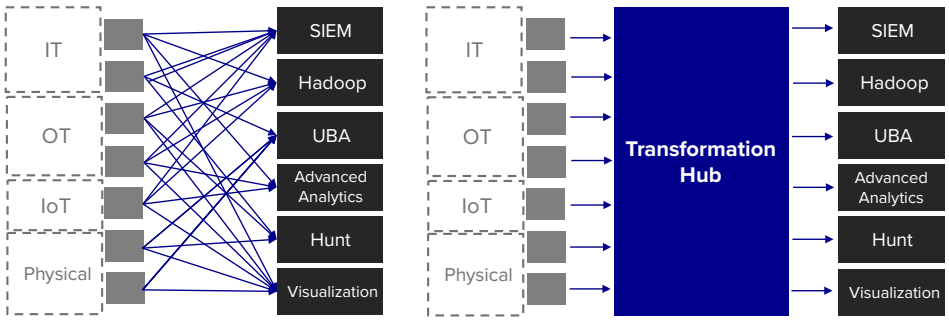

Figure 4. Intelligent message bus architecture

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 Security Open Data Platform comes with the Transformation Hub, 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 ArcSight SODP's Kafka based message bus for your IT data needs. ArcSight SODP also offers advanced HA capabilities through Transformation Hub Kafka replication.

In conclusion, ArcSight Security Open 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. ArcSight SODP scales with your enterprise and adds meaning to data to that analysts can act upon organized information instantly.

Learn more at
www.microfocus.com/sodp

760-000035-003 | O | 10/23 | © 2023 Open Text