splunk>

Swimming in Sensors, Drowning in Data:

Navigating OT Modernisation with Splunk Edge Hub

SOMERFORD
Delivering Innovation

Objective

This white paper provides insights into the impact of IT/OT convergence, and explores the opportunities created by leveraging an AI-powered, integrated platform that puts data at the center of every action – and keeps organisations at the cutting edge.

Executive Summary

In the era of Industry 4.0, the Industrial Internet of Things (IIoT) explosion across the process and discrete industrial landscape has brought forth a range of Information Technology [IT] and Operational Technology [OT] convergence challenges. Organisations increasingly seek holistic solutions to transform siloed data from digital and physical environments into actionable insights. Enter Splunk Edge Hub, a leader for organisations aiming to modernise their OT. Combined with the AI-powered, enterprise-scalable analytics platform from Splunk, the Edge Hub enables organisations to predict issues and threats, analyse them intelligently, and respond quickly before downtime occurs by integrating data from the Edge.

Putting Data Front and Center

More than a decade ago, United States Air Force Captain David Deptula offered a prophetic insight to US Intelligence Office military strategists about a future overwhelmed by data from a proliferation of sensors—a scenario of “swimming in sensors and drowning in data.” This prediction has become increasingly relevant today. Digital transformation includes distributing the enterprise to the edge— demanding operations and data architecture that is fully connected and secured.

Gartner predicts that 50 percent of enterprise- managed data will be created outside the cloud amid a tripling of IoT devices from 2020 to 2030. The global Internet of Things (IoT) market size is projected to grow from $714.48 billion in 2024 to $4,062.34 billion by 2032, at a compound annual growth rate (CAGR) of 24.3%. This exponential growth underscores the immense potential of edge computing and data analytics. The stakes are high—but the opportunity is vast—encompassing smart manufacturing, data centers, network closets, analytics and visualisation, robotics and automation, and detection and response to the edge within various industries.

While the convergence of OT and IT promises a new level of operational efficiency and innovation, it also introduces challenges, including a lack of visibility, risk of downtime, and coordination across all data flows, tools, environments, and processes. These hurdles impact an organisation’s ability to optimise performance from an observability and security perspective. **Among those challenges:**

Business Continuity.

In a global survey of over 2,100 security and operations professionals in 7 countries and across 11 industries, we discovered that when companies get resilience right, they can save an average of $48 million annually in downtime costs. In addition to minimising downtime, resilient organisations also corral the value of digital transformation to adapt to changing markets, overcome competitive disruptions, and achieve better financial performance overall.

Remote Asset Monitoring and Predictive Maintenance.

A Deloitte study found that equipment failure constituted 42% of unplanned downtime for industrial manufacturers. The challenge of equipment failure is especially egregious at the edge—under conditions that have traditionally been difficult to monitor due to temperature or pressure extremes, dust, grit, or water.

Equipment failure constituted

42%

of unplanned downtime

Sustainability.

Although regulations vary globally, sustainability is good for business. Beyond the added potential of tax incentives and credits, sustainability commitments focus on maximising asset performance, encouraging innovation, protecting brand, and attracting talent. Seventy-eight percent of CEOs in 2023 reported acting on creating climate-friendly products and services in response to customer demand—up from just 25% in 2020. Leveraging technology solutions that help organisations reduce energy usage, optimise resource consumption, and minimise waste is a welcome capability. For example, access to data from OT can help an organisation innovate and optimise its approach to blending energy solutions by calculating how much money is saved using solar versus other methods of energy generation.

78%

of CEOs in 2023 reported acting on creating climate friendly products

Supply Chain Efficiency and Traceability.

Traceability introduces new ways to add value to the supply chain but demands visibility into every aspect of a product's lifecycle. The vast volume of systems and technologies that touch each product's lifecycle is exorbitant. Most organisations have the data—somewhere—but are challenged to use it to innovate and optimise operations, and when captured, often these pieces and parts create their own data silo. Never before has a product provided a standard entry point for metrics and OT data, streaming in near-real time to a centralised data platform for analysis and intelligent insights. "Traditionally, 70% of manufacturing data goes unused or underutilised. With APIs, the barriers between systems are breaking down, and more organisations can see and understand what impacts performance and, in turn, focus investment with higher quality providers or in parts that outperform.

70%

of manufacturing data goes unused or underutilised.

Splunk Edge Hub: Maximising the ROI of OT/IT Convergence

Blind spots across data silos, increasingly sophisticated threats, and disparate tools demand a systematic approach to converging data from IT and physical environments. That data—from sensors, IoT devices, and industrial equipment—has historically been hard to access but is critical to increasing resilience against asset failure, inefficiency, and product quality. Those data problems also stretch to magnify existing and new security challenges—extending to inefficiencies like alert fatigue and mundane tasks—challenges organisations are having trouble solving as teams face talent shortages and retention issues.

Splunk Edge Hub is designed to bridge that gap.

Splunk Edge Hub is a multi-component solution that includes a GPU-powered hardware device and intelligent operating systems (OS) combined with the Splunk Platform and solutions. This open, extensible platform simplifies aggregating data for real-world applications and tools for partners to build upon. Maintaining that data in one place better protects resources, minimises system outages, and improves orchestration across all tools--and corporate IT and plant-level OT environments—to optimise operations. Splunk supports any environment and has existing integrations with hundreds of other technologies to support existing architectures and seamless additions afterward.

Splunk Edge Hub Architecture

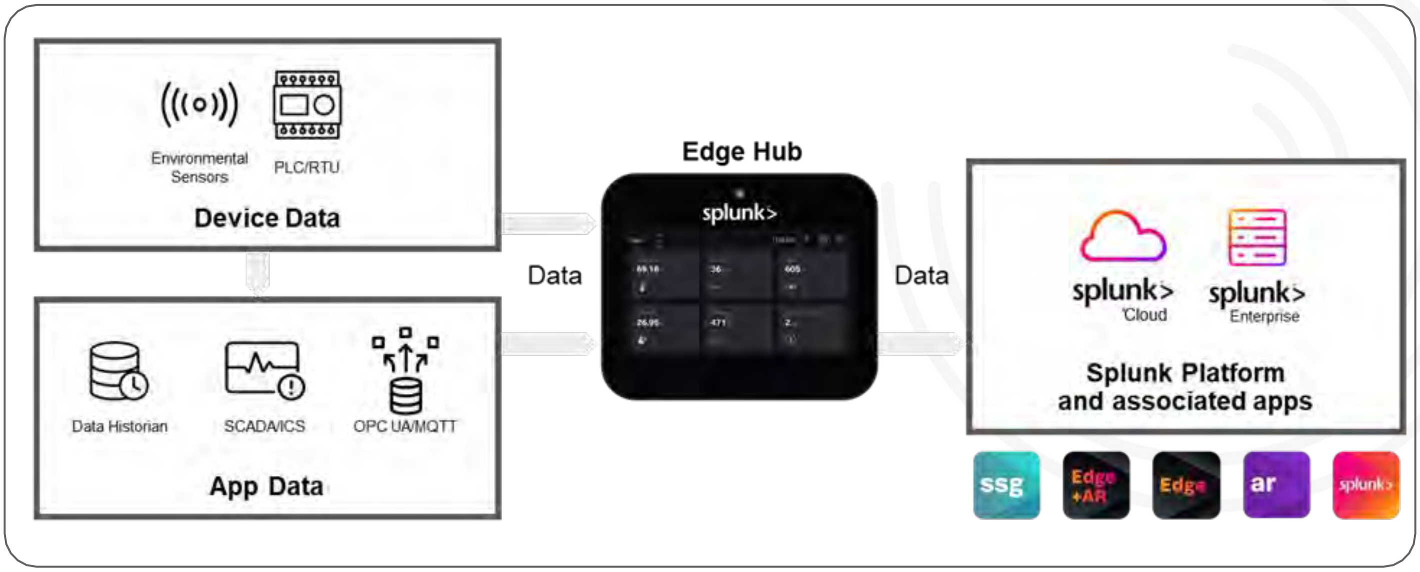


Figure 1. In the Splunk Edge Hub Architecture, sensors connect to Splunk Edge Hub, which sends the sensor data to the Splunk Platform analytics and condition monitoring on the data.

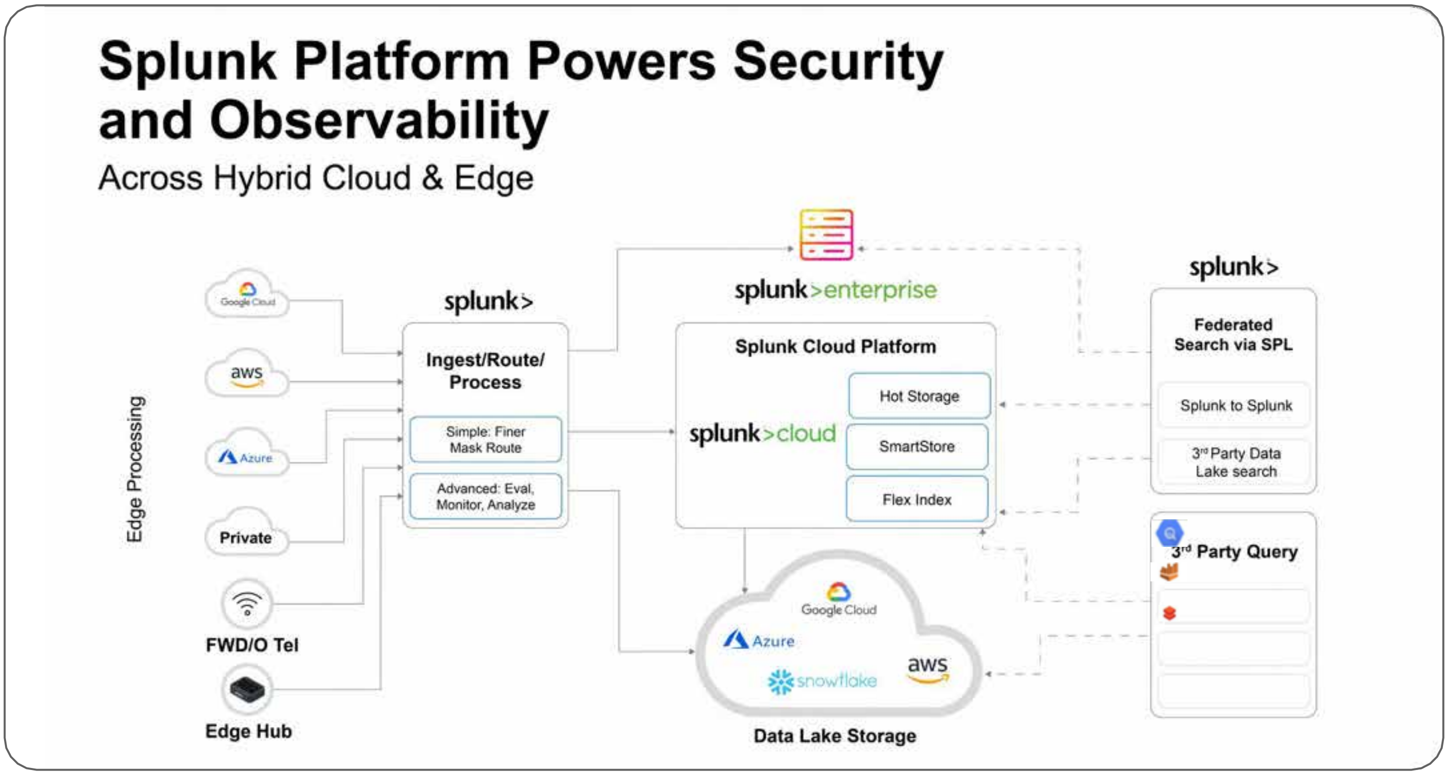
Splunk Edge Hub Extends Protection and Performance to the Edge

Optimised to work with predictive analytics capabilities in the Splunk Platform, Splunk Edge Hub addresses specific security and observability challenges at the Edge. Splunk Edge Hub can retrieve data directly from sensors connected to Splunk Edge Hub, analyse for conditions, and then send the sensor data to the Splunk Platform. With a single command and in a single pane of glass, users can manage data from Splunk Cloud Platform, data from other servers (e.g., Kepware, AutoSol, Matrikon) along with the entire fleet of edge processors providing visibility into both inbound and outbound data volumes at scale.

Splunk Edge Processor uses Splunk Processing Language 2 (SPL2), a second-generation solution, to give customers the flexibility to shape and format data exactly how they want before sending it to be indexed. Splunk Edge Hub can capture data from historians, SCADA, or other control or MES/MOM systems in industrial use cases to create new analytical advantages. Additionally, Splunk solutions can be deployed on-premises for air-gapped or highly classified areas.

In addition, with thousands of purpose-built data source integrations and Splunk base apps, teams can extend the value of the Splunk Platform as the business evolves. Wherever data resides, Splunk Edge Hub helps organisations put data at the center of everything they do.

The Splunk Platform Architecture



Splunk Platform Powers Security and Observability

Across Hybrid Cloud & Edge

Figure 2. The flexible Splunk Platform powers security and observability across hybrid clouds and to the Edge.

Security to the Edge and Back: Accelerate Detection, Investigation, and Response

Splunk Edge Hub is a critical part of a holistic solution that enables organisations to evolve toward the security operations center (SOC) of the future—one that takes a more agile, intelligent, and integrated approach to security. Federation supercharges threat detection, investigation, and response (TDIR). Enhanced visibility and a streamlined process for investigating incidents mean better and faster response coordination. Out-of-the-box machine learning (ML) features reduce time spent analysing data—and enable teams to adapt to meet unique security needs without restrictions. Simply put: More data and faster analysis lead to a better security posture.

Securing OT Equipment. Just as IT has quickly learned of the vulnerability of server-connected printers providing access to the network, OT is noting similar challenges with IoT devices and sensors, further broadening potential attack surfaces. Teams must secure OT or risk creating additional exposure.

Data centralisation is critical to surfacing risks and resolving incidents quickly. While competitive monitoring tools focus on basic metrics and availability, the Splunk platform digs deeper into the rich insights within log and event data. Powerful search language and the ability to correlate across disparate data siloes enables teams to pinpoint the root cause of incidents to ensure they don't happen again. As a result, ITOps teams have reduced MTTR by over 95% and reduced high-priority incidents by over 50%, improving IT efficiency for competitive advantage and boosting customer experiences.

Splunk Edge Hub integrates with leading OT security technologies—including inventory discovery and management systems, network monitoring and anomaly detection solutions, endpoint monitoring, and patch management tools. Thus, Splunk makes it easy for organisations to bridge protections across the vulnerable "air gap."

Detect Unauthorised Use/Access. The Splunk platform helps secure and reduce risk to the production environment by providing investigations and data analysis in the Splunk Platform rather than directly on production systems. Teams using the Splunk Platform can easily revoke credentials from analysts who no longer need production system access, resulting in a more secure environment less prone to human error.

Automate and Accelerate Compliance. As organisational needs and regulatory requirements change, teams need to be able to quickly respond securely—and with accuracy. When changes need to be made, Splunk Enterprise and Splunk Cloud Platform give ITOps teams the data needed to safely and securely roll out and roll back changes at a cloud scale. Automating routine and time-consuming tasks and implementing custom compliance and reporting dashboards can help ITOps teams meet current needs better and scale effectively. Teams can convert logs to metrics, finding correlations and pinpointing trends without the constraints of conventional database structures. What's more, filtered data sets are still federated, so teams are not creating new silos—and when audits demand detail, the data is retained with necessary granularity and easy access to fulfill compliance mandates.

Observability: Enrich Insights Across IT and OT Environments

With cloud-native technologies and microservices, businesses are mastering increasingly complex systems to extract more value, explore new use cases and applications, and enable the seismic shift from reaction to planned response.

Infrastructure monitoring to save time, resources, and costly rework. “Splunk Edge Hub enables us to provide our customers with an end-to-end solution for accessing industrial sensor, maintenance, and operations data at scale”, according to Jason Oney, President of Strategic Maintenance Solutions, a Splunk partner who is a global leader in the implementation, enhancement, and validation of Enterprise Asset Management (EAM) and Calibrated Asset Management systems. “With minimal configuration needed, data can now be seamlessly streamed into the Splunk Platform, allowing our customers to start down the Industrial Transformation journey quickly.”

Managing against downtime is best done proactively.

Monitoring critical data center operations can help ITOps teams leapfrog business intelligence (BI) or reporting teams, which are often hampered by slow and brittle extract, transform, and load (ETL) processing. Splunk Edge Hub enables users to consolidate and organise sensor data from all OT—including 3rd party monitoring systems—between Splunk Edge Hub OS to IP devices on a network using the Simple Network Management Protocol (SNMP) protocol. The platform thus enables teams to analyse machine data to uncover how systems and services are performing in real-time to reduce environmental impact, reduce network outages, and automate reporting requirements.

Hedge against downtime with predictive maintenance and performance analytics.

Sensor data or data from IoT devices at the edge can be used to identify risks or anomalies to help businesses anticipate failures before they occur. Using this data to manage OT assets has a range of benefits. Taking early action can help prevent downtime, save money, and extend the life of the equipment. It enables teams to create more efficient and predictable maintenance schedules and allows mitigation to occur earlier. With Splunk, manufacturing organisation scan prioritise incidents and standardise workflows that impact key success metrics like the reduction of MTTD and MTTR across security and IT, increased (Overall Equipment Effectiveness), and asset uptime across OT. Once teams lock in better operational performance, they can focus on innovation and new opportunities to improve the customer experience—and their bottom line.

Observability: Enrich Insights Across IT and OT Environments

With cloud-native technologies and microservices, businesses are mastering increasingly complex systems to extract more value, explore new use cases and applications, and enable the seismic shift from reaction to planned response.

Infrastructure monitoring to save time, resources, and costly rework.

“Splunk Edge Hub enables us to provide our customers with an end-to-end solution for accessing industrial sensor, maintenance, and operations data at scale”, according to Jason Oney, President of Strategic Maintenance Solutions, a Splunk partner who is a global leader in the implementation, enhancement, and validation of Enterprise Asset Management (EAM) and Calibrated Asset Management systems. “With minimal configuration needed, data can now be seamlessly streamed into the Splunk Platform, allowing our customers to start down the Industrial Transformation journey quickly.”

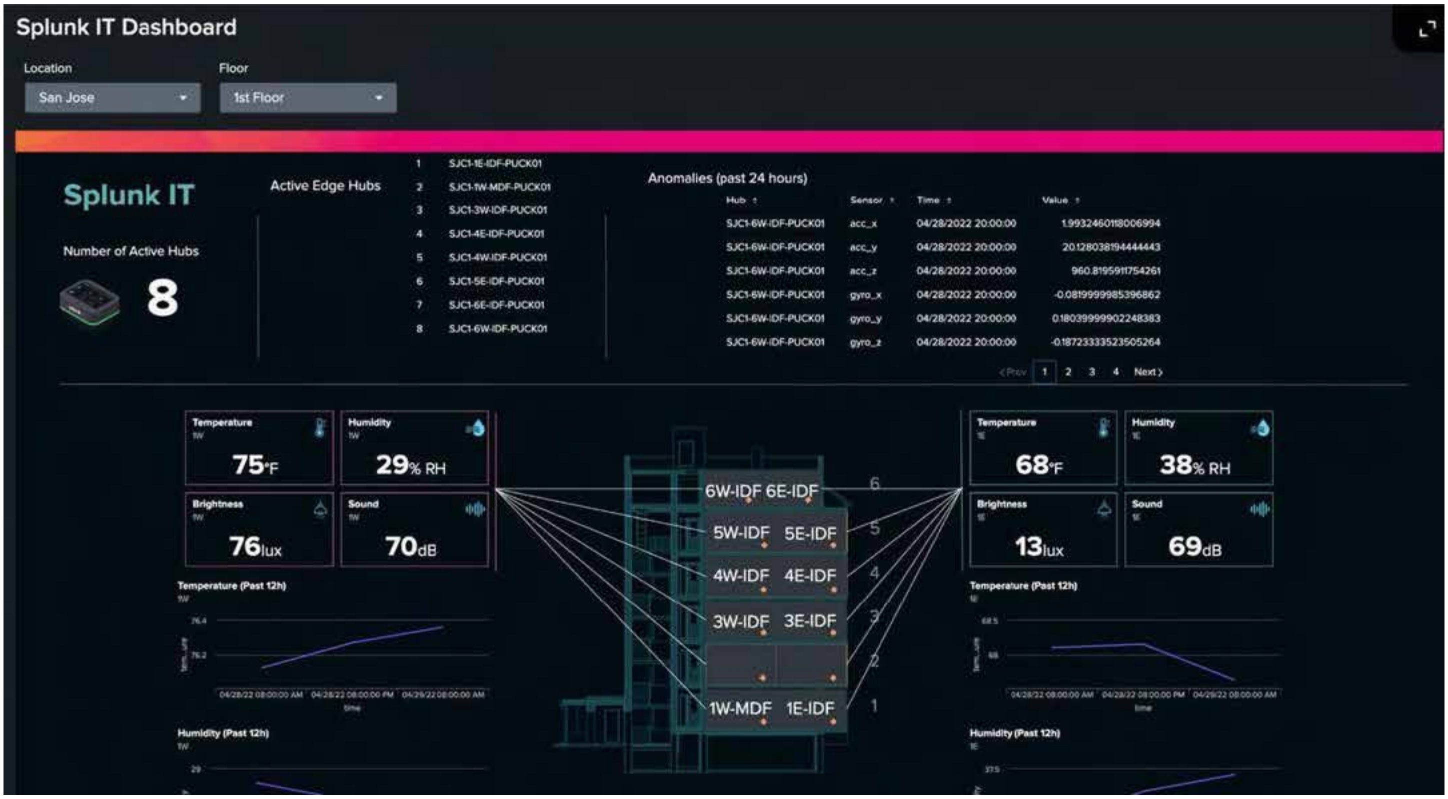
Managing against downtime is best done proactively.

Monitoring critical data center operations can help ITOps teams leapfrog business intelligence (BI) or reporting teams, which are often hampered by slow and brittle extract, transform, and load (ETL) processing. Splunk Edge Hub enables users to consolidate and organise sensor data from all OT—including 3rd party monitoring systems—between Splunk Edge Hub OS to IP devices on a network using the Simple Network Management Protocol (SNMP) protocol. The platform thus enables teams to analyse machine data to uncover how systems and services are performing in real-time to reduce environmental impact, reduce network outages, and automate reporting requirements.

Hedge against downtime with predictive maintenance and performance analytics.

Sensor data or data from IoT devices at the edge can be used to identify risks or anomalies to help businesses anticipate failures before they occur. Using this data to manage OT assets has a range of benefits. Taking early action can help prevent downtime, save money, and extend the life of the equipment. It enables teams to create more efficient and predictable maintenance schedules and allows mitigation to occur earlier. With Splunk, manufacturing organisation scan prioritise incidents and standardise workflows that impact key success metrics like the reduction of MTTD and MTTR across security and IT, increased (Overall Equipment Effectiveness), and asset uptime across OT. Once teams lock in better operational performance, they can focus on innovation and new opportunities to improve the customer experience—and their bottom line.

Splunk Edge Hub Dashboard



Splunk IT Dashboard

Location: San Jose

Floor: 1st Floor

Splunk IT

Number of Active Hubs: 8

Active Edge Hubs

1	SJC1-1E-IDF-PUCK01
2	SJC1-1W-MDF-PUCK01
3	SJC1-3W-IDF-PUCK01
4	SJC1-4E-IDF-PUCK01
5	SJC1-4W-IDF-PUCK01
6	SJC1-5E-IDF-PUCK01
7	SJC1-6E-IDF-PUCK01
8	SJC1-6W-IDF-PUCK01

Anomalies (past 24 hours)

Hub	Sensor	Time	Value
SJC1-6W-IDF-PUCK01	acc_x	04/28/2022 20:00:00	1.9932460118006994
SJC1-6W-IDF-PUCK01	acc_y	04/28/2022 20:00:00	20.128038194444443
SJC1-6W-IDF-PUCK01	acc_z	04/28/2022 20:00:00	960.8195911754261
SJC1-6W-IDF-PUCK01	gyro_x	04/28/2022 20:00:00	-0.0819999985396862
SJC1-6W-IDF-PUCK01	gyro_y	04/28/2022 20:00:00	0.18039999902248383
SJC1-6W-IDF-PUCK01	gyro_z	04/28/2022 20:00:00	-0.18723333523505264

Figure 3. Users can correlate information across IT and OT to create customisable dashboards that enable monitoring, analytics, and fast detection and response across their ecosystem.

“In today’s fast-paced business landscape, innovation is key to staying ahead of the competition,” said Bongsu Cho, Vice President of the AI & Big Data Division at LGE, a partner who relies on Splunk to help them disrupt traditional industry models to drive innovation with edge computing and AI. “Splunk Edge Hub enables us to go beyond data and automate our physical operations.”

Aggregate data from disparate OT/IoT sources to enrich visibility and drive business resilience. With customised solutions built by Splunk Edge Hub Partners, users are empowered to shape data in a way that provides the most value. No matter the data source—machine data, logs, and events—holistic visibility enables teams to import data or train AI and ML algorithms from anywhere. Splunk Edge Hub is compatible with third-party sensors and integrations. SPL2 lends a hand by filtering verbose data sources to attack data sprawl. Data is collected and indexed from any location and can be enriched and managed to route chunks of data from the edge or cloud into the Splunk platform or ship it to third-party data lakes to optimise for performance based on the use case. Edge Processor gives users control over data in motion, improving productivity simply and at scale by helping organisations organise and prioritise data according to use case and location.

Splunk Partners have always been instrumental in delivering custom security and observability solutions using Splunk capabilities. Selected for their proven record of delivering edge technology solutions across industries, Splunk Edge Hub partners provide the critical domain expertise necessary to accelerate the detection, investigation, and response to operational interrupts and security alarms in physical and industrial environments.

Conclusion

Splunk Edge Hub streamlines the integration of data from various sources into Splunk's AI-powered, enterprise-scalable analytics platform, extending its capabilities to address specific security and observability challenges at the edge. With its focus on improved analytics and reporting, Splunk Edge Hub enables organisations to predict issues and threats, analyse them intelligently, and respond quickly, before downtime occurs. Splunk continues to lean into its partner community to remain innovative, bridge into evolving needs at the edge, and meet our joint customers where they are—at the cutting edge.

SOMERFORD
Delivering Innovation

Somerford are an Elite Splunk Partner with expert certified Splunk Edge Hub consultants offering unparalleled value from our services. As well as the Splunk Edge Hub, Somerford Associates is on hand to deliver other Splunk services to meet any requirement.

- In-House Support Desk
- Annual In-Person Device Check
- Account Management
- Expert Implementation

Somerford's Splunk Edge Hub '101' Showcase

-

Watch our 20-minute showcase to understand Splunk Edge Hub and our partnership with Splunk for onboarding and support.

WATCH NOW

splunk> turn data into doing