A Roadmap to Digital Resilience for the Enterprise

Key strategies for security, IT and engineering leaders

splunk>

From downtime to thriving: Start here

You score four tickets to the concert of the decade. Checkout is a breeze. Your child settles into their seat as the pilot announces an on-time departure. Both events occur without fanfare — and that's a good thing.

Because when the opposite unfolds, the backlash is noisy, quick and costly. When downtime comes between you and your Taylor Swift ticket, the world immediately knows. When ransomware leads to system outages and a canceled flight, it can ruin your holiday — and the chances you'll use that airline again.

At a time when organizations are no longer indistinguishable from the digital systems they rely on, disruptions aren't just expensive — they can cost an organization its reputation and its loyal customer base. And crucially, each disruption comes between a team and its ability to innovate, impacting tomorrow's bottom line. It's not a matter of if something happens — it's a matter of when. Most organizations experience around 10 days of unplanned downtime per year.

That's why today's leaders are investing in digital resilience. When issues are resolved even faster — or avoided altogether — and teams have the time and tools to innovate, success is immediate and lasting. Products fly down conveyor belts and off shelves. Deliveries land on doorsteps, right on time. Flights are made. Loyal customers stay, new customers join and businesses scale.

In fact, we believe digital resilience is the defining factor of successful companies this decade.

And that's why we've created a digital resilience journey based on our experience with the world's largest and most complex organizations, combined with the expertise of some of the smartest minds in security and observability. Through each stage of the journey, you'll detect, investigate and resolve problems even faster — driving greater digital resilience across your organization, no matter the challenge.

Organizations with advanced digital resilience capabilities see major benefits

$48M annual savings on downtime costs

2x more likely to be fully prepared to adapt

2.5x more likely to report the majority of digital transformation projects as successful

Source: Digital Resilience Pays Off

Beyond silos and swivel chairs

Collaboration is key — no person (or team) is an island. But more tools, more data, lots of alerts and limited visibility across increasingly complex environments can hinder cross-functional collaboration.

In every organization, teams have shared needs and shared barriers to success. We've found these challenges to be the ones security, ITOps and engineering teams most cite as getting in the way of their work:

1

Complex environments

Legacy, multi-cloud and hybrid — oh my! When teams can't see interdependencies in their systems and how changes can impact service health or their organization's overall security posture, it can be a huge barrier to digital resilience.

2

Siloed teams and tools

When teams aren't set up to collaborate — and when they're inundated with lots of tools, alerts and data — manual, disjointed workflows can lead to a lot of "I don't knows."

3

Reactive response

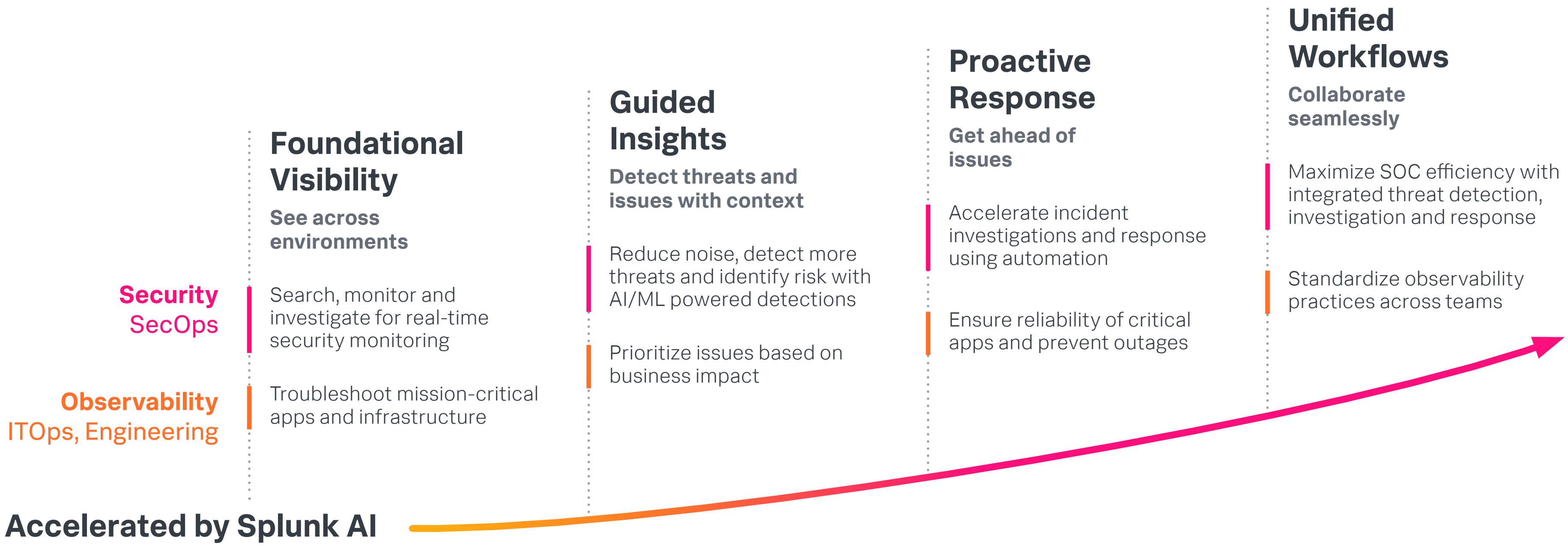
There's only so much time in a day. Understaffed teams spend their time sifting through alerts and fighting fires, with limited time and resources to prevent issues from happening.

Taking the next step

Digital resilience is a journey. But the path is far from linear. And, it can vary greatly by organization size, mission and industry. So we've created a model to help your security, ITOps and engineering teams expand into new and complementary use cases across security and observability. It'll take you from getting visibility to being more prioritized and proactive, integrating workflows in and between teams for more resilient digital infrastructures.

In the following pages, we'll walk you through four steps towards greater digital resilience. Through the journey, you'll learn how to help your teams overcome the complexities, threats and disruptions that come between you and your mission — so you can keep doing what you're doing, and keep doing it better. No matter what.

The Path to Greater Digital Resilience



Security
SecOps

Observability
ITOps, Engineering

Foundational Visibility

See across environments

Search, monitor and investigate for real-time security monitoring

Troubleshoot mission-critical apps and infrastructure

Guided Insights

Detect threats and issues with context

Reduce noise, detect more threats and identify risk with AI/ML powered detections

Prioritize issues based on business impact

Proactive Response

Get ahead of issues

Accelerate incident investigations and response using automation

Ensure reliability of critical apps and prevent outages

Unified Workflows

Collaborate seamlessly

Maximize SOC efficiency with integrated threat detection, investigation and response

Standardize observability practices across teams

Accelerated by Splunk AI

Below, we dive into the four key stages to help your organization achieve greater resilience across security, ITOps and engineering.

1 Foundational visibility

See across environments

What it is

Resilience starts with end-to-end visibility. Organizations need to be able to see across their entire digital footprint and processes at scale, so that ITOps, engineering and security teams can understand what's happening across their organizations and detect, investigate and fix problems before it's too late.

Why it matters

When you have foundational visibility, you can use your organization's data to answer questions concerning the end-to-end health and security of your IT environment. Instead of searching one application or tool at a time, you can string together different types of data from a number of different sources — quickly finding, fixing and contextualizing issues before it's too late. Foundational visibility bridges gaps across legacy, hybrid, multicloud and edge environments, so teams can understand their data, wherever it resides.

How to achieve it

To develop foundational visibility, you need to be able to ingest, normalize and index log, metric and trace data from across your infrastructure in order to quickly perform search and analysis. You should use a single platform that can process data from a range of tools, systems and applications, to better break down data silos and streamline operations.

Make sure you're also thinking about optimizing storage costs by smartly filtering and routing your data and remember that data federation is vital at this foundational stage. Ensure you can search across distributed environments from cloud to on-prem and the edge. After all, full visibility means just that: Seeing, managing and securing all your data, no matter where it's stored.

Case study: Visibility from the store to your door

Having eyes into store operations helps Papa Johns keep up with increased customer demand while empowering vital field operations.

3K+

stores monitored

> **"Splunk's sophisticated platform helps us measure the heartbeat of our system, connecting the dots between the millions of transactions going through our entire ecosystem. The end-to-end visibility into our environment via Splunk is crucial in our complex hybrid world."**
>
> Sarika Attal, VP of Enterprise Architecture and Technology Services at Papa Johns

2

Guided insights

Detect threats and issues with context

What it is

Nowadays, advanced organizations aim to empower teams with guided insights — making sure users and teams can prioritize the right things at the right times. By understanding enterprise risk and getting a live real-time view into service health, your teams can focus on issues with the most potential business impact.

Why it matters

ITOps and security practitioners' most precious resource is their time. Hundreds of daily alerts can constantly pull them in different directions, without a clear way to prioritize which ones matter the most. Knowing the magnitude or potential impact of a service degradation or threat allows teams to focus their work on the most important business services.

How to achieve it

Organizations should expand their monitoring, alerting and response capabilities to understand how threats and incidents impact business service health. IT teams can use visualizations to quickly identify high-risk events, and map components of different services to understand interdependencies. Security teams can enrich and correlate alerts with context from additional data sources so they can automate triage. With guided insights, increasingly powered by AI/ML, practitioners spend less time on non-actionable alerts and false positives.

Case study: Faster, smarter investigations and effective threat prevention

Splunk's dashboards help Check Point visualize the current state of its systems, and automated alerts notify them of any malicious activity or network vulnerabilities. The Global Chief Information Security Officer (CISO) at Check Point, Jony Fischbein, says Splunk also allows his team to quickly and effectively investigate potential harmful issues — such as developers taking source code out of the office, or a new vulnerability appearing in a product they use — before they can cause any damage.

5x

faster security investigations

> **"We now know what to investigate and whether we've solved the problem. And not just because someone has a gut feeling about it. The data shows us for certain."**
>
> Jony Fischbein, Chief Information Security Officer at Check Point

3 Proactive response

Get ahead of issues

What it means
To further build digital resilience, organizations are able to get ahead of issues and develop proactive response capabilities. These organizations have situational awareness and automation while simultaneously ensuring the reliability of consumer-facing applications.

Why it matters
The longer it takes to resolve an issue, the greater the potential impact. Organizations suffer from nearly 10 days of downtime per year, costing them an average of $87 million. Adversaries can remain undiscovered in your network with an average of nine weeks of dwell time. By becoming proactive, organizations can prevent some of these issues before customers ever notice, or before they impact the business.

How to achieve it
Teams can develop analytics using machine learning to rapidly detect advanced threats or identify patterns that can lead to latency or errors. As a result, teams are able to reinvest more time in activities like threat hunting and improving their detections, or proactively exploring their data to find other opportunities to improve.

Case study: A three-times faster response time to security events
Using real-time insights from Splunk, Carrefour now responds three times faster to security threats, making smarter decisions about preventing incidents. The team can now intervene during incidents before they cause damage to systems or affect customers. In the event of a breach, it gathers information about what went wrong so it can improve its systems in the future.

3x

faster threat response times

> **“Splunk raises the alert, opens a ticket and contacts the on-call security operations center (SOC) analyst. It’s the cornerstone of our security operations.”**
>
> Romaric Ducloux, SOC Analyst
> at Carrefour

4 Unified workflows

Collaborate seamlessly

What it means
When organizations unify workflows within and across teams, they can collaborate seamlessly — enabling them to build repeatable and automated processes for real-time insights, improved productivity and ultimately more secure, reliable digital services.

Why it matters
When workflows are spread across disjointed tools, teams can miss critical details, leading to longer time to detect, investigate and respond. Coordinating security workflows helps maximize SOC efficiency, and standardizing observability practices improves developer productivity. This is only possible with shared data and tool sets, so teams share a common language that makes them faster and more efficient. Ultimately, shared data and tooling also makes it easier for cross-team collaboration across SecOps, ITOps and engineering to troubleshoot and resolve complex issues fast.

How to achieve it
Empower teams with a unified view across all their tools that infuses insights and automation across their entire experience. Teams can orchestrate actions with playbooks that automatically triage and contain a malicious attachment from a phishing email. For developers, synthetic tests can highlight problems before the code is released, and user monitoring gives insight into the user experience along with any potential issues so that the code can be rolled back if and when needed.

Case study: 90% faster MTTR during a 300% surge in orders
Throughout the years, Rappi has risen to customers' expectations for speed and convenience — from offering reliable performance for its mobile apps and website to delivering merchandise fast, often in under 30 minutes. Rappi's mobile app development team strives to release new app versions every two weeks via a phased rollout. As each phase launches, Engineering Manager Jose Felipe Lopez's team keeps an eye out for issues, watching for any spikes in app crash rates.

90%+

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

> **"We're all attuned to the potential business impact of app errors or poor performance, so we're grateful that Splunk Observability Cloud helps us be proactive about reliability and resilience."**
>
> Jose Felipe Lopez, Engineering Manager at Rappi

Enter Splunk: The key to enterprise resilience

The world's largest organizations rely on Splunk for their mission-critical operations to ensure they keep their digital systems secure and reliable. Here's how Splunk's Unified Security and Observability Platform can help your organization on its path to greater resilience.

The security journey

Without the right strategy, security teams are flying blind. Suddenly, cyberattacks have the potential to grow into catastrophic events with serious ramifications for organizations both big and small. Even the largest, most profitable companies in the world have fallen victim to malware that might have been detected with a better, more unified solution.

But it's not all doom and gloom (we hope). To tackle threats that loom large, the answer is to become ***digitally resilient*** — the cornerstone of any organization's success and survival in the digital age. By starting ***or*** stepping up your organization's security practice and preparedness — progressing through each stage of the journey depending on their level of maturity and needs — you can better prepare for all manner of threats, attacks, compromises and other adverse events.

Armed with the right tools, capabilities and know-how, security teams are well positioned to monitor, detect and respond to events before it's too late, homing in on vulnerabilities across their security stack — mitigating risk and plugging holes before irreparable damage is done.

This is a world where threat detection and response happens faster. And where organizations become increasingly resilient as they expand into new cases — not only to better protect their business, but to also accelerate growth.

Splunk empowers the entire security journey

Foundational visibility

Search, monitor and investigate for real-time security monitoring

Get full visibility to quickly detect malicious threats in your environment. Build a foundation with Splunk Enterprise, Splunk Enterprise Security and Splunk Security Essentials for security monitoring, incident management and compliance.

Guided insights

Detect threats and issues with context

Prioritize actions with 1,400 out-of-the-box (OOTB) detections that combine threat intelligence and machine learning models with risk-based alerting (RBA) to guide analyst efforts where they're needed most.

Proactive response

Accelerate incident investigations and response using automation

Automate repetitive tasks, investigation and response to increase efficiency and productivity with Splunk SOAR.

Unified workflows

Maximize SOC efficiency with integrated threat detection, investigation and response

Seamlessly detect, investigate and respond to threats using one unified security operations experience for your SOC.

If security is Batman, then observability is Robin

By now, it should be clear that adopting digital resilience is a journey. Wherever you are on the path, Splunk has the tools to take your observability practice to the next level.

The average organization deploys dozens of tools to monitor different parts of their stack. As teams adopt disconnected tools, they face:

- Blind spots
- Increased toil
- Cascading issues

All of these factors increase the likelihood that a critical signal — like a failure, error or outage — goes unnoticed. Downtime and outages cost organizations real dollars. How many?

Way too many.

The stakes are high. According to Digital Resilience Pays Off, each hour of downtime costs about $365,000. To provide an uninterrupted customer experience, companies are forced to course correct more frequently.

But it doesn't have to be that way. Before you sing your favorite sad country song, let's suggest a better way. With a healthy observability practice, ITOps and engineering teams can lower the cost of unplanned downtime — building digital resilience holistically and organically. A robust observability practice will tell you:

1. **If there's a problem and where it's happening.**
2. **Its impact on the business.**
3. **Why it's happening.**
4. **How to fix it.**
5. **Who can fix it.**
6. **How to prevent the problem in the future.**

Now, if all of that sounds familiar, it's for a good reason. Splunk has always been in the observability business — we just didn't call it that earlier on. When you think back to why Splunk was created, it was to help ITOps teams find needles across all of their haystacks and keep their apps and infrastructure up and running. If that sounds a lot like the digital resilience journey, then you're on the right path.

Splunk empowers the entire observability journey

Foundational visibility

Troubleshoot mission-critical apps and infrastructure

Gain full fidelity visibility across your entire environment with Splunk Enterprise and Splunk Cloud Platform to understand critical services and establish a troubleshooting baseline using metrics and logs.

Guided insights

Prioritize issues based on business impact

Splunk IT Service Intelligence (ITSI) gives ITOps teams a single, live view of business service health with glass tables and service analyzers so they can prioritize actions, reduce alert noise and understand impact of changes.

Proactive response

Ensure reliability of critical apps and prevent outages

Engineers can use AutoDetect and machine learning capabilities in Observability Cloud to identify unusual changes or anomalies in infrastructure. Use Application Performance Monitoring (APM) and Infrastructure Monitoring (IM) to quickly identify hot spots. Incident intelligence routes incidents to the appropriate developers and site reliability engineers (SREs) — sending incidents to the right people at the right time.

Unified workflows

Standardize observability practices across teams

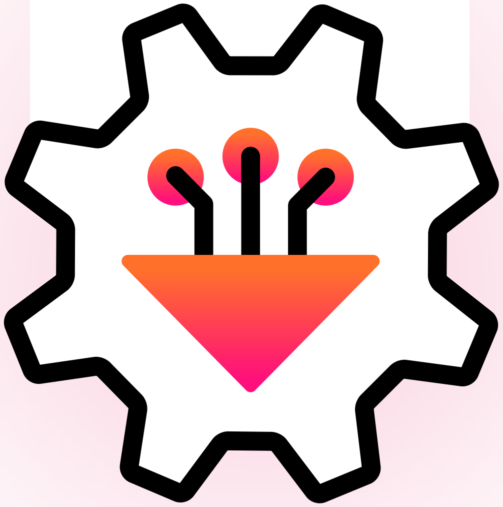
Splunk Observability helps standardize observability practices across teams, helping improve developer productivity and bring teams together with shared data, context and workflows to accurately find and fix issues originating anywhere in their stack.

Unifying the journeys

Planning and forecasting your maturity journey across security and observability often happens in a vacuum. This results in a number of inefficiencies, including data overlap, cost implications, process mishaps and more. For these reasons, organizations seeking a strategic approach to digital resilience should synchronize their efforts across security and observability. A unified platform provides 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 accelerating the other.

How does a unified platform help in the real world? Let's bring this to life. Consider a website that goes down or has significantly degraded performance. Did it go down because of malicious traffic, misconfigured API updates or a real demand spike? Without using a unified security and observability platform, it's often difficult and slow to tell. Security teams may start responding to a perceived attack only to discover that the problem should also be handled by ITOps or the engineering team.

With Splunk, security, ITOps and engineering teams get solutions built for their specific needs as well as the benefits of a unified platform. By using Splunk for both security and observability, teams gain a shared view of data. A shared view with a common search language and tooling simplifies cross-team collaboration to proactively prevent issues from becoming major disruptions, absorb shocks from digital disruptions and accelerate transformation.



Ready to learn more?

Find out how to protect your organization and modernize your **security** and **observability** practice with Splunk.

24-504250-Splunk-A Roadmap to Digital Resilience for the Enterprise-EB-116