2025 Cisco Cybersecurity Readiness Index

South Korea

Global Executive Summary

A few short years after Gen AI was introduced, artificial intelligence (AI) continues to change the tech industry at record speed, as businesses race to launch new technology and to meaningfully implement it as part of their IT strategies.

While AI brings promise of new possibilities, it also adds layers of complexity to an already complicated security landscape. It's challenging for companies to both embrace and secure AI. What's more, there's a disconnect between general understanding of the threats posed by AI and what it takes to secure organizations against those threats. Globally, nearly nine out of 10 (86%) business leaders with cybersecurity responsibilities reported at least one AI-related incident in the past 12 months. Just 48% believe that their employees understand how malicious actors are using AI to enhance their attacks. Under half (45%) feel their company has the internal resources and expertise to conduct comprehensive AI security assessments. However, only 10% consider AI to be the most challenging aspect of their security infrastructure to protect. As AI-enabled threats become increasingly sophisticated, these threats will only rise.

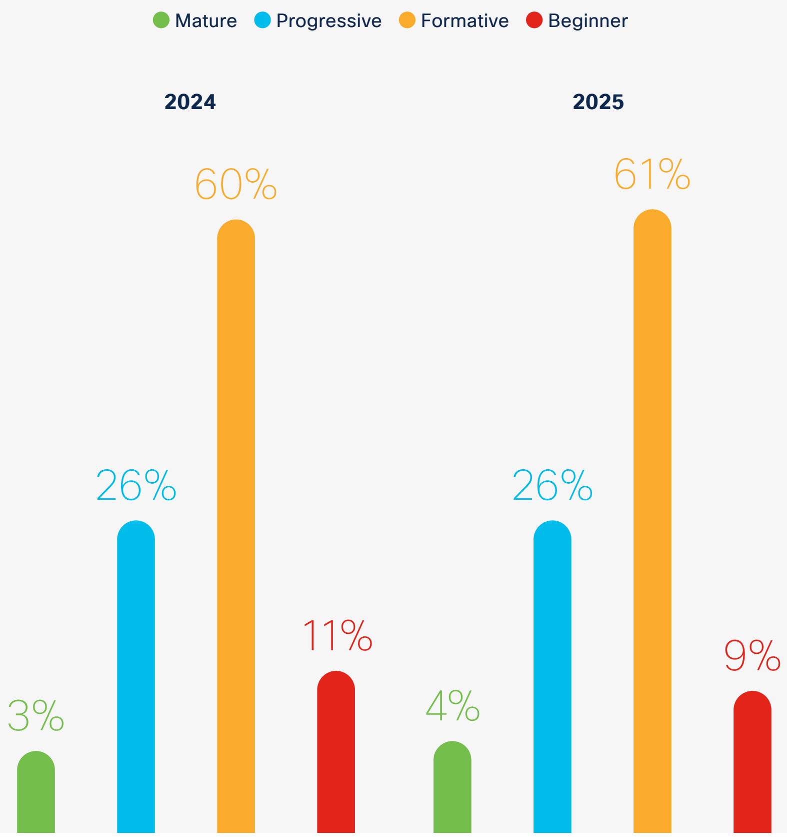
Cisco's third annual ***Cybersecurity Readiness Index*** is our updated guide that addresses the current global cybersecurity landscape and assesses how ready companies are to face today's cybersecurity risks. It is based on a double-blind survey of 8,000 businesses and cybersecurity leaders across 30 global markets. Respondents represent a broad range of private sector industries, including financial services, retail, technology services, and manufacturing.

The 2025 edition of this study shows that readiness remained flat from 2024. Based on five pillars of cybersecurity readiness that are most relevant to securing today's organizations – **Identity Intelligence**, **Machine Trustworthiness**, **Network Resilience**, **Cloud Reinforcement**, and **Artificial Intelligence (AI) Fortification**.

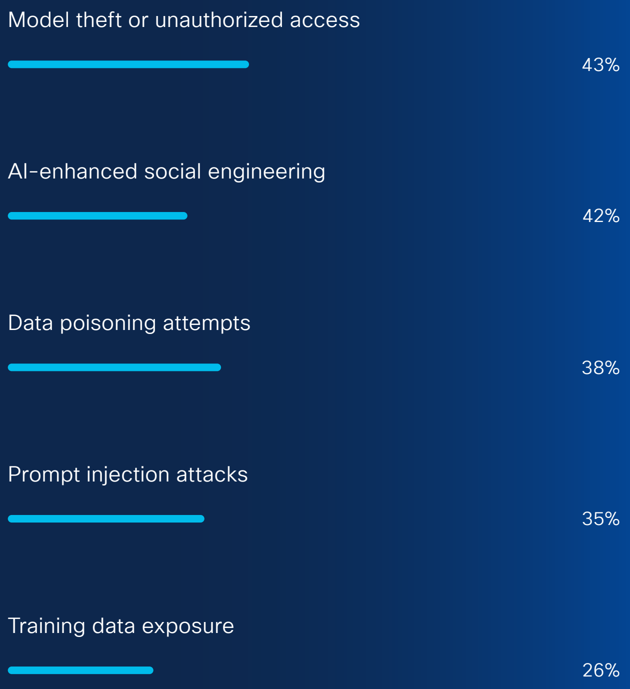
A mere four percent of companies globally (as opposed to three percent in 2023) reached the Mature stage of readiness. Alarmingly, nearly three quarters (70%) remain in the bottom two categories (Formative, 61% and Beginner, nine percent) – with little change from last year. As threats continue to evolve and multiply, companies need to enhance their preparedness at an accelerated pace to remain ahead of malicious actors.

In terms of the pillars of readiness, this year's results reflect that globally, the largest increase is in Machine Trustworthiness (12% Mature), which saw the most growth compared to seven percent in 2024. Conversely the report saw the lowest levels of maturity in AI Fortification (seven percent), Network Resilience (seven percent), Identity Intelligence (six percent), and Cloud Reinforcement (four percent), all trailing with single-digit performance.

Global Overall Readiness (YoY)



Types of AI-related security incidents companies experienced



Threats to AI systems and secure data processes remain a blind spot for many companies, despite an abundance of active and increasingly sophisticated attacks. Added to that is a general lack of employees' understanding of the security risks that come with using and developing AI applications.

Only 49% of respondents globally believe employees fully understand AI-related cybersecurity threats, which commonly take the form of model theft or unauthorized access, AI-enhanced social engineering, or data poisoning attempts.

This lack of understanding is overshadowed by the increasingly widespread adoption of AI, particularly Generative AI (GenAI). While half (51%) of companies require their employees (51%) to utilize approved third-party GenAI tools through a security service, nearly a quarter (22%) have unrestricted access to publicly available tools. This unrestricted access puts sensitive company data at serious risk and could lead employees to inadvertently propagate threats.

Regardless of how employees use AI at work, IT teams have limited visibility and control, with 60% saying they can't see specific prompts or requests made by employees using GenAI tools.

Unregulated AI deployments, or shadow AI, pose significant cybersecurity and data privacy risks, as it is hard for security teams to monitor and control what they can't see. 60% stated they lack confidence in their ability to identify the use of unapproved AI tools in their environments.

AI-related risks are further muddying waters in an already-complex operating environment involving hybrid workers, unmanaged devices, and solution sprawl. This builds the case for more action and investment.

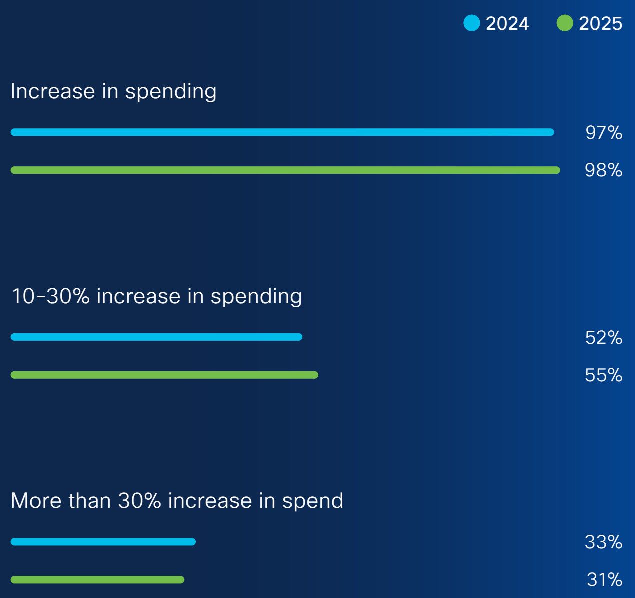
Globally, nearly half of respondents (49%) experienced at least one cyberattack within the past year, and nearly three quarters (71%) of those surveyed believe that a cybersecurity incident is likely to disrupt their organizations' business within the next 12 to 24 months. However, most companies remain underprepared to prevent or manage these threats, with cybersecurity readiness levels remaining essentially static in the past 12 months.

As many employees continue to follow a hybrid work structure, around one third of respondents (31%) report that on average, employees at their companies log in to six different networks per week to work, while 84% say employees access company networks from unmanaged devices.

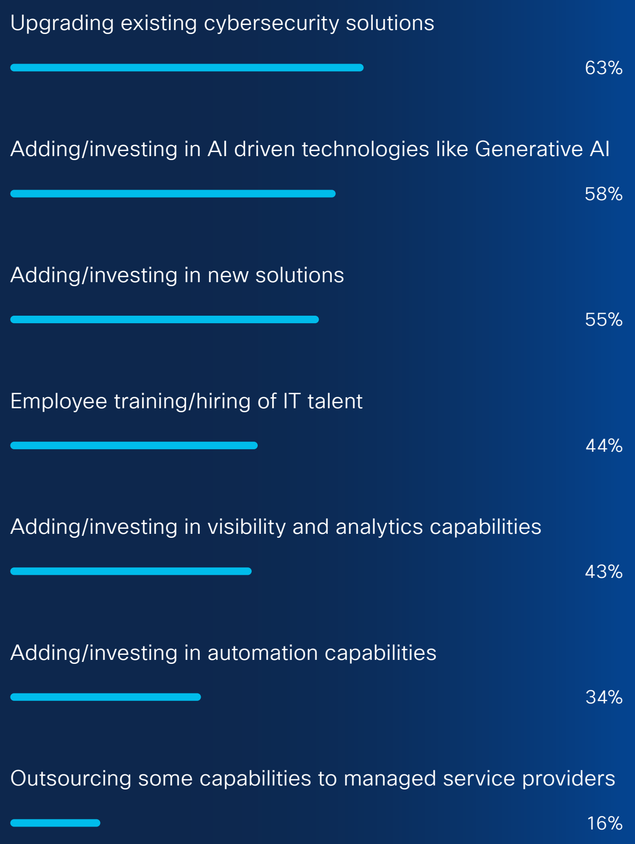
To make things more complicated, more than three quarters (77%) of respondents say that adopting too many cybersecurity solutions slowed down their team's ability to detect, respond, and recover from incidents they are trying to prevent. Seven in 10 (70%) say their companies have more than 10 point solutions in their security stack, with 26% admitting that they have more than 30.

As we've seen in our past reports, the talent shortage continues to be a barrier to cybersecurity readiness that slows how quickly solutions can be deployed. Globally, a large majority (86%) of respondents view a shortage of cybersecurity talent as a challenge, with 39% describing this as a significant challenge. Over

Planned increase in cybersecurity infrastructure spending



Planned security investments



half (53%) report having more than 10 cybersecurity positions to fill, and 88% say these roles account for over 10% of their team's headcount gap.

More positively, companies recognize the need for more investment in cybersecurity. Almost all (96%) respondents globally plan to upgrade or restructure their IT infrastructure within the next two years, the same number as in 2024. This may reflect an understanding that their infrastructure is currently falling short, with only 34% feeling very confident in the resilience of their company's current cybersecurity infrastructure against attacks.

Nine out of ten respondents said their company's cybersecurity budget has increased in the past 12 to 24 months. Of these, 93% reported increases of at least 10%, and nearly 30% saw increases of 30% or more. However, the pace of budget increases appears to be slowing as fewer respondents (87%) expect future increases to exceed 10%.

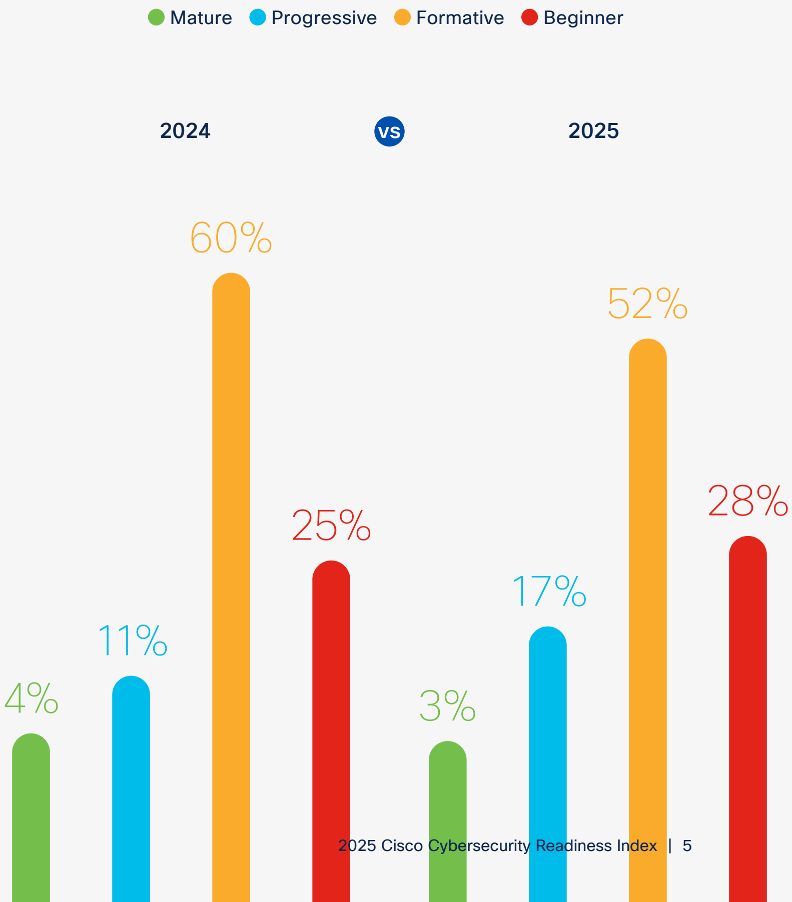
Even though cybersecurity budgets have increased for many, overall IT spend allocated to cybersecurity decreased, with only 45% of respondents saying their company allocates more than 10% of their IT budget to cybersecurity, compared to 53% in 2024. Increases in overall IT spend are outpacing growth in cybersecurity budgets, and unless these two are aligned, it will become harder to defend a growing IT infrastructure in an intensifying threat environment.

It is crucial that companies understand their cybersecurity readiness and acknowledge the pillars in which they fall short. By identifying weak spots, they can focus resources on improving those areas to better defend against increasing digital threats.

Extent of budget increase

	% among respondents reporting increase in past 12-24 months	% among respondents predicting increase in the next 12 months
Less than 10%	7%	13%
10 – 20%	32%	29%
21 – 30%	31%	27%
31 – 50%	19%	18%
51 – 75%	7%	8%
76 – 100%	3%	4%
More than 100%	1%	1%

South Korea Overall Readiness (YoY)



Identity Intelligence

Managing access to network and systems remains a critical priority amid an intensifying threat environment. Malicious actors are using ever more sophisticated means in their attempts to access networks, including AI-powered phishing and deepfakes, requiring responses that can verify identities quickly, accurately, and at scale.

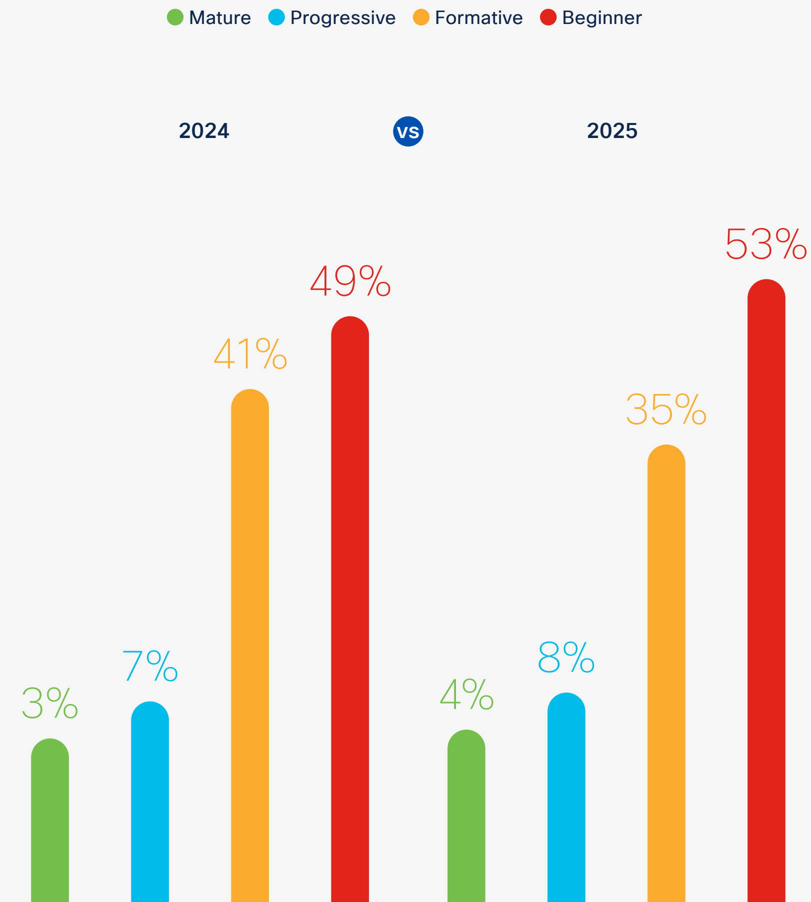
In 2025, Identity Intelligence readiness has slightly decreased in South Korea, with fewer companies moving from the Beginner to the Formative stage and achieving partial deployment. Just four percent of companies classified as Mature. This suggests that organizations are grappling with unexpected complexities or resource limitations in the final stages of implementation.

AI has proved to be a boon to practitioners seeking to bolster solutions to verify and secure identity. Of those companies in South Korea adopting Identity Intelligence solutions, 30% have significantly integrated AI into these capabilities.

The top two most adopted solutions for Identity Intelligence in South Korea are continuous risk-based access analytics (to spot identity anomalies) at 52% and real-time risk-based privilege access policies at 45%.

Identifying suspicious behavior and anomalies is becoming a key priority for companies in relation to Identity Intelligence. Almost a fifth (15%) of respondents in South Korea rank Identity as their company's top cybersecurity challenge.

Identity Intelligence Readiness



Machine Trustworthiness

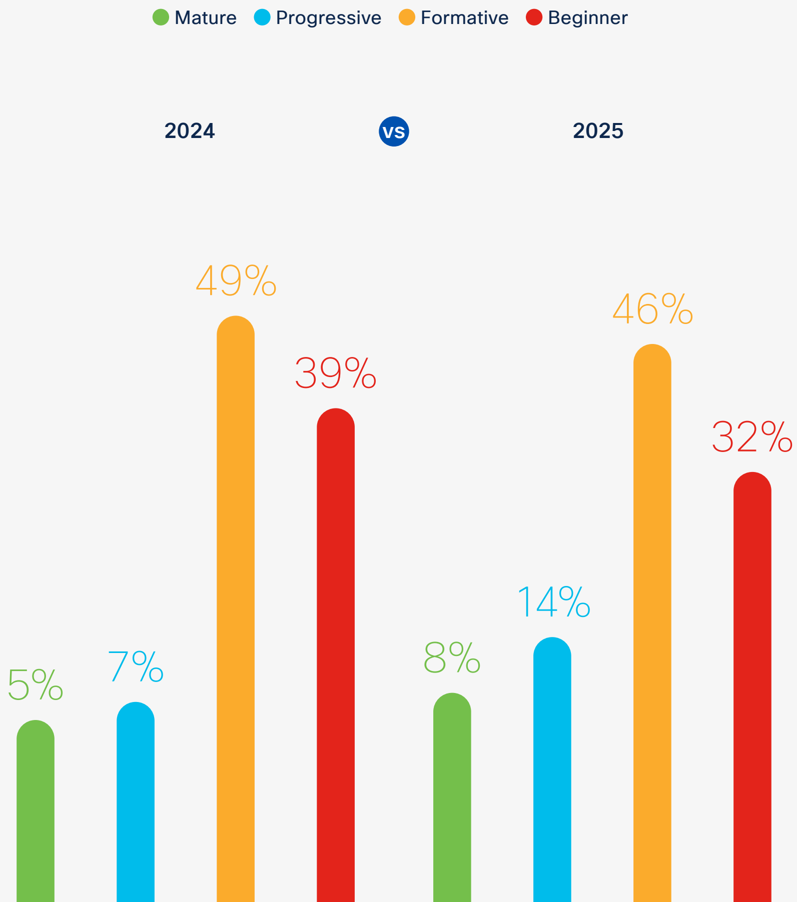
The ongoing prevalence of hybrid work continues to pose a challenge to machine integrity – employees are logging into company networks from a vast range of devices, many of which are unmanaged. Concurrently, a growing array of devices are connected to the internet, from everyday household items to industrial machinery. This Internet of Things (IoT) landscape significantly expands the attack surface for malicious actors.

In 2025, we observed a minor shift in how ready companies in South Korea are for Machine Trustworthiness, with a three percent increase in those reaching the Mature category. This suggests that some companies are progressing towards fully implementing solutions that ensure device integrity. However, only eight percent of companies are in the Mature category, highlighting that while there is forward progress, many still face challenges in achieving full readiness in this area.

Given the scale of the task at hand, it's no surprise that AI is increasingly being used to manage machine integrity. Among companies adopting the various machine protection solutions in South Korea, on average, 33% are incorporating AI to a significant extent.

As for the core machine protection capabilities, more than half (59%) of respondents in South Korea said they have adopted built-in protections such as Firewall and IPS. Companies recognize the position of Machine Authentication of Integrity such as Basic Input Output System (BIOS), with 34% rolling out these solutions. Machine behavior and anomaly-protection tools are useful for defending against machine threats, with 53% adopting this solution.

Machine Trustworthiness Readiness



Network Resilience

Hybrid work environments are here to stay, and securing corporate networks has become increasingly complex. Employees now access critical data from multiple locations and devices, often beyond traditional security perimeters. Networks are evolving to handle sensitive data across cloud, on-premise, and in edge environments. Meanwhile, AI is reshaping cybersecurity in both attack and defense strategies.

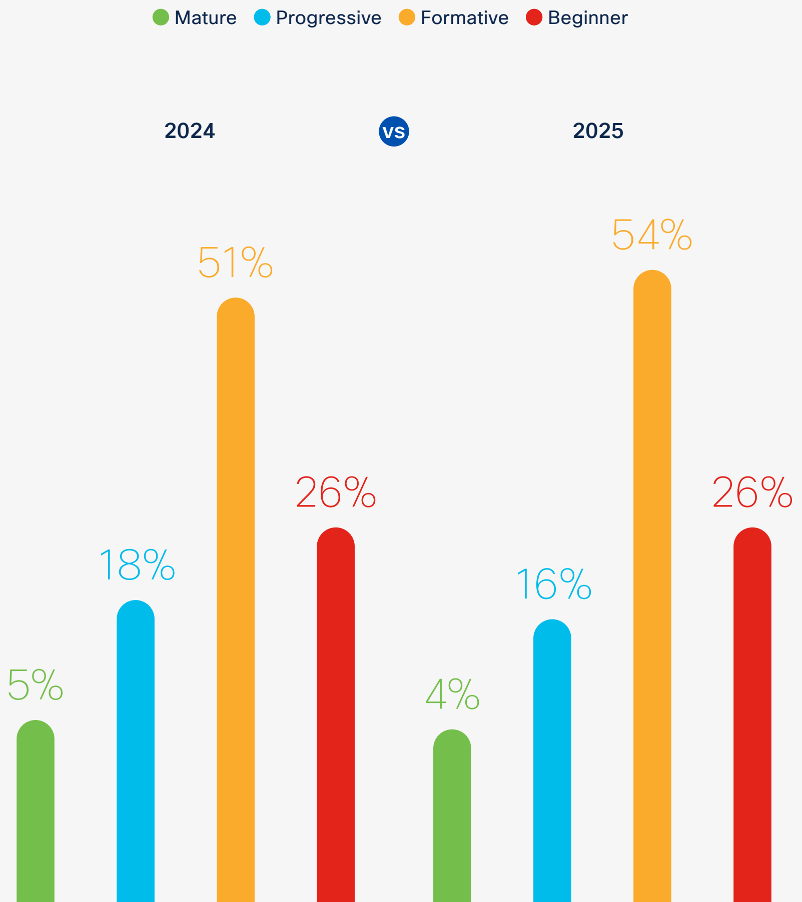
Given the rise in data center traffic flows and complex networking threats, it's unsurprising that just over a third (35%) of respondents in South Korea ranked Network Resilience as the most challenging to protect – more than any other pillar.

Network Resilience in South Korea is sliding backward, with a notable shift from Progressive (two percent decrease) to Formative (three percent increase). This downgrade suggests that rather than progressing toward more robust, proactive security models, many appear to be losing ground, possibly due to the technical and financial challenges associated with upgrading legacy network defenses.

Companies are increasingly integrating AI-driven solutions to strengthen Network Resilience, detect anomalies, and respond to threats in real time. 32% of companies in South Korea that have adopted network protection solutions have significantly incorporated AI in their network defenses.

Overall, companies recognize the urgency of enhancing their Network Resilience. Under half (44%) plan to implement segmentation within the next year, with another 43% planning to roll it out in the next one to two years.

Network Resilience Readiness



Cloud Reinforcement

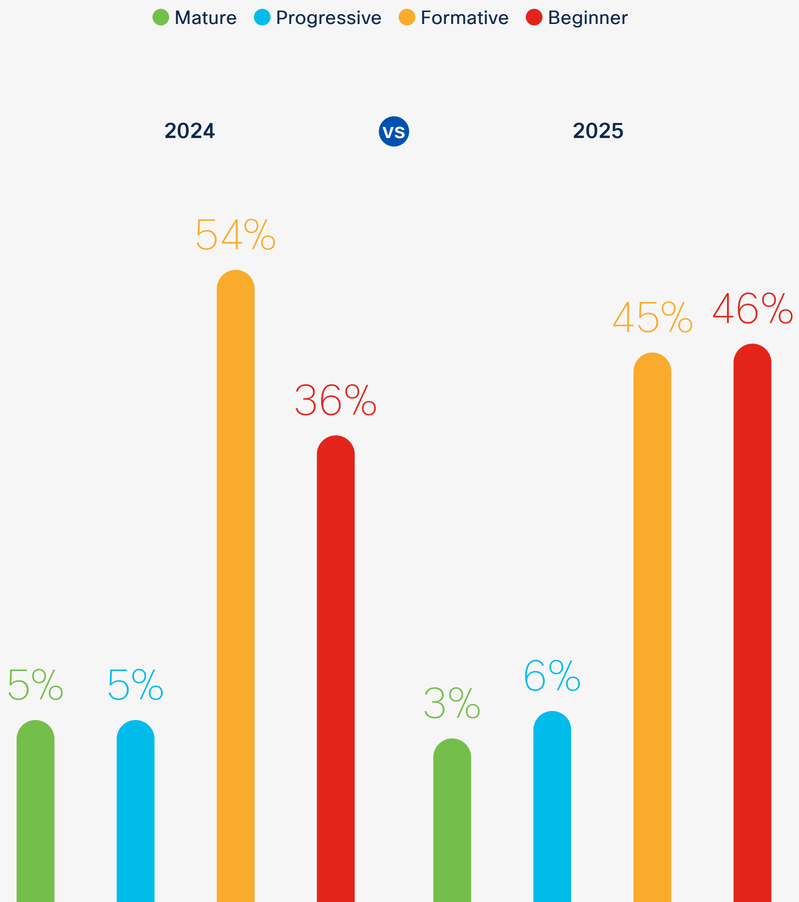
As companies migrate more workloads and data to the cloud, security challenges continue to escalate. The attack surface is expanding and adversaries are leveraging AI to automate attacks, exploit misconfigurations, and bypass traditional security controls.

In 2025, Cloud Reinforcement readiness in South Korea slightly decreased as the share of Mature companies sits at three percent, while most companies remain in the Formative and Beginner levels.

The increasing adoption of cloud and AI in today's market is in direct conflict with the overall lack of progress in cloud security readiness, suggesting that companies are leaving major gaps that can be exploited by attackers. Without more decisive action, businesses risk an ever-widening gap in their cloud environments.

Our survey underscores a growing reliance on AI-driven cloud security measures. Among companies that have adopted cloud security solutions in South Korea, 32% are significantly incorporating AI into these defenses. Yet despite this widespread uptake of AI enhancements, the rollout of basic functions remains low.

Cloud Reinforcement Readiness



AI Fortification

AI is providing more security assurances across various solutions, but businesses are cautious about viewing the technology as a guaranteed layer of protection. Automation is becoming a key component of security systems and protocols, but a trust and comfort gap remains between the current approach of partial automation and full automation.

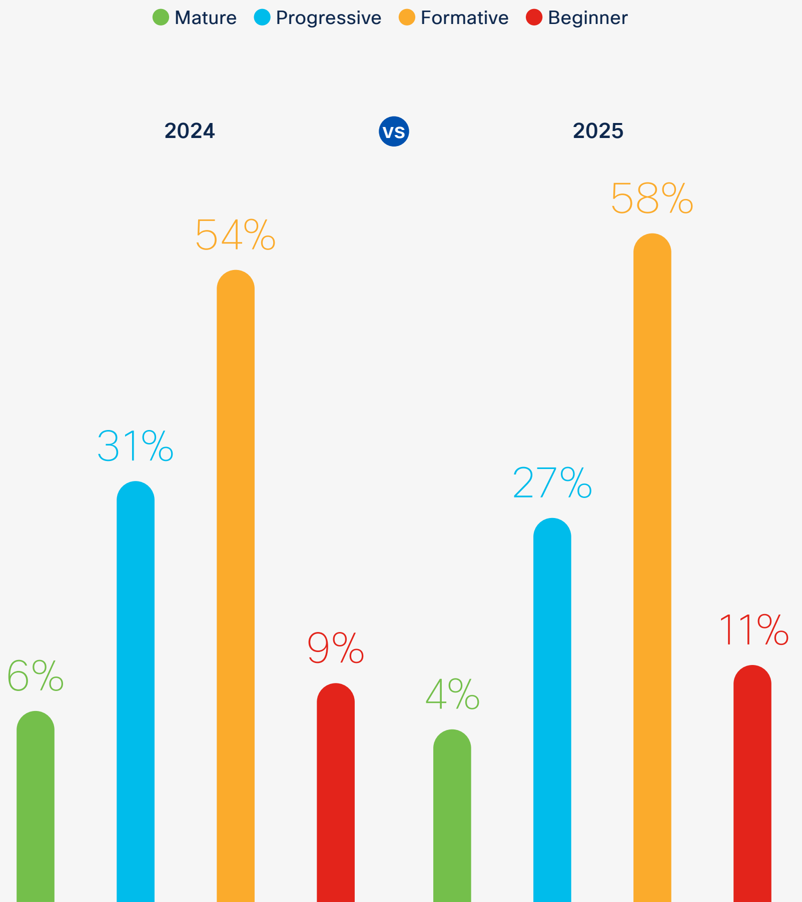
In South Korea, very little has changed in terms of overall AI Fortification readiness since the 2024 report, highlighting persistent uncertainties around AI-driven cybersecurity automation. While there have been significant advancements in AI, its deployment in cybersecurity defenses appears to have stalled, suggesting that companies are still grappling with concerns around trust, effectiveness, and integration.

Automation is a work in progress, and it can be a valuable tool in the arsenal of overworked cybersecurity teams. All (100%) respondents report that their companies would be comfortable with some degree of security automation. However, just 17% report that they would be comfortable with fully automating their systems.

In terms of specific areas of cybersecurity, almost eight in 10 (78%) of respondents in South Korea say their companies are at least partly using AI technologies, such as GenAI, in threat intelligence. AI is also largely being used in the areas of threat detection (83%), threat response (67%), and incident recovery (62%). However, the degree to which they rely upon AI for these tasks is still growing. For example, with red teaming AI models and applications as the most common area of deployment for AI, only 29% are fully automating their defenses in this area.

Other areas such as threat detection (20%), infrastructure upgrades (17%), rule testing (13%), and policy deployment (10%), are yet to cross significant comfort thresholds. AI has more to prove in these areas and we can expect it to take longer for that game-changing trust-level to be reached.

AI Fortification Readiness



Recommendations

1 **Identity Intelligence:** Create a robust identity security strategy that includes comprehensive identity visibility and Zero Trust with Passwordless and/or multi-factor authentication, supported by AI detections.

2 **Machine Trustworthiness:** Implement a zero-trust security model to verify every user and device before granting access to the network. This approach helps ensure trusted access and acts as both the first and last line of defense.

3 **Network Resilience:** Organizations need to treat this pillar with significant urgency and move beyond partial implementation as they prepare their networks for the era of AI.

4 **Cloud Reinforcement:** Companies must move beyond fragmented security strategies and invest in a unified, proactive model enhanced by AI.

5 **AI Fortification:** Develop a robust AI security strategy that includes securing both the use of AI technologies and the models upon which AI technologies are built.

About the Research

The ***2025 Cisco Cybersecurity Readiness Index*** is based on a double-blind survey of 8,000 business leaders who have cybersecurity responsibilities in their companies. The companies cover 30 territories in North America, Latin America, EMEA and Asia Pacific: **Australia**, **Brazil**, **Canada**, **Mainland China**, **France**, **Germany**, **Hong Kong SAR**, **India**, **Indonesia**, **Italy**, **Japan**, **Malaysia**, **Mexico**, **Netherlands**, **New Zealand**, **Philippines**, **Poland**, **Saudi Arabia**, **Singapore**, **South Africa**, **South Korea**, **Spain**, **Sweden**, **Switzerland**, **Taiwan**, **Thailand**, **UAE**, **UK**, **United States**, and **Vietnam**.

We looked at 31 different solutions across the five core pillars of cybersecurity protection: **Identity Intelligence**, **Machine Trustworthiness**, **Network Resilience**, **Cloud Reinforcement**, and **AI Fortification**. Respondents were asked to indicate which of these they had deployed, the stage of deployment, and if these solutions were not already deployed then what budgets had been approved, and the intended timeline of deployment. Each solution was assigned individual weightings based on its relative importance in helping safeguard the applicable pillar. Company scores were based on the deployment stage of solutions across five pillars. Partially deployed solutions received a 50% weight, while fully deployed solutions were given a 100% weight.

The scores for each pillar are then combined and weighted to arrive at an overall cybersecurity readiness score for each company. The importance of each pillar was weighted as Identity Intelligence (25%); Network Resilience (25%); Machine Trustworthiness (20%); Cloud Reinforcement (15%); and AI Fortification (15%).

The respondents are drawn from 18 industries: business services; construction; education; engineering, design, architecture; financial services; healthcare; manufacturing; media and communications; natural resources; personal care and services; real estate; restaurant services; retail; technology services; transportation; travel services; wholesale; and 'others.'

The research was carried out in January and February 2025 using online interviews.

Measuring security readiness – weightings

Pillars and solutions	*Weightings*
Identity Intelligence	**25**
Cross-context identity posture assessment	20
Cross-context identity analytics and recommendations	20
Identity behavior analytics	20
Continuous risk-based access analytics (to spot identity anomalies)	20
First authentication serves as passwordless authentication	20
Machine Trustworthiness	**20**
Machine authentication and integrity (BIO Security)	20
Mobile Device Management (MDM)	20
Machine behavior and anomaly detection tools	20
Built-in protections (Firewall/IPS)	10
Endpoint protection tools (EDR/XDR)	20
Machine update policies (Vulnerability Management)	10
Network Resilience	**25**
Segmentation	20
Micro-segmentation	15
Firewall	25
Encrypted traffic analytics (without having to decrypt the traffic)	15
Network behavior anomaly detection tool (all cardinal directions)	15
Network sandbox	10
Cloud Reinforcement	**15**
Host firewall	10
Dynamic vulnerability workload protection	15
Application-centric protection tools	15
Visibility analytics tools (all network cardinal directions)	10
Hybrid ZTA with centralized policy and distributed enforcement	15
SASE/SSE	15
Capabilities to deploy and enforce consistent policies across multiple clouds	20
AI Fortification	**15**
Understanding threats posed by AI	10
Understanding how malicious actors are using AI	10
Using Gen AI to understand threats better based on their dataset	10
Integrating AI in Identity Intelligence solutions	20
Deploying AI to verify Machine Trustworthiness	15
Leveraging AI in Network Resilience solutions	20
Using AI in Cloud Reinforcement	15

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**