WHITE PAPER

The Power of a Data-to-Everything Platform

How Splunk brings data to every question, every decision and every action

splunk> turn data into doing™

Data is transformative.

We're living in a world of unprecedented innovation. Data, and the technology used to understand it, is transforming how we work and live. Whole industries are evolving before our eyes, and even the smallest-sized organizations are now global. The rate of change is not slowing down. We're at the cusp of an even bigger wave of digital acceleration. Networks are going 5G, the number of connected devices has blown past 22 billion according to Strategy Analytics — headed for 38.6 billion by 2025, and 50 billion by 2030. At the same time, automation is bringing efficiency and responsiveness to business, not to mention convenience to our daily lives. Technologies like blockchain open new possibilities, and artificial intelligence, fueled by the explosive growth of data, brings unprecedented insight at previously unimaginable speed.

Companies that have harnessed their data are thriving, and many of the others have fallen behind. Or fallen. Leaders understand; their organizations are spending billions of dollars and countless hours to try to better tap their data. They're wrangling, integrating and managing massive volumes of data across countless systems. But all this work has kept their focus on data sources instead of data outcomes.

Yes, data is transformative. Not because we have it, but because of what we do with it. It's vital to bring data to every question our organizations ask, every decision we make and every action we take. But in an evolving and increasingly connected world that produces ever more data, the challenge is how to not only keep up with it all, but turn it quickly into insight and action. Data comes in different forms, from varying sources — many that organizations have yet to tap.

The effort has taken the form of "digital transformation" — a decades-old practice of rebuilding around the power of data and technology. Transformation never ends. Organizations will always have to manage and secure their data — but that's table stakes. In an age of digital acceleration, data is the essential asset that drives every innovation, every strategy, and every success.

Achieving this data-enriched state requires a single platform that frees organizations to take action without worrying about where their data is or where it comes from. It must be a robust platform that lets a nontechnical business user run a report and lets a data scientist run wild. The entire organization must be able to leverage the power of data through a singular, holistic platform. This cohesive approach means fewer, smarter technology investments, less complexity and fewer barriers between data and action.

We call this the Data-to-Everything Platform.

Ask three core questions.

How does the transformative Data-to-Everything Platform bring data to every strategic and tactical decision? Each organization's challenges are unique, but three overarching questions span industries, ambitions and use cases:

1. **What's happening in my organization?** You need a real-time snapshot that tells you the status of systems, applications and the business. In a world driven by consumer expectations and split-second disruptions, lagging indicators and outdated reports aren't enough.

2. **How do I turn data into action?** It's not just what you know; it's what you do with your knowledge in the moment of opportunity or crisis. From orchestration to automation, the right tools will enable you to respond more quickly, with greater certainty.

3. **How do I prepare for the data-driven future?** The data needs of tomorrow require organizations to prepare for an accelerated world in which expansive data access, faster decisions and visibility across more types of data are imperative.

The Splunk platform does exactly this. It addresses all three key questions, giving organizations: unprecedented visibility into data across their organizational landscape; insight and the ability to act; and the breadth and scale to incorporate exponential growth, new streams of data, and opportunities that have yet to emerge.

1 It's time to bring data to every question.

Keeping up with all the data in our organizations is even more complicated than many have thought. We're familiar with the data challenges: the velocity, volume and variety of data. But there's another factor that, quite naturally, has been overlooked. Call it visibility. Those rivers of fast-moving, multifaceted data have never been the whole picture. There's a whole class of data we've missed: dark data.

Dark data is all the unknown and untapped data across an organization, particularly that which is generated by systems, devices and interactions. And the whole point of artificial intelligence and automated decision-making is to take the most complete picture your data can provide to make smarter, faster decisions. But how complete, how smart, are those decisions if you're ignoring vast swaths of your data?

Tapping your dark data can seem daunting, but all that digital exhaust from the activities of users, systems, applications and devices can help develop a more holistic picture of what's happening across the organization. Harnessed properly, this overlooked asset can help drive successful transformation and solve myriad challenges, in real-time, like never before.

Splunk's powerful approach to understanding your data focuses on unprecedented capabilities to observe, investigate and monitor your data.

Observe all your data: any type, any location, any source

Collect and index data from virtually any source, whether structured in databases, unstructured in a data lake, or previously unknown (dark). Often, machine data is dark; this high-volume, high-velocity data is highly variable and incredibly diverse — and simply overwhelming for traditional system management, SIEM, CEP/ECA and log management. You can spend weeks or months building custom connectors for each data source. Helped by the expansive Splunkbase collection, the Splunk platform takes data from all of it: packaged and custom applications, app servers, web servers, databases, networks, virtual machines, telecom equipment, operating systems, sensors and much more. You don't need to "understand" the data up front; load it into the Splunk platform with a simple wizard, or stream data from remote systems at scale.

Investigate at speed — without limits

The powerful indexing and search technology of Splunk redefines speed and responsiveness by not requiring you to structure your data before you start asking questions. This schema-on-read approach enables you to search billions of events in seconds and start seeing results immediately. Analyze real-time streaming data and understand behavior in historical context, all through the same interface.

Monitor your data environment

Purpose-built solutions extend the Splunk platform to monitor your specific environment, offering rich dashboards and KPI tracking, investigative capabilities, workflows and more. Achieve and maintain operational excellence with Splunk Enterprise Security, Splunk User Behavior Analytics, Splunk IT Service Intelligence and Splunk for Industrial IoT. The ability to proactively monitor your assets and infrastructure — from the app level to IoT devices — lets you spot issues before they become crises.

Use Case: Analytics-First Approach to Business Processes

Mobility and always-on connectivity let you interact with your data anytime, anywhere, to deliver a superior customer experience, improve efficiencies and reduce costs. This allows IT to add more value to the business by simplifying increasingly complex IT systems and processes, and it lets business users more easily access new insights and information. Splunk's solution for business analytics discovers, analyzes, visualizes and monitors event data from any source, such as applications, mobile devices and servers to provide insights to IT, while giving line-of-business teams a complete understanding of their business operations, to drive greater efficiency and efficacy.

2 It's also time to turn data into action.

What good is it to *know* if you can't *do*? Imagine seeing an immediate market opportunity or a sudden infrastructure overload or a security breach happening right now — and having no way to act. Data is a business asset, and like any other asset, the value is not in having it, but how you use it to create positive outcomes. Splunk makes it possible to analyze your data to draw deeper insight, and to act on that understanding with unprecedented speed.

Anyone can analyze anything

Explore and interact with your data through a powerful interface. Business users can quickly derive keen insights with the simple drag-and-drop user interface, analyzing data without learning the Splunk Search Processing Language (SPL). Pattern detection, instant pivot and an advanced field extractor make it easy for everyone in your organization to turn dark data — structured or unstructured — into powerful insights.

Splunk incorporates artificial intelligence and machine learning capabilities to identify potential problems or insights from the interactions of millions of items of data across your organization. Machine learning rapidly analyzes vast quantities of data to help separate signal from noise. Anomaly detection, baseline samples, and behavioral observation and modeling register connections and causal relationships that might otherwise go undetected. As the platform learns over time, its increasing accuracy helps it become a uniquely valuable expert, laser-focused on the specific problem at hand.

Act quickly — with confidence

Splunk goes beyond monitoring with advanced analytics fueled by artificial intelligence and machine learning, collaborative tools and automation — all from a single platform. The Splunk platform connects users to the information they need most, in real time. From contextual alerts and dashboards to mobile apps, augmented reality, natural language processing or enterprise-grade incident response and investigation, Splunk users can choose how they consume and interact with their data. On-call teams are empowered to find and fix problems faster with automated and insightful incident response.

Splunk Use Case: Real-Time Data to Detect Unknown and Advanced Security Threats

Thousands of organizations rely on Splunk to modernize and strengthen their cyber defense strategy. Splunk software allows enterprises to monitor, report and analyze real-time data and terabytes of historical data located on-premise or in the cloud. The Splunk security approach lets you:

- Map and visualize any potential attack scenario against your most valuable data assets
- Conduct statistical analysis for advance pattern detection and threat defense
- Use automated searches to continuously monitor for abnormal patterns of behavior in host, network and application data — correlating with an understanding of where critical data resides, who should have access, and an analysis of typical vs. abnormal behavior patterns
- Employ custom and out-of-the-box correlation searches to help find threats and determine security and compliance posture

While freeing teams from time-consuming basic management and an excess of false alarms, the cutting-edge combination of anomaly detection and machine learning within Spunk improves the security team's crucial ability to detect unknown and advanced threats.

3 The building blocks are in place; you can prepare for the future now.

Every organization must work to ensure its ability to not only keep up with the ever-faster flow of endless data, but also to bring rich data to every decision, and quickly turn those insights into the best course of action.

Splunk is committed to empowering organizations to understand and act on their data like never before. We continually invest in technological development to expand users' ability to access data across their organization, across new data types, and with

the power of new technology, including artificial intelligence and machine learning. The holistic, source-agnostic data platform, rich developer ecosystem and scalable, hybrid architecture of Splunk will continue to allow organizations to push the boundaries of how they bring data to everything they do.

Tap an expansive ecosystem

As an open platform, Splunk empowers third-party developers to build new apps, and new experiences, using Splunk tools, SDKs, APIs and sample apps and code, to deliver new insights via prebuilt searches, dashboards and visualizations. The new Splunk Developer Cloud enables modern cloud developers to write to new Splunk APIs to access services in a new way, to develop apps that access Splunk in modern languages via RESTful APIs.

Developers have delivered more than 2,000 applications and add-ons in the open Splunkbase marketplace.

Move analytics to the data stream

Splunk Data Stream Processor lets customers collect, process and deliver data to multiple destinations in milliseconds. Moving analytics to the stream means turning raw data into high-value information, getting real-time business insights and protecting sensitive data.

Process massive data sets

Splunk Data Fabric Search lets you search on a massive scale. Process billions of events and conduct searches across multiple Splunk deployments, to reduce mean time to detect (MTTD) and mean time to resolution (MTTR).

Talk with your data

The Splunk platform uses natural language processing so that users can ask questions of their data without knowing how to use the Splunk search language. Get answers instantly from the dashboards on your mobile device, and leverage saved searches associated with various user intents.

View data in context

Splunk AR offers an augmented reality shortcut to accessing any Splunk dashboard by simply scanning a QR code or NFC tag with a mobile device. Enhancing the user experience, Splunk AR overlays live, augmented reality gauges onto real-world objects.

Splunk Use Case: Comprehensive Infrastructure and Operations Monitoring

When IT systems fail, organizations can lose not just money, but customers and reputation. Splunk helps IT reduce failures by proactively monitoring across IT silos to:

- Ensure uptime
- Rapidly pinpoint and resolve problems
- Identify infrastructure service relationships
- Establish baselines and report on internal SLAs or those of service providers

Delivering a comprehensive view of IT infrastructure, the Splunk platform unifies and correlates logs and metrics to provide an integrated experience for monitoring, troubleshooting and alerting.

Automated incident management with Splunk VictorOps® integrates metrics, logs and your monitoring toolset into a single source of truth so that on-call teams can quickly fix problems. Teams can collaborate via chat integrations and alert routing through mobile and web interfaces, and post-incident reports help teams constantly improve performance and reduce outages.

A powerful platform today, evolving tomorrow

A platform that brings data to every decision and action is a considerable step beyond the more focused solutions and point products many organizations rely on today. There are benefits to this true platform approach, as well as a singular need. Start with three essential benefits:

Scale: A data-to-everything platform must scale and evolve. Rapid and unpredictable change is a hallmark of the new data landscape, and a solution that cannot deliver creative flexibility is no solution at all.

The Splunk platform lets you scale your installation — from a single commodity Windows, Linux or Unix server, to the largest multi-geography, multi-datacenter or cloud-based infrastructure indexing hundreds of terabytes of data per day. You can scale Splunk horizontally and vertically by simply adding more computing power. You can run a distributed configuration on different physical servers, a combination of virtual and non-virtual servers, or on a large multicore, multiprocessor machine. Balance workloads by configuring multiple indexers and search engines across your configuration. Search head clustering enables additional concurrent searches and reduces total cost of ownership by eliminating the need for NFS storage requirements.

Flexibility: Silos are the enemy of enterprise-wide visibility, and the insights it can bring. Reflecting today's distributed, virtualized and cloud-native environments, the Splunk platform lets you search, monitor and analyze all your data from every device and every application, whether on-premises, virtual or in the cloud. For instance, Splunk Enterprise Cloud delivers powerful platform features as a cloud service. The Splunk Enterprise AMI is available for Amazon Web Services (AWS) environments. On the operations end, Splunk Business Flow provides continuous transparency into end-to-end business processes to identify opportunities for improvement or to minimize deviations from performance expectations. Finding and fixing problems, following the trail of an attacker, tracing transactions and gaining new efficiencies from your organization's vast array of data is suddenly faster and easier — by orders of magnitude.

Reliability: Availability and security are not usually discussed as primary features, but they're absolutely essential underpinnings. Data integrity and availability provide greater protection against data loss, and maintain productivity and the ability to work at market speed because your data is available when you need it. To keep your data secure, Splunk supports advanced anonymization, masking confidential data from results. Private consumer, healthcare or corporate information requires secure access, transport and storage. Encrypted access to data streams, using protocols such as TCP/SSL, is vital for ensuring data security. User access should also be secured using protocols such as HTTPS or SSH for command-line access. Further, Splunk has developed a vast community of passionate, knowledgeable partners and experts who make it easier and faster to get started and to focus on business outcomes.

Splunk Use Case: Predictive Analytics for Industrial Management

Industrial organizations are increasingly looking at IoT and machine data to better monitor operations and predict maintenance needs. But disparate data and the lack of a consolidated, real-time view force a frustratingly reactive approach. Data can come in many forms — an alarm or alert, a work order or a critical event — and can be missed without a consolidated view, costing millions of dollars in revenue from unscheduled downtime, poor operator productivity and bad quality.

Splunk for Industrial IoT delivers real-time predictive analytics, letting organizations proactively optimize operations and improve performance. The Splunk platform collects, analyzes and visualizes real-time and historical data from any source — including sensors, OT connected assets and products — to create a simple real-time view of complex industrial data.

And finally, there's an essential, future-facing need to bring all our data into a single platform that lets us ask any question, any time: *You just don't know what you just don't know*. It's one thing to get the same reports and dashboards faster, and with better data. But the kind of innovation that transforms businesses and disrupts industries comes from unexpected moves — insights drawn not from the key dashboard that's built out of a legacy spreadsheet, but from new combinations of data, providing new answers to previously unasked questions. It's how you enable collaboration across departments, drawing from diverse perspectives to solve challenges and uncover opportunities. That is how you find new customer segments and conceive entirely new product and service offerings. That's how you suddenly understand social sentiment or supply chain efficiencies and make next-level leaps, rather than incremental advancements.

Accelerating into the data-driven future

Where data was once a side effect of early digital processes, it's now the core asset of any organization. Where it once manifested as a primitive, reactive dashboard cataloging lagging indicators, it's now the essential element for smart, fast decisions and strategic innovation. Data matters to every team in every organization, and that means data must be brought not only to every action and decision, but to every department, from IT to business units to senior leadership.

As the sheer amount of data being created rises to once unimaginable quantities, and new technologies produce novel ways to disrupt or be disrupted, every organization must evolve into a cutting-edge data business. Yet everyone, from technical users to the executive level, knows that they have value trapped in their data, and they struggle to get it out.

Splunk is the Data-to-Everything Platform. It allows every organization to more fully realize the value of its data, even as the sheer amount of data, and the speed of the digital marketplace, reach almost unimaginable levels. Insights hidden in our vast troves of data, and the technologies that uncover them, are producing new opportunities, and novel ways to disrupt and be disrupted. By bringing data to every question, decision and action, organizations can thrive in an era of digital acceleration.

Next Steps

Understanding the essential value of a Data-to-Everything Platform, you're ready to explore how Splunk helps you realize the full business and operational potential of your data to drive innovation, ensure operational excellence, and secure your data infrastructure.

Explore **our full suite of products** to find the specific starting point for your journey.

Or dive right in: **Download the free trial** and see for yourself what the Splunk platform can do for your data strategy.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

2019-Splunk-BRAND-ThePowerofaData-to-EverythingPlatform-110-WP