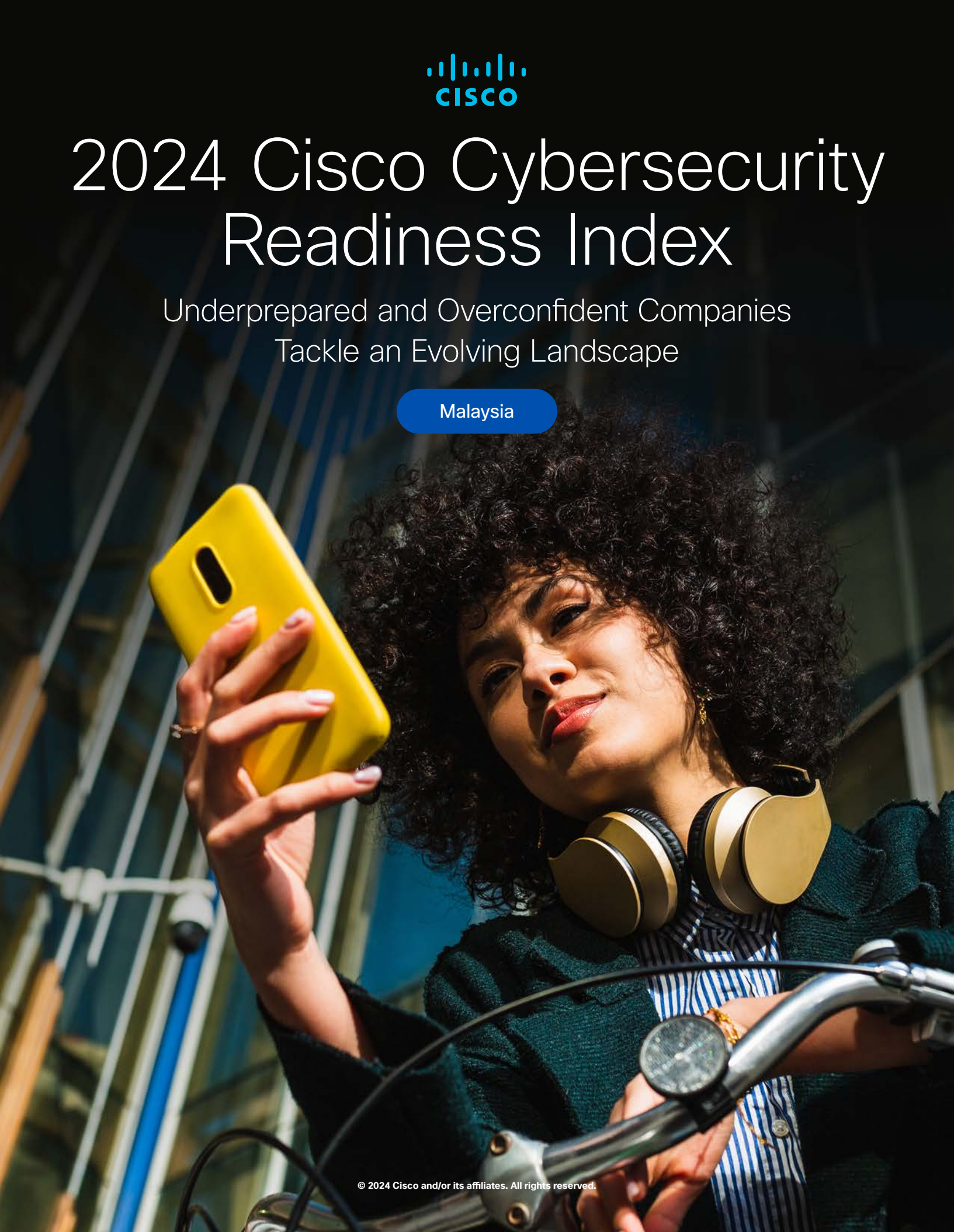
2024 Cisco Cybersecurity Readiness Index

Underprepared and Overconfident Companies Tackle an Evolving Landscape

Malaysia



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.

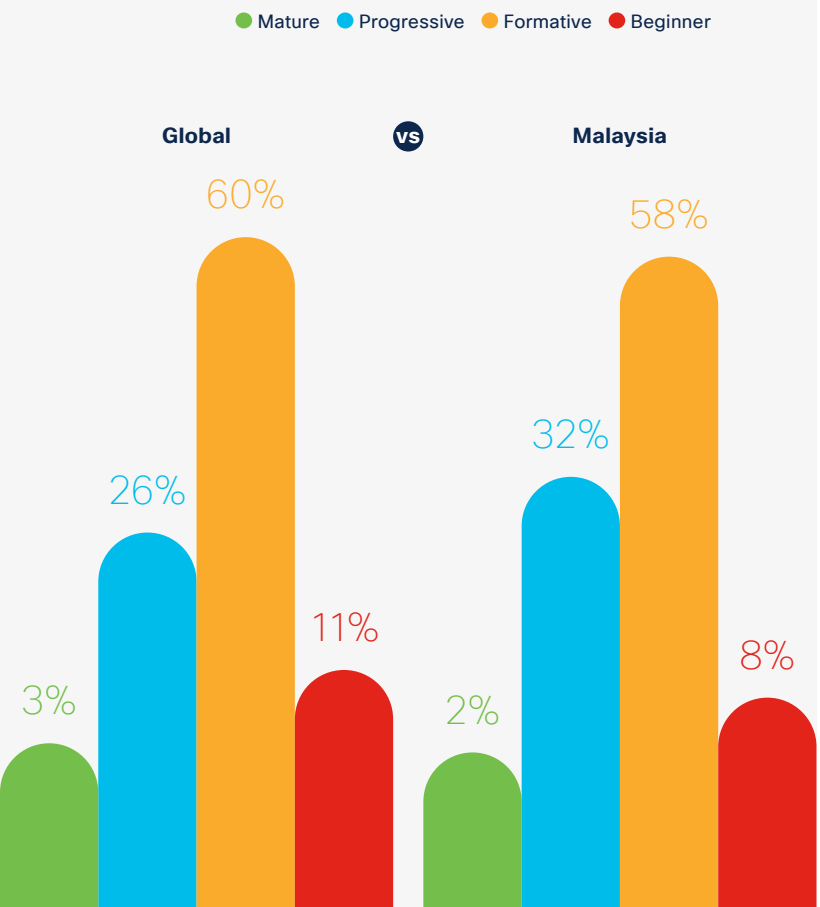
Based on five pillars of cybersecurity readiness that are most relevant to securing today's organizations – **Identity Intelligence**, **Network Resilience**, **Machine Trustworthiness**, **Cloud Reinforcement**, and **Artificial Intelligence (AI) Fortification** – the 2024 edition of this study shows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

The State of Global Cybersecurity Readiness

When assessing global cybersecurity readiness for this Index, 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 Malaysia, 2% of organizations are at the Mature stage of readiness, 32% are at the Progressive stage, 58% are Formative, and 8% are Beginners.

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.

Overall Readiness



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 is that despite this lack of readiness, 31% of companies feel 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 that 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 and human power can be dedicated to cybersecurity. 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).

Closing the Readiness Gap

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.

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 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

Identity Intelligence

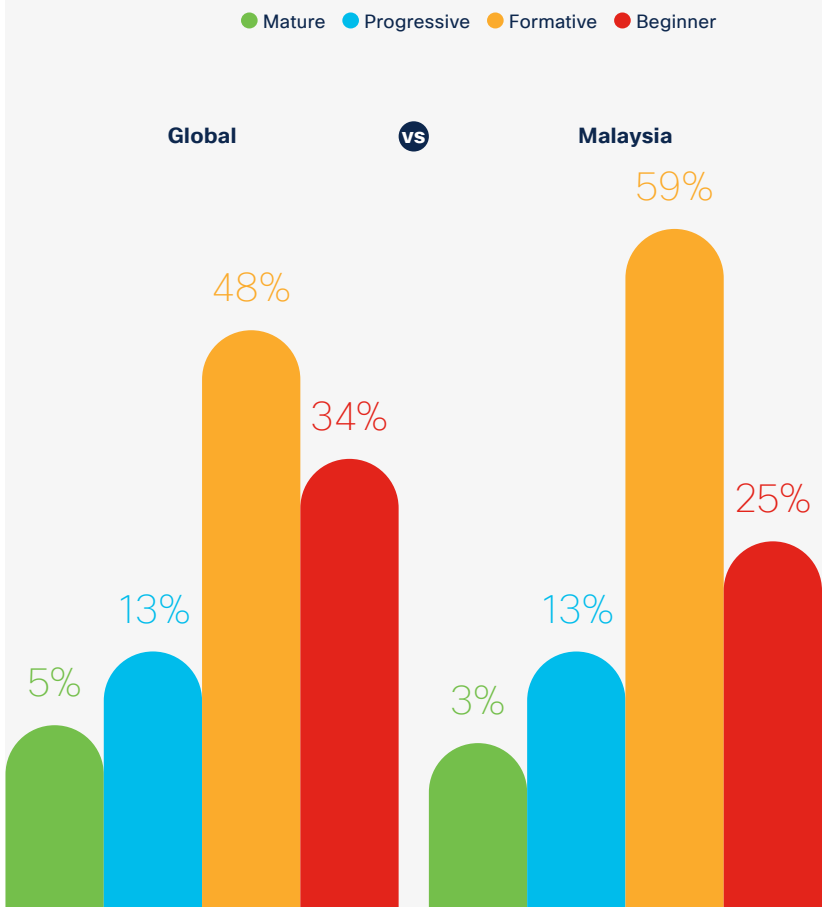
There is significant progress to be made to meet the challenge of Identity Intelligence. Only 5% of organizations globally fall into the Mature category, with 13% in the Progressive segment. The majority fall into the more basic levels of readiness, with 48% in the Formative category and 34% as Beginners.

The situation is slightly worse in Malaysia as only 3% of organizations fall into the Mature category, with 13% in the Progressive segment. 84% of organizations in Malaysia fall into the Formative (59%) or Beginner (25%) category, which is worrying given the clear threat presented by identity management.

Until recently, security practitioners' focus had traditionally been on creating a strong perimeter to keep out potential threats by mostly relying on identity management solutions such as data stores that contain information like a user's username, password, and identity.

However, in today's distributed working environments, Identity Intelligence involves a lot more checkpoints such as understanding the user's 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**, all while ensuring a seamless user experience.

Identity Intelligence Readiness



Machine Trustworthiness

The level of readiness to tackle the cybersecurity challenge on the machine front is still low. Only 7% of companies globally are in the Mature category, with a further 21% at the Progressive stage. However, nearly three-quarters of companies are either in the Beginner (24%) or Formative (48%) category.

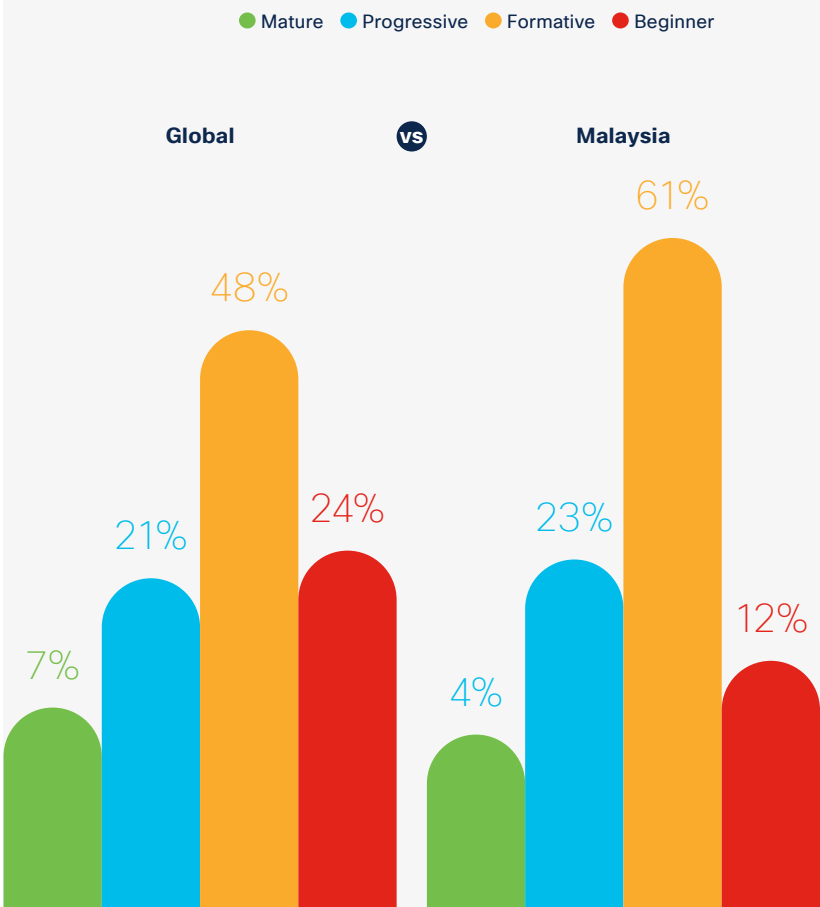
In Malaysia, only 4% of organizations are at the Mature stage of readiness, while nearly a quarter (23%) are at the Progressive stage. In line with global averages, nearly three-quarters (73%) of Malaysian organizations are either in the Formative (61%), or Beginner stage (12%).

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, smartphones, smart watches and beyond – employees are working from and connecting to a wide range of devices, and every connected device presents a new attack opportunity for malicious actors. So, no matter what the device, if it is connected to the network, it needs to be protected.

Despite many companies claiming to have machine protection solutions, deployment remains partial. Fifty-six percent of companies globally are either at the very start of their journey or only partially down the path. Respondents also ranked machines as the fourth most challenging pillar to protect, indicating either their confidence in their ability to secure machines or their lack of understanding of the full scale of risks associated with OT and IoT devices.

Machine Trustworthiness Readiness

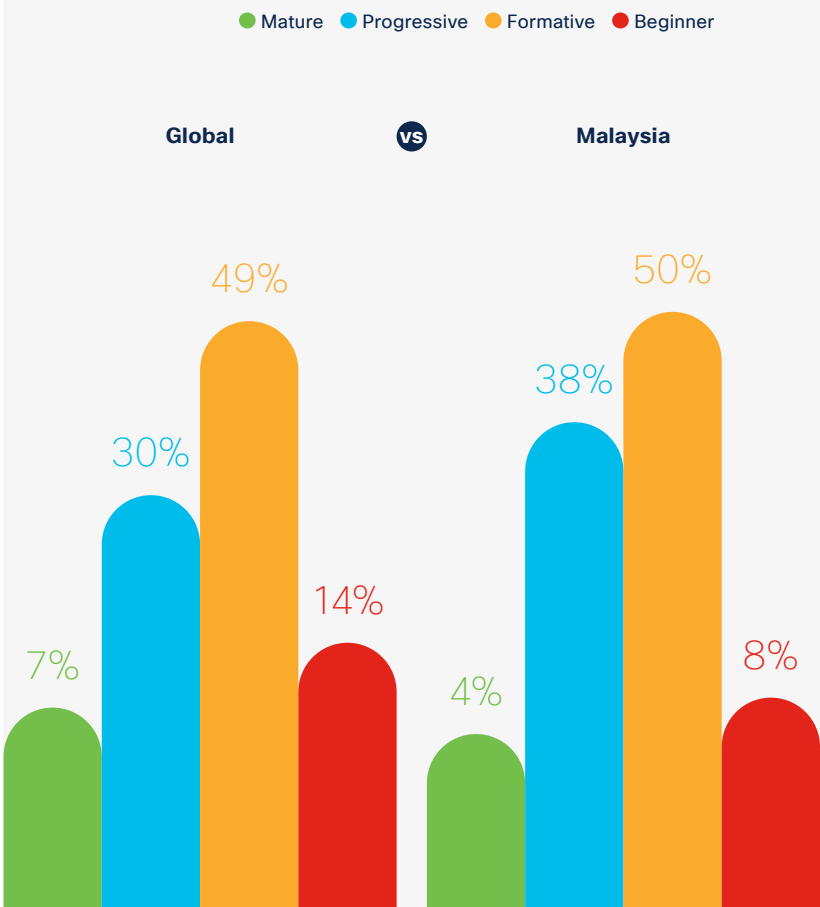


Network Resilience

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.

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. And companies recognize this, with network protection ranking second in the list of their top four cybersecurity challenges.

Network Resilience Readiness



That is why companies need to build resilient networks with solutions such as segmentation, micro-segmentation, network sandboxes, firewalls, and anomaly detection tools. Encrypted traffic analytics can also help identify malicious data packets without decryption. While some companies are making progress on this, the scale of deployment is still an issue, many of them having only partially deployed network resilience solutions.

While our respondents recognize this, their organizations are lagging far behind in their preparations to tackle the cybersecurity risks on this front. Nearly two-thirds of companies globally (63%) are either in the Formative or Beginner category and just 7% sit in the Mature category – the most advanced state of readiness.

In Malaysia, 4% of organizations are at the Mature stage of readiness, 38% are at the Progressive stage, half (50%) are at the Formative, and just 8% are Beginners.

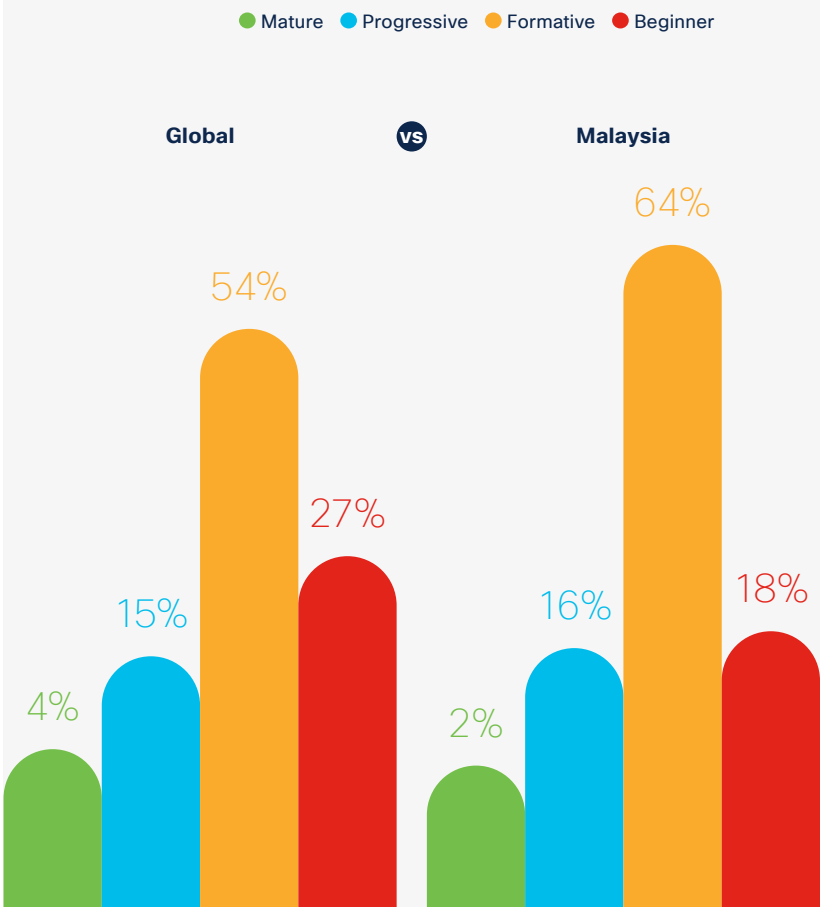
Cloud Reinforcement

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

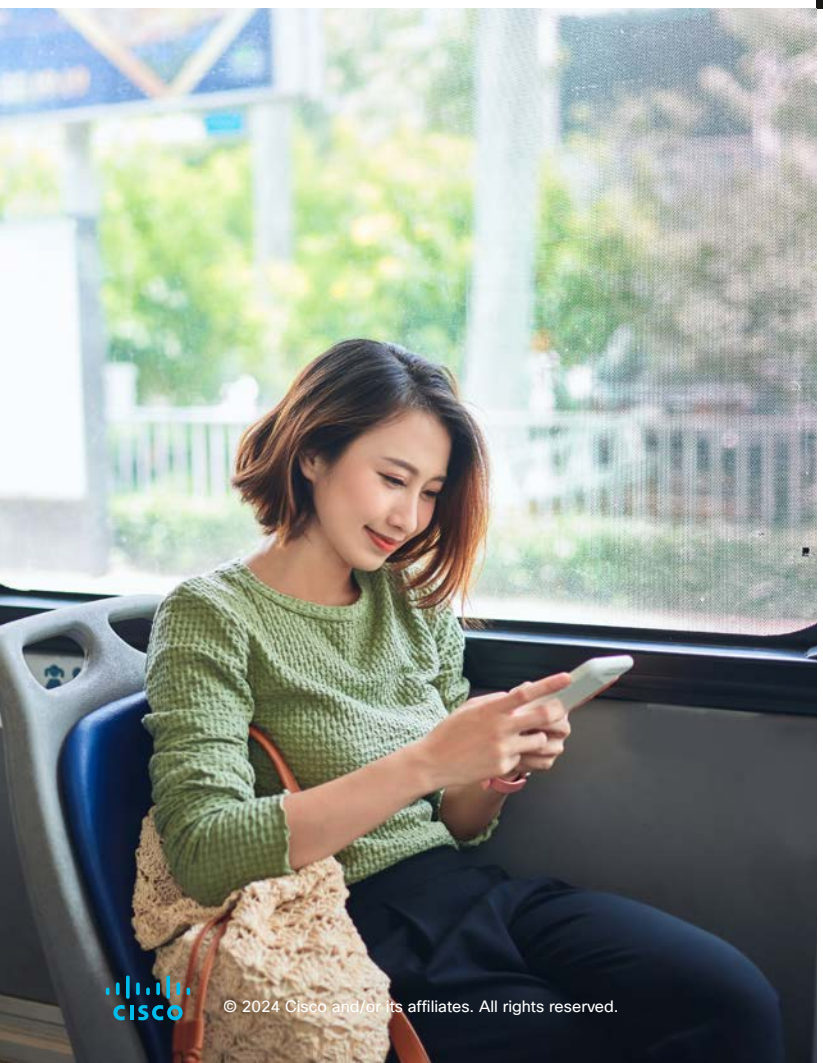
These cloud service providers implement their own security measures and practices to protect the infrastructure and data they host, and organizations largely depend on these security measures for protection.

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 expose businesses to a variety of vulnerabilities. Respondents have recognized the challenge and almost all have started to deploy some kind of solution to reinforce cloud security. The issue, though, is that the scale of deployment remains low.

Cloud Reinforcement Readiness



With companies adopting a hybrid cloud operating model, they 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 globally have deployed this capability.



Our survey shows that only 4% of companies globally are in the Mature stage in this pillar, the smallest number across the five areas that we have assessed. Meanwhile, 81% of companies globally are in the Formative or Beginner stage.

In Malaysia, 2% of organizations are at the Mature stage of readiness, 16% are at the Progressive stage, most (64%) are Formative, while only 18% are Beginners.

AI Fortification

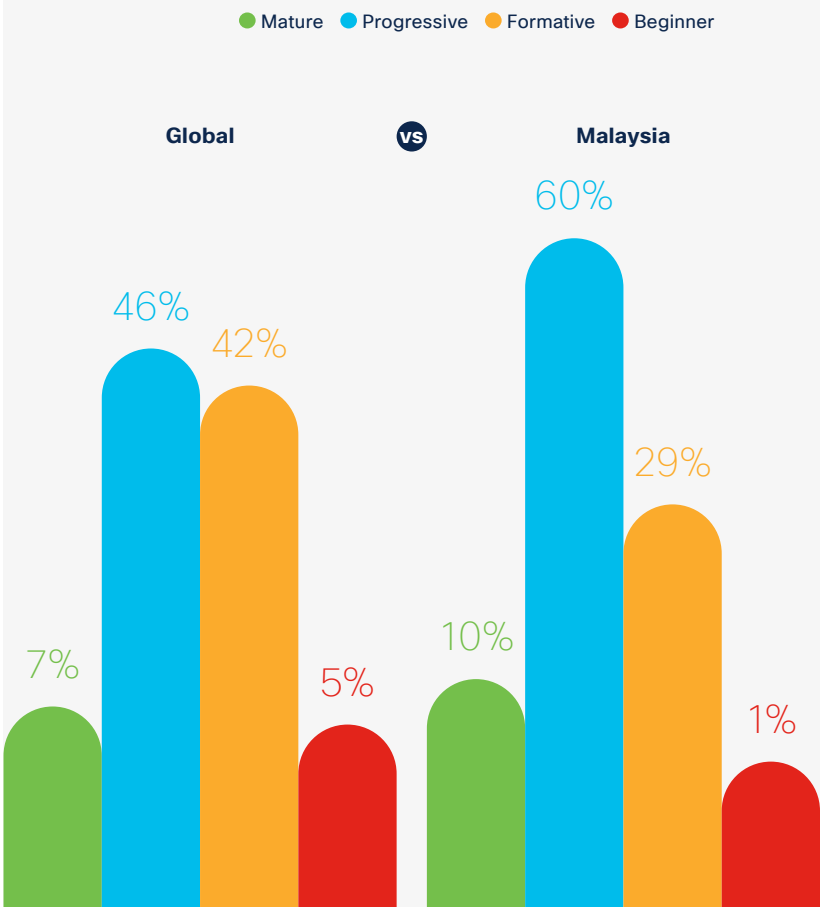
The meteoric rise of Generative AI continues to create a plethora of opportunities for organizations, and cybersecurity solutions are no exception. But AI has also been leveraged by bad actors to wreak havoc on unprepared targets. As such, integrating AI into frontline defenses has become a critical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

Despite the potential benefits of using AI to secure networks and identities, protect machines, and reinforce cloud security, more than half of organizations have not yet deployed AI in any of the four cybersecurity pillars. This suggests that there is still a significant opportunity for organizations to leverage AI as part of their overall cybersecurity strategy.

The nascent stage of AI's integration across cybersecurity functions explains why organizations at the Progressive (46%) stage account for most of our survey respondents, followed by 42% Formative, 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.

In Malaysia, one in 10 (10%) organizations are at the Mature stage of readiness in AI Fortification, most organizations (60%) are at the Progressive stage, 29% are Formative, and only 1% are Beginners.

AI Fortification Readiness



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

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**