Executive Predictions 2024

What business and technology leaders should know in the era of AI.

splunk>

The future starts now.

It’s the dawn of a new era. For some, AI is a dream come true: It empowers autonomous vehicles to drive people down bustling city streets and generates a comprehensive itinerary for their upcoming Paris vacations. For others, AI has them questioning the future of their careers.

At the end of every year, Splunk senior leadership offers predictions for the year ahead, forecasting trends and sharing insights to set business and technology leaders up for success. Splunk leaders predict that all roads lead to AI, making it crucial for executives to understand its role in the future of business.

Yes, there is a lot of hype around AI, but the technology has passed the point of no return. "We're already seeing exponential growth in terms of the value AI can unlock," says Hao Yang, Splunk VP of artificial intelligence. "There's no way you can remove it from the equation now."

"In the coming year, business leaders will be much more focused on the actual outcomes they can expect from AI," says Splunk CEO Gary Steele. "Right now, there are a lot of interesting, conceptual conversations taking place, but that will soon shift to: What can AI actually deliver for my organization — and in what timeframe?"

Splunk Chief Strategy Officer Ammar Maraqa believes that next year, people will begin to realize that AI isn't the magic they hoped for. "Although AI is a transformational technology, it's not pixie dust. It will not solve everything."

For all the buzz around AI, there will be plenty more on executives' minds next year. From sustainability to consolidating tools in a bid to simplify and manage costs, 2024 will be defined by transformation. And we'll see board priorities and C-suite roles transform dramatically too, as governments around the world pass tougher laws around data privacy, cybersecurity and digital resilience. "Organizations can't afford to be down or compromised in any way, which poses an existential risk to the business," says Tom Casey, Splunk SVP of products and technology.

Splunk research reveals that, on average, organizations experience 10 days of unplanned downtime each year. And soon, mandates will force that number down closer to zero, especially for critical services. "Globally, we're going to see a push towards a requirement for companies to report on their resilience posture beyond basic business continuity and risk management," says Casey. "Businesses will have to prove that they have the capability to respond to natural disasters, the next pandemic and regional infrastructure disruptions."

In this new era, one thing is for certain: Business and technology leaders will forge deeper relationships and work together to navigate across uncharted territory.

Contents

Prediction: AI

AI will drive valuable, incremental gains in efficiency and productivity in the short term — but business leaders will have to see it to believe it. Step changes in business impact are still 12 to 24 months out.

Here's a bold claim: AI will have as big of an impact on business as the internet. But according to CEO Gary Steele, it will take time to get there.

One day, AI-driven insights, automation and productivity tools will make organizations more efficient, so employees can be free to create and innovate. And while AI seems to improve by orders of magnitude every day, most is not enterprise-ready — yet.

"We are only scratching the surface of what AI can do for business," says Hao Yang, VP of artificial intelligence.

And it'll start with automation. "Automation is going to be a big focus area in the development of AI since it will be an important productivity driver in business," says Chief Strategy Officer Ammar Maraqa, adding that automation will ultimately free up workers to be more creative. "One day, we will look back and realize that there was an abundance of talent with skills that would have been better utilized elsewhere within an organization."

But that's not all — AI will also help companies manage risk. For Splunk CTO Min Wang, the true value-add of AI lies in proactive security. She predicts AI will show greater potential next year when it comes to protecting organizations from cyber attacks. "Leveraging predictive and generative models, AI will provide better ways for security teams to distill information, find patterns and prioritize threats," she says.

However, there are quality concerns. "When it comes to generative AI, models cannot be 100% accurate," Wang explains. In particular, organizations are anxious about AI hallucination, which happens when a large language model (LLM) that powers a generative AI application produces fabricated information.

According to Wang, this problem cannot be eliminated without a total breakthrough on how the generative model is produced. "This certainly reinforces the importance of always keeping humans in the loop," she adds.

No doubt, AI will get more negative press next year. "By the end of 2024, we will have reached the peak of the AI hype cycle," says Tom Casey, SVP of products and technology. "People will start to realize the inaccuracies in some of the broad-based public models and we'll see a turn towards the trough of disillusionment. Nevertheless, we are going to see some pragmatic and practical uses of AI emerge."

"The beauty of AI is that it cuts across every type of organization," Steele says, "so we will see it leveraged across verticals with equal impact."

What about the public sector? According to LaLisha Hurt, Splunk industry advisor for the public sector, federal government, governments will embrace AI in enterprise-level software to help find efficiencies and enhance productivity of workers across agencies.

AI is still very much in the nascent stage, and in the short term, its real value doesn't replace the expertise required to operate it. "Most of the current AI use cases are not production hardened and won't be for another 12 to 24 months," says Simon Davies, Splunk SVP and general manager in APAC. "Long term, there is tremendous value to be realized, but it's not mature enough to fully take advantage of — yet."

Although it's early days, that doesn't mean organizations shouldn't be investing in building competencies and capabilities around AI. However, companies can't rely on it for everything. "AI has a difficult time reproducing the spirit of creativity and innovation," Maraqa says. "That will be one thing AI will not easily replace."

> “
>
> **We are only scratching the surface of what AI can do for business.**
>
> Hao Yang, VP of Artificial Intelligence, Splunk

Prediction: Resilience

Resilience will become non-negotiable as governments around the world mandate it.

In response to the rise of new threats and the critical importance of digital systems on economic output, regulators are beginning to enact strong compliance frameworks and strict governance on how businesses should prepare for and operate through adverse events.

"Building and maintaining the right readiness and resilience will be mandated rather than organizationally defined for large enterprises," says Simon Davies, SVP and general manager in APAC. In fact, this is already happening. For example, Australia introduced the Security of Critical Infrastructure Act 2018 (SOCI Act) to enhance and safeguard the resilience of 11 critical infrastructure sectors. The mandate requires organizations to submit a plan and formally attest to their resilience capabilities annually.

Meanwhile, the United States recently announced the National Cybersecurity Strategy, stressing the importance of digital resilience to national security. "There is already strong guidance in place through the Cybersecurity and Infrastructure Security Agency (CISA), a division of the Department of Homeland Security, that state and local governments should take advantage of right now," says LaLisha Hurt, industry advisor for the public sector, federal government.

In the EU, there are resilience mandates for specific industries, such as the Digital Operational Resilience Act (DORA) for the financial sector. And this past year, the European Commission proposed the Cyber Resilience Act, which aims "to ensure more secure hardware and software products."

"For specific mandates within Europe and the UK, it still hasn't been defined exactly what businesses will be required to do," says Mark Woods, Splunk chief technical advisor in EMEA. "Nevertheless, anticipated legislation is driving large enterprises to fundamentally change the way they not only value digital resilience, but reposition their business and operations from that perspective." No matter what mandates emerge, understanding how to effectively measure resilience strategies and capabilities will be foundational. "You can't change what you can't measure," he says.

"In 2024, digital resilience will be the key ingredient for enterprise success, and organizations will bake it into every aspect of their business," says Chief Strategy Officer Ammar Maraqa. "If an organization is able to achieve that, they will further drive innovation."

Prediction: C-suite transformation

CISOs, CTOs and CIOs will become more critical roles in the C-suite, and CFOs and CLOs will increasingly become cybersecurity experts.

With more sophisticated cyberattacks and new SEC rules on disclosing cybersecurity risk management, strategy, governance and incidents, C-suite roles are expanding. It will be an important success factor for the CISO, CTO, CIO — and even the CFO and CLO — to effectively communicate cyber risks and resilience strategies to key stakeholders.

"2024 is going to be a watershed moment for board interactions," says Splunk CISO Jason Lee. With the SEC's new regulations on cyber disclosures taking effect, board meetings are going to look vastly different. "Although the threat landscape will mostly stay the same in 2024, AI could make it much easier for adversaries to carry out attacks."

Companies cannot let down their guards. And to CEO Gary Steele, it's all about risk management. "Cybersecurity is a function of how to best manage risk for an organization," he says. "So the CISOs of tomorrow will need to work across the organization to manage that risk."

"Cyber risk is becoming an existential risk," says Tom Casey, SVP of products and technology. "And an organization's cyber posture could be the difference between not just losing business, but being out of business, which means CFOs and CLOs will need to get involved."

Boards are creating cybersecurity committees that encompass security, resilience and compliance. "When the committee reviews the cybersecurity posture of a company, it needs a comprehensive view of risk across the entire business," says Chief Strategy Officer Ammar Maraqa. "So the roles of CISO, CTO and CIO will broaden and become more strategic. And because of the new SEC reporting requirements around cyber, CFOs and CLOs will be required to become more cybersecurity savvy."

> “
> **...an organization's cyber posture could be the difference between not just losing business, but being out of business.**
>
> Tom Casey, SVP of Products and Technology, Splunk

A lot rides on security and tech leaders these days. “Next year a CISO, CTO and CIO’s biggest challenge will be to better educate stakeholders on the risks their organizations face so they can effectively prioritize and build strategies to address them,” says Simon Davies, SVP and general manager in APAC. “How secure is secure? How resilient is resilient? These are difficult questions to answer.” How do they drive these critical conversations?

“Boards value solid data,” says CTO Min Wang. “With increasing visibility on cybersecurity and digital resilience strategies, technology leaders must make a clear case for their investments. But they must also be proactive. Providing regular updates to the board and other critical stakeholders, even when not directly asked, fosters an environment of trust and transparency, which enables any organization to work more effectively.”

It also means being honest with the board about current processes and procedures. “Technology leaders must define where the weaknesses are and what their plans are to improve,” continues Wang. “And, more importantly, what type of investment is needed to make that happen.”

For Lee, it all boils down to language — new rules and regulations are forcing more in-depth conversations around an organization’s security and resilience profiles. Lee asks, “How do you translate security strategy and posture so that an investor can understand?” Technology leaders must learn to “talk the talk” when it comes to business, and they must learn it fast.

In 2024, being a great technologist won’t be enough. “When CISOs, CTOs and CIOs are excellent communicators,” Davies says, “they are able to unlock tremendous value for their organizations.”

Prediction: Sustainability

Organizations will ditch standalone sustainability "targets" and ESG will become the new "business as usual."

As we continue to accelerate towards the climate crisis point of no return, it's now become critical for organizations to integrate sustainability into every business decision for a more holistic environmental, social and corporate governance (ESG) approach.

"Executives won't rethink business plans to meet sustainability targets," says Mark Woods, chief technical advisor in EMEA. "Rather than it being a separate initiative, business leaders will refocus and have sustainability as part of their overall business objectives." Woods explains that the problem with standalone sustainability targets is that they don't drive real change.

Starting next year, regulation will prompt companies in certain regions to examine their sustainability practices. The European Sustainability Reporting Standards (ESRS) take effect in 2024, requiring organizations with offices in the EU to provide detailed metrics and reports on their ESG impacts. Globally, standards set by the International Sustainability Standards Board (ISSB) establish a new baseline for sustainability and climate reporting. In the United States, the SEC proposed rule on climate-related disclosures will join current and planned regulations in several other countries.

"What excites me about the ESRS and other mandates like it is that they serve as an impetus for organizations around the world to be more holistic in their approach to sustainability, which will help foster a greener future without detracting from business objectives," Woods explains.

"Currently, sustainability tends to be built into the OT layer rather than the IT layer," says Simon Davies, SVP and general manager in APAC. "For technology professionals, their role will be to help their colleagues unlock new opportunities from a sustainability point of view. That's where the big shifts will be made."

That's the crux of the matter. According to Woods, next year more organizations will elevate sustainability to the IT layer, where it will live as part of normal business operations.

The bottom line: Sustainability is good for business. “When you think holistically about sustainability, what we call ‘green data’ is actually the same data that keeps a business running, just viewed through a sustainability lens,” Woods says. Since that data is already part of day-to-day operations, business leaders are empowered to make smarter sustainability improvements — without it being a separate initiative.

“Mandates are a real step forward in our efforts to fight climate change,” says Petra Jenner, Splunk SVP and general manager in EMEA. “But there is still more work to be done.” Next year, expect more organizations to recognize the correlation between ESG and ROI.

Prediction: Regulation

Fueled by the AI boom, data privacy regulation will accelerate. As a consequence, an abundance of established companies will be unable to (or choose not to) provide their services in certain regions.

Data privacy has been a regulatory concern for decades, but with the meteoric rise of generative AI free from rules, governments are scrambling. Expect next year to get pretty messy.

“AI is the burning platform that is going to cause an eruption of regulation changes,” says LaLisha Hurt, industry advisor for the public sector, federal government. “There are already myriad concerns about basic data privacy. Now, with AI added to the mix, the policy machine will have to work even faster to stay ahead and keep everyone and their data safe.”

CISO Jason Lee warns that as companies begin to employ AI, it’s vital for business and technology leaders to understand the type of data that’s being collected and how it will be used. “There are clearly very positive uses for AI,” he says, “but how do you make sure your IP doesn’t wind up in an LLM?”

“There is no AI without data,” says Petra Jenner, SVP and general manager in EMEA. “And since regulation is driven by innovation, the regulatory landscape within Europe is rapidly changing.”

According to Mark Woods, chief technical advisor in EMEA, there are already specific acts being developed around AI and the use of personal data, which have caused companies to choose to not launch certain services within Europe. “We’ve already seen some warning signs that the EU will not stand for the way in which some of these companies are handling sensitive data,” he says.

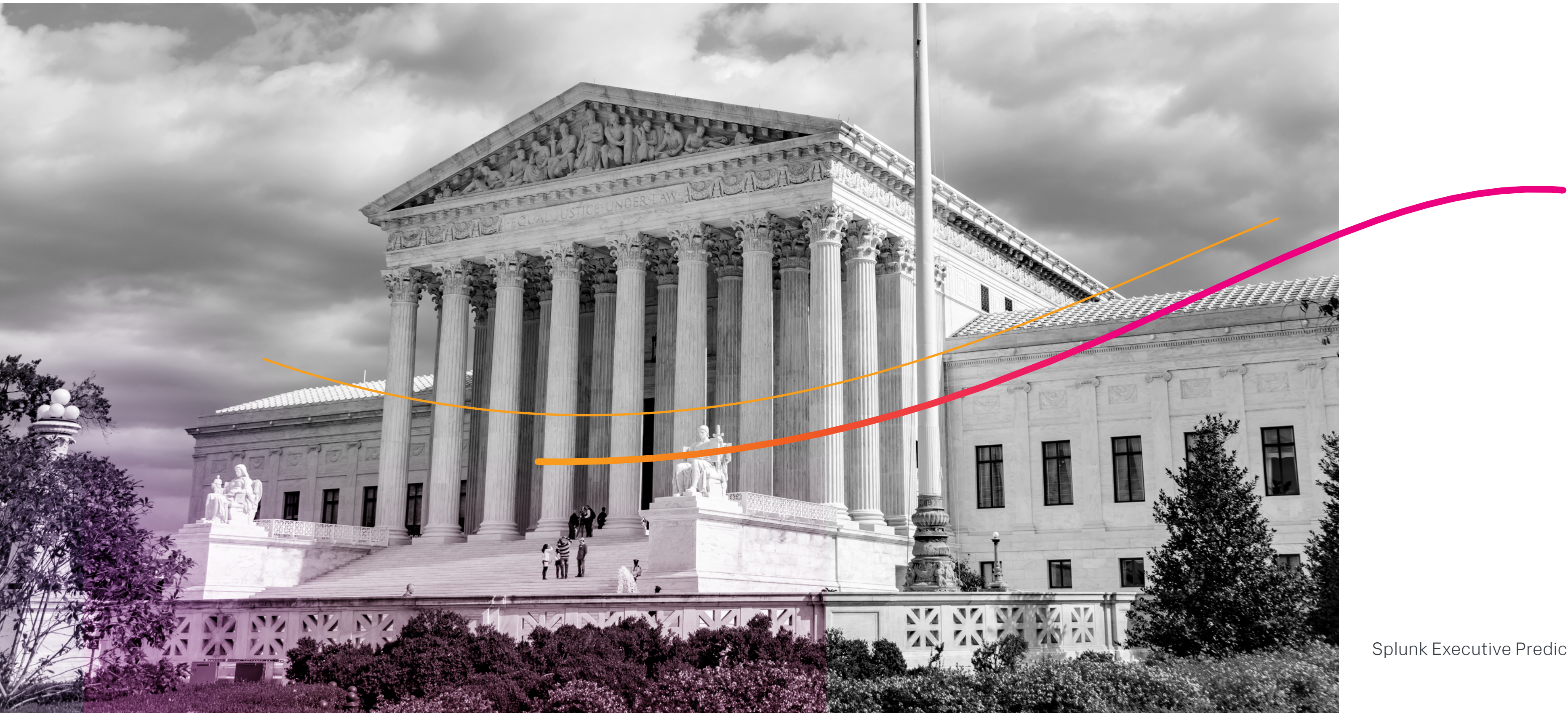
And it’s not just Europe. “Governments around the world are becoming more active in ensuring that industry is meeting their obligations around data privacy,” says Simon Davies, SVP and general manager in APAC. “In Australia, we’ve seen the government clearly make it board-level accountability, from a fine point of view, for data privacy breaches. We’re seeing similar conversations occurring in Japan, where this is becoming a national interest.”

These concerns shouldn't eclipse the overall good AI will provide. "It would be foolish to say that because of these risks, no person or organization should ever use AI," says Hao Yang, VP of artificial intelligence. "But regulators need to ensure that there are guard rails in place first to protect user data."

"What governments should not do is outright forbid AI," Hurt says. "That would only set us all back." But that's exactly what's happening. With concerns mounting, countries have been swift to enact all-out bans on certain AI platforms. And in 2024, we'll see a lot more of this.

AI hysteria is creating fractured regulation. "These knee-jerk reactions — where countries are eliminating access to certain services — will only accelerate and cause a great deal of confusion and complexity for businesses next year," says Tom Casey, SVP of products and technology.

Hurt stresses that at this early stage, education about AI's promises and pitfalls is crucial, even at a basic level. Governments and technology companies must work together to keep users' data safe.



Prediction: Consolidation

Unchecked operational complexity and rising costs will drive tool consolidation with an emphasis on simplicity, visibility and shared context.

More tools. More money. More problems. Eliminating redundancy, guesswork and friction from operations is key to building and maintaining a robust resilience strategy.

"In this uncertain economic environment, consolidation will be used as a vehicle to help drive down operational costs," says Petra Jenner, SVP and general manager in EMEA. "Organizations must learn to extract the most value from fewer services."

There's more benefit to consolidation than cost savings alone. "To cut down on operational complexity, organizations will first drive for simplicity at the user level," says Mark Woods, chief technical advisor in EMEA. Woods points out that most internal users today are stuck in a vicious cycle, continuing to implement more tools to plug visibility gaps.

"Today's technology leaders are given the dual task of making everything better — while also making it cheaper," Woods says. "In actuality, consolidation is an excellent vehicle to achieve just that. It drives down costs while instilling architectural discipline." End users can focus on specializing in a domain, versus a specific tool.

On the security side, CISO Jason Lee predicts that next year, CISOs will be on the hunt for one solution to work holistically across their entire hybrid cloud environment. "They don't want to pick one vendor for cloud and one for on-prem," Lee says. "They want a one-stop shop that can be leveraged across the entire threat profile." This cloud fragmentation hurts security posture because it obscures a CISO's visibility. "As a CISO, I want one vendor that I can apply to the entire environment. Successful companies are the ones driving for this visibility."

And in security, context is king. "It's critical to have visibility to not only understand the data, but to build context," Jenner says. According to Woods, context is what ultimately allows visibility to have value. "Driving for visibility without context is madness," Woods says. "Consolidating tools or vendors provides an opportunity to add context to the data and make it more shareable and consistent."

"Businesses are realizing that real value comes from having fewer platforms and vendors to manage, which ultimately enables greater context sharing when operating in a moment of crisis," says Tom Casey, SVP of products and technology. "Consolidation down to a single suite of tools in the SOC and a single suite of tools in the NOC is essential from an efficiency perspective."

Leading to brighter horizons.

This year, as we celebrate Splunk’s 20th anniversary and enter into the era of AI, we thought it only fitting to ask our senior leadership team one final question: What do you envision for the world in 2044?

“In 20 years, we will have fully realized the benefits of AI in everything we do,” says CEO Gary Steele. “It will be a core tenet in every process across every organization. And not only will we all be that much more efficient as a result, but we’ll deliver far better outcomes.”

Simon Davies, SVP and general manager in APAC, envisions a massive transformation in the human-to-technology interface, where systems will have the ability to self-engineer, self-heal and self-automate tasks. “In 20 years, SecOps will be able to send virtual agents across sets of infrastructure to identify vulnerabilities as new threats emerge, gathering all the endpoint data that’s been potentially exposed. And they’ll be able to automate that in just one line of instruction. This shift in the way data will flow around the digital lifeblood of systems and processes will allow organizations to work more seamlessly,” he says.

“There will be no phones in 20 years because there will be a completely different form factor,” predicts Tom Casey, SVP of products and technology. “AI will play a huge role in driving the value of smarter assistive technology, which will ultimately eliminate the need for standard forms of interaction in two-dimensional space.”

Mark Woods, chief technical advisor in EMEA, predicts that we will have a decentralized internet that is divided amongst services and access. “There will be a service layer, a consumer layer, and at that point, we could even have an automation and AI layer.”

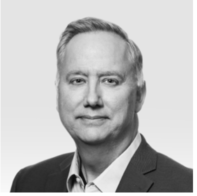
“We’re going to look back 20 years from now and realize that we underestimated the level of disruption and value of AI in our daily lives,” says Chief Strategy Officer Ammar Maraqa, “and underappreciated its capabilities.”

And by 2044, Hao Yang, VP of artificial intelligence, predicts that AI could become so intelligent that we have to rethink what artificial intelligence actually means. “Human-level intelligence for these systems, what we call artificial general intelligence, is on the horizon.”

“In this new era of AI, the future is bright,” says CTO Min Wang. “Humanity will become even more innovative and creative, reaching towards our next great achievements. Personally, I am most looking forward to witnessing the advancement of affordable space travel. With the help of AI, humanity can — quite literally — reach for the stars.”

To build our brightest future, business and technology leaders must learn to expect the unexpected. With every new innovation, challenges will arise. But if there’s one thing we can predict for certain, it’s that together, we will build a safer and more resilient digital world. Looking ahead 20 years, we see that the foundation has already been laid. In the era of AI, business and technology leaders will continue to influence and inspire with ingenuity — and build a brighter future for all.

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.

Petra Jenner

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

Simon Davies

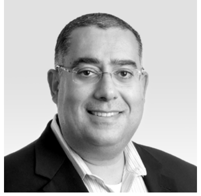
As senior vice president and general manager in APAC, Simon is responsible for the full portfolio of Splunk solutions in the Asia-Pacific and Japan markets. He is a veteran of Microsoft, Salesforce, Oracle and Citibank.

Jason Lee

As Splunk's chief information security officer, Jason is responsible for all facets of security engineering, assurance, policy, compliance, awareness and physical security across the organization. A technology industry leader with over 20 years of experience, most recently, Jason led security at Zoom.

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.



Ammar Maraqa

Ammar is Splunk's senior vice president and chief strategy officer. Back in the day, he led corporate strategy at Cisco, was part of the M&A team there, held product roles at Dell and started his career as a consultant with Bain & Co.

Gary Steele

Gary is the president and CEO of Splunk and a member of our board of directors. Prior to joining Splunk in 2022, Gary was the founding CEO of Proofpoint, where he led the company's growth from an early-stage start-up to a leading, publicly traded security-as-a-service provider.

Mark Woods

As Splunk's chief technical advisor in EMEA, Mark has been an engineer, consultant, entrepreneur and CTO. He helps executive teams and international policymakers understand the seismic potential of technology and data-enabled approaches.

Min Wang

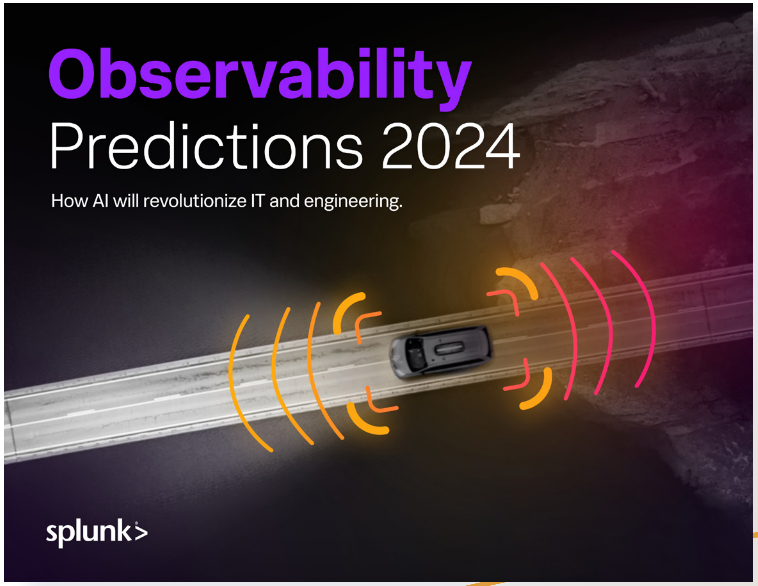
Min is Splunk's chief technology officer. With over 20 years of experience in research and development with a focus on AI, ML, data analytics and enterprise cloud, Min most recently led a team at Google responsible for critical components of the company's AI-driven Google Assistant.

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.

For more 2024 predictions, read our observability and security reports.

Read now



Observability
Predictions 2024

How AI will revolutionize IT and engineering.

splunk>

Security
Predictions 2024

From ransomware to resilience, and how AI will impact a changing threat landscape.

splunk>

splunk>®

Keep the conversation going with Splunk