



What is the Splunk Health Check and Assessment?

The Splunk Health Check is a comprehensive, data-driven assessment of your Splunk environment. It leverages our industry-leading Splunk subject matter experts—whose knowledge and deep expertise enable impactful and actionable environmental discovery and recommendations—resulting in an optimal architecture and configuration bolstered by enhanced security and resiliency.

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.

Splunk Health Check and Assessment Service

The Splunk Health Check and Assessment from Connection is a comprehensive service that helps to proactively identify and resolve performance bottlenecks, configuration issues, and potential risks within your Splunk environment. Leveraging the advanced diagnostic and analytics capabilities of our Splunk subject matter experts, this service delivers actionable insights that support faster remediation, improved reliability, optimized performance, and reduced operational risk.

Customer Benefits of the Splunk Health Check and Assessment

Our experienced Splunk consultants deliver a streamlined, yet comprehensive, Splunk health check and assessment that provides deep and actionable insights. Working with your organization, our professional services team leverages the outputs of the health check to drive concrete outcomes—delivering improvements in observability, performance, resiliency, and security. Additional benefits of the Splunk Health Check include:

- **Independent Expert Analysis:** Gain objective insights from certified professionals who bring expertise and experience interpreting complex Splunk environments.
- **Rapid Time-to-Value:** Our streamlined diagnostics approach enables comprehensive assessments to be completed in a single week.
- **Visibility into Hidden Problems:** The Health Check identifies underlying problems—such as data parsing issues, instance misconfiguration, security vulnerabilities, or ineffective SPL queries—that often go undetected by routine audits.
- **Baseline for Future Improvements:** The establishment of a performance and configuration baseline to measure progress against—and to support future initiatives and business processes such as Splunk environment expansion, executive review sessions, or governance, compliance, and security audits.
- **Justification for IT Investment:** Documented findings highlight opportunities for cost savings, realization of platform value, and performance optimization—supported by concrete technical evidence while outlining business impacts.

Beyond Actionable Insights: Potential Outcomes and Next Steps

- **Actionable Remediation Plan:** Receive a prioritized list of Splunk environmental issues with clear remediation guidance—focused on impact, urgency, and effort.
- **Remediate Identified Issues:** Our Splunk experts can help you prioritize and address the most critical misconfigurations, performance obstacles, and cost inefficiencies uncovered during the Splunk Health Check and Assessment.
- **Development of a Long-term Optimization Plan:** Health Check and Assessment findings can be leveraged to guide strategic environment growth, user adoption planning, cost minimization measures, and platform alignment with organizational initiatives.
- **Schedule Follow-up Validation:** Our Splunk specialists can work with you to plan a follow-up engagement to verify remediation effectiveness and validate that performance baselines have improved.

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:

- 1. 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.
- 2. 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.
- 3. Observability and Application Performance:** Monitor how applications and infrastructure behave in production, especially in complex cloud and microservices environments.
- 4. Compliance and Reporting:** Retain logs and generate audit reports showing access, changes, and security events.

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

Related Splunk Services Offerings and Add-on Service Modules:

- **Security Use Case Workshop:** A full review of your Splunk security detections which uses the MITRE framework to categorize and identify undetected threat vectors—and then provide recommendations and step-by-step guidance to comprehensively defend against broad-spectrum threat vectors.
- **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!

What Is Included in the Splunk Health Check and Assessment?

- Environment discovery and usage mapping
- Configuration validation and performance metrics
- Architectural and systems review
- Data ingestion evaluation
- Search and user behavior analysis
- Documentation of findings and prioritized recommendations

Splunk Health Check and Assessment Deliverable Report

The Splunk Health Check concludes with a report which includes the following:

- Executive Summary
- Architecture and System Overview and Recommendations
- Search, Indexing, and Data Overview and Recommendations
- Configuration and Security Overview and Recommendations
- Miscellaneous Overview and Recommendations
- Summary of Findings with Prioritized Recommendations and Roadmap

The Splunk Health Check and Assessment report provides a comprehensive overview of environment health, performance, inventory, and security insights based on data collected. The report summarizes the top findings with evidence, enumerates expected outcomes of executing upon the report's recommendations, and concludes with a prioritized implementation roadmap.



Unlock the Full Value of Splunk with Connection

Expert-led Services to Maximize Your Splunk Investment

To learn more about the Splunk Health Check and Assessment Service, contact your Connection Account Team today!

1.800.998.0067 ■ www.connection.com/services