Path to Resilience

Building a Leading Observability Practice

How ITOps and engineering teams can use Splunk to improve their digital resilience

splunk> a cisco company

“Warp one, engage!”

The scene opens. Captain Jean Luc Picard leans forward in his oversized captain’s chair, eyes intent on the static starscape in front of him. He raises his hand as he gives the order. The stars begin to move and lengthen to dashes as light years flash by.

No, you’re not in the wrong e-book. Think of the Enterprise as, well, an enterprise: an entity reliant on a complex and distributed set of digital systems and tech stacks working in concert to ensure mission success.

The bridge of the starship Enterprise offers a stellar metaphor for an ideal observability practice. With full-stack, end-to-end visibility, Captain Picard and his crew quickly spot, understand, explain and remediate unexpected behavior across the ship’s entire environment — from vessel control to communications and tactical systems. To the delight of audiences across the show’s seven-season run, most issues are found and fixed before they turn catastrophic.

Whatever their mission, enterprises are increasingly relying on observability for greater digital resilience, avoiding blind spots, increased toil and alert storms …

- To deliver the bridesmaid dress unwrinkled and on time
- To make sure dinner arrives piping hot
- To cinch a winning Formula 1 Grand Prix

… and to boldly go where no one has gone — sorry, we had to.

50%

increased developer efficiency during incidents

RENT THE RUNWAY

90%+

faster MTTR thanks to real-time visibility with Splunk’s observability products

Rappi

100kHz

of data streamed and analyzed per second for real-time decision making

McLaren FORMULA 1 TEAM

The fault in our data

It's not the data's fault, really. It's just that there's so much of it. It can get scattered and hard to navigate. As businesses continue to modernize their digital systems, there's a lot more to monitor and react to — more ephemeral cloud architectures, more frequent software changes, more data emitted across fragmented tools and possibly worst of all, *more alerts*.

As the complexity of our digital systems expands, so does the constellation of things that could possibly go wrong. And we know that downtime is costly — businesses report an average of 240 hours of unplanned downtime per year, to the tune of a lost $87 million in revenue and productivity. For ITOps and engineering teams, the cost is comparatively high. In State of Observability, an alarming 38% of respondents noted increased turnover on their team as a direct consequence of critical issues like downtime.

With a mature observability practice, organizations have more visibility into their vast, interwoven environments and are able to achieve greater digital resilience. This means fewer outages, less latency, faster issue resolution and happier customers and employees.

Per Forrester, organizations with Splunk Observability report:

70% decrease in system outages

75% decrease in MTTR

250 hours more uptime

243% ROI

IDC

Ranked #1

in ITOps and Analytics Market Share

in SIEM Market Share

Gartner

A Leader

#1 Vendor in SIEM and ITOM HPA software market share

Gartner® Magic Quadrant™ for Security Information and Event Management

GIGAOM

A Leader

in Cloud Observability, APM, AIOps and Incident and Task Management

Quadrant Knowledge Solutions

A Leader

in Quadrant Knowledge Solutions' SPARK Matrix for Cloud Observability and ITIM Tools

Digital resilience at enterprise scale

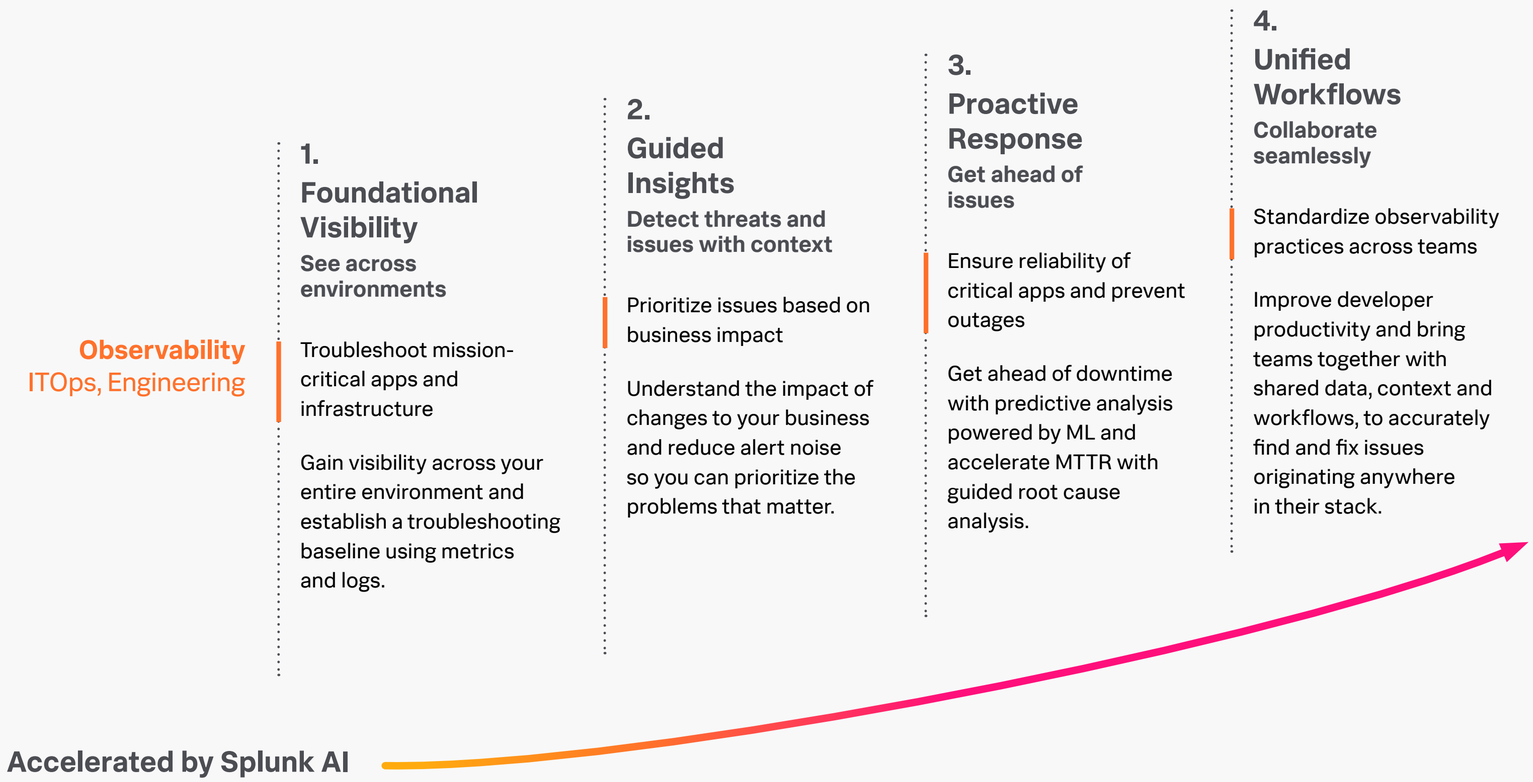
All hands on deck. It takes SecOps, ITOps and engineering teams working together to ensure digital systems are reliable, trustworthy and secure. That's why we've created a model to guide teams as they expand into new and complementary use cases across security and observability.

For ITOps and engineering teams, this journey toward greater digital resilience will help you wrangle complex environments and break down silos to gain full visibility and business context — helping you stay light years ahead of issues. Or at least find and fix the critical ones fast.

"I don't remember the last time someone has woken up over Thanksgiving to deal with an outage. Holidays used to be tumultuous from a tech perspective due to increased customer demand. Since we've upped our usage and adoption of Splunk, we haven't had a single major outage, and the last critical incident was resolved in less than 15 minutes."

— Stephanus Meiring, VP of Engineering, Rent the Runway

Build a Leading Observability Practice: Journey Stages



Make it so: Propelling the entire observability journey

The world's largest organizations rely on Splunk to help keep their digital systems secure and reliable. With Splunk's Unified Security and Observability Platform, organizations can overcome the complexities, threats and disruptions that come between them and their mission — helping them move from foundational visibility, through understanding risk and performance and getting ahead of major issues, to unified workflows that allow teams to collaborate seamlessly.

In the following pages, we'll share ways you can mature and modernize your observability practice — including check-in questions to help you self-score and determine how to most effectively allocate resources and staff.

As you embark on the journey, remember the wise words Lieutenant Commander Data shared: "The effort yields its own rewards." The most important thing is to start. The time is now, and we'll show you the way.

The Path to Digital Resilience

Unlocking key observability use cases on your resilience journey

1. Foundational visibility

See across environments

Organizations need to be able to see across their entire digital footprint to establish a troubleshooting baseline using metrics, traces and logs — and be able to quickly identify potential issues.

The problem

Today's ITOps teams are tasked with the challenge of solving problems across increasingly complex architectures, using dozens of tools to monitor different parts of their tech stack. Disconnected tools lead to data silos, blind spots and a lot of guesswork and long war room calls. The result? Costly and time-intensive investigations and slow MTTx.

The Splunk solution

Visibility is fundamental for a reason. When teams can string together different types of data from a number of different sources, they're better able to support operational resilience mandates, resolve production issues faster and more proactively, optimize resources — and ultimately make sure their organization's digital systems are reliable.

1. **Troubleshoot mission-critical apps and infrastructure:** Splunk Enterprise and Splunk Cloud Platform help teams centralize logs and apply powerful analytics so they can gain visibility across siloed log data sources. This way, they can quickly troubleshoot problems in mission-critical apps and infrastructure — detecting and resolving issues quickly and effectively to keep digital systems up and running.
2. **Optimize data management:** With robust features and capabilities like Ingest Actions and Data Management Pipeline Builders, Splunk Cloud Platform and Splunk Enterprise help teams simplify data management to ensure data is in the right shape to troubleshoot faster while maintaining cost-effectiveness and helping reduce noise. Splunk is also revolutionizing federated access to data to help ITOps get insights from data wherever it lives.
3. **Optimize hybrid application performance:** "How is X issue affecting my business outcomes and end-user experiences?" Splunk AppDynamics gives teams business context they need to focus on what matters most. It provides data deep into the technology stack, from third-party APIs, the network, and down to the code level. And with Business Performance Analytics dashboards, stakeholders from business owners to ITOps leaders can get an at-a-glance view of business health.
4. **Optimize cloud monitoring:** With Splunk Infrastructure Monitoring (part of Splunk Observability Cloud), ITOps teams managing hybrid infrastructure can troubleshoot cloud-native performance issues. By correlating real-time metrics with logs to troubleshoot faster, teams can improve MTTD/MTTR and optimize costs.

Check-in

- ☐ **Do you have to look across multiple systems to pinpoint an issue?**
  Are you able to quickly tell if an incident is a SecOps, engineering or ITOps issue, or are you spending too much time troubleshooting to get to the root cause?
- ☐ **How do you use metrics and logs today?**
  Do you struggle to make the best use of your logs across disparate tools? Do you correlate real-time metrics with logs to troubleshoot faster and improve MTTD/MTTR?
- ☐ **Do you need better tools for more visibility across systems?**
  More tools don't equal better visibility. The average organization has dozens of tools to monitor different parts of their tech stack, creating silos that result in blind spots.
- ☐ **Are you facing a constant trade-off between wanting to make the most of your telemetry but balking at the costs associated with doing so?**
  You're not alone. Organizations struggle to efficiently collect, manage, and control the exploding volumes of data they collect, manage, and store — and too many pipeline tools can make matters worse, leading to more toil and longer MTTx.
- ☐ **Can you visualize how performance improvements or degradations are affecting business outcomes?**
  Can you see how end-users interact with your applications? And how easily can you share that information with everyone who needs to stay in-the-know?
- ☐ **How do you isolate problems in your environment today?**
  Monitoring that samples data or offers a disjointed user experience can make it challenging to isolate the source of an issue.

carhartt®

Over its more than 130-year history, the Carhartt brand has become synonymous with high-quality, durable, and comfortable workwear that's attracted generations of skilled tradespeople and fashion-forward casual consumers alike. As the business now moves to more flexible, agile, and scalable cloud systems to support its exponential growth, Carhartt needs to keep systems running 24/7 without compromising service availability or performance. With Splunk AppDynamics, Carhartt teams can now proactively identify potential service issues, enhancing customers' trust in the purchasing process.

Virtually eliminated costly service or application downtime, avoiding millions of dollars in lost revenue

AppDynamics is the only solution to offer visibility into every corner of our environment and identify areas of weakness and opportunity.

— Tim Masey, Vice President, IT Infrastructure & Security, Carhartt

2. Guided insights

Detect threats and issues with context

With deep visibility and context into the health and performance of all IT assets and entities, teams can reduce alert noise and prioritize issues based on business impact — sparing teams a lot of unnecessary false leads and toil.

The problem

Every alert, everywhere, all at once. ITOps and engineering teams often investigate incidents in a vacuum, where duplicate and irrelevant alerts make it hard to triage and respond, understand how incidents are impacting the business and, critically, can lead to staff burnout, quickly.

The Splunk solution

With a single live view of all your critical IT assets, entities and applications, your ITOps teams have the context to assess service health and troubleshoot problems more efficiently. Also, your site reliability engineers can identify the impact of planned and unplanned changes to their environment, recognizing what could be a problem before it actually turns into one. By effectively tracking MTTD, MTTR and other important SLOs and KPIs, your teams will be able to improve costs and the end user experience.

1. **Reduce alert noise:** With intelligent event correlation across multiple tools and Adaptive Thresholding, both features in Splunk ITSI, ITOps teams can reduce alert noise, isolate and prioritize actionable events, and accelerate use case analysis.
2. **Debug problems in microservices:** With Splunk Observability Cloud, engineers can quickly find and fix problems resulting from planned and unplanned changes in their microservice-based apps. Log Observer Connect provides the teams with all their logs from Splunk Enterprise or Splunk Cloud, alongside their real-time metrics and traces for full-contextual analysis. This way, teams get the full picture of what's happening, who's experiencing issues, and why and how it's impacting their business.

Check-in

- ☐ **Can you guess at how many/what percentage of alerts each day are non-actionable?**
  Understanding how much time your team is spending on going through non-actionable alerts is a critical first step. If less than 60% of alerts are important, there's room for improvement.
- ☐ **Do you have any form of correlation in place to group and prioritize alerts?**
  Your team could benefit from having all their events — enriched with relevant context — in one place without jumping between tools.
- ☐ **How many people are required to resolve issues today?**
  You know the saying: Two's company, three's a crowd. An explosion of dependencies in cloud-native environments means no single engineer has the ability to contextualize and resolve an issue. As a result, more people are required when an issue occurs, increasing overhead costs and reducing the amount of time building new code.
- ☐ **How do you currently get an understanding of the business impact that performance issues have across your microservice-based apps?**
  Lengthy and complicated debugging processes put stress on engineers and increase costs by making teams send log data to multiple vendors.
- ☐ **Do your engineers have all the telemetry data they need in one place?**
  Your developers need telemetry data to debug issues in their services. If they have all the relevant metrics, traces, and logs on one dashboard, they can optimize performance.

Care.com®

With a vision to centralize monitoring, Care.com needed an observability solution that could provide granular visibility to refactor its monolithic architecture into microservices. Now with Splunk, Care.com understands its entire environment to find and fix errors faster, improve application architecture and accelerate feature releases.

More than 80% faster issue resolution

I don't think we would have been able to release our features without Splunk APM because we wouldn't have had the ability to see if the product was working and troubleshoot any unforeseen issues.

— Sean Schade, Principal Architect, Care.com

3. Proactive response

Get ahead of issues

With predictive analysis and guided root cause analysis, teams can move from being reactive to proactive and ensure the reliability of critical apps, accelerating MTTR and ensuring exceptional customer experiences.

The problem

All too often ITOps and engineering teams are the last to know when something goes wrong with a critical app. By the time the angry tweets and irate customers start calling in, it's too late. You customers will immediately look for another alternative, and that's just simply not good. Without the ability to stay ahead of your apps' performance and intimately know what your customers are experiencing through every step of their user journey, by the time you find out about an issue, it can be too late to repair the damage to your brand's reputation and revenue.

The Splunk solution

In an ideal world, your team would be able to prevent incidents from becoming outages that impact your customers' experience — and your brand's reputation and bottom line. With an enterprise-grade platform that helps teams operate efficiently and within budget, engineers can easily scale, manage their workloads, and share best practices so they can improve MTTR and ensure consistent, optimal user experience.

1. **Improve end-user experiences:** With Splunk Observability Cloud and Splunk AppDynamics, teams with managing microservices-based or 3-tier applications get detailed front-end metrics that go beyond basic availability. They're able to measure online and network performance proactively through synthetic tests that validate the actual experience of each and every user and connect user experience to business outcomes.
2. **Detect and prioritize app security vulnerabilities:** With application security, a feature of Splunk AppDynamics, teams can collaborate more effectively with SecOps teams to quickly detect and protect against vulnerabilities and attacks while prioritizing response based on business risk.

> **We replaced our monolith with micro-services so that every outage could be more like a murder mystery.**
>
> — Cory Watson, Former Observability Lead, Stripe

Check-in

- ☐ **Are you regularly spotting and stopping incidents before your customers notice?**
  Imagine how much easier (and quieter) your job would be if you had predictive alerting and analysis to spot incidents before they happen or customers notice.
- ☐ **Are your web and mobile app users increasingly abandoning your online services?**
  Without a holistic view of how the interaction of front-end applications, third party APIs, backend performance, and the network impact the user experience, it's hard to ensure that customer experience is at the level it should be.
- ☐ **Do your front-end metrics go beyond basic availability?**
  To validate the actual experience of each and every user, you need a complete picture of end user experience.
- ☐ **Does your threat scanning solution give you business context?**
  Teams need to know where vulnerabilities and threats impact their applications, how likely a risk is to be exploited, and how much business risk each issue presents.
- ☐ **On the topic of security, are you able to automatically block threats in real time?**
  Safeguarding customer data is paramount. With runtime application security, ITOps and engineering teams can collaborate more effectively with SecOps teams to protect customers and business alike.

Resilience in action

Rappi

To keep up with skyrocketing demand for its delivery services during the pandemic, Rappi needed scalable, powerful observability tools to ensure customers could place and receive orders quickly and reliably. With the Splunk platform, Rappi meets high shopper expectations for smooth ordering via mobile apps and websites, enabling fast delivery of local goods and services to doorsteps in nine countries.

90%+ faster MTTR thanks to real-time visibility with Splunk's observability products

300% growth managed with real-time monitoring during the pandemic

We're all attuned to the potential business impact of downtime, so we're grateful that Splunk Observability helps us be proactive about reliability and resilience with end-to-end visibility into our environment.

— Jose Felipe Lopez, Engineering Manager, Rappi

4. Unified workflows

Collaborate seamlessly

Improve developer productivity and bring ITOps, engineering and SecOps together with shared data, context and workflows to accurately find and fix issues originating anywhere in their stack.

The problem

Developers just want to build things. Rigid tools that don't let teams operationalize at scale lead to low adoption, developer toil, delayed software deliveries and high costs. And since interdependencies are only becoming more complex, it can be difficult to connect the dots and make sure that business stakeholders get timely, executive-level visibility into what they care about — like revenue, shopping carts, or hospital beds, for example. The most advanced teams look for opportunities to share data with and collaborate across their security counterparts to empower that visibility.

The Splunk solution

With an enterprise-grade platform, engineering teams can easily scale, manage their workloads and share best practices so they can operate efficiently and within their budget. And with self-service observability tooling at scale, developers and SREs can spend less time managing their toolchain and more time building and delivering cool software.

1. **Align IT and business with service monitoring:** Track custom digital, non-digital and non-technical KPIs with Splunk IT Service Intelligence (ITSI) and Splunk Observability Cloud so your business stakeholders have a real-time view of what they care about on Glass Tables.
2. **Standardize observability practices across teams:** Splunk Observability Cloud is 100% OpenTelemetry-native, which allows engineers to instrument data once so they can get to building apps, regardless of scale. And with enterprise cost and access controls, teams can ensure their budget and data are both protected.

> **It used to take us days to find out about issues with a new release. Now with our custom dashboard built with Splunk Dashboard Studio, we can pinpoint and fix a problem on the same day so that customers can place orders seamlessly.**
>
> — Willie James, Director of Resiliency Services, Papa Johns

Check-in

- ☐ **How do you manage the costs and access of your monitoring tools?**
  Are there overage charges due to managing the costs of monitoring tools that prevent vital stakeholders from seeing what they care about or need to operate?
- ☐ **Are you easily able to manage access to data or create and share best practices?**
  How are you preventing accidental changes or leaks?
- ☐ **Do you use templates to streamline workflows?**
  Manually building charts, dashboards, detectors and configurations takes time and increases toil — getting in the way of being able to scale.
- ☐ **How quickly (and easily) can you manage user privileges?**
  When admins can centrally manage user privileges, they can better ensure data is safe from accidental changes or leaks. Does everyone have customizable dashboards that show the performance of what the business actually cares about?
- ☐ **How flexibly can your teams navigate emerging governance requirements?**
  Are you able to set up and monitor key metrics to identify infractions or highlight where risk is elevated beyond the norm?

PAPA JOHNS®

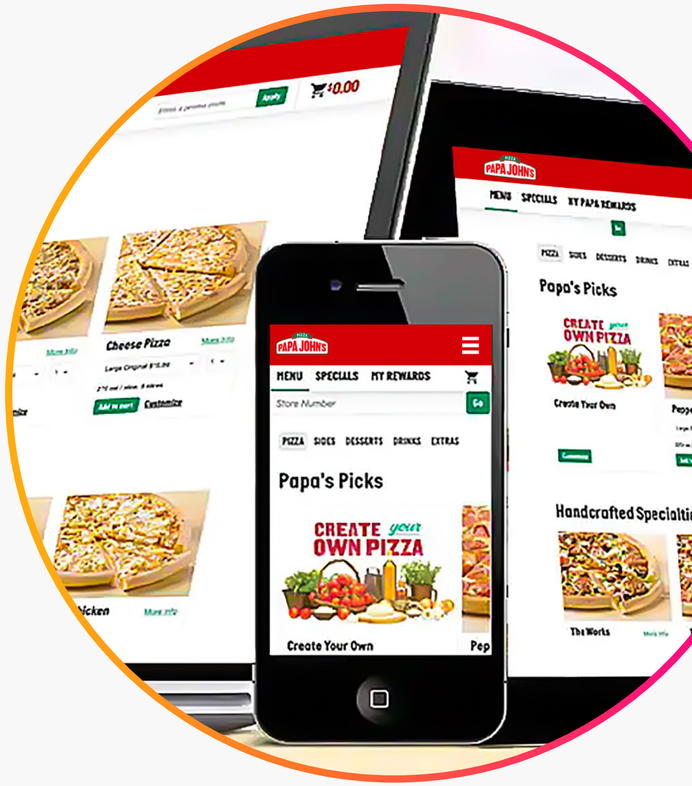
Papa Johns needed better visibility across its complex hybrid environment and operations — from interwoven technology and logistics to e-commerce channels and supply chain processes. With the visibility afforded by Splunk, Papa Johns bakes security and resilience into every process, system and architecture so that everything works together to deliver a satisfying customer experience for its millions of weekly transactions.

Gained end-to-end visibility across millions of weekly transactions and hundreds of applications

Safeguards systems and protects data for more than 26 million Papa Rewards members

Proactively identifies problems across 3,200+ stores

Improves customers' ordering experience by fixing issues in new releases within hours, versus days



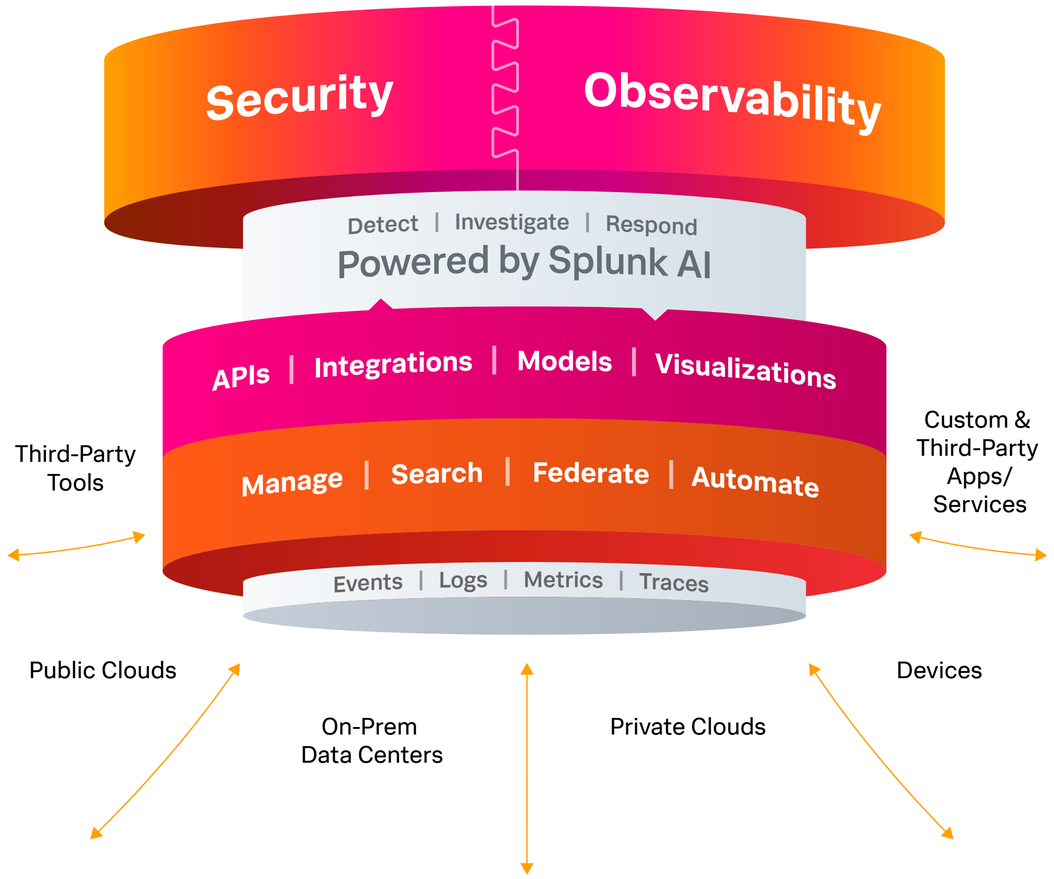
We're in the 'moment business.' When customers order, they need speed at that moment … With Splunk's observability and AIOps capabilities, we have information at our fingertips so we can react and innovate faster on behalf of our restaurants.

— Yasaswi Pulavarti, VP of Digital Engineering and Services, Papa Johns

A unified approach to digital resilience

With Splunk's Unified Security and Observability Platform, SecOps, ITOps and engineering teams have comprehensive visibility across the hybrid and edge technology landscape, as well as powerful tools for investigation and response, at scale, with the added benefit of one journey reinforcing and even accelerating the other.

You've seen how Splunk advances observability across use cases. By using Splunk for both security and observability, teams gain a shared view of data with a common search language and tooling, simplifying cross-team collaboration to drive greater digital resilience across your organization.



Solve problems in seconds with the only full-stack, analytics-powered and OpenTelemetry-native observability solution.

Start your free trial.

Keep the conversation going with Splunk.

splunk> a cisco company

25_CMP_ebook_path-to-resilience-building-a-leading-observability-practice_v2