Troubleshoot Mission-Critical Apps

Improve visibility across data sources.

splunk>

IT operations (ITOps) teams deal with constantly changing and increasingly complex technical landscapes due to the acceleration of technical innovation and company mandates for cloud transformation and IT modernization. Sometimes they are tasked with finding and fixing issues amid an ocean of data. The ocean doesn't stay still. Storms blow in and out. Clear skies and calm days transform to rough waves and back again.

The metaphysical poet, Rumi, said: "You are not a drop in the ocean. You are the entire ocean in a drop." It's a wonderful quote about how we interpret a large and beautifully complex world. Does it relate to IT troubleshooting? Well, not exactly.

Rumi said this several centuries ago. As prescient as he was, it's doubtful that he could imagine IT, let alone the demands on siloed teams troubleshooting across multiple dashboards. But, if we consider the quote just as we would if we were looking across a seemingly infinite ocean as it disappears on the horizon, parallels emerge.

IT is responsible for monitoring, managing and troubleshooting a rapidly evolving and complex environment — including hundreds of applications, servers and virtual machines. The average enterprise runs constant streams of data in disparate forms, and IT teams must find a way to consolidate and monitor them all.

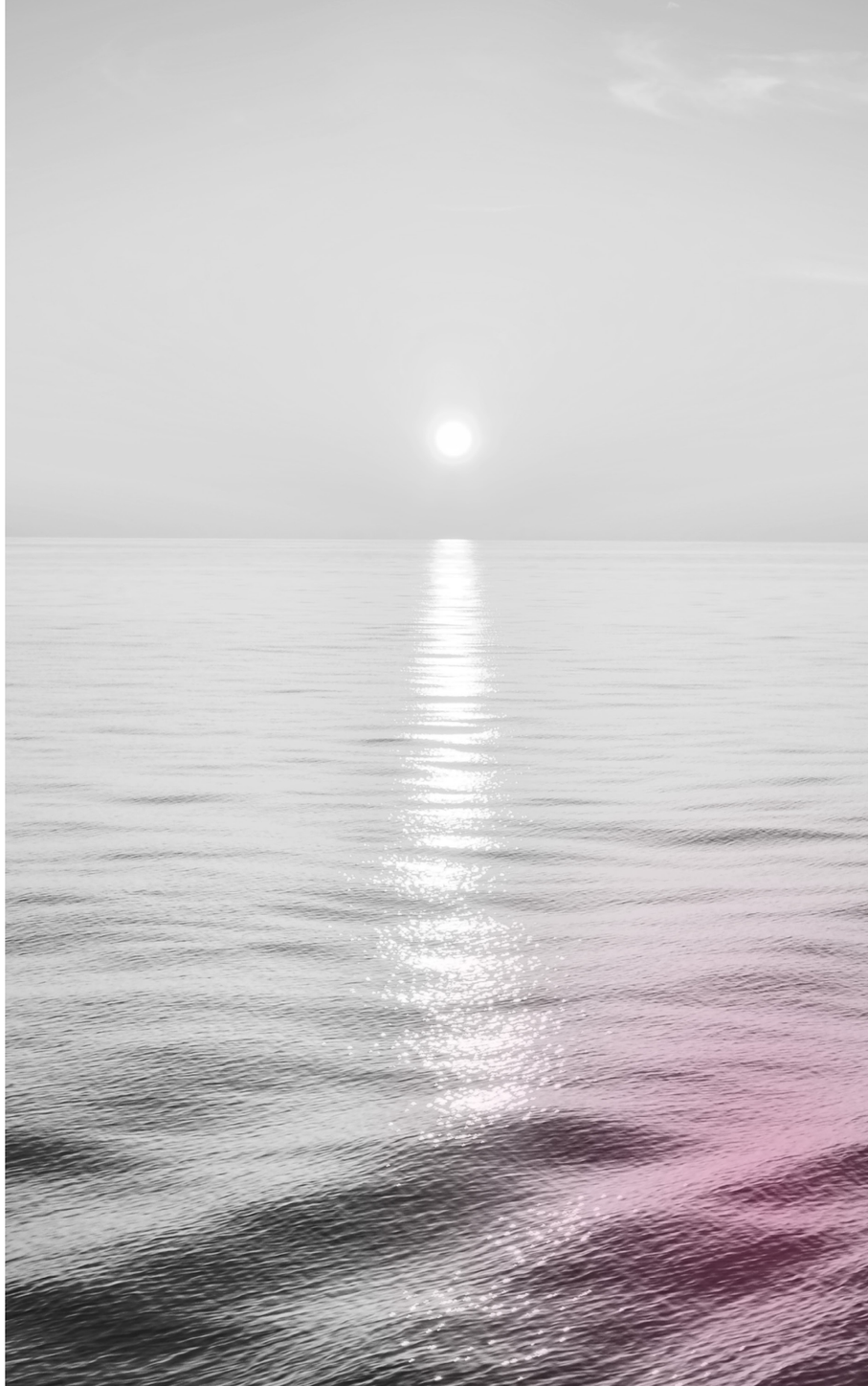
Organizations grapple with too many divergent systems and tools that create data silos, each monitoring a layer of the stack, but failing to see the system as a whole — muddying the holistic visibility required to detect and resolve an incident. Wouldn't it be great if they could distill all those terabytes of data into a single drop of water? When you gain visibility across all your systems, you gain the ability to:

- Find and fix problems faster
- Improve reliability
- Build excellent customer experiences

As over-taxed ITOps teams swivel between disparate views to conduct their analysis, time-series data like logs are seemingly infinite. New logs are generated and keep flowing, and technicians may save only a summary rollup, resulting in incomplete data. That stresses teams and puts them in firefighting mode, shuffling between too many dashboards as they frantically seek to find shelter from the storm. (Yes, that's a mixed metaphor, but it's a complex world that we all too frequently try to distill into a single line of fortune cookie wisdom.)

Complexity is *the* fundamental challenge teams must solve to succeed in the multi and hybrid cloud world.

Teams would thrive if they had the tools to concentrate their own oceans into a single drop of water. They need actionable insights in real time. Instead, they often get incomplete data sets that don't let them see all the way to the horizon.



Challenges

IT landscapes are constantly changing due to technical innovation, **cloud transformation and IT modernization initiatives**. These initiatives introduce complexity.

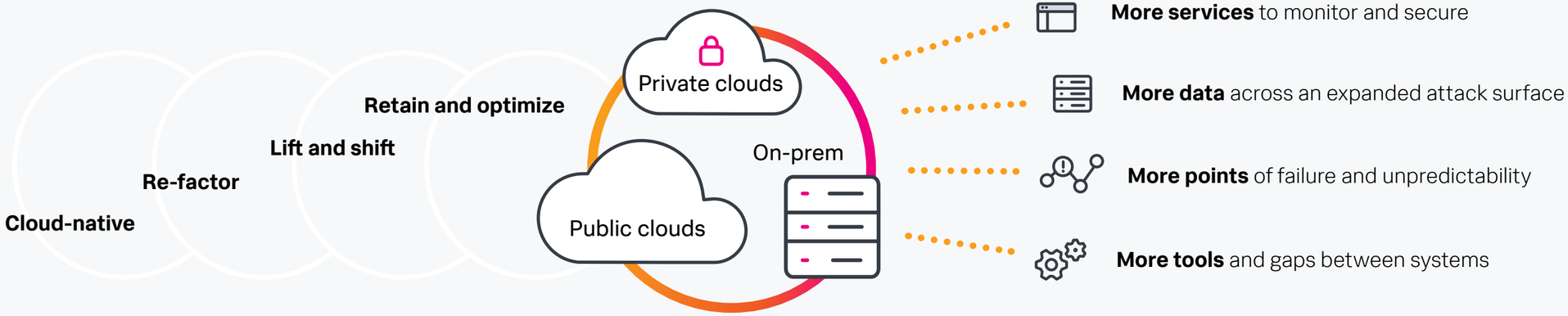
Instead of managing data centers just on premises, you now monitor an on-prem data center while also managing multiple public and private clouds.

Instead of just protecting information inside the firewall, security teams protect sensitive data flowing across an expanded attack surface outside the firewall, while also tracking different security postures, depending on the cloud provider.

Application development teams are moving towards an engineering culture with decentralized control and more complex interdependencies, causing unpredictability. There are more tools to manage these different systems (which incur cost), but gaps still persist between those systems.

IT landscapes are constantly evolving

through cloud transformation and IT modernization initiatives.



So, what are the top challenges, and what's driving the need for a renewed approach?

1. Data silos and tool sprawl

You likely have too many monitoring and management tools. Because of the complex technology landscape, siloed domain knowledge usually exists between teams that use these different types of tools. We bet more than one of these issues feels familiar to you:

- Data from different tools isn't always visible to all the teams that need to see and work with it.
- Even if the data is available, it lacks context to help your teams identify root cause and fix issues quickly.
- Data fragmentation leads to an inefficient use of data.

IT teams need consolidated tool sets that they can manage and scale with limited bandwidth and budget.

2. Lack of visibility across processes

IT and business teams both depend on data to make important business decisions. However, IT and business teams don't speak the same language when it comes to data. Often, the business doesn't understand or know how to translate what systems and application performance metrics mean in hard terms to business priorities.

IT needs to align with the business and establish KPIs that can be monitored and visualized in real time. When it comes to incident response, business service owners need to have visibility into the status of an incident or outage so they can proactively alert customers with resolution updates.

3. No proactive incident detection

Of course, preventing incidents and unplanned downtime in the first place is a goal that every ITOps team strives for. However, getting there takes time. Most ITOps teams are still very reactive to incidents, with no predictive service analysis. Incident response processes are dated and time consuming — requiring phone trees, manual troubleshooting and war rooms. When you are slow to detect and resolve issues, you lose customers. The opportunity costs are often immeasurable.

ITOps teams need to keep up with innovation, embracing predictive analytics and AIOps capabilities to shift from reactive to proactive.

Here are common ways businesses can address all that complexity:

- **Implement automation tools:** By automating and consolidating certain IT troubleshooting tasks, businesses can reduce the time it takes to identify and resolve issues. Automation tools that reduce tool sprawl can help with tasks such as system monitoring, log analysis and issue identification.
- **Establish clear escalation paths:** When IT issues arise, it's important to have a clear process in place for escalating the issue to the appropriate team members or departments. Businesses can reduce the time it takes to get the right people involved in resolving the issue.
- **Foster collaboration:** Collaboration between IT teams and other departments within the business can accelerate IT troubleshooting. By encouraging collaboration, businesses can channel the expertise of multiple teams and individuals to quickly identify and resolve issues. This can also help to prevent future issues by identifying and addressing root causes.

ITOps challenges

Data silos and tool sprawl

- Data fragmentation and blind spots result in inefficient use of data
- Data inconsistencies across different tools leads to inaccurate reporting, affecting decision-making and problem resolution

Lack of visibility across data sources

- Difficult to monitor end-to-end infastructure
- Lack of correlation between events across multiple data sources
- Manual hunting for anomalous trends

Reactive vs. proactive response

- Reactive response to incidents
- Dated incident response process
- Alert fatigue

Achieving comprehensive visibility

Would you believe us if we told you there's a better way? You should. By now, we kind of know what we're talking about. And it's not just 13th-century poetry.

You see, most organizations rely on disjointed tools to patch together a picture of what's going on across their environment. There may be one tool for each cloud and on-prem deployment, several for each layer of the technology stack and a smattering for different business processes.

Organizations should aim to provide holistic visibility of their machine data, logs and events, regardless of the source. Too often, organizations fall short of holistic visibility.

There are multiple ways to arrive at incomplete data. For example, let's use the tool sprawl issue described above.

- You might have ten tools, and it takes work to assign metrics to all of them.
- You have to keep each of those data telemetry flows coming in.
- Your other monitoring tools cannot handle the volume of data you are trying to monitor, so you have to look at samples of the data. (This is called sampling.)

Let's say you look at every 10th log report, or summarize the long form logs into short form KPIs. Or maybe you have each tool monitored by its own monitoring system, but no way to see across all ten tools' monitor dashboards. That's no way to see the ocean in a single, crystal-clear drop.

We've highlighted a handful of reasons for incomplete data. It could be any of them, or it might be that you're simply not monitoring all of your logs. The result is a valiant, yet failed, attempt at gaining the visibility teams need to find and fix issues fast. What you should aim to do is prevent disruptions from happening in the first place. Yes, the goal is to avoid downtime, but in our current environment, slow is the new down.

ITOps teams often tackle data sprawl that is driven by digital transformation initiatives. They are tasked with bringing together data from across their organization's hybrid or multi-cloud technology estate at scale. Data should be stored at full fidelity, which allows customers to analyze current and historical incidents. Splunk Enterprise and Splunk Cloud Platform helps ITOps teams to analyze and optimize cloud usage and spend by reporting on infrastructure usage and provisioning. IT teams need comprehensive visibility across all of their data — that's our drop of the ocean, and it's unfathomably powerful.

What you should aim to do is prevent disruptions from happening in the first place. In our current environment, slow is the new down.

The key to digital resilience

Organizations need to build digital resilience — keeping their systems secure and reliable in the face of digital disruptions — or they jeopardize the ability to accomplish their missions.

There are three common challenges that can get in the way of being digitally resilient.

1. Complexity increases risk

To keep up with the rapid pace of change, most large organizations now have sprawling interdependent hybrid and multi-cloud technology stacks that often rely on third-party services. These complex systems have more points of failure and larger attack surfaces that threat actors can exploit.

2. Siloed tools and teams impede detection and response

Many IT and security issues start out looking the same way — a service is down or degraded. When a security analyst, IT analyst and an engineer need to work together, they are often frustrated by the inability to work off the same data or use the same searches or playbooks. Because of the point solutions that most teams employ — which take just a slice of data and only work for specific functions — it's cumbersome to work both within and across teams to identify and remediate the root cause. Disparate tools simply don't work well together given their distinct schemas, query languages and workflows for detection, investigation and response. Without a shared understanding of the data and the ability to collaborate and prioritize, teams can't effectively spot and solve problems and ultimately deliver the best experiences to their customers.

This challenge is further exacerbated by the hybrid cloud reality, and the number, type and complexity of incidents increases. The result is not only slower and less effective response, but also a decreased ability to prioritize incidents with the highest business impact. It's no wonder the average organization suffers from 10 whole days of unplanned downtime per year to their critical services, with an average reported cost of $87 million.[1]

3. Organizations need to shift from reactivity to proactivity

It's crucial to get ahead of issues before they happen to be truly digitally resilient. Disruptions have the potential to shut down mission-critical systems and bring business to a halt, and waiting to respond until these disruptions happen is not an effective strategy. However, empowering teams to be proactive is challenging amid the ongoing skills gap and continued pressure to do more with less. With teams in reactive "fire-fighting" mode, they're not able to move quickly — and, crucially, adapt to changing conditions. This reality leads to a vicious cycle that threatens system reliability and security.

To build digital resilience, the concept can't be an afterthought. SecOps, ITOps and engineering teams need to work together to detect and predict issues, find root causes, assess risk and impact radius, and remediate quickly, accurately and at scale. Truly resilient organizations don't just deal with problems when they inevitably arise. They build security and IT guardrails into their engineering processes from the start.

All your teams can get end-to-end visibility of your machine data, logs and events, with context, for every interaction and business process — regardless of the source. With one single source of truth, teams can:

- Get holistic visibility of the organization's machine data, logs and events, regardless of the source.
- Accelerate mean time to detection, investigation and response.
- Support operational resilience mandates and initiatives while keeping customers' production environments secure.
- Optimize resources with informed, data-driven decision-making, while reducing manual and time-consuming tasks.

The journey begins by centralizing visibility of structured and unstructured logs data — all of it. By bringing data together from across your organization's hybrid or multi-cloud technology estate, teams can tackle data sprawl, analyze current and historical events, and analyze and optimize cloud usage and spend.

1 Digital Resilience Pays Off, Splunk sponsored research published on 2/21/23

How does a unified platform help?

A unified security and observability platform routes, filters, masks, enriches and transforms incoming data. Teams eliminate data silos by bringing together data from across their entire technology landscape.

Splunk's Unified Security and Observability Platform enables SecOps, ITOps and engineering teams to ensure that their mission-critical digital systems stay secure and reliable. With Splunk, teams can quickly and accurately identify the root cause, determine the impact radius and prioritize incidents for response. Splunk brings together a valuable combination of capabilities that enable these teams to detect, investigate and respond to incidents quickly at scale, working individually or across teams, seamlessly. Splunk delivers the combination of:

- **Security and observability on a shared data platform:** A shared view of data, with common query language and tooling simplifies cross-team collaboration enabling teams to rapidly detect, investigate and respond to incidents, and build digital resilience.
- **Hybrid, scalable, and interoperable:** For large enterprises, having a vast, complex and interconnected technology stack spread across on-prem and multiple clouds is the reality. Over the years, new technology is layered on top of legacy technology, creating a long tail of critical assets. Adding to the complexity is the need for geo-collocation, driven by legal or organizational mandates. Splunk works seamlessly to make this a reality — supporting both cloud and on-prem work loads, enabling search across modern and legacy architecture. Splunk is data source agnostic and works with your multi-vendor tools, across generations of technologies. The world's largest organizations rely on Splunk for their mission-critical operations, demonstrating the unparalleled scale our technology can handle.
- **Comprehensive visibility across environments:** Splunk provides an end-to-end view of digital systems — including third-party and custom software — across on-prem, public and private cloud, and the edge. We do this with business context and without data sampling. This enables SecOps, ITOps and Engineering teams to easily access and visualize data and dependencies across their entire technology stacks, simplifying incident analysis.
- **Rapid detection, investigation and response:** Splunk has pioneered — and been the consistent leader in — helping organizations pinpoint the root cause of incidents, at nearly any scale. Our valuable investigative approach helps organizations rapidly and proactively monitor and detect issues. When incidents require human-led response, Splunk provides advanced, AI/ML guided troubleshooting that tells teams which alerts are critical, where to look, and how things could be impacted downstream. This increases overall productivity by reducing alert fatigue and guesswork while minimizing the need for costly war rooms to troubleshoot and resolve issues. With Splunk's built-in automation and orchestration capabilities, organizations can automatically respond to many incidents without human intervention. This frees analysts from repetitive tasks and helps teams scale up quickly, empowering them to respond effectively when time is of the essence. Splunk also helps simplify human-led response by connecting the right people and teams to all the relevant information, providing guidance on how to resolve. This reduces churn and shortens time to respond.
- **Simplified collaboration within and across teams:** When teams need to work together, shared data visibility makes it easier to detect, understand and prioritize incidents by business value. A common query language and visualization tools help SecOps, ITOps and engineering teams build on each other's work, and protects against "lost in translation" problems. With better collaboration between teams and greater situational awareness when issues occur, organizations can optimize usage of precious people resources while minimizing disruptions and downtime.

The reality is that most organizations rely on disjointed tools — not just across teams, but also for each cloud and on-prem deployment, different layers of the technology stack, not to mention different business processes. This, combined with the increasing complexity inherent in the modern technology landscape, leads to swivel chair operations for security and monitoring.

With OpenTelemetry, you benefit from open source data collection, so you can avoid vendor lock-in and maintain full control of your data.

Customer success stories

Organizations use Splunk for their complex technology hybrid landscapes. They must achieve visibility across their entire digital ecosystem in order to avoid downtime and to stay resilient — proactively addressing issues before customers are affected.

The companies featured in this section use Splunk to build resilience across all their digital systems, making them lighter on their feet and a step ahead of disruptions. With Splunk, these organizations can predict and prevent major outages and transform their businesses.

These customers go beyond simple monitoring — they are industry leaders that use the Splunk platform to integrate continuous monitoring, predictive issue detection, and intelligent web, API and mobile optimization into their observability practices.

Puma

Key challenges

PUMA lacked insight into customer orders on its e-commerce websites, which led to poor customer experience and missed sales opportunities.

Key results

With Splunk Cloud Platform, PUMA now monitors events as they happen, performs quick investigations and rectifies problems before they prevent customers from making purchases online.

Splunk saves PUMA time and makes more money for the company. Since its busiest regions earn tens of thousands of dollars in sales per hour on their e-commerce sites, any delay in detecting and fixing order failures quickly adds up.

An unresponsive inventory system, for example, cost PUMA $108,000 in lost sales when it prevented customers from making purchases. The system is queried as part of each order to ensure available stock. When it failed, it cost PUMA both revenue and hard-earned customer goodwill.

"Now, with Splunk, we would see right away what's causing that inventory issue, and we could fix the problem so customers could continue to buy merchandise," Gaskin says. "Before using Splunk, we had no visibility into our e-commerce activity at this granular level. We had to wait until a customer or someone on our content team noticed it and complained about it. By that time, we'd already lost money and frustrated customers."

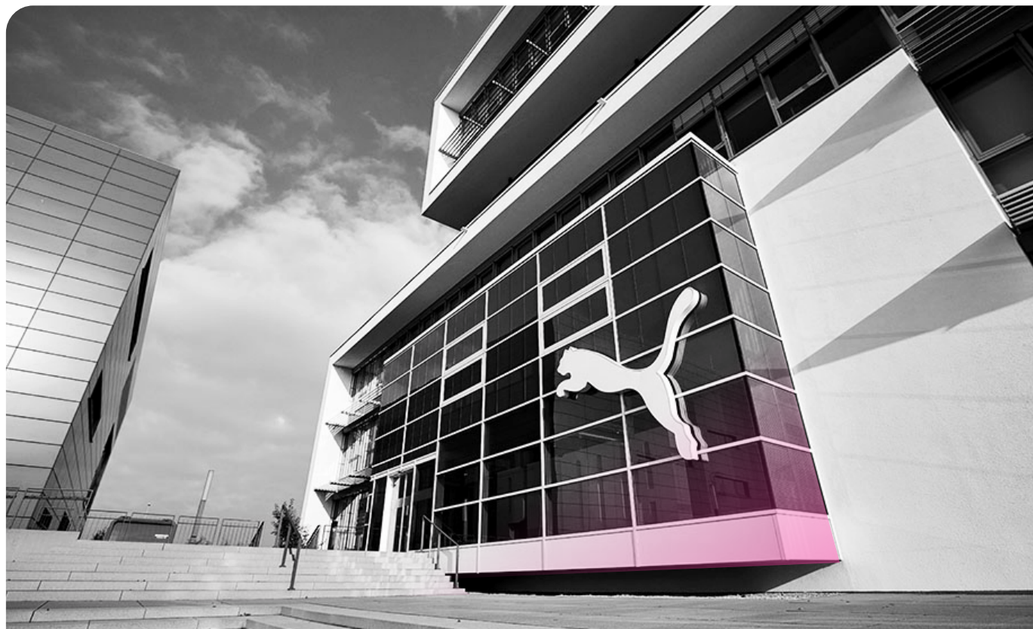
We've decreased our average time to detect issues to 15 minutes with AIOPS and Splunk, compared to hours previously. And because we also know exactly where the issue lies, we can escalate and fix the issue quickly and effectively.

Michael Gaskin, Senior DevOps Manager for Global E-Commerce, PUMA

45
worldwide PUMA.com sites with enhanced monitoring

$10k+
per hour in boosted revenue

15min
to detect order issues, compared to hours previously



Heineken

Key challenges

To keep everything across brewing, supply chain and financial processes running smoothly around the clock, Heineken needed granular visibility into its expansive systems.

Key results

With the real-time visibility that Splunk provides, Heineken has increased uptime for its foundational integration platforms and drastically reduced operational issues — ensuring quality beer is delivered whenever, wherever customers want.

Heineken distributes nearly 50 billion liters of beer every year to urban metropolises and far-flung destinations worldwide, and each bottle must have the same high quality and refreshing taste. Meeting those expectations at such tremendous scale requires fine-tuned precision across all of Heineken's processes, which is why the brewer turned to Splunk for visibility into its expansive systems. Now, Heineken connects its more than 5,000 applications to translate real-time integration data into business value for teams around the world. Not only have operational incidents plummeted as a result, but Heineken is now also predicting and proactively preventing incidents in critical systems (such as the packaging line) for processes as smooth as its beer.

We're evolving to become the best-connected brewer. Splunk helps show us where things go right and wrong across markets so we have both global transparency and local responsibility.

Ronald den Elzen, Chief Digital & Technology Officer, Heineken

Improved real-time data exchange
to increase reliability for supply chain, ordering and distribution processes

Improved efficiency and performance
across 160 breweries in 117 countries

Drastically reduced operational incidents
for better uptime and seamless, 24/7 operations

Nasdaq

Key challenges

In shifting both its products and internal operations to a SaaS model over the course of 10 years, cloud pioneer Nasdaq needed a data platform to fulfill its hybrid needs.

Key benefits

With the Splunk platform, Nasdaq ensures reliability for its main trading platform and more than 3,900 Nasdaq-listed companies while releasing SaaS-based business solutions with speed and confidence.

While Nasdaq already relied on the Splunk platform for IT operations and security, the enterprise turned to Splunk to help pave the way for a successful cloud journey — while still maintaining visibility into its evolving hybrid environment.

A successful and secure
shift to a DevOps and SaaS-based operating model to quicken the speed of innovation.

Accelerated time to market
through real-time insights into how customers use Nasdaq's products and solutions.

Improved ability
to make quick, smart decisions by unifying data from disparate infrastructures, applications and operating systems.

> **Whether it's an on-prem, hybrid or cloud environment, the Splunk platform supports every type of infrastructure, data type and data structure to make disparate data available, queryable and actionable.**

Brad Peterson, Executive Vice President and CTO/CIO, Nasdaq

Domino’s

Key challenges

During peak sales times, the need for reliable systems becomes even more critical. While Domino’s faces many peak days and times throughout the year, no event demands more precision than Super Bowl Sunday, during which Domino’s sells nearly 2 million pizzas — most of which are ordered in the same 45-minute window.

Key benefits

To meet expectations on football’s biggest day, Domino’s has a war room where a wide range of teams (from IT network and infrastructure to marketing and communications) rely on Splunk to monitor key metrics like performance, system health and customer volume. By using Splunk to bring data to every question and decision, Domino’s keeps operations smooth during even the busiest of times.

Today, Domino’s dominates as the leader in global sales, thanks in large part to a data-first approach to everything from behind-the-scenes IT and security operations to daily customer interactions like ordering and delivery. To stay number one, the pizza powerhouse uses Splunk to inform decisions, drive innovation and satisfy customers’ cravings for speed, quality and convenience.

Splunk makes sure that simplicity for the customer doesn’t mean overwhelming complexity for those managing the technology. “With all the additional channels to order through, we have to be able to monitor everything from security and operational aspects to new releases and developments — and that’s all fed into Splunk,” Cox says. “Splunk helps us with every real-time transaction. We can understand what’s happening with our orders, services, website and applications. When we have all that data together, we can improve processes both internationally and domestically.”

Nearly every team at Domino’s uses Splunk in some way. They don’t want to see whether a single component is healthy — they want to see the whole picture integrated with sales data, revenue and more. That way they can see the impact their decisions have on the whole business.

Mike Cox, Operational Intelligence Architect, Domino’s

On Super Bowl Sunday,
Domino’s sells nearly 2 million pizzas — about 40 percent more than on a normal Sunday.

1 million
pizzas sold daily in the U.S.

At Splunk, we believe there is a better way.

Splunk is built for the reality of securing, operating and innovating fast and effectively in the multi cloud and hybrid environment. Nobody wants one tool to monitor AWS, another for GCP, and still another for their on-prem infrastructure. And they don't want one tool for infrastructure, another tool for network monitoring, and another separate tool for application monitoring. That's why we provide an open, extensible data platform that supports shared data so that all teams can get end-to-end visibility, with context, for every interaction and business process. You can have consistent security and observability, from on-prem to multi-cloud to edge, on one platform. The result is that you can rapidly isolate the signal from the noise and take action fast.

Provide holistic visibility of your organization's machine data, logs and events, regardless of the source

Splunk Enterprise and Splunk Cloud Platform enables ITOps teams to tackle data sprawl that is driven by digital transformation initiatives. Our platform enables ITOps teams to bring together data from across their organization's hybrid or multi-cloud technology estate, and do it at scale. Data is stored at full fidelity which allows customers to analyze current and historical incidents. Splunk Enterprise and Splunk Cloud Platform helps ITOps teams to analyze and optimize cloud usage and spend by reporting on infrastructure usage and provisioning.

Help accelerate mean time to detection, investigation and response

By centralizing data across tools and surfacing key risks, Splunk empowers ITOps teams to streamline and standardize workflows to reduce meantime-to-detection (MTTD) and meantime-to-response (MTTR). With Splunk, ITOps teams have reduced MTTD by over 80%[2] and reduced high priority incidents by over 50%, improving IT efficiency for competitive advantage and boosting customer experiences. Splunk Enterprise and Splunk Cloud Platform enable fast and extensive issue investigation for ITOps teams through the identification of emerging issues, deep root cause analysis, and rapid incident resolution. With schema-on-the-fly and a powerful search language, Splunk allows you to quickly pinpoint incident start times, correlate across disparate data silos, and obtain the true root cause of incidents to ensure they cannot happen again. Most competitive monitoring tools only focus on basic metric and availability monitoring. Splunk goes deeper and helps ITOps teams to get proactive notification of system and application health with rich insights only found within log and event data. IT and DevOps teams can also build on Splunk's logging capabilities by reusing logs for cloud-native application and infrastructure debugging in combination with traces and metrics through Log Observer Connect.

Support operational resilience mandates and initiatives while keeping the customer's production environments secure

Splunk Enterprise and Splunk Cloud Platform give ITOps teams the data needed to safely and securely roll out and roll back changes at cloud-scale. In addition, with ~1,000 purpose-built data source integrations and 2,800+ Splunkbase apps, ITOps teams using the Splunk platform can extend value as they evolve their business. Splunk secures and reduces risk to the production environment by providing investigations and data analysis in Splunk rather than directly on production systems. ITOps teams using Splunk can easily revoke credentials from analysts who no longer need production system access, resulting in a more secure environment that is less prone to human error.

Optimize resources with informed, data-driven decision-making, while reducing manual and time-consuming tasks

The Splunk platform helps ITOps teams and executive stakeholders analyze machine data so they can understand how systems and services are performing. Splunk can help ITOps teams accomplish this understanding without a reliance on Business Intelligence (BI) or reporting teams who are often hampered by slow and brittle Extract, Transform, and Load (ETL) processing. Splunk Enterprise and Splunk Cloud's custom compliance and reporting dashboards can efficiently scale to suit any enterprise ITOps teams' demands. Splunk helps ITOps teams gain efficiencies by automating routine and time-consuming tasks, and through Splunk's custom dashboards and reports, these teams can reduce manual tasks while proactively analyzing custom scripts developed by their teams.

Federated search for S3

While data continues to grow and change exponentially, not all data is created equal — data has different formats and quality and changes with age. Additionally, cost restrictions can lead to data silos, which inhibit holistic visibility and result in inefficient use. This motivates organizations to adopt cloud object storage services to address their needs related to scalability, performance, cost efficiency, security and compliance. Splunk can now search Amazon S3, the largest cloud object storage service in the market today.

2 Customer examples include: Rappi, Vesca, Lenovo, Puma

Ready to learn more?

Find out how to protect your business and modernize your observability practice with Splunk.

Free trial

splunk>

23-397801-Splunk-Troubleshoot Mission-Critical Apps-EB-107