Monitor
Deloitte.

Beyond defence: Positioning Singapore as Asia's cybersecurity innovation hub

Outlook, growth opportunities, and strategic shifts

September 2026

Contents

Executive Summary

01 Outlook: Global developments in cybersecurity

- Cybersecurity is experiencing disruption globally, across nine key trends in **technology, geopolitics, and regulation.**
- Among the nine key trends, **six have greater impact and momentum** in driving cybersecurity capability needs, **led by the Evolution in AI** trend.

02 Growth opportunities: Singapore is well-positioned to generate value amidst disruption

- Singapore is at the forefront of these disruptions and is well positioned to generate significant value.
- Singapore's **right-to-play** is underpinned by: 1) Conducive conditions for **innovation**; 2) High cybersecurity **spend**; 3) Robust **ecosystem** of cybersecurity players; 4) Sustained **government** support in cybersecurity and frontier technologies.
- Translating Singapore's cybersecurity strengths across demand, innovation, supplier ecosystem, and government support could unlock **2,300 new jobs** and grow the industry to reach as much as **USD 4.8B by 2030.**

03 Strategic shifts: To capture key growth opportunities

- **Five growth opportunities** have emerged as anchor bets for the next phase of Singapore's cybersecurity journey: **1) AI-enabled security platforms; 2) Enterprise Post-Quantum Cryptography (PQC) migration platforms; 3) Sovereign & enterprise cloud resilience; 4) Cyber-physical resilience platform; 5) Trust & security for next-gen connectivity.**
- To capture and generate value from the growth opportunities, Singapore should pursue **five strategic shifts**: 1) Build **new capabilities** that leverage and amplify Singapore's strengths; 2) Position strategically to draw **foreign investments**; 3) Motivate businesses **to adopt services for nascent capabilities** 4) **Export Singapore's strengths regionally**; 5) Focus on **higher-value new cybersecurity jobs.**

Research & data sources

Baseline market size estimates and projected growth are based on a combination of publicly available sources and an industry survey commissioned by the Cyber Security Agency of Singapore and led by Deloitte Singapore, which included ~160 industry respondents within the Singapore cybersecurity ecosystem, across buyers, suppliers, and enablers.

Growth opportunities and strategic shifts were identified using Deloitte-developed models, including an analysis of 700+ companies operating within Singapore's cybersecurity ecosystem.

These findings were subsequently validated through focus group discussions with ~30 experts from cybersecurity companies, institutes of higher learning, and government agencies.

The views, opinions, analyses and recommendations expressed in this publication are those of Deloitte and are based on information available as at the date of publication. They do not necessarily reflect the views, positions or endorsements of the Cyber Security Agency of Singapore (CSA) or any other governmental or regulatory authority. References to, or information obtained from, external sources are included for general informational purposes only and should not be construed as an endorsement, validation or approval by such sources.

This publication does not constitute legal, regulatory, cybersecurity or other professional advice, and readers should obtain appropriate professional advice before acting on any information contained herein.

01

Outlook: Global developments in cybersecurity

Cybersecurity is experiencing global disruption, driven by nine key trends across technology, geopolitics, and regulation

Legend: *Technology* | *Geopolitical* | *Regulatory*

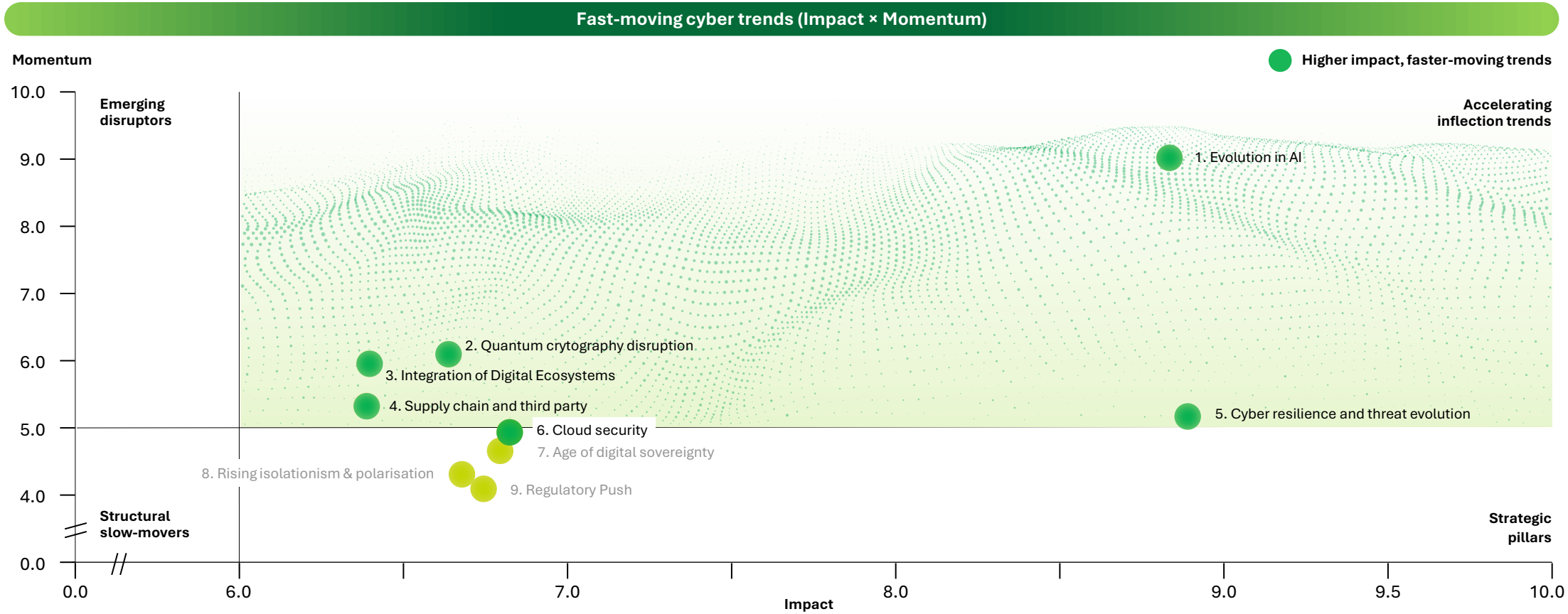
Key developments

Assistive to autonomous AI	Safe readiness through PQC & crypto-agility	Cross-sector digitalisation	Supply-chain & CI/CD compromise	Cybercrime	Cloud-native & multi-cloud resiliency	Transition to digital sovereignty	Tariffs & trade policy uncertainty	Elevation of CISO accountability & governance
Exploitation & adaptation of adversarial AI	"Harvest-now, decrypt-later" threats	Next-gen connectivity & infrastructure	Software supply-chain transparency	Identity-centric security models	Sovereign & distributed cloud models	Trusted decentralised infrastructure	Regional war & conflict	Regulatory & compliance complexity
AI governance & assurance				Zero-trust			State-linked disinformation campaigns	
Evolution in AI	**Quantum cryptography disruption**	**Integration of digital ecosystems**	**Supply chain & third party**	**Cyber resilience & threat evolution**	**Cloud security**	**Age of digital sovereignty**	**Rising isolationism & polarisation**	**Regulatory push**
AI reshapes the digital ecosystem, expanding attack & defence surfaces	Advancements in quantum computing will shatter existing encryptions	Integration across different ecosystems blurs boundaries & heightens the threat landscape	Compromised supply chains erode trust across interconnected digital ecosystems	Adaptive defence against escalated threats against the cyber landscape	Evolving cloud models challenge security boundaries and systemic dependency risks	Foreign influence concerns driving push for localisation of tech ecosystems	Driving fragmentation of digital trust, global collaborations and interoperability	Growing tech & cyber mandates in response to the growing threat landscape

9 key trends

Source(s): Deloitte analysis

Among the nine key trends, six have greater impact and momentum in driving cybersecurity capability needs, led by the Evolution in AI trend



Note(s): Scoring methodology: Each trend's impact was assessed across 10 cybersecurity domains against 6 impact areas (e.g., regulatory requirements, technology ecosystem and threat landscape). Each applicable impact area was scored 1 if impacted (otherwise 0), based on responses to the Deloitte Cybersecurity Industry Landscape Survey 2025. Scores were averaged across domains and converted to a 10-point scale. Momentum was assessed based on responses to the Deloitte Cybersecurity Industry Landscape Survey 2025, with the resulting survey score weighted against a 10-point digital-interest score derived from average Google Trends activity for related keywords from October 2024 to September 2025.
Source(s): Deloitte Cybersecurity Industry Landscape Survey 2025; Google Trends & Glimpse; Deloitte analysis

02

Growth opportunities: Singapore is well-positioned to generate value amidst disruption

Singapore is at the forefront of these disruptions and is well positioned to generate significant value

Singapore's right-to-play is underpinned by...

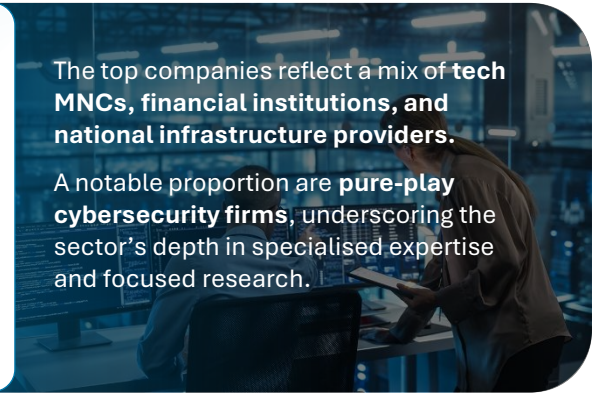
1. Conducive conditions for innovation
2. High cybersecurity spend
3. Robust ecosystem of cybersecurity players
4. Sustained government push in cybersecurity and frontier technologies

Source(s): Deloitte analysis

Singapore's strong innovation activity is illustrated in its cybersecurity related R&D hiring and spending

Top 20 hirers of cybersecurity R&D

1	NCS	6	Accenture	11	Seagate Technology	16	Singtel
2	Ensign InfoSecurity	7	Palo Alto	12	UOB	17	PayPal
3	CrowdStrike	8	Dell	13	ST Engineering	18	Alibaba Cloud
4	M.Tech	9	Microsoft	14	OCBC	19	Cloud4C
5	Google	10	FireEye	15	Visa	20	Aspire Systems



The top companies reflect a mix of **tech MNCs, financial institutions, and national infrastructure providers.**

A notable proportion are **pure-play cybersecurity firms**, underscoring the sector's depth in specialised expertise and focused research.

Top 20 spenders of cybersecurity R&D

1	Palo Alto	6	Microsoft	11	Ensign Infosecurity	16	Trend Micro
2	Alibaba Cloud	7	StarHub	12	Salesforce	17	Huawei
3	Fortinet	8	Seagate Technology	13	Check Point	18	Mastercard
4	Visa	9	Grab	14	Google	19	Group-IB
5	ST Engineering	10	Singtel	15	NCS	20	AWS

The top cybersecurity R&D spenders span **cloud platforms, financial institutions, and digital service providers.**

Most of the top cybersecurity R&D spenders operate outside the cybersecurity supplier ecosystem.

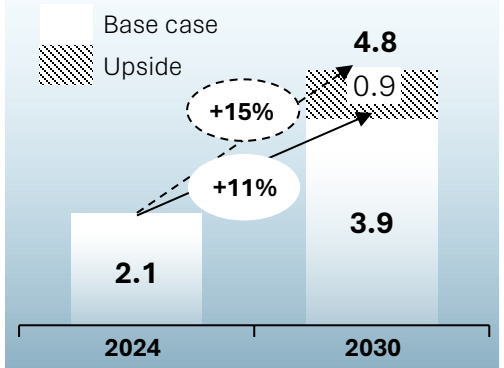
Source(s): S&P Capital IQ, Emerging Market Information Service (EMIS), D&B Hoovers, Deloitte analysis

Singapore's cybersecurity spend is projected to grow >11%, driven by cloud and AI adoption across six key sectors facing regulatory, cyber attacks, and digitalisation pressures

Top 6 sectors

Singapore cybersecurity market

USD B



Upside to >15% driven by

1.1× **Cloud**
Singapore plan to expand DC capacity by >1/3

1.4× **AI**
SGD 1B+ 5-year National AI R&D Plan

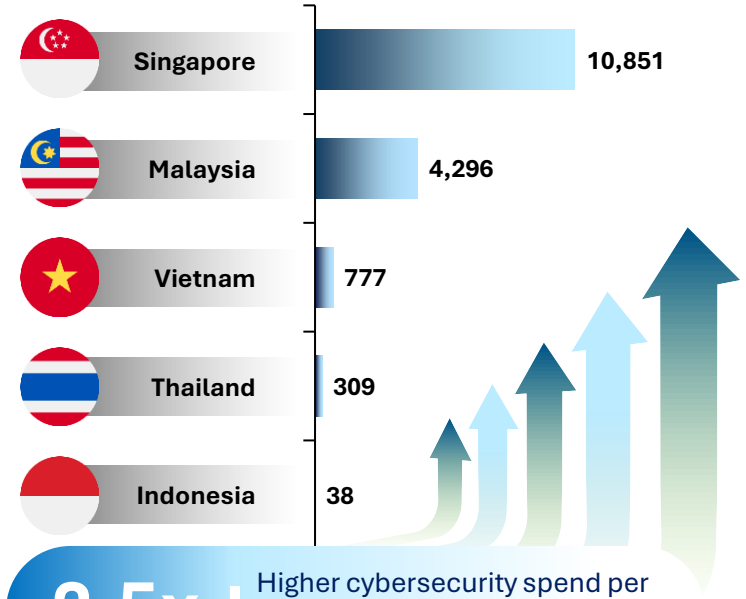
Sector	2024 spend, USD B	CAGR (24'-30')	Rationale for spend
BFSI	0.5	16%	• Singapore banks face **~1,830 cyberattacks weekly** as one of the world's global financial hubs • **CTREX[2], MAS' 2024 quantum-risk advisory and FSTI 3.0[3] quantum/AI funding** drive cybersecurity spend
Infocomm & media	0.4	11%	• **Highest technology spend** of any sector (~USD 15B by 2030, 14% CAGR) and the largest share of incidents (26%) • Cloud and data centre providers are now regulated as **Foundational Digital Infra under CSA (Amendment Act) 2024**
Manufacturing	0.3	12%	• Contributes to **~20% of GDP**, making cyber downtime a high-value operational and economic risk • **159 ransomware cases in 2024, up 21%,** plus IT-OT/IoT adoption, driving investment in OT security
Government	0.3	10%	• **>60% of FY2024 ICT procurement spend** went to digital infrastructure modernisation, **ageing systems set to double by 2029** • **GCC2.0[4], GovZTNA[5] and GCSOC[6]** strengthen whole-of-government cybersecurity capabilities
Healthcare	0.1	10%	• The **2018 SingHealth breach** (1.5M patient records) remains the catalyst for sustained investment • **Health Information Act requirements** take effect from 2027, requiring **NEHR[7] -linked providers** to meet cyber requirements
Maritime	0.03	12%	• **World's busiest transshipment port**, with Tuas Port set to reach **65M TEUs by 2040s** • **Maritime Cyber Assurance and Operations Centre, mandatory digital bunkering, and maritime 5G initiatives are driving cybersecurity investment**

Note(s): 1. Determined by taking an aggregated view of both cybersecurity spend and growth, 2. Cyber and Technology Resilience Experts Panel established by MAS in 2024, 3. Financial Sector Technology and Innovation, 4. Government on Commercial Cloud 2.0, 5. Government Zero Trust Architecture, 6. Government Cyber Security Operations Centre, 7. National Electric Health Record
Source(s): Gartner, Mordor Intelligence, Deloitte Cybersecurity Industry Landscape Survey 2025, PSPC Singapore, European Repository of Cybersecurity Incidents for Singapore, Check point, Singstat, GovTech, MOH, MPA, Deloitte Analysis

2 High cybersecurity spend

Singapore leads SEA in cybersecurity spend intensity, with enterprises spending >2.5x of the next closest peer, while other neighbouring countries remain early-stage growth markets

Cybersecurity spend per capita (USD) (2030)[1]



2.5x Higher cybersecurity spend per capita than Malaysia, the next closest country in SEA

Note(s): Figures are indicative only, based on internal estimates, assuming a constant enterprise base and the projected 2030 cybersecurity market size of each country
Source(s): Gartner, Mordor Intelligence, CSA Singapore, NACSA Malaysia, Rajah & Tann, HBT Law, CAN, EDB, Malaysia Ministry of Digital, AIBP, Deloitte analysis

Singapore leads SEA in cybersecurity spend intensity...

01 Mature, operationalised regime; Peers are catching up

- **Singapore** has had a **dedicated Cybersecurity Act since 2018**, strengthened by 2024 amendments
- **Malaysia's Cyber Security Act** only came into force in **2024**
- **Indonesia still relies on a patchwork of regulations** without a standalone cybersecurity law

02 Digital ecosystem makes Singapore structurally cyber-intense

- **~37%** of ASEAN cloud spend; one of APAC's densest DC markets with **~1%** vacancy, nearing **1GW** in 2024
- Home to **~4,200** regional MNC headquarters, the highest in APAC between 2013 and 2023, driving outsized data and cybersecurity exposure

03 Deepest, most structured talent base

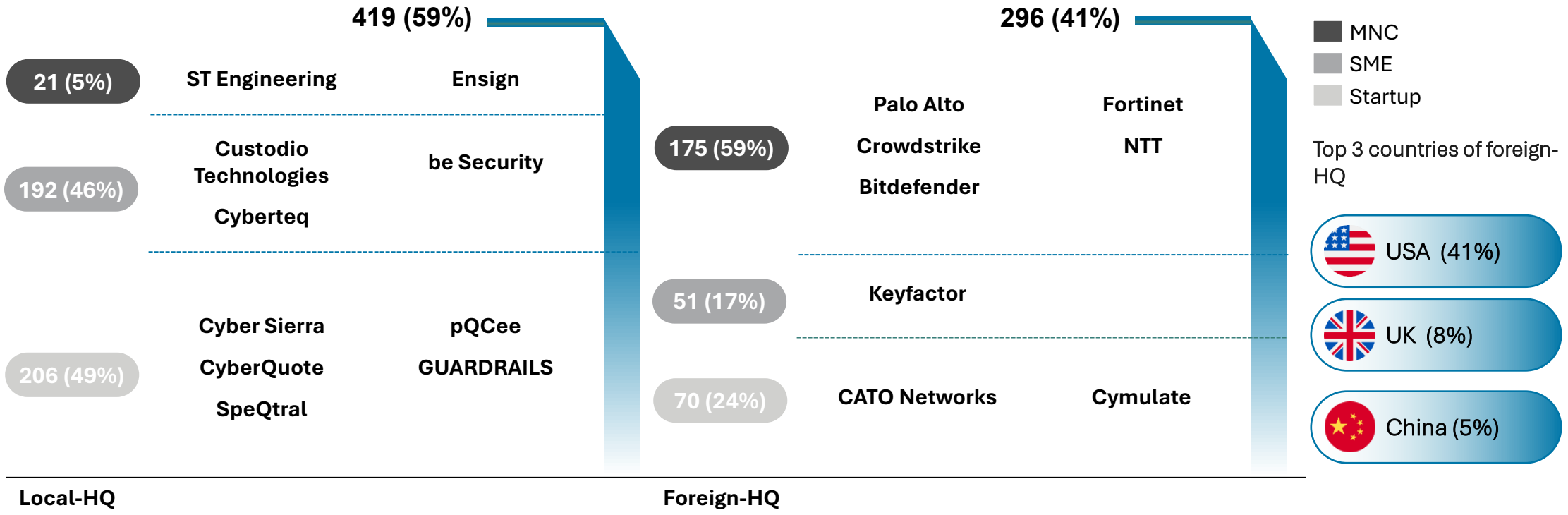
- **Singapore moved earlier** to institutionalise national cyber talent pipelines, with SG Cyber Talent in 2020 and CyberSG TIG in 2024
- **SEA peers are catching up**, with Malaysia's Cybersecurity Academy and Thailand's National Cyber Academy (THNCA) launched in 2025

04 Unmatched cybersecurity & AI innovation density

- Hosts **500 of the region's 700** AI startups in the region
- Secured **USD 1.31B in private AI funding** from 2H 2024 to 1H 2025
- Home to former **Innovation Cybersecurity Ecosystem at Block71 (ICE71),** the region's first cybersecurity start-up hub

Among ~700 cybersecurity companies, Singapore has a rich ecosystem of players, from local-HQ startups & SMEs to foreign-HQ MNCs, supporting a depth of innovation and regional scale

Singapore is both a local supplier base and a regional hub for global players, combining both the depth of innovation from start-ups and SMEs, and the scale and credibility from MNCs



Note(s): 1. Startup is defined as ≤ S$100 million in revenue or ≤ 200 employees, ≤ 10 years since incorporation, 2. SME is defined as ≤ S$100 million in revenue or ≤ 200 employees, > 10 years since incorporation, 3. MNC is defined as > S$100 million in revenue and > 200 employees with operations beyond Singapore
Source(s): TIG Cyber Catalogue, IMDA, CSRO Licensed Service Providers, F6S , Lusha, GovWare, Tracxn, Deloitte Analysis

Sustained government support is catalysing cybersecurity spending and innovation across three fronts

01 Frontier technology investments drive demand for cybersecurity

USD 800M*
National AI R&D Plan
Investment to strengthen Singapore's AI R&D capabilities from 2025-2030, driving demand for secure AI infrastructure capabilities.

USD 200M
Quantum
Investment to boost quantum tech research and talent over 5 years, under National Quantum Strategy.

USD 30B
RIE 2030
Investment to strengthen capabilities in AI, data, and compute, increasing the need for security-by-design across frontier technologies.

02 Cybersecurity regulations fuel spending

Cybersecurity Amendment Act (2024)
Expands cybersecurity obligations beyond Critical Information Infrastructure (CII) to include Systems of Temporary Cybersecurity Concern (STCCs) and other critical systems.

Digital Infrastructure Act (announced in 2025)
Upcoming baseline requirements to strengthen the resilience and security of major cloud service providers and data centres.

Proposed guidelines on AI risk management (2025)
Applies to all financial institutions and establishes expectations for AI governance, risk management, and lifecycle controls.

03 Grants, R&D funding, and ecosystem programmes grow local cybersecurity supply ecosystem

USD 792M
Startup Singapore Equity scheme
Funding allocated in 2026 to support promising deep-tech start-ups and strengthen the broader frontier technology ecosystem on which cybersecurity firms can build, collaborate, and scale.

USD 12M
Cybersecurity R&D funding
Awarded to 18 projects under CyberSG R&D Programme Office, converting research into deployable solutions and build the local supply ecosystem.

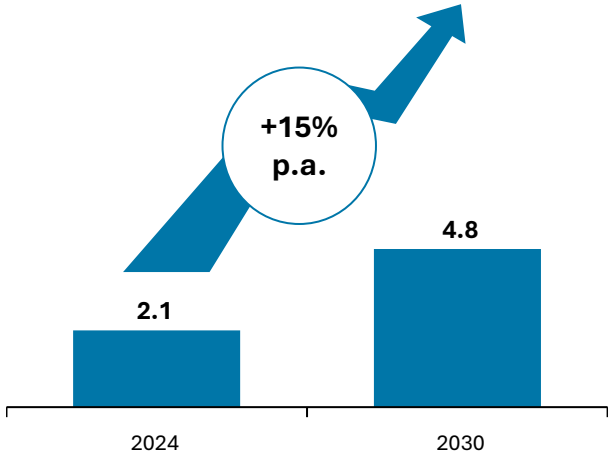
USD 90M
CyberSG ecosystem funding
Allocated to the CyberSG R&D Programme Office and the CyberSG Talent, Innovation and Growth Collaboration Centre (TIG Centre) to develop talent and promote innovation.

Note(s): 1. Research, Innovation, and Enterprise 2030, 2. Systems of Temporary Cybersecurity Concern
Source(s): Deloitte Analysis, IMDA, CSA, Budget 2026, The Straits Times

*Figures converted to USD

Translating Singapore's cybersecurity strengths in demand, innovation, supplier ecosystem, and government support, could grow the industry to USD ~4.8B and create 2,300 new jobs by 2030

Market size (USD B)



New jobs created by 2030

+2,300 new jobs

(USD 108,000 annual wage/worker in 2030)

Based on 9,500 workers and an average annual wage of USD 62,000 per worker in 2024

Sources of value leaks today

Reliance on foreign vendors	Despite high cybersecurity spending, Singapore remains highly reliant **on foreign vendors (~50% vs. 20% in mature markets such as UK)**
Local IP creation	Despite strong innovation momentum, **cybersecurity IP creation remains limited**, making up **<3% of SG's ICT IP filings**
SG Cybersecurity exports	Local supplier exports contribute only **34% of revenue** (vs. UK: 55%, China: 60%) suggesting **headroom to scale regionally**

3 moves to capture the value

Ride the new tech wave

Shift to higher-value emerging tech (e.g. AI security, PQC) to drive margins and productivity via premium services and AI-enabled workflows

Build exportable, IP-driven firms

Scale local IP, start-ups and R&D to capture domestic demand and expand globally to drive export growth

Grow high-wage roles

Develop high-skill frontier roles and expand the local talent pipeline to build domestic capability and reduce reliance on imported expertise

Source(s): Singstat, World Bank, SkillsFuture, MOM, UK Security Export Statistics 2030, Deloitte Analysis

03

Strategic shifts: To capture key growth opportunities

5 growth opportunities have emerged as anchor bets for the next phase of Singapore's cybersecurity journey

1 AI-enabled security platforms

~30

Global market size, USD B (2024)

+24% CAGR

(2024-2030)

Why now

Singapore is actively pushing **AI governance** (AI Verify, Model AI Governance Framework), lifting demand for AI-specific security controls

Right to play

East-west hub for frontier model assurance in **multi-model and agentic AI**

2 Enterprise PQC migration platform

0.3

+40% CAGR

Enterprise adoption is still nascent, creating runway for innovation within PQC

PQC migration support across discovery tools, platform & services

3 Sovereign & enterprise cloud resilience

~10

+25% CAGR

DSTA's 2025 selection of an air-gapped Oracle Cloud Isolated Region validates the need for sovereign isolation and resilient operations

Build **sovereign-grade** cloud security **on hyperscaler ecosystems** for **data, access and recovery**

4 Cyber-physical resilience platform

~20

+13% CAGR

IT–OT convergence; ransomware +21% to 159 cases in 2024, with manufacturing being the most affected sector

Leverage **testbed strengths** and **cyber-informed engineering** know-how

5 Trust & security for next-gen connectivity

6

+30% CAGR

Telco anti-scam enforcement is intensifying, MDDI disrupted 60,000 scam lines in 2025

Replicate **SG's 5G capabilities in 6G security**

Source(s): Grand View Research, MarketsandMarkets, Cyber Security Agency, DSTA, MDDI, Deloitte analysis

To capture and generate value from the growth opportunities, Singapore needs to embark on 5 strategic shifts

Build capabilities that leverage and play to Singapore's strengths

Posture strategically to draw foreign investments to support capability building

Motivate businesses to adopt services for nascent capabilities to drive demand for capability build

Export Singapore's strengths regionally, with differentiated approaches for products vs. services focus

Focus on higher-value new cybersecurity jobs to manage redundancies from disruptive tech

Shift #1: Build cybersecurity capabilities that best leverage and play to Singapore's strengths

Growth opportunity	Key capabilities to build[1]	What each enables
AI-enabled security platforms	Multi-model security testing & red teaming	Stress-tests AI systems with attacker techniques; validates the full AI workflow
	Multi-agent runtime defence	Enforces guardrails on what AI agents can access and execute
Enterprise PQC migration platform	Automated discovery tools	Discovers cryptographic use beyond network- and certificate-level
	PQC migration-as-a-service	Inventorises crypto usage and runs enterprise-wide migration
	PQC migration platform	Deployable SDKs / libraries embedding quantum-safe crypto into existing protocols
Sovereign & enterprise cloud resilience	Sovereign crypto-agile key control stack	Hardware vault that stores encryption keys and logs / controls access
	Multi-cloud machine identity defence	Monitors machine accounts; protects API keys, service accounts, and tokens
	Cleanroom cloud incident recovery	AI-orchestrated real-time recovery that prioritises critical systems
Cyber-physical resilience platform	Cyber-physical exposure management	Discovers IT, OT, and IoT assets and maps realistic attack paths
	Sector OT cyber ranges & scenarios	Industry-specific cyber ranges emulating real systems, data flows, and threats
Trust & security for next-gen connectivity	5G network API security services	Standardised telecom APIs to verify if a number / SIM was changed
	Intent-driven security for 6G networks	Monitors core network functions, identity (SIM / eSIM), edge and devices

Across all

AI-enabled SOC
AI-augmented monitoring & detection across all platforms

AI-enabled VAPT
Continuous AI-driven vulnerability assessment & pen-testing

AI-enabled compliance
Automated, continuous compliance and assurance

Note(s): 1. Non-exhaustive
Source(s): NIST, CSA, GSMA, Deloitte analysis

Shift #2: Position strategically to attract foreign investments to help build capabilities

Singapore has limited cybersecurity-focused VCs

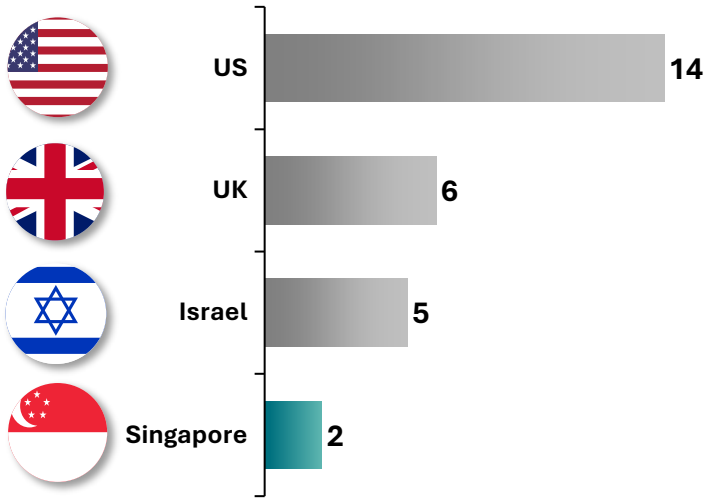
02 of 15

Global top cybersecurity-focused VCs active in Singapore, with the rest mainly operating in the US, UK and Israel

Lightspeed

Sequoia

Cybersecurity VC count by country



Room to attract global capital, drawing on 2 proven models

Government-backed global innovation prize competition

Multi-year AI cybersecurity competition (AIxCC)

USD 30M

Global prize pool

- Global draw for frontier-AI labs, Anthropic, Google, Microsoft & OpenAI supplied models and credits
- Attract top teams worldwide onto a global stage (DEFCON)
- Winning systems open-sourced for commercialisation

Learnings for Singapore

Host a flagship cybersecurity challenge, build global visibility and pull in frontier-AI labs and talent

Government x Platform co-investment fund

Crowdstrike **Accel**

USD 100M

Strategic fund (Falcon Fund II)

- Co-invests in cybersecurity startups; grow fund from USD 20M (Fund I) to USD 100M (Fund II)
- Portfolio firms gain API integration, CrowdStrike Marketplace access & go-to-market

Learnings for Singapore

Government partners a hyperscaler / platform to anchor a co-investment fund here, drawing in capital, platform access, and follow-on investors

Source(s): AIxCC, Crowdstrike, Deloitte analysis

Shift #3: For nascent capabilities, Singapore can drive enterprise adoption, enabling suppliers to build capability; PQC is a case in point where limited demand constraints supply

4 demand-side drivers – for supply to follow *(PQC as example)*

Signal

Set national PQC migration roadmap with deadlines to replace today's at-risk encryption

How it drives supply
Clear demand signal by a fixed date enables suppliers to build required PQC capability

Gap today
No SG PQC roadmap yet, only Quantum-Safe Handbook & Readiness Index

Mandate

Embed PQC-readiness and crypto-agility clauses in procurement requirements and regulations, starting with government and CII

Guaranteed demand from contract clauses gives suppliers the assurance to build capability

The Cybersecurity Amendment Act (2024) widened CII oversight but does not require PQC

Activate

Run an awareness campaign for CISOs, tech, and procurement leaders

Buyers with awareness begin asking for PQC, triggering vendors to offer it

National campaigns target the public cyber-hygiene, not enterprise PQC

Fund

Extend cybersecurity grants to PQC to lower upfront costs, especially for SMEs that may not yet see PQC as an urgent budget item

Visible grant-backed demand gives PQC suppliers confidence to build and commercialise solutions

PSG[1] funds basic SME cyber-hygiene (Cyber Essentials), not PQC migration

Singapore's supply base today *(PQC as example)*

10+ players exist
in SG today, however the market remains limited where few are pure-play PQC, with the majority offering it within broader portfolios

pQCee | **PQStation** | **Aires AQT**

ST Engineering | **NCS** | **i-Sprint** | **Sixscape**

...among others

- Pure-play PQC
- PQC within broader portfolio

Notes(s): 1. Productivity Solutions Grant (PSG)
Source(s): IMDA, MAS, CSA, GovTech, CSA, Company websites of PQC suppliers in SG, Deloitte analysis

Shift #4: Singapore should focus not only on domestic capability building, but also on regional scale-up and exporting its differentiated strengths

What Singapore can potentially export regionally

Cloud security

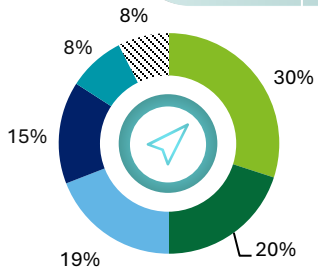
Convert GCC[1] from a domestic cloud reference into an export platform, showcasing SG cloud security solutions and linking local startups to international demand

Proven abroad: Estonia exports its digital-government know-how via e-Estonia Briefing Centre, the same can be done for cloud security

OT security

Turn **Singapore's OT strengths** - 5 iTrust / SUTD testbeds, OT roadmap, training and OT-ISAC[2], into **G2G2B regional testbeds** that help companies validate, reference and win OT projects abroad

EU FEDeRATED (2019–2024) demonstrates a scalable multi-country living-lab model, with 15 partners, 22 labs across Europe, ~200 stakeholders (not OT security specific)



Priority export markets

Export revenue share by country

- Malaysia
- Rest of SEA
- UK/US
- China
- Rest of APAC
- Others

Export strategy should differ by company model

Services -led

- Leverage SG's **strong base of cybersecurity managed and professional services providers** to export services (e.g., PQC migration)
- **Scale through regional delivery teams and partner networks** to localise implementation

For example...
Ensign

SG-based cybersecurity services firm with ~1,000 employees, offices across multiple APAC countries, and ranked 1st in Asia in MSSP Alert's Top 250 MSSP 2024

Products -led

- **Compete in specialised product niches** (e.g., AI security)
- **Scale through integration and channels**, by plugging into major cloud / security platforms, and connecting with global distributors, investors and enterprise buyers

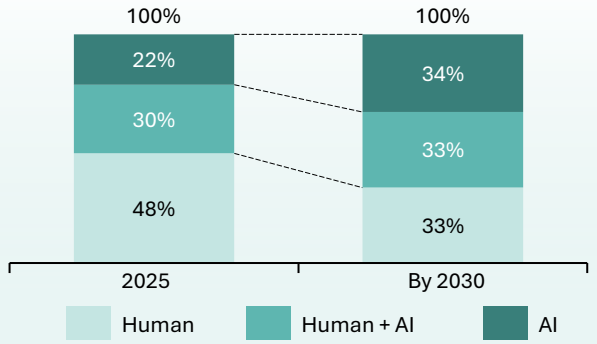
For example...
Horangi Cybersecurity

SG-based cloud-security startup acquired by Bitdefender, with its cloud security capabilities added into Bitdefender's GravityZone portfolio to reach a larger global customer base

Note(s): 1. Government on Commercial Cloud, 2. OT Cybersecurity Information Sharing and Analysis Centre (OT-ISAC)
Source(s): EU-FEDeRATED, e-Estonia Briefing Centre, Business Wire, Bitdefender, Deloitte analysis

Shift #5: Pivot focus towards higher-value new cybersecurity jobs aligned with the growth opportunities to manage the impact of redundancies from disruptive technologies

AI is reshaping how cyber work gets done...



Human-only work falls ~15 pts (48% → 33%) as AI augments routine tasks

...Shifting the role mix from automatable to higher-value

At risk — automatable

- **Security operations analyst**
- **Associate security analyst**

Emerging — higher-value roles

- OT cybersecurity engineer
- AI behaviour auditor
- AI cybersecurity specialist
- Cybersecurity data scientist
- Quantum-ready cryptography advisor

To capture the shift to higher-value work, focus on 3 levers

Hire for technical readiness

Weigh projects, labs, certs, and portfolios; AI does not replace complex technical judgement

Hire interdisciplinary talent

Value cross-discipline capabilities and transferable soft skills

Reward skills, not tenure

Variable pay tied to proven skills and a shift from tenure-based to skills-based pay

Source(s): WEF, Fortinet, Centre for Cybersecurity Institute, Deloitte analysis

Conclusion

All in all, amidst the disruptive developments in global cybersecurity, Singapore has a strong role to play as a **cybersecurity innovation hub for APAC.**

Strong cybersecurity innovation **elevates Singapore's *trust* factor** and brings **purpose to Singapore's bold investments in frontier technologies.**

Cybersecurity is a space where **sharpness of capabilities is of greater importance than scale.** Singapore being a **small yet highly innovative** nation, is well positioned to **build those sharp and forward-looking capabilities** for its own demand, for ASEAN's demand and also for global demand.

The **future of cybersecurity** will be **shaped not by the largest players,** but by those who are **agile and innovative** enough to see around the corner and **steer frontier technologies** to make our digital world safe and trusted.

Acknowledgements

Samrat Bose
Partner,
Monitor Deloitte
Deloitte Southeast Asia
sambose@deloitte.com

Chong Chor Ming
Senior Manager,
Monitor Deloitte
Deloitte Singapore
chorchong@deloitte.com

Annabelle Li
Senior Consultant,
Cyber Strategy & Transformation
Deloitte Singapore
annabli@deloitte.com

Marcus Cheung
Consultant,
Monitor Deloitte
Deloitte Singapore
macheung@deloitte.com

Edna Yap
Leader,
Cyber Strategy & Transformation
Deloitte Southeast Asia
edyap@deloitte.com

Teo Kay Lynn
Senior Manager,
Cyber Strategy & Transformation
Deloitte Singapore
kateo@deloitte.com

William Tang
Consultant,
Monitor Deloitte
Deloitte Singapore
willitang@deloitte.com

Leong Kai Seng
Director,
Cyber Strategy & Transformation
Deloitte Singapore
kaisleong@deloitte.com

Eugene Ho Kok Jun
Manager,
Monitor Deloitte
Deloitte Singapore
kokho@deloitte.com

Mah Kar Lyn
Consultant,
Monitor Deloitte
Deloitte Singapore
kmah@deloitte.com

Monitor
Deloitte.

Deloitte.