splunk> a CISCO company

2025

Splunk Predictions

How leaders will drive digital resilience forward

This time last year, generative AI was still fairly novel; CISOs, CIOs, and CTOs were just beginning to lead entirely new conversations with their boards about business risk and materiality; and the U.S. government had recently introduced its National Cybersecurity Strategy.

While we should continue to take stock of progress and change over the past year, I urge you to keep your gaze forward. Looking ahead and preparing for the future is the foundation of digital resilience. The most adaptable organizations harness the winds of change to propel growth and innovation. As they do, they'll rise above any predictable — or unpredictable — event that comes their way.

At the close of every year, Splunk leaders and technology experts propose business and technology predictions for the year to come. With perspectives shaped by careers in tech and countless customer conversations, our team offers advice on future trends and possible impacts for organizations to consider as part of strategic planning. This time, we're proud to include insights from Cisco's leadership as well.

Our goal is to inspire proactive and holistic thinking, from ITOps and engineering to the security operations center (SOC) and the boardroom. Data regulations continue to shift, leadership wants AI investments to deliver real business returns, and resilience is harder to achieve with an expanding hybrid, multicloud ecosystem and rapidly evolving network demands. The most successful leaders will reflect on what it all means and thoughtfully prepare to be well-positioned for every possible outcome.

Gary Steele
President, Go-to-Market, Cisco
GM, Splunk

Moving forward

There is no shortage of change on the horizon: Data regulations are a moving target. Major outages have increased scrutiny of technology vendor security and uptime. Observability is transforming from a reactive to a proactive practice. These events will reshape how executives respond to governance, plan their investments, and adapt to an expanding threat landscape. In the year ahead, business and technology leaders will collaborate more extensively in their search for pivotal solutions that drive sustainable growth, innovation, and resilience.

As organizations raced to adopt AI-driven solutions and demonstrate their business value, 2024 proved generative AI is no passing fad. “AI is pervasive in its influence,” says Splunk SVP and General Manager of Observability Patrick Lin. Splunk and Cisco leaders predict AI’s grip will only intensify next year.

But whether it’s a security, observability, or business application, AI must prove its worth. It also needs to make financial sense. For example, large language models (LLMs) run on expensive GPU servers. Next year, AI will be all about the ROI, and executives will ask themselves some tough questions.

AI won’t be the only thing shaking up businesses next year. After a turbulent 2024 in which digital disruptions impacted millions, organizations will team up with their vendors to continue building resilience. As the geopolitical landscape evolves globally, regions will de-harmonize regulation, forcing CISOs, CIOs, and general counsels to stay vigilant and agile through uncertainty. Meanwhile, ITOps and engineering teams will use observability data to influence product roadmaps.

For business and technology leaders, 2025 will require a keen sense of creativity when it comes to problem-solving. “Modeling resilient behavior and showing flexibility and openness to change is a hallmark of future-proof executive teams,” says Jeetu Patel, EVP and chief product officer at Cisco. As a result, executives will emerge from next year smarter and stronger than ever.

Modeling resilient behavior and showing flexibility and openness to change is a hallmark of future-proof executive teams.

Jeetu Patel, EVP and Chief Product Officer, Cisco

Contents

PREDICTION

Governments will finally define cybersecurity “materiality.”

Your government identification number, home address, and banking information may already be on the dark web. If you paid attention to headlines in 2024, data breaches were almost as common as the weather report. Any incident that compromises customers’ personally identifiable information (PII) would surely be considered “material” — wouldn’t it?

“Right now, no jurisdiction clearly defines materiality for cybersecurity incidents,” says Splunk CISO Michael Fanning. The current SEC definition is hazy at best: any event considered significant to an investor when making investment decisions. “As it stands, materiality is entirely subjective. It’s whatever the company deems.” As such, an unintentional infraction could put even the most well-intentioned company in hot water.

Armed with AI, cybercriminals will only increase the volume and sophistication of attacks next year, leaving organizations more liable and vulnerable. “Attackers are going to weaponize AI in ways that will be challenging to predict,” says Jeetu Patel, EVP and chief product officer at Cisco. But here’s something we *can* predict: Threat actors will launch a record number of attacks next year on critical infrastructure, the supply chain, and even governing bodies, forcing governments worldwide to define a material cybersecurity incident in clear terms.

Frank Dimina, Splunk’s SVP and general manager, Americas, acknowledges it’s time to stop the guesswork. An explicit definition of materiality will catalyze companies to enhance cybersecurity practices, such as leveraging AI in the SOC to help gather, understand, and correlate signals and better strategize for future incidents. “Governments must redefine what constitutes a material event,” he says, “understanding that it’s not just a cyber issue but a broader question of resilience.”

Dimina believes the definition of materiality should not be limited to successful attacks that cause measurable damage. Even an extended recovery period — from any disruption — should prompt penalties. “A lengthy recovery signals materiality, highlighting the need for a robust, holistic approach to digital resilience. The ultimate test lies in how quickly a company can recover.”

Defining materiality will be a welcomed regulatory change benefiting governments, businesses, and the public. By creating unified standards and guidelines, companies will better respond to incidents and build long-term security and trust. “When it comes to resilience,” says Simon Davies, Splunk’s SVP and general manager in APAC, “‘good enough’ will no longer be acceptable.”

Governments must redefine what constitutes a material event, understanding that it’s not just a cyber issue but a broader question of resilience.

Frank Dimina, SVP and General Manager, Americas, Splunk

PREDICTION

There will be no digital resilience without vendor resilience.

If 2024 taught us anything, it's that a vendor's code error or security lapse can uproot entire financial systems, halt business operations indefinitely, and sever ties to emergency services. And the problem is only expanding. Complex network architectures across more clouds and vendors make it more difficult for businesses to remain resilient.

"You have to trust not only your provider but also every provider who is *their* provider," states Will Eatherton, SVP of networking engineering at Cisco. "Today, many ITOps organizations still contend with a lack of full visibility into their own infrastructure and things within their control — let alone anything else that affects it."

According to Gretchen O'Hara, VP of worldwide channels and alliances at Splunk, these interdependencies create a domino effect across an organization's infrastructure and security. "If one piece topples — even at the very end — the whole chain can come crashing down."

Moving forward, companies will prioritize ITOps and security solutions that enable full transparency across their digital ecosystems. They'll also work hand-in-hand with vendors to align security governance and IT protocols to avoid getting caught up in a mass disruption event.

"Next year, the focus will be on business continuity if an organization loses a third-party vendor to an outage or security failure," says Splunk CISO Michael Fanning. "We'll see more strategic planning around vendor resilience than ever and more investments to ensure the business is not impacted." And since an organization's vendor vulnerabilities are now its own, they will be assessed under a more powerful microscope.

Innovations like AI-powered risk forecasting can help companies predict security threats and service disruptions. They can also develop adaptive SLAs — and more severe penalty clauses — that dynamically adjust based on real-time performance data and event urgency.

Defending business continuity is also in technology vendors' best interests, so expect these requirements to become a two-way street. Vendors may also dictate practices to customers, such as requiring stronger security measures and certain ITOps assurances. They will also attempt to align with their customers' resilience philosophy and execution. In practice, this could mean strengthening processes for reporting incidents and outages promptly and communicating real-time updates during disruptions. The bottom line: A more collaborative and communicative approach is key.

You have to trust not only your provider but also every provider who is *their* provider.

Will Eatherton, SVP of Networking Engineering, Cisco

This collaborative approach includes ensuring all parties have access to the bigger picture. “Whether it’s observability or security, it’s all about telling and understanding the full story of an incident,” says Mike Horn, SVP and general manager of security at Splunk. *“What happened? Why is this important? What do we need to do to address it?”*

To create this shared understanding, companies may enhance how they collaborate with vendors, for instance, by conducting joint risk management and response planning. Organizations could even augment their SOC staff with a managed security service provider to keep up with events and coordinate real-time responses. This way, companies have more visibility and control when working with a vendor to restore services or can quickly navigate to a fallback option in an emergency.

“How does an organization prepare for the unknown?” asks Petra Jenner, Splunk SVP and general manager in EMEA. “Well, that’s exactly what digital resilience is. Executive teams are finding new, innovative ways to safeguard it.”

PREDICTION

Student-powered SOCs will bridge public sector talent gaps.

Threats are growing exponentially, budgets and talent are not. No industry feels this pain more than the public sector.

In 2023, federal agencies reported over 32,000 cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA), an increase of 9.9% from the year prior. “Cybersecurity is a never-ending arms race,” says Frank Dimina, Splunk SVP and general manager, Americas. “Given talent shortages and the vast budget differences between the public and private sectors, governments have an even steeper hill to climb. This will have to change because they’re targeted more than anyone.”

To manage this influx of threats, governments will tap into one of our most precious resources: students.

Student-powered SOCs are a foundational pillar of the “Securing Your Future State” initiative that aims to unite state agencies, higher education, the private sector, and local communities to safeguard their state’s digital ecosystem while fostering the next generation of cybersecurity experts. Student-powered SOCs enable the public sector to address mounting security concerns head-on while lowering costs and solving the growing talent crisis — all while serving as training grounds for students, where they gain real-world experience.

Technology companies and managed service providers are training students to fill immediate cybersecurity gaps — and for the professional workplace after graduation. “Higher education provides the talent, training, and staffing at a much lower cost, while the public sector provides the digital infrastructure, data centers, and funding,” says LaLisha Hurt, Splunk industry advisor for the public sector, federal government. “This is a powerful combination that leads to a shared service that can be scaled to other local agencies.”

Although some states are beginning to build student-powered SOCs, according to Dimina, we’ll see more next year due to ever-increasing talent and budget shortages. The same goes for Europe. Although these programs aren’t widespread in the region, the trend will likely grow as skill shortages increase and organizations build stronger academic relationships. Like their professional counterparts, student-powered SOCs provide 24/7 monitoring and threat detection. They are also an additional resource during incidents, relieving some of the burden on state and local government security teams.

“What’s great about these programs is that they provide students with hands-on experience in a SOC,” says Dimina. “When you think about helping the community, municipalities can even easily expand it to job retraining for veterans right out of service — the possibilities are endless. Any way you look at it, everyone wins.”

> **Given talent shortages and the vast budget differences between the public and private sectors, governments have an even steeper hill to climb. This will have to change because they’re targeted more than anyone.**
>
> Frank Dimina, SVP and General Manager, Americas, Splunk

PREDICTION

Geopolitics will reshape data residency regulations.

Hitting moving targets isn't easy. A rise in nationalism will continue to impact cyber policies, fracturing regional regulation. Consequently, CISOs, CIOs, and general counsels will join forces to proactively address shifting compliance demands.

"Political shifts in the U.S. are also happening in Europe, which could lead to a very different regulatory landscape than we see today," says Petra Jenner, Splunk SVP and general manager in EMEA. "This could cause incremental uncertainty for many organizations. It could end up that, once again, every country has its own laws to have different controls over certain data."

For example, laws controlling data sources, storage locations, ownership, and usage could vary from country to country. "I'm concerned about the lack of willingness to harmonize regulation," Jenner adds.

Splunk's SVP of Products and Technology, Tom Casey, agrees. "Shifts towards nationalism could drive more data sovereignty requirements and regulations that are less normative for a time, particularly in Europe," he says. "So we may see a fracturing of regulation that overlaps in a non-consistent way. It will make retention policies and compliance management all the more critical."

Historically, the EU has worked hard to harmonize regulations within its borders. However, political changes in the region next year — such as a rise in right-wing populism — could force organizations operating there to be more agile with governance. "CISOs are really going to care about the regulatory aspect of where data lives, what systems are acting on that data, and what data is used to train different models," says Mike Horn, Splunk SVP and general manager of security. CISOs have the most at stake if cited for non-compliance, so they will play a key role in carrying out these plans. In this regard, they may take an inherently conservative approach, such as limiting where company data is stored.

But CISOs can't do it alone. According to Casey, CISOs and CIOs need the help of general counsels to set the organization's priorities and sponsor policies and programs that support global compliance. Moving forward, they will operate within a shared plane of existence to develop a unified risk management strategy that is comprehensive in scope with both reactive and proactive elements.

For example, expect more organizations to form cross-functional task forces to monitor regulatory shifts, assess impacts, and implement necessary changes across an organization. We'll also see technology leaders and legal counsel make joint decisions on technology investments, infrastructure, and vendors to comply with data residency requirements. They may also borrow a practice from SecOps, ITOps, and engineering teams to conduct scenario planning exercises and simulations. The most successful partnerships will leverage shared dashboards and reporting tools to stay up-to-date on compliance and respond quickly to new governance.

These practices will ensure the organization stays compliant and resilient and help it avoid hefty fines or restrictions.

Shifting regulation on data residency, privacy, and AI usage could disrupt new and existing businesses in the AI era.

Petra Jenner, SVP and General Manager in EMEA, Splunk

PREDICTION

AI exploration will give way to AI expectations.

In 2023, global AI investments reached an estimated $154 billion. Where did it all go? At least some of it went to digital assistants and dog bowls in 2024, a year in which AI was injected into just about everything — necessary or not. That's not all — according to Goldman Sachs, big tech alone is on track to shell out over $1 trillion in the coming years.

"The pressure to realize the benefits of AI today is significant, but AI infrastructure is still in its early stages," says Will Eatherton, SVP of networking engineering at Cisco. "Organizations are experimenting and adjusting their strategies every few months through trial and error."

But boards are getting anxious about ROI, and their enthusiasm is waning.

"The initial AI hype is starting to wear off as the true economics of many programs, and potentially even some pilots, is failing to deliver outcomes," says Simon Davies, Splunk SVP and general manager in APAC. Next year will be about mapping ROI to AI projects and proving value as executives stop writing blank checks and strategically fund AI investments with real results they can tout to their boards.

Tom Casey, Splunk's SVP of products and technology, agrees: "There have been a lot of exploratory projects over the last year, and now we're starting to see a shift towards much more practical ones with real targeted returns for the business."

One such practical AI use case is boosting the productivity of entry-level workers. "One of the biggest problems in security is there aren't enough skilled workers to fill SOC analyst roles," continues Casey. "AI is going to help lower the barrier to entry and effectiveness for those who are early in their careers or making job changes."

The biggest dividends may come from AI investments that improve operations, such as in the SOC to help set alerts or automatically generate run books. And AI can do much more, according to Mark Maslach, Splunk GVP of global technical sales, observability. He envisions AI driving anomaly detection and root cause analysis, as well as predicting issues and automating responses.

"One trend that will evolve next year in observability is AIOps," says Maslach. "Specifically AI in IT operations. We'll see an influx of automation." According to Splunk's State of Observability report, 52% of survey respondents already leverage AIOps within their observability toolset, while another 29% are in the deployment process. Almost half of those employing AIOps are using it for automation, determining root causes, and responding to and remediating incidents with greater intelligence.

Casey predicts companies will bake AI tools into routine workflows rather than just investing in sweeping AI platforms. "Most executives have now realized that it's more about the AI use cases and how you embed those capabilities into tools and applications," agrees Davies. "It's not a separate activity."

Whatever form factor AI takes, organizations will have to prove its worth to their boards. "Organizations are exploring use cases that leverage their own enterprise data and significantly enhance their business," says Mark Patterson, chief strategy officer at Cisco. "Across the board, executives are investing in use cases to prove models and discover ROI for their business."

> **It's the difference between a science experiment and real productization.**
>
> Hao Yang, VP of Artificial Intelligence, Splunk

PREDICTION

The future of large language models (LLMs) will be small.

You're back in college, tasked with writing a final term paper on the French Revolution for your world history course. After preliminary online research, you head to the main campus library to gather your source materials. You wouldn't leave with every book the library carries — you'd only check out a handful that pertains to the French Revolution — right?

That's how Splunk's VP of Artificial Intelligence, Hao Yang, describes the current state of LLMs. "Today's LLMs know everything. But do you really need that all the time? If you reduce the model to a reasonable size that fits your specific use case, you can reduce the cost significantly."

Enter domain-specific small language models (SLMs), which deliver unprecedented accuracy while significantly reducing operating costs and environmental impact. Even so, general-purpose LLMs will still have a home in most organizations.

According to Cisco Chief Strategy Officer Mark Patterson, organizations will pursue domain-specific SLMs next year for three key reasons: They consume less energy, don't rely on publicly available data (which is reaching its limit), and are more accurate.

"From an environmental perspective, I look at the numbers from these data centers that use tremendous amounts of energy," says Yang. "That will be a huge problem if everyone builds their business on AI and LLMs. We need to rethink these architectures."

Patterson agrees, viewing small language models as the obvious solution. "AI power consumption is predicted to increase to 1000 terawatt-hours by 2026," he says. "A shift towards smaller, more efficient models massively reduces the demands of AI models on their underlying compute infrastructure." From a cost standpoint, less energy means more savings (plus, SLMs are generally cheaper to train and deploy).

Regarding data limits, research suggests we could run out of high-quality, publicly available training data by 2026. "This is driving enterprises to seek smaller language models trained on domain-specific data sets to specialize in a particular area," continues Patterson. "The outcome of this trend is smaller, more specialized models that perform better at their assigned tasks." For example, you may build a domain-specific model that understands network configuration or can assist with automation and assurance. In this way, SLMs will better serve organizations looking to employ AI for specific applications — similar to a subject matter expert.

> **We're just beginning the next chapter of AI. The next generation of LLMs will be domain-specific.**
>
> Hao Yang, VP of Artificial Intelligence, Splunk

In our 2024 Executive Predictions report, Splunk leaders voiced concerns over the quality of LLM outputs. Since SLMs are far more accurate for any given use case, they could help reduce the risk of AI hallucinations, which occur when an LLM that powers a generative AI application produces fictitious information. “We know quality is important,” says Tom Casey, Splunk’s SVP of products and technology. “Higher efficacy models yield better results.”

However, for some use cases, organizations will still lean on LLMs to get the job done. In 2025, Casey predicts organizations will use both large and small language models. “I think corporations have to use a mix of general-purpose LLMs trained on broad data sets in the public domain and smaller language models trained on domain-centric data,” adds Casey.

In practice, companies will leverage LLMs for general knowledge queries, data analysis, and strategic planning, while SLMs are ideal for niche automation tasks, specialty security applications, and tailored content generation.

PREDICTION

Observability data will influence product roadmaps.

Monitoring today's complex application architectures is, well, complex. And the consequences can be dire if something in your environment goes wrong. According to Splunk's The Hidden Costs of Downtime report, downtime and service degradation cost the Global 2000 $400 billion annually. And that figure doesn't take into account indirect costs like lingering reputational damage. Poor digital experiences cramp consumer loyalty and public perception, costing companies much more in the long run.

To neutralize these financial consequences, ITOps and engineering teams will trace the connection between system performance issues and critical business metrics the C-suite cares about most, such as growth rate, customer conversion, and revenue. Ultimately, observability will transform from reactive troubleshooting of production issues to proactive influence of the product roadmap, advising where software developers should focus their time — driving enhanced customer experiences.

"Keeping things running is table stakes," says Splunk's SVP of Products and Technology Tom Casey. "Now, how do you show the value of the table stakes? You need to be able to map that up into something that the C-level understands."

Next year, ITOps and engineering teams will begin to measure ROI differently. "There is impact to digital experience on critical, customer-facing applications measured through revenue loss, customer satisfaction, NPS scores, and customer retention rates," says Mark Maslach, Splunk GVP of global technical sales, observability.

Patrick Lin, Splunk SVP and general manager of observability, agrees that next year, observability practices will begin to view performance through the lens of customer experience. "A few years back, most of the discussion on observability centered on the need for logs, metrics, and traces to enable log-based troubleshooting, APM, and infrastructure monitoring. Digital experience monitoring has become a core element as well. It's not just about back-end systems. It's about the actual customer experience and being able to measure that end-to-end, including the connectivity across both owned and unowned networks."

Observability initiatives built with customers in mind from the get-go allow ITOps and engineering teams to examine relationships such as how site speed impacts conversion rates and if there's a correlation between performance and user drop-off. With this context, companies will begin to leverage observability data early in the software development cycle, informing and optimizing application code and features and impacting product roadmaps — transforming observability from reactive to proactive.

Keeping things running is table stakes. Now, how do you show the value of the table stakes?

Tom Casey, SVP of Products and Technology, Splunk

AI plays a role in this transformation. Cisco EVP and Chief Product Officer Jeetu Patel believes it will help practitioners connect the dots between business risk and observability data more easily. “AI will make the notion of ‘data-driven decisions’ a reality,” he says. “Organizations don’t lack the data they need to make critical decisions; they lack the ability to make sense of it. AI changes the game with its ability to correlate and summarize data in different formats and understand relationships between data that aren’t easily discernible.” Ultimately, this will give business and technology leaders full insight into what’s really happening in their organizations.

“The ultimate goal of observability is achieving a positive end-user experience,” says Lin. Leveraging observability data early in the software development cycle will not only improve customer experience, it will help prioritize issues, align teams, drive proactivity, and make it easier to measure the ROI of observability initiatives.

“Think of it as analyzing the cost of downtime across the entire organization, at any level of granularity and in real time,” says Casey. “And — this is key — doing it in terms the business already understands.”

Expanding opportunities in the AI era

For decades, inequality has escalated between those with access to data, skills, and resources — and those without. Now, AI broadens opportunities for everyone. From correlating observability data and customer experience to helping predict security threats and service disruptions — companies, governments, students, and non-profits will all benefit from AI in the long run.

"Government-led initiatives often set the stage for industry responses," says Frank Dimina, Splunk SVP and general manager, Americas. "As AI makes accessing and understanding vast amounts of data easier, it also creates opportunities for positive outcomes on a much wider scale. With humans in the loop, AI democratizes data literacy. And data literacy is an essential element to both individual and global prosperity."

But the current workforce — and those eager to break in — need support to seize the moment.

"Reskilling and upskilling employees is a global need," says Cisco's Chief Strategy Officer Mark Patterson. "Failing to do so could result in trade and social imbalances, technological stagnation, and national security threats. Investing in a long-term roadmap for an inclusive and skilled workforce will help *all* populations participate and thrive in the AI era." We can only solve tomorrow's challenges together.

The most successful companies will proactively invest in employee training and transformation planning. "Ninety-two percent of jobs are expected to undergo some level of transformation due to advancements in AI," continues Patterson. "The work begins with identifying and enabling new skills and required training — for example, prompt engineering, AI ethics, and AI literacy."

Ultimately, easier access to data will aid the next generation of problem-solvers, yielding a more equitable, sustainable, and resilient world. "Data is not only the lifeblood driving better business outcomes," says Splunk SVP and General Manager in APAC Simon Davies. "It's the seed that transforms and catalyzes innovative solutions." Solutions like crop health monitoring, gene therapy, and wildlife preservation — all of which will change our world for the better.

As companies and the public sector strive for greater data democratization and equity in the AI era, there's one more — albeit surprising — benefit to note. "AI will make us more human again," predicts Petra Jenner, Splunk SVP and general manager in EMEA. "Think about our uniquely human skills: trust, empathy, connectedness. In an AI-driven world, these will become more relevant than ever."

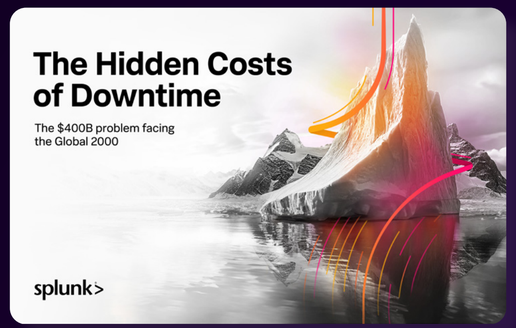
> **AI will make us more human again. Think about our uniquely human skills: trust, empathy, connectedness. In an AI-driven world, these will become more relevant than ever.**
>
> Petra Jenner, SVP and General Manager in EMEA, Splunk

Strengthen digital resilience with Splunk

Perspectives by Splunk — by leaders, for leaders

Learn how leaders tackle today's most pressing challenges, including AI, emerging threats, and the changing compliance landscape.

Read executive insights



Uncover downtime's $400B impact

Global 2000 companies lose billions annually due to digital outages or degradation. Learn how the most resilient organizations dodge financial damage.

Get the report

Contributors

Tom Casey
As Senior Vice President of Products and Technology, Tom is responsible for evolving Splunk's market-leading unified security and observability platform. With over 25 years of experience, he has held leadership positions at DocuSign, Apptio, and Microsoft. He holds a B.S. from the University of Arizona.

Simon Davies
As Senior Vice President and General Manager in APAC, Simon is responsible for the full portfolio of Splunk solutions in the Asia-Pacific and Japan markets. He is a veteran of Microsoft, Salesforce, Oracle, and Citibank.

Frank Dimina
Frank Dimina is senior vice president and general manager, Americas at Splunk, leading sales, engineering, business development, partner, and go-to-market strategies for the region, including the public sector. He has held leadership roles at Check Point, Symantec, and Riptech Inc., and has extensive experience scaling teams and leveraging data to drive customer outcomes.

Will Eatherton
Will is the senior vice president of Cisco's networking engineering team. In this role, he leads a wide-ranging group responsible for data center, web, service provider, and campus solutions. Will is also an active technology researcher, author, and speaker. His current focus includes high-performance ethernet fabrics for AI infrastructure and enabling enterprise generative AI with ethernet AI networking.

Michael Fanning
Michael is chief information security officer at Splunk, responsible for security engineering, assurance, policy, compliance, and awareness. With over 20 years of experience in the technology industry, Michael has worked in various security roles at Microsoft, Raytheon, and Symantec. Most recently, he was director of cloud security at Oracle.

Mike Horn
Mike is the senior vice president and general manager for Splunk's security business. Mike joined Splunk via the acquisition of TwinWave, where he was co-founder and CEO. Prior to that, Mike was responsible for multiple security products at Proofpoint, including Targeted Attack Protection, Threat Response, and Emerging Threat Intelligence.

LaLisha Hurt
LaLisha is a public sector industry advisor at Splunk responsible for providing thought leadership, business strategy, executive advisory support, and industry subject matter expertise to the federal government. An IT and security leader, she has served at organizations in both the public and private sectors.

Mark Maslach
Mark leads the observability technical sales team at Splunk. In his 26 years with Cisco, Mark has held senior leadership positions in direct sales, sales operations, and product management. He has a passion for incubating and scaling innovation, enabling Cisco customers to successfully navigate their digital resilience journey.

Mark Patterson
As Cisco's Chief Strategy Officer, Mark Patterson is responsible for driving the company's overall strategic direction, including acquisitions, investments, and emerging technology incubation efforts to create new markets and fuel growth. Throughout his 24 years at Cisco, Mark has held a number of functional leadership roles in finance, sales, and strategy and planning.

Petra Jenner
Petra is senior vice president and general manager in EMEA for Splunk. Previously, she held leadership roles at Salesforce, Microsoft, Check Point, and Pivotal. She holds a master's degree in business and IT and studied international management at the Stanford Graduate School of Business in Singapore.

Gretchen O'Hara
Gretchen is vice president of worldwide channels and alliances at Splunk, responsible for evolving Splunk's channel strategy and ecosystem to improve the customer and partner experience and scaling Splunk solutions to support customers operating in a distributed, hybrid, multicloud world. She has over 25 years of experience in channel sales, marketing alliances, and ecosystem development.

Gary Steele
Gary Steele is Cisco's president, go-to-market, leading a unified organization across Cisco's sales, partner, and global marketing teams to accelerate customer outcomes and drive growth across the enterprise. In addition, Gary leads Splunk at Cisco. A highly regarded technology executive and cybersecurity expert with over 30 years of experience, he has a proven track record of successfully scaling SaaS operations and growing multi-billion dollar global enterprises.

Patrick Lin
Patrick Lin is senior vice president and general manager, observability at Splunk. He joined Splunk in 2019 through the acquisition of SignalFx, where he was the chief product officer. Patrick is the former VP of product management at VMware, where he led the teams responsible for the virtual infrastructure platform.

Jeetu Patel
Jeetu Patel is Cisco's executive vice president and chief product officer. He's focused on bringing the power of the Cisco portfolio together to connect and protect every aspect of customers' businesses in the AI era. He has 20+ years of senior leadership experience driving product design, innovation, and business growth.

Hao Yang
As Vice President of Artificial Intelligence, Hao leads Splunk's team of software engineers and data scientists to accelerate the company's innovations in AI. Previously, Hao served as VP of artificial intelligence at Visa and has held several positions with globally-recognized companies including Google, Nokia, and IBM.

About Splunk

Splunk, a Cisco company, helps make organizations more digitally resilient. Leading organizations use our unified security and observability platform to keep their digital systems secure and reliable. Organizations trust Splunk to prevent infrastructure, application, and security incidents from becoming major issues, recover faster from shocks to digital systems, and adapt quickly to new opportunities.

Keep the conversation going with Splunk.

splunk> a CISCO company

24_CMP_report_predictions-2025_v12