Hewlett Packard Enterprise

GENESIS
SWISS TEAM AG

HPE ArcSight Data Platform

Collect, normalize, and enrich data to expand visibility for intelligent security operations, laying the foundation for better detection, investigation, and response to threats

Key benefits:

- Provide flexibility to use solutions suitable for specific business needs
- Expand visibility of data and scale faster for a secure infrastructure
- Optimize resource time with centralized environment management
- Enrich data with security context for better threat detection

Highlights:

- Open architecture for data to be used across the security posture for all SOCoperations
- Scalability through variety and velocity to support large environments
- Centralized console for easy and efficient management of security posture

Growing complexity of IT environments coupled with the sophistication of threats that target critical assets creates new security challenges for organizations of all sizes. To address these challenges, successful organizations are shifting to intelligence-driven security operations centers that provide full data visibility to use the information for advanced analytics effectively. Visibility of the entire infrastructure is the key to better detection, investigation, and response to threats. Businesses today need a data collection platform that is reliable and secure, and helps them operate efficiently and effectively at low budgets.

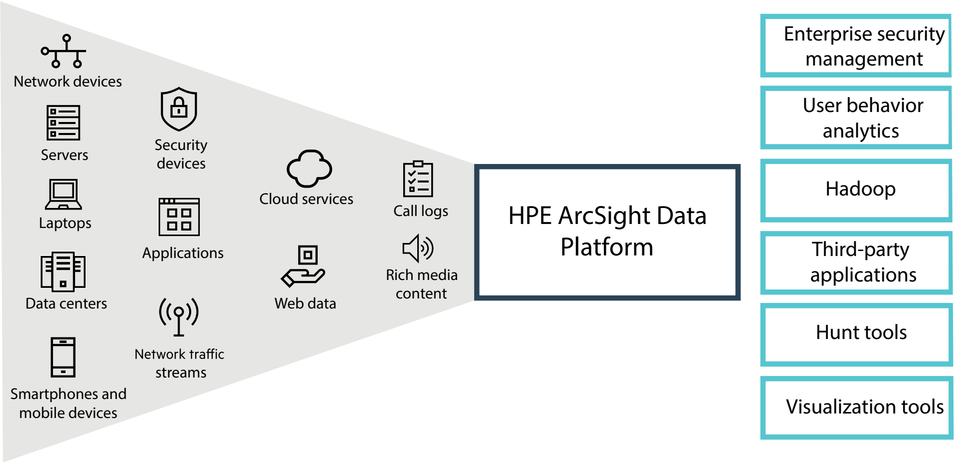
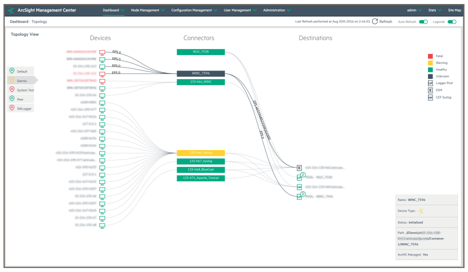


Figure 1. HPE ArcSight Data Platform

HPE ArcSight Data Platform (ADP) 2.0 is an open and scalable solution to collect, normalize, and enrich data for compliance, regulations, security, IT operations, and log analytics. It can collect data from any source (for example, logs, sensors, stream network traffic, security devices, web servers, custom applications, cloud services, and others) to expand the visibility of data and provide flexibility to consume data in any applications.

Open architecture for wider range of applications

HPE ADP 2.0 delivers an open architecture that can send event data to third-party applications such as Hadoop, data lakes, or even proprietary in-house applications. This empowers security operations centers (SOCs) with the flexibility to choose how they store, search, and analyze data.



Name : WINC_7596

Device Type :

Status : Initialized

Path : //Dennis/n… /Container 1/WINC_7596

ArcMC Managed : Yes

Figure 2. HPE ArcSight Management Center Topology View

HPE ADP 2.0 is powered by a Kafka-based Event Broker, which provides an open architecture that allows organizations to adopt an intelligence-driven security operations model quickly. This capitalizes on investment by utilizing captured data over multiple use cases. Easy integration with third-party applications, in addition to HPE ArcSight Enterprise Security Management (ESM) and HPE ArcSight User Behavior Analytics (UBA), reduces time to build an advanced SOC. It further assists in leveraging multiple applications for analytics-based detection, incident response, visualization, and hunt.

Scalability through variety and velocity

With HPE ADP 2.0, businesses can easily expand the size and breadth of a deployment. Security teams can begin with a small, midsized, or large deployment and add new processing or functional capabilities on the fly. HPE ADP 2.0 collects data from all types of devices. Over 350 out-of-the-box connectors save time and effort that goes into onboarding data sources, along with the token-based wizard to build customized connectors. Supporting newer versions of devices is quicker with new connector parsers released every four weeks.

Enterprises can now operate large security operations effectively by processing information quickly, and allowing more users to operate at the same time. The Event Broker acts as a data hub, which collects information at one million events per second. HPE ADP 2.0 is designed for supporting large SOC operations by allowing 100 concurrent searches so that multiple users can operate at the same time.

Easier management through centralized console

All HPE ADP 2.0 components are configured, managed, and monitored easily through the centralized management console. It means that actions on hundreds of nodes can be performed at once, which effortlessly supports large-scale deployment.

Newly added device monitoring provides full visibility into all end devices, which HPE ADP 2.0 collects data from, enhancing a capability to identify the specific device in issue and reduce time to make an informed decision to fix any problem quickly. Visualized metrics are effective to get a snapshot of health environment as well as to provide a granular view with a simple drill down.

Reliable data collection for security

Raw log data is useless for security operations. Logs from heterogeneous vendor devices and applications contain inconsistent formats and different terminologies. Without understanding data upfront, it is hard to investigate alerts or analyze events. HPE ADP 2.0 normalizes and categorizes data immediately as it collects, and enriches it with security context. As a result, HPE ADP 2.0 enables faster correlation and threat detection as the data is already structured and organized with security contextbefore it is consumed at the next stage—security investigation or eventcorrelation.

To meet compliance regulations as well as to prevent data manipulation by cyber attacks, it is important to ensure reliability and integrity of log data. HPE ArcSight Data Platform 2.0 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).

Learn more at
hpe.com/software/adp