

Governing Hybrid Enterprises

Visibility, Automation, Compliance, and Spending Across Application Networks

An AlgoSec report

TABLE OF CONTENTS

INTRODUCTION 3

VISIBILITY 4

- The visibility gap is structural 4
- Tool proliferation without unified coverage 5
- Applications changed the visibility problem 6
- What attackers see that defenders miss 7

COMPLIANCE 8

- Compliance has become a continuous operational requirement 8
- Configuration drift is the compliance gap nobody sees coming 9
- Third-party dependencies are a compliance blind spot 10
- Zero trust intent is high, but compliance reality is not 11

AUTOMATION 12

- Automation is a governance tool, not an efficiency tool 12
- Where automation creates governance value 13
- The consolidation shift is enabling governed automation 14
- Where automation programs still fail 15

SPENDING 16

- The market is growing faster than governance 16
- Regulated industries are increasing security spend in direct response to incidents 17
- Where security budgets are actually going 18
- The cost of under-investment is now quantified 19

ABOUT ALGOSEC 20



INTRODUCTION

Regulated enterprises have been building hybrid infrastructure for years. Cloud platforms, on-premises data centers, SaaS applications, third-party APIs, and AI-enabled services now operate side by side as a single, permanently distributed estate. The architecture decisions that created this environment were made incrementally, driven by competitive pressure, modernization mandates, and the practical limits of what could realistically be migrated or replaced.

The result is an operating model that most security teams were not designed to govern. Environments change continuously. Applications span multiple infrastructures. Policies enforced in one domain drift in another. Third-party dependencies multiply faster than they are mapped. And regulators through DORA, NIS2, and sector-specific frameworks are now demanding continuous, demonstrable evidence of control rather than periodic documentation of intent.

This report examines four dimensions where the governance gap is widest and the operational stakes are highest: visibility, compliance, automation, and spending. Each section draws on primary research, industry surveys, and incident data to show where regulated enterprises stand today, where the gaps are costing them most, and what the organizations closing those gaps are doing differently.

The central argument is straightforward. Hybrid infrastructure is permanent. Governing it properly is now a financial and regulatory imperative, and the cost of doing so is measurably lower than the cost of not.

The visibility gap is structural

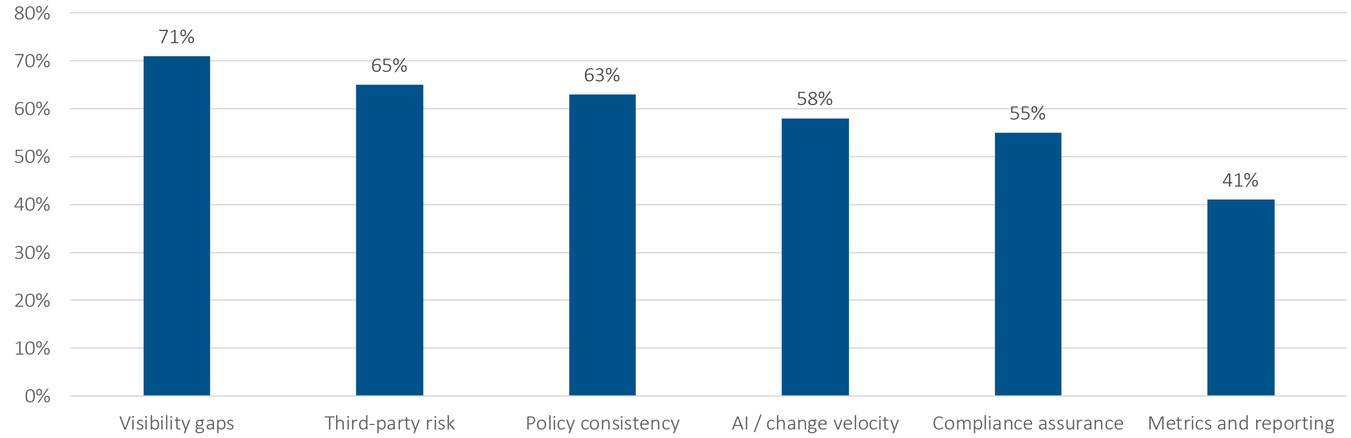
Security teams in regulated enterprises have more monitoring tools than ever before. They can inventory cloud assets, review firewall rules, track endpoint activity, and observe network traffic within defined domains. That level of domain visibility is mature, widespread, and insufficient.

The governance problem in hybrid application environments is not domain visibility. It is contextual visibility: the ability to understand how applications, connectivity paths, policies, ownership, and compliance obligations link together across cloud and on-premises infrastructure simultaneously. Without that chain of understanding, security teams are managing parts of an environment they cannot see as a whole.

According to the AlgoSec State of Network Security 2026, based on responses from 504 security, network, and cloud professionals across 28 countries, 71% of security teams report persistent visibility gaps as their primary governance challenge. [1] The Gigamon 2025 Hybrid Cloud Security Survey, drawing on more than 1,000 security leaders, found that 91% reported their visibility had been compromised in hybrid cloud environments over the prior 12 months. Not reduced. Compromised. [2] 48% of those respondents reported insufficient east-west traffic visibility, meaning they cannot adequately inspect lateral movement between applications and environments. [2]

Top hybrid governance gaps reported by security teams

Source: AlgoSec State of Network Security 2026 [1]



[1] AlgoSec, State of Network Security 2026. Survey of 504 professionals across 28 countries, conducted H2 2025.

[2] Gigamon, 2025 Hybrid Cloud Security Survey. Survey of 1,000+ security leaders.

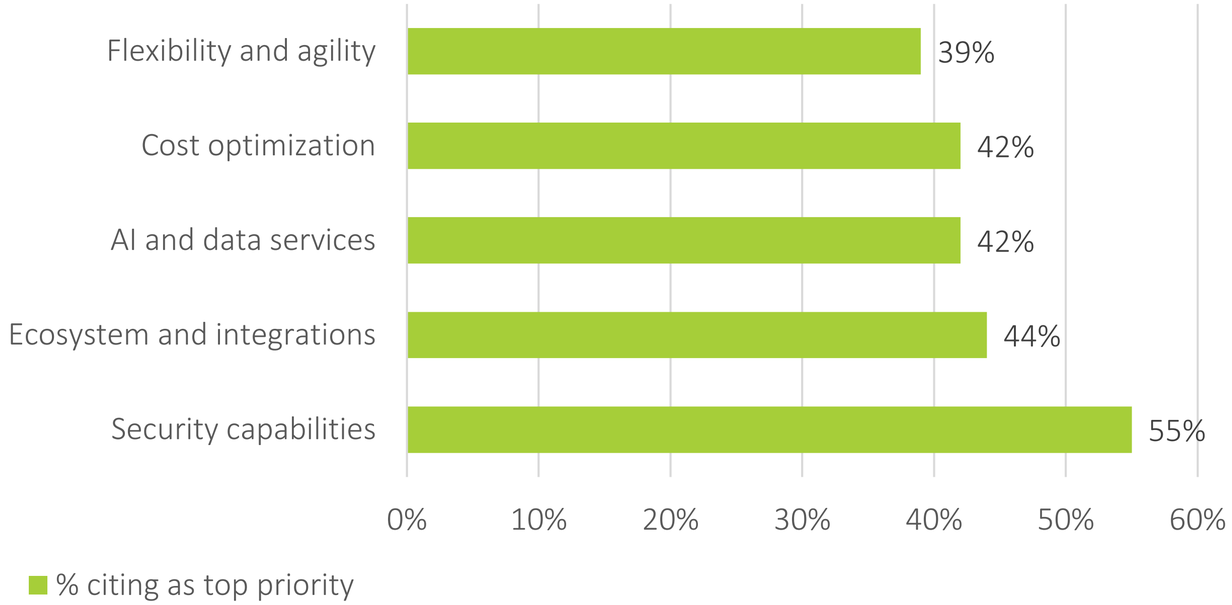
Tool proliferation without unified coverage

Organizations are not short of security products. The problem is that those products were built for individual environments, not for hybrid application estates. According to Enterprise Strategy Group research, when looking only at public cloud infrastructure, most organizations already use multiple overlapping tools: CSP network firewalls (79%), CSP security groups (68%), third-party network firewalls (59%), proxies (34%), and microsegmentation tools (28%). [3]

The result is fragmented coverage with no unified picture of how application connectivity flows through it. In 2026, the AlgoSec State of Network Security report confirms the industry response: 75% of organizations have now consolidated at least some portion of their security tools or policies under a single platform or management layer. [1] 55% of companies now select cloud platforms primarily based on security capability, confirming that every infrastructure decision has become a security decision. [1] Gartner reported worldwide end-user spending on public cloud services reached $723.4 billion in 2025, up from $595.7 billion the prior year, with security ranking as the top selection criterion above cost, AI services, and ecosystem integrations. [4]

Tool proliferation without unified coverage

Source: AlgoSec State of Network Security 2026 [1]



[1] AlgoSec, State of Network Security 2026. Survey of 504 professionals across 28 countries, conducted H2 2025

[3] Enterprise Strategy Group / TechTarget, The Case for Convergence in Hybrid Multi-cloud, Application-centric Networks. John Grady, Principal Analyst. June 2025. Commissioned by AlgoSec

[4] Gartner, Worldwide Public Cloud End-User Spending Forecast, November 2024

Applications changed the visibility problem

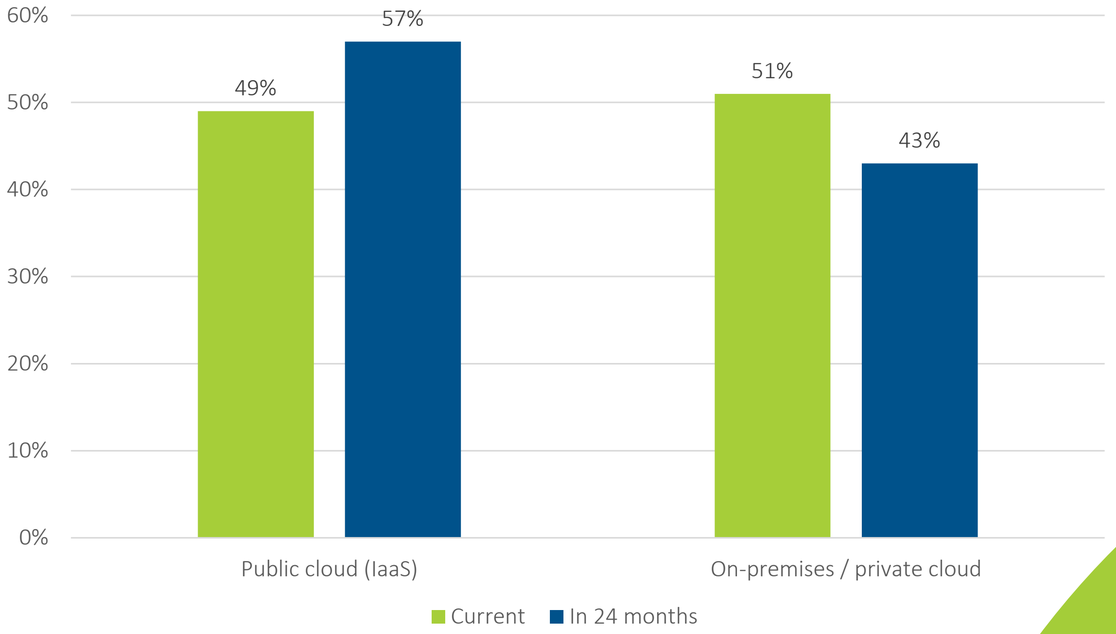
The scale of application environments compounds the problem. Enterprise Strategy Group research found that 60% of organizations are running at least 250 total production business applications, and 85% are using two or more cloud service providers. [3] At the same time, 43% of applications are expected to remain on-premises even as cloud adoption grows, meaning hybrid application estates are permanently split. [3]

A single business application may have its front end in public cloud, its data layer on-premises, its authentication through a SaaS provider, and its integrations through third-party APIs. Securing it requires understanding every connectivity path it touches across every environment it spans. Most security tools were not designed around that model. They were designed around infrastructure: devices, rules, ports, IP addresses. As Enterprise Strategy Group notes, that approach made sense when applications were monolithic and centralized. As applications have become distributed and hybrid, port and protocol visibility no longer captures what security teams need to govern. [3]

The 2026 data reflects how this is reshaping priorities. For the first time, maintaining consistent policies across on-premises and cloud environments (58.6%) has overtaken lack of visibility into cloud applications (54.3%) as the top cloud security challenge. [1] Private cloud also rose to third position among the most-used cloud platforms in 2026, up from further down the rankings, as enterprises seek greater control and data sovereignty alongside public cloud deployments. [1]

Application hosting split, current vs. 24 months

Source: Enterprise Strategy Group, The Case for Convergence in Hybrid Multi-cloud Networks, June 2025 [3]



[1] AlgoSec, State of Network Security 2026. Survey of 504 professionals across 28 countries, conducted H2 2025

[3] Enterprise Strategy Group / TechTarget, The Case for Convergence in Hybrid Multi-cloud, Application-centric Networks. John Grady, Principal Analyst. June 2025. Commissioned by AlgoSec

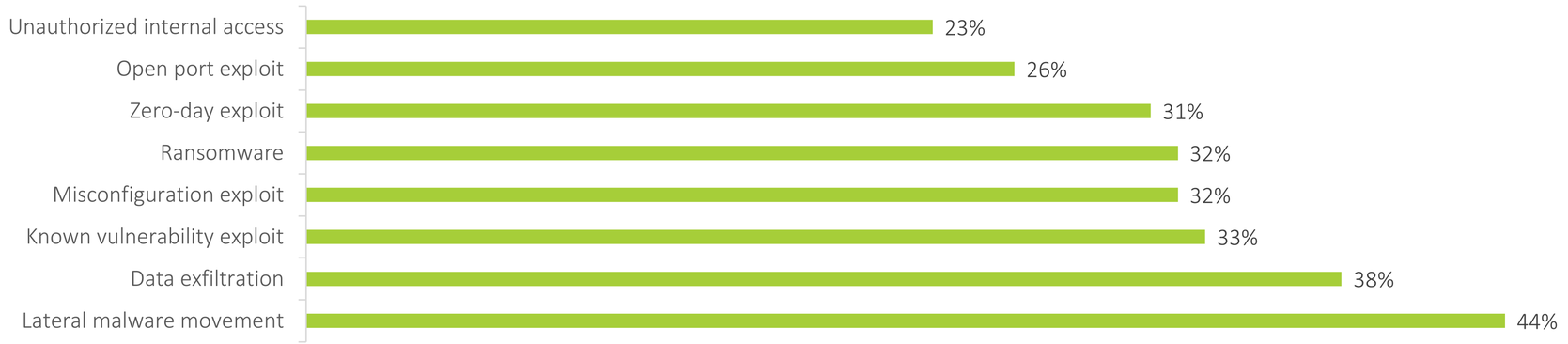
What attackers see that defenders miss

The east-west visibility gap is where the threat consequence becomes concrete. Attackers operating inside hybrid environments move laterally, exploiting application connectivity paths that security teams cannot observe. According to Enterprise Strategy Group research, the most common attack type reported against public cloud infrastructure was malware moving laterally from other parts of the environment, cited by 44% of organizations that experienced a breach. Data exfiltration followed at 38%, and exploitation of misconfigurations at 32%. [3]

The threat landscape intensified further in 2025 and into 2026. CVE disclosures increased 16% from H1 2024 to H1 2025, with 161 vulnerabilities actively exploited in that period alone. [5] Phishing attacks have surged 1,200% since generative AI went mainstream in 2022, while more than 90% of defensive AI capabilities are being outsourced to third parties, creating new dependency and visibility risks. [6] The Gigamon 2025 Hybrid Cloud Security Survey found that 55% of organizations experienced a breach in the prior 12 months, and 50% said their own tools failed to detect it. [2] In regulated industries, healthcare breaches average $9.77 million and financial services breaches average $6.08 million per incident. [7] In the most severe cases, such as the February 2024 ransomware attack on Change Healthcare, a single governance failure cost UnitedHealth Group over $1.6 billion and disrupted claims processing for thousands of providers nationwide. [8]

Attack types experienced on public cloud infrastructure

Source: Enterprise Strategy Group, The Case for Convergence in Hybrid Multi-cloud Networks, June 2025 [3]



[3] Enterprise Strategy Group / TechTarget, The Case for Convergence in Hybrid Multi-cloud, Application-centric Networks. John Grady, Principal Analyst. June 2025. Commissioned by AlgoSec

[5] Recorded Future, H1 2025 Malware and Vulnerability Trends Report

[6] McKinsey, AI Is the Greatest Threat and Defense in Cybersecurity Today, 2025

[7] IBM, Cost of a Data Breach Report 2024

[8] UnitedHealth Group, Q1 2025 Earnings Disclosure; Reuters, “UnitedHealth projects $1.6 billion hit from Change Healthcare cyberattack,” April 2024

Compliance has become a continuous operational requirement

Traditional compliance models were built for stable environments. Annual assessments, quarterly audits, point-in-time certification cycles these frameworks assumed infrastructure that changed slowly and predictably. Hybrid application environments have made that assumption obsolete.

Environments now change continuously through cloud deployment pipelines, infrastructure-as-code updates, container orchestration, API integrations, and vendor-driven service modifications. According to research on automated compliance management in hybrid cloud architectures, a large regulated enterprise may execute thousands of change events per day across its estate. [1] Each one is a potential compliance event. None of them wait for the next audit cycle.

The regulatory response has been direct. DORA, which came into full effect across EU financial services in January 2025, and NIS2, which extended cyber resilience obligations across critical infrastructure sectors, both require organizations to demonstrate operational resilience continuously rather than document it periodically. [2] Under these frameworks, regulators do not accept a policy that was reviewed last quarter. They require evidence that controls performed across the actual change events, incidents, and operational conditions of the review period. That evidence only exists if compliance is embedded in operations, not conducted alongside them.

Shift in compliance model requirements under modern frameworks

Source: ISACA, DORA and NIS2 Connection Points and Key Differences, 2025 [2]

Compliance dimension	Legacy model	DORA / NIS2 model
Evidence standard	Documented policy	Demonstrated control
Review cadence	Annual / quarterly	Continuous
Scope	Internal systems	Internal + third parties
Accountability	Compliance team	Board level
Audit trigger	Scheduled	Event-driven

[1] Automated Compliance Management in Hybrid Cloud Architectures, peer-reviewed research, 2025

[2] ISACA, DORA and NIS2: Connection Points and Key Differences, 2025

Configuration drift is the compliance gap nobody sees coming

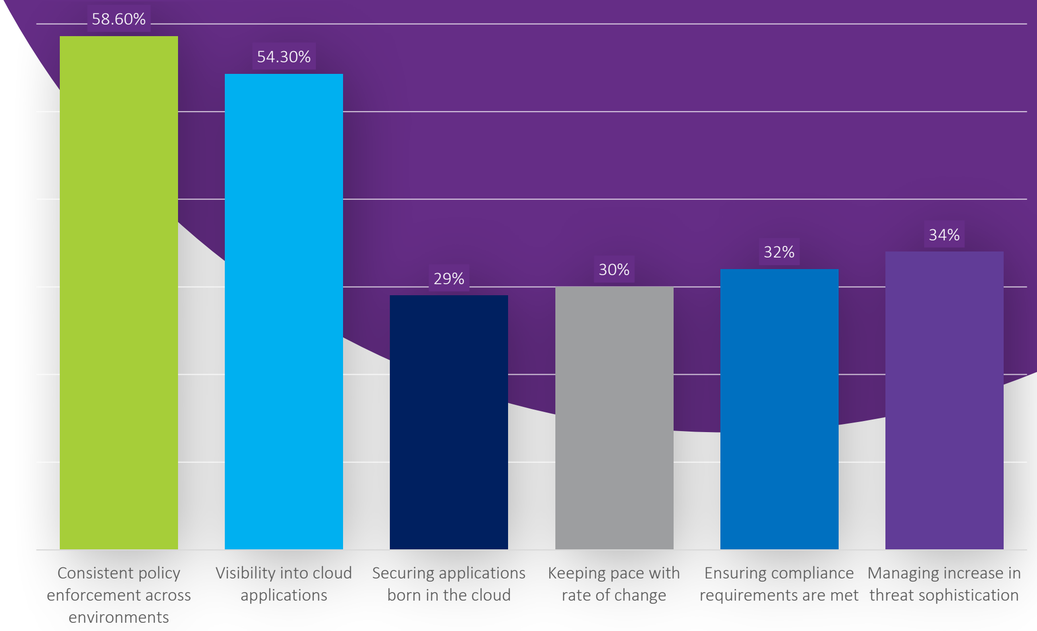
Even when controls are well designed at deployment, hybrid application environments erode them quietly. Repeated changes across SaaS platforms, cloud infrastructure, and network layers create divergence between approved configurations and actual configurations. There is no single failure event, just an accumulation of small differences, each individually justifiable, that collectively represent significant compliance exposure.

This is known as configuration drift, and it is one of the most underreported governance risks in regulated industries. According to research published in 2025, unaddressed configuration drift leads directly to security vulnerabilities, compliance failures, and operational disruption in multi-cloud and hybrid environments. [3] The AlgoSec State of Network Security 2026 confirms that policy consistency has overtaken visibility as the top reported cloud security challenge, with 58.6% of practitioners citing it as their primary operational problem. [4] That shift reflects the accumulated weight of configuration drift across estates that have been changing continuously for years without a unified enforcement model.

In banking, 6 in 10 financial institutions report that more than 25% of their workload now resides in the cloud, and 84% say cloud and edge computing are relevant to their business. [5] That scale of distributed infrastructure means configuration drift is not a niche risk. It is a daily operational condition that compliance programs were not designed to manage.

Top cloud security challenges reported by practitioners (2026)

Source: AlgoSec State of Network Security 2026 [4]; Enterprise Strategy Group, June 2025 [6]



[3] Hybrid Configuration Drift Management: Governance and Automation for On-Premise, Cloud, and Container Environments

[4] AlgoSec, State of Network Security 2026. Survey of 504 professionals across 28 countries, conducted H2 2025

[5] McKinsey and Institute of International Finance, Global Banking Annual Review, 2025

[6] Enterprise Strategy Group / TechTarget, The Case for Convergence in Hybrid Multi-cloud, Application-centric Networks. John Grady, Principal Analyst. June 2025.

Third-party dependencies are a compliance blind spot

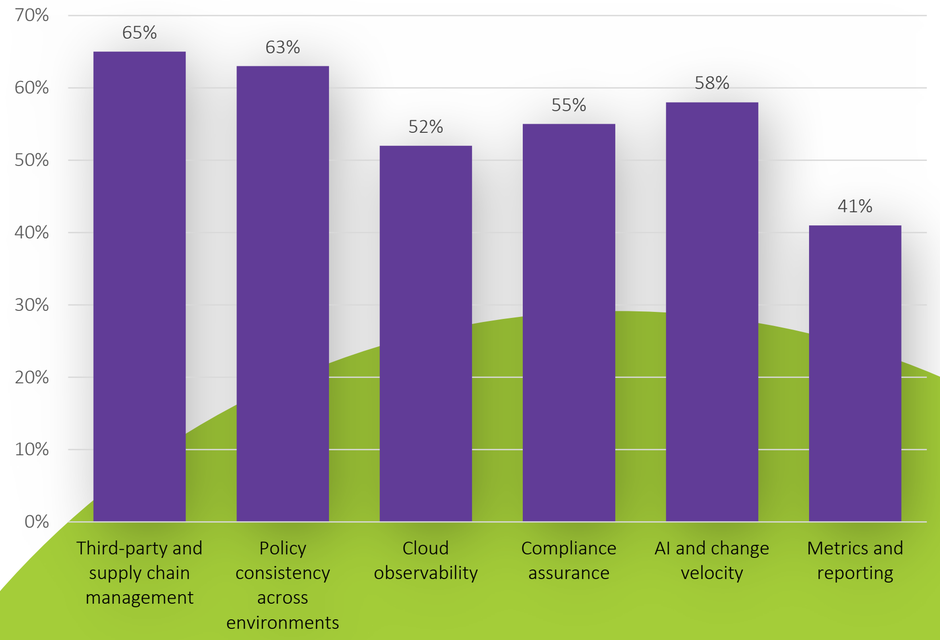
Regulated enterprises have extended their application estates well beyond their own infrastructure. Banking institutions depend on software vendors, managed service providers, payment processors, and open banking API partners. Healthcare organizations depend on electronic health record systems, medical device networks, pharmacy platforms, and clinical decision support tools most of which are externally provided and updated on vendor-controlled timelines.

According to McKinsey research cited in the AlgoSec 2026 State of Network Security report, 12% of data breaches across industries in 2023 occurred via attacks on third-party software vendors. [4] The AlgoSec State of Network Security 2026 survey found that 65% of security teams cite third-party and supply-chain management as a capability requiring significant improvement. [4] Supply chain attacks have simultaneously emerged as the most common cyberthreat category facing businesses, surpassing direct infrastructure attacks for the first time. [7]

Under DORA and NIS2, third-party oversight is a compliance obligation, not an operational preference. Financial institutions subject to DORA must maintain registers of third-party ICT providers, conduct risk assessments of critical dependencies, and demonstrate that their resilience posture accounts for supplier failure scenarios. [2] Most regulated enterprises have not yet built the application-level visibility required to satisfy those obligations, because they cannot fully map which applications depend on which third-party services and how those dependencies behave under stress.

Security capability gaps requiring improvement ranked by % of firms citing

Source: AlgoSec State of Network Security 2026 [4]



[2] ISACA, DORA and NIS2: Connection Points and Key Differences, 2025

[4] AlgoSec, State of Network Security 2026. Survey of 504 professionals across 28 countries, conducted H2 2025

[7] CrowdStrike / Verizon, Supply Chain Attack Threat Intelligence Summary, 2025

Zero trust intent is high, but compliance reality is not

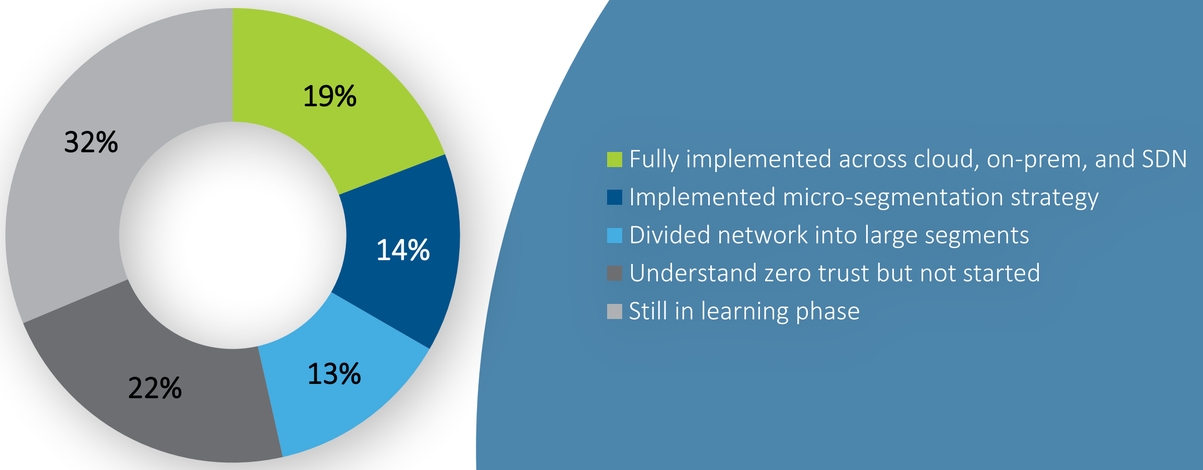
Zero trust has become the dominant compliance architecture reference in regulated industries. The principle of continuous verification, least-privilege access, and granular application-level controls aligns directly with what DORA, NIS2, and sector regulators require. The implementation reality, however, is significantly behind the intent.

The AlgoSec State of Network Security 2026 found that only 19% of organizations have fully implemented zero trust across cloud, on-premises, and SDN environments. [4] 31% are still in the learning phase, up from 20% the prior year, indicating that while more enterprises are engaging with the concept, fewer are moving to execution. [4] Gartner projects that by the end of 2026, only 10% of large enterprises will have a mature and measurable zero trust program in place. [9]

The gap between intent and implementation has direct compliance consequences. Organizations that report zero trust adoption to regulators but have not enforced it at the application connectivity level are carrying undocumented exposure. Emergency access exceptions, stale firewall rules, overly permissive cloud security groups, and unsegmented lateral paths all persist in environments that nominally operate under zero trust policies. According to the AlgoSec 2026 report, 65% of security teams report that AI investment in 2026 is focused on visibility and risk prioritization rather than threat response, precisely because the foundational compliance and policy layer remains unmapped. [4]

Zero trust implementation status (2026)

Source: AlgoSec State of Network Security 2026 [4]; Gartner, Zero Trust Maturity Forecast, January 2023 [9]



[4] AlgoSec, State of Network Security 2026. Survey of 504 professionals across 28 countries, conducted H2 2025

[9] Gartner, Predicts 2023: Zero Trust Will Be Tested, January 2023

Automation is a governance tool, not an efficiency tool

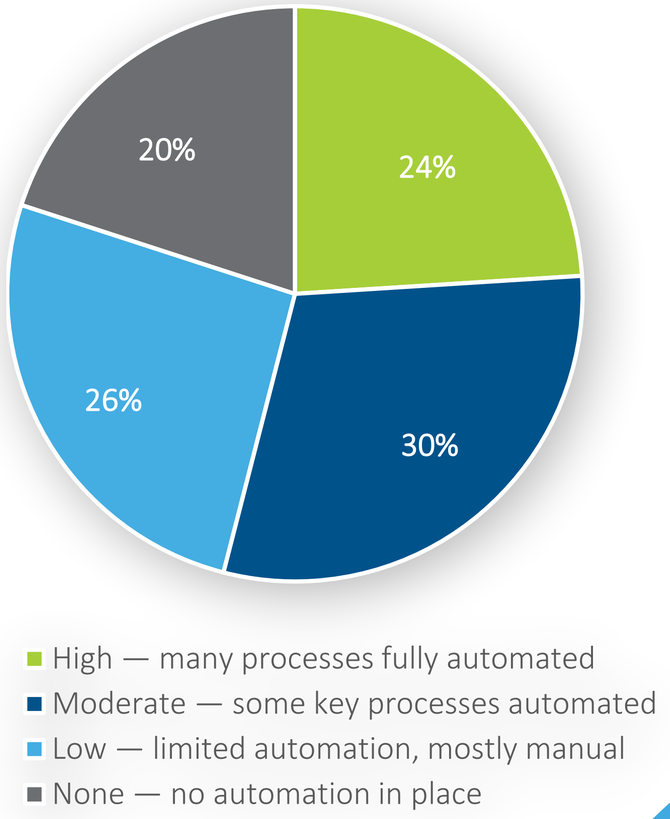
Automation in hybrid enterprises is routinely framed as a speed and cost problem. That framing leads organizations to implement it in the wrong place. The more consequential role of automation in regulated hybrid environments is governance at scale. Human workflows alone cannot keep pace with the volume of change introduced by cloud-native delivery, multi-environment networking, and continuous third-party integration.

The financial case for governance-driven automation is now quantified. According to the IBM Cost of a Data Breach Report 2024, organizations with extensive AI and security automation deployed saved an average of $2.22 million per breach compared to those without, and identified and contained breaches 108 days faster. [1] That gap is not explained by better threat detection alone. It reflects the difference between environments where policy is continuously validated and enforced, and environments where it is reviewed periodically and manually.

Despite this, automation maturity across the industry remains uneven. The AlgoSec State of Network Security 2026, based on responses from 504 professionals across 28 countries, found that 24% of organizations operate at a high level of automation, 30% at a moderate level, 26% at a low level, and 20% still rely primarily on manual processes. [2] Nearly half of all organizations have reached moderate to high automation levels, but the maturity gap between those using automation strategically and those applying it reactively remains wide.

Current automation maturity levels in network security management (2026)

Source: AlgoSec State of Network Security 2026 [2]



[1] IBM, Cost of a Data Breach Report 2024

[2] AlgoSec, State of Network Security 2026. Survey of 504 professionals across 28 countries, conducted H2 2025

Where automation creates governance value

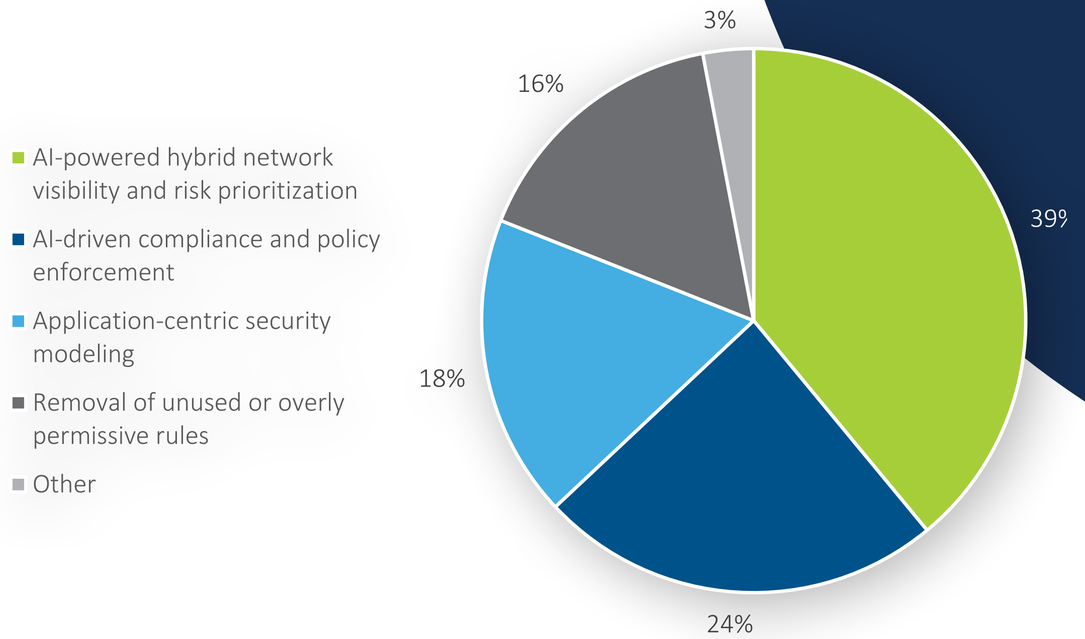
The governance value of automation is determined by its position in the change workflow. Organizations that have moved beyond task-layer automation provisioning, ticket execution, routine rule changes and embedded automation into policy validation, risk analysis, and compliance verification are seeing materially different outcomes.

Forrester Research found that organizations deploying automated policy management and change workflows reduced security-related operational costs by an average of 30% while simultaneously improving audit readiness and compliance reporting turnaround. [3] McKinsey's Global Banking Annual Review 2025 found that 80% of financial institutions consider applied AI and automation relevant to their business operations, and 37% plan to increase generative AI investment by more than 20% in the coming year, with governance and risk management cited among the primary use cases. [4]

The AlgoSec State of Network Security 2026 found that organizations are increasingly deploying automation for automated risk analysis, change verification, and compliance tracking areas previously dominated by manual oversight. [2] 39% of security teams cite AI-powered hybrid network visibility and risk prioritization as the use case with the greatest near-term impact, followed by AI-driven compliance and policy enforcement at 24%, and identification and removal of unused or overly permissive rules at 16%. [2]

AI and automation use cases with greatest impact over next 2 years

Source: AlgoSec State of Network Security 2026 [2]



[2] AlgoSec, State of Network Security 2026. Survey of 504 professionals across 28 countries, conducted H2 2025

[3] Forrester, "Security And Risk Leaders: Research, Guidance, And Tools," Forrester, accessed June 1, 2026.

[4] McKinsey, Global Banking Annual Review 2025

The consolidation shift is enabling governed automation

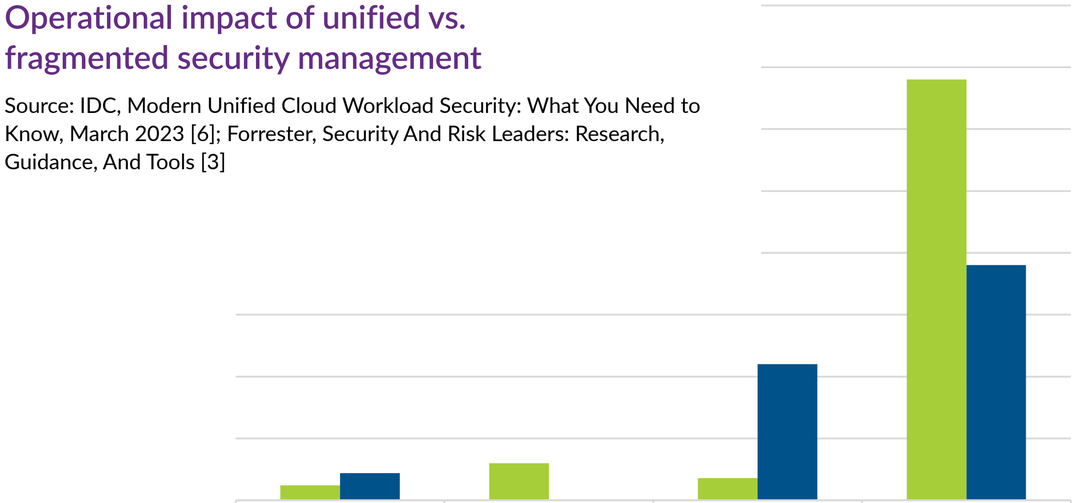
Effective governed automation requires a unified management layer. Organizations cannot automate policy enforcement across environments they cannot see coherently, and they cannot validate changes against compliance requirements using disconnected tools. The consolidation trend underway in 2026 is creating the operational foundation that governed automation depends on.

Gartner projects that by the end of 2026, 60% of new SD-WAN purchases will be part of a single-vendor SASE offering, up from 15% in 2022, reflecting consolidation at the network layer that directly enables unified automated policy enforcement. [5] At the platform level, the AlgoSec State of Network Security 2026 found that 75% of organizations have consolidated at least some security tools under a single management layer, with 10% achieving full consolidation. [2] At the team level, 36% of organizations report that cloud, network, and security teams now share tools, and 20% operate as fully consolidated teams. [2]

IDC research found that enterprises operating from a unified security management platform reduced mean time to remediate policy violations by 45% compared to those managing security across three or more disconnected tools. [6] This matters for automation because consolidation removes the fragmentation that causes automation programs to underperform. When cloud, network, and security teams operate from separate platforms, automation at the task layer scales those silos rather than bridging them.

Operational impact of unified vs. fragmented security management

Source: IDC, Modern Unified Cloud Workload Security: What You Need to Know, March 2023 [6]; Forrester, Security And Risk Leaders: Research, Guidance, And Tools [3]



	Mean time to remediate policy violations (by days)	Security operational cost reduction (by percentage)	Audit preparation time (by hours)	Policy violations identified per quarter (by count)
Unified platform	12	30	18	340
Fragmented tools (3+)	22	0	110	190

[2] AlgoSec, State of Network Security 2026. Survey of 504 professionals across 28 countries, conducted H2 2025

[3] Forrester, “Security And Risk Leaders: Research, Guidance, And Tools,” Forrester, accessed June 1, 2026

[5] Gartner, Analysis of Forces Reshaping the SD-WAN Landscape, 2025. Cited in Fierce Network

[6] IDC, Modern Unified Cloud Workload Security: What You Need to Know. March 2023

Where automation programs still fail

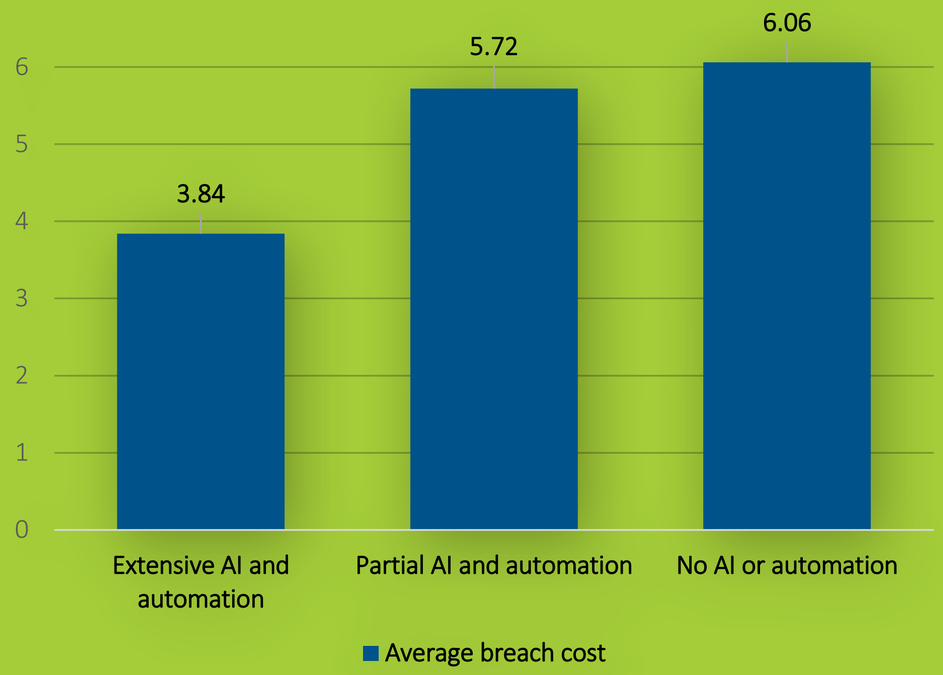
Despite measurable progress, significant barriers remain. Many organizations have implemented automation within specific domains cloud provisioning, firewall rule changes, ticket workflows without connecting those automations to a shared governance model. The result is automation without orchestration: individual workflows that move faster without improving oversight.

The Verizon 2024 Data Breach Investigations Report found that misconfiguration and errors remained one of the top root causes of breaches, present in 14% of all incidents analyzed, a figure that has remained stubbornly consistent across years, precisely because misconfiguration is a governance failure that speed alone does not fix. [7] In regulated industries, the risk of partial automation is not simply inefficiency. An automated process that executes changes without validating them against compliance requirements can produce audit gaps, policy drift, and configuration inconsistencies at machine speed.

According to a Ponemon Institute study, when cyber incidents disrupted healthcare workflows, 71% of affected organizations reported delays in procedures and tests that resulted in poor patient outcomes. [8] The healthcare sector's 75% increase in IT security spending following the Change Healthcare attack documented in Bain and KLAS Research reflects an industry that has absorbed the cost of under-governed automation and is now investing to close the gap. [9] Speed without governance does not reduce risk in regulated environments. It accelerates it.

Average breach cost by security automation level

Source: IBM, Cost of a Data Breach Report 2024 [1]



[7] Verizon, Data Breach Investigations Report 2024

[8] Ponemon Institute, Impact of Cyber Attacks on Patient Safety and Care Delivery, 2024

[9] Bain and KLAS Research, Healthcare Cybersecurity Investment Trends, 2025

The market is growing faster than governance

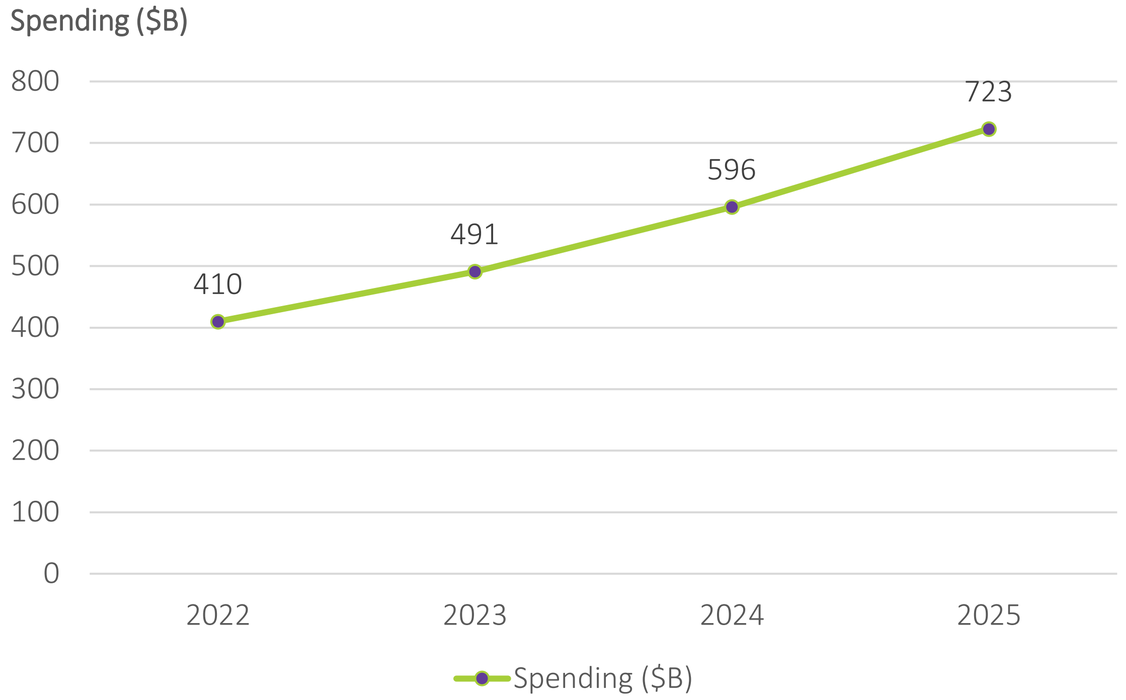
Hybrid infrastructure investment is accelerating across regulated industries, and the spending trajectory shows no signs of slowing. Gartner reported that worldwide end-user spending on public cloud services reached $723.4 billion in 2025, up from $595.7 billion in 2024, a 21% year-over-year increase. [1] The global hybrid cloud market, valued at $196 billion in 2025, is forecast to reach $578 billion by 2034, growing at a compound annual rate of 13 to 16%. [2]

What is notable about current spending patterns is that security has become the primary driver of infrastructure decisions, not cost or performance. The AlgoSec State of Network Security 2026 found that 55% of organizations now select cloud platforms primarily based on security capability the first time security has ranked above cost optimization, ecosystem integrations, and AI services as the top selection criterion. [3] Deloitte's 2024 findings corroborate this shift, confirming that security plays a major role in cloud investment decisions across enterprise segments. [4]

The challenge is that infrastructure spending and governance capability are not scaling at the same rate. Environments are expanding faster than the control models organizations use to manage them, creating a widening gap between what is deployed and what is governed.

Global public cloud end-user spending 2022 to 2025 ($B)

Source: Gartner, Worldwide Public Cloud End-User Spending Forecast, November 2024 [1]



[1] Gartner, Worldwide Public Cloud End-User Spending Forecast, November 2024

[2] Fortune Business Insights / MRFR, Hybrid Cloud Market Size and Forecast, 2025

[3] AlgoSec, State of Network Security 2026. Survey of 504 professionals across 28 countries, conducted H2 2025

[4] Deloitte, Security's Role in Cloud Investment Decisions, 2024

Regulated industries are increasing security spend in direct response to incidents

Spending patterns in banking and healthcare are being shaped as much by incident response as by modernization strategy. In healthcare, Bain and KLAS Research found that 75% of providers and payers increased IT spending over the past year, and 70% said they were directly affected by the Change Healthcare cyberattack. [5] Organizations are allocating greater cybersecurity spend as a direct response to that disruption, with the attack serving as a sector-wide forcing event that elevated governance investment from a strategic priority to an operational necessity.

In financial services, McKinsey's Global Banking Annual Review 2025 found that 6 in 10 financial institutions report more than 25% of their workload now resides in the cloud, and 57% of firms are concerned about keeping pace with emerging technologies. [6] 31% are not confident their current capabilities can mitigate the associated risks, despite significant ongoing investment. [6] The Institute of International Finance reports that financial services cybersecurity spending has grown consistently above sector GDP for three consecutive years, driven by regulatory pressure, incident response, and the expanding attack surface created by hybrid modernization. [7]

Healthcare IT and cybersecurity spending response post-Change Healthcare

Bain and KLAS Research, Healthcare Cybersecurity Investment Trends, 2025 [5]; McKinsey, 2025 [6]

Indicator	% of organizations
Increased IT spending over past year	75%
Directly affected by Change Healthcare attack	70%
Increased cybersecurity spend as direct response	60%
Reporting ransomware incidents nearly doubled vs. prior year	128% increase (YoY)

[5] Bain and KLAS Research, Healthcare Cybersecurity Investment Trends, 2025

[6] McKinsey, Global Banking Annual Review 2025

[7] Institute of International Finance, Financial Services Cybersecurity Spending Report, 2025

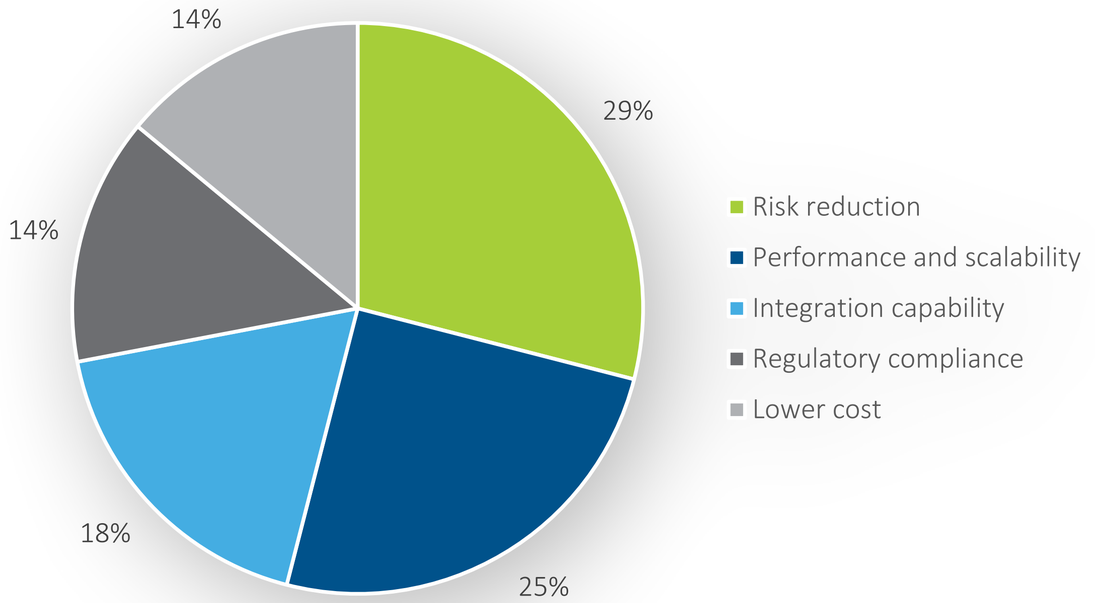
Where security budgets are actually going

Security spending in 2026 is concentrating around consolidation, visibility, and AI-assisted governance rather than point solutions. The AlgoSec State of Network Security 2026 found that risk reduction is the primary driver of security management solution selection at 29%, followed by performance and scalability at 25%, integration capability at 18%, regulatory compliance at 14%, and cost reduction at 14%. [3] That ranking signals a meaningful shift: buyers in regulated industries are prioritizing demonstrable risk reduction and integration over cost efficiency.

At the platform level, Palo Alto Networks and Fortinet have consolidated their positions as the top two enterprise firewall vendors in 2026, with both platforms gaining share on the basis of integrated security and networking rather than raw inspection performance. [3] The SASE market is projected by Gartner to grow at a CAGR of 26% between 2025 and 2028, exceeding $30 billion by the end of the decade, driven by enterprise demand for unified connectivity and security control. [8] IBM's $6.4 billion acquisition of HashiCorp in 2024 was explicitly framed around infrastructure automation and governance at scale, a strategic signal about where enterprise value is accruing in hybrid environments. [9]

Primary drivers for security management solution selection (2026)

Source: AlgoSec State of Network Security 2026 [3]



[3] AlgoSec, State of Network Security 2026. Survey of 504 professionals across 28 countries, conducted H2 2025

[8] Gartner, SASE Market Forecast and Growth Projections, 2025

[9] IBM, HashiCorp Acquisition Announcement, April 2024

The cost of under-investment is now quantified

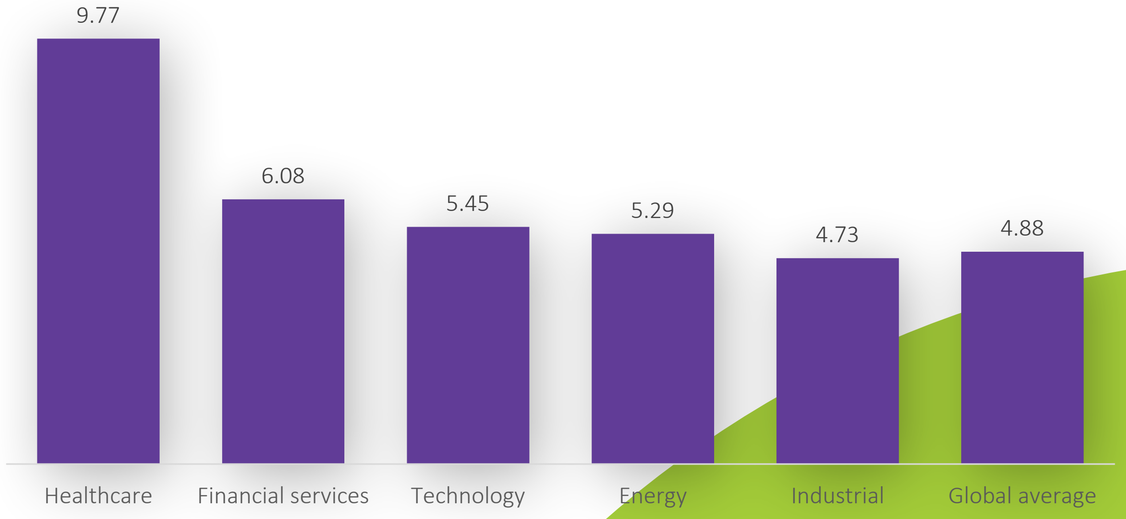
The financial consequence of governance under-investment in hybrid environments is no longer theoretical. The IBM Cost of a Data Breach Report 2024 found that the global average breach cost reached $4.88 million, the highest figure ever recorded and a 10% increase over 2023. [10] In financial services the average stands at $6.08 million, and in healthcare at $9.77 million figures that reflect not just remediation costs but regulatory penalties, operational disruption, and reputational damage. [10]

The Change Healthcare ransomware attack in February 2024 produced the most documented case of hybrid governance failure at scale. UnitedHealth Group reported $872 million in direct costs in Q1 2025 alone, with total projected losses exceeding $1.6 billion. [11] The attack disrupted claims processing for over 900 hospitals and 70,000 pharmacies across the United States, demonstrating that governance failures in interconnected hybrid application environments carry systemic, not just organizational, consequences. [11]

Against those figures, the $2.22 million average saving per breach for organizations with extensive security automation documented by IBM represents one of the clearest returns on governance investment available to security leaders making the case for budget. [10] The math is direct: the cost of governing hybrid environments properly is materially lower than the cost of governing them poorly.

Average breach cost by industry ($M, 2024)

Source: IBM, Cost of a Data Breach Report 2024 [10]



[10] IBM, Cost of a Data Breach Report 2024

[11] UnitedHealth Group, Q1 2025 Earnings Disclosure; Reuters, “UnitedHealth projects $1.6 billion hit from Change Healthcare cyberattack,” April 2024

ABOUT ALGOSEC

AlgoSec, a global cybersecurity leader, empowers organizations to securely accelerate application delivery up to 10 times faster by automating application connectivity and security policy across the hybrid network environment.

With two decades of expertise securing hybrid networks, over 2200 of the world's most complex organizations trust AlgoSec to help secure their most critical workloads.

AlgoSec Horizon platform utilizes advanced AI capabilities, enabling users to automatically discover and identify their business applications across multi-clouds, and remediate risks more effectively. It serves as a single source for visibility into security and compliance issues across the hybrid network environment, to ensure ongoing adherence to internet security standards, industry, and internal regulations.

Additionally, organizations can leverage intelligent change automation to streamline security change processes, thus improving security and agility.

Learn how AlgoSec enables application owners, information security experts, SecOps and cloud security teams to deploy business applications faster while maintaining security at www.algosec.com.

For more information, visit www.AlgoSec.com

algosec