2025 Cisco Cybersecurity Readiness Index

Readiness remains flat as AI transforms the industry

Contents

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. 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.

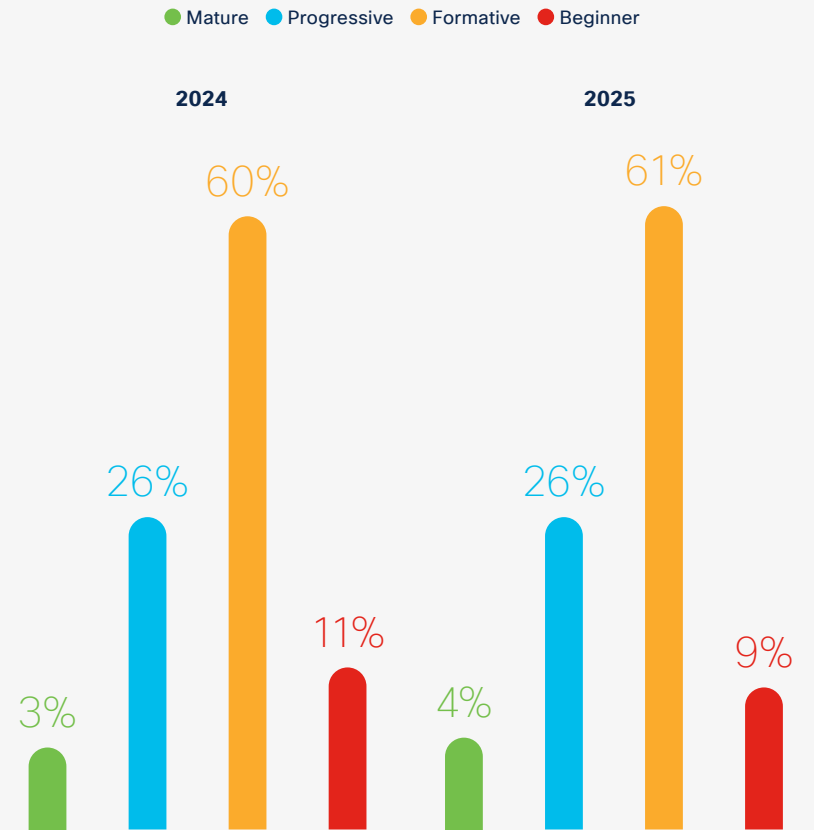
Cisco's third annual ***Cybersecurity Readiness Index*** is our updated guide that addresses the current global cybersecurity landscape and assesses how ready companies are to face today's cybersecurity risks. It is based on a double-blind survey of 8,000 businesses and cybersecurity leaders across 30 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 (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 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 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 GenAI. While half (51%) of companies require their employees 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.

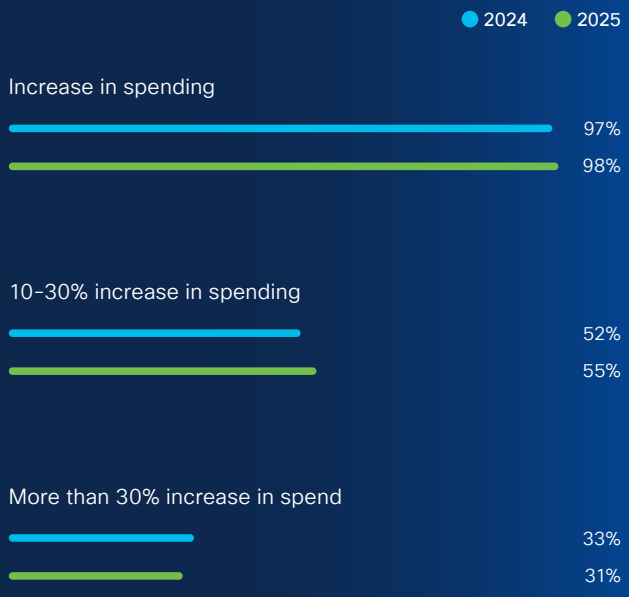
Globally, nearly half of respondents (49%) experienced at least one cyberattack within the past year, and nearly three quarters (71%) of those surveyed believe that a cybersecurity incident is likely to disrupt their organizations' business within the next 12 to 24 months. However, most companies remain 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.

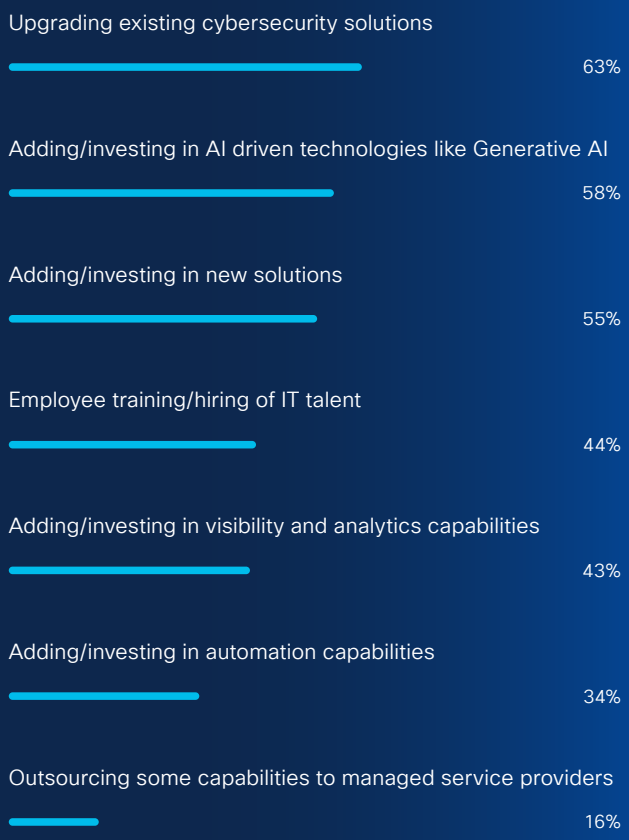
To make things more complicated, more than three quarters (77%) of respondents say that adopting too many cybersecurity solutions slowed down their team's ability to detect, respond, and recover from incidents they are trying to prevent. Seven in 10 (70%) say their companies have more than 10 point solutions 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. A large majority (86%) of respondents view a shortage of cybersecurity talent as a challenge, with 39% describing this as a significant challenge. Over half

Planned increase in cybersecurity infrastructure spending



Planned security investments



(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 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%

Benchmarking Readiness

Based on data from a double-blind survey of 8,000 business leaders across 30 global markets, the ***2025 Cybersecurity Readiness Index*** assesses five critical pillars of cybersecurity preparedness: **Identity Intelligence**, **Machine Trustworthiness**, **Network Resilience**, **Cloud Reinforcement**, and **AI Fortification**. Within these pillars, we identified 31 different solutions required to be defined as ready.

To assess readiness, we asked respondents which of these solutions their companies had in place, and their progress in deployment. We scored companies based on their deployment of these solutions, with each solution assigned a specific weight within the broader thematic pillars.

We combined organizational readiness scores in each pillar to assess overall readiness. In this calculation, the pillars are assigned weightings reflecting their relative importance in a cybersecurity posture: Identity Intelligence (25%); Network Resilience (25%); Machine Trustworthiness (20%); Cloud Reinforcement (15%); and AI Fortification (15%).

A complete explanation of the methodology is included at the end of this report.

Based on the overall score, companies were categorized into one of four stages of readiness:

Mature — **Score 70 to 100**
Companies that have achieved advanced stages of deployment and are most ready to address contemporary risks across the full spectrum of cybersecurity solutions. A complete explanation of the methodology is included at the end of this report.

Progressive — **Score 41 to 69**
Companies deploying a considerable number of solutions and performing above average on cybersecurity readiness across a range of areas.

Formative — **Score 11 to 40**
Companies that have some level of deployment but are performing below average on cybersecurity readiness across a range of areas.

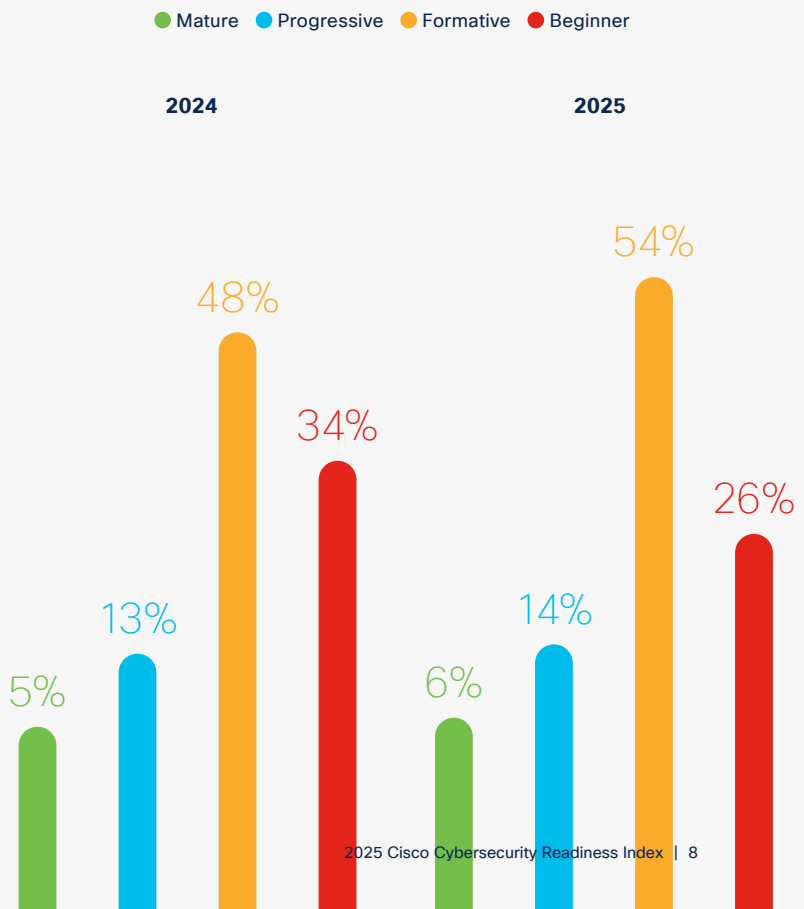
Beginner — **Score 0 to 10**
Companies at the initial stages of deploying solutions.

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.

The Cisco Talos 2024 Year in Review highlights identity as a key theme for security incidents, with threat actors targeting users' digital footprints for malicious purposes. Identity-based attacks were dominant, accounting for 60% of all Cisco Talos Incident Response (Talos IR) cases. Actors relied on identity attacks to facilitate major phases of their operations: initial compromise, lateral movement, privilege escalation, and more. Difficult to prevent and even harder to detect, identity-based attacks proved to be highly effective in 2024, allowing adversaries to go unnoticed for longer periods of time by using compromised valid accounts,

Identity Intelligence Readiness



no longer using detectable malware, and sometimes leading to unfettered access to entire networks.

In 2025, Identity Intelligence readiness slightly improved, with more companies moving from the Beginner to the Formative stage and achieving partial deployment. Full deployment remains stagnant, leaving just six percent of companies classified as Mature. This suggests that organizations are grappling with unexpected complexities or resource limitations in the final stages of implementation.

Failure to protect and secure identities can lead to significant reputational risk and should be an area of greater focus. This is especially important as AI can both heighten vulnerabilities and improve protection.

AI is proving to be a boon to practitioners seeking to bolster solutions to verify and secure identity. Because securing digital identities is crucial, companies are increasingly implementing AI-driven solutions to keep them safe. Of those companies adopting identity solutions, nearly half (47%) significantly integrated AI into these capabilities.

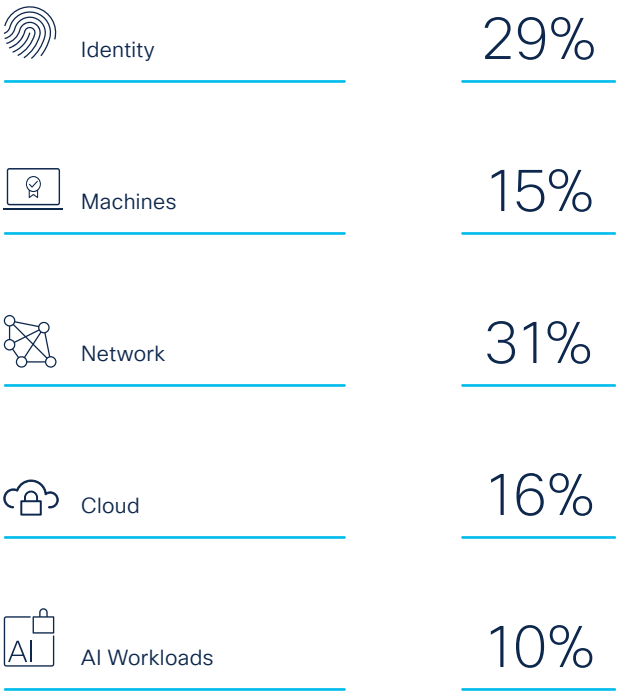
Currently, we see identity solutions being adopted at varying rates, due to their effectiveness, ease of implementation, regulatory compliance, cost, user experience, and vendor support. These barriers are likely slowing, but not stopping companies from deploying new solutions. Advances in AI could help reduce barriers in the near future.

The top two most adopted solutions for Identity Intelligence are identity behavior analytics tools at 54%, and continuous risk-based access analytics (to spot identity anomalies) at 51%. These tools are still a long way from being fully deployed. Solutions that facilitate initial authentication for passwordless access throughout a user's session currently have a lower adoption rate of 36%.

Identifying suspicious behavior and anomalies is becoming a key priority for companies in relation to Identity Intelligence. More than one quarter (29%) of respondents rank Identity as their company's top cybersecurity challenge, the second highest of any pillar.

Striking a balance between seamless user experience and robust identity protection is a delicate task. Businesses are actively deploying tools to achieve this balance more effectively, continuously adjusting and adapting to the ever-evolving landscape of threats and risks.

Areas companies find most challenging to protect against cyberattacks

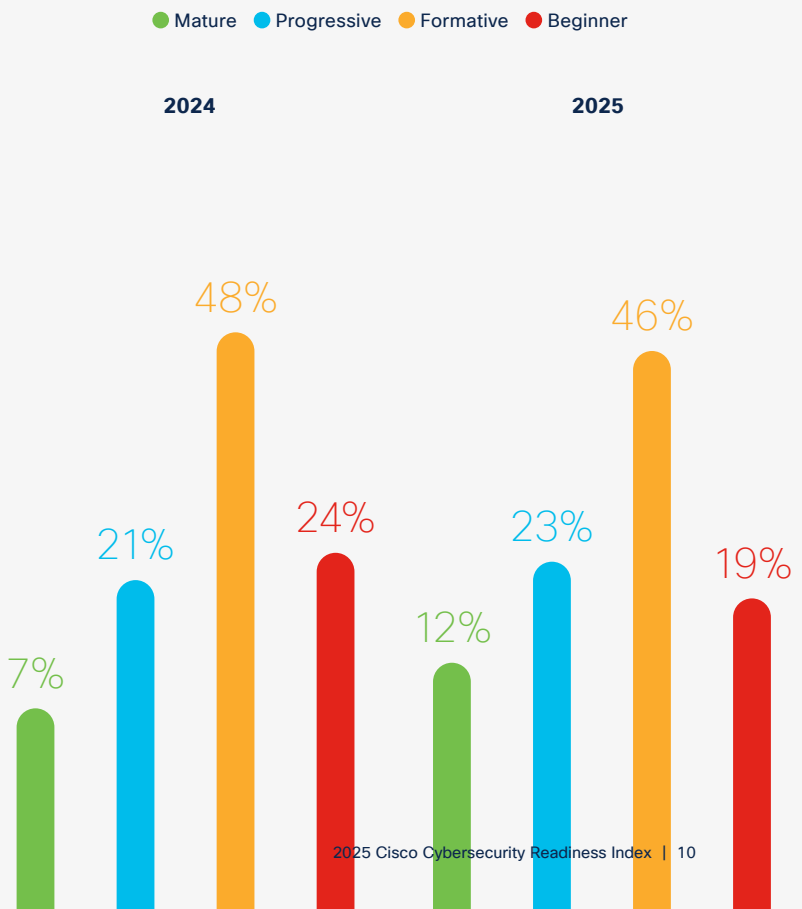


Machine Trustworthiness

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 observe a moderate shift in how ready companies are for Machine Trustworthiness, with a more than five 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 12% 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.

Machine Trustworthiness Readiness



AI plays a crucial role in monitoring and securing these interconnected devices, leveraging machine learning to detect anomalies and respond to threats in real-time. However, the same AI capabilities can be exploited by attackers to launch more sophisticated and targeted attacks, making it imperative for companies to stay vigilant and continuously enhance their security measures.

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, on average, 46% are incorporating AI to a significant extent.

On core machine protection capabilities, more than half (59%) of respondents 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 56% rolling out these solutions. Machine behavior and anomaly-protection tools are useful for defending against machine threats, with 51% adopting this solution.

Despite these efforts, the scale of deployment is lagging. Half (50%) of the companies are either just starting or only partially along the path of implementing machine protection solutions. While 53% have fully deployed Machine Authentication and Integrity capabilities, only 52% have fully implemented Built-in Protections.

Looking ahead, 53% of companies plan to deploy Mobile Device Management (MDM) within the next 12 months. Additionally, 25% are looking to implement Machine Authentication and Integrity, while 50% are focusing on Machine Update Policies. Despite these plans, only 12% of companies are in the Mature category for machine security, with 65% still in the two lagging categories of readiness.

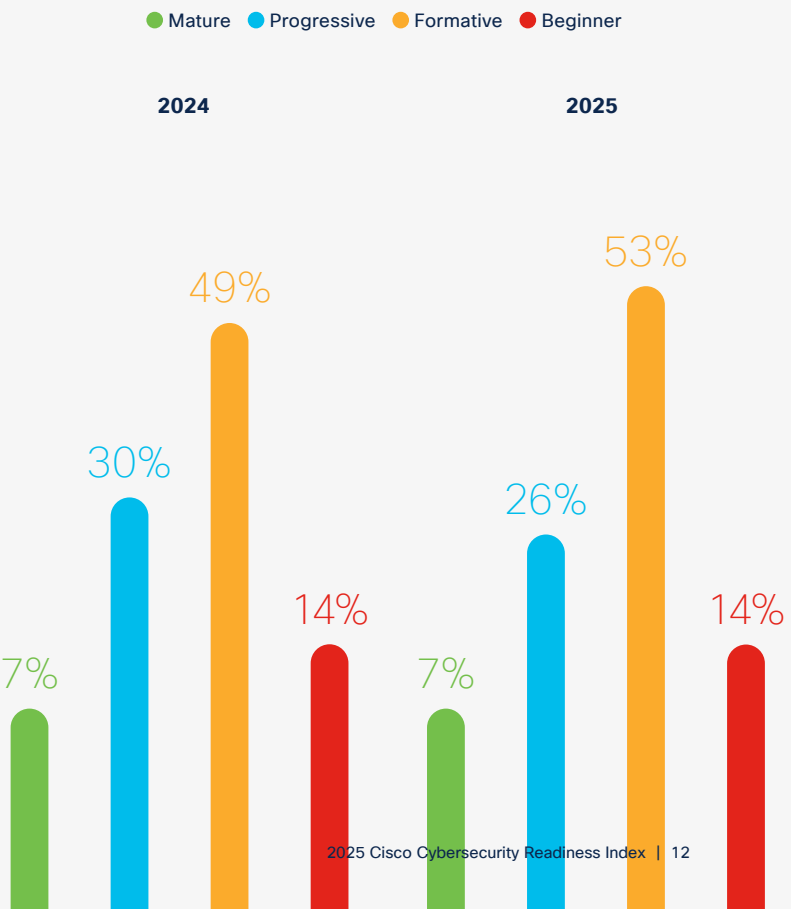
The growing reliance on AI for machine security underscores the importance of staying ahead of potential threats. As AI tools become more sophisticated, so do the tactics of malicious actors, making it crucial for companies to continuously enhance their security measures.

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. AI is reshaping cybersecurity in both attack and defense strategies.

Data center capacity is expected to grow by 19–22% annually until 2030, driven by AI workloads. This surge in traffic presents new security challenges as threat actors use AI to automate phishing, create deepfake social engineering attacks, and deploy adaptive malware. The shift to hybrid work exacerbates these challenges with unmanaged devices and frequent logins from multiple networks, providing ample opportunity for AI-powered threats like credential stuffing and automated lateral movement within compromised networks.

Network Resilience Readiness



With the rise in traffic flows and complex networking threats, it's unsurprising that nearly a third (31%) of respondents ranked Network as the most challenging pillar to protect – more than any other area.

Network Resilience is sliding backwards, with a notable shift from Progressive (four percent decrease) to Formative (four 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. As networks become more distributed across cloud, on-premise, and edge environments, the cost and expertise required to maintain resilience may be proving overwhelming for many companies.

AI also has the potential to fundamentally transform network defenses. Companies are increasingly integrating AI-driven solutions to strengthen Network Resilience, detect anomalies, and respond to threats in real time. On average, 47% of companies that have adopted network protection solutions have significantly incorporated AI in their network defenses.

It's no surprise that most of the top-targeted vulnerabilities are many years old, highlighting ongoing challenges in patch management for companies. According to the Cisco Talos 2024 Year in Review, unpatched/vulnerable systems were the second most common security weakness observed in 2024.

Beyond AI-specific threats, companies must adopt robust strategies to bolster Network Resilience. Essential measures include network segmentation, micro-segmentation, firewalls, and advanced network behavior anomaly detection systems capable of identifying malicious activity from all network cardinal directions. Additionally, encrypted traffic analytics can help uncover hidden threats within encrypted data streams without the need for decryption, preserving both security and privacy.

Despite widespread awareness of these threats, defensive measures are inconsistently deployed. While 69% of companies report using firewalls as a primary security layer, only 55% of them have reached full implementation. Network behavior anomaly tools, being used by 56% of companies, also suffer from slow deployment, with just 46% of this group achieving full rollout. Similarly, 53% of companies adopted encrypted traffic analytics, but under half (46%) of them have fully deployed these tools.

Widespread adoption of advanced network security solutions continues to be hindered by a combination of cost, complexity, and resource constraints. Simpler, more cost-effective measures like segmentation and firewalls are more likely to be fully deployed, whereas sophisticated solutions such as micro-segmentation and sandboxing require significant infrastructure and expertise.

Nevertheless, companies recognize the urgency of enhancing their Network Resilience. More than half (52%) plan to implement segmentation within the next year, with another 35% planning to roll it out in the next one to two years. Similarly, 51% aim to deploy firewalls within the next 12 months, while 40% anticipate doing so within two years.

The maturity of Network Resilience efforts remains a concern. Only seven percent of companies fall into the Mature category, indicating a high level of preparedness, while 26% are in the Progressive stage, a four percent drop from 2024. Alarmingly, 63% of companies still operate at the Formative or Beginner level. As AI-powered threats continue to evolve at a rapid pace, companies must move beyond partial implementations and fragmented security postures to build a truly resilient, AI-ready defense framework.

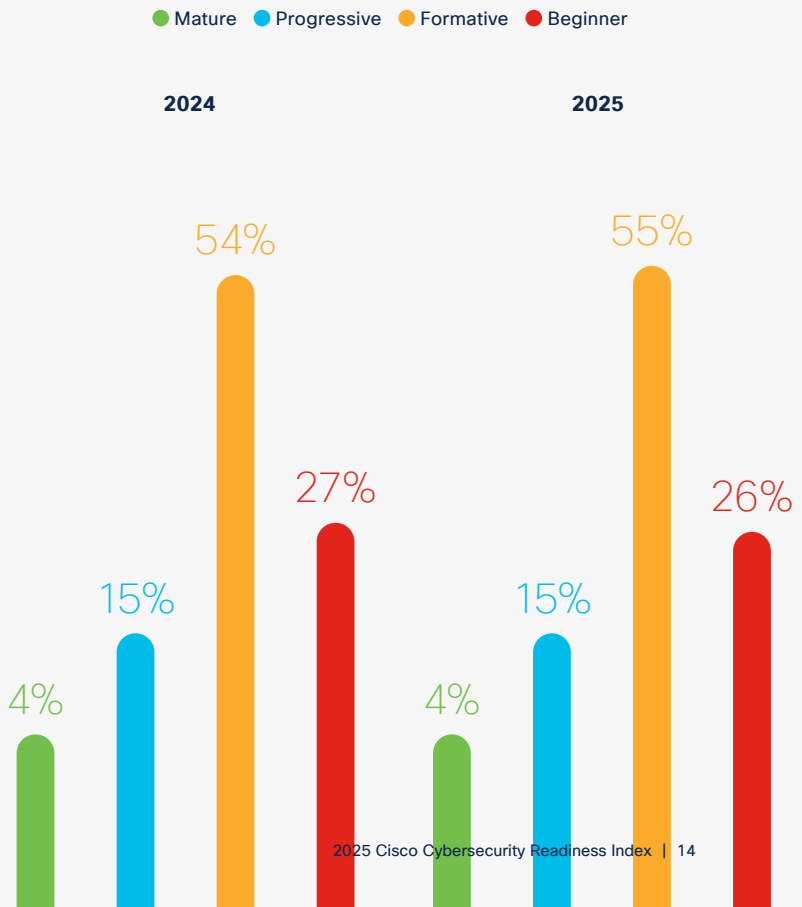
Cloud Reinforcement

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 remains stagnant, with organizations struggling to achieve full maturity, as partial rollouts prevail. 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 security 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, 46% are

Cloud Reinforcement Readiness



significantly incorporating AI into these defenses. Yet despite this widespread uptake of AI enhancements, the rollout of basic functions remains low.

There are still a number of companies that have not begun adopting cloud security solutions. Of those who have, host firewalls (53%) and visibility analytics tools (47%) lead in implementation, likely due to their immediate security benefits and ease of deployment. In contrast, there is a lag in the deployment of more advanced capabilities like hybrid zero-trust architectures (40%) and policy enforcement across multiple cloud environments (36%).

These gaps reflect a broader trend: while companies acknowledge the importance of cloud security, execution remains a challenge. Cost, complexity, and integration hurdles are slowing progress, particularly for solutions requiring centralized coordination and cross-cloud interoperability.

Despite these obstacles, momentum is building. Among companies yet to implement cloud security solutions, the majority (79%) plan to do so within the next one to two years.

Security maturity levels remain concerning, as the share of Mature companies in the Cloud Reinforcement category remains at four percent, with most still falling into the Formative and Beginner levels. This suggests that while many businesses are progressing toward cloud security, few have developed the comprehensive, scalable defenses needed to counter cloud security threats.

As cloud adoption accelerates, companies must move beyond fragmented security strategies and invest in unified, AI-enhanced defenses. Companies risk leaving critical workloads exposed to an evolving threat landscape that is increasingly automated, adaptive, and relentless – highlighting a need for proactive reinforcement.

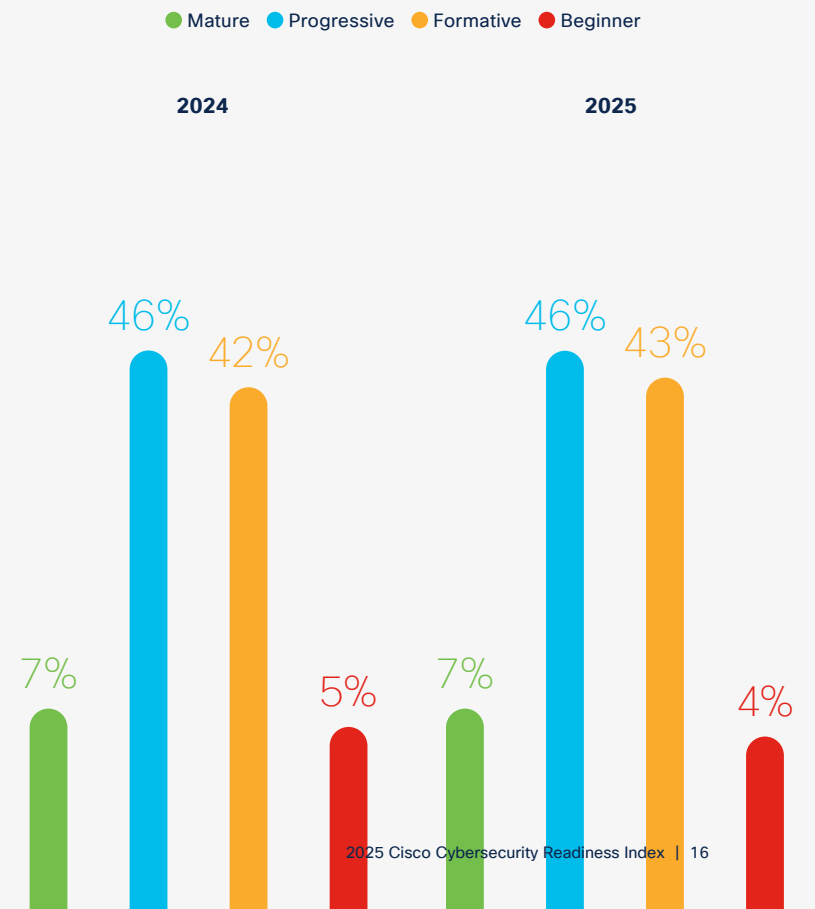
Artificial Intelligence (AI) Fortification

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 there is a trust and comfort gap between the current approach of partial automation and full automation.

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.

Many security leaders hesitate to fully embrace AI-driven defenses, either due to technical feasibility issues, regulatory concerns, or difficulties in adapting AI models

Artificial Intelligence Readiness



to evolving threats. Until these barriers are addressed, AI's potential in cybersecurity remains promising yet unrealized.

Automation is a work in progress, and it can be a valuable tool in the arsenal of overworked cybersecurity teams. The vast majority (97%) of respondents report that their companies would be comfortable with some degree of security automation. However, just 33% report that their organizations would be comfortable with fully automating their systems.

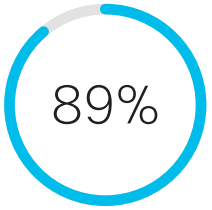
Cybersecurity teams are forging ahead in their use of AI to gather threat intelligence. Almost nine in 10 (89%) say their companies are at least partly using AI technologies, such as GenAI, to develop a better understanding of threats. As AI becomes more adept at delivering threat intelligence, it is likely to build credibility behind its deployment to broader fortification efforts.

AI is largely being used in the areas of threat detection (85%), threat response (71%), and incident recovery (70%). However, the degree to which companies rely upon AI for these tasks is still growing. For example, with threat detection as the most common area of deployment for AI, only 27% of respondents are fully automating their defenses in this area. Red teaming AI models and applications is the area with the next highest level of full automation, at 22%.

Other areas such as rule testing (12%), infrastructure upgrades (12%), policy creation (nine percent), and incident response (three percent), 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.

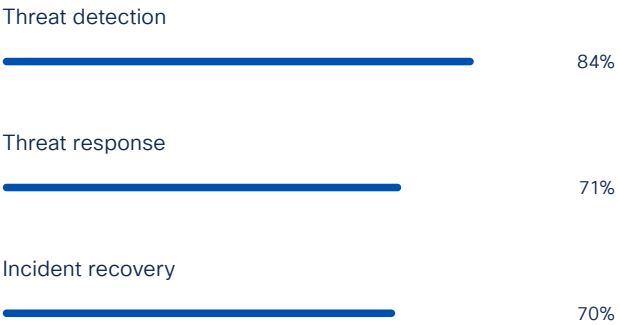
Cybersecurity practitioners are making extensive use of AI in policy assessment, with deployment to identify duplicate, overlapping, or contradictory policies (78%), for policy recommendations (78%), and for policy enforcement (71%). Respondents have more comfort here around using AI to check and enforce existing systems, while also permitting it to make recommendations that can subsequently be evaluated.

As threats continue to evolve, so do the solutions deployed to counter them. Companies are embedding AI more deeply within these solutions as they take a cautious step toward further automation. Many businesses are recognizing the significant role that AI Fortification must play in their overall cybersecurity protocols, and they are in the process of testing and refining where and how to best deploy it.



say their companies are at least partly using AI technologies to develop a better understanding of threats

Areas where companies are integrating AI



Industry and Size Matter

Looking at the industries with the highest levels of cybersecurity readiness, they tend to be dominated by those with the most to lose from cybersecurity incidents, and the most to gain from keeping threats at bay.

Malicious actors are leveraging AI to launch more sophisticated cyberattacks on all industries, with awareness of these threats differing significantly. Respondents from Healthcare companies report the lowest levels of understanding (39%) around AI-powered threats, while the Technology and Financial Services industries have the highest awareness (55%). The lack of awareness in Healthcare is particularly concerning given the vast amount of patient data, diagnostic tools, and critical infrastructure involved.

The level of awareness around AI threats in Technology Services is unsurprising, due to the highly technical knowledge base of their employees. The industry is highly risk-aware, and has surpassed others in overall readiness since 2024, taking a leading position across all five pillars. Media and Communications, along with Natural Resources sectors like oil, mining, and forestry, follow closely, each with six percent of companies in the Mature category. Readiness among the top three industries from 2024, namely Travel Services, Business Services, and Manufacturing, appears to be stagnating.

Despite the strong showing of Natural Resources companies in the Mature category, a relatively large number (16%) are also at the Beginner level. This polarity could be due to strict compliance measures imposed upon the industry in more developed markets, and comparatively lax approaches in others. As Natural Resources companies vie for a piece of the renewables and electric vehicles supply chain, they will come under increasing scrutiny, which will likely include data and cybersecurity requirements.

Natural Resources performs well in Identity Intelligence, as these companies often manage critical infrastructure and face stringent regulatory requirements, prioritizing strong identity controls to prevent breaches.

For Network Resilience, Media and Communications, Retail, and Technology Services lead, each with 10% of companies in the Mature category. Media and Communications companies face constant cyber threats targeting digital content and customer data. Retailers, handling large-scale transactions and payment systems, prioritize network security to prevent breaches and fraud.

A strong showing for Media and Communications (15% Mature) in Machine Trustworthiness may be explained by the need for strong endpoint security in content distribution and broadcast infrastructure, and thus also performs well here. For Cloud Reinforcement, Natural Resources leads at nine percent Mature, as the sector increasingly adopts cloud solutions to manage remote operations and industrial IoT securely.

Technology Services leads again in AI Fortification, with 10% of companies reaching Mature – equal to 2024 – highlighting their proactive approach to both the risks and opportunities of AI-driven cybersecurity. Financial Services follows closely, leveraging AI to detect fraud and automate threat response.

While low awareness around AI-powered threats across critical services is concerning, the challenges vary considerably by company size, with smaller companies often at a greater disadvantage due to the limited resources and oversight they tend to have in this area. Disparities in overall readiness levels between small and large companies will also influence their ability to tackle AI-driven threats.

Concerned about data leaks fueling more cyberattacks, IT teams everywhere are struggling to monitor employee requests to GenAI tools. Often grappling with limited budgets and the absence of dedicated cybersecurity teams, smaller companies are particularly vulnerable, with 65% reporting a lack of visibility into employee use of AI, compared to 51% of medium-sized companies and 54% of large enterprises. Further, 60% of companies lack confidence in identifying unapproved AI tools, with smaller businesses struggling the most (68%), compared to 51% of both medium and large enterprises.

Readiness levels across industries (top and bottom three)

Mature

Technology Services 6%

Media and Communications 6%

Natural Resources 6%

Beginner

Natural Resources 16%

Wholesaling 15%

Healthcare 14%

A lack of control over employee use of AI could render small companies particularly vulnerable to attacks, changing the current state of play. At present, larger companies face the greatest risk of cyberattacks, with 57% reporting at least one incident in the past year—higher than both medium (54%) and small (44%) businesses. However, experience breeds expertise; 64% of large enterprises express confidence in navigating cybersecurity challenges, compared to smaller counterparts.

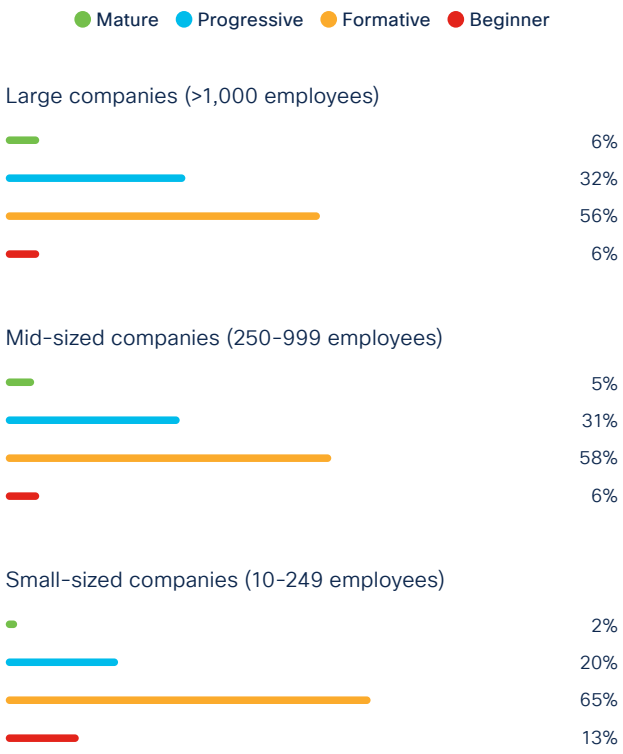
As for overall readiness to confront threats new and old, mid-sized companies show strong potential, with five percent reaching the Mature category. While they may lack the deep budgets of larger enterprises, they benefit from greater agility, allowing them to deploy cybersecurity measures more efficiently without the bureaucratic hurdles of bigger firms.

Unsurprisingly, it is the large-sized companies — those with more than 1,000 employees — that are best prepared with more companies in the Mature category (six percent) than their smaller competitors, and more in the Progressive category (32%) too.

Smaller companies tend to lag in readiness, with 65% in Formative and 13% in the Beginner category. However, their performance has improved year-over-year, particularly in AI Fortification, where the share of Beginner companies dropped from 32% in 2023 to 16% in 2024. This suggests that while small businesses may struggle with maintaining visibility of employee use of AI, they are rapid early-stage adopters of AI-driven security, likely due to their need for cost-effective, automated solutions.

While companies of all sizes are most advanced in Machine Trustworthiness, 24% of small businesses remain at the Beginner level - three times the number in Mature (eight percent). This marks a shift from last year, when Network Resilience was the strongest pillar across all sizes.

Overall readiness by company size



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 were 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 were 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**