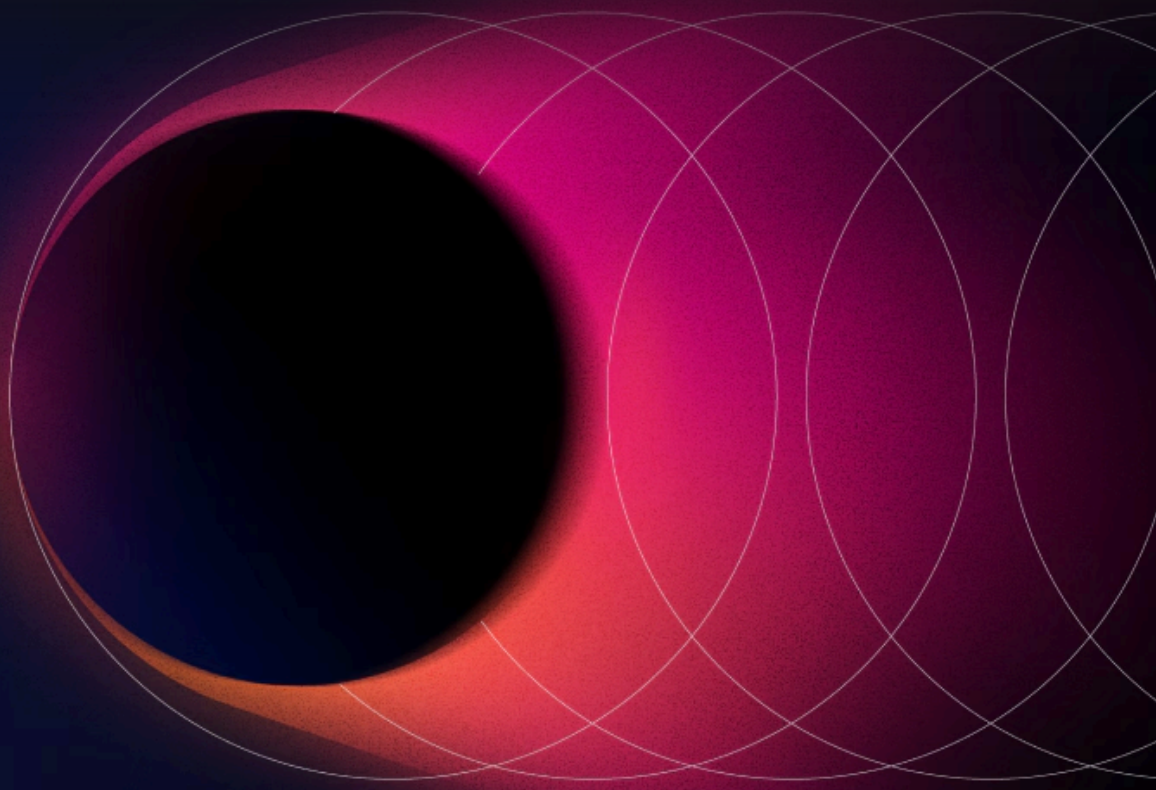
LOGICALIS
Architects of Change

splunk>
a CISCO company

Solution Brief

Logicalis + Splunk

Mastering observability: Powering predictive intelligence through unified data



Optimize digital performance with Logicalis and Splunk

Logicalis brings over 25 years of experience guiding customers through technological change. Together with Splunk, a Cisco company, we give organizations unified visibility across their entire digital footprint, bringing security and observability together on one data platform.

We go beyond basic tool deployment to design, integrate and manage Splunk as your central data backbone, turning massive volumes of telemetry into usable, prioritized insights. The result is a unified, proactive observability model that optimizes performance, strengthens resilience and fuels digital transformation on a global scale.

7,000

professionals managing the full lifecycle

30+

territories, so your Splunk investment delivers long-term value



Visibility that enables confidence in scaling AI

The complexity of today's enterprise tech stacks across all apps and services, both on-prem and across multiple clouds, is impacting resilience and slowing innovation. Without a structured data foundation, AI initiatives often fail because the underlying data is disconnected or lacks context.

Logicalis and Splunk let you see across the entire stack, from the application to the network, so you can stop issues before they become major incidents and scale AI securely.

Common challenges

Siloed operations	Teams use disconnected tools, leading to fragmented timelines and conflicting conclusions.
Data exhaustion	Overwhelming telemetry volume explodes costs without providing actionable operational value.
Weak foundations	Poorly structured data prevents the effective scaling of AIOps and predictive modelling.
Security gaps	Limited visibility into risks driven by ungoverned AI usage across various tools.

Turning telemetry into Splunk intelligence

Logicalis uses Splunk to normalize logs, metrics and traces from across your environment into a single source of truth. We prioritize critical data to ensure your teams focus on what matters for operational stability.

- **Domain correlation:** Correlate events across network, security and application layers to identify root causes faster, instead of working in isolated organizational silos.
- **Actionable normalization:** Transform raw telemetry from networks, clouds, applications and security tools into structured, actionable data that drives real operational value.
- **Unified truth:** Design data pipelines so security and operations teams share the same visibility, enabling faster resolution of complex, cross-domain performance issues.

End-to-end visibility, from edge to cloud

De-risk modernization and build a resilient, observable, global foundation

We help you structure and connect data properly in Splunk to feed AIOps and SecOps models and then scale. This foundation allows for predictive insights, helping you detect potential failures and security anomalies before they impact users, turning reactive maintenance into proactive optimization.

Predictive insights
Advanced anomaly detection identifies potential infrastructure failures before they result in costly, user-facing outages.

Contextual integrity
Ensure data context is preserved across the stack for the success of machine learning and AIOps initiatives.

Real-time operations
Use Splunk analytics across all your telemetry to run the enterprise in real time, fulfilling the promise of a data-driven digital strategy.

AI readiness
Build environments that are resilient and observable before scaling high-stakes AI workloads.

Proven with Logicalis customers



Vertically integrated manufacturer/retailer
Logicalis helped the customer get observability across off-the-shelf ERP and custom applications through Splunk AppDynamics, resulting in better performance and more reliable core services for the business.



Food distributor
Logicalis delivered a managed Splunk-based SIEM solution to manage the entire Cisco and IBM estate, centralizing security events through the customer's Cisco MXDR environment to reduce costs and improve security coverage.

Security-first infrastructure and proactive threat hunting

Logicalis positions Splunk as the data and analytics backbone of your security operations, a high-fidelity intelligence center for your SOC. We create a closed-loop system where security telemetry from the endpoint to the cloud, including your Cisco security controls, is normalized and contextualized within Splunk.

Security operations backbone

Unified SIEM and XDR workflows	Logicalis integrates XDR, including Cisco XDR, directly into your Splunk environment, so security and operations teams work from a single, correlated truth.
Operationalizing global telemetry	We pull rich data from across your security stack into Splunk, including Cisco Umbrella, Duo and Secure Firewall, transforming raw logs into tangible security metrics and cross-domain visibility.
Managed defense at scale	Our managed security teams, the first to launch Cisco MXDR, use Splunk's analytics to manage complex, multi-vector threat hunting across global infrastructures.
Runbook-driven response	Beyond simple dashboards, we build the correlation logic and automated runbooks required to detect and mitigate threats before they escalate into outages.
Zero-trust validation	We use Splunk to monitor and enforce zero-trust policies across your architecture, ensuring identity control is baked into every layer of the digital environment.

Ready to get started?

Contact your Logicalis Account Representative today to modernize your observability strategy with Logicalis and Splunk, a Cisco company.



Contact us

LOGICALIS Architects of Change | splunk> a cisco company

© 2026 Logicalis. All rights reserved.

CISCO PARTNER
Cisco Preferred Cloud and AI Infrastructure Partner
Cisco Preferred Security Partner
Cisco Preferred Collaboration Partner
Cisco Preferred Services Partner
Cisco Preferred Networking Partner
Splunk Partner