2026 ANNUAL STATE
OF SASE + AI REPORT

VERSA

The Cost of Complexity

Executive summary

For decades, enterprise networking and security evolved along parallel tracks, accumulating separate tools, vendors, priorities, and ways of working. This fragmented approach may have been tolerable when the pace of change was slower, but AI has changed the calculus entirely.

As AI accelerates the speed, scale, and sophistication of both business operations and cyber threats, what was once a manageable inefficiency has become a structural liability. We can call this liability the “complexity tax”: the measurable cost enterprises pay every day for running fragmented, siloed networking and security environments.

Versa’s inaugural annual State of SASE + AI Report illuminates how the complexity tax is playing out across every dimension of the enterprise, from cost overruns to security exposure to stalled innovation. The findings are based on a survey of 525 senior IT and security decision-makers at organizations with 1,000 or more employees.

Collectively, these IT leaders’ responses reveal that the burden of complexity is tangible, widespread, and fundamentally unsustainable. The numbers tell the story. More than half of organizations (53%) are absorbing higher operational costs from redundant tooling, 73% have lost critical project time to integration failures, and 35% have paid the steepest price of all: a security breach caused or worsened by poor coordination between networking and security teams. Taken together, these aren't isolated inefficiencies but the compounding costs of a structural problem.

AI is turning a chronic problem into an acute one. Among our respondents, 95% say AI is forcing their networking and security teams to collaborate more closely. That process is exposing organizational and architectural gaps that have gone unaddressed for years, as human organizational dynamics intersect with the mounting weight of fragmented technology decisions.

Encouragingly, most organizations are not standing still. Nearly all respondents (99%) have already identified convergence as a strategic priority, and many are actively restructuring how networking and security teams collaborate. While the route is not simple, the direction of travel is clear.

Key insights from IT & security leaders

Security breaches

35% of organizations **suffered a security breach** in the past year that was caused or worsened by poor coordination between networking and security teams.

Rising costs

53% report **higher operational costs** from managing redundant and overlapping networking and security tools.

Project delays

73% say the **technical complexity of integrating new solutions** has caused a critical project to be delayed or unsuccessful in the past year.

The human factor

64% say **conflicting priorities between different teams** have caused projects to fail or stall during the past year.

AI as a forcing function

95% agree that **the rise of AI** is forcing their networking and security teams to collaborate more closely.

Moving toward convergence

99% say that **moving to a more converged, unified networking and security model** is a recognized organizational goal.

Planning purgatory

76% of **organizations in the planning phase** have had critical projects delayed or derailed by budget disagreements between networking and security teams.

Strengthening security

58% of organizations **cite strengthening security posture as a top driver of convergence**, nearly three times as many cite lowering total cost of ownership (19%).

01

The complexity tax

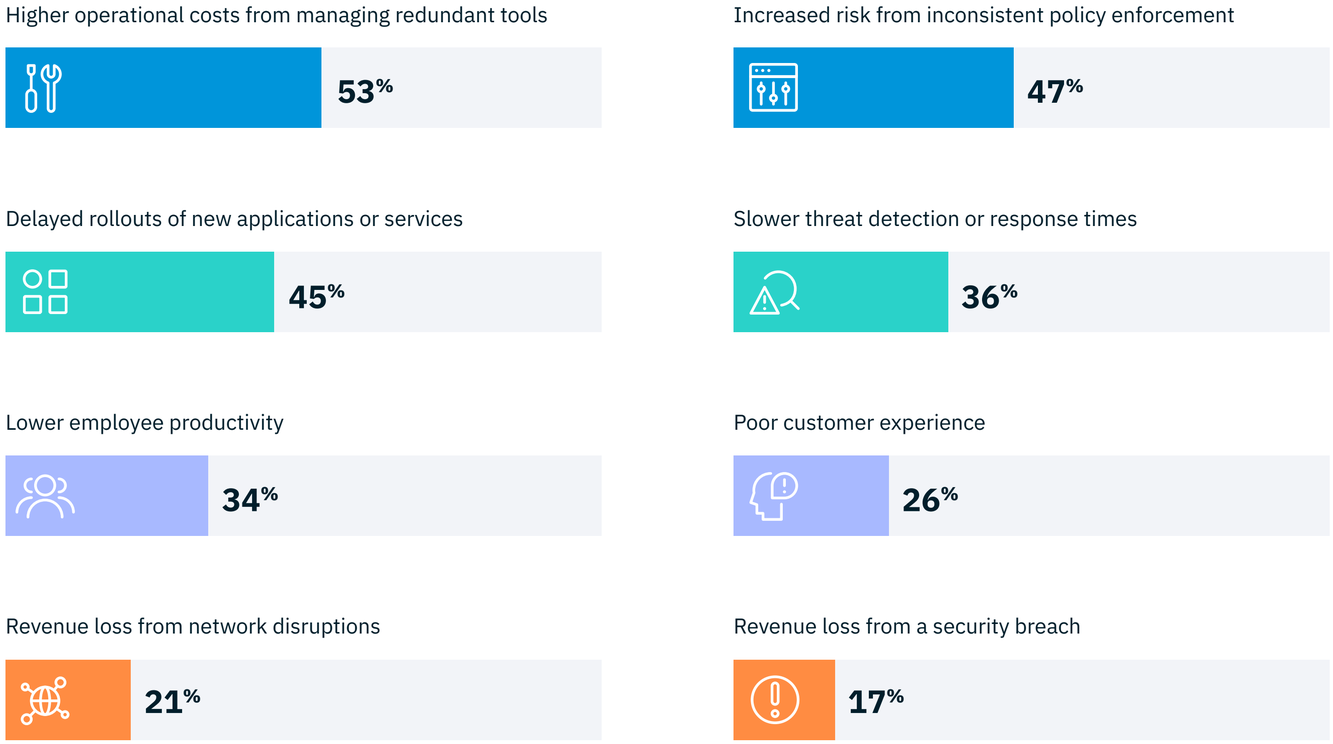
What fragmentation is actually costing enterprises

The complexity tax shows up in every layer of the enterprise, from budget lines consumed by redundant tools to security incidents exacerbated by poor coordination to product launches that fall victim to organizational gridlock. It also takes a human toll, felt by employees who can't get access to the tools they need to do their jobs and customers who encounter the latency and disruption that fragmented environments produce.

53% of senior leaders say they're incurring higher operational costs from managing redundant tools.

THE HIDDEN COSTS OF FRAGMENTATION

% of organizations reporting this impact in the past 12 months



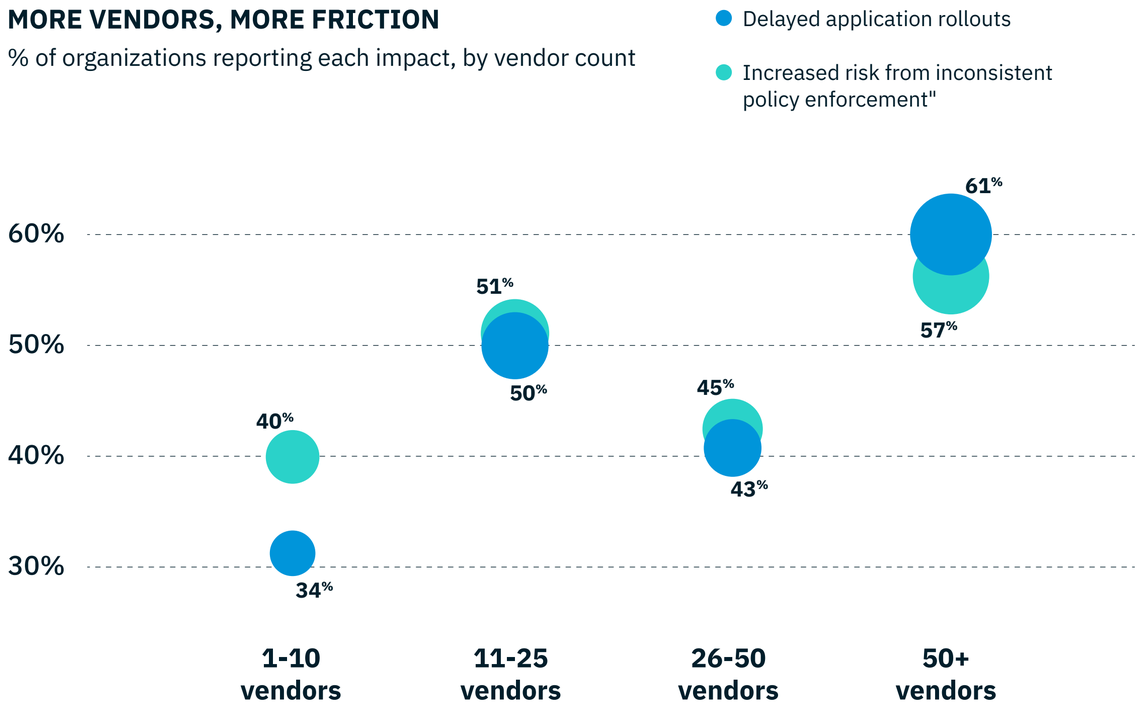
The vendor sprawl penalty

The data reveals a relationship between the number of vendors in an organization's environment and the severity of the business impacts it experiences.

Organizations juggling 50 or more vendors are nearly twice as likely to report delayed application rollouts as those with the leanest stacks (61% vs. 34%) and significantly more likely to report inconsistent policy enforcement (57% vs. 40%).

MORE VENDORS, MORE FRICTION

% of organizations reporting each impact, by vendor count



"Without security concerns holding us back, we could finally stop fighting fires and begin creating faster, more inventive products."

— C-LEVEL RESPONDENT

DIFFERENT SIZES, DIFFERENT PAIN POINTS

The complexity tax doesn't hit every organization the same way. Size shapes where the pressure lands most.

52% of larger enterprises (10,000+ employees) report that complexity has **delayed the rollout of new applications or services**

56% of mid-sized enterprises (1,000-4,999 employees) report that **higher operational costs from managing redundant and overlapping tools**

02

Twin culprits

Technical debt & human dynamics

Behind the complexity tax are two interlinked forces, both with deep roots. One is technological: Years of piecemeal, best-of-breed vendor decisions have left organizations managing sprawling environments that were never designed to work as a whole. The second is human: Years of siloed decision-making have left teams with misaligned priorities, unclear ownership, and governance structures ill-suited to the collaborative orchestration that convergence requires.

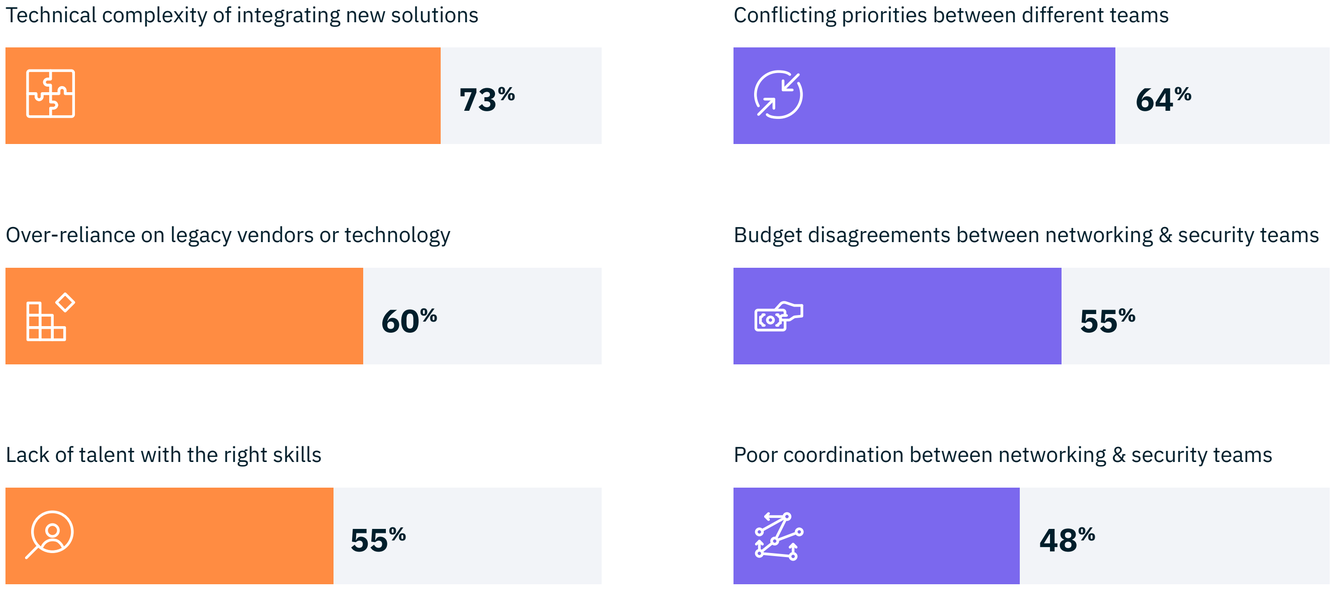
When we asked decision-makers what causes critical projects to fail, they pointed to both technological and human factors.

73% of organizations say that the technical complexity of integrating new solutions has delayed or derailed projects during the past year.

64% of organizations say projects have failed or stalled due to conflicting priorities between different teams.

WHAT'S DERAILING PROJECTS

Frequent or occasional cause of project delay or failure, past 12 months



Where technology & organizational dynamics collide

Legacy architecture makes organizational alignment harder because teams are managing incompatible systems with limited shared language. At the same time, siloed teams make modernization slower because no one owns the full picture. Breaking the cycle means addressing both simultaneously, not sequentially.

The weight of past decisions

AI is forcing organizations to reckon with the structural consequences of fragmented procurement decisions made over decades.

More than half of organizations (60%) cite over-reliance on legacy vendors as a cause of critical project failure.

Human friction

When projects collapse, technology isn't the only culprit. Competing priorities, misaligned budgets, poor coordination, and other organizational dynamics are often at play.

"The rapid adoption of generative AI and large language models requires secure, high-performance access to cloud resources while protecting sensitive data — forcing networking and security teams to collaborate on policy enforcement, traffic monitoring, and access controls in real time."

— VICE PRESIDENT RESPONDENT

The ownership dilemma

Clarity around SASE ownership remains elusive. While 43% of decision-makers believe ownership should sit with a joint committee, with equal representation from security and networking, only 30% have implemented shared ownership.

The C-suite disconnect

Where leaders stand on SASE ownership depends largely on where they sit. When asked who should own the SASE strategy, C-suite executives and directors land in different places. That distance in perspective has consequences for how decisions get made and how long they take.

C-level executives are more than twice as likely as directors to believe that SASE ownership should sit with executive leadership (53% vs. 20%).

Directors are more likely than their C-suite colleagues to favor a joint committee (45% vs. 29%).

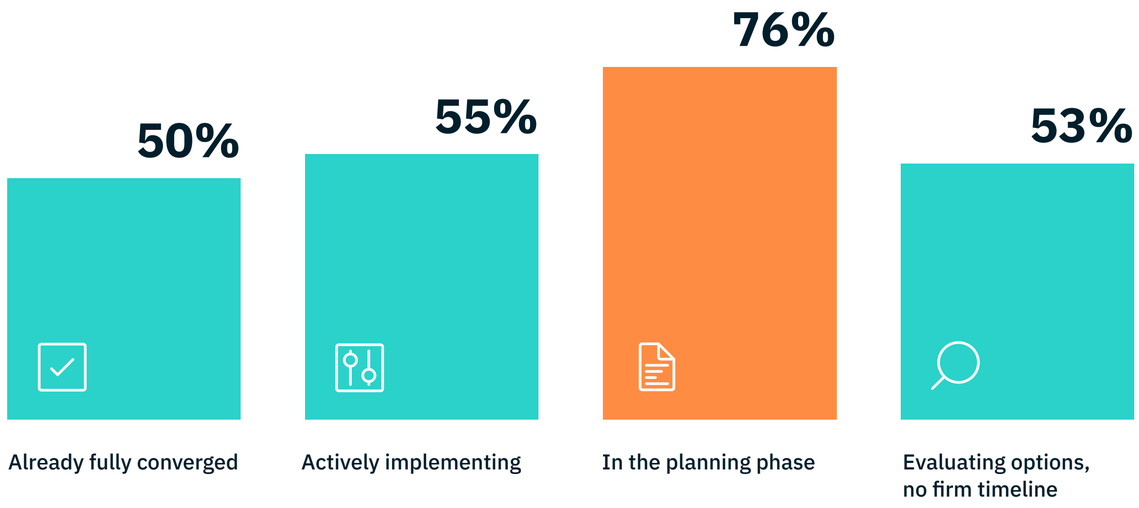
Planning purgatory

Internal conflict runs highest during the SASE planning phase, when organizations are making decisions that will shape their architecture for years. For teams accustomed to operating independently, planning demands something new: consensus on ownership, budget, and vendor strategy, all at once.

76% of organizations in the planning phase report frequent or occasional budget disagreements between networking and security teams.

BUDGET CONFLICT PEAKS AT THE PLANNING PHASE

% experiencing frequent or occasional budget disagreements, by SASE journey stage



03

The convergence challenge

If the complexity tax is the problem, convergence is nearly unanimously recognized as the solution. Almost every leader we surveyed (99%) says their organization has identified convergence as a recognized organizational goal, and 95% agree that AI is what's making that goal urgent.

The AI effect

When we asked leaders what single AI-driven change most requires collaboration, three clear themes emerged: AI is generating more traffic, enabling faster and more sophisticated attacks, and demanding a speed of response that neither team can deliver alone.

“The massive amount of new threat vectors created by AI has made it all but impossible for the two teams to not collaborate at this point. It was a problem we realized very early.”

— DIRECTOR

“AI tools require massive data access, cloud connectivity, APIs, and model integrations, which blurs the line between network performance and security risk.”

— C-LEVEL

“AI traffic is unpredictable, so networking and security teams have to work together to spot threats in real time.”

— DIRECTOR

“Risks are bleeding into the scope of both teams.”

— DIRECTOR

It’s not (just) about the money

Strengthening security posture (58%) and improving visibility and control (56%) lead the list, while only 19% cite cost savings. This signals that convergence is considered a strategic imperative rather than an incremental budget exercise.

WHY ORGANIZATIONS ARE PURSUING CONVERGENCE

% citing as a top-3 driver

What leaders say is in the way

Leading barriers to convergence include technical complexity and integration issues (55%) and skills gaps (45%). More than a third of organizations (35%) cite teams’ resistance to change as a significant barrier, a reminder that convergence is as much an organizational challenge as a technical one.

WHAT’S STANDING IN THE WAY OF CONVERGENCE

% citing a significant challenge to implementing a converged networking & security model

CONCLUSION

The path ahead

Most leaders have identified convergence as a strategic priority, named the barriers standing in the way, and in many cases begun the work. But the data in this report underscores the urgency of the challenge. AI is not waiting.

The speed at which AI is reshaping network architecture, generating new threat vectors, and blurring the boundaries between security and networking means that the timeline for convergence has compressed. Organizations that treat it as a multi-year background initiative are likely to find that the gap between where they are and where they need to be is widening faster than they can close it.

The leaders who navigate this next chapter successfully will simultaneously prioritize the human and technical dimensions of the challenge, recognizing that progress on one without the other rarely holds. From this foundation, they can move swiftly to establish clear ownership, consolidate the vendor environment, and create the cross-functional structures that allow networking and security to operate as one.

We asked leaders to imagine how a perfectly converged networking and security model would impact their business. Here's what they said.

"It would dramatically reduce risk while accelerating innovation, giving the business faster, safer access to data, simplified operations, lower costs, and greater confidence deploying new digital initiatives."

— DIRECTOR

"The biggest impact would be unprecedented operational agility. By eliminating the silos between networking and security, we move from a reactive posture to a proactive one."

— VICE PRESIDENT

"We would spend less time fighting fires and more time driving innovation and supporting business growth."

— DIRECTOR

"The achievement of real-time autonomous resilience, where AI can detect and stop threats instantly across our global network without impacting user performance or requiring manual coordination."

— DIRECTOR

The complexity tax is not a fixed cost. For organizations that make convergence a reality, AI moves from a source of exposure to a source of competitive advantage.

“The complexity tax has been hiding in plain sight for a decade. The good news is that leaders now see the problem clearly: 99% have named convergence a strategic priority. The work ahead is to bring teams and technology together to execute.”

— KELLY AHUJA, CEO, VERSA

METHODOLOGY

The 2026 Annual State of SASE + AI Report is published by Versa. This is the inaugural edition of an annual benchmark series. This report is based on a survey, conducted in March 2026, of 525 senior IT and security decision-makers in the United States. All respondents hold titles of Director or above — including C-level executives, Vice Presidents, Directors, and Network/Security Architects — at organizations with 1,000 or more employees. Respondents span Financial Services, Retail & E-commerce, Energy/Oil & Gas, Manufacturing, Healthcare & Life Sciences, Technology/Media/Telecom, and Government & Public Sector.

ABOUT VERSA

Versa, the global leader in unified networking and security, enables organizations to create self-protecting networks that radically simplify and automate their network and security infrastructure. Powered by AI, the VersaONE Universal SASE Platform delivers converged SSE, SD-WAN, and SD-LAN solutions that protect data and defend against cyberthreats while providing a superior digital experience. Thousands of customers globally, with hundreds of thousands of sites and millions of users, trust Versa with their mission-critical networks and security. Versa is privately held and funded by investors such as Sequoia Capital, Mayfield, and BlackRock.

For more information, visit www.versa-networks.com and follow Versa on LinkedIn and X (Twitter) @versanetworks.