Building Your Resilient Enterprise for AI, with AI

How AI-fueled solutions and partner ecosystems drive business transformation

splunk>
a CISCO company

Table of Contents

BACK TO TOP

Powering and protecting the AI era

Picture it: the SOC is humming. The team is focused as a new service comes online. Analysts lean into their screens as they clear tickets and scan alerts. But hidden in the stream of logs, an attacker is at work. They move faster than human eyes can track. With a single click, sensitive data is exposed. What should have been time spent on progress turns into triage.

In the AI era, triage can be faster, smarter, and more resilient, especially when fueled by quality data. Jumping in as a trusted teammate, AI quickly searches and analyzes data where it lives, connects anomalies, identifies compromised accounts, and collaborates seamlessly with your team to coordinate the right response. Analysts confirm the action, generate the incident report instantly, and return to the work that moves the business forward. That's the vision Splunk and Cisco showcased at .conf25.

Splunk and Cisco are reimagining a blueprint for digital resilience — for AI and with AI. The key lies in leveraging intelligent data fabric to unlock one of the world's most valuable yet underutilized resources: machine data. Cisco Data Fabric, powered by the Splunk platform, transforms streams of data into actionable intelligence that helps customers accelerate decision-making, reduce operational risk, and fuel innovation.

Backed by a powerful ecosystem of partners delivering AI-fueled solutions, Splunk and Cisco empower organizations so that:

- AI speeds threat detection and response, while humans stay in control.
- A secure cloud sets the foundation for safe innovation at scale where security is built in, not bolted on.
- AI-native platforms deliver the data needed to build and secure the AI era.

This e-book shows how Splunk and its partner ecosystem are building that infrastructure today — helping you turn data into defense and AI into action.

The future of resilience is here: for AI, with AI.

Section 1

Intelligent threat detection and response

DATAMINR

Outsmart the AI-powered adversary

Your adversaries have a new teammate: AI. And unfortunately, traditional threat intelligence cannot keep up. Manual monitoring, human-led validation, and delayed responses leave organizations exposed while AI-powered threat actors move at machine speed. The old “detect, validate, then respond” playbook is simply too slow for today’s reality.

The next era of cyber defense isn’t about adding more feeds or analysts. It’s about embracing real-time, actionable intelligence to drive preemptive defense. The SOC of the future is an intelligence-driven nerve center that fuses signals from across the external threat landscape with internal enterprise data, enriching context instantly — and continuously — in real time as attacks and threats evolve so security teams act swiftly and decisively.

That’s the vision behind **Dataminr**, a pioneering AI platform, and Splunk’s partnership: helping enterprises turn overwhelming streams of both external and internal security signals into trusted, actionable intelligence. Organizations get ahead of attackers by combining the risk-based alerts and advanced security detection in Splunk with Dataminr’s real-time, AI-powered intelligence platform that can surface the earliest signals of cyber events, risks, and threats from over 1 million public data sources.

It’s not about chasing every noisy alert that reduces SOC efficiency and limits your team’s ability to mount an effective response to fast-moving critical cyber threats. It’s about creating a new model where the right rich context lets your defense keep pace with the speed of AI.

38% **of CISOs surveyed said the most worrisome perceived AI threats are more automated and efficient attacks.**

Source: Splunk, The CISO Report, 2025

BACK TO TOP

Fight AI with AI

Detect and respond faster

Move from days-long validation cycles to real-time insight and rapid disruption.

Work smarter, not harder

Shift your team from triage to high-value work with smart automation.

Build a proactive defense

Use early threat signals to adapt defensive postures and preempt zero days before “Day Zero.”

DEEPWATCH

Cut the noise. Stop the threats.

Security teams today are under siege not just from adversaries, but from the endless stream of alerts their tools generate. False positives pile up, real threats hide in the noise, and overextended analysts face fatigue that leaves organizations vulnerable.

The future of effective defense isn't about collecting more data. It's about sharpening focus. High-performing security teams are rethinking detection strategy to emphasize signal quality over signal quantity — curating detections, enriching context, and applying risk scoring to concentrate human effort where it matters most.

This shift is more than a technology play. It's a cultural one: reframing SOC operations from alert clearinghouses to intelligence-driven decision centers. It's about building trust so when an alert fires, it's worth acting on.

Deepwatch, a leader in managed detection and response (MDR), has spent a decade managing and enhancing the Splunk security information and event management (SIEM) platform with custom detections to tackle this issue. Deepwatch built its Guardian MDR Platform to cut through the noise — leveraging Splunk to deliver curated detection engineering, dynamic risk scoring (DRS), and strategic insights that help customers zero in on what matters most.

47% **of security leaders surveyed cited alerting issues as a top source of inefficiency in the SOC.**

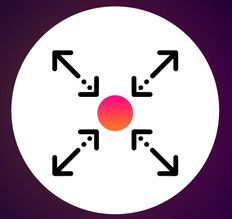
Source: Splunk, The State of Security, 2025

BACK TO TOP

Make every alert count

Turn down the volume

Reduce the noise with over 98% reduction in alert volume to free analysts for high-value work.



Detect at scale

More data doesn't have to mean more alerts. It can mean smarter, more targeted ones.

Accelerate response

Adaptive prioritization and routing accelerates threat response.

EY

Turn behavior into foresight

Security is no longer about spotting the unusual — it's about understanding the meaningful. A single failed login or odd script execution might not raise alarms, but when those signals line up across users, systems, and days, they reveal intent. And intent is where risk lives.

The problem: most security programs are still tuned for snapshots, not storylines. Alerts fire in isolation, creating noise instead of clarity. What's needed is the ability to connect fragments into a timeline — to see not just what happened but how it unfolded. That's how insider threats and living-off-the-land attacks finally come into focus.

User and entity behavior analytics (UEBA) makes this shift possible. Splunk brings the scale: unifying diverse data, surfacing behavior over time, and applying machine learning (ML) to detect patterns that traditional rules miss. **EY**, a global IT services powerhouse, brings the discipline: enriching detections with business context, tuning AI and ML models to reduce noise, and building maturity into SOC operations. Together, Splunk and EY move organizations from reactive alerts to proactive insight at enterprise scale.

The payoff is clarity. Security teams move from chasing anomalies to understanding intent. Leaders gain confidence that their teams can identify risky behavior earlier — before it becomes a business impact.

56% **report high success in using AI/ML to improve staff efficiency, specifically through correlating events and prioritizing alerts.**

Source: Splunk, State of Observability, 2024

BACK TO TOP

Clarity ahead

From noise to narrative

Risk isn't revealed in single alerts, but in patterns across time and context.

From anomalies to intent

ML and risk scoring sharpen detections, so analysts focus on what truly matters.

From overwhelmed to ROI

Fewer tickets and more focus deliver improved SOC efficiency and ROI.

RED HAT

Build resilience with self-healing security

No SOC can out-click or out-staff its way ahead of today's machine-speed threats. The path forward isn't more alerts — it's self-healing security that responds as fast as attacks unfold. Self-healing security is not just automation for automation's sake. It is a system that detects disruptions, decides on the correct response, and executes recovery before users feel the impact.

Self-healing does not remove people from the loop; it redefines their roles. Analysts apply strategy and judgment, while automation handles the noise and repetition. Intelligent detection surfaces the signals that matter, intelligent response applies them instantly and consistently. The outcome is digital resilience: fewer disruptions, lower risk exposure, and more time for teams to focus on proactive defense.

Splunk unifies data across the enterprise, enriching it with context and analytics to reveal early, correlated, and explainable signals. **Red Hat**, an open hybrid cloud technology leader, offers Ansible®, an automation platform that transforms those signals into event-driven workflows that execute with guardrails and governance.

Together, Splunk and Red Hat Ansible© form the nervous system and muscle of self-healing to close the detection-to-response loop. The result? Defense that doesn't just react but also restores itself, keeping services steady and secure.

74%

of security pros surveyed rate detection engineering as the most important future skill for the SOC.

Source: Splunk, State of Security, 2025

BACK TO TOP

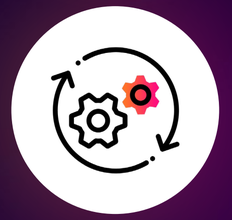
The anatomy of resilient security

Respond at machine speed

Close the gap between detection and defense to limit impact and reduce risk.

Act on trusted signals

Make data-driven decisions with unified, context-rich data.



Automate with discipline

Scale security without losing control with policy-driven workflows.

TENABLE

Close the vulnerability gap

Every organization has critical exposures in its infrastructure. In security operations, analysts must take into account the business impact and the criticality of those exposures along with the alert information. That's why reviewing every alert without this context is not just inefficient — it's counterproductive. The smarter move is to zero in on the alerts that truly put the business at risk, and that's where exposure management comes in.

Instead of treating all exposures as equal, exposure management unifies security visibility, insight, and action across the attack surface. **Tenable**, a leader in exposure management, aggregates and normalizes data from its native sensors with other tools from your security stack. Tenable's Vulnerability Priority Rating (VPR) and Asset Criticality Rating (ACR) then reveal what's been exploited in the wild and whether it's on a business-critical asset. This rich information helps SOC analysts zone in on the alerts that pose the greatest risk to the organization. That focus turns the SOC from an endless flood of alerts into a precise, measurable practice.

Splunk helps put an end to analyst fatigue with an AI-powered security platform that provides full-fidelity visibility and context from the cloud to the edge for greater threat detection. Tenable then sharpens the focus with contextual risk intelligence to surface which exposures are under attack, then ranks them accordingly. Together, Splunk and Tenable give SOC teams a ranked plan of action instead of an overwhelming backlog.

The result is security that runs at the pace of risk. Analysts can confidently prioritize, demonstrate progress, and give business leaders proof that while activity may be going up, their risk is also going down.

55% **of SOC teams surveyed say they are dealing with too many false positive alerts.**

Source: Splunk, State of Security, 2025

BACK TO TOP

Protect what matters most

Prioritize what counts

Combine exposure insights with asset criticality to zero in on true business impact.

Expose the attack path

Correlate exposures across the attack surface to reveal potential lateral movement and mitigate threats before they happen.

Speed threat detection

Improve threat detection, investigation, and response (TDIR) with comprehensive, risk-based visibility.

Section 2

A secure cloud for the AI era

ACCENTURE

Embrace AI without the complexity

Call it what it is: cloud has entered its AI era. Embracing a broader spectrum of cloud and AI capabilities injects a staggering wave of IT complexity. It is a delicate balancing act: achieving the stability of an efficient and secure hybrid IT estate while unleashing greater agility and innovation.

The answer lies in trusted context and insights. Without correlated, high-quality visibility, even advanced models risk misfires. You need a control layer where data is unified, AI is guided, and outcomes are measurable.

Accenture, a global technology consulting firm, introduces its Continuum Control Plane (CCP), which takes an agentic approach to achieve visibility. With Splunk at its core, CCP helps you integrate today's complex IT estate into a unified, AI-driven command center that delivers the visibility you need with role-based AI agents to help you surface insights and respond faster for real-time decision support.

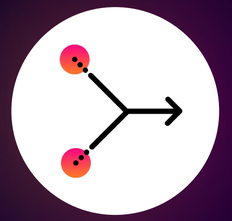
What's emerging is a model where cloud security and innovation advance not by adding more tools, but by embedding AI agents on top of trusted data to drive measurable outcomes.

59% **of security leaders have *moderately* or *significantly* boosted their efficiency with AI.**

Source: Splunk, The State of Security, 2025

BACK TO TOP

Stability and agility



Simplify governance

Embed intelligence into a unified layer and apply consistent governance at scale.

Go from reactive to proactive

Unlock insights that support predictive maintenance and automate operational tasks within Splunk security orchestration, automation, and response (SOAR).

Power agentic AI with trusted data

Give AI the full picture so its recommendations become trusted guidance.

AWS

Use zero trust for real results

Zero trust has been called everything from a buzzword to a blueprint. The principle — "never trust, always verify" — is simple. The challenge is making it work across every identity, device, network, and application without slowing your organization down.

That's why zero trust can't remain an abstract strategy. Zero trust is about outcomes: reducing the likelihood and impact of breaches, containing incidents before they spread, and enabling teams to innovate in the cloud without introducing new risks. Achieving that requires more than policies. It demands continuous verification, automated response, and a unified view across an increasingly complex digital footprint.

Forward-leaning organizations are proving it can be done with **Amazon Web Services (AWS)**, the world's most comprehensive and broadly adopted cloud. AWS provides a secure, governed cloud backbone with Splunk delivering real-time analytics and automated playbooks that operationalize trust. Instead of chasing compliance checkboxes, enterprises can build a living system of verification and response.

The AWS Landing Zone Accelerator gets organizations to a well-governed environment fast with preconfigured essentials, so security leaders don't trade speed for control. Additional ecosystem partners, such as CrowdStrike, Okta, Zscaler, and XQ Message, add strong posture, identity, and access controls, but Splunk and AWS remain at the center, unifying visibility with a secure, scalable cloud backbone.

The result? Zero trust you can actually operate day to day.

61% **of all organizations now have a defined zero trust security initiative in place, and another 35% plan to implement one within the next 18 months.**

Source: Okta, The State of Zero Trust Security 2023

BACK TO TOP

In data we trust

Simplify compliance

Meet regulatory demands while strengthening your overall posture.

Reduce risk, respond faster

Contain threats in real time with continuous monitoring and automated playbooks.

Build for the future

Modernize in the cloud with security that scales alongside innovation.

GOOGLE

Bring sovereignty and unified security together

Data's gravity favors sovereignty: the closer it stays to home, the stronger your oversight. That's why governments and enterprises are adopting sovereign and air-gapped clouds. They keep data in-country, satisfy regulators, and strengthen trust. As AI workloads scale, the need for trusted, in-region telemetry becomes even sharper.

But while these models promise sovereignty, they also introduce new operational challenges. Local environments can fragment visibility, making it harder for SOC teams and operators to connect the dots at speed. Data often stays siloed, and without internet connectivity, teams must process signals locally or risk losing the real-time context they need to stay ahead of attacks or disruptions.

The answer is embedding observability and analytics directly inside these restricted environments. Together, Splunk and **Google** make sovereignty work. Google Cloud, a leading comprehensive cloud computing service, provides the sovereign foundations — air-gapped and dedicated clouds built to keep data local and under national control. The Splunk AI-powered platform builds on top of that, delivering the real-time visibility and analytics those environments can't provide on their own, without ever touching the public internet.

Disconnected environments do not have to mean compromise. With Splunk and Google Cloud, security leaders can keep data local, stay compliant, and still operate at the speed of modern threats.

63% **of SOC leaders surveyed agree that domain-specific AI extremely or significantly enhances security operations compared to publicly available tools.**

Source: Splunk, State of Security, 2025

BACK TO TOP

Stay centered

Protect trust and revenue

Sovereign and air-gapped clouds meet regulatory demands and keep customer confidence intact.

Maintain continuity

Splunk ensures operations stay resilient with unified visibility even when networks are disconnected.

Accelerate response

Real-time insights within Google Cloud sovereign environments cut downtime and reduce risk exposure.

MICROSOFT

Accelerate security with AI

AI copilots have proven that automation can save time and reduce toil. But it's just the start. The real shift is agentic AI that understands context, proposes actions, and scales expertise. What does that mean for the SOC?

Agents can help cut through the alert noise, remove the team's burden of repetitive work, and scan for patterns at machine speed. Humans stay in command, guiding strategy, validating actions, and applying judgment where it matters most. The result is a SOC that responds faster, misses less, and focuses forward.

Together, Splunk and the **Microsoft** Azure cloud platform make it possible to power the future of agentic AI as a core layer of your defense, not a side experiment. Splunk delivers unified visibility across hybrid environments, along with equipping every analyst with AI to minimize manual effort, accelerate investigations, and respond faster using natural language queries, guided workflows, instant summaries, and automated reports. Microsoft Azure provides the scale. Azure's trusted global cloud infrastructure lets you run AI workloads as a cloud-native function — elastic and agile — to deliver digital resilience in ways no one else can.

The SOC of the future won't be measured by how many copilots it runs but by how seamlessly humans and AI work as one to accelerate security.

64%

of survyed ITOps and engineering professionals with a leading observability practice *always* or *often* use emerging AI technologies like agentic AI.

Source: Splunk, State of Observability, 2025

BACK TO TOP

Add AI to the team

Detect and act faster

Deliver the right infrastructure to power agents that help teams detect and act on threats faster.

Ignite innovation

Automation absorbs routine work, so analysts focus on higher-value investigations and strategy.

Unlock value

Fewer false positives, faster response, and streamlined compliance deliver measurable outcomes.

Section 3

AI-infused data management

BITSIO

Turn data overload into breakthroughs

Most organizations don't have a data problem — they have a data blind spot. Logs and telemetry pour in by the terabyte, but only a fraction is ever put to use. The result is wasted investment, rising storage bills, inefficient cost models, and leaders questioning whether all that data is actually making the business smarter.

The future of data-driven business won't be defined by how much information you collect — especially in the AI era. It will be defined by how well you can govern, optimize, and transform that data into insight that drives a competitive edge and empowers your AI innovation.

This isn't just a tooling challenge. It's about reframing your entire data strategy from passive collection to strategic clarity: deciding which signals matter, where insights can unlock efficiency, how to manage and govern data life cycles, and how AI can extend resilience across the enterprise.

That's where **bitsIO** — big data experts specializing in data security, observability, and analytics solutions — and Splunk step in. The Splunk platform enables end-to-end visibility from edge to cloud so you can surface actionable insights from your data. bitsIO has invested in AI-driven innovations like *datasensAI*, that light up the dark corners of enterprise. It helps customers govern data more effectively, optimize storage, and identify new high-value use cases.

Organizations can take control of unused data. bitsIO doesn't just analyze information — it empowers you to act on it. The result is accelerated modernization and resilience that anticipates disruption.

This is the future we believe in: one where every signal counts, every insight is actionable, every terabyte is optimized, and every business is equipped to thrive in a world defined by change.

90% **of enterprise data remains unstructured — a missed opportunity for governance, cost optimization, growth, innovation, and operationalization by leveraging AI.**

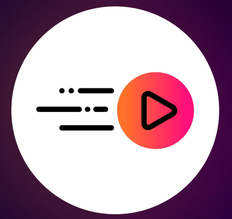
Source: TechRadar, "Transforming dark data into AI-driven business value," July 14, 2025

BACK TO TOP

It's go time

Unlock hidden data

Turn 80% of unused Splunk data into doing with AI-powered recommendations.



Migrate with speed

Shift from QRadar to Splunk faster and smarter using AI-driven use case mapping.

Automate resilience

Extend SOAR beyond security to gain efficiency and empower leaders to adapt with confidence.

GIGAMON

Eliminate blind spots with deep observability

AI-empowered security promises faster detection, smarter automation, and more resilient operations. But in reality, AI is only as good as the data it ingests. Logs and metrics can show data moved. What they can't always reveal is the nature of the data and why. And without that context, the outputs of even the most advanced models risk being incomplete, slow, or misleading.

The truth lies deeper in the network. Every anomalous connection, every expired certificate, every shadow IT device leaves a trace in the flow of traffic. But left raw, those traces are too fragmented and too overwhelming to fuel AI-powered processes with confidence. To make AI insights and actions trustworthy, enterprises must first make their network intelligence usable.

Gigamon, which offers a deep observability pipeline, partners with Splunk to make this shift possible by efficiently delivering network-derived telemetry to Splunk security and observability tools. Together, they're helping organizations move from simply collecting packets to harnessing them as a reliable, high-fidelity input for AI. The result is a new foundation of trust, where every decision is sharper, faster, and more secure.

By transforming traffic into structured, enriched telemetry, Splunk and Gigamon give AI the context it needs to separate real risk from background noise. Compliance becomes continuous rather than episodic. Mean time to resolution shrinks as insights point directly to failing systems or suspicious sessions. And leaders gain something beyond dashboards — they gain confidence that AI-driven answers are rooted in verifiable truth.

73%

of organizations surveyed say that AI has helped enhance data quality by automating repetitive tasks.

Source: Splunk, The New Rules of Data Management, 2025

BACK TO TOP

Mind the gap

Turn your network into a sensor

Passive observation of network traffic reveals critical insights about protocols, applications, and risks.

Keep compliance continuous

Map network activities to compliance frameworks, like those for the payment card industry and zero trust.

Don't miss a beat

Enriched telemetry closes the visibility gaps that traditional logs miss.

NETSCOUT

Turn packets into problem-solvers

When it comes to investigating and analyzing the root cause of service performance issues or security threats, metrics, events, logs, and traces (MELT) can show you the symptoms, but often leave gaps in visibility. However, packets — which traverse the network and capture every action and transaction — remain the ultimate source of truth. The challenge is that raw packets are noisy, requiring significant effort and resources to extract meaningful insights.

Solve this with Smart Data® — highly efficient, low-volume, curated metadata. Behind Smart Data is **NETSCOUT**, the company that large enterprises, telcos, and government agencies rely on for real-time visibility into their networks and digital infrastructure. The company uses its patented Deep Packet Inspection (DPI) technology, which transforms noisy packet data at the source into metadata, enriches MELT, and empowers Splunk's AI and automation tools to deliver deeper, real-time observability and security intelligence with confidence, in ways MELT alone cannot.

For example, a healthcare provider faced critical slowdowns when accessing electronic medical records. MELT data alone provided inconclusive results. With NETSCOUT's Smart Data enriching MELT in Splunk, the IT team uncovered the true cause: a decommissioned DNS server not sending any MELT data was still attempting to direct traffic. During the investigation, they discovered shadow IT infrastructure and rogue services. Problem detected. Problem remediated. Patients protected.

That's the power of feeding Splunk with smarter, more efficient data that enriches other data sources. Packets stop being clutter and start becoming problem-solving context for MELT. AI models sharpen. Security analytics uncover what MELT alone can't. And teams shift from reactive firefighting to proactive, and even predictive observability and a stronger security posture.

73% **of organizations that make data quality a priority say mean time to respond (MTTR) has improved.**

Source: Splunk, The New Rules of Data Management, 2025

BACK TO TOP

Proof is in the packet

Detect and resolve faster

NETSCOUT metadata in Splunk closes observability gaps and speeds mean time to knowledge (MTTK).

Identify rogue infrastructure

Asset reconciliation with NETSCOUT Smart Data ensures Splunk reflects the real environment, helping eliminate shadow IT.

Strengthen security

Combining packet-derived Smart Data with MELT accelerates investigation and delivers faster, more definitive answers.

PRESIDIO

From messy data to meaningful progress

Data is the essential fuel for an AI-powered future. But too often, organizations are stuck in neutral and that leaves them spending more time wrangling and preparing data than using it to power insights, secure environments, or build the next wave of AI innovation.

Innovative digital leaders won't succeed by collecting more data but by making existing data work harder. Without the right data served up at the right time to the right audience, business outcomes will never be met. That means eliminating the friction between raw information and actionable intelligence. And, it means building governance, accuracy, and visibility into everyday operations from the start.

Presidio, a leading global digital services provider, and Splunk work together to help organizations turn into a competitive advantage. Use your own data to unlock progress with Presidio's Atlas platform, built natively within Splunk. Atlas fuses automation, intelligence, and expert on-demand services to improve data management, optimize your Splunk environment, and deliver faster time to value. It also acts as a force multiplier for teams that need to move fast, stay accurate, and keep their focus on mission-critical work.

57% **of security leaders surveyed report losing valuable time during investigations due to gaps in their data management strategies.**

Source: Splunk, State of Security, 2025

BACK TO TOP

Take IT forward

Unlock speed to insight

Move beyond data prep bottlenecks so teams can focus on advancing AI, analytics, and security outcomes.

Build trust in data

Bake governance, accuracy, and visibility into operations — without slowing down innovation.

Scale human potential

Use automation as a multiplier, enabling leaner teams to achieve outsized impact.

CONCLUSION

Innovation starts with partnership

Partnership will shape the next era of AI. Picture a world where a powerhouse ecosystem of partners work together to build digital resilience for AI and with AI from edge to cloud. That's part of the vision shared during the Splunk .conf25 keynote. Listen to the replay to learn more.

Watch Replay Now

Want more? Watch additional highlights from .conf25.

splunk> a CISCO company

Learn more:

www.splunk.com