OpenText SIEM Open Data Platform

Unlocking and sustaining the value of your cybersecurity solutions

Key Capabilities

- Includes SIEM Message 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
- 400+ out of box connectors collect data from all source types
- Includes SIEM Management Center provides an end to end picture of your security environment

A recent report revealed that 68% of companies experience between 11 and 30 external attacks a year[1]. Threats to organizations from cyberattacks are increasing each year and the some attacks like the one on MGM Resorts International costing over $100 million alone[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 is likely to reach 394 zettabytes by 2028, up from just two zettabytes in 2010[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.

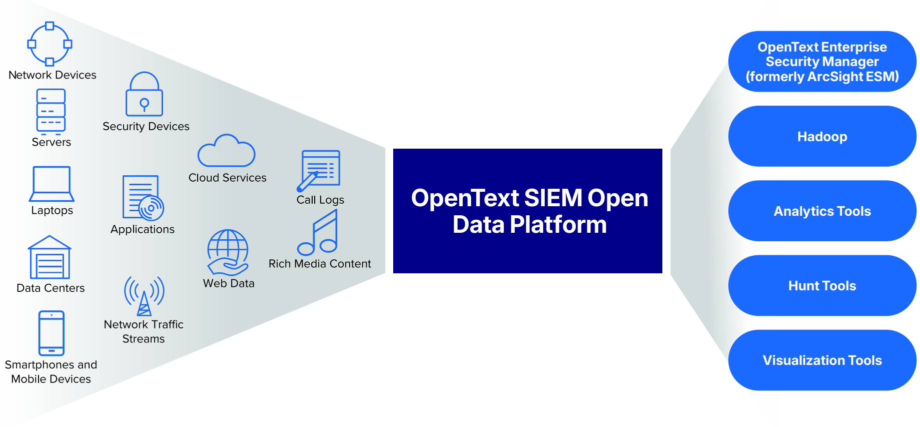


Figure 1. Data from everywhere to anywhere: Open Architecture

Benefits

- Expand data visibility to reduce risk of attack, reputational damage
- Reduce risk through faster threat detection and response
- Efficiently utilize your 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

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

OpenText™ SIEM Open Data Platform offers a future-ready data solution that enriches data in real time and supports open standards for better threat detection. Using OpenText SmartConnectors collects data and enriches it in realtime to give analysts organized information that can be acted upon instantly. With our intelligent OpenText SIEM Message Hub, built on a foundation of Apache Kafka, SIEM Open 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, SIEM Open Data Platform allows you to collect data from all types of data sources. 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 SIEM Message Hub receives 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. SIEM Open Data Platform comes with OpenText Management Center, which provides intuitive visuals and metrics on the health of your security data pipeline. An end-to-end view of all your devices, connectors, and destinations helps identify data issues instantly and reduces time to remediate them. Our management console makes management of SOC data pipeline resources easier than ever. It saves time by introducing the Instant Connector Deployment feature and by helping you perform actions on hundreds of connectors at one time, effortlessly.

SIEM Open Data Platform simplifies security data operations and helps improve attack detection by allowing you to expand your security data coverage. It optimizes the collection and management of large volumes and varieties of data, at high velocity.

Deliver Insight with Real-Time Security Context

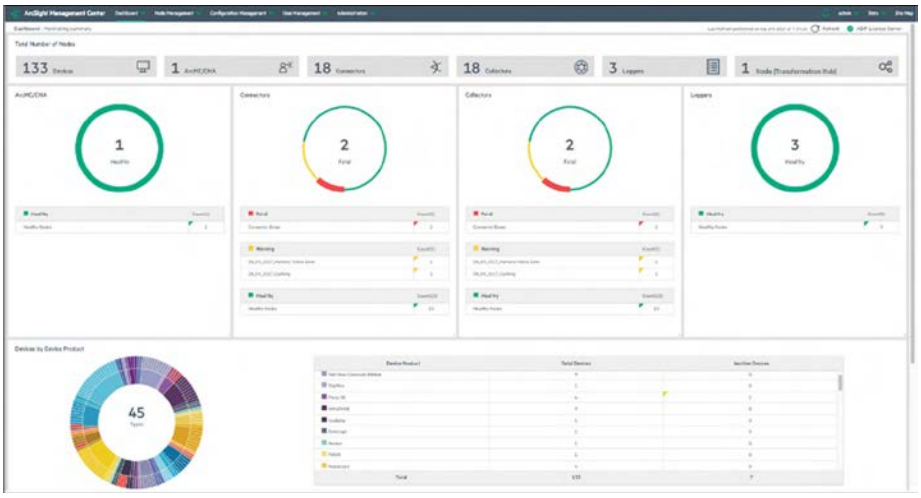


Figure 2. SIEM Open Data Platform centralized management console—dashboards

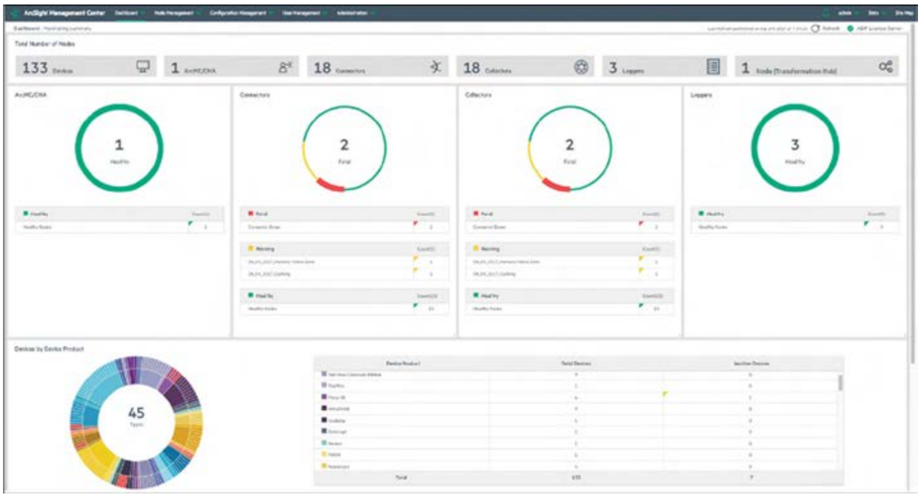


Figure 3. SIEM Open Data Platform centralized management console—end to end monitoring

SIEM Open Data Platform utilizes SmartConnectors to enrich raw data in real-time to give analysts organized information that can be acted upon instantly. SIEM Open Data Platform SmartConnectors normalize, categorize and enrich data during ingestion to add OpenText's cybersecurity expertise developed over decades. The data is therefore already structured and organized, enabling faster, accurate investigation and event correlation to aid threat detection.

To meet compliance requirements as well as to prevent data manipulation by cyberattacks, it is important to ensure reliability and integrity of data. SIEM Open Data Platform encrypts security log data to mitigate interception and protect data integrity. All data in motion is secured by transport layer security (TLS).

Capitalize with Open Architecture

Delivering more security data sources and increasingly higher volumes of data for real-time analytics and data retention requirements, N:1 architectures are an impediment to the growth and needs of Security Operations. SIEM Open Data Platform comes with the SIEM Message 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 security devices. This increases the return on your investment by utilizing collected security data for multiple use cases, reducing the complexity of your data pipeline future-proofing your security operations.

The open architecture gives you the flexibility to choose how you store, search, and analyze data, and utilize the security data from best of breed technologies.

SIEM Open Data Platform also offers advanced high availability capabilities through SIEM Message Hub Kafka replication.

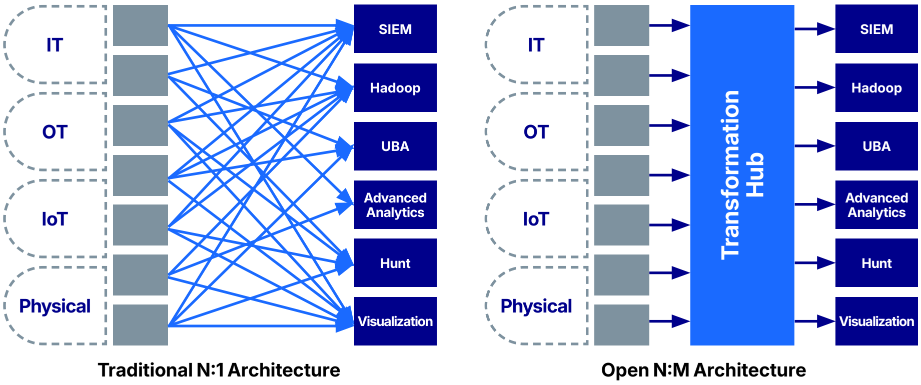
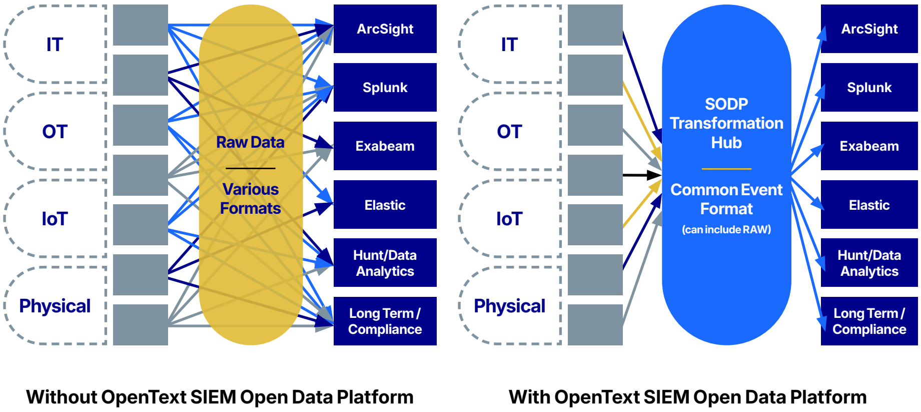


Figure 4. Intelligent message bus architecture

Resources

Learn more at
cybersecurity.opentext.com ›

In conclusion, OpenText SIEM Open Data Platform offers a future-ready security data pipeline solution that normalizes and enriches security data in real time for better threat detection. Its open architecture message bus allows you ingest data from all sources and route it to multiple destinations. SIEM Open Data Platform scales with your enterprise, adds meaning to data for security analysts, and simplifies and future proofs your security data pipeline.



[1] Ponemon Institute - Cost of Insider risk Global Report 2025
[2] Verizon's 2024 Data Breach Investigations Report - 2024
[3] IDC - Worldwide IDC Global DataSphere Forecast, 2024–2028: AI Everywhere, But Upsurge in Data Will Take Time