Cybersecurity Resilience in Mid-Market Organizations

The 2025 Benchmark Study Across Asia Pacific and Japan

A Tech Research Asia Insights Report
Commissioned by Palo Alto Networks
JAPAC Edition | April 2025

© 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Foreword

The typical mid-market organization is navigating an increasingly complex and hostile threat landscape today:

- Attacks are more sophisticated and often AI-driven, evading traditional security solutions
- A lack of skilled cybersecurity practitioners weakens cyber defenses
- With hybrid work, more connected devices and the popularity of cloud-based applications, the attack surface has grown
- Multiple cybersecurity implementations can be a challenge to manage

These challenges can only be addressed with more support to demystify cybersecurity and strengthen cyber resilience.

Mid-market organizations are already prime targets for cybercriminals with their relatively tight tech budgets and small IT teams, coupled with access to larger enterprises and a significant amount of intellectual property. There is no better time to transform the narrative.

The inaugural Palo Alto Networks Cybersecurity Benchmark for mid-market organizations in Asia-Pacific and Japan (JAPAC), together with recommendations for next steps, will be a key catalyst for positive change.

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

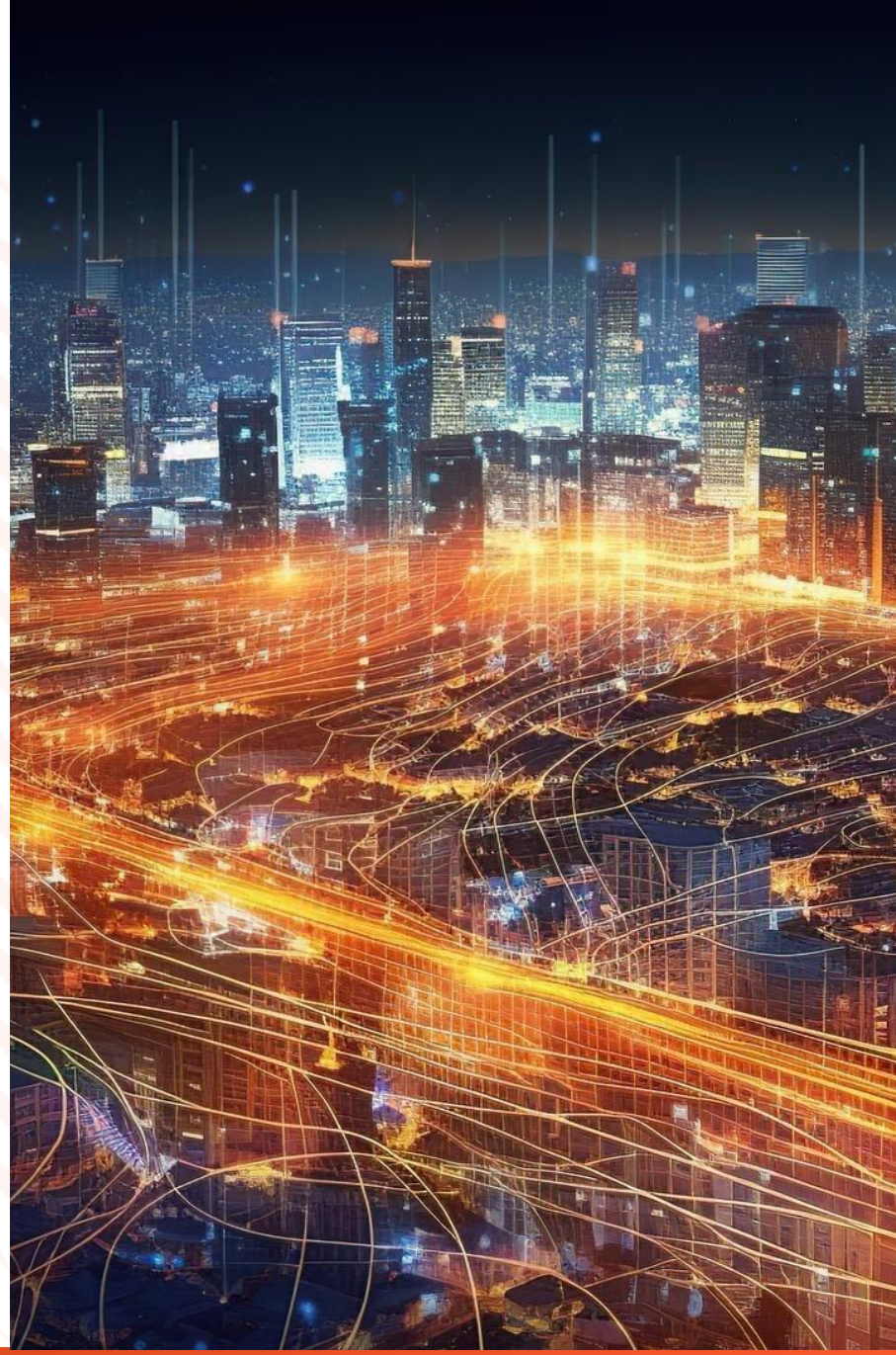
The Palo Alto Networks Cybersecurity Benchmark Study for Asia Pacific and Japan

Much of what is known about cybersecurity addresses large enterprises, and the insights typically originate from beyond the JAPAC region, or cover a handful of markets in JAPAC at best.

This is why Palo Alto Networks collaborated with Tech Research Asia (TRA) to find out how mid-market organizations in JAPAC are approaching cybersecurity. An additional goal was to enable peer benchmarking for JAPAC mid-market organizations.

The data referenced in this report was drawn from an online panel in November 2024. Respondents held senior IT or cybersecurity roles in 2,817 organizations with 200–700 employees. Insights were gathered across 12 JAPAC countries and territories, averaging 234 responses per country.

These findings form the foundation of the Palo Alto Networks Cybersecurity Benchmark, providing in-depth profiles across the region. Designed to drive improvement, the benchmark also examines how organizations lead, prioritize, and fund their cybersecurity strategies.

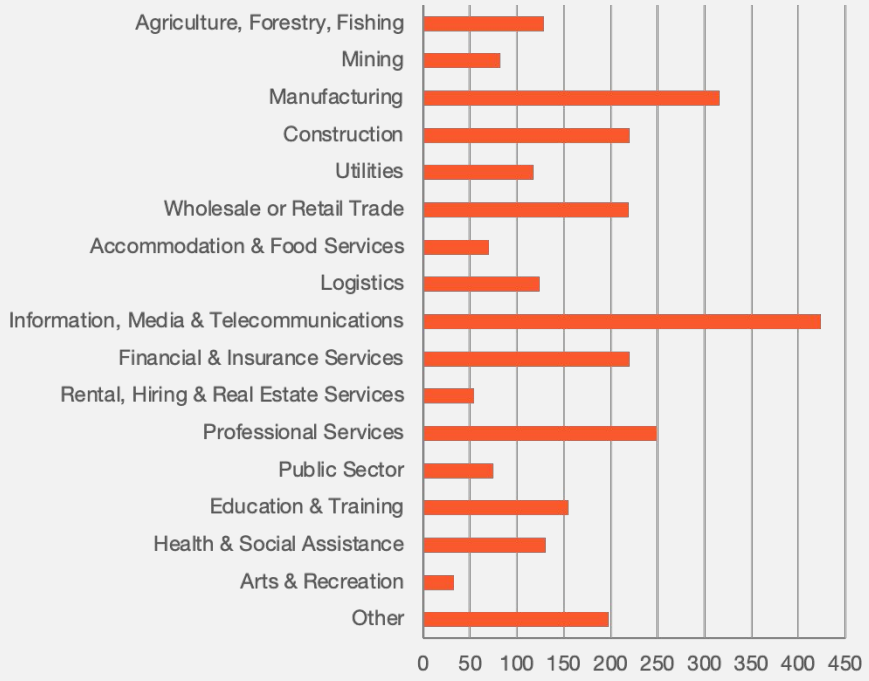


 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

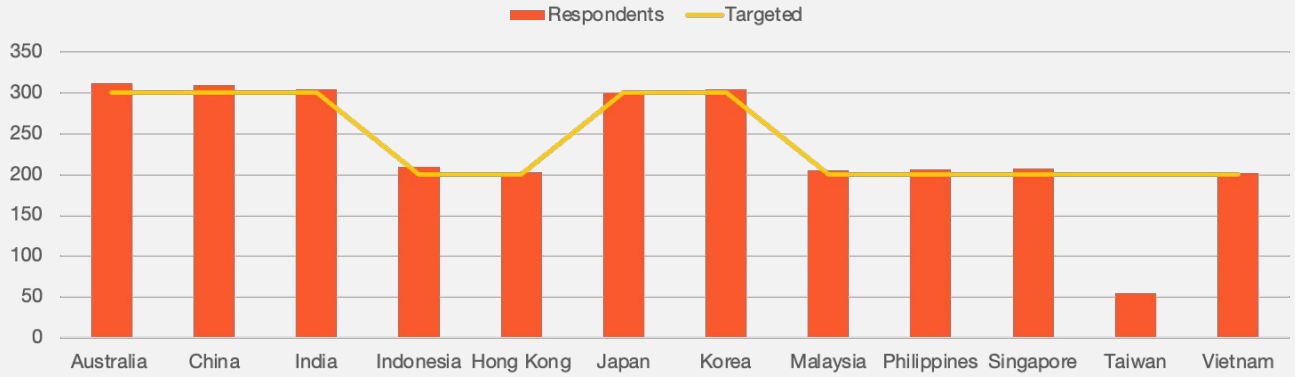
Total respondents:
2,817
(targeted 2,750)

Mid-market company:
200–700
employees

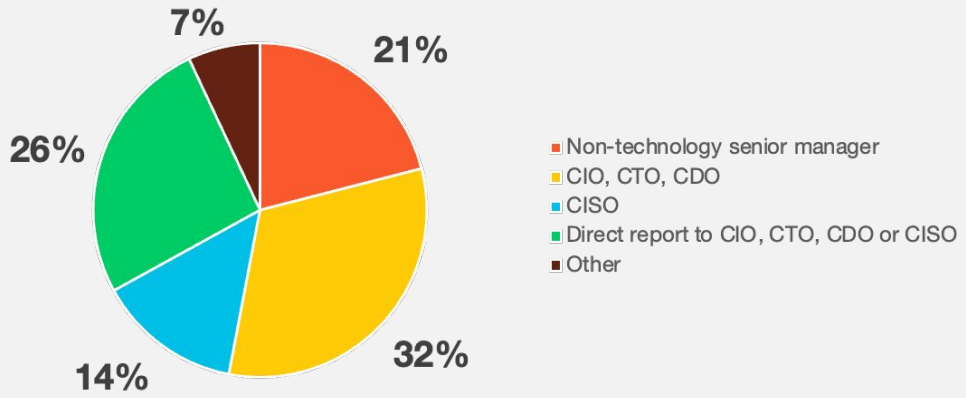
Industry Sector



Total Respondents



Respondent Role



 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Top Cybersecurity Priorities

Asia-Pacific mid-market organizations have ranked cybersecurity as a top-three business priority, focusing on **protecting customers** and **intellectual property** while supporting **digital transformation.**

Mid-market organizations plan to focus on specific technologies and services to improve their resilience in the next 12—24 months.

Top priorities businesses want cybersecurity to support

Protecting customers

Supporting digital transformation programs

Protecting intellectual property

Top 3 investment strategies over the next 12 months

Strengthening policies and governance, risk and compliance (GRC)

Optimizing internal cybersecurity ecosystems through improving education, automation and processes

Recruiting/upskilling their own cybersecurity professionals

Top 3 investment priorities to support the strategies, over the next 24 months

Cloud security posture management (CSPM)

Identity and access management (IAM)

Security information and event management (SIEM)

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

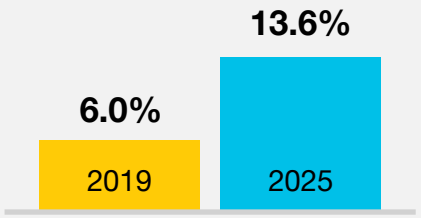
Top Cybersecurity Investment Strategies

Over the past five years, the proportion of IT budgets allocated to cybersecurity has more than doubled—**from 6% to 13.6% today**.

Approximately **91%** of mid-market organizations intend to either **maintain or increase their cybersecurity spending** within the next 12 months.

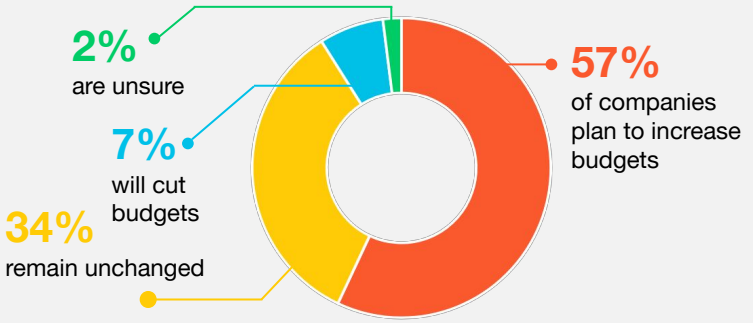
In terms of procurement preferences, **70%** of organizations now **favor flexible payment models** such as subscription-based, consumption-based, or outcome-based arrangements, rather than traditional upfront payments.

Percentage of IT budget dedicated to cybersecurity

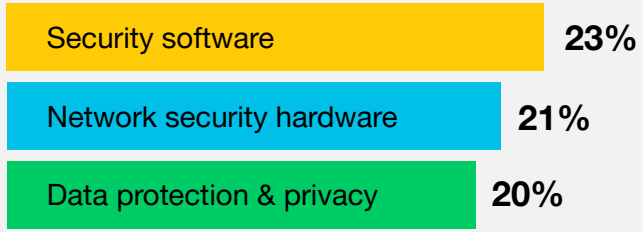


Mid-market organizations in Singapore, Malaysia, and Indonesia expect to invest even more in cybersecurity.

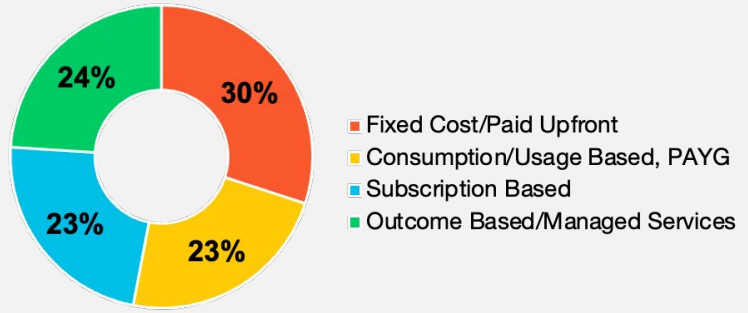
Cybersecurity budgets over the next 12 months



Top 3 areas where cybersecurity spend will increase more than 10%:



Current payment models for cybersecurity spend



 I © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

About the Cybersecurity Benchmark

The Cybersecurity Benchmark shows cybersecurity maturity and performance for mid-market organizations in JAPAC.

It provides a holistic overview of how organizations with 200 to 700 employees are performing with their cybersecurity operations. The benchmark is also designed to help organizations strengthen their cybersecurity and resiliency through peer benchmarking.

Overall, companies are relatively confident regarding their cybersecurity capabilities with a total score of 19.01 in JAPAC.

Benchmark score average **19.01** out of 25

Using a scale of 1 (lowest) to 5 (highest), organizations self-assessed their performance against **5 parameters**:

1. **Execution of Cybersecurity Strategy**
   Measures how well an organization is executing against its cybersecurity strategy and goals.
2. **Cybersecurity in the Business**
   Assesses if cybersecurity activities have been effectively incorporated into business operations.
3. **Performance of Operational Capabilities**
   Measures how specific cybersecurity approaches and activities have performed.
4. **Maturity of Cybersecurity Usage**
   Assesses the usage maturity levels of specific cybersecurity solutions.
5. **Alignment with the NIST 2.0 Framework**
   Measures the adoption level of an abridged NIST 2.0 framework *(Govern, Identify, Protect, Detect, Response & Recovery.)*

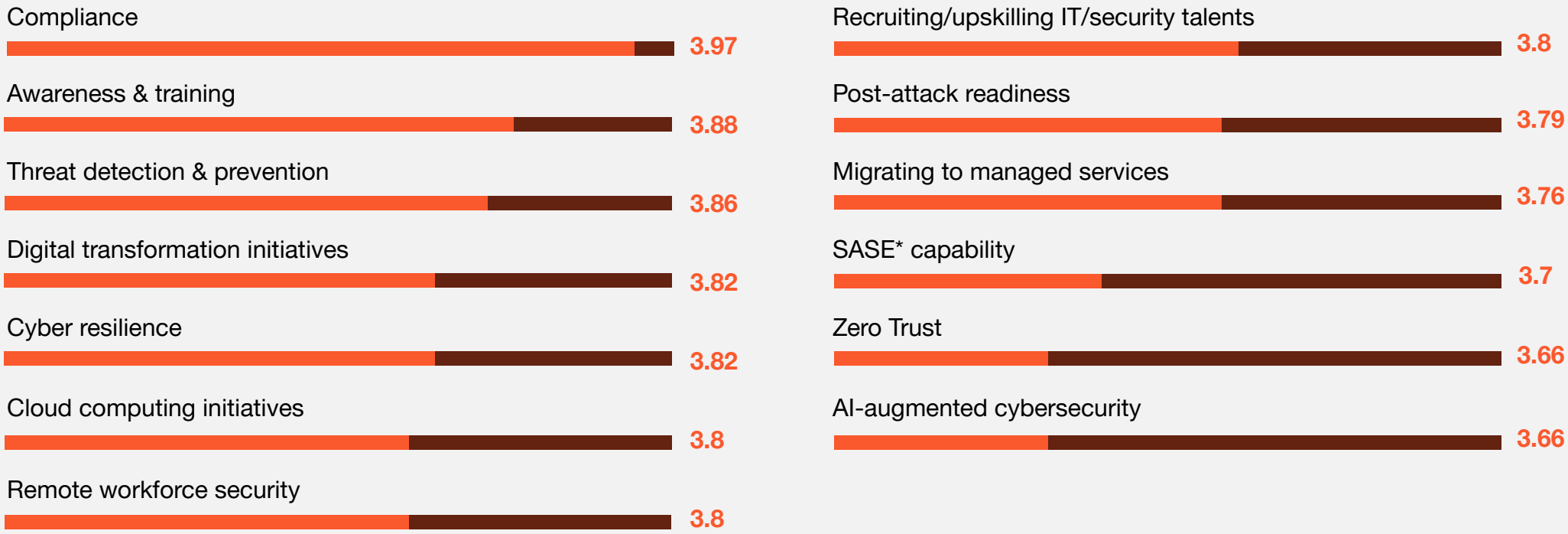
These scores were then aggregated to create an overall rating of maturity and performance. Ratings for each parameter were tallied to create a total score with a maximum of 25 points.

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Organizations are relatively bullish with their progress. Organizations are **dedicating most of their efforts to legal and regulatory compliance**, **education**, as well as threat detection and prevention, and have made the **least progress on adopting Zero Trust and AI cybersecurity** approaches.

AVERAGE SCORE
3.79 / 5.0

Execution of Cybersecurity Strategy: Category benchmark scores (Visual range shown below: 3.5 - 4.0)



*SASE stands for secure access service edge.

Issue assessed: "How would you rate your progress on executing against your company's cybersecurity goals?"

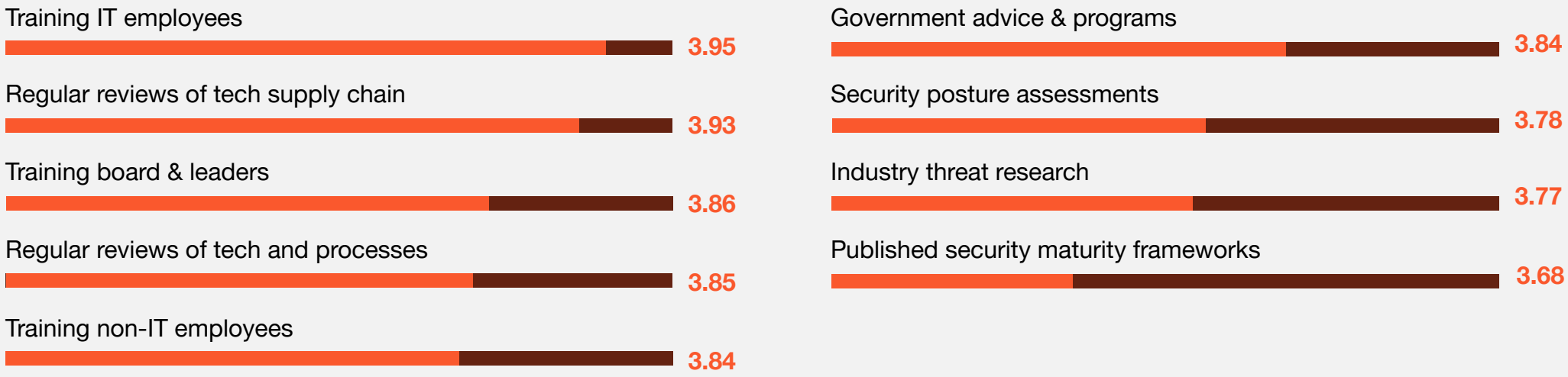
 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Organizations are **investing in educating and training IT employees** on cybersecurity and **reviews of the technology supply chain**, but need to take a more proactive approach towards **preventive measures such as security posture assessments, understanding industry threats, and security benchmarks.**

AVERAGE SCORE
3.83 / 5.0

Cybersecurity in the Business: Category benchmark scores

(Visual range shown below: 3.5 - 4.0)



Issue assessed: "How well does your company incorporate the following activities into its business and cybersecurity operations?"

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Organizations are making strides through **organization-wide training** and by **enhancing cybersecurity staffing and capabilities**. However, more investment is still needed in **AI-augmented cybersecurity** and in **building resilience against prolonged ransomware attacks**.

AVERAGE SCORE
3.89 / 5.0

Performance of Operational Capabilities: Category benchmark scores

(Visual range shown below: 3.5 - 4.0)

Issue assessed: "How would you score your company's operational performance in each of the following areas?"

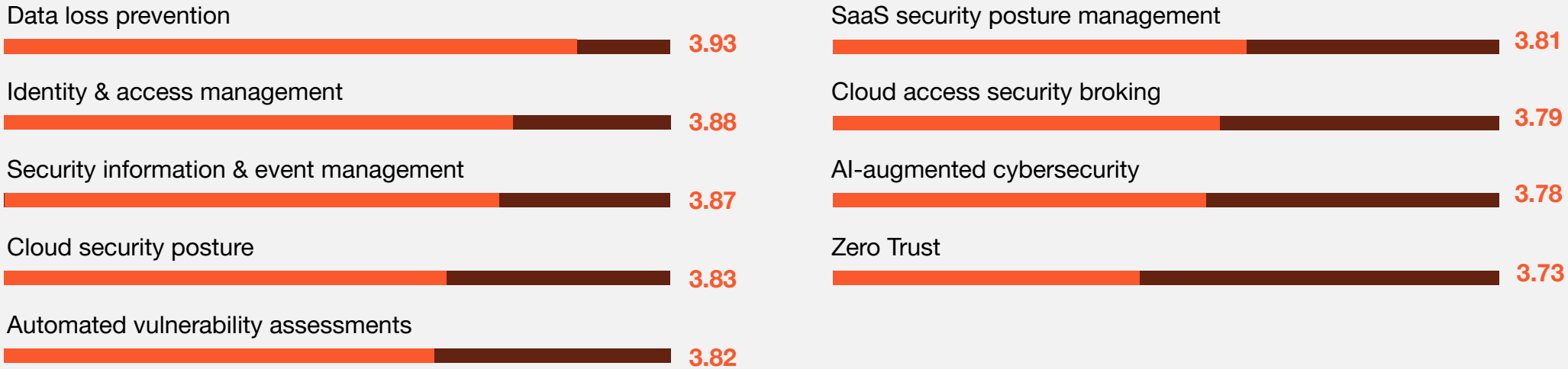
 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Data Loss Prevention **(DLP)**, Identity and Access Management **(IAM)**, and Security Information and Event Management **(SIEM) solutions are the most widely adopted**. Meanwhile, **adoption of Zero Trust frameworks, AI-driven cybersecurity, and Cloud Access Security Broker (CASB) solutions is still developing** as organizations continue to strengthen their security posture.

AVERAGE SCORE
3.83 / 5.0

Maturity of Cybersecurity Usage: Category benchmark scores

(Visual range shown below: 3.5 - 4.0)



Issue assessed: "What rating would you give to the maturity of use of the following solutions inside your company?"

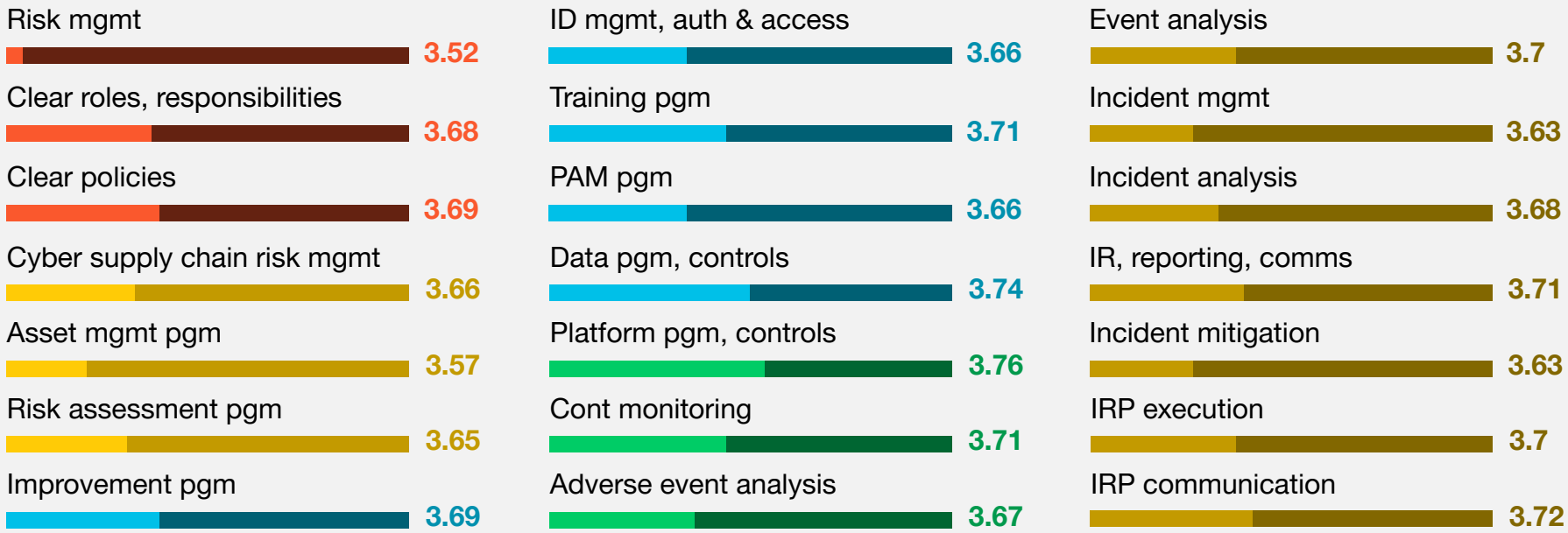
 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Governance and identity aspects of the framework – such as asset management, risk management and clarity of roles, responsibilities and policies – **lag behind** more widely prioritized areas in **threat protection, detection, response and recovery.**

AVERAGE SCORE
3.67 / 5.0

Alignment with the NIST 2.0 Framework: Category benchmark scores

(Visual range shown below: 3.5 - 4.0)



Overall assessment by organizations

- **Govern: 3.64**
- **Identify: 3.64**
- **Protect: 3.71**
- **Detect: 3.69**
- **Response & Recovery: 3.68**

IR stands for incident response | IRP stands for IR plan | PAM stands for privileged access management

Issue assessed: "How would you rate your company's adoption and implementation of the following cybersecurity framework categories?"

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Partners: The Route to Success

Today, 53% of mid-market organizations rely on partners to support their cybersecurity activities. Partnerships will only increase over time as more vendors, more regulations, and the rising complexity of developing robust cybersecurity organization-wide accelerate demand for partner services.

Cybersecurity roles and responsibilities

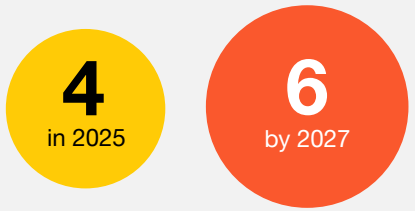
87% have a formally-appointed cybersecurity leader

- **24%** are IT managers reporting to the Chief Information Officer (CIO)
- **17%** are CIOs
- **14%** are IT managers reporting to the Chief Information Security Officer (CISO)

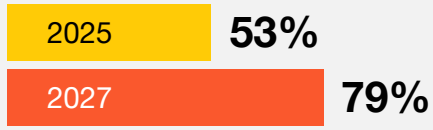
13% have no formally-appointed cybersecurity role

- **35%** share responsibility across IT teams
- **17%** on 'people doing the right thing'
- **13%** share responsibility across executive managers
- **10%** do not assign anyone cybersecurity responsibilities

Average number of core cybersecurity solution vendors



Percentage of mid-market organizations relying on partner support



Partner support insights

- Where demand for partners will be needed **most** in the next 2 years

Education and training

Identity access management

Application and data security

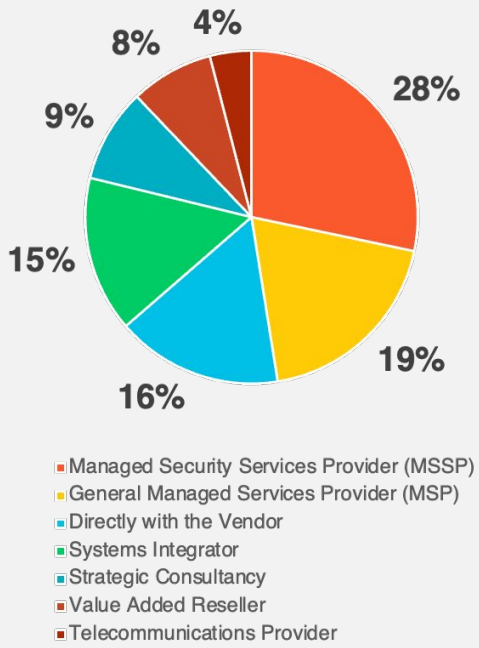
 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Partner Selection Criteria

Mid-market organizations have many considerations when it comes to assessing cybersecurity services partners, and typically prefer to work with managed security service partners (MSSPs). While pricing plays a significant role, the benefits that can influence decision makers positively include the ability to integrate new solutions with legacy infrastructure, as well as expertise in AI-augmented solutions.

On the other hand, partners who fail to live up to expectations are likely to find themselves on shaky ground. Organizations will even look for a new partner if their partner suffers a breach or outage, if there are supply chain issues, or if the solutions deployed work poorly.

What type of partner does your company prefer to work with for cybersecurity solutions and support?



Top attributes that influence partner selection

- Ability to integrate new solutions to existing technology
- Artificial intelligence (AI) supported products/solutions
- Technical expertise and certifications

**Excluding pricing*

Top partner mistakes to avoid

- Overpromising and under-delivering
- Not tailoring to what the customer needs
- Lack of business/sector understanding

Top reasons why organizations change partners

- A breach or major outage
- Supply chain issues
- Poor performance of deployed solution(s)

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

The Palo Alto Networks Perspective

While mid-market organizations are making progress, critical gaps in cyber resilience remain.

Enhancing governance, improving security posture, and building cyber talent are top priorities for this business segment.

To address these challenges, Palo Alto Networks offers comprehensive security platforms that enable organizations to achieve unified management, cost efficiencies, and stronger security outcomes.

Protecting customers

Proactive security in a growing threat landscape

Customer trust is fundamental to business success, yet the report reveals that threats continue to pose significant risks. Palo Alto Networks **Precision AI™**-driven platforms with **Unit 42 threat intelligence** deliver enterprise-grade **threat detection, automation, and Zero Trust security.**

Supporting digital transformation

Security as an enabler of innovation

Organizations rely on service partners and need agile systems to scale and innovate. Palo Alto Networks supports them with **unified security management** that simplifies operations, ensures compliance, and seamlessly **protects hybrid and multi-cloud environments.**

Safeguarding intellectual property

Strengthening cyber defenses for critical assets

Maintaining visibility and control over critical assets is a key challenge. Organizations need **real-time data loss prevention (DLP) and secure access solutions**. By adopting **Zero Trust principles**, businesses can protect proprietary data, reduce exposure, and maintain trust in an evolving threat landscape.

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Building a Secure Future for JAPAC

The need for a **proactive and unified security strategy** has never been greater. Palo Alto Networks supports the implementation of forward-thinking approaches with an **integrated security ecosystem**, through **Network Security, Cloud Security, and AI-Driven Security Operations**:

Comprehensive Network Security

Next-Generation Firewalls (NGFW), Software Firewalls (SWFW), and Cloud-Delivered Security Services (CDSS) provide real-time threat prevention, deep visibility, and AI-powered defense, with integrated Unit 42 threat intelligence and Precision AI™ to stop ransomware, data breaches, and unauthorized access.

Secure, Scalable Cloud Connectivity

Prisma Access enables consistent Zero Trust security policy enforcement across all types of application traffic (private, SaaS, internet), fully integrating Prisma Access Browser to enable a secure workspace for every user and device, irrespective of location.

AI-Driven Security Operations

Cortex XDR and the Cortex Cloud Platform leverage AI-powered threat detection, automated response, and security orchestration, enabling organizations to streamline security management, reduce complexity, and strengthen cyber resilience.

As more mid-market organizations shift towards subscription-based security for flexibility and cost efficiency, Palo Alto Networks is ready to help with provider and distributor partners to jointly deliver pay-as-you-go security, helping businesses scale protection, reduce overheads, and stay secure without infrastructure complexity.

Explore how we can help mid-market businesses build a more secure, resilient, and digitally-empowered future

EXPLORE HOW

Book an assessment of your security posture with us*

BOOK NOW

**For a full security check, choose the "Enterprise Cyber Security (concise)" assessment. It covers security Strategy and Capability Maturity across all areas of architecture in 60–90 minutes.*

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Australia

Benchmark score average

19.05

out of 25

Average number of core cybersecurity vendor solutions

TOP 3

Business Cyber Drivers

- Protecting customers
- Protecting intellectual property
- Improving GRC capabilities

Investment Priorities

- Strengthening security policies
- Educating employees
- Strengthening cyber resiliency

Deployed Cyber Solutions

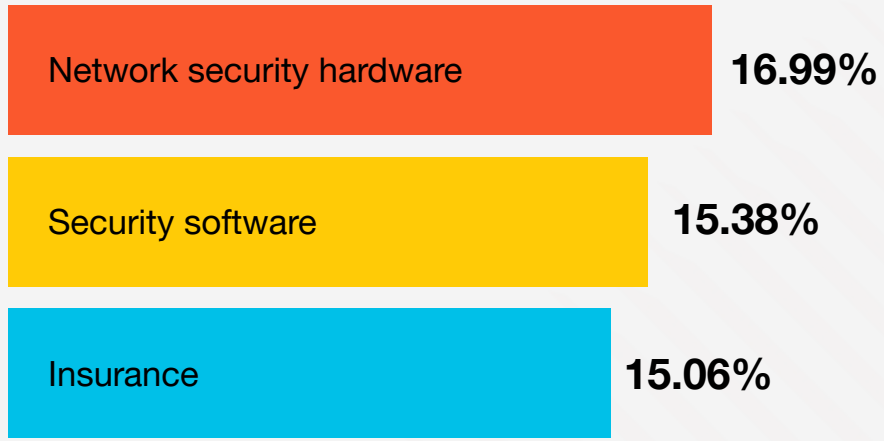
- Application and data security
- Cloud and emerging technology
- Operational and network security

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

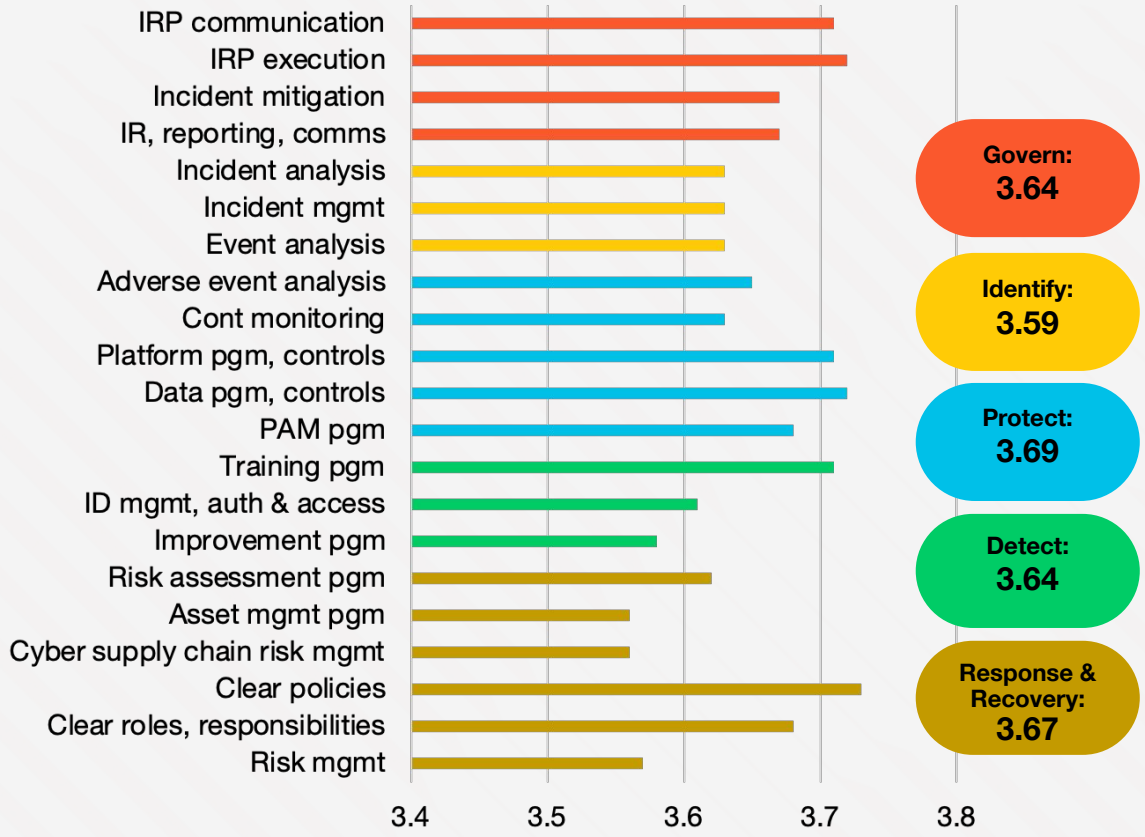
Australia

Cyber budget as % of revenue **13.6%**

Top 3 areas where cybersecurity spend will increase more than 10%



Country NIST framework

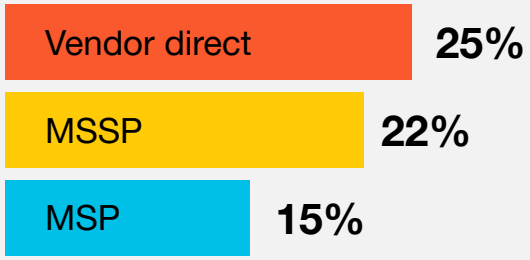


Visual range shown above: (3.4 - 3.8)

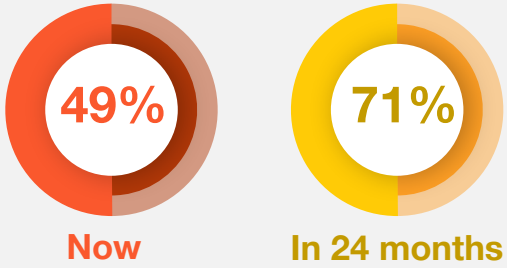
 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Australia

Top 3 preferred partner types for cybersecurity solutions and support



Percentage of organizations using partners



Partner support insights

Where demand for partners will be needed **most** in the next 2 years

- Cloud and emerging technology
- Security monitoring + operations (SOC)
- Application and data security

Top attributes that influence partner selection

- Cyber resiliency capabilities (31.4%)
- Proven track record and industry experience (29.5%)
- Ability to integrate new solutions to existing technology (28.2%)

**Excluding pricing*

Top reasons why organizations change partners

- Poor solution performance (40%)
- Budget change (39%)
- Breach or major outage (35%)

**Excluding pricing*

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

China

Benchmark score average

19.62

out of 25

Average number of core cybersecurity vendor solutions

TOP 3

Business Cyber Drivers

- Supporting digital transformation activities
- Governance, risk and compliance activities
- Ensuring supply chain performance and delivery

Investment Priorities

- Optimizing the security ecosystem
- Supporting visibility across cybersecurity assets
- Recruiting/ upskilling IT and cybersecurity professionals

Deployed Cyber Solutions

- Security monitoring + operations (SOC)
- Application and data security
- Operational and network security

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

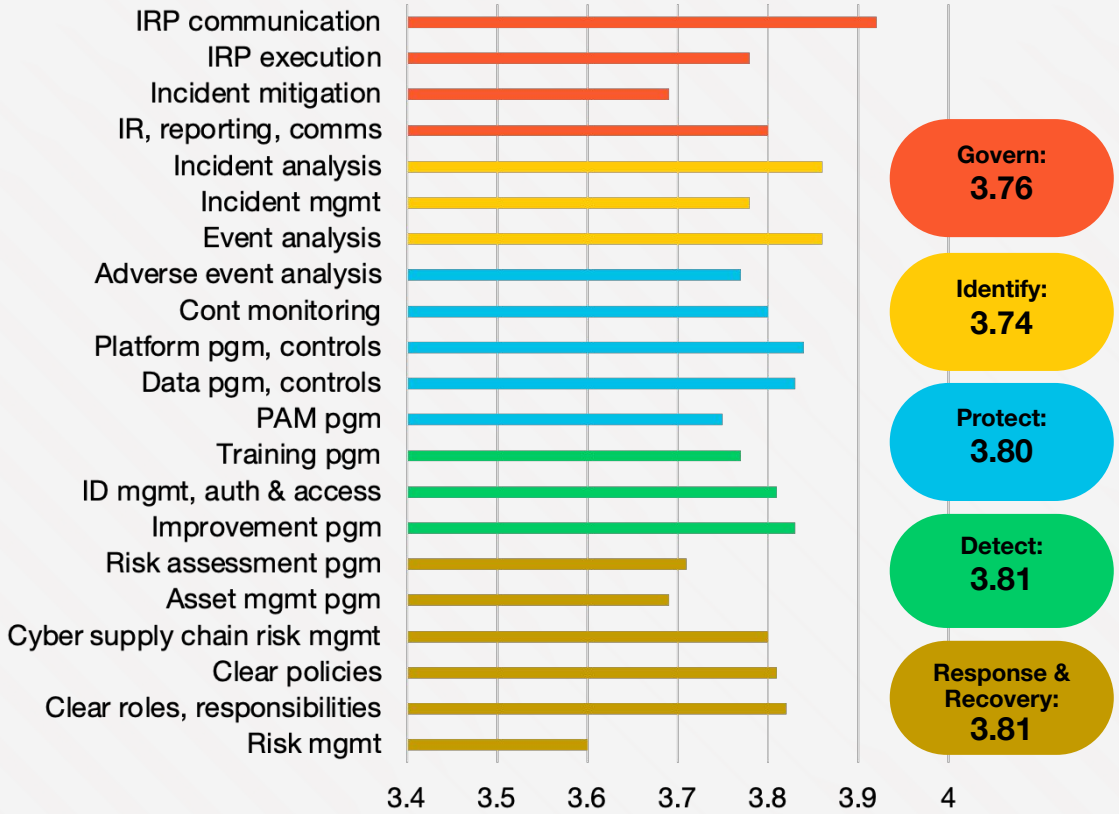
China

Cyber budget as % of revenue **14.6%**

Top 3 areas where cybersecurity spend will increase more than 10%

Network security hardware	14.52%
Data protection & privacy	13.55%
Strategy, talent & governance, risk & compliance	13.55%

Country NIST framework

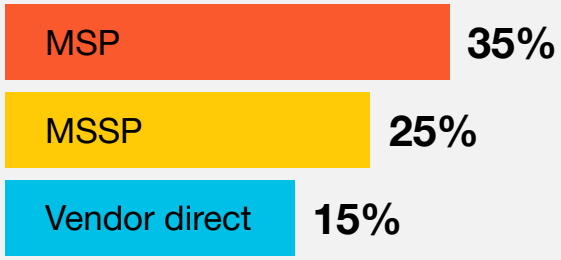


Visual range shown above: (3.4 - 4)

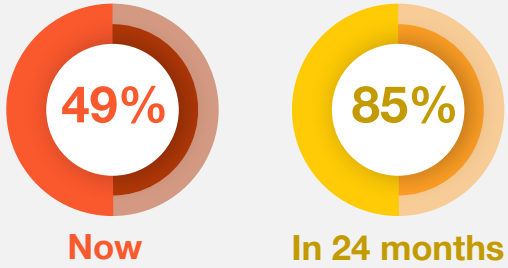
 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

China

Top 3 preferred partner types for cybersecurity solutions and support



Percentage of organizations using partners



Partner support insights

Where demand for partners will be needed **most** in the next 2 years

- Cloud and emerging technology
- Education and training
- Threat and vulnerability management

Top attributes that influence partner selection

- Ability to integrate new solutions to existing technology (33.5%)
- Tailored solutions (33.2%)
- AI supported products/solutions (30.3%)

*Excluding pricing

Top reasons why organizations change partners

- Breach or major outage (48%)
- Poor solution performance (41%)
- Supply chain issues (40%)

*Excluding pricing

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

India

Benchmark score average

20.30

out of 25

Average number of core cybersecurity vendor solutions

TOP 3

Business Cyber Drivers

- Protecting customers
- Supporting digital transformation activities
- Financial operations

Investment Priorities

- Defending against AI threats
- Recruiting/upskilling own IT and security professionals
- Providing employees with security awareness and training

Deployed Cyber Solutions

- Application and data security
- Security monitoring + operations (SOC)
- Cloud and emerging technology

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

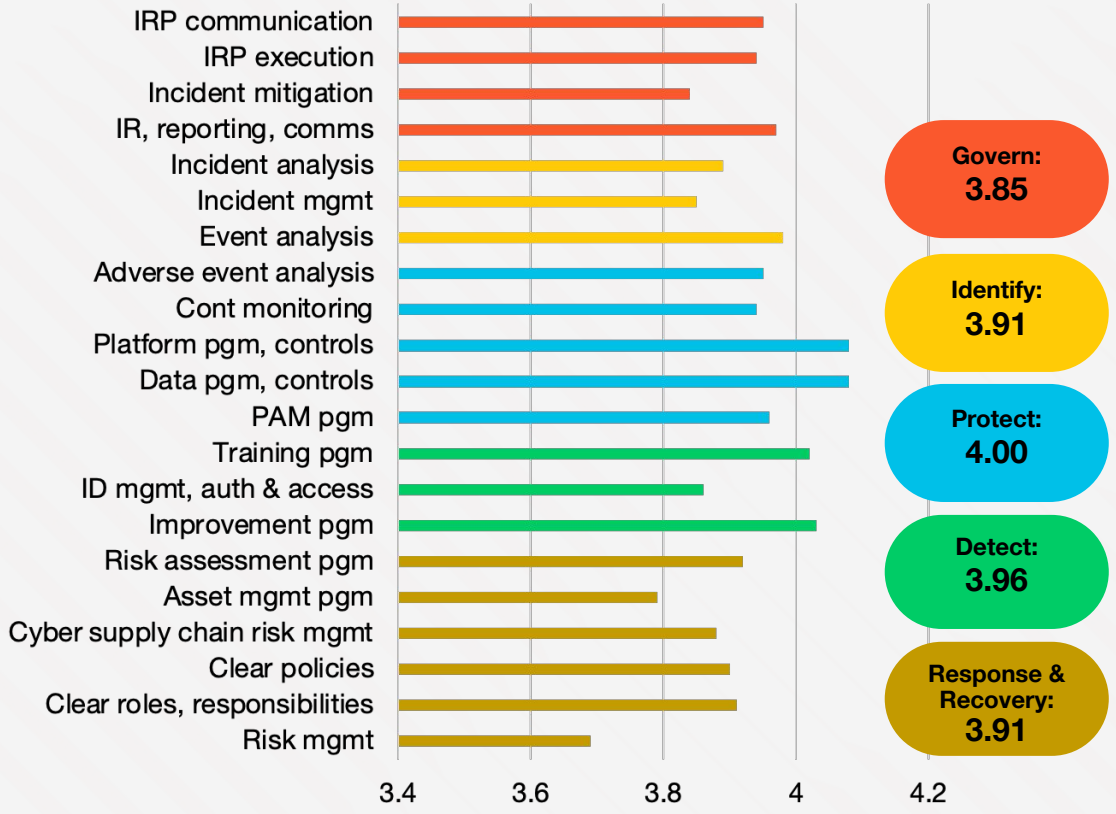
India

Cyber budget as % of revenue **13.0%**

Top 3 areas where cybersecurity spend will increase more than 10%

Specific AI capabilities	41.45%
Security software	41.45%
Insurance	39.14%

Country NIST framework

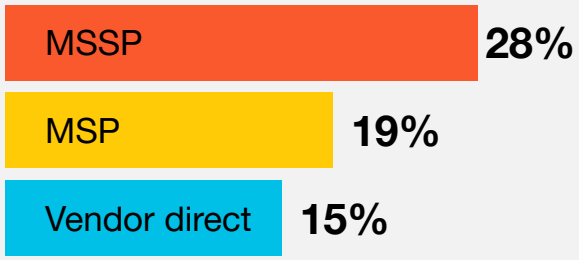


Visual range shown above: (3.4 - 4.2)

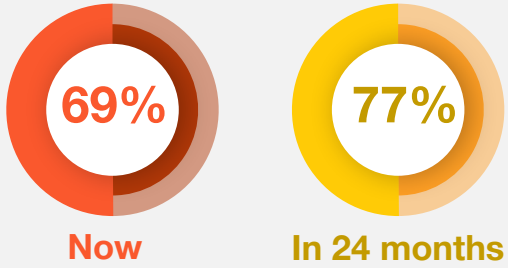
 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

India

Top 3 preferred partner types for cybersecurity solutions and support



Percentage of organizations using partners



Partner support insights

Where demand for partners will be needed **most** in the next 2 years

- Identity and access management (IAM)
- Security monitoring + operations (SOC)
- Operational and network security

Top attributes that influence partner selection

- AI-supported products/solutions (44.4%)
- Technical expertise and certifications (29.3%)
- Cyber resiliency capabilities (29.3%)

**Excluding pricing*

Top reasons why organizations change partners

- Supply chain issues (49%)
- Penetration testing results (38%)
- Poor solution performance (38%)

**Excluding pricing*

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Indonesia

Benchmark score average

20.65

out of 25

Average number of core cybersecurity vendor solutions

TOP 3

Business Cyber Drivers

- Supporting digital transformation activities
- Protecting customers
- Governance, risk and compliance activities

Investment Priorities

- Strengthening cyber resiliency
- Recruiting/ upskilling own IT and security professionals
- Optimizing the security ecosystem

Deployed Cyber Solutions

- Application and data security
- Security monitoring + operations (SOC)
- Cloud and emerging technology

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

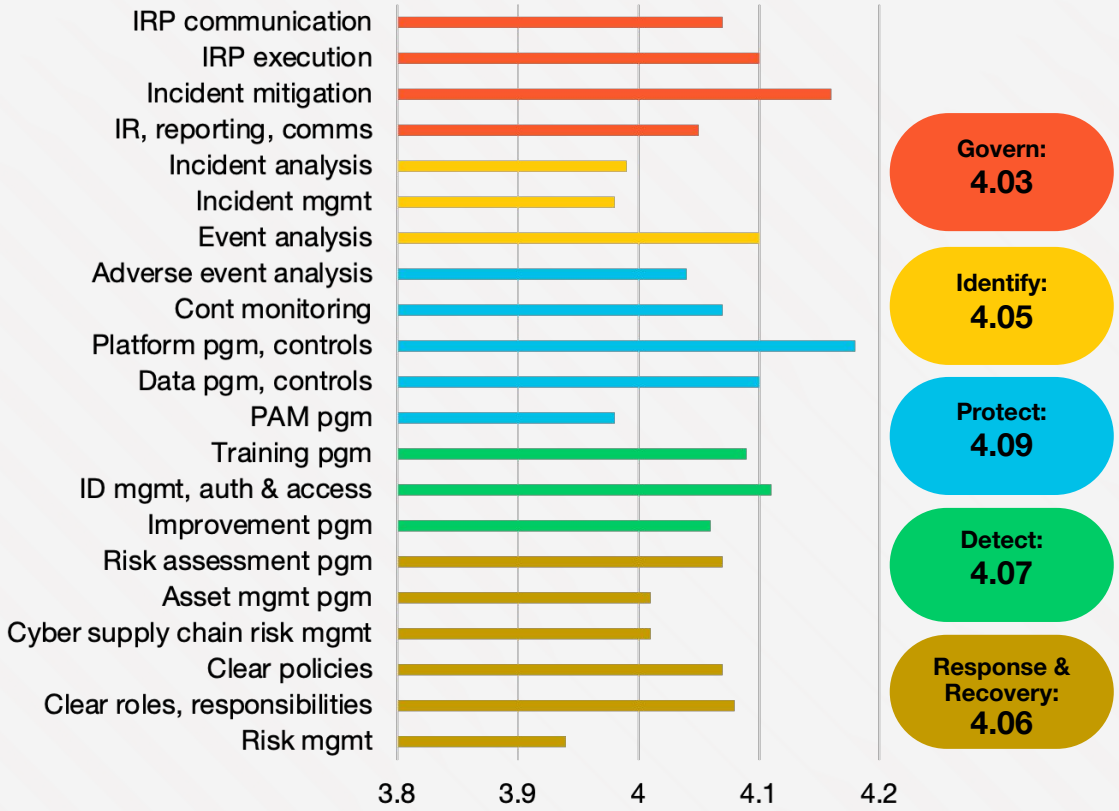
Indonesia

Cyber budget as % of revenue **14.4%**

Top 3 areas where cybersecurity spend will increase more than 10%

Data protection & privacy	29.67%
Security software	29.67%
Network security hardware	29.67%

Country NIST framework

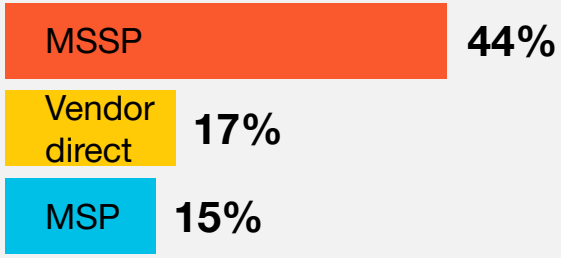


Visual range shown above: (3.8 - 4.2)

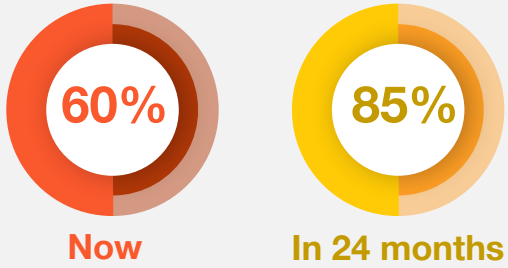
 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Indonesia

Top 3 preferred partner types for cybersecurity solutions and support



Percentage of organizations using partners



Partner support insights

Where demand for partners will be needed **most** in the next 2 years

- Threat and vulnerability management
- Education and training
- Cloud and emerging technology

Top attributes that influence partner selection

- Cyber resiliency capabilities (34.9%)
- AI-supported products/solutions (34.0%)
- Technical expertise and certifications (31.1%)

*Excluding pricing

Top reasons why organizations change partners

- Penetration testing results (36%)
- Supply chain issues (35%)
- Poor solution performance (33%)

*Excluding pricing

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Hong Kong

Benchmark score average

19.04

out of 25

Average number of core cybersecurity vendor solutions

TOP 3

Business Cyber Drivers

- Supporting digital transformation activities
- Protecting customers
- Governance, risk and compliance activities

Investment Priorities

- Optimizing the security ecosystem
- Supporting visibility across cybersecurity assets
- Providing employees with security awareness and training

Deployed Cyber Solutions

- Security monitoring + operations (SOC)
- Application and data security
- Identity and access management (IAM)

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

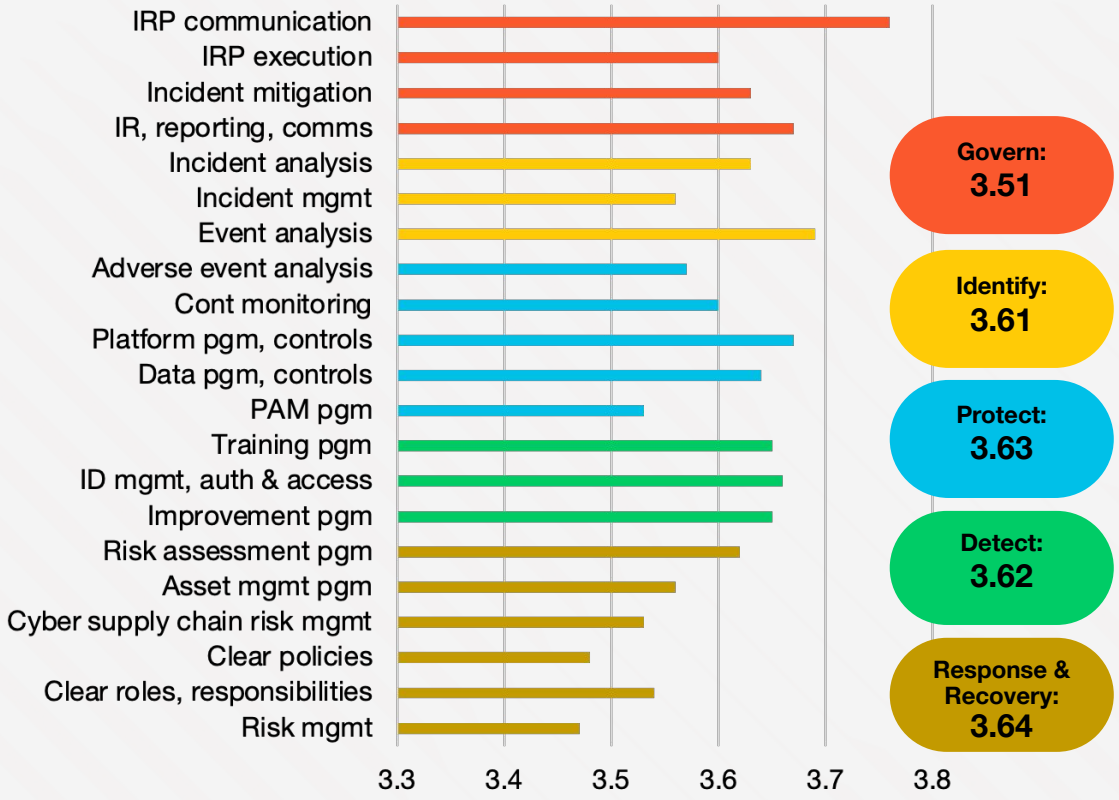
Hong Kong

Cyber budget as % of revenue **13.5%**

Top 3 areas where cybersecurity spend will increase more than 10%

Application security	19.2%
Specific AI capabilities	18.72%
3rd party security professional services	18.72%

Country NIST framework

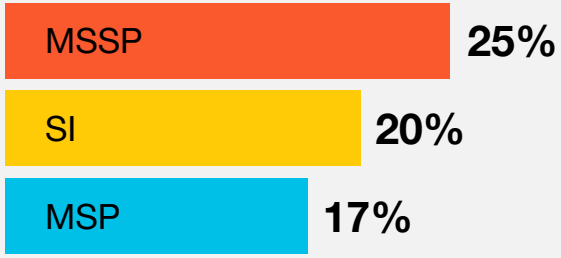


Visual range shown above: (3.3 - 3.8)

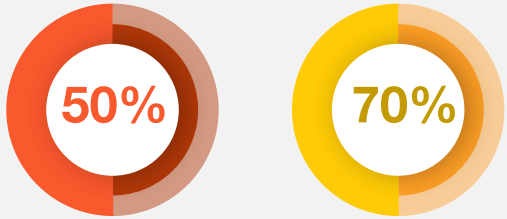
 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Hong Kong

Top 3 preferred partner types for cybersecurity solutions and support



Percentage of organizations using partners



Partner support insights

Where demand for partners will be needed **most** in the next 2 years

- Application and data security
- Cloud and emerging technology
- Operational and Network Security

Top attributes that influence partner selection

- Comprehensive service offering (29.6%)
- Technical expertise and certifications (28.6%)
- Tailored solutions (28.1%)

**Excluding pricing*

Top reasons why organizations change partners

- Budget change (38%)
- Breach or major outage (37%)
- Supply chain issues (35%)

**Excluding pricing*

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Japan

Benchmark score average

16.67

out of 25

Average number of core cybersecurity vendor solutions

TOP 3

Business Cyber Drivers

- Protecting customers
- Protecting intellectual property
- Governance, risk and compliance activities

Investment Priorities

- Supporting visibility across cybersecurity assets
- Strengthening security policies
- Legal and regulatory compliance

Deployed Cyber Solutions

- Application and data security
- Threat and vulnerability management
- Operational and network security

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

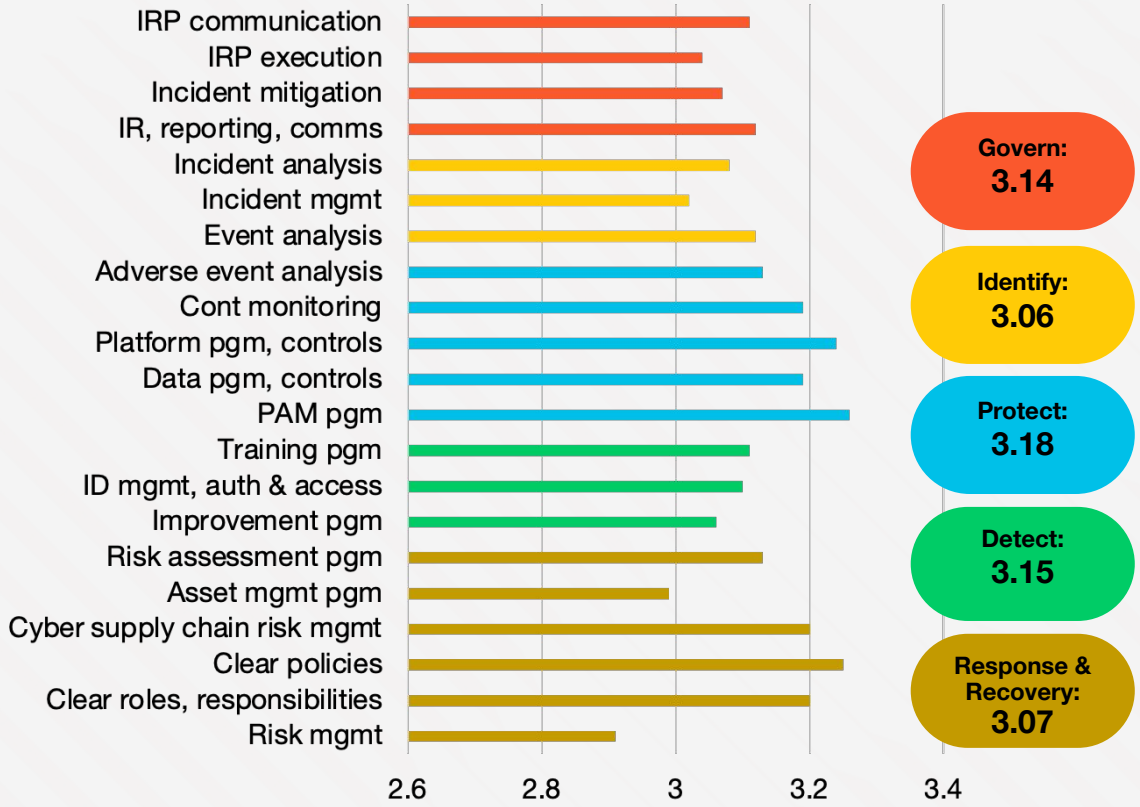
Japan

Cyber budget as % of revenue **12.4%**

Top 3 areas where cybersecurity spend will increase more than 10%

Training/education	11.3%
Network security hardware	10%
Specific AI capabilities	9.6%

Country NIST framework

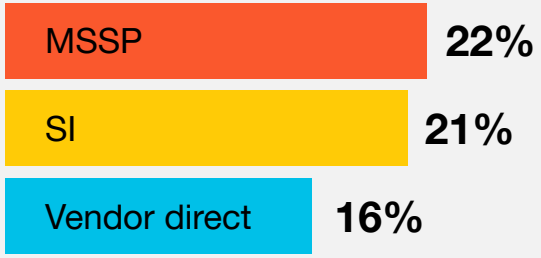


Visual range shown above: (2.6 - 3.4)

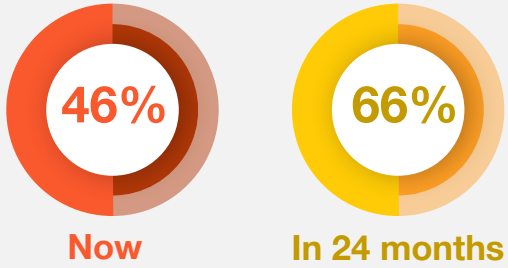
 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Japan

Top 3 preferred partner types for cybersecurity solutions and support



Percentage of organizations using partners



Partner support insights

Where demand for partners will be needed **most** in the next 2 years

- Cloud and emerging technology
- Threat and vulnerability management
- Endpoint and mobile security

Top attributes that influence partner selection

- Proven track record and industry experience (34.3%)
- Technical expertise and certifications (30.7%)
- Alignment with compliance and regulatory requirements (28.3%)

**Excluding pricing*

Top reasons why organizations change partners

- Breach or major outage (41%)
- Supply chain issues (33%)
- Budget change (33%)

**Excluding pricing*

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Korea

Benchmark score average

18.46

out of 25

Average number of core cybersecurity vendor solutions

TOP 3

Business Cyber Drivers

- Protecting intellectual property
- Protecting customers
- Supporting digital transformation activities

Investment Priorities

- Strengthening security policies
- Defending against AI threats
- Recruiting/ upskilling own IT and security professionals

Deployed Cyber Solutions

- Security monitoring + operations (SOC)
- Application and data security
- Operational and network security

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

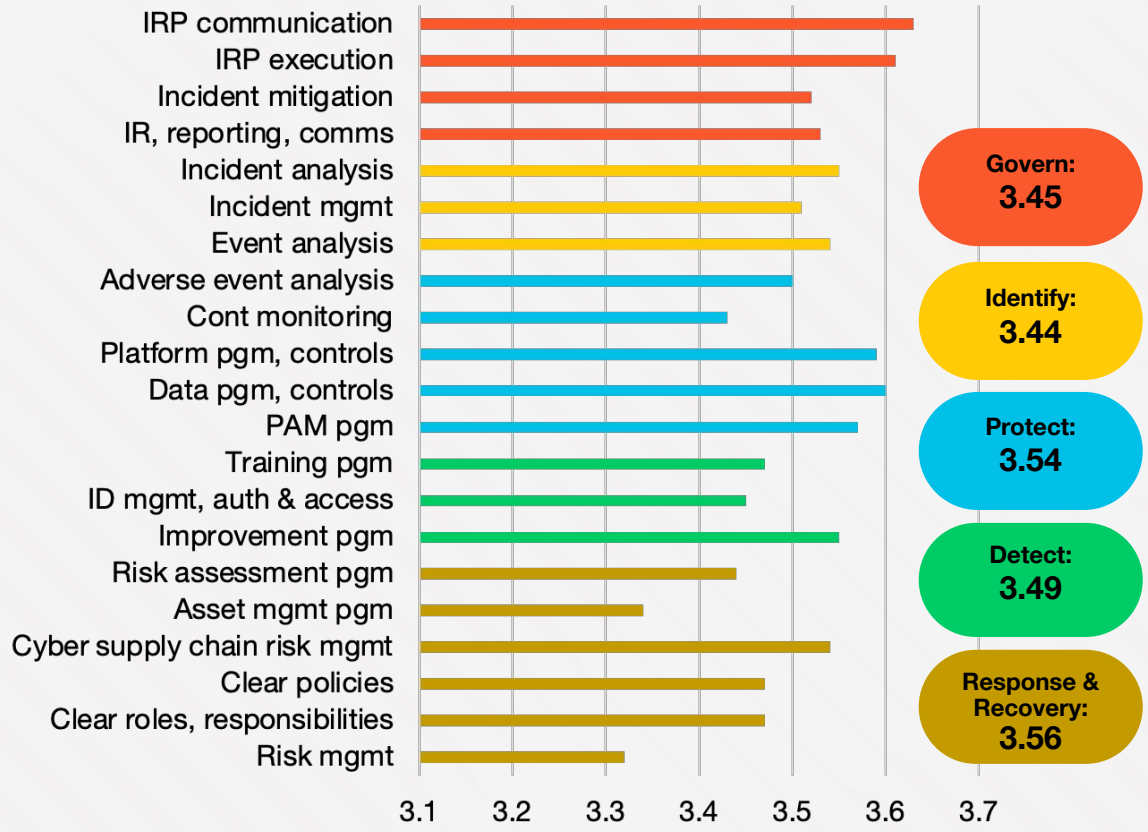
Korea

Cyber budget as % of revenue **13.2%**

Top 3 areas where cybersecurity spend will increase more than 10%

Security software	17.11%
Application security	16.12%
Incident response & recovery	15.79%

Country NIST framework

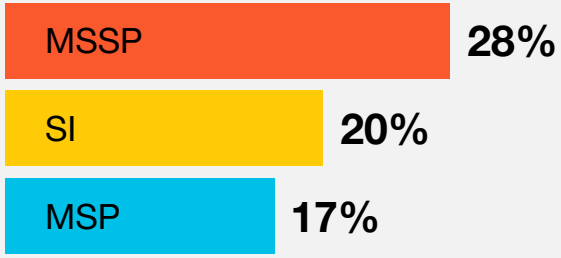


Visual range shown above: (3.1 - 3.7)

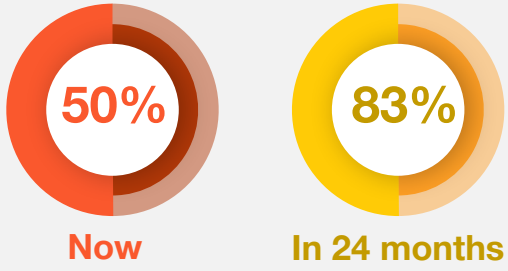
 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Korea

Top 3 preferred partner types for cybersecurity solutions and support



Percentage of organizations using partners



Partner support insights

Where demand for partners will be needed **most** in the next 2 years

- Cloud and emerging technology
- Operational and network security
- Threat and vulnerability management

Top attributes that influence partner selection

- Tailored solutions (29.9%)
- Proven track record and industry experience (28.3%)
- Ability to integrate new solutions to existing technology (28.0%)

**Excluding pricing*

Top reasons why organizations change partners

- Breach or major outage (39%)
- Poor solution performance (35%)
- Supply chain issues (34%)

**Excluding pricing*

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Malaysia

Benchmark score average

19.54

out of 25

Average number of core cybersecurity vendor solutions

TOP 3

Business Cyber Drivers

- Supporting digital transformation activities
- Protecting intellectual property
- Financial operations

Investment Priorities

- Providing employees with security awareness and training
- Recruiting/ upskilling own IT and security professionals
- Optimizing the security ecosystem

Deployed Cyber Solutions

- Application and data security
- Cloud and emerging technology
- Operational and network security

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

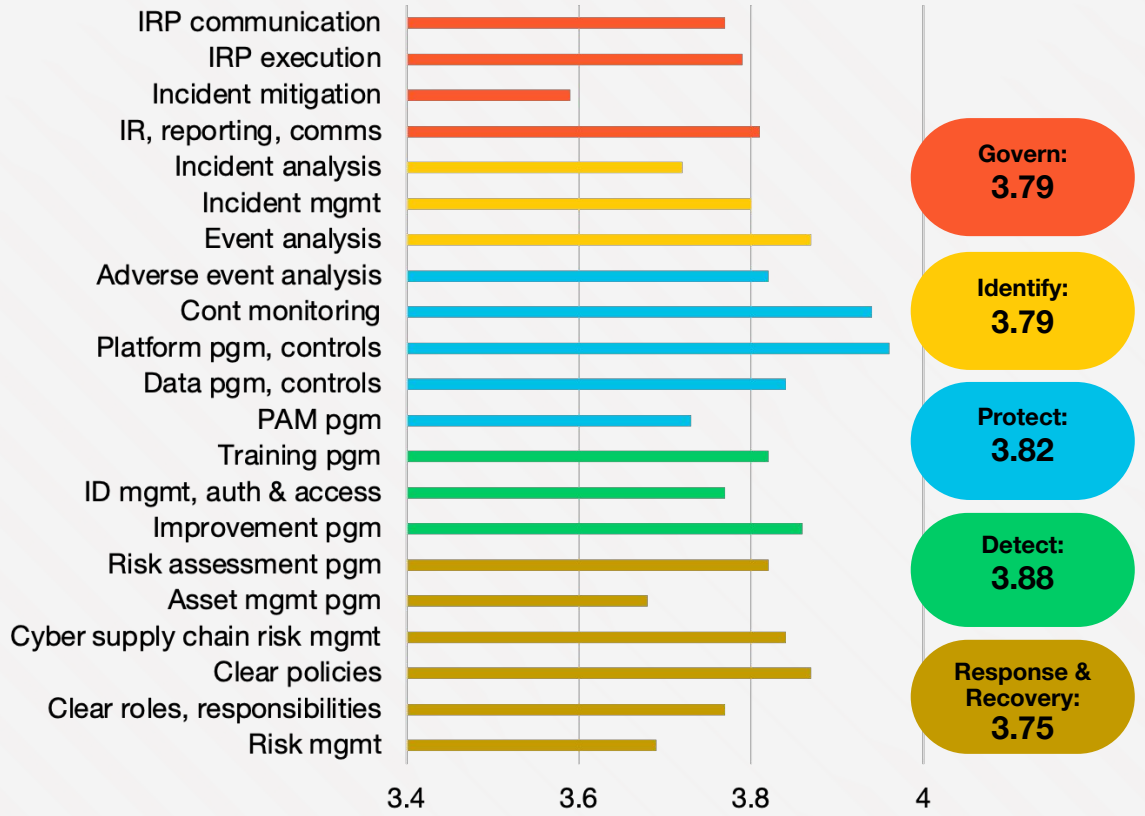
Malaysia

Cyber budget as % of revenue **14.5%**

Top 3 areas where cybersecurity spend will increase more than 10%

Data protection & privacy	32%
Security software	24.88%
Training/education	24.88%

Country NIST framework

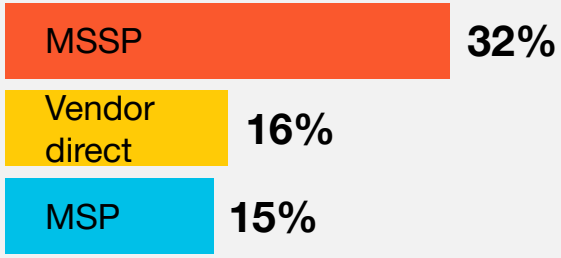


Visual range shown above: (3.4 - 4.0)

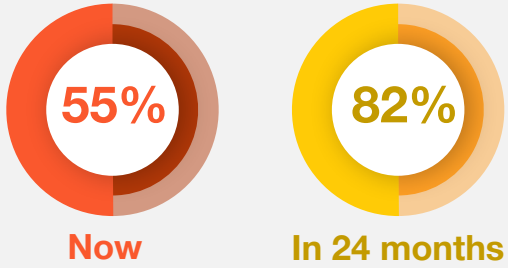
 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Malaysia

Top 3 preferred partner types for cybersecurity solutions and support



Percentage of organizations using partners



Partner support insights

Where demand for partners will be needed **most** in the next 2 years

- Cloud and emerging technology
- Education and training
- Operational and network security

Top attributes that influence partner selection

- Cyber resiliency capabilities (32.2%)
- Technical expertise and certifications (31.7%)
- Ability to integrate new solutions to existing technology (30.2%)

**Excluding pricing*

Top reasons why organizations change partners

- Poor solution performance (41%)
- Budget change (35%)
- Poor technical support (31%)

**Excluding pricing*

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Philippines

Benchmark score average

20.21

out of 25

Average number of core cybersecurity vendor solutions

TOP 3

Business Cyber Drivers

- Protecting customers
- Protecting intellectual property
- Supporting digital transformation activities

Investment Priorities

- Providing employees with security awareness and training
- Strengthening cyber resiliency
- Recruiting/ upskilling own IT and security professionals

Deployed Cyber Solutions

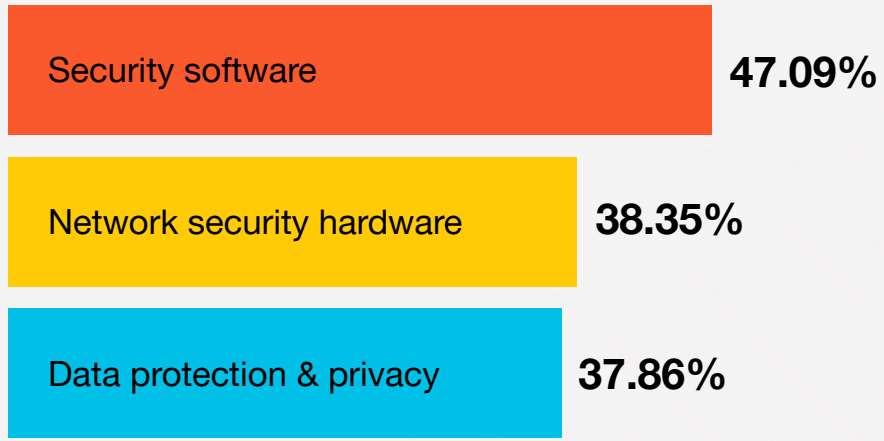
- Application and data security
- Security monitoring + operations (SOC)
- Operational and network security

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

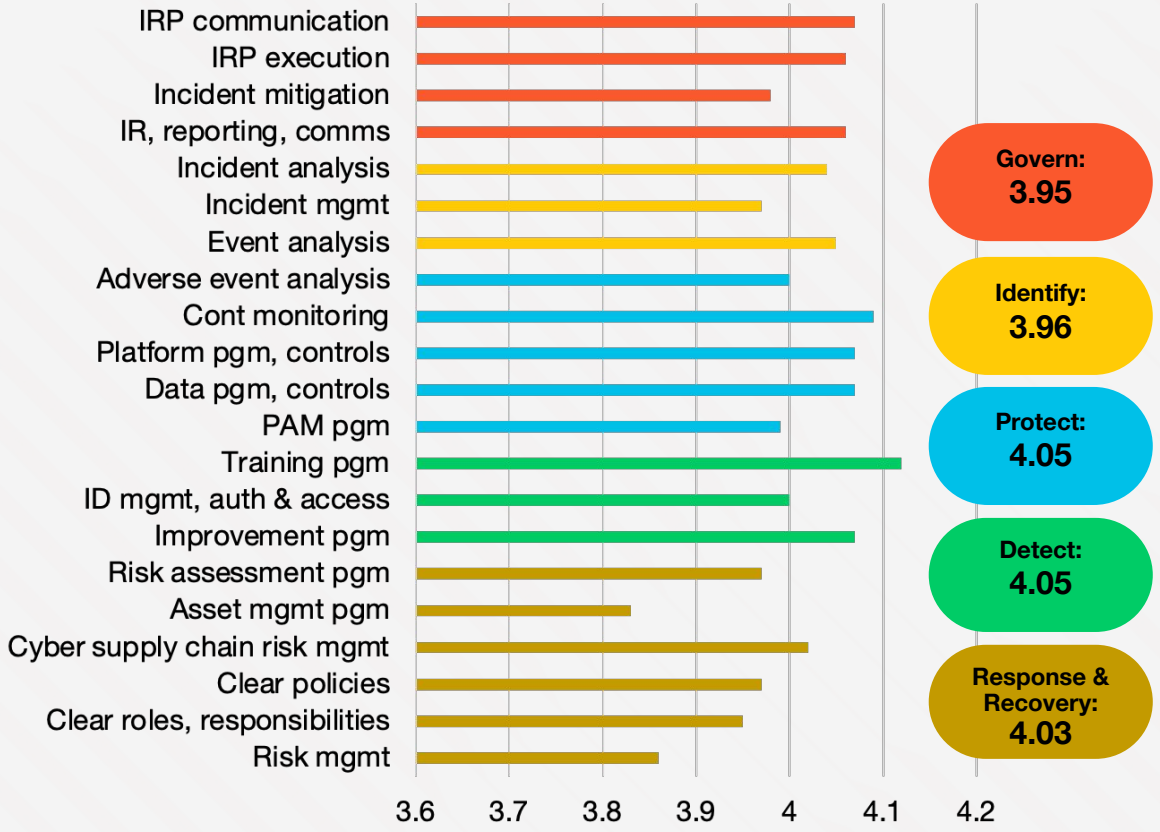
Philippines

Cyber budget as % of revenue **13.3%**

Top 3 areas where cybersecurity spend will increase more than 10%



Country NIST framework

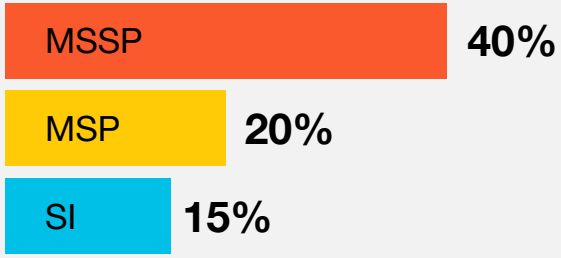


Visual range shown above: (3.6 - 4.2)

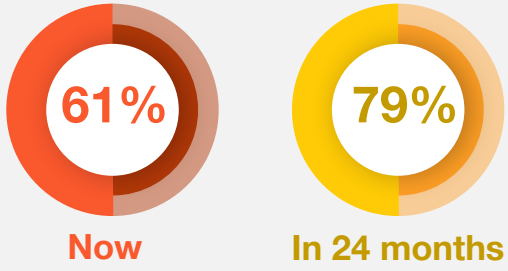
 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Philippines

Top 3 preferred partner types for cybersecurity solutions and support



Percentage of organizations using partners



Partner support insights

Where demand for partners will be needed **most** in the next 2 years

- Cloud and emerging technology
- Education and training
- Security monitoring + operations (SOC)

Top attributes that influence partner selection

- Technical expertise and certifications (35.9%)
- Cyber resiliency capabilities (29.1%)
- Knowledge transfer and training (27.2%)

**Excluding pricing*

Top reasons why organizations change partners

- Poor solution performance (43%)
- Breach or major outage (40%)
- Supply chain issues (39%)

**Excluding pricing*

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Singapore

Benchmark score average

19.28

out of 25

Average number of core cybersecurity vendor solutions

TOP 3

Business Cyber Drivers

- Governance, risk and compliance activities
- Business resiliency and related capabilities
- Supporting digital transformation activities

Investment Priorities

- Strengthening security policies
- Recruiting/ upskilling own IT and security professionals
- Strengthening cyber resiliency

Deployed Cyber Solutions

- Application and data security
- Identity and access management (IAM)
- Cloud and emerging technology

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

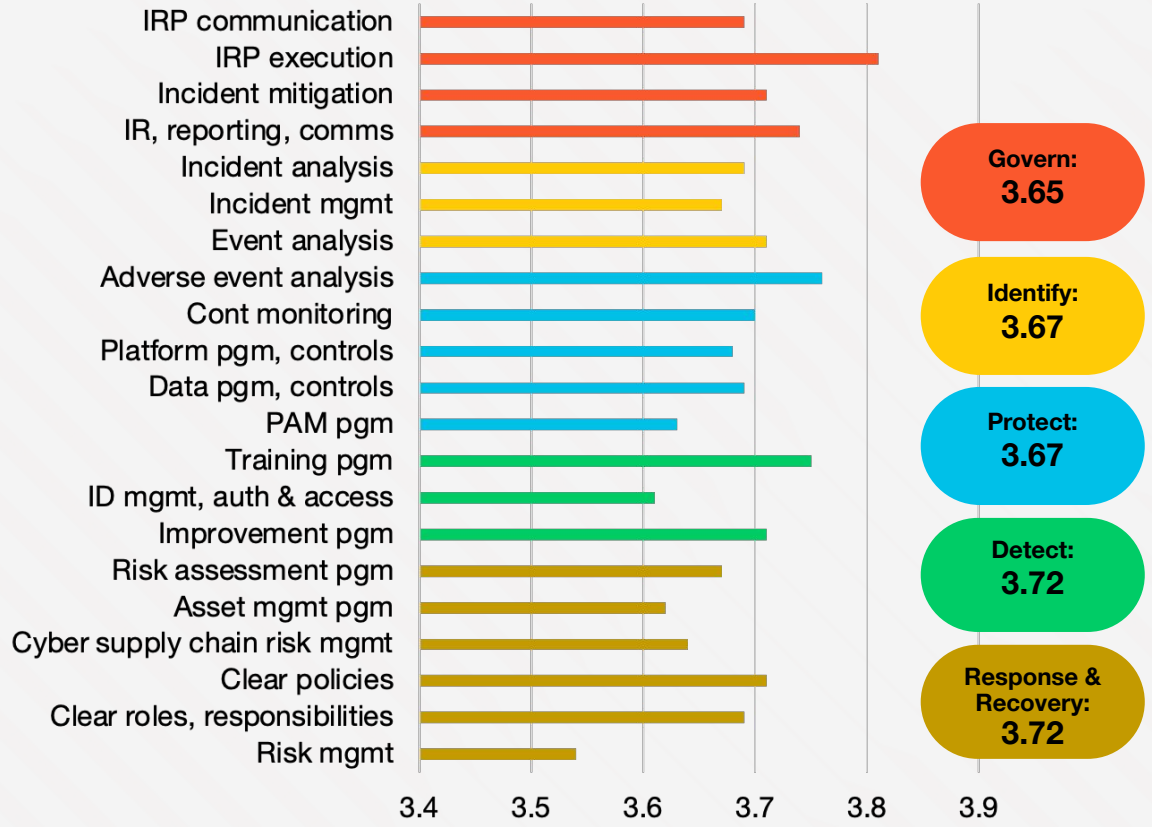
Singapore

Cyber budget as % of revenue **15.2%**

Top 4 areas where cybersecurity spend will increase more than 10%

Data protection & privacy	20.29%
Security software	18.36%
Application security and Identity & access management	15.94%

Country NIST framework



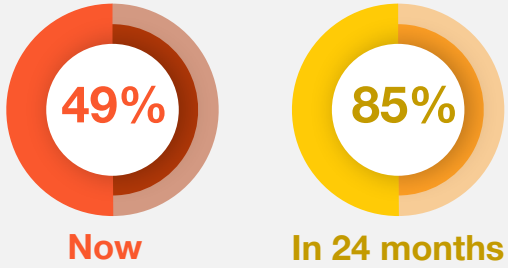
Visual range shown above: (3.4 - 3.9)

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Singapore

Top 3 preferred partner types for cybersecurity solutions and support

Percentage of organizations using partners



Partner support insights

Where demand for partners will be needed **most** in the next 2 years

- Threat and vulnerability management
- Cloud and emerging technology
- Education and training

Top attributes that influence partner selection

- Proven track record and industry experience (27.5%)
- Flexible pricing/utility based pricing (27.1%)
- Technical expertise and certifications (26.6%)

**Excluding pricing*

Top reasons why organizations change partners

- Regulatory/legislative changes (36%)
- Budget change (36%)
- Penetration testing results (35%)

**Excluding pricing*

 I © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Taiwan

Benchmark score average

19.44

out of 25

Average number of core cybersecurity vendor solutions

TOP 3

Business Cyber Drivers

- Protecting intellectual property
- Governance, risk and compliance activities
- Protecting customers

Investment Priorities

- Optimizing the security ecosystem
- Providing employees with security awareness and training
- Defending against AI threats

Deployed Cyber Solutions

- Threat and vulnerability management
- Security monitoring + operations (SOC)
- Operational and network security

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

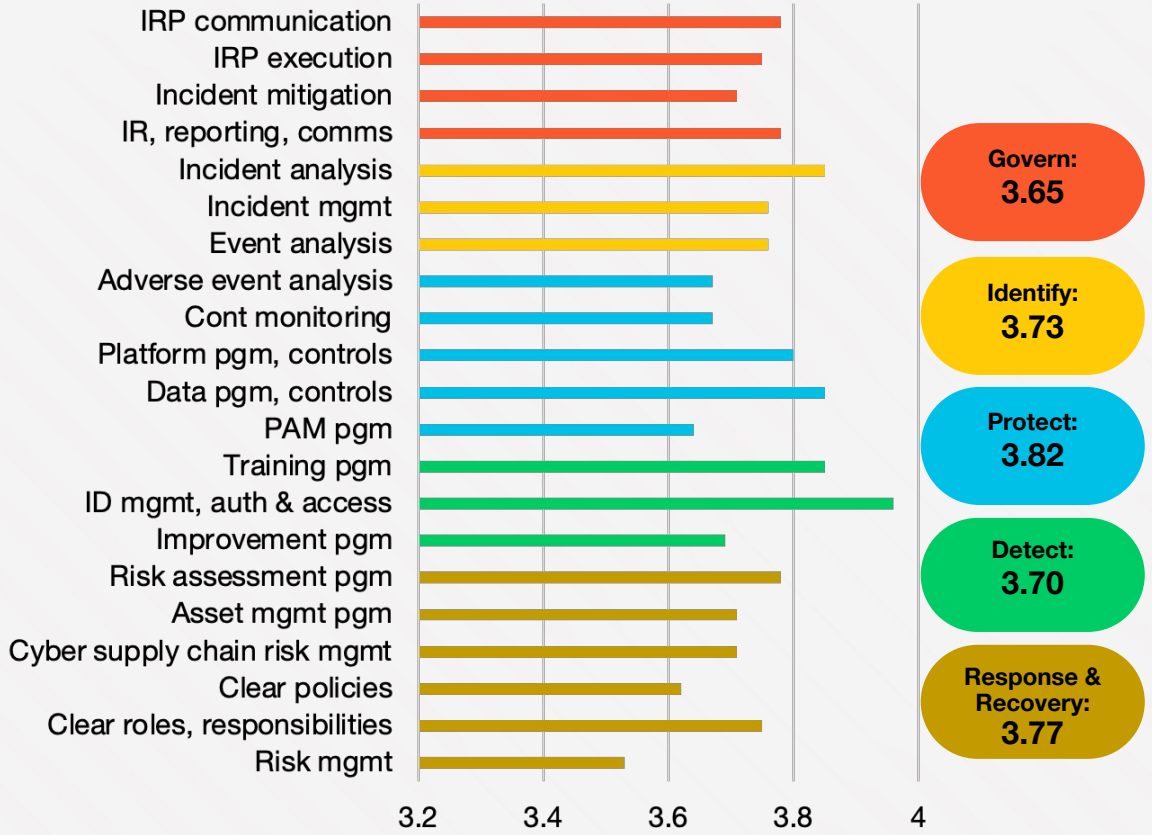
Taiwan

Cyber budget as % of revenue **11.5%**

Top 3 areas where cybersecurity spend will increase more than 10%

Network security hardware	32.73%
Training/education	27.27%
Strategy, talent & governance, risk & compliance	21.82%

Country NIST framework

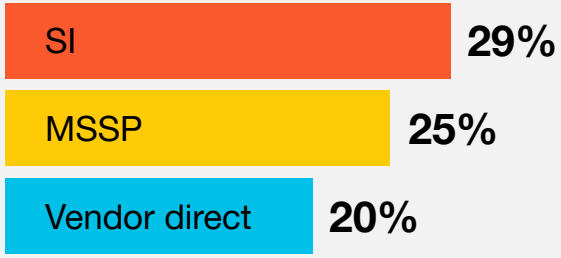


Visual range shown above: (3.2 - 4.0)

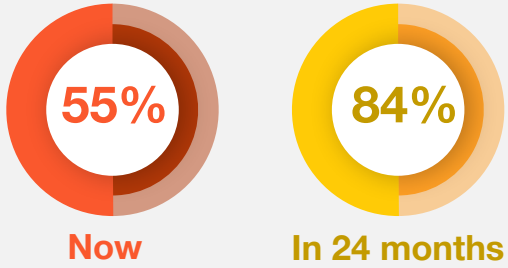
 | © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Taiwan

Top 3 preferred partner types for cybersecurity solutions and support



Percentage of organizations using partners



Partner support insights

Where demand for partners will be needed **most** in the next 2 years

- Cloud and emerging technology
- Security monitoring + operations (SOC)
- Threat and vulnerability management

Top attributes that influence partner selection

- Tailored solutions (32.7%)
- Alignment with compliance and regulatory requirements (32.7%)
- AI-supported products/solutions (30.9%)

**Excluding pricing*

Top reasons why organizations change partners

- Supply chain issues (40%)
- Breach or major outage (38%)
- Penetration testing (33%)

**Excluding pricing*

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Vietnam

Benchmark score average

19.76

out of 25

Average number of core cybersecurity vendor solutions

TOP 3

Business Cyber Drivers

- Protecting intellectual property
- Ensuring supply chain performance and delivery
- Governance, risk and compliance activities

Investment Priorities

- Strengthening security policies
- Optimizing the security ecosystem
- Providing employees with security awareness and training

Deployed Cyber Solutions

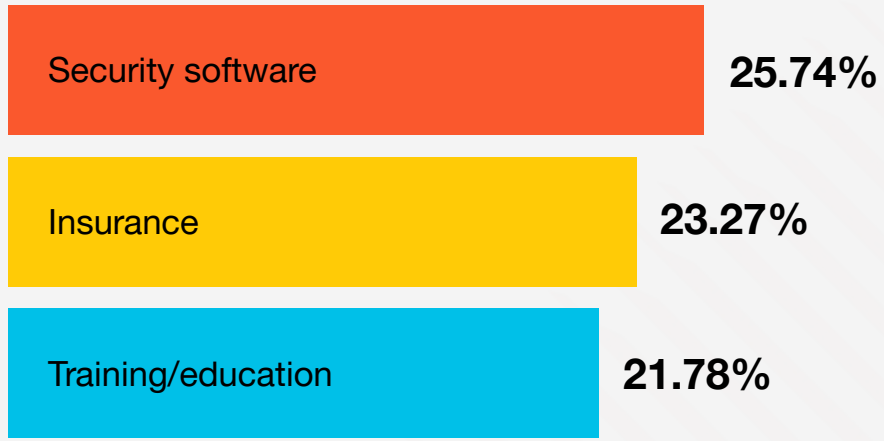
- Application and data security
- Security monitoring + operations (SOC)
- Cloud and emerging technology

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

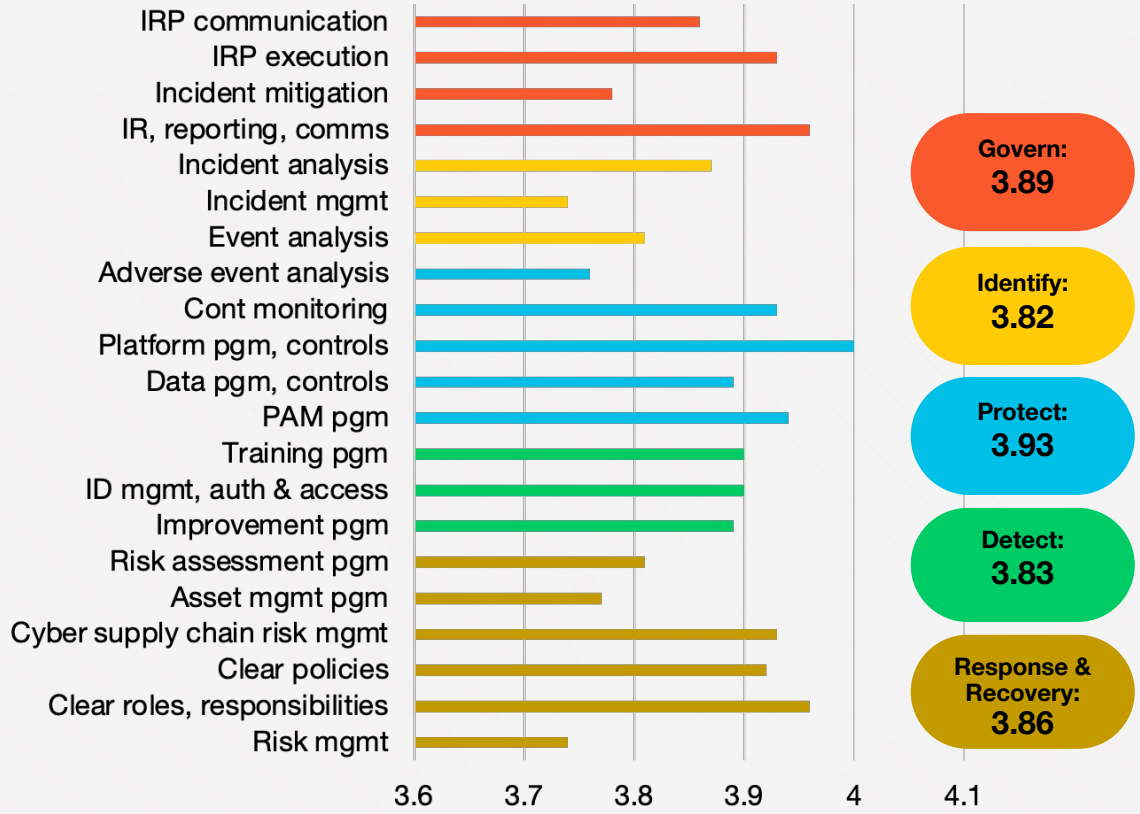
Vietnam

Cyber budget as % of revenue **14.0%**

Top 3 areas where cybersecurity spend will increase more than 10%



Country NIST framework

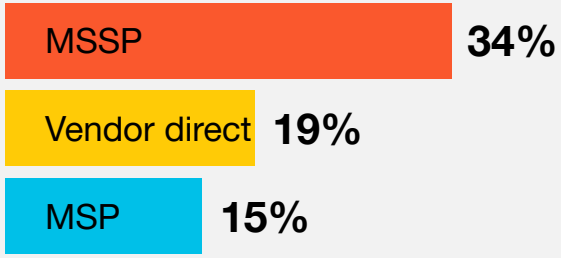


Visual range shown above: (3.6 - 4.1)

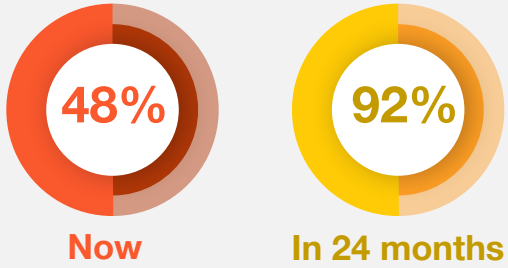
 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Vietnam

Top 3 preferred partner types for cybersecurity solutions and support



Percentage of organizations using partners



Partner support insights

Where demand for partners will be needed **most** in the next 2 years

- Cloud and emerging technology
- Threat and vulnerability management
- Education and training

Top attributes that influence partner selection

- Ability to integrate new solutions to existing technology (33.7%)
- Tailored solutions (30.7%)
- AI-supported products/solutions (25.2%)

*Excluding pricing

Top reasons why organizations change partners

- Supply chain issues (41%)
- Poor solution performance (41%)
- Breach or major outage (36%)

*Excluding pricing

 © 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

About Palo Alto Networks

Palo Alto Networks is the global cybersecurity leader, committed to making each day safer than the one before with industry-leading, AI-powered solutions in network security, cloud security and security operations. Powered by Precision AI, our technologies deliver precise threat detection and swift response, minimizing false positives and enhancing security effectiveness. Our platformization approach integrates diverse security solutions into a unified, scalable platform, streamlining management and providing operational efficiencies with comprehensive protection.

From defending network perimeters to safeguarding cloud environments and ensuring rapid incident response, Palo Alto Networks empowers businesses to achieve Zero Trust security and confidently embrace digital transformation in an ever-evolving threat landscape. This unwavering commitment to security and innovation makes us the cybersecurity partner of choice.

At Palo Alto Networks, we're committed to bringing together the very best people in service of our mission, so we're also proud to be the cybersecurity workplace of choice, recognized among Newsweek's Most Loved Workplaces (2021–2024), with a score of 100 on the Disability Equality Index (2024, 2023, 2022), and HRC Best Places for LGBTQ+ Equality (2022). For more information, visit www.paloaltonetworks.com.

Palo Alto Networks, Prisma, Cortex, Cortex XSIAM, Cortex XDR, Cortex Xpanse, Cortex XSOAR, Precision AI and the Palo Alto Networks logo are trademarks of Palo Alto Networks, Inc. in the United States and in jurisdictions throughout the world. All other trademarks, trade names, or service marks used or mentioned herein belong to their respective owners.

About TRA

Tech Research Asia (TRA) is a technology research, consulting and advisory firm working across Asia Pacific specializing in analyzing trends in technology and the impact on business value. We help organizations across the region, technology vendors and channel partners build deeper market understanding and improve their business results. We are rigorous, fact-based, open, and transparent. And we offer research, consulting, engagement and advisory services. We also conduct our own independent research on the issues, trends, and strategies that are important to executives and other leaders that want to leverage the power of modern technology.
www.techresearch.asia

Copyright and Quotation Policy

The Tech Research Asia name and published materials are subject to trademark and copyright protection, regardless of source. Use of this research and content for an organization's internal purposes is acceptable given appropriate attribution to Tech Research Asia. For further information on acquiring rights to use Tech Research Asia research and content please contact us via our website or directly.

Disclaimer: You accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from using this research document and any information or material available from it. To the maximum permitted by law, Tech Research Asia excludes all liability to any person arising directly or indirectly from using this research and content and any information or material available from it. This report is provided for information purposes only. It is not a complete analysis of every material fact respecting any technology, company, industry, security or investment. Opinions expressed are subject to change without notice. Statements of fact have been obtained from sources considered reliable, but no representation is made by Tech Research Asia or any of its affiliates as to their completeness or accuracy.