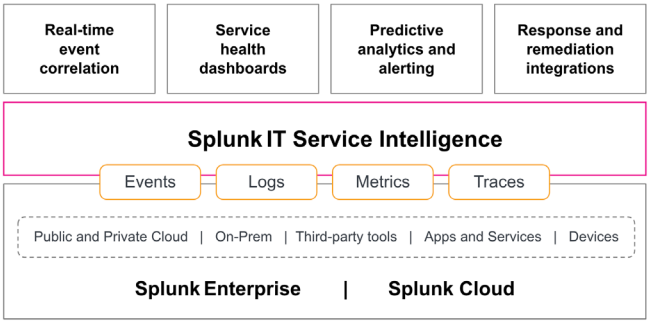
splunk>

PRODUCT BRIEF

Splunk IT Service Intelligence

Proactively prevent outages with AIOps

- **Align IT with the Business**
  A single live view of relevant IT and business services data makes it easy to view service health and troubleshoot. Reduce unplanned downtime by 60%.
- **Reduce Alert Noise**
  Reduce alert noise by 95% and MTTR by 90%.
- **Proactively Prevent Outages**
  Prevent service degradations 30 minutes in advance and reduce total incidents by 45%.



In increasingly complex environments, IT teams need to support even more business-critical services. Traditional ITOps tools aren't equipped to manage hybrid environments and can prevent teams from effectively supporting business demands. Splunk® ITSI equips organizations with the agility, tools and visibility required to protect today's business-critical services and their hybrid environments.

Splunk® IT Service Intelligence (ITSI) is an AIOps, analytics and IT management solution that helps teams predict incidents before they impact customers. Using AI and machine learning (ML), ITSI correlates data collected from monitoring sources and delivers a single live view of relevant IT and business services, reducing alert noise and proactively preventing outages.

Built on Splunk® Enterprise or Splunk® Cloud, Splunk® ITSI quickly identifies problems and delivers guided troubleshooting and actionable next steps. Predictive performance dashboards monitor service health, and integrations with IT service management (ITSM) and orchestration tools, like Splunk® On-Call and Splunk® SOAR, teams can monitor, detect, respond and resolve incidents all from one place.

Leidos

Fortune 500 Defense and Technology Leader

Leidos implemented Splunk to manage 120 services and 20 management systems. As a result, they reduced alert noise by 98%, reducing 3,500 daily events to 50 actionable tickets.

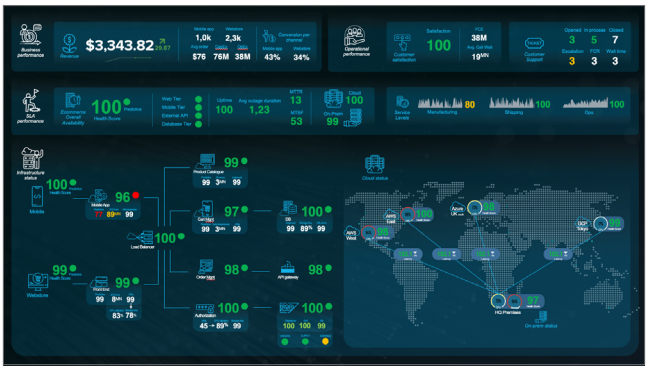
Talk Talk

United Kingdom Telecommunications and Connectivity Provider

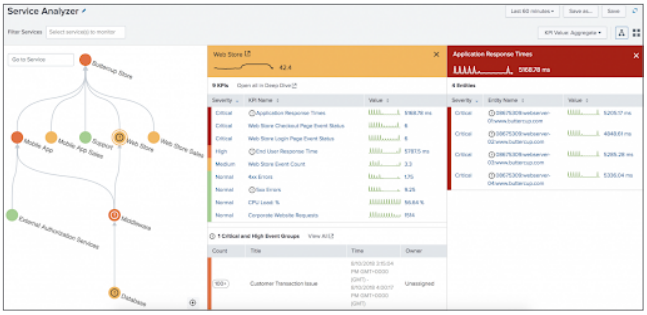
With 4 million customers and 6 million tests per day, TalkTalk required real-time performance monitoring for hundreds of metrics. Within a year of adopting Splunk, customer service improved and TalkTalk's Net Promoter Score (NPS) increased by 22 points.

End-to-end service visibility

Glass Tables: Monitor business performance and service health with pre-built or custom dashboards in this single pane of glass view.



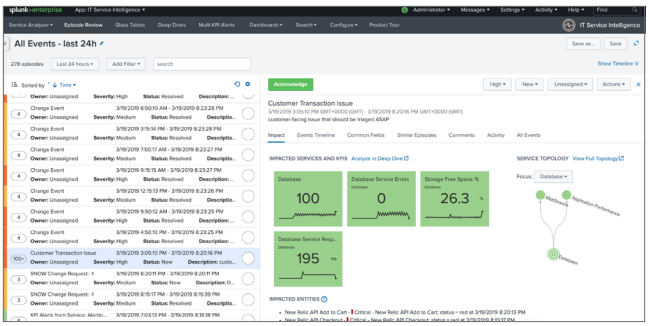
Service Analyzer: Visually correlate services to underlying infrastructure with a tile or tree view. Drill down to identify root cause from service monitoring dashboards by following a directed troubleshooting workflow.



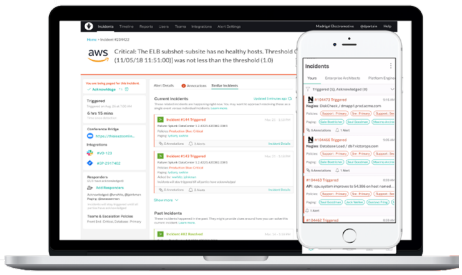
Deep Dives: Use side-by-side displays of multiple services and correlate metrics over time to identify root causes.

Alert Noise Reduction

Intelligent Event Management & Analytics: Collect and enrich events from multiple sources into a single alerting framework. Real-time, automated event correlation triggers alerts as data enters the system, using out-of-the-box (OOTB) machine learning policies for immediate noise reduction. Incidents are automatically prioritized by service score and impact.

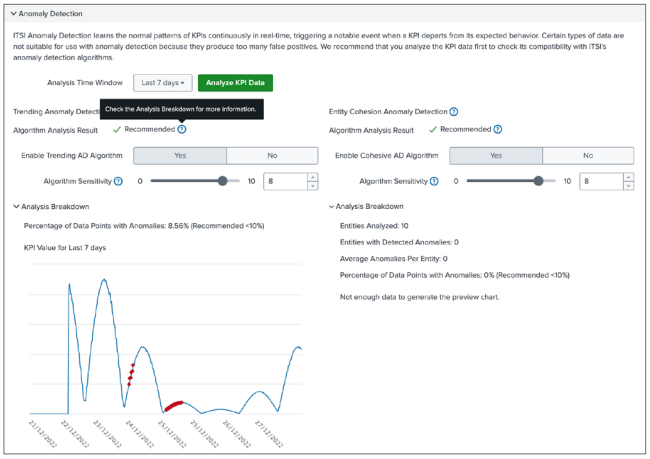


Integrations with External ITSM Tools: Trigger service ticketing, on-call response or automated playbooks directly from your incident review for fast incident resolution.

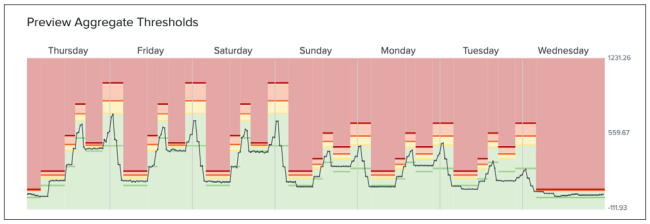


Proactive Outage Prevention

Anomaly Detection: Use historical data to alert on unexpected behavior for one or multiple events. Patterns are continuously updated in real time.

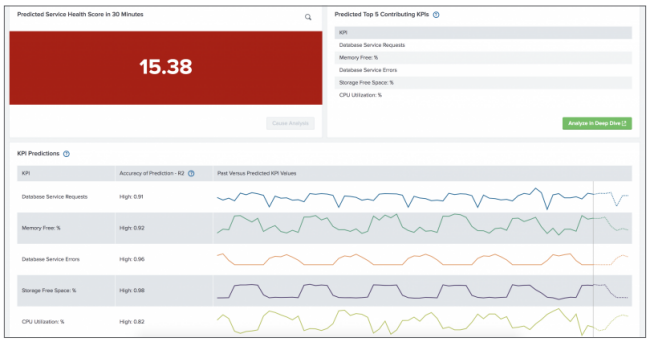


Static and Adaptive Thresholding: Set static or adaptive thresholds to enable alerts only when behavior strays from normal. With adaptive thresholding, machine learning automatically updates thresholds based on observed behavior so your alerts don't become stale. Set custom threshold windows for special times during the year where the regular severity levels don't apply — like Black Friday.



Predictive Analytics

Predict future incidents up to 30 minutes in advance using machine learning and historical service health scores. The top five contributing service metrics are displayed to guide troubleshooting.



ITSI product page

24-351320-Splunk-ITSI Product Brief-107

Splunk for Observability

Quickly find, analyze and resolve incidents anywhere in your stack (multicloud to microservices to serverless) to lower MTTR, deliver high performing applications and world-class customer experiences.

Modern application challenges

The need for innovation and faster software development is driving profound changes in how applications are built and operated. The adoption of microservices architectures, elastic cloud infrastructure (containers, Kubernetes, functions, etc.) and agile DevOps models increases velocity, but also complexity as systems become more dynamic, unpredictable and noisy. Traditional, disjointed monitoring tools can't provide the speed, scale and analytics capabilities needed to support modern digital business like real-time visibility, smart altering and rapid troubleshooting.

Why legacy monitoring tools make your job harder:

- **Missing data.** Many monitoring tools sample (or throw out) data and impose limitations on the structure of data they ingest. This creates critical visibility gaps both for users and analytics algorithms, resulting in missed detection of customer-impacting issues and longer issue resolution times. In ephemeral cloud-based environments, sampling techniques can result in a lack of visibility when performing root-cause analysis or retrospectives. Finally, most legacy platforms simply can't ingest anywhere near the full firehose of data that modern apps emit.
- **Slow performance.** Microservice architecture creates a complex web of interactions and relationships. Containers spin up and down in a matter of minutes. Serverless functions are invoked on the order of seconds. Monitoring tools that weren't built to operate at this speed and scale or to quickly handle bursts in traffic miss issues and are ineffective.
- **Lack of intelligence.** Because modern applications run across large numbers of microservices, huge amounts of data are generated from each transaction. Most monitoring tools don't come with any built-in intelligence that add relevant context of the data. Out of the box settings generate too many alerts, and it takes too many people too long to figure out what the problems are.
- **Too many tools.** Because legacy tools simply weren't built for modern application environments, customers often must adopt multiple tools to gain insight into their operations. This leads to tool sprawl, data silos, disjointed workflows and additional training and operation costs.

Splunk helps organizations (DevOps engineers, SREs and more):

Deliver products faster
Accelerate your software delivery process and time to market to meet business objectives more quickly.

Improve customer experience and retention
Catch and fix problems faster to reduce downtime, avoid war rooms and improve performance, customer experience and satisfaction.

Improve operational efficiency and TCO
Simplify the observability toolchain, get better visibility and control into cloud utilization and right-size your environments.

Reduce unplanned work
Proactively improve code releases and system architecture with system visibility and better tools for monitoring, troubleshooting and incident response.

Splunk's Observability Cloud

Splunk Observability Cloud is purpose-built to address these monitoring challenges and help you conquer complex environments and applications, reduce time to detect and time to resolve, deliver the best possible end user experiences and consolidate tools. With our products tightly integrated into Observability Cloud, you get a single, comprehensive view across all your data and all your systems so that your teams can operate effectively and efficiently while streamlining workflows, training and budgets.

Splunk Infrastructure Monitoring

Monitor any stack, on-prem, hybrid/multicloud at any scale, all in real time

Splunk APM

Troubleshoot microservices and application issues with NoSample™ full-fidelity distributed tracing

Splunk Log Observer

Investigate and explore logs in context without learning a query language

Splunk RUM

Measure end-to-end user experience with frontend user monitoring

Splunk Synthetic Monitoring

Proactively improve customer experience with API and browser monitoring and web optimization

Splunk On-Call

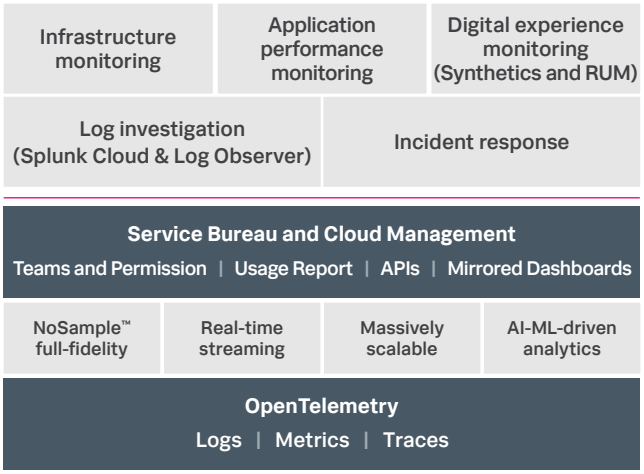
Make on-call suck less with intelligent and automated incident response and collaboration

Go from problem detection to resolution in minutes

Splunk Observability Cloud is the only full-stack, analytics powered and enterprise-grade observability solution. It provides a single, consistent user experience across all metric, trace and log data. One seamless and streamlined workflow can be used during the whole life cycle of issues for monitoring, troubleshooting, investigation and resolution. Whether you're a frontend developer who needs to know what end customers are experiencing, a backend developer building the most performant APIs and services or an SRE who's frequently on call, Splunk's Observability Cloud helps you get the analytics driven, context-rich insight you need to quickly resolve outages. You can also leverage deep insights to proactively prevent issues from arising.

Built for any application, any infrastructure, any business process

Splunk's Observability Cloud helps improve release quality and velocity, improve developer efficiency, and minimize downtime with the following capabilities.



1) **NoSample™ full-fidelity ingest.** Troubleshoot needle-in-a-haystack, unknown failure conditions, and make sure you have the data when you need it. Send your full firehose of metric, trace and log data — no sampling, no filtering. Go back in time to view full traces even for instances that no longer exist.

2) **Real-time streaming.** Significantly reduce MTTR. Detect and alert on critical patterns within seconds, not hours, irrespective of data structure or format.

3) **Massively scalable.** Future-proof your observability investment with a solution that will scale with you and can meet the needs of any cloud-native environment, no matter how large (up to PBs of ingest per day) or how complex (multiple cloud environments all integrated into one system of record), without compromising performance.

4) **AI/ML-driven analytics.** Context-rich directed troubleshooting correlates data from multiple sources in real time to point you to the root cause of problems during incidents. "Related Content" provides in-context exploration, so you can view logs, metrics and traces in context of each other in a single click. Eliminate 100+ person conference bridges and large war rooms. Quickly make sense of all your data, and dramatically reduce MTTD and MTTR. Leverage real-time analytics and dynamic baselines to surface the patterns that are relevant to you and proactively deliver actionable insights. Automatically identify outliers to speed troubleshooting. Leverage infinite cardinality to isolate issues by tenant, region, etc.

5) **Open-standards based.** Own and control your data. OpenTelemetry democratizes access to all telemetry data as well as helps organizations avoid vendor lock-in. OpenTelemetry also provides context for all data sources. Optional lightweight agents are open source and add even more functionality.

6) **Centralized cost and usage management and best practices.** Enterprise-focused features provide complete transparency into and control over usage amounts, eliminating surprise bills. Mirrored dashboards and one-click sharing to common tools help reduce duplicated work and increase consistent adoption of best practices across the enterprise. Observability-as-code provides flexibility and standardization across users.

Use cases

- Cloud migration
- Cloud infrastructure monitoring (Hybrid/multicloud, Kubernetes monitoring, container monitoring, serverless monitoring, virtualization monitoring)
- Application performance monitoring and troubleshooting
- Application investigation and debugging
- SLI/SLO monitoring
- Real user monitoring
- Endpoint (API) uptime and performance
- Synthetic transactions and API testing
- Application life cycle monitoring
- Incident response automation

Observability is critical to success, but it's not often an organization's core competency. That's why it's important to partner with an observability solutions provider like Splunk that can support your digital initiatives.

Trusted by 20,000 customers worldwide and 91 of the Fortune 100

Splunk customers have seen the following benefits

45%
reduction of high-priority incidents

80%
faster MTTD for better customer experiences

36x
faster accurate, AI-driven alerts. Delivered in seconds not minutes.

90%
reduced incident investigation time

80K
saved in overages

30%
faster page loads

96%
faster feature releases

70%
improvement in developer efficiency

“One single component does not guarantee you are observable. It’s the correlation and analysis of all the data — metrics, traces and logs — that deliver observability. Splunk provides this for us so we can focus on innovating and delivering great customer experiences.”

Eric Irwin, Director of Engineering, Quantum Metric

QuantumMetric

Powered by the world’s only Data-to-Everything Platform: built for security, IT, DevOps. Learn more about Splunk Observability Cloud here: https://www.splunk.com/en_us/observability.html

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

21-17881-Splunk for Observability-101-SG