2024 Cisco Cybersecurity Readiness Index

Underprepared and Overconfident Companies Tackle an Evolving Landscape

Contents

Executive Summary

Today's threat landscape is more complicated than ever, and organizations are struggling to maintain a foothold. Billions of users, devices, and IoT devices are connecting to enterprise networks, cloud applications, and data at a scale unlike anything we have seen in the past.

At the same time, companies are facing a complicated and diverse threat landscape that goes beyond ransomware and phishing. In the past year alone, many also encountered credential stuffing, supply chain attacks, social engineering, and cryptojacking. Separately, according to the latest *Cisco Talos Year in Review*, in 2023, cyber threat actors frequently exploited older software vulnerabilities in common applications.

Advancements in artificial intelligence (AI) and the mainstream availability of capabilities like Generative AI are empowering malicious actors to deploy more sophisticated, targeted attacks. Companies are struggling to respond, often slowed down by their own overly complex security stacks that have multiple point solutions. The lack of skilled

professionals remains an issue. Compounding the problem, many of these positions remain unfilled.

To successfully face this high-stakes, complex environment, organizations must always stay ahead to adequately ensure cybersecurity resilience.

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

Based on five pillars of cybersecurity readiness that are most relevant to securing today's organizations – **Identity Intelligence**, **Network Resilience**, **Machine Trustworthiness**, **Cloud Reinforcement**, and **Artificial Intelligence (AI) Fortification** – the 2024 edition of this study shows very few organizations prepared to defend against today's rapidly evolving threat landscape.

Only 3% of respondent organizations qualify for the Mature category. Nearly three-quarters (71%) fall in the bottom two categories (Formative, 60% and Beginner, 11%). In terms of the pillars of readiness, we found the strongest performance in Network Resilience and AI Fortification, both with 7% of companies in the Mature category. The lowest levels of readiness were in Cloud Reinforcement and Identity Intelligence, with 4% and 5% of companies ranked as Mature respectively.

This lack of readiness is substantial despite almost three-quarters of companies (73%) believing a cybersecurity incident will disrupt their business in the next 12-24 months. What is surprising, though, is that despite this lack of readiness, 80% of companies feel moderately to very confident in their ability to stay resilient amidst this evolving cybersecurity landscape. While this number is down from last year, it does underline a gap that suggests companies may have misplaced confidence in their ability to navigate the threat landscape and are not properly assessing the true scale of the challenges they face.

There are positive signs as well. Despite their sense of confidence, organizations recognize the threats. In response to the heightened risk, 91% have increased their cybersecurity budgets over the past one to two years, and the majority expect their budgets to increase further in the coming one to two years.

Unsurprisingly, readiness also correlates to an organization's size, as more budget can be dedicated to cybersecurity in larger companies. Those with more than 1,000 employees exhibit higher rates of maturity, while medium-sized organizations (250-1,000 employees) are not far behind. This is true across the globe and the various industries surveyed.

This study found the top industries in terms of overall cybersecurity readiness are Financial Services, Technology Services, Media and Communications, and Manufacturing (all with 30% or more in the upper Mature and Progressive categories of readiness). The industries requiring the most improvement are Personal Care and Services, Education, and Wholesale (each with between 15% and 18% in the Beginner category, the lowest in the Index).

Although companies have been devoting more focus and money to address cyber threats, and expect to accelerate these efforts further over the next 12-24

months, the current readiness levels are low. In short, the sophistication, scale and frequency of cybersecurity threats are currently outstripping protective measures being taken by companies.

As such, companies need to ensure that in addition to securing additional funding, they also accelerate the deployment of cybersecurity solutions. As they do that, they should adopt a platform approach to ensure that various solutions on their stack can be integrated so they can leverage them fully. In the absence of this, organizations remain vulnerable to attacks. We have included specific recommendations at the end of this Index.

This Index provides a comprehensive view of what organizations need to be ready to tackle the security challenges of the modern world, and more importantly where companies across the globe are lacking. It provides a detailed point of reference and serves as a guide on what organizations need to do to improve their cybersecurity resilience.

Overall Readiness

Mature
3%

Progressive
26%

Formative
60%

Beginner
11%
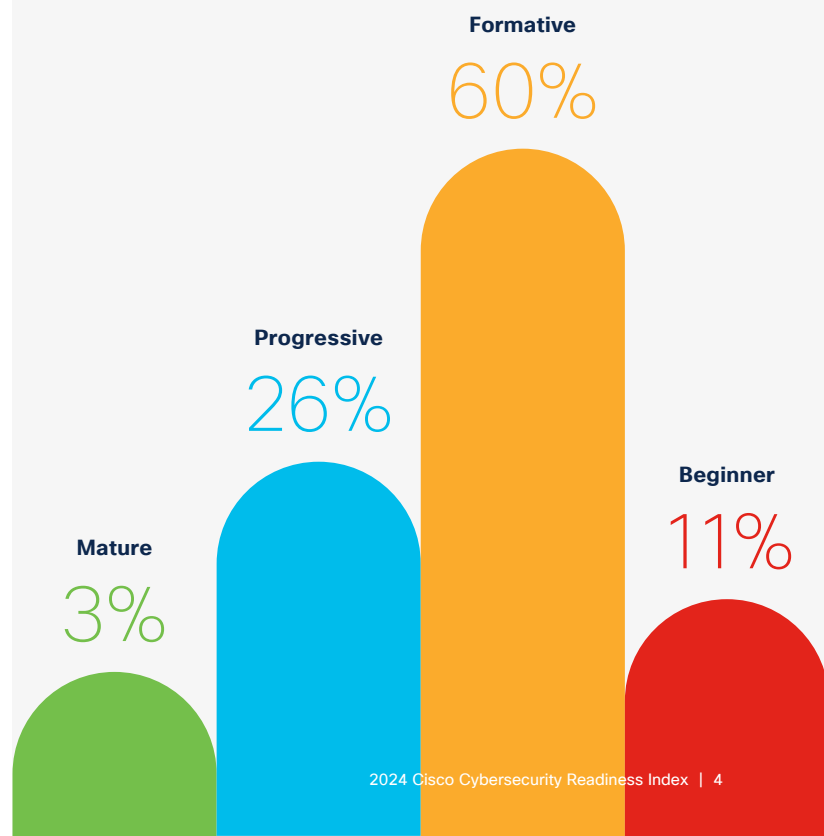
Benchmarking Readiness

Based on data from a double-blind survey of 8,136 business leaders across 30 global markets, the 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. The pillars have been updated since the 2023 edition to reflect the evolution of the cybersecurity landscape, including the growing importance of AI.

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

Organizational readiness scores in each pillar have then been combined to assess overall readiness. In this calculation, pillars themselves 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%).

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

- **Beginner** (Scoring less than 11): Organizations at the initial stages of deploying solutions.
- **Formative** (Scoring 11 – 40): Organizations that have some level of deployment but are performing below average on cybersecurity readiness across a range of areas.
- **Progressive** (Scoring 41 – 69): Organizations deploying a considerable number of solutions and performing above average on cybersecurity readiness across a range of areas.
- **Mature** (Scoring 70 and higher): Organizations 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.

Measuring Security Readiness in the Modern World

Identity Intelligence

- Cross-context identity posture assessment
- Cross-context identity analytics and recommendations
- Identity behavior analytics
- Continuous risk-based access analytics (to spot identity anomalies)
- First authentication serves as passwordless authentication

Machine Trustworthiness

- Machine authentication and integrity (BIO Security)
- Machine management (MDM)
- Machine behavior and anomaly detection tools
- Built-in protections (Firewall/IPS)
- Endpoint protection tools (EDR/XDR)
- Machine update policies (Vulnerability Management)

Network Resilience

- Segmentation
- Micro-segmentation
- Firewall
- Encrypted traffic analytics (without having to decrypt the traffic)
- Network behavior anomaly detection tool (all cardinal directions)
- Network sandbox

Cloud Reinforcement

- Host firewall
- Dynamic vulnerability workload protection
- Application-centric protection tools
- Visibility analytics tools (all network cardinal directions)
- Hybrid Zero Trust Architecture (ZTA) with centralized policy and distributed enforcement
- SASE/SSE
- Capabilities to deploy and enforce consistent policies across multiple clouds

AI Fortification

- Understanding threats posed by AI
- Understanding how malicious actors are using AI
- Using Gen AI to understand threats better based on their dataset
- Integrating AI in Identity Intelligence solutions
- Deploying AI to verify Machine Trustworthiness
- Leveraging AI in Network Resilience solutions
- Using AI in Cloud Reinforcement

An Evolving Threat Landscape Proves Costly

Globally, the cybersecurity threat landscape continues to evolve rapidly and remains challenging, with more than half of organizations (54%) having experienced a cybersecurity incident in the past year, and three-quarters (73%) of all organizations believing they are likely to be disrupted by a cybersecurity incident in the next 12-24 months.

A key trend that this year's Index highlighted is that companies now see external actors as a bigger threat than internal ones. Among those surveyed, 62% highlighted that external actors are their biggest threat, while only 31% said the same for internal actors. This is a marked shift from 2023 when the two were seen as almost equal threats. One of the key drivers of this turnaround could be the fact that cybersecurity threats from external actors are becoming increasingly sophisticated.

While malware (76%) and phishing (54%) continue to remain the top types of attacks experienced, 37% of

Types of Attacks Experienced by Companies

Malware	76%
Phishing	54%
Credential Stuffing	37%
Supply Chain and Social Engineering Attacks	32%
Cryptojacking	27%

companies were impacted by credential stuffing, 32% had supply chain and social engineering attacks, and 27% said they suffered cryptojacking incidents in the past year.

The challenges for organizations are only becoming greater as the world of hybrid work continues to add another layer of complexity to the threat landscape. The Index shows that 91% of employees across organizations are using multiple networks to connect to work. In fact, nearly one in three (29%) employees move between at least six networks weekly. 85% of organizations say their employees access company platforms from unmanaged devices and 43% of those employees report spending 20% of their time logged onto company networks from such devices.

This is making security professionals nervous. Four out of five organizations (82%) cite remote logins as a heightened threat vector, with the main concerns being the use of unsecured Wi-Fi networks, the inability to monitor threats across multiple networks, and the use of unmanaged devices.

The financial impact of these incidents is significant. Among those that suffered an incident in the past year, more than half (52%) said it cost their organization at least US$300,000, while 12% said the impact was US$1 million or more. An interesting trend that stood out was the fact that the majority of the companies that had an impact of US$1 million or more, were those that have annual revenues of more than US$100 million. On the other hand, the majority of those who said the impact was less than US$200,000 were companies with annual revenues less than US$2 million. Based on those responses, the total financial impact among companies which suffered a cybersecurity incident in the past year was around US$3.38 billion.

Greater Threats Require Greater Resources

What is encouraging to see is that organizations are starting to take action with over half (52%) planning to significantly upgrade their IT infrastructure in the next 12-24 months, a marked increase from 2023 when just one-third (33%) planned to do so. Most prominently, organizations plan to upgrade existing solutions (66%),

2024 Cisco Cybersecurity Readiness Index | 7

deploy new solutions (57%), and invest in AI-driven technologies (55%) for gains in productivity and consistency. In addition, nearly one-third (33%) said they are also planning to invest in automation capabilities which shows that businesses are starting to realize that given the scale of the challenge at hand, they need to fight it at machine scale.

To fund these initiatives, more than nine out of 10 (91%) companies substantially increased their cybersecurity budgets in the past 12-24 months. More than six out of 10 (61%) increased their budgets by at least 20%, with three out of 10 (30%) increasing by 30% or more. The main factors driving these large increases in cybersecurity budgets include increased risk due to digitization, growth in types of attacks and threats, financial impact of cyber incidents, and increasing sophistication of attacks.
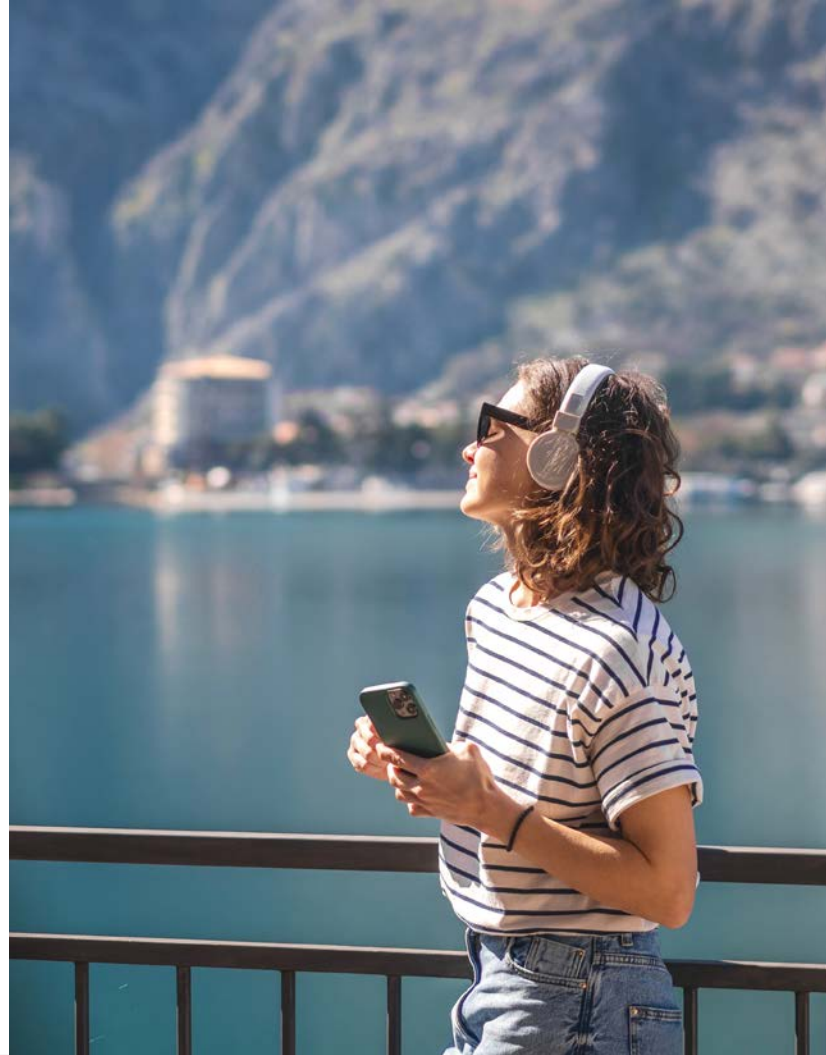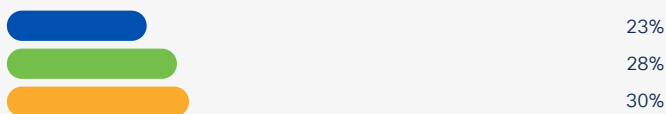
Number of Unfilled Cybersecurity-Related Positions

- 🔵 Large companies (>1,000 employees)
- 🟢 Mid-sized companies (250-999 employees)
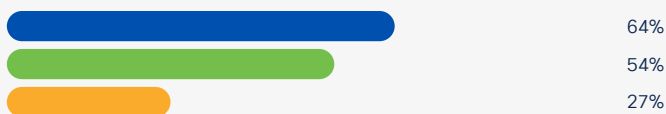- 🟠 Small-sized companies (10-249 employees)

Between 1 – 5

🔵	13%
🟢	18%
🟠	43%

Between 6 – 10

🔵	23%
🟢	28%
🟠	30%

More than 10

🔵	64%
🟢	54%
🟠	27%
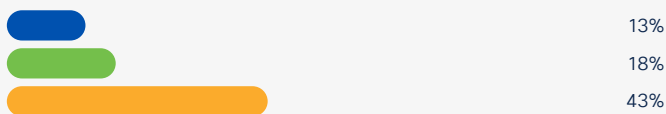
This trend is expected to accelerate as we look ahead, with 97% of companies planning increased spending on cybersecurity in 2024, including over half (52%) of all companies who plan to increase their cybersecurity budgets by 11% to 30% and more than one-third (33%) planning to increase budgets by even more.

Cybersecurity is also consuming an ever-growing share of overall IT budgets, with a majority (53%) of organizations surveyed devoting more than 10% of their total IT budget to cybersecurity — up from only 29% of organizations that allocated a similar amount in 2023. This highlights that executive leadership teams understand the critical nature of cybersecurity and its importance to their business growth.

However, progress is being stifled by a critical shortage of talent, which was highlighted as an issue for nearly nine out of 10 companies. Almost half (46%) of the companies said they had more than 10 unfilled cybersecurity roles on their teams at the time of our survey.

While the biggest talent shortages are felt in the larger organizations, the resource crunch is being felt by even relatively small companies (those employing less than 250 employees).

While companies race to ramp up resources, the complexity of their security stack is further slowing them down or making their responses less efficient. More than two-thirds (67%) of companies said they have more than 10 point solutions in their security stack, with 25% admitting that they have more than 30 point solutions. This reflects the way in which the industry has evolved over the years – as new threats emerged, new solutions were developed and deployed to counter them, either by existing vendors or new ones. For the most part, it worked at the time. However, as digitization has picked up pace, and as threats continue to evolve and become more sophisticated, this approach is now having the exact opposite effect. Four in five companies (80%) admit that having multiple point solutions is slowing down their team's ability to detect, respond to, and recover from incidents.

The State of Global Cybersecurity Readiness

The evolving threat landscape, resource challenges, and complexity of networks, cloud and applications are taking a toll on today's organizations. When assessing overall cybersecurity readiness for this Index, only 3% of respondent organizations qualify for the Mature category, 26% as Progressive, 60% as Formative, and 11% as Beginner.

We see that the impact of the rapidly evolving threat landscape has increased the demand for organizations to ensure a more holistic and in-depth approach to security.

The following sections of this Index contain a deeper analysis of our Index pillars and the state of cybersecurity readiness of companies.
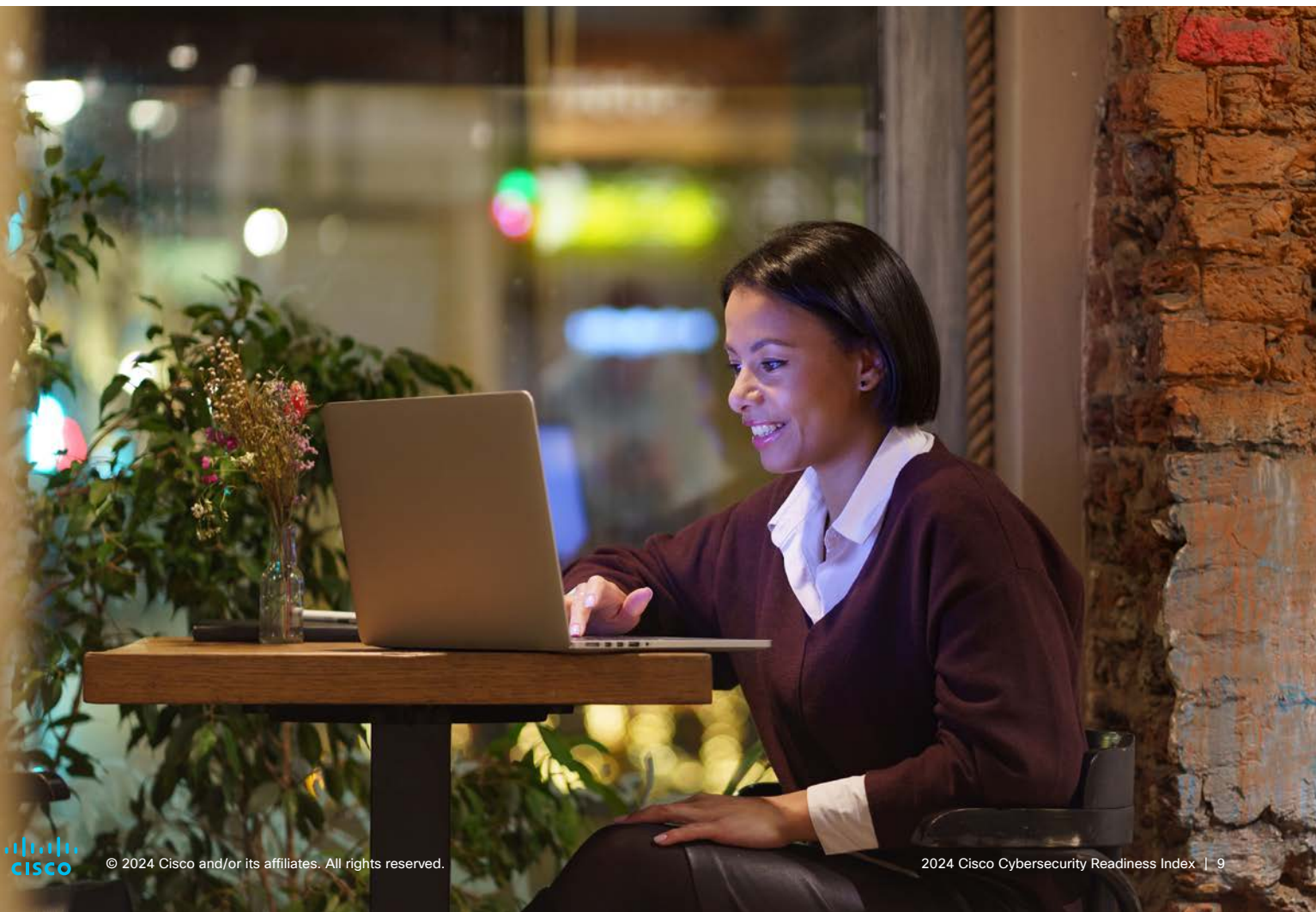
Identity Intelligence

Until recently, security practitioners' focus had traditionally been on creating a strong perimeter to keep out potential threats. This approach assumes that anyone who has accessed the network is authorized to be there.

To manage access, companies have relied on identity management solutions such as data stores that contain information like a user's username, password, and identity. A user provides this information to log in, and if it matches the stored information, they are granted access.

However, in today's distributed environments where data can be spread across limitless services, devices, applications, and users, it is not enough to know just who is trying to access network resources, but practitioners also need to understand the context of each access request. The first line of defense against potential security threats, Identity Verification, involves more checkpoints, such as understanding a user's

Identity Intelligence Readiness

Formative
48%

Beginner
34%

Progressive
13%

Mature
5%
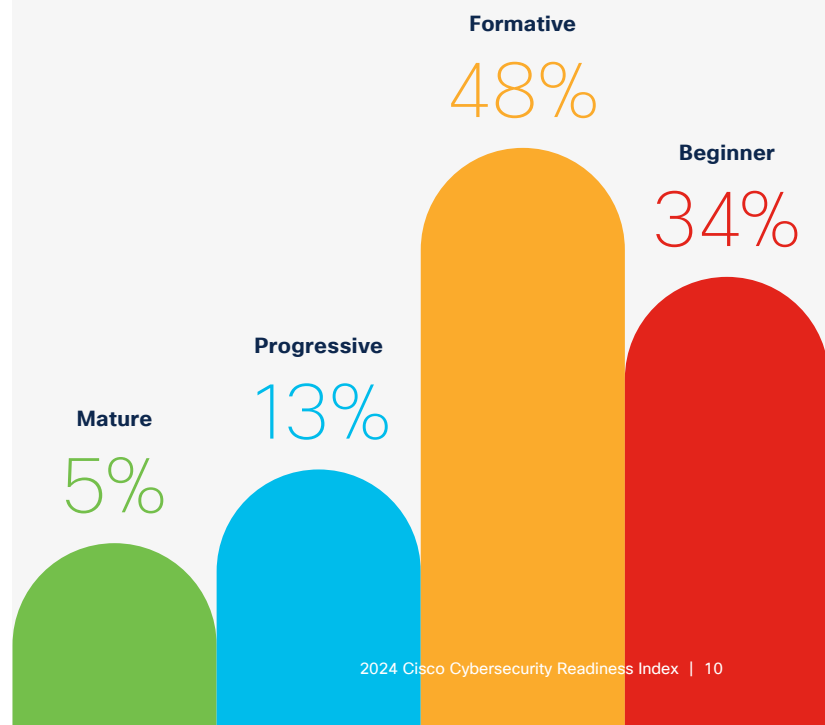
identity across different contexts, analyzing their behavior, and providing accurate recommendations for access control and security policies. More than that, companies should be able to identify patterns, detect anomalies, and predict a user's future actions based on the analysis of their behavior and have the capability to provide real-time assessment of risks associated with it. **We should no longer be asking "can" the user have access, but "should" the user have access**.

While rising to the growing concerns around identity protection is no small feat, companies must also ensure a seamless user experience for employees while guarding their data and platforms.

Areas Companies Find Most Challenging to Protect Against Cyberattacks

|	
Identity Intelligence	36%
Network Resilience	34%
Cloud Reinforcement	17%
Machine Trustworthiness	13%

On the back of all these added complexities, we see gaps in companies' maturity when it comes to Identity Intelligence, with more than four in five (82%) in either the Formative or Beginner categories, and only 13% qualifying as Progressive and 5% as Mature.

Adding to that, our research underscores identity protection as a major challenge, with 36% of respondents ranking it as their organization's top cybersecurity challenge, up from 24% in 2023. Given the understanding of the task at hand, it is no surprise that 99% have implemented some kind of identity management solution.

The most deployed identity solutions among respondents were Identity Behavior Analytics tools, which have been deployed by 54% of all companies. Also deployed by around half of all companies are continuous risk-based access analytics (50%), cross-context identity analytics and recommendations (48%), and real-time risk-based analytics (46%) tools. Cross-context identity posture assessment and passwordless authentication are deployed by around one-third of all companies (37% and 31% respectively).

Amongst companies that have not yet deployed these identity solutions, around half (51%) plan to do so in the next 12-24 months. Only around 10-12% do not currently plan to deploy these solutions. This represents a marked increase in the sense of urgency around deploying multiple identity management systems since we last surveyed companies in 2023. At that time 69% of companies who had not deployed identity management solutions had no intent to do so.

The rising deployment of AI technologies is both enabling new potential threat vectors and helping deploy identity management systems. The good news is that companies are already starting to leverage these capabilities. On average nine out of 10 companies said they are at least partially using AI in their various solutions to verify and secure identity.
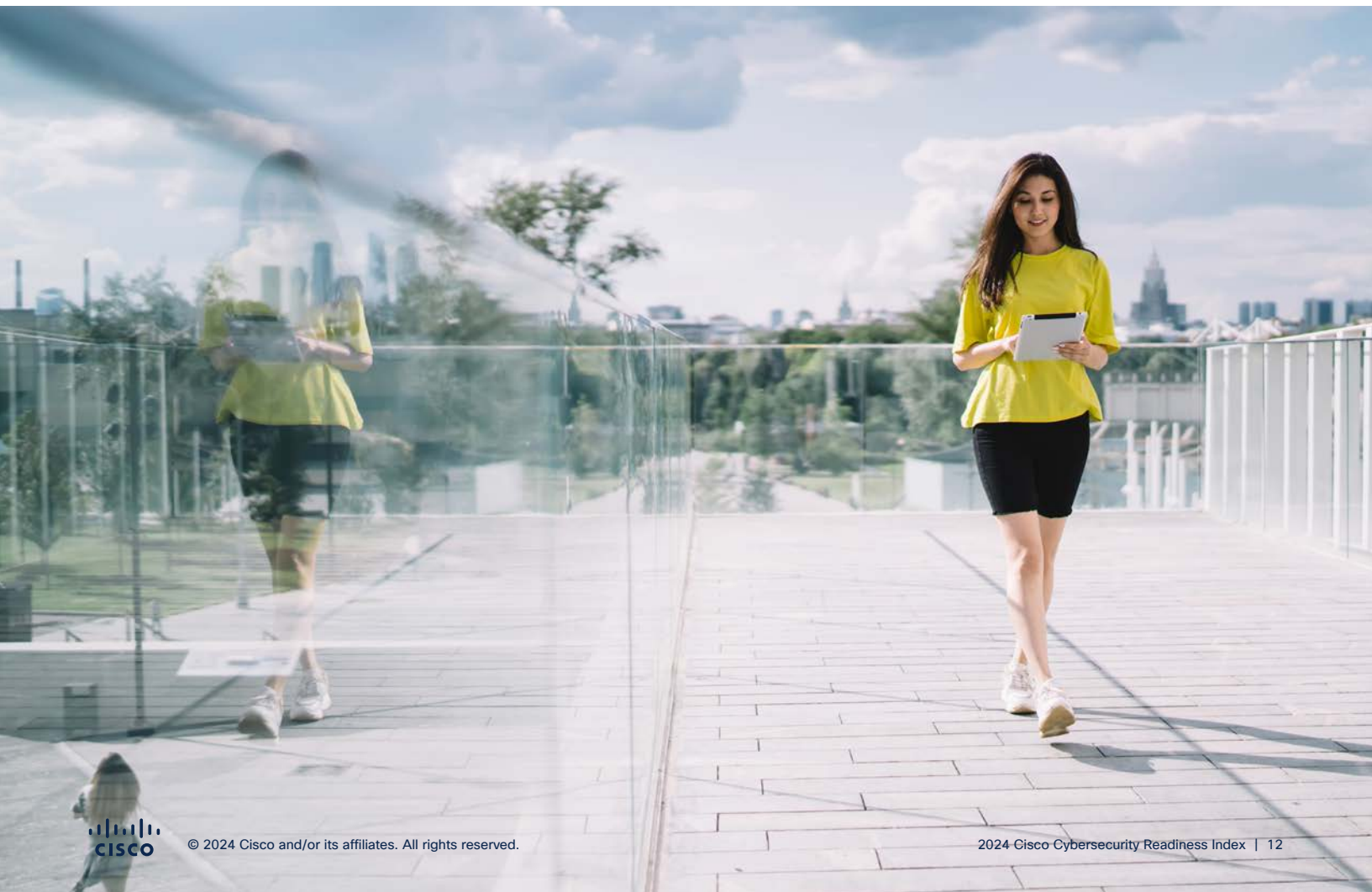
Machine Trustworthiness

The need to access data on the move and in a variety of forms has created an explosion in the number of devices employees use. From laptops, to tablets, to smartphones and smart watches – employees are working from a range of devices.

This hunger for on-the-go access created an explosion in the number of connected devices in recent years, and this trend is going to continue. And it is not just devices such as laptops, tablets, and smartphones that are getting connected, there has been a significant increase in the number of other smart devices that are coming online. According to industry estimates, billions of new devices are expected to get connected over the next few years, generating data running into zettabytes. These range from soil moisture detectors, connected microscopes, plant machinery, and even door security systems.

Machine Trustworthiness Readiness

Mature 7%

Progressive 21%

Formative 48%

Beginner 24%
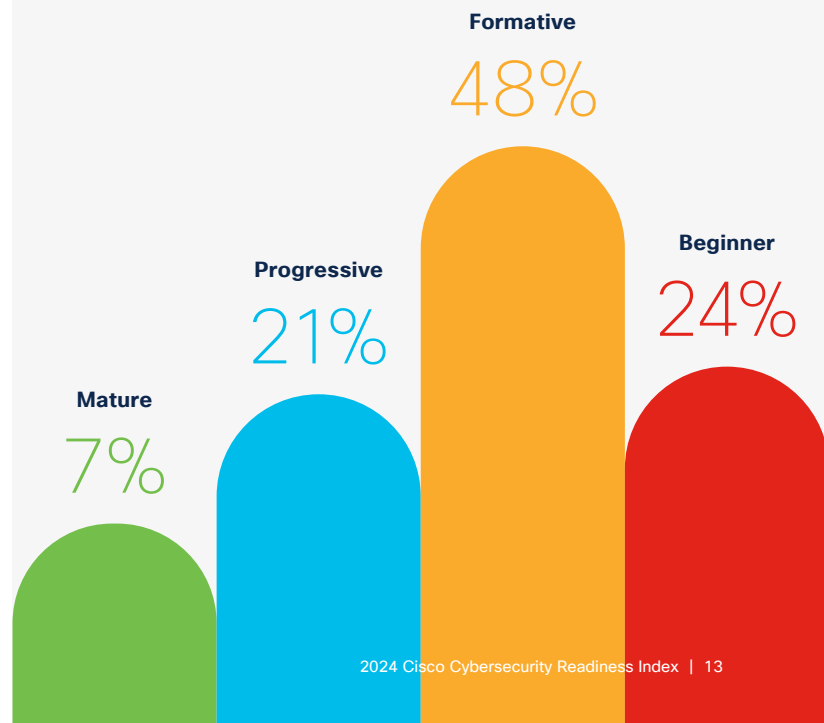
However, every connected device presents a potential entry point for malicious actors to infiltrate an organization's network. There have been — and continue to be — significant data breaches originating from access through devices that are not protected. So, no matter what type of device connects to a network, it needs to be protected.

To do so effectively, organizations must authenticate the integrity of the device that is about to be connected and have built-in protections and endpoint protection tools. This will allow them to remotely manage the device and detect any anomalies in how that device is behaving in real time.

To that effect, we see that nearly two-thirds (63%) of our respondents have chosen to use built-in solutions such as host-based firewalls and IPS as key solutions to protect machines. Organizations recognize the privileged position of basic input/output system (BIOS) in initializing operating systems and their associated vulnerabilities, with 57% rolling out solutions in this area. Machine behavior and anomaly-protection tools have also proven valuable in a company's arsenal to defend against machine threats, with 47% deploying this solution.

However, there are two key trends of particular concern. Firstly, the scale of deployment remains predominantly partial. This is why, despite the high number of respondents saying they have machine protection solutions in their posture, nearly half (49%) of the companies are either at the very start of their journey, or only partially down the path. While we did not ask respondents to explain why the deployment of any solution is only partial, it could be because of multiple factors such as shortage of talent that is hindering timely completion of deployment, lack of in-depth understanding of a particular solution to ensure full scale deployment, issues with interoperability with other solutions in the security stack, or any combination of internal or external factors.

The second concerning trend is that when asked how challenged they feel when it comes to protecting various pillars that are assessed in the Index, respondents ranked machines as fourth, behind identity, network, and cloud. This could either be driven by them feeling confident in their ability to secure machines, or that they have not yet assessed the full scale of the risks they face on this front, especially as a range of OT and IoT devices start to get connected.
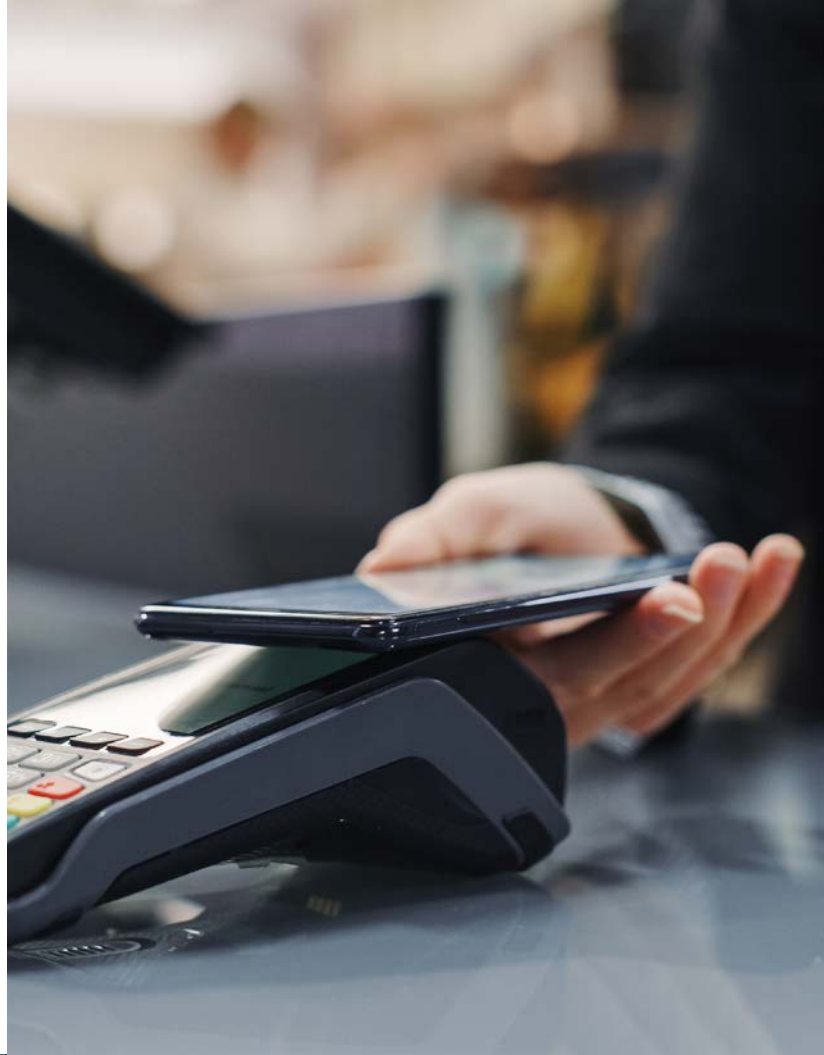
There is the possibility that in some industry sectors there may even be an assumption that attacking a device is not the most lucrative thing for malicious actors — it is just a means to go after the identity and the network. Whatever the reason might be, it is critical to address this discrepancy because the findings of the Index show that readiness on this front has dropped drastically in the past year.

Only 7% of companies are in the Mature category in this pillar and a further 21% are in the Progressive category. Three out of four (73%) companies are in the two lagging categories of readiness, with 48% in the Formative stage and 24% rated as Beginners.
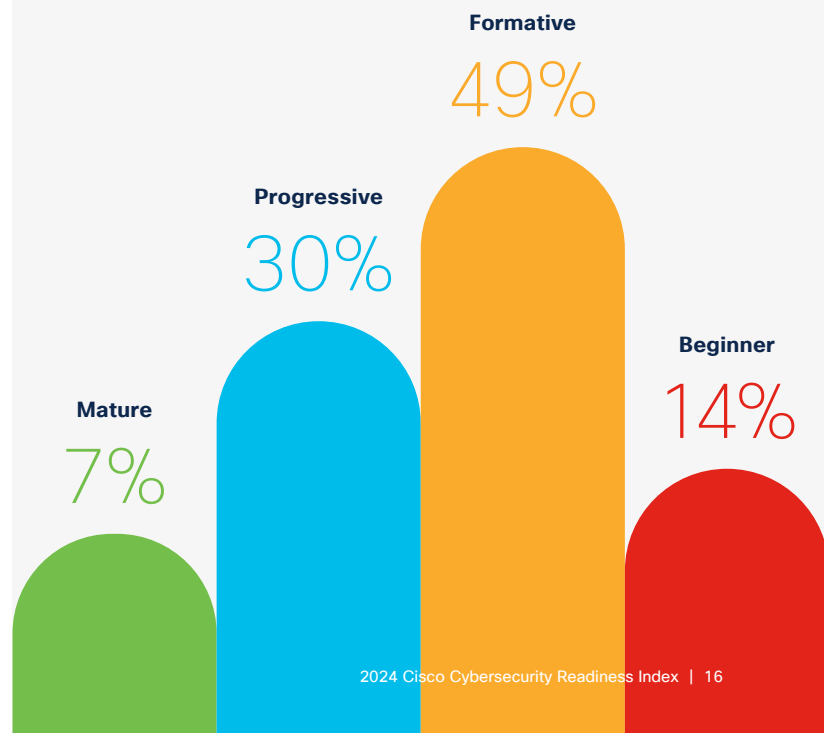
Network Resilience

With today's hybrid work environment calling for flexibility not only in the number and type of devices that employees use, but also in where they log in from, and where the data they need to access is stored and processed, network protection has never been more important for cybersecurity resilience.

The growth of cloud strategies — a bedrock of hybrid work — means that employees need to be able to roam across multiple networks throughout their day, rendering the network more vulnerable to cyberattacks.

When it comes to cyberattacks, there were more than 2,800 publicly disclosed data breaches[1] in 2023 alone — involving over 8.2 billion records stolen. And the likelihood is that this is just the tip of the iceberg — with thousands more data breaches taking place in less well-known organizations.

1. https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023#:~:text=According%20to%20our%20research%2C%20there,total%20to%20over%205%20billion.

Network Resilience Readiness

Formative
49%

Progressive
30%

Beginner
14%

Mature
7%

To make matters more complicated for organizations, the majority of the data that moves across networks is now encrypted. This is making it doubly difficult for companies to spot malicious packets of data that may have been injected to attack the network.

That is why companies need to build resilience in their networks through concepts such as segmentation, micro-segmentation, network sandboxes, firewalls, and network behavior anomaly detection tools that can detect irregularities from all network cardinal directions. In addition, they need solutions like encrypted traffic analytics that can help them identify malicious packets of data in encrypted data traffic without having to decrypt it, so they can keep both the data and their network secure.

The good and the bad news is that companies across the globe recognize this challenge, with network protection ranking second in the list of their top four cybersecurity challenges.

With these trends, the findings of this pillar show that most have opted to use firewalls with built-in Intrusion Prevention Systems (IPS). Nearly three-quarters (74%) of firms surveyed said they had deployed this capability, with network behavior anomaly detection tools ranking number two (55% said they have deployed this), and encrypted traffic analytics coming in third at 53%. Segmentation and micro-segmentation tied at fourth place (37%).

However, the issue is that the scale of deployment is not keeping pace. Of those companies that have firewalls with built-in IPS, only 55% have fully deployed them, while 26% had only done a partial deployment at the time of the survey, and another 9% had just started the deployment. It is a similar story for network behavior anomaly detection tools. Of those who deployed these tools, only 48% reported full deployment, while 38% are at a partial stage, and 12% have just started.

The number is even lower for micro-segmentation and encrypted traffic analytics (ETA). Among those who implemented micro-segmentation, 45% partially deployed, while for those who have ETA capabilities, 39% have deployed those partially and 11% have just started. Perhaps unsurprisingly as a result, only 7% of companies are in the Mature category, and 30% are in the Progressive stage of readiness in this pillar. This clearly shows that more work needs to be done as 63% of companies fall in the Formative or Beginner categories.

Cloud Reinforcement

As organizations increasingly shift their operations to the cloud, there is a growing need for improved cloud security. Unlike on-premises infrastructure, where businesses own their systems, third-party service providers often manage cloud infrastructure.

These cloud service providers implement their own security measures and practices to protect the infrastructures and data they host, and organizations largely depend on these security measures for protection. However, while these measures are generally robust, they may not necessarily cater to the unique security requirements and policies of each organization and may potentially – and accidentally – expose businesses to a variety of vulnerabilities.

For instance, there might be certain security protocols that the cloud provider doesn't cover, or there might be differences in security standards. The third-party's security measures might not be as comprehensive or as stringent as the company's internal policies.

Cloud Reinforcement Readiness

Formative
54%

Beginner
27%

Progressive
15%

Mature
4%
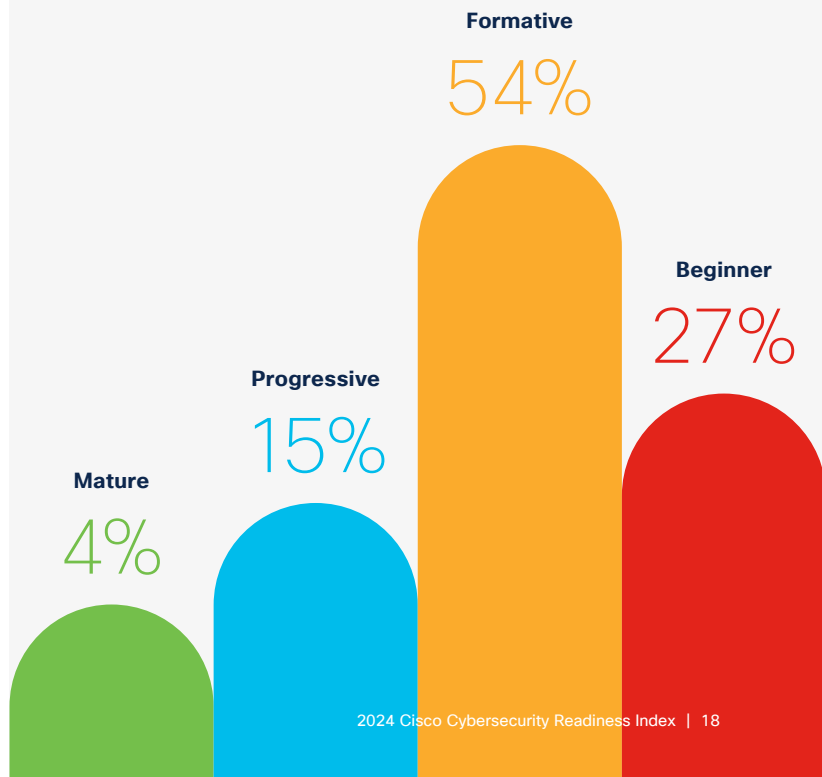
Also, potential gaps in a third party's security measures might go unnoticed, creating weak points that could be exploited. Therefore, to mitigate these risks, organizations should take proactive steps to enhance their cloud security.

Respondents have recognized the challenges, and almost all (98%) have deployed some kind of solution to reinforce cloud security. About six in 10 (59%) have opted to use a host software firewall, but application-centric protection tools were a close second with 49% of organizations choosing this to protect themselves. Less popular are dynamic vulnerability workload protection (46%) and visibility analytics tools (45%). ZTA, with centralized policy and distributed enforcement, ranked fifth.

While host software firewalls proved to be the most frequently deployed solution amongst surveyed organizations, only 63% have fully deployed it. Meanwhile 28% said they are at a partial state of deployment, while 9% said they have either just started deployment or not yet begun.

Deployment of application-centric protection tools is catching up, with 44% fully deployed and 52% presently deploying. The good news for nervous CEOs and those responsible for data governance is that most respondents who do not have this deployed (83%) plan to deploy application protection solutions within 24 months.

As organizations look to improve their cybersecurity posture, they should keep in mind that proactive coordination is paramount when dealing with cloud and application security risks. Bad actors can take advantage of gaps and delays between siloed security and application teams, resulting in costly and damaging consequences.

As business models move from static to dynamic, organizations must look at increasingly novel approaches such as Secure Access Service Edge (SASE) to be adequately prepared to tackle the risks these shifts present. SASE combines traditional network security functions with software-defined wide-area networking (SD-WAN) capabilities.

While SASE is a critical solution that allows organizations to provide secure and reliable access to cloud-based applications, only 22% of organizations have deployed it. Among the companies that are still deploying SASE, only 38% said they are planning to roll out within the next 12 months.

Finally, companies must be able to manage, apply, and maintain consistent security and operational rules across different cloud platforms. Having this ability not only ensures enhanced security and compliance by ensuring all platforms follow the same rules but also simplifies management and oversight, as an organization needs to manage only a single set of policies. Unfortunately, only 31% of companies have deployed this capability.

Based on the state of deployment of various capabilities, the majority of organizations fall into the Beginner (27%) or Formative (54%) categories for Cloud Reinforcement, with only 15% qualifying as Progressive and 4% as Mature.
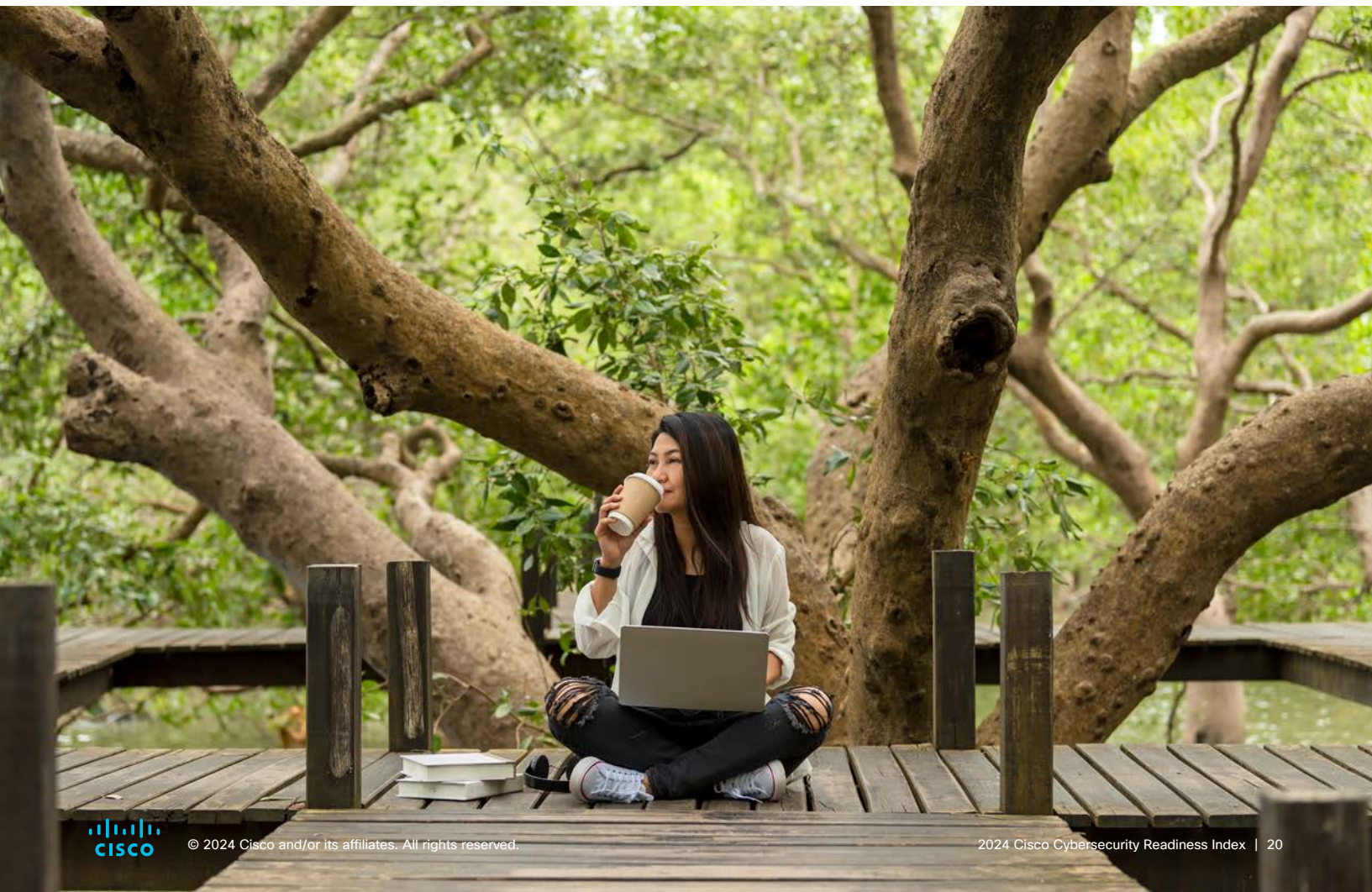
AI Fortification

The meteoric rise of Generative AI continues to create a plethora of opportunities for organizations, and cybersecurity solutions are no exception. But AI has also been leveraged by bad actors to wreak havoc on unprepared targets. As such, integrating AI into frontline defenses has become a critical ingredient to cybersecurity readiness and forms a new pillar in this year's Index.

When it comes to securing networks, a majority (52%) of organizations have yet to significantly incorporate AI into their security solutions. Those that have, usually choose to harness AI in either firewalls or segmentation to boost network protection. Organizations also report significant integration of AI into micro-segmentation and encrypted traffic analytics.

AI Fortification Readiness

Mature
7%

Progressive
46%

Formative
42%

Beginner
5%
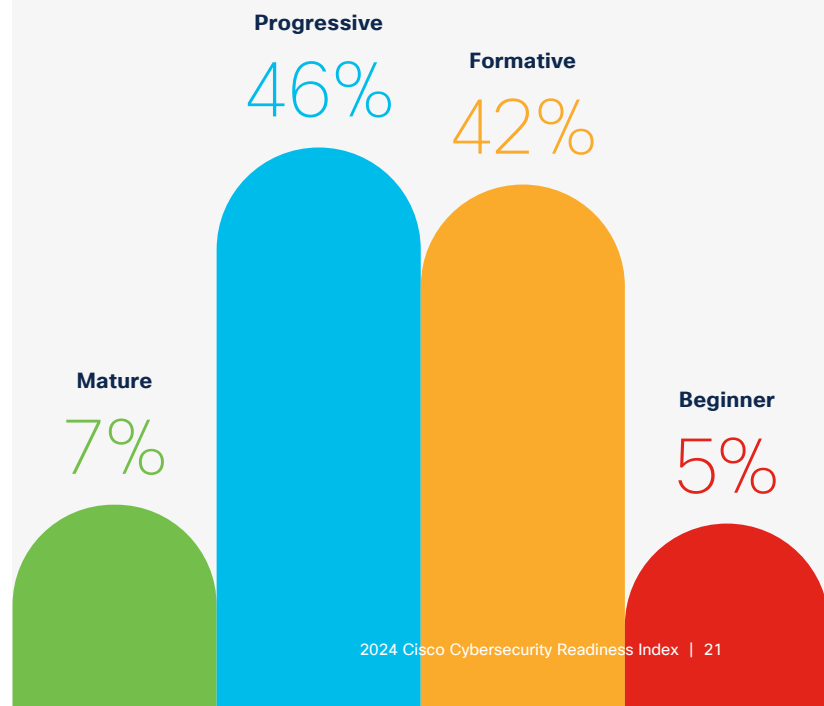
AI has also offered support for organizations looking to bolster identity intelligence solutions, but most have yet to significantly deploy AI in verifying and securing identity.

In this domain, significant AI deployment is mostly seen in posture assessments, monitoring passwordless authentication, and forming real-time, risk-based privilege access policy.

The management and protection of machines is another key area in which organizations could leverage AI for more support, with 55% yet to achieve significant rollout. Our respondents most frequently report significant use of AI in machine authentication and integrity (BIOS). Built-in protections such as firewalls and endpoint protection tools were also popular areas for major AI deployments.

With cloud reinforcement at the top of many cybersecurity leaders' minds, more can be done to bolster defenses with AI. Fifty-two percent of organizations are yet to harness AI in cloud defense applications. The highest portion report significant deployment of AI in host firewalls, followed by dynamic vulnerability workload protection and deploying and enforcing consistent policies across multiple clouds.

The nascent stage of AI's integration across cybersecurity functions explains why organizations at the Formative (42%) stage account for most of our survey respondents, followed by 46% Progressive, 7% Mature, and just 5% at the Beginner stage. This shows that while the vast majority have made some progress there is still a considerable way to go.

Industry and Size Matter

As we look at the industries that are most ready for the challenges ahead, 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.

Travel Services, often faced with the enormous challenge of keeping travelers' personally identifiable information safe, has one of the highest number of organizations in the Mature category (4%). The other two industries tied for highest number of companies in the Mature category are Manufacturing and Business Services, which include accounting, professional services, consulting, and advertising. This reflects the need to protect the large volume of valuable and confidential information these companies hold for their clients.

This leaderboard showcases significant changes since our 2023 survey, when the three industries leading the pack in terms of overall cybersecurity readiness were Retail, Financial Services and Healthcare, respectively. None of these sectors made the top five this year, though Financial Services did rank sixth in terms of overall maturity.

At the other end of the scale among major industries is Education, where a little over 17% of organizations fall into the Beginner category. The Education sector's large attack surface, combined with inconsistent cybersecurity awareness among users and limited budgets means that more safeguards are required to protect educators and students alike.

If we look at each of the five pillars of cybersecurity readiness, several other industries stand out in their preparedness to protect specific areas of their operations. Business Services and Media and Communications are equally the most progressed industries in Identity Intelligence, with 6% of organizations rated as Mature. It is no surprise that these industries are proactive in mitigating identity-related risk, which could involve bad actors using such companies' intellectual property in ransomware attacks.

In relation to Network Resilience, Technology Services and Travel Services lead the way with 9% of companies in both industries in the Mature segment.

When it comes to Machine Trustworthiness, respondents from the Healthcare industry show a high level of readiness (8% Mature), coming in second place after Technology Services (9%). Healthcare also tops the Readiness Index in Cloud Reinforcement (5% Mature). Given that healthcare organizations store large volumes of sensitive patient data on their machines and clouds, robust defenses in this area are critical.

Technology Services organizations have been quick to recognize both the risks and opportunities presented by AI, with 10% of companies categorized as Mature in the AI Fortification measure. This level of maturity far outstrips that of other industries, in which the learning curve to AI adoption in cybersecurity functions may be steeper.

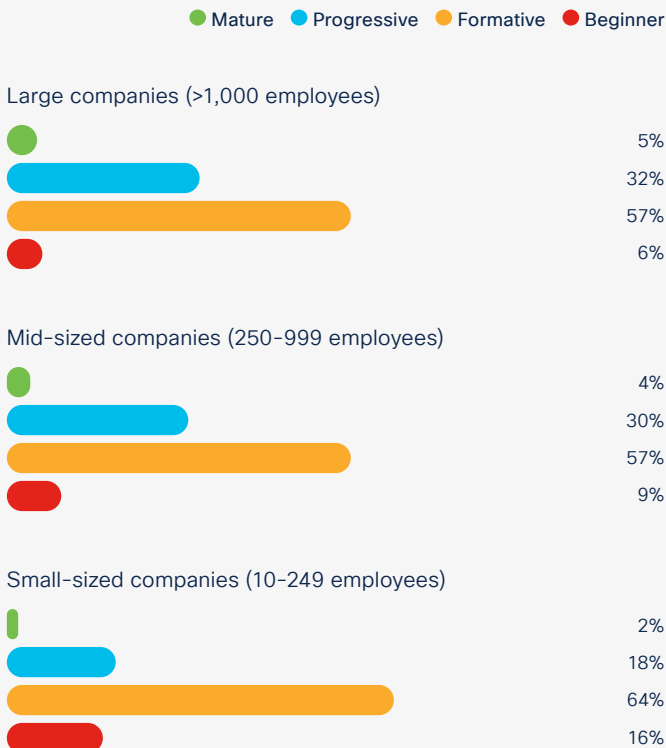## Readiness Levels Across Industries (Top and bottom three)

Mature

✈	Travel Services	4%
💼	Business Services	4%
🏭	Manufacturing	4%

Beginner

♡	Personal Care and Services	18%
👤	Education	17%
📦	Wholesaling	15%

Overall Readiness by Company Size

● Mature ● Progressive ● Formative ● Beginner

Large companies (>1,000 employees)

● Mature	5%
● Progressive	32%
● Formative	57%
● Beginner	6%

Mid-sized companies (250-999 employees)

● Mature	4%
● Progressive	30%
● Formative	57%
● Beginner	9%

Small-sized companies (10-249 employees)

● Mature	2%
● Progressive	18%
● Formative	64%
● Beginner	16%

As we might expect, there are differences in readiness depending on the size of the organization. Unsurprisingly, it is the large-sized companies — those of more than 1,000 employees — that are best prepared with more organizations in the Mature category (5%) than their smaller competitors, and more in the Progressive category (32%) too.

Mid-sized organizations are not far behind with 4% in the Mature category. While they may not enjoy the same budgets as their larger counterparts, they often benefit from being agile enough to be able to deploy without the bureaucracy of larger businesses.

It goes without saying, unfortunately, that smaller organizations – those of up to 250 employees – tend to be less ready, with large numbers dropping into the Formative (64%) and Beginner (16%) categories. With the inclusion of the AI Fortification pillar in the Index, the performance of small organizations has improved year-on-year (32% in the Beginner category in 2023). This may be because AI-enhanced cybersecurity has allowed smaller organizations to plug some of the labor and expertise gaps that set them apart from larger counterparts, although clearly this alone is not sufficient to level the playing field.

What's more, small organizations show a greater disparity between the two ends of the readiness spectrum. There are several times more Beginners than Mature organizations among smaller organizations in most pillars of security readiness. The exception to this is in the AI Fortification pillar, where there are fewer than double the number of Beginner companies compared to Mature. This smaller gap may be due to small businesses having less manpower and more agility, thus spurring the rapid introduction of AI to cybersecurity functions.

AI aside, while organizations of all sizes are most progressed in Network Resilience, 16% of small-sized organizations are in the Beginner category, significantly more than those that fall into the Mature category (2%). The disparity could be due to the diversity among companies of this size, which may comprise family businesses, professional services firms, tech start-ups and more — all with varying levels of know-how. With small and medium enterprises representing about 90% of businesses and more than 50% of employment worldwide[2], more support is needed to help them ramp up their security readiness.

---

2. https://www.worldbank.org/en/topic/smefinance
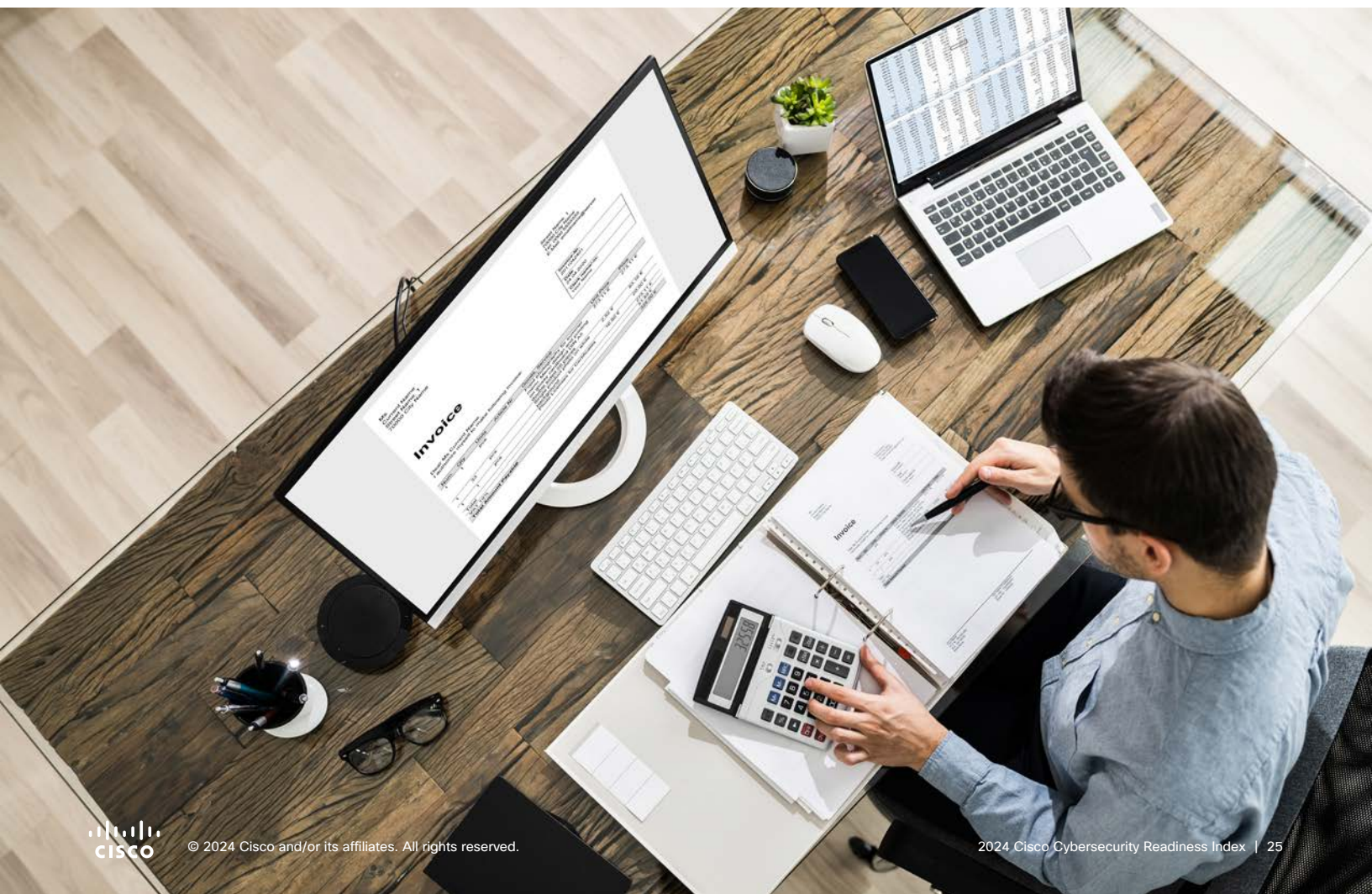
Underprepared and Overconfident

All five pillars of security need to be protected and work in harmony; otherwise, organizations risk being a greater target for bad actors. Our report finds that organizations globally recognize the urgency to continually up their cybersecurity game, as evidenced by the increasing focus and expanding headcount and budgets being devoted to addressing cybersecurity threats.

Unfortunately, these efforts have overall been insufficient in addressing the rapid increase in the frequency and sophistication of cybersecurity threats.

The overall state of achieving cybersecurity readiness, therefore, is still in early maturity – and presents a challenge for today's organizations.

Several industries appear to have been unable to sustain the momentum in across-the-board efforts to maintain security readiness, with all three industries that were leading the pack in terms of overall cybersecurity readiness in 2023 – Retail, Financial Services and Healthcare – failing to make the top five this year.

Since the last survey, the normalization of hybrid work has proliferated potential network risks, with 29% of employees hopping between at least six networks weekly and 85% of companies saying their employees access company platforms from unmanaged devices.

As a result of the increasing complexity of cybersecurity threats, companies faced a more complex variety of attacks in the last year from ransomware (35%), credential stuffing (37%), supply chain attacks (32%), social engineering (32%), and cryptojacking (27%). The situation continues to evolve as 11% of companies predict AI-related cyber threats to be among the top three risks in the year ahead.

The financial impacts of cybersecurity incidents continue to remain pronounced, with most incidents triggering losses of at least US$300,000, and 12% exceeding US$1 million.

Adding to this, many organizations have accumulated multiple point solutions over the years, which now adds complexity to the landscape. In fact, 67% of organizations indicated they have 10 or more solutions deployed in their security stacks, and a staggering 80% acknowledge that multiple point solutions impede their team's efficiency in detecting, responding to, and recovering from security incidents. This becomes even more complex with a shortage of skilled talent in the sector, with 46% of companies having more than five positions unfilled at the time of the survey.

While cybersecurity readiness is very low across the board, the lack of preparedness evidenced in the Identity Intelligence and Cloud Reinforcement pillars is particularly acute and this needs to be the focus of serious increased investment over the next 12–24 months. To help close the security gap, companies should continue to keep abreast of the latest advances in AI-powered security technologies — as malicious actors looking to exploit vulnerabilities will be.

Despite increasing threats, a worrying 80% of companies feel moderately to very confident in their ability to stay resilient amidst this evolving cybersecurity landscape. It highlights a mismatch in what companies think they can handle versus what they may be able to handle in the wake of a rapidly evolving cybersecurity landscape.

The good news is that organizations realize the need to act, with over half planning to significantly upgrade their IT infrastructure in the next one to two years. Companies are also ready to increase security budgets as they see a rise in risks due to digitization, a growth in types of attacks and threats, and a heavy financial impact. Almost nine in 10 (86%) expect their cybersecurity budget to grow by more than 10% in the next 12 months.

Although companies have been devoting more focus, money and resources to address cyber threats, and expect to accelerate these efforts further over the next 12–24 months, the current readiness levels are low. In short, the sophistication, scale and frequency of cybersecurity threats are currently overwhelming protective measures being taken by companies. Solutions deployment is not being rolled out as quickly as it needs to be, leaving some organizations vulnerable to attack.

When the consequences of cyberattacks are so clear to see, readiness must be a priority for all organizations, and deployment of solutions needs to be accelerated even further.
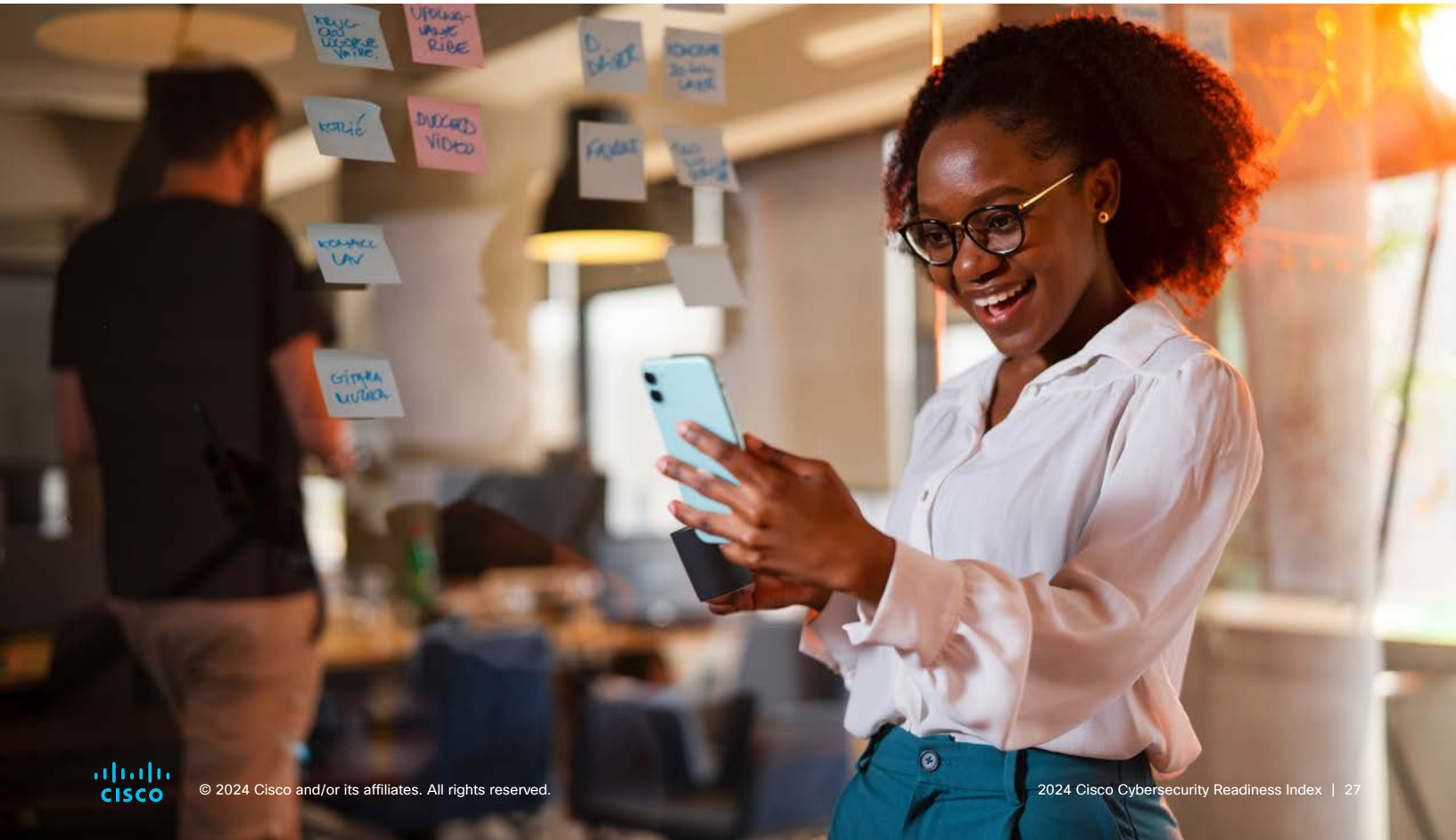
Recommendations

1. Continue to accelerate investment in protective cybersecurity measures across the board, including adopting a platform approach to ensure all solutions in the security stack can be leveraged to their maximum ability.

2. Urgently assess and close vulnerability gaps created by unmanaged devices and unsecured Wi-Fi networks.

3. Keep abreast of the latest developments in Generative AI technology and leverage them to enhance security programs and operational resilience.

4. Ramp up the recruitment and upskilling of in-house talent to close cybersecurity talent gaps. Where possible, leverage the advancements in AI to augment and automate tasks while leaning on external cybersecurity expertise to help close key gaps in building and operating cybersecurity infrastructure.

5. Establish a company baseline of how 'ready' you are across the five major security pillars, continually monitor, and act where needed.

About the Research

The **2024 Cisco Cybersecurity Readiness Index** is based on a double-blind survey of 8,136 private sector business leaders who have cybersecurity responsibilities in their organizations.

The organizations 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**, **USA**, 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. The scores for each organization were then derived based on the stage of deployment of various solutions under each of the five pillars, with partially deployed solutions assigned a 50% weighting and fully deployed solutions weighted at 100%.

The scores for each pillar are then combined and weighted to arrive at an overall cybersecurity readiness score for each organization. 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 2024 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
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
Machine Trustworthiness	**20**
Machine authentication and integrity (BIO Security)	20
Machine 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
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