FEATS OF STRENGTH

A BUSINESS-FOCUSED CYBERSECURITY MAGAZINE

Redefining Leadership in the Age of AI

How leaders are balancing innovation with control

Featuring:

BRADLEY SCHAUFENBUEL
VP and CISO, Paychex

DEB BRIGGS
VP & CSO, NETSCOUT

ELLIOTT FRANKLIN
SVP and CISO, Fortitude Re

FRED BRET-MOUNET
CISO, Accela

JACOB COMBS
CISO and Chief Product Security Officer, Tandem Diabetes Care

KATHRYN BURGNER
Information Security Lead, Strategic Advisor, knownwell

RICK ORLOFF
CISO, Everpure

ROLAND CLOUTIER
Former CISO

April 2026

K logix

TABLE OF CONTENTS

FEATURES

April 2026

MAGAZINE CONTRIBUTORS

Katie Haug - Editor in Chief
VP Marketing, K logix

Kevin West - Editor
CEO, K logix

Emily Graumann - Graphics
Graphic Designer, K logix

ABOUT K LOGIX

Our white-glove approach empowers leaders to advance their security programs and strategically align with the business to reduce risk.

We craft our services to address specific customer and industry challenges. One of the ways we do this is through our thought leadership, business-focused publication *Feats of Strength*. Through hundreds of CISO interviews, we extract trends in order to provide services that align business to information security.

DEAR READERS,

In this issue of *Feats of Strength*, we focus on a shift that every security leader is navigating in real time. Artificial intelligence is no longer a future concept. It is actively shaping how organizations operate, how risk is introduced, and how security teams respond. The eight leaders featured in these pages are experiencing that shift firsthand, each bringing a unique perspective on what it takes to lead in this environment.

Across these conversations, a consistent theme emerges. AI is accelerating everything, from innovation to risk, but the real challenge is not the technology itself. It is how leaders adapt to it. From governance and data protection, to human risk and operational scale, these leaders are building programs that can keep pace while staying grounded in what matters most. Their insights reflect a broader reality: **success is not defined by how quickly AI is adopted, but by how effectively it is managed**.

Alongside their stories, we share key trends drawn from these discussions to provide a clearer view into how security leaders are approaching AI today. What stands out is not a single strategy, but a shared mindset. The leaders in this issue are not reacting to change. They are shaping it, creating clarity where there is uncertainty, and guiding their organizations forward.

We hope this issue offers practical insight and perspective as you navigate your own approach to AI and security. The landscape will continue to evolve, but the leaders who succeed will be those who can balance progress with discipline and move forward with intention.

- Katie Haug, Editor in Chief

The AI Security Shift:

What Leaders Are Seeing Now

By Katie Haug

Across conversations with security leaders featured in Feats of Strength, one thing is clear: artificial intelligence is no longer a future consideration. It is actively reshaping how organizations operate and how risk is introduced.

But while AI is the catalyst, the story is not about technology alone. It is about leadership. It is about how security leaders are adapting to a faster, more complex environment while still maintaining control and trust.

There is also a noticeable shift in how these leaders talk about their role. The conversation has moved beyond tools and threats. It is now centered on decision making, prioritization, and how to guide an organization through change that is happening faster than most teams are built to handle.

The following themes reflect what leaders are experiencing today. Not in theory, but in practice.

AI IS NOW A CORE SECURITY PRIORITY

AI has moved beyond experimentation. It is now embedded in how organizations build and compete.

Security leaders are no longer asking if AI will impact their programs. They are managing that impact in real time, often while the business is already moving ahead.

At Paychex, Bradley Schaufenbuel describes the urgency clearly. “Most businesses see its adoption as essential to their survival,” he says on page 9. “Non-adoption or slow adoption of AI is seen as an existential threat.”

This shift is forcing a change in how priorities are set. AI is not replacing other risks, but it is influencing how they are evaluated. Leaders are looking at how AI intersects with existing programs, from data protection to third party risk, and adjusting accordingly.

In many cases, AI is also becoming a forcing function. It exposes gaps that may have existed for years but were not as visible. Data classification, access control, and visibility into usage patterns all become more urgent when AI is introduced.

The role of the CISO is evolving alongside this shift. AI is not a project to evaluate. It is a capability that must be enabled and secured at the same time. That requires a different mindset, one that is comfortable operating without complete information and making decisions as conditions change.

AI IS ALREADY SCALING SECURITY OPERATIONS

While much of the conversation around AI focuses on risk, leaders are already using it to improve how security operates.

The most immediate impact is scale. AI allows teams to handle increasing workloads without adding headcount, while also improving speed and decision making.

At Paychex, AI is already embedded in operations. “We are using AI agents to automate alert triage, alert data enrichment, and investigative processes in our security operations center,” Bradley explains on page 8.

At Fortitude Re, Elliott Franklin has taken a similar approach. “We have implemented over 100 automated responses and playbooks,” he says on page 12.

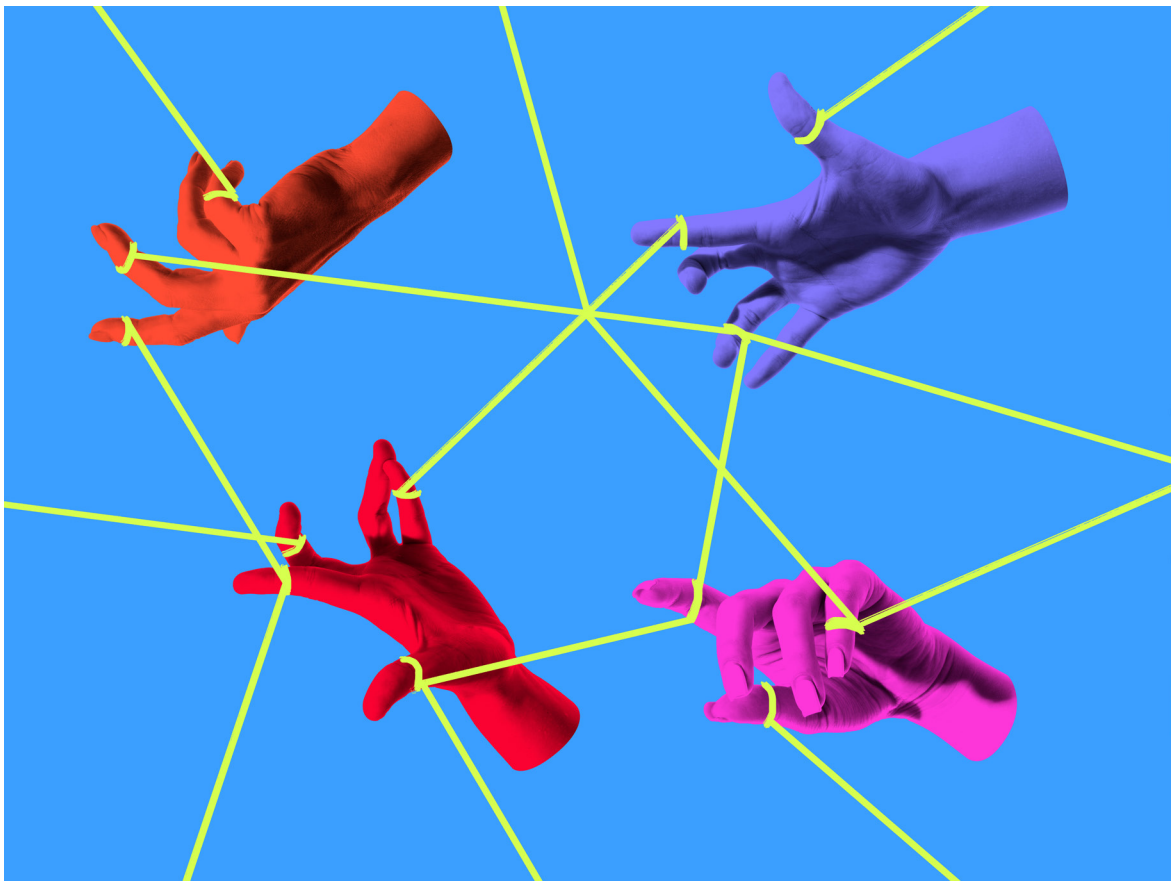
For Jacob Combs at Tandem Diabetes Care, the value goes beyond automation alone. “Automation has always been here, but now we have context,” he explains on page 16.

This shift toward context driven automation is critical. It allows teams to prioritize faster and reduce noise so they can focus on what matters most.

It is also changing expectations. What once required multiple analysts and several hours can now happen in minutes. That creates a new baseline for performance. Leaders are not just asking how to improve efficiency. They are asking how to redesign workflows entirely.

There is also a cultural shift that comes with this. Teams must learn to trust automation while still maintaining oversight. That balance is not always easy, especially in environments where accountability is high and the cost of mistakes is significant.

The leaders who are making progress are the ones who are treating AI as an extension of their team, not as a replacement. They are defining where automation adds value and where human judgment remains essential.



GOVERNANCE IS BECOMING AN ONGOING DISCIPLINE

As adoption accelerates, governance is no longer a theoretical framework. It is becoming an active discipline that must keep pace with the business.

Leaders are building structures that can evolve alongside how AI is used across the organization.

At Paychex, this takes the form of a formal governance body. “We assembled an AI Governance Council that includes all lines of defense,” Bradley explains on page 9.

Jacob Combs reinforces that governance is not static. “You can’t just set it and forget it,” he says on page 16. “You must manage it into the long term to make sure it’s still functioning and not drifting.”

At NETSCOUT, Deb Briggs highlights the reality of keeping pace. “There is an AI governance committee,” she says on page 11, pointing to how quickly these efforts must evolve.

What is changing is not just the presence of governance, but how it is applied. Instead of acting as a checkpoint, governance is becoming part of the workflow. It must operate at the same speed as the business, which requires clarity and simplicity.

Leaders are also recognizing that governance is not just about policy. It is about visibility and accountability. Understanding where AI is being used, what data it is accessing, and who is responsible for it becomes essential.

In many organizations, this is still a work in progress. The pace of adoption often outstrips the ability to govern it. That gap is where risk begins to accumulate.

THE BUSINESS IS MOVING FASTER THAN EVER

One of the most consistent themes across leaders is the pace at which the business is moving.

AI has lowered the barrier to entry for innovation. Development cycles are faster, and new capabilities are being introduced at scale.

At Accela, Fred Bret-Mounet sees this firsthand. “We are getting flooded with new business ideas, new solutions, new internal tools,” he says on page 14.

Elliott Franklin captures the pressure this creates. “Many businesses want everything immediately,” he says on page 12.

This acceleration is not limited to one part of the organization. It is happening across development, operations, and even business units that previously had limited technical involvement.

For security leaders, this creates a fundamental shift. They are no longer reviewing decisions after they are made. They are being asked to participate in them as they happen.

This requires a different approach to engagement. It is less about enforcement and more about partnership. Leaders must understand the business context, provide guidance quickly, and help teams move forward without unnecessary friction.

The challenge is that speed and control are often in tension. Moving too slowly can create frustration and lead to workarounds. Moving too quickly can introduce risk that is difficult to unwind.
Navigating that tension is becoming one of the defining responsibilities of the modern security leader.

AI RISK IS ROOTED IN DATA AND IDENTITY

While AI introduces new capabilities, the underlying risks are familiar. They are rooted in data and identity.

As AI systems access and process information at scale, controlling how data is used and who has access becomes critical.

Elliott Franklin reinforces this focus. “Identity and access management is an important area to focus on,” he says on page 13.

Jacob Combs highlights the speed of the challenge. “As this data starts flying around at superhuman speeds, how are we going to make sure that we’re not losing anything or sending anything out inappropriately?” he asks on page 17.

What is changing is not the nature of the problem, but the scale. AI increases the volume of data being processed and the number of systems interacting with it.

It also introduces new forms of identity. Machine identities, service accounts, and API driven interactions all expand the attack surface. Managing these identities becomes just as important as managing human users.

Leaders are focusing on visibility. They want to know where data is going, how it is being used, and what controls are in place. Without that visibility, it becomes difficult to manage risk effectively.

This is where foundational security practices become critical. Data classification, access control, and monitoring are not new concepts, but they take on new importance in an AI-driven environment.

HUMAN RISK IS EXPANDING AS THE THREAT LANDSCAPE ACCELERATES

AI is changing both sides of the security equation. It is making attackers more effective while increasing pressure on defenders.

At Paychex, Bradley describes the shift clearly. “Attackers are already leveraging AI to automate their attacks and improve the sophistication of those attacks,” he says on page 8.

“AI is also being leveraged to generate deepfakes that are driving up the success rate of phishing and social engineering techniques,” he explains.
Kathryn Burgner brings it back to people. “It lowers those barriers,” she says on page 18.

What this creates is a more dynamic threat environment. Attacks can be generated faster and at greater scale. They can also be more convincing, making it harder for individuals to detect them.

At the same time, defenders are using AI to improve detection and response. Automation helps reduce response times and allows teams to handle more incidents.

The challenge is that both sides are improving at the same time. This creates a constant race, where the advantage is not fixed.

As a result, leaders are placing more emphasis on human behavior. Training, awareness, and making secure actions easier are becoming critical parts of the strategy.

Human risk is no longer a secondary concern. It is central to how organizations think about security.

SECURITY TEAMS ARE EVOLVING, NOT SHRINKING

Despite concerns about automation, leaders are not reducing their teams. They are redefining how work gets done.

AI is taking on repetitive tasks and lower value work, allowing security professionals to focus on higher impact areas.

At Everpure, Rick Orloff puts it simply. “If AI is replacing my folks, I have them doing the wrong job,” he says on page 21.

Roland Cloutier highlights the shift in structure. “How do I reduce the number of people in my SOC by letting tier one and

tier two work be done by AI?" he asks on page 23.

At NETSCOUT, Deb Briggs reinforces the intent. "Rather than replacing analysts, the goal is to augment and upskill them," she says on page 10.

This evolution is not just about tools. It is about how teams are organized and how work is defined.

Entry level roles may change, and certain tasks may disappear, but the need for skilled professionals remains. In many cases, it becomes even more important.

Leaders are investing in their teams, helping them build new skills and adapt to changing expectations. The focus is on growth, not reduction.

This reflects a broader shift in the industry. Security is becoming more strategic, and the people within it must evolve accordingly.

WHAT COMES NEXT

Before looking ahead, the patterns across leaders are clear:

- AI is already embedded in how organizations operate
- The business is moving faster, and security is expected to keep pace
- Risk is centered on data, identity, and human behavior
- Governance must evolve alongside adoption
- Security teams are being redefined, not reduced

These are not isolated trends. They are interconnected shifts that are redefining how security programs are built and led.

Across all of these themes, one thing stands out. AI is accelerating everything, but leadership is what determines the outcome.

The leaders who are succeeding are not the ones who have all the answers. They are building programs that can adapt and teams that can evolve. They are comfortable operating in environments where the pace is high and the direction is not always clear.

At Fortitude Re, Elliott Franklin captures this mindset. "We cannot say no. Instead, the focus is on helping the business move forward safely by establishing clear guardrails and frameworks," he says on page 13.

That shift, from control to guidance, is defining the next generation of security leadership.

Looking ahead, the priorities are becoming more concrete.

Leaders are focusing on strengthening the foundations that will allow AI to scale safely. This includes improving visibility into data, tightening identity controls, and making governance part of how work gets done rather than a separate process.

There is also a growing recognition that speed will not slow down. If anything, it will increase. That means security programs must be designed to operate under pressure. They must be able to respond quickly, make decisions with limited information, and adjust as conditions change.

At the same time, the human element cannot be overlooked. As AI becomes more embedded, the role of people becomes more important, not less. Communication, trust, and clarity will continue to shape how effectively organizations navigate this shift.

The future of security will not be defined by technology alone. It will be shaped by leaders who can translate complexity into action and guide their organizations through uncertainty.

And the organizations that succeed will not be the ones that move the fastest or the safest.

They will be the ones that can do both.

PROFILES IN *Confidence*

BRADLEY SCHAUFENBUEL

VP and CISO
Paychex

Headquarters: Rochester, NY

Employees: 19,000+

Annual Revenue: $5.57 Billion

Bradley Schaufenbuel has served as Vice President and Chief Information Security Officer at Paychex for over six years, where he leads the company's global cybersecurity strategy. With a career rooted in financial services and strong security leadership, Bradley brings a pragmatic approach to protecting the business.

At Paychex, Bradley operates at the intersection of innovation and risk, helping the organization adopt new technologies such as artificial intelligence while maintaining strong governance and resilience. His leadership reflects a broader shift in the role of the modern CISO, one that requires balancing speed and business enablement in an environment defined by constant change.

MANAGING RISK IN A CONSTANTLY CHANGING ENVIRONMENT

For Bradley, uncertainty is not new, even as the pace of change accelerates. "The pace of change in the cybersecurity field is accelerating, but we have not changed the way we manage uncertainty," he explains. At Paychex, this discipline is embedded into daily operations. "We hold a daily standup in our Cyber Fusion Center where we review economic and geopolitical events and their potential impact on the cybersecurity landscape."

When risk levels shift, the response is immediate and deliberate. "If the risk posed by these changes is material, we then take proactive steps to mitigate those risks," he says. Recent geopolitical events have required rapid adjustments. "The Iran conflict is the latest example of that. We immediately raised our cyber threat level, which meant putting more eyes on glass in our security operations center, focusing threat hunts on techniques used by Iranian APT groups, and accelerating the SLA for remediation of critical vulnerabilities."

BALANCING COST, RISK, AND INNOVATION

"Security budgets are tightening," he says. "There is the expectation that the adoption of AI will drive productivity improvements that will lower costs."

At the same time, expectations continue to rise. "CISOs are also being asked to defend their organization against an accelerating volume of attacks that are AI-driven as well as to govern and secure their organizations' adoption of AI," he explains. This dual pressure is forcing leaders to rethink how they allocate resources. "You end up consolidating existing tools to free up capital to adopt tools that address new threats. It is a delicate balancing act."

AI AS THREATS AND ADVANTAGES

Bradley views AI as a defining force for the future of cybersecurity. "AI is proving to be transformational to both attackers and defenders," he says, "Attackers are already leveraging AI to automate their attacks and improve the sophistication of those attacks."

AI is changing the nature of identity-based attacks. "AI is also being leveraged to generate deepfakes that are driving up the success rate of phishing and social engineering techniques and defeating authentication systems."

At the same time, defenders are using AI to improve their own capabilities. "Defenders are leveraging AI to detect and respond to cyber-attacks faster and to automate the work of defenders," Bradley explains. At Paychex, these use cases are already operational. "We are using AI agents to automate alert triage, alert data enrichment, and investigative processes in our security operations center, which has allowed us to significantly reduce our meantime to respond to cyber-attacks."

Looking ahead, he sees an ongoing race between attackers and defenders. “It will continue to be a cat-and-mouse game between attackers and defenders, with each racing to adopt leading edge technology to advance their respective aims.”

ENABLING AI WHILE GOVERNING IT RESPONSIBLY

As AI adoption accelerates, the business is moving quickly and looking to security for guidance. “The question the business is asking me and most of my peers right now is ‘How can we adopt AI quickly, but also safely and responsibly?’” Bradley says.

The stakes are high. “Most businesses see its adoption as essential to their survival,” he explains. “Non-adoption or slow adoption of AI is seen as an existential threat.” This urgency changes the role of the CISO. “CISOs do not really have the option of saying no to AI or following a slow and methodical process to get to yes.”

Instead, the focus is on enabling adoption with strong guardrails. “They need to have a clear strategy for governing and securing AI, and the timeline for the execution of that strategy must be short.”

At Paychex, that strategy is formalized through a cross-functional governance model. “We assembled an AI Governance Council that includes all lines of defense,” Bradley explains. “That body generated an AI ethics policy that sets forth broad principles for the responsible adoption and development of AI.”

Governance extends beyond policy into execution. “The AI Governance Council reviews and approves every AI use case,” he says. The organization is also implementing technical controls to support that oversight. “We are also evaluating or putting into place tools to govern and secure AI applications, like LLM and MCP gateways that enforce guardrails around the actions of AI agents, automated AI red teaming tools, and dedicated instances of AI applications to avoid data leakage.”

SCALING SECURITY THROUGH AI AND AUTOMATION

AI is also helping Bradley address one of the most persistent challenges in cybersecurity: scale. “We have already developed AI agents for alert triage, alert data enrichment, and investigative tasks that have allowed us to shift tier one SOC analysts to higher value security work,” he says.

The team is continuing to expand these capabilities. “We are in the process of designing or developing AI agents to perform vulnerability triage work, identity and access management tasks, and penetration testing and red teaming.”

These investments are not about reducing headcount, but about enabling growth without adding friction. “These investments in AI are designed to allow us to keep up with a growing volume of work without expanding the size of our team.”

CONTINUOUS MONITORING AND CONTROL OF AI SYSTEMS

Once AI systems are deployed, maintaining visibility and control is critical. “We are building most of our AI agents, generative AI applications, and machine learning applications on platforms that generate detailed operational telemetry,” Bradley explains.

That data feeds directly into existing security operations. “That telemetry is being ingested into our security event and information management system, which is monitored around the clock for anomalous activity by our cyber fusion center.”

He also emphasizes the importance of identifying unsanctioned usage. “We have systems in place for discovering all AI models, MCP servers, AI agents, and AI applications, and alerting us to any unsanctioned AI in our environment.”

Advanced protections are also being implemented to address emerging attack vectors. “We have put in place technology that detects prompt injections, model poisoning, and other real time attacks on AI applications and blocks malicious behavior.”

ALIGNING SECURITY WITH BUSINESS OUTCOMES

Bradley anchors his program in widely recognized frameworks to ensure consistency and credibility. “We align our overall cybersecurity program with the NIST Cybersecurity Framework as well as the ISO 27001 standard,” he says.

This structured approach also supports executive communication. “This allows us to communicate to the executive team that we have adopted industry best practices, and we are either doing that well, or there is room for improvement.”

Beyond AI, his priorities reflect a broader business alignment. “Some areas of focus for us over the next 18 months are improving the cyber resilience of our organization, enabling the business to monetize its data assets while preserving the privacy and security of individual employees and customers, and creating a new source of revenue for the company.”

ADAPTING TO WHAT COMES NEXT

For Bradley, the defining challenge ahead is not any single technology, but the pace of change itself. “What will matter most in cybersecurity over the next 12 to 18 months is the ability of cybersecurity teams to innovate quickly and rapidly adapt to a technological environment and a threat landscape that are changing at an ever-increasing pace,” he says.

His perspective is grounded in a simple but powerful principle. “As Charles Darwin said, it is not the strongest that survive, but those that best adapt to change,” he notes. “You are either going to embrace change or become a victim of change.”

PROFILES IN *Confidence*

DEB BRIGGS

VP & CSO
NETSCOUT

Headquarters: Westford, MA

Employees: 2,000 (as of 3/31/25)

Revenue: $822.7 Million (as of FY25 ending 3/31/25)

Deb Briggs approaches cybersecurity with a practical mindset shaped by experience and scale. As Chief Security Officer at NETSCOUT, she leads security in an environment where visibility and performance are core to both the business and its customers. Her role requires balancing innovation with control, especially as artificial intelligence rapidly changes how organizations operate.

Rather than viewing AI as a single initiative, Deb breaks it down into focused, actionable areas. Her approach is grounded in real use cases and an understanding that security teams must evolve just as quickly as the technology itself.

AI AS A THREE-PART STRATEGY

For Deb, AI is not one problem to solve, but several. "For us, it is a three-dimensional problem," she explains.

The first area is automation of structured processes, where AI can immediately create efficiency. Deb focuses on applying AI to repeatable, high-volume tasks such as customer questionnaires/audits, RFP responses, and other standardized workflows. These are areas where consistency matters and where automation can significantly reduce manual effort while improving speed and accuracy.

The second area is security operations, where AI can support detection and response. While the potential is significant, Deb remains realistic about current limitations. Deb says, "Rather than replacing analysts, the goal is to augment and upskill them."

The third area is governance and visibility, which she sees as the most critical and challenging. As AI adoption grows across the business, maintaining control becomes increasingly difficult. "Because we are very AI-forward and we want people to get the most they can out of tools, we have to make sure we have strong governance in place," she explains.

THE REALITY OF AI ADOPTION

One of the biggest challenges Deb highlights is the gap between how quickly businesses want to move and how prepared they are to manage the risk.

"Right now, businesses just want free reign with AI. At the same time, many users do not fully understand the implications of data protection," explains Deb.

This creates an environment where AI can unintentionally expose information that was previously harder to access. For Deb, this is not a theoretical concern. It is happening now, and it is forcing organizations to confront long-standing issues around data management and control. Agentic AI is moving faster than most can imagine. The conversation is no longer about what it can do, but how we control identity, access, and logging. Not as enhancements, but as foundational requirements. This is a case where the tools and controls have not kept up with the rapid growth of the technology.

GAINING VISIBILITY INTO THE UNKNOWN

To address these challenges, Deb focused first on understanding the scope of AI usage across the organization. "We have an AI inventory tool," she says.

What she discovered was immediate and eye-opening. "Just three days in, it found 300 AI apps, and I almost fell off my chair," she recalls. Within a short period of time, that number continued to grow.

This level of visibility changed the conversation. Her experience is similar to many other security leaders in her position, it is becoming clear that AI is already widespread

and largely untracked. For Deb, this reinforced the need for continuous monitoring and stronger governance.

BUILDING GOVERNANCE THAT SCALES WITH THE BUSINESS

As AI adoption accelerates, Deb has focused on building governance structures that can scale alongside the business. "There is an AI governance committee," she says, describing a cross-functional approach that brings together key stakeholders to guide responsible AI use. Deb notes, "What's interesting about this committee is the speed at which it needs to operate to keep up with AI acceleration inside and outside our business."

For Deb, effective governance goes beyond policy. It requires alignment, clear ownership, and the right level of support to ensure it works in practice. "This does not come without resources," she explains, emphasizing that governance must be backed by investment and shared accountability across the organization.

Her approach reflects a broader leadership mindset. Governance is not about slowing innovation, but about enabling it in a way that is sustainable. By building the right structure and support around AI, Deb is helping NETSCOUT move forward with confidence while maintaining control.

AVOIDING THE MISTAKES OF THE PAST

Deb draws a clear parallel between the rise of AI and earlier challenges in identity and access management, where rapid growth outpaced visibility and control. She sees the same pattern emerging again as organizations quickly adopt AI without fully understanding what is being built, who owns it, or how it is being used.

Her concern is not the technology itself, but the lack of structure around it. Without clear ownership and foundational controls, AI agents can quickly multiply and introduce risk in ways that are difficult to detect or manage.

For Deb, the priority is ensuring that organizations do not repeat past mistakes. By establishing stronger visibility and accountability early, she is focused on helping the business scale AI in a way that is both controlled and sustainable.

AI AS A FORCE MULTIPLIER

Deb sees AI as a practical way to scale security operations, particularly in areas that are structured and data-intensive. Functions like vulnerability management and analysis are well suited for AI, where large volumes of information need to be processed quickly and consistently.

Rather than replacing people, her focus is on enabling them. AI allows her team to move faster, reduce manual effort, and spend more time on higher-value work that requires judgment and experience.

She also highlights AI's ability to analyze and correlate massive amounts of data at a speed that would not be possible manually. When applied thoughtfully, these capabilities strengthen the team's effectiveness and allow security to operate at a level that keeps pace with the business.

LEADING AT THE PACE OF CHANGE

She describes the current moment of AI with a familiar analogy. "I feel like I am in that *I Love Lucy* episode where the chocolates are coming down the conveyor belt. Right now, it is manageable, just like AI, but as the episode continues they cannot keep up, and the chocolates start flying everywhere. Lucy ends up covered in chocolate, stuffing it in her apron. The question that none of us know is how fast that AI conveyor belt can be turned up."

That uncertainty captures the challenge facing security leaders today. The pace of innovation continues to accelerate and expectations from the business are increasing.

At NETSCOUT, Deb is focused on building a program that can keep up. One that combines visibility and governance, and ensuring her team is prepared not just for where AI is today, but for how quickly it will evolve.

PROFILES IN *Confidence*

ELLIOTT FRANKLIN

SVP, CISO
Fortitude Re

Headquarters: Bermuda

Employees: 550+

Annual Revenue: Private Company

Elliott Franklin leads security at Fortitude Re with a perspective shaped by both technical experience and a deep understanding of the human side of cybersecurity. Elliott is responsible for protecting sensitive data and ensuring resilience in an environment where risk is constant and expectations are high.

His approach to security and leadership reflects a broader shift in the role of the CISO. Security is no longer just about controls and compliance. It is about enabling the business, adapting to rapid change, and building programs that can withstand both technical and human pressures.

STAYING GROUNDED IN THE FUNDAMENTALS

In the face of geopolitical and economic uncertainty, Elliott's approach is intentionally steady. "You cannot ignore it, but at the same time, we do not change," he explains.

Rather than reacting to every new threat or headline, his team remains focused on core disciplines such as identity and access management, monitoring, and response. Threat intelligence from industry groups like ISACs provides additional context, but it does not change the foundation of the program.

For Elliott, consistency is what allows organizations to remain effective even as the external environment evolves. "We try to stay focused on the basics regardless of what is going on," he says.

SECURITY AND BUSINESS LEADER

Elliott sees a clear shift in how CISOs must operate today. "We have to be business leaders now," he says.

Rather than leading with regulatory requirements or security mandates, his focus is on understanding business priorities and aligning security to support them.

"We are asking the business for their priorities," he explains. "How can we help the company make money or be productive?"

This shift changes how security is perceived. Instead of being a gatekeeper, the CISO becomes a partner who helps accelerate outcomes. "If we can accelerate things," he says, "they will not even see it as a security project."

AI AS OPPORTUNITY

Elliott describes AI as a rapidly evolving force that is already reshaping how security teams operate. "We are definitely taking advantage of what AI has to offer," he says.

At Fortitude Re, AI is being used to automate operational tasks and improve response times. The team has implemented agents and automated playbooks that support detection, triage, and response, allowing them to act faster than traditional processes would allow.

"We have implemented over 100 automated responses and playbooks," he explains. This includes taking decisive action when needed. "We have given them permission to take action," he says, noting that in some cases that may include shutting down systems to stay ahead of a threat.

For Elliott, the priority is clear. Speed matters, and automation is essential to keeping pace.

BALANCING SPEED WITH CONTROL

While the business is eager to adopt AI, Elliott emphasizes the importance of doing so responsibly. "Right many, many businesses want everything immediately," he says.

Elliott believes the role of security is not to slow that momentum, but to guide it. He explains, “We cannot say no. Instead, the focus is on helping the business move forward safely by establishing clear guardrails and frameworks.”

At Fortitude Re, that guidance is grounded in established standards. “These are not our rules,” he says. “If we follow the NIST AI risk management framework, it makes it easy to explain.” This approach allows the team to support innovation while maintaining consistency and control.

IDENTITY AND DATA AS THE CORE PRIORITIES

Beyond AI, Elliott remains focused on foundational areas that continue to drive risk. “Identity and access management is an important area to focus on,” he says.

As organizations adopt more SaaS applications and AI systems, managing both human and non-human identities becomes increasingly complex. APIs, tokens, and service accounts expand the attack surface, requiring greater visibility and control.

At the same time, data protection remains a constant challenge. Understanding where data lives and how it moves across environments is critical, particularly as employees adopt new tools at a rapid pace.

For Elliott, these are not new problems, but they are becoming more urgent as the environment evolves. “We are trying to understand what is being uploaded and where it is going,” he explains.

RESILIENCE AS A CORE DISCIPLINE

Resilience is another key area of focus, particularly as organizations face a growing range of disruptions.

Elliott emphasizes the importance of planning for outages, ransomware, and other operational risks. This includes ensuring that backups are secure and the organization can continue operating even during an incident. “It is an insurance policy,” he explains.

While resilience may not always be a visible priority, it is essential to long-term success.

THE HUMAN SIDE OF CYBERSECURITY

Looking ahead, Elliott believes one of the most important areas of focus will not be technology, but people. “Technology really is last,” he says.

As AI continues to reshape the industry, it is also creating new pressures for security professionals. Concerns about job displacement and constant exposure to risk can take a significant toll. “AI is making practitioners even more afraid,” he explains.

Elliott is particularly focused on the impact this has on mental health, both within the workplace and at home. “We cannot continue to sustain the pressure that CISOs have to always be protecting the company without having health issues,” he says.

This perspective reflects a broader leadership responsibility. Building a strong security program is not just about tools and processes, it is about supporting the people behind them.

LEADING THROUGH CHANGE

For Elliott, the future of cybersecurity will be defined by how leaders balance technology and risk with human impact.

The pace of change will continue to accelerate, driven by AI and evolving threats. But success will depend on more than technical capability. It will require clear communication and a focus on both business outcomes and team well-being.

At Fortitude Re, Elliott is building a program that reflects that balance, one that stays grounded in fundamentals and recognizes that behind every system is a team that must be supported to succeed.

PROFILES IN *Confidence*

FRED BRET-MOUNET

CISO

Accela

Headquarters: San Ramon, CA

Employees: 500+

Annual Revenue: Private Company

Fred Bret-Mounet leads security at Accela with a perspective shaped by decades of experience building and evolving security programs across fast-moving technology environments.

His leadership reflects a broader shift in the role of the CISO. The challenge is no longer just about managing risk, but about keeping pace with a level of technological acceleration that is fundamentally changing how software is built and secured.

AI HAS CHANGED THE PACE OF EVERYTHING

For Fred, the biggest shift in cybersecurity today is not subtle. “Right now, the panic moment is AI,” he says.

In a matter of months, the landscape has transformed. What once required specialized skills is now widely accessible. “It used to be that you needed to have skills and expertise to build software. You do not need that anymore,” he explains.

At Accela, that shift is already visible. “We now have 500 software developers. Everybody has their Claude license and they go at it,” Fred says.

While this unlocks innovation, it also introduces scale challenges that security teams are not traditionally built to handle. “We are getting flooded with new business ideas, new solutions, new internal tools,” he explains. “And we just barely have time to react if we ever find out about it.”

For Fred, this is the defining tension of the moment. The business is accelerating, and security must find a way to keep up.

REINVENTING THE ROLE OF SECURITY

Rather than resisting that change, Fred sees it as an opportunity to rethink how security operates.

“For the last 25 years, my job has been to get in the way of things,” he says. He describes a traditional model where security reviews happen late, often forcing teams to go back and fix issues after the fact.

That approach is no longer viable at the current pace. “If we do not adapt, we are doomed,” he says.

Instead, Fred is focused on embedding security directly into how work gets done. His goal is to define clear requirements and standards that are automatically applied as developers build. “If I play my cards right, I have a shot at making developers meet my expectations from the get-go,” he explains.

This shift represents a fundamental change in mindset. Security is no longer a gate at the end of the process instead it becomes part of the process itself.

MANAGING AI THROUGH AI

To address the scale challenge, Fred is exploring a model where AI helps secure AI-driven development. “My theory at this point is that I will manage AI through AI,” he says.

Instead of relying on manual reviews, he is implementing AI agents that evaluate work as it progresses. These systems can assess risk, determine whether additional review is needed, and even generate threat models in a fraction of the time it would take a human.

“Claude will build a threat model that is of better quality than a human that is not motivated to do so,” he explains.

This approach allows his team to focus on what matters most. “I am hoping I will take the edge off and have my team focus on the true risk, not the rubber stamping process,”

Fred says.

For him, the opportunity is clear. By leveraging AI in the right way, security can scale alongside the business instead of becoming a bottleneck.

VISIBILITY AS THE FOUNDATION

While AI introduces new capabilities, Fred is clear that many of the core challenges remain unchanged. “You cannot protect what you do not know of,” he says.

His focus is on building comprehensive visibility across the organization, including systems, data, and what he refers to as the “virtual workforce” of AI agents. “We need to have an inventory of virtual workforce. What do they do, who manages them, and where can you find them?” he explains.

This visibility is critical not only for security, but for understanding value. “We are spending an obscene amount of money in AI right now, and we do not have good controls to understand what the ROI is,” he says.

For Fred, inventory is not just a technical requirement. It is the foundation for control, accountability, and decision-making.

AI WILL RESHAPE THE WORKFORCE

Fred is also candid about the broader impact AI will have on how organizations operate. “I suspect we are going to see a serious amount of restructuring in the next six months,” he says.

While AI will improve efficiency, it will also change the types of roles organizations need. Some functions will be automated, while others will evolve to focus on oversight, problem solving, and higher-level decision-making.

At the same time, he emphasizes the importance of long-term thinking. Eliminating entry-level roles entirely could create gaps in the future pipeline of talent.

His perspective reflects a balanced view. AI will drive change, but how organizations manage that transition will determine long-term success.

RETHINKING SECURITY FUNDAMENTALS

Beyond AI, Fred remains focused on core security disciplines that continue to challenge organizations. Inventory, access control, and patching remain top priorities. “We do not know our perimeter,” he says.

He also highlights identity and access management as an ongoing issue. “We give access to people without thinking it through,” he explains.

Patching is another area where he sees an opportunity for change. Rather than relying on manual processes, he advocates for a more automated approach. “We humans are not able to keep up with patching requirements,” he says.

These priorities reinforce a consistent theme. Even as AI transforms the landscape, the fundamentals still matter.

ADAPTING TO WHAT COMES NEXT

For Fred, the defining challenge is not just AI itself, but the speed at which everything is evolving.

The combination of increased development velocity, expanding attack surfaces, and rising expectations from the business is forcing security leaders to rethink how they operate.

At Accela, Fred is focused on building a program that can adapt to that reality. One that integrates security into development, leverages AI to scale, and maintains visibility across an increasingly complex environment.

Because in this new era, standing still is not an option.

PROFILES IN *Confidence*

JACOB COMBS

CISO & Chief Product Security Officer

Tandem Diabetes Care

Headquarters: San Diego, CA

Employees: 2,500+

Annual Revenue: $1.015 Billion (GAAP)

For almost three years, Jacob Combs has led the security program at Tandem Diabetes Care, where his approach to cybersecurity is grounded in pragmatism and adaptability. In an industry defined by constant change, he doesn't see uncertainty as a new challenge, but as the baseline.

Rather than trying to predict every possible threat, Jacob has built his program around the core principle of resilience.

He explains, "When I joined, I focused on this idea of resilience. It's all about our ability to detect, respond, and recover to an attack that occurs. It is still very important today."

For him, that capability is a great safety net, ensuring the organization can withstand what it cannot predict. It also allows the business to move forward with confidence, knowing that even in the face of increasingly complex attacks, they have a strong, resilient security program.

AUTOMATION WITH CONTEXT

For Jacob, the most immediate impact of AI is not just automation, it is automation with context.

"Automation has always been here, but now we have context," he says. "It is not only automating and moving quickly, but gathering and analyzing the context to give my team the ability to make a decision very quickly."

This added layer of context is critical in reducing noise and improving prioritization. It represents a shift from reactive security to more informed decision making.

"Now we can understand priority right away," he explains, describing how enriched insights help teams cut through things like false positives, and focus on what truly matters.

LEADING AI ADOPTION

Within Tandem, Jacob has positioned himself as a key leader in the company's AI journey.

"They're looking to security to help build the guardrails so they can ensure AI is done safely," he says.

In a highly regulated healthcare environment, that responsibility carries significant weight. It requires balancing innovation with compliance, while ensuring speed does not come at the expense of safety or trust.

To support this, Jacob helped establish an internal AI governance council. He says, "We've built our own internal AI governance council where we talk about these things and start planning and designing the next steps forward."

ONGOING GOVERNANCE

For Jacob, AI governance is not a one-time framework, it is an ongoing operational discipline that requires continuous oversight.

"You can't just set it and forget it. You must manage it into the long term to make sure it's still functioning and not drifting or making mistakes," he explains.

That shift introduces a new layer of complexity. Unlike traditional systems, AI requires continuous measurement over time, with clear accountability for outcomes and performance.

As Jacob sees it, organizations are not just managing technology, they are managing behavior. "It's almost like managing another employee, but a lot faster," he says, pointing to the need for clear rules around access and oversight as these systems begin to operate more autonomously.

CONTROLLED PATH FOR AI

Jacob is taking a deliberate, controlled path when it comes to AI.

“We’ve solidified around Copilot because it keeps our data inside, and we’re essentially blocking the rest until we get official agreements and licensing in place,” he explains.

This measured approach allows his team to build confidence in how AI is deployed, while minimizing unnecessary exposure. It also creates a foundation for scaling more advanced use cases over time.

As the organization evolves, new challenges are emerging, particularly around autonomous systems.

“If we start using these agents and they start making decisions on their own, where does that human in the loop preside? What are the rules and performance management structures we have around that?”

DRIVING EFFICIENCY ACROSS THE ORGANIZATION

Jacob is also using AI to reshape how his team spends their time.

Rather than applying AI to security tooling, he has focused on eliminating low-value work. By offloading administrative tasks, his team can concentrate on higher-impact activities.

“I want my team to be able to focus on security work, and AI is helping because they can spend less time on things like project updates and documentation,” he says.

This shift not only improves efficiency but also elevates the role of the security team, allowing them to spend more time on their core work.

BALANCING INNOVATION WITH RISK

As AI enthusiasm grows across the business, Jacob often finds himself balancing momentum with caution. His role is to enable progress without exposing the organization to unnecessary risk.

“I’m trying to balance the need for the business to move forward without having to potentially lose our shirt because we take some outsized risk.”

As Tandem expands its AI capabilities, Jacob is prioritizing one critical area: data. With data moving faster than ever, maintaining control becomes essential.

Jacob comments, “A big one for me is around data security, because that is so crucial to having functional AI systems. As this data starts flying around at superhuman speeds, how are we going to make sure that we’re not losing anything or sending anything out inappropriately?”

LOOKING AHEAD

As the pace of change continues to accelerate, Jacob sees the next year as a balancing act between innovation and discipline. AI will continue to evolve, and with it, the expectations placed on security leaders.

For Jacob, success will not come from trying to predict every outcome, but from building systems that can adapt in real time. His focus remains on enabling the business to move forward confidently, while he supports growth.

PROFILES IN *Confidence*

KATHRYN BURGNER

Information Security Lead, Strategic Advisor

known**well**

Headquarters: Boston, MA

Employees: 100+

Annual Revenue: Private

Kathryn Burgner brings a perspective shaped by the realities of healthcare, where trust and patient data are tightly connected. In a rapidly evolving environment, her role requires balancing innovation with responsibility, ensuring that security supports both patient outcomes and business growth.

Her leadership reflects a broader shift in cybersecurity. It is no longer just about implementing controls. It is about prioritizing risk, enabling the business, and building a culture where security is understood and embraced across the organization.

PRIORITIZING WHAT MATTERS MOST

In a time defined by economic pressure and geopolitical uncertainty, Kathryn's approach is grounded in focus and discipline. "We are really trying to prioritize ruthlessly based on risk exposure, impact, and third-party dependency," she explains.

Rather than trying to address every possible threat, her team concentrates on what is most relevant to the business and its patients. This includes evaluating current risks and aligning security efforts to where they will have the greatest effect. At the same time, efficiency is critical.

"We are always trying to be cost efficient and make sure we are scaling in a way that is smart and right-sized for where we are at in our journey as a company," she says. This balance between focus and efficiency allows her team to move forward with clarity, even in uncertain conditions.

SECURITY AS A BUSINESS ENABLER

Kathryn sees a clear shift in how security leaders must operate today. "We really need to focus on risk reduction and measurable results," she says.

That focus is closely tied to partnership across the organization. Security is no longer a standalone function. It must be integrated into how the business operates and grows.

"Being an enabler, not just an enforcer or just a cost center," she explains, is essential to building credibility and driving impact.

In healthcare, that alignment is especially important. Trust is directly connected to patient experience, making security a core part of delivering value to the business and its customers.

AI AND THE RISE OF HUMAN RISK

When it comes to AI, Kathryn's perspective is centered on its impact on people. "It lowers those barriers," she says, referring to how AI makes it easier for both innovation and malicious activity.

While AI creates opportunities for automation and efficiency, it also increases exposure to human risk. Phishing, social engineering, and other attacks become easier to execute, expanding the threat landscape beyond traditional boundaries. For Kathryn, this shifts the focus of security.

"We are going to need to think about how quickly we can operationalize defenses to human risk while using AI to combat AI," she explains. This includes proactively identifying exposed data, understanding where risk exists, and building defenses that can keep pace with evolving threats.

BALANCING SPEED AND SAFETY

One of the biggest challenges with AI is balancing rapid adoption with responsible use. "Anyone can use it," Kathryn says.

The question is not whether AI will be used, but how safely

and effectively it is implemented. “If we focus too much on the regulatory side, we may miss the speed,” she explains. “But those regulations are there for a reason.”

For Kathryn, the answer lies in balance. By prioritizing risk and evaluating use cases carefully, organizations can move quickly while still protecting sensitive data and maintaining trust. In healthcare, that balance is critical. Patient data and regulatory requirements create a higher standard for how technology must be deployed.

BUILDING A CULTURE OF SECURITY

Rather than relying solely on policies and controls, Kathryn emphasizes culture as a key driver of security success. “The biggest thing we are trying to do is create a culture of security that is transparent and collaborative,” she says.

Her goal is to make security approachable, not intimidating. “Security is not looked at as an enforcer or punishment, but more of an enabler,” she explains.

This approach is particularly important in healthcare environments, where clinicians and providers are focused on patient care and do not have time to navigate complex security processes.

“We need to make it very easy for them to be successful,” Kathryn says. By building trust internally, her team is able to reduce human risk and encourage collaboration across the organization.

EVOLVING SKILLS IN THE AGE OF AI

As AI continues to evolve, Kathryn sees a shift in the skills required for security teams. “I do not think roles will simply be replaced,” she says. Instead, professionals will need to adapt, developing new capabilities around data analysis, modeling, and working effectively with AI tools.

“How can we teach the skills to work with AI,” she explains, rather than focusing on specific tools that may quickly become outdated. This shift reflects a broader change in the workforce. The ability to adapt and apply new technologies will be more important than any single technical skill.

A FRAMEWORK FOR GROWTH

To guide her program, Kathryn relies on established frameworks that provide structure without limiting flexibility. “We use NIST CSF 2.0 as a strategic security enabler,” she says.

This allows her team to measure progress, define maturity, and align security with the company’s growth. “We think about how we are scaling our business and then scaling our security at the right ratio,” she explains.

By focusing on incremental progress, her team avoids becoming overwhelmed while still building a strong foundation.

FOCUSING ON IDENTITY AND PREVENTION

Looking ahead, Kathryn is prioritizing areas that directly reduce risk, particularly identity and human behavior. “Identity and access management is still an important area,” she says.

In addition, her team is focused on preventing attacks before they occur by making secure behavior the easiest path. “We need to make it very easy for them to do the right thing,” she explains.

This approach reflects a shift toward proactive security, where the goal is to reduce risk at its source rather than simply responding to incidents.

BALANCING INNOVATION AND TRUST

For Kathryn, the future of cybersecurity will be defined by balance. “The continued balance between the speed of using new technologies and prevention is going to be so important,” she says.

Organizations must move quickly to remain competitive, but they must also maintain the trust of their customers and stakeholders. At knownwell, that trust is central to everything.

“Our core focus is earning and maintaining patient trust while still enabling growth and innovation,” Kathryn explains. This balance between speed, security, and trust defines her approach to leadership, and positions her team to succeed in a rapidly changing environment.

PROFILES IN *Confidence*

RICK ORLOFF

CISO

Everpure

Headquarters: Santa Clara, CA

Employees: 6,000+

Annual Revenue: $4 Billion

Rick Orloff leads security at Everpure, formerly Pure Storage, shaped by years of experience navigating evolving threats and business challenges. His perspective reflects a broader shift in cybersecurity leadership, one that moves beyond prevention and more toward resilience and enabling the business to move faster without necessarily increasing risk.

At Everpure, Rick focuses on building a strong security program, grounded in fundamentals and complimented with leading edge capabilities.

RESILIENCE IS KEY

For Rick, resilience is not a response to today's environment, it is the baseline requirement for operating in it. As geopolitical tensions and economic pressures continue to evolve, security programs must be built to withstand disruption, not just prevent it.

"Relying on resilience is not new," he says. Rather than treating each new threat as a separate problem to solve, Rick believes organizations need a durable foundation that can absorb change. A well-designed resilience strategy allows teams to adapt as new risks emerge, without needing to rebuild their approach each time the landscape shifts.

"If you do not have a resilience program already, you are doing something wrong," he explains.

This shift reflects a broader evolution in security leadership. The goal is no longer just to defend against specific threats, but to ensure the organization can continue to operate and recover quickly, regardless of what those threats or global changes may be.

FROM PREVENTION TO CONTAINMENT AND RECOVERY

Rick also highlights a fundamental shift in how CISOs think about security. "Threat actors are probably going to get in at some point," he says.

As a result, the focus has moved away from trying to build impenetrable defenses and has moved toward controlling impact. Rick explains that leaders are now asking different questions. How do we minimize exposure? How do we reduce blast radius? How do we recover quickly? Can we operate while experiencing technical interruptions?

This evolution reflects a more realistic view of the threat landscape. Security is no longer defined by keeping attackers out, but by how well an organization can respond when something goes wrong.

STRUCTURING AI WITH CLEAR GUARDRAILS

As AI adoption accelerates, Rick approaches it with a structured framework designed to balance enablement with control. "I structure AI as a swim lane," he explains.

On one side are governance and risk controls, including policies, identity management, and oversight. On the other are technical controls that define how AI systems interact with data and environments along with the ability to identify deviations.

Rick says that identity is one of the key principles. Each AI system must operate with its own unique identity and clearly defined permissions based on the Principle of Least Privilege. This prevents overexposure and limits the potential impact of misuse or compromise.

Equally important is controlling access to data. AI systems should only be able to interact with the specific data sets required for their function, with monitoring in place to detect any deviation. "If it goes anywhere else, I get an alert," Rick

explains.

This combination of governance and technical enforcement creates a model that allows organizations to adopt AI confidently while maintaining control.

ENABLING THE BUSINESS WITH AI

Rick is clear that the role of security is not to block innovation, but to support it. “From the executive level, it is more about how we can enable AI,” he says.

Business leaders expect security to manage risk, but they also expect security to help accelerate adoption of new technologies. That requires a structured process for evaluating and approving tools without introducing unnecessary friction.

At Everpure, that process is grounded in clarity. If a tool does not meet core requirements including identity management or data protection, it is not approved. If it does, it can be enabled quickly and safely. This approach positions security as a partner rather than a barrier.

AI AS A FORCE MULTIPLIER FOR TEAMS

Rick also sees AI as an opportunity to elevate how security teams operate.

“If AI is replacing my folks, I have them doing the wrong job,” he says.

Rather than eliminating roles, AI allows teams to shift focus. Routine tasks and lower severity issues can be automated, freeing experienced professionals to focus on more complex and critical work.

“If I can have AI handle my lower severity stuff, I can have my top talent focus on critical things,” he explains.

This shift is not about reducing headcount. It is about increasing impact and ensuring that teams are working on the problems that matter most.

A NEW SECURITY DOMAIN EMERGING

Looking ahead, Rick expects AI to fundamentally reshape the structure of cybersecurity itself. “I think there is going to be a whole new specialist area, a whole new security domain purely on technical AI security controls,” he says.

As AI systems become more autonomous and capable, they will require new skill sets and specialized controls.

Rick comments that this evolution mirrors previous shifts in the industry, such as the rise of cloud security, but with greater speed and broader impact.

ADAPTING TO CONTINUOUS CHANGE

Rick has seen this pattern before. New technologies emerge, are initially resisted, and eventually become foundational.

“Back in the day, I was one of those guys that said I am not putting my company data in someone else’s cloud,” he recalls.

Today, cloud is standard. He expects AI to follow a similar trajectory, but at an exponential pace eclipsing Moore’s law.

His focus is on building a program that can evolve alongside that change. One that combines resilience, structured governance, and strong fundamentals, while enabling the business to take advantage of what comes next.

PROFILES IN *Confidence*

ROLAND CLOUTIER

Former Global CISO
TikTok, ADP and EMC

Current Principal
The Business Protection Group

A STRATEGIC VIEW ON CYBERSECURITY

After more than 30 years in cybersecurity leadership, including roles as Global CISO at TikTok, SVP and CSO at ADP, and VP and CSO at EMC, Roland has shifted into a strategic advisory role, supporting CISOs, CEOs, general counsels, and chief trust officers. Having led security at some of the world's largest organizations, he is now intentionally taking a step back from the day-to-day CISO seat to focus on guiding others.

While he may no longer sit in the operational role, his perspective remains rooted in the realities of running a modern security program.

That vantage point allows him to see trends across organizations, particularly as security leaders navigate increasing complexity and the growing influence of AI.

RESILIENCE AS THE FOUNDATION

Despite the innovation happening across the industry, Roland is clear that the core mission of cybersecurity has not changed.

"At the end of the day, we are operational business protection specialists for the company," he explains.

In today's environment, that responsibility starts with resilience. Rather than trying to anticipate every possible threat, the focus is on ensuring the business can continue operating through disruption.

Roland shares, "We have to start with resilience, how do we help the business maintain a minimum viable company, and how do we help ourselves maintain a minimum defensible company?"

This foundation on resilience, awareness of the threat landscape, and strong teams remains critical. But how organizations achieve it is being rapidly reshaped by AI.

AI DRIVING VISIBILITY AND BETTER DECISIONS

For Roland, one of the most immediate impacts of AI is the ability to gain deeper visibility into complex environments.

"The ability to apply generative AI and LLMs and getting information to make smarter, better decisions is going to give us such amazing transparency," he says.

This shift is not limited to one function. It extends across risk, compliance, and control validation, fundamentally improving how security teams understand their environments and prioritize action.

"It's going to be amazing, and almost every major program in stacks are going to benefit from it."

By accelerating how information is gathered and interpreted, AI is enabling faster, more informed decision making across the board.

FROM RESPONSE TO AUTO-REMEDIATION

Beyond visibility, AI is also transforming how organizations respond to threats.

"We have an opportunity today to stop malicious activity before it happens, and revert to last known good instead of having to perform incident response," Roland explains.

This would mark a shift from lengthy investigations and recovery cycles toward faster, more automated responses.

"There's going to be some new defense and auto remediation capabilities that we wouldn't have even imagined two years ago."

As these capabilities mature, they will significantly reduce both the time and effort required to manage security incidents.

SECURING AI-DRIVEN DEVELOPMENT

AI is also accelerating how software is built, creating new challenges for security teams.

"We have machine generated code that is coming at us in waves. To keep pace, organizations must rethink how they approach application security. We have to apply a new capability to consume all of that information, ensure that it's secure code, and do it at the speed that our business is building it," Roland says.

This creates an opportunity to embed security directly into development processes.

"We'll be able to implement guardrails automatically and actually be better and more secure because we can keep up with the speed of development."

EXPANDING THE ROLE OF THE CISO

As AI adoption accelerates, expectations of security leaders are expanding as well.

"CISOs have three jobs when it comes to AI," Roland explains. "One is to enable the company to run fast with AI. The second is to protect against new AI attacks. And the third is to be better business owners."

The first responsibility of enablement marks a significant shift. Security is no longer just protecting the organization, but actively supporting innovation. However, at the same time, adversaries are evolving quickly.

Roland notes that this requires organizations to continuously adapt their defenses while also improving how security teams operate as part of the broader business.

REDEFINING SECURITY TEAMS AND WORK

AI is also reshaping how security teams are structured and where human effort is applied.

"How do I reduce the number of people in my SOC by letting tier one and tier two work be done by AI?" Roland asks.

Instead of eliminating roles, organizations are shifting focus toward higher-value work.

"What I need is a human in the loop to validate the output, help prioritize, and integrate with the business. In areas like compliance and risk, this shift is already underway. I can do your compliance automatically and don't need six people collecting information. I can press a button and do it now," comments Roland.

This allows teams to focus more on strategy and decision making, rather than manual processes.

LOOKING AHEAD

As organizations continue to adopt AI at scale, Roland sees the next year as a period of rapid transformation. Security leaders will need to move faster and rethink how their teams and technologies operate.

At the same time, the fundamentals remain unchanged. Resilience and strong decision making will continue to define effective programs.

In Roland's view, the organizations that succeed will be those that embrace AI thoughtfully, using it to enhance, not replace, human judgment, while maintaining the discipline needed to protect the business in an increasingly complex environment.

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

617.860.6485
KLOGIXSECURITY.COM

FEATS OF STRENGTH