Connection
we solve IT

Splunk Professional Services

Connection's Splunk Professional Services leverage the advanced technical expertise of our Splunk subject matter experts to help organizations at any place in their Splunk journey. For first-time Splunk customers, our Splunk specialists help organizations to quickly adopt and realize the value of the Splunk platform, whether on-premises or in the cloud. For those with an existing Splunk footprint, we understand that many organizations have made significant investments in Splunk, yet still struggle with rising ingest costs, unused capabilities, and stalled adoption due to limited expertise and architectural complexity. Connection helps organizations move from data overload to decisive action, transforming Splunk into a fully adopted, optimized platform that delivers real outcomes across security, observability, and IT operations.

Splunk and Actionable Data: The Power of a Unified Data Platform

Splunk gives organizations visibility into the health, security, and performance of IT systems by turning raw machine data into actionable intelligence.

Splunk is a data analytics platform designed to help IT operations and security teams leverage the massive volumes of machine-generated data produced by modern systems—servers, applications, networks, cloud services, and security tools. Splunk centralizes this data and makes it searchable and actionable in near-real-time. Splunk elevates an organization's data into operational and security intelligence that helps reduce downtime, improve resilience, and manage cyber risk. Organizations utilize Splunk in four primary operational domains:

- **IT Operations and Reliability**: Quickly diagnose outages, performance slowdowns, and system failures by correlating logs and metrics across the entire environment, reducing downtime and improving service availability.
- **Cybersecurity (SIEM/SOAR/XDR)**: Detect and investigate threats by analyzing activity from firewalls, endpoints, identity systems, and cloud platforms. Splunk can generate alerts, support incident response, and help meet regulatory requirements.
- **Observability and Application Performance**: Monitor how applications and infrastructure behave in production, especially in complex cloud and microservices environments.
- **Compliance and Reporting**: Retain logs and generate audit reports showing access, changes, and security events.

Connection's Splunk Services combine Cisco Gold Partner expertise with Keos's elite engineering to deliver end-to-end value. **Splunk + Keos = Actionable Data**

Connection's End-to-end Splunk Professional Services:

Connection's Splunk services are described below, organized into the following domains:

- Exploratory, Remediation, and Optimization Services
- Foundational Adoption and Implementation Service
- Splunk Observability Platform Implementation Services
- Splunk Enterprise Security (ES) Implementation Services
- Splunk Expansion Add-ons and Consulting Services

splunk> a CISCO company

From Tool Sprawl to Operational Clarity—Turning Data into Doing

Organizations need outcomes, not more platforms to manage. As environments grow more complex, we provide a practical way to cut through noise, control cost, and act faster by aligning security, operations, and infrastructure on a single platform. Connection's comprehensive portfolio of Splunk Services offerings can easily be leveraged to fit the immediate needs and future roadmap of any organization.

Connection partners with Keos to deliver industry-leading professional services for Splunk adoption and optimization. Keos is Splunk's largest professional services provider in the U.S., holding the highest certifications across the entire Splunk portfolio, with 10 years of experience delivering Splunk services. Offerings encompass the entire lifecycle spectrum—from design and architecture to full platform implementation and expansion services—with performance optimization and environment remediation ensuring operational, data, and licensing efficiency.

Why Connection?

Connection offers products, technical expertise, services, and solutions to help your business adapt to the ever-changing technology landscape. Connection designs and deploys infrastructure solutions tailored to each customer's unique business needs, enabling them to optimize spend while enhancing agility.

Connection
we solve IT

OUR SPLUNK SERVICES AT A GLANCE

Exploratory, Remediation, and Optimization Services

Assess the current environment, uncover gaps, and identify opportunities for optimization.

Includes: Product evaluations, architectural workshops, license optimization, and health checks.

Foundational Adoption and Implementation Service

Establish a solid Splunk foundation, onboard critical data sources, and accelerate adoption with certified expertise.

Includes: Core deployment, data ingestion, staff augmentation, and retained Splunk experts.

Observability Platform Implementation Services

Extend Splunk into full-stack observability to deliver real-time insight into applications, infrastructure, and service health.

Includes: Splunk Observability Cloud and ITSI implementations.

Enterprise Security (ES) Implementation Services

Modernize security operations with SIEM, SOAR, UEBA, and AI-driven analytics that reduce noise and strengthen threat response.

Includes: ES deployment, use case development, SOAR automation, UEBA, RBA, and AI enablement.

Splunk Expansion Add-ons and Consulting Services

Scale and transform the platform with on-premises to cloud migration, new capabilities, and enhanced data ingestion functionality.

Includes: Splunk Cloud migration and Edge Processor implementation.

Splunk Exploratory, Remediation, and Optimization Services:

- **Splunk Product Evaluation and Planning (POC)**: To evaluate if Splunk is the proper solution for your organization, Connection's subject matter experts will architect, install, and configure a fully functioning Splunk POC environment using real customer data, then illustrate Splunk's capabilities while demonstrating its performance.
- **Splunk Health Check**: A comprehensive review of your Splunk environment from the operating system up. This one-week health check and assessment deep-dives into the Splunk architecture, data onboarding configurations, search/indexing practices, overall security posture, user behavior, and more.
- **License Reduction and Optimization Service**: This service begins with a full review of all cost-drivers within your Splunk environment, providing expert recommendations on cost reduction—then delivers with a hands-on implementation of cost optimization measures averaging 20% savings!

Splunk Foundational Adoption and Implementation Service:

The Splunk Core Implementation service is typically the first step for customers new to Splunk, and who may also wish to adopt the Observability and/or Enterprise Security (ES) platforms.

- **Splunk Core Implementation**: Connection's Splunk specialists work with you to understand your infrastructural, operational, and compliance requirements to architect and design a Splunk architecture optimized to fit your needs. The Splunk application is then installed and configured in a cloud or on-premises environment. Centralized management is deployed for ongoing monitoring and maintenance. Documentation of the deployment is delivered along with preliminary training on platform usage and operations.
- **Splunk Data Ingestion**: Following the deployment or expansion of the Splunk platform, additional data feeds may be needed to increase visibility, cover specific use cases, or protect against specific threat vectors. This add-on service allows for additional data to be added to Splunk Enterprise or Splunk Cloud.
- **Splunk General Consulting – Staff Augmentation**: Following a Splunk platform implementation or enhancement, more KPIs, alerting, and service onboarding may be necessary to increase visibility and monitoring. This add-on service provides additional resources to perform Splunk configuration and onboarding tasks.

Splunk Observability Platform Implementation Services:

- **Splunk Observability Implementation**: Architect, install, and configure OpenTelemetry (OTel) collector agents for the ingestion of logs, traces, and metrics. Data is normalized and leveraged within O11y's three primary tools: Application Performance Management, Real User Monitoring, and Synthetic User Monitoring. Dashboarding is created for holistic visualization, and alerting is configured.
- **Splunk ITSI Implementation**: Architect, install, and configure Splunk ITSI as the foundation of the Splunk Observability posture. Data is normalized, and assets onboarded for data enrichment. The Service Analyzer tree is assembled with KPIs and dynamic thresholding to provide clear monitoring of both infrastructure and services. Correlation searches and event aggregation policies are built to provide insightful alerting and contextual information for investigation and remediation.

Splunk Enterprise Security (ES) Implementation Services:

A comprehensive implementation of Splunk Enterprise Security (ES) may follow the sequence of services outlined below:

- **Splunk Enterprise Security (ES) Implementation**: Architect, install and configure Splunk Enterprise Security as the foundation of the Splunk security posture. All data is normalized for data model use, and Assets and Identities are aggregated for data enrichment.
- **Splunk Use Case Development Workshop**: A complete mapping of the organization's threat vectors is performed in alignment with the MITRE framework, in order to define which security detections are required.
- **Splunk Risk Based Alerting Implementation**: All detections outlined previously are written, tested, and scheduled for active security coverage. Connection's algorithm will be used to integrate data enrichment and further maximize alert fidelity.
- **Splunk AI Enablement**: Additional AI-enabled security detections are written, tested, and scheduled to achieve increased coverage and fidelity.
- **Splunk SOAR Implementation**: Architect, install, and configure Splunk SOAR to become the executive arm of the organization's security posture, acting upon the alerts generated by Splunk Enterprise Security.
- **Splunk SOAR Playbook Implementation**: Construction of custom automations (playbooks) that respond to threats generated by Enterprise Security.
- **Splunk UEBA Implementation**: Architect and configure Splunk UEBA (User and Entity Behavior Analytics) for advanced security anomaly detection. UEBA is trained on the organization's asset and identity information and then integrated with Splunk Enterprise Security and Splunk SOAR, enabling the detection and contextualization of anomalous behavior amongst security events, resulting in more rapid investigation and remediation.

Splunk Expansion Add-Ons and Consulting Services:

The following are common services that supplement or transform an existing Splunk deployment:

- **Splunk Edge Processor Implementation**: Architect, install and configure Splunk Edge Processor for advanced data ingestion capabilities, from data parsing to transformation to routing. Data pipelines will be constructed in SPL2 for complete control of incoming data sources, all managed through a single control plane.
- **Splunk Cloud Migration**: Migrate an organization from an existing on-premises Splunk environment to a new Splunk Cloud instance, preserving all data onboarding pipelines and knowledge objects. This includes multi-phase validation of data routing and the decommissioning of the original on-premises Splunk infrastructure.

Cisco Partner

Unlock the Full Value of Splunk with Connection

Expert-led Services to Maximize Your Splunk Investment

To learn more about our Splunk Professional Services, contact your Connection Account Team today!

1.800.998.0067 ■ www.connection.com/services