

# Cybersecurity – Solutions and Services

A research report comparing provider and software vendor strengths, challenges and competitive differentiators

Customized report courtesy of:



Executive Summary 03

Provider Positioning 06

## Introduction

Definition 14

Scope of Report 15

Provider Classifications 15

## Appendix

Methodology & Team 54

Author & Editor Biographies 55

About Our Company & Research 57

## Identity and Access Management (IAM) 17 - 21

Who Should Read This 18

Quadrant 19

Definition & Eligibility Criteria 20

Observations 21

## Data Leakage/Loss Prevention (DLP) and Data Security 22 - 26

Who Should Read This 23

Quadrant 24

Definition & Eligibility Criteria 25

Observations 26

## Advanced Endpoint Threat Protection, Detection, and Response (Advanced ETPDR) 27 - 31

Who Should Read This 28

Quadrant 29

Definition & Eligibility Criteria 30

Observations 31

## Technical Security Services 32 - 38

Who Should Read This 33

Quadrant 34

Definition & Eligibility Criteria 35

Observations 36

Provider Profiles 38

## Strategic Security Services 39 - 45

Who Should Read This 40

Quadrant 41

Definition & Eligibility Criteria 42

Observations 43

Provider Profiles 45

## Managed Security Services — Large Accounts 46 - 52

Who Should Read This 47

Quadrant 48

Definition & Eligibility Criteria 49

Observations 50

Provider Profiles 52

Report Author: Craig Baty

### Remote working continues to drive cybersecurity demand

#### The cybersecurity landscape in Australia continues to evolve rapidly.

The growing importance of cybersecurity is changing the way Australian enterprises procure cybersecurity services. Senior management is often being included in the decision-making on cybersecurity products and strategies, and they are expressing interest in understanding all aspects of cyber risks. Heightened awareness of cyberattacks and stricter regulations and legislation are further raising the maturity levels.

**Australian organisations are demanding cybersecurity solutions** that are both simple and flexible. Cybersecurity

providers should look to develop more comprehensive offerings that target an increasingly diverse customer base, while also adapting to their rapidly changing needs.

Digital transformation initiatives that take advantage of cloud technologies and enable remote working are driving demand for more cybersecurity solutions in Australia.

**Technologies that support this increase in remote working** include endpoint protection, secure web gateways, identity and access management (IAM), secure access service edge (SASE), and web application firewalls. Demand in Australia for cloud-based detection and response solutions, such as endpoint detection and response (EDR) and managed detection and response (MDR), is expected to grow considerably.

**Australian organisations are increasingly**

# Australian Security Market will strongly expand



**relying on identity and access management platforms** to streamline processes, reduce costs, maintain high levels of security, and improve customer experiences to drive further growth. Australian enterprises purchasing IAM-related tools should make a balanced decision based on their individual requirements. Factors that need to be rigorously assessed include vendor support, partner networks, and the vendor's product development roadmap. Due to the continued global market drivers of cloud and hybrid IT, digital transformation, and zero-trust security, an IAM platform has become one of the most important technology investments that an organisation will make. These trends have accelerated during the past year or two, as companies of all sizes and industries have had to realign their delivery models to engage with more customers online.

### **Data loss/prevention (DLP) software**

has become a much more mature and important market in Australia, especially since the reinforcement of the Australian Privacy Act in 2018. Stricter privacy regulations, particularly the introduction of the Notifiable Data Breaches (NDB) scheme as part of the new legislation, have elevated data protection measures to much greater prominence. The CIO, CTO, or CISO is typically the decision-maker for purchasing DLP solutions. Many large Australian enterprises have now set up the chief compliance officer position. Organisations procuring DLP solutions should seek local partner choices and assess their implementation capabilities, after-sales support, and licensing models. They should consider data masking, also known as data obfuscation tools, if compliance is a significant concern.

### **The adoption of Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR) solutions**

has risen significantly because an increasing number of Australian employees are working remotely from unsecure networks.

**Technical security services (TSS)** providers in Australia are enhancing their breadth of services, especially around governance, risk, and compliance (GRC). GRC practices, which were once focused solely on business factors, now cover cybersecurity because of the cost implications as well as the impact on the brand value following a data breach or ransomware attack. Thus, Australian enterprises are becoming increasingly aware of the financial and reputational costs of cybercrimes. Since the introduction of stricter privacy laws and the NDB scheme, many organisations have employed a data security officer or compliance officer.

**The managed security services (MSS) market** both in Australia and globally is evolving from security operations centres (SOCs) to complex, AI-powered cyber defence organisations. Many service providers in this space have a strong specialisation. Managed cybersecurity services have become a continuous and essential process for enterprises.

**SSS in Australia** are increasingly being driven by rapid changes in the threat landscape and legislation. These changes include Australia's new privacy laws, heightened awareness of security issues, and the increased hacking activities that accelerated during the COVID-19 pandemic. Many Australian and global organisations in this space are hiring specialists and announcing new service offerings.

**The Australian security market will strongly expand** over the next five years. Cloud security and IAM are predicted



to be the fastest-growing segments of this market. A growing number of new people will be needed to fill the jobs necessary to support the rising demand for cybersecurity services in Australia. In addition, many roles across businesses and governments will have to enhance their cyber awareness and increase their skill levels.

**In addition, artificial intelligence (AI) in cybersecurity is expected to grow exponentially,** driven by Internet of Things (IoT) adoption, cyberthreats, and concerns of data privacy and regulations. Next-generation identity and access management, messaging, and network security will be key areas for enterprise cybersecurity investments in the next two years.

The Australian Government launched its Cyber Security Strategy in 2020 in an effort to protect Australia's critical infrastructure from persistent and

significant cyberthreats. Federal spending on cybersecurity will increase to AUS\$1.66 billion over the decade. The government also has a strong focus on law enforcement and on strengthening Australia's national cybersecurity organisations: the Australian Cyber Security Centre (ACSC) and the Australian Signals Directorate. It will work with large businesses and managed service providers to improve the tools available to ensure that companies have the capacity to combat security threats.

Federal spending on cybersecurity will increase to AUS\$1.66 billion




## Provider Positioning

Page 1 of 8

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Accenture	Not In	Not In	Not In	Leader	Leader	Leader
Akamai	Contender	Not In	Contender	Not In	Not In	Not In
ASG	Not In	Not In	Not In	Not In	Contender	Contender
Atos	Product Challenger	Not In	Not In	Contender	Contender	Contender
Bitdefender	Not In	Not In	Leader	Not In	Not In	Not In
Blackberry (Cylance)	Not In	Not In	Contender	Not In	Not In	Not In
Broadcom	Product Challenger	Leader	Leader	Not In	Not In	Not In
Capgemini	Not In	Not In	Not In	Leader	Product Challenger	Product Challenger
CGI	Not In	Not In	Not In	Product Challenger	Product Challenger	Leader
Check Point	Contender	Rising Star ★	Product Challenger	Not In	Not In	Not In



 Provider Positioning

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Cisco	Not In	Not In	Contender	Not In	Not In	Not In
CrowdStrike	Not In	Not In	Leader	Not In	Not In	Not In
CTM	Not In	Not In	Not In	Contender	Not In	Product Challenger
CyberArk	Leader	Not In	Not In	Not In	Not In	Not In
CyberCX	Not In	Not In	Not In	Leader	Leader	Leader
CyberProof	Not In	Not In	Not In	Not In	Product Challenger	Contender
Cybereason	Not In	Not In	Contender	Not In	Not In	Not In
Darktrace	Not In	Not In	Product Challenger	Not In	Not In	Not In
Data#3	Not In	Not In	Not In	Contender	Contender	Not In
Datacom	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger




## Provider Positioning

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Deloitte	Not In	Not In	Not In	Leader	Leader	Leader
DriveLock	Not In	Product Challenger	Not In	Not In	Not In	Not In
DXC Technology	Not In	Not In	Not In	Leader	Leader	Leader
Empired	Not In	Not In	Not In	Contender	Not In	Not In
EY	Not In	Not In	Not In	Product Challenger	Leader	Not In
Forcepoint	Not In	Leader	Not In	Not In	Not In	Not In
ForgeRock	Product Challenger	Not In	Not In	Not In	Not In	Not In
Fortinet	Product Challenger	Contender	Not In	Not In	Not In	Not In
F-Secure	Not In	Contender	Not In	Not In	Not In	Not In
Fujitsu	Not In	Not In	Not In	Leader	Leader	Leader






 Provider Positioning


	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Google	Not In	Contender	Not In	Not In	Not In	Not In
Happiest Minds	Not In	Not In	Not In	Not In	Not In	Contender
HCL	Not In	Not In	Not In	Rising Star ★	Product Challenger	Rising Star ★
HelpSystems	Not In	Contender	Not In	Not In	Not In	Not In
IBM	Leader	Leader	Product Challenger	Leader	Leader	Leader
Infosys	Not In	Not In	Not In	Leader	Contender	Product Challenger
Kasada	Not In	Leader	Leader	Not In	Not In	Not In
Kaspersky	Not In	Not In	Product Challenger	Not In	Not In	Not In
KPMG	Not In	Not In	Not In	Not In	Leader	Not In
LastPass	Rising Star ★	Not In	Not In	Not In	Not In	Not In



 Provider Positioning

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
LTI	Not In	Not In	Not In	Not In	Not In	Contender
Macquarie Telecom Group	Not In	Not In	Not In	Product Challenger	Rising Star ★	Product Challenger
Micro Focus	Product Challenger	Not In	Not In	Not In	Not In	Not In
Microland	Product Challenger	Not In	Not In	Not In	Not In	Not In
Microsoft	Leader	Leader	Leader	Not In	Not In	Not In
Netskope	Not In	Product Challenger	Rising Star ★	Not In	Not In	Not In
NTT	Not In	Not In	Not In	Leader	Leader	Leader
Okta	Leader	Not In	Not In	Not In	Not In	Not In
One Identity (OneLogin)	Product Challenger	Not In	Not In	Not In	Not In	Not In
OpenText	Not In	Contender	Not In	Not In	Not In	Not In



 Provider Positioning


	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Oracle	Market Challenger	Not In	Not In	Not In	Not In	Not In
Palo Alto Networks	Not In	Contender	Contender	Not In	Not In	Not In
Ping Identity	Leader	Not In	Not In	Not In	Not In	Not In
Proficio	Not In	Not In	Not In	Contender	Not In	Not In
Proofpoint	Not In	Market Challenger	Not In	Not In	Not In	Not In
PwC	Not In	Not In	Not In	Product Challenger	Leader	Not In
Rapid7	Contender	Not In	Product Challenger	Not In	Not In	Not In
RSA	Leader	Not In	Not In	Not In	Not In	Not In
SailPoint	Leader	Not In	Not In	Not In	Not In	Not In
Secureworks	Not In	Not In	Not In	Not In	Product Challenger	Contender



## Provider Positioning

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Sekuro	Not In	Not In	Not In	Contender	Not In	Not In
SentinelOne	Not In	Not In	Contender	Not In	Not In	Not In
Solarwinds	Contender	Not In	Not In	Not In	Not In	Not In
Sophos	Not In	Not In	Contender	Not In	Not In	Not In
TCS	Not In	Not In	Not In	Contender	Contender	Contender
Tech Mahindra	Not In	Not In	Not In	Leader	Contender	Product Challenger
Telstra	Not In	Not In	Not In	Leader	Leader	Leader
Tesserent	Not In	Not In	Not In	Leader	Leader	Leader
Thales	Product Challenger	Not In	Not In	Not In	Not In	Not In
Trellix	Not In	Leader	Product Challenger	Not In	Not In	Not In



 Provider Positioning

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Trend Micro	Not In	Market Challenger	Product Challenger	Not In	Not In	Not In
Trustwave	Not In	Product Challenger	Not In	Contender	Product Challenger	Product Challenger
Unisys	Market Challenger	Not In	Not In	Market Challenger	Market Challenger	Leader
Varonis	Not In	Product Challenger	Not In	Not In	Not In	Not In
Vectra	Not In	Not In	Not In	Product Challenger	Contender	Product Challenger
Verizon	Not In	Not In	Not In	Leader	Leader	Leader
VMWare Carbon Black	Not In	Leader	Leader	Not In	Not In	Not In
WatchGuard	Not In	Not In	Contender	Not In	Not In	Not In
Wipro	Not In	Not In	Not In	Leader	Leader	Leader
Zscaler	Not In	Product Challenger	Not In	Not In	Not In	Not In



This report compares cybersecurity solutions and services in Australia.

Simplified Illustration Source: ISG 2022



### Definition

This report compares cybersecurity solutions and services in Australia.

- Identity and Access Management (IAM)
- Data Leakage/Loss Prevention (DLP) and Data Security
- Advanced Endpoint Threat Protection, Detection, and Response (Advanced ETPDR)
- Technical Security Services (TSS)
- Strategic Security Services (SSS)
- Managed Security Services (MSS)

Enterprises are adopting emerging technologies to embark on their digital transformation journey to stay competitive. The growing adoption of

these technologies, along with new tools to deliver efficiency and speed, has led to an increase in threat attack surface.

With the ever-changing threat landscape and stringent regional regulations and compliances, enterprises need to take a detailed and inclusive approach to cybersecurity. They can help safeguard their businesses by implementing a mix of security products and services across areas to achieve a robust, secure framework to reduce risk exposure.

Yet deploying adequate security tools does not mean that an enterprise will be immune to vulnerabilities. The human factor remains the weakest link in the security wall.



### Scope of the Report

In this ISG Provider Lens™ quadrant study, ISG includes the following six quadrants: Identity and Access Management (IAM), Data Leakage/Loss Prevention (DLP) and Data Security, Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR), Technical Security Services (TSS), Strategic Security Services (SSS) and Managed Security Services (MSS).

The ISG Provider Lens™ Cybersecurity – Solutions and Services 2022 study aims to support ICT decision-makers in making the best use of their tight security budgets by offering the following:

- Transparency on the strengths and cautions of relevant providers
- A differentiated positioning of providers by market segments

- A perspective on local markets

For IT providers and vendors, this study serves as an important decision-making basis for positioning, key relationships and go-to-market (GTM) considerations. ISG advisors and enterprise clients leverage the information from ISG Provider Lens™ reports while identifying and evaluating their current vendor relationships and potential engagements.

### Provider Classifications

The provider position reflects the suitability of IT providers for a defined market segment (quadrant). Without further additions, the position always applies to all company sizes and industries. In case the IT service requirements from enterprise customers differ and the spectrum of IT providers operating in the local market is sufficiently wide, a further differentiation of the IT providers by performance is made

according to the target group for products and services. In doing so, ISG either considers the industry requirements or the number of employees, as well as the corporate structures of customers and positions IT providers according to their focus area. As a result, ISG differentiates them, if necessary, into two client target groups that are defined as follows:

- **Midmarket:** Companies with 100 to 4,999 employees or revenues between US\$20 million and US\$999 million with central headquarters in the respective country, usually privately owned.
- **Large Accounts:** Multinational companies with more than 5,000 employees or revenue above US\$1 billion, with activities worldwide and globally distributed decision-making structures.

The above segmentation was not applied for the Australian market due to its relatively smaller scale compared to other global markets.

The ISG Provider Lens™ quadrants are created using an evaluation matrix containing four segments (Leader, Product Challenger, Market Challenger and Contender), and the providers are positioned accordingly. Each ISG Provider Lens quadrant may include a service provider that ISG believes has strong potential to move into the Leader quadrant. This type of provider can be classified as a Rising Star.

**Number of providers in each quadrant:** ISG rates and positions the most relevant providers according to the scope of the report for each quadrant and limits the maximum of providers per quadrant to 25 (although exceptions are possible).

*(Continues on next page)*





### Provider Classifications: Quadrant Key

**Product Challengers** offer a product and service portfolio that reflect excellent service and technology stacks. These providers and vendors deliver an unmatched broad and deep range of capabilities. They show evidence of investing to enhance their market presence and competitive strengths.

**Contenders** offer services and products meeting the evaluation criteria that qualifies them to be included in the IPL quadrant. These promising service providers or vendors show evidence of rapidly investing in products/services and a follow sensible market approach with a goal of becoming a Product or Market Challenger within 12 to 18 months.

**Leaders** have a comprehensive product and service offering, a strong market presence and established competitive position. The product portfolios and competitive strategies of Leaders are strongly positioned to win business in the markets covered by the study. The Leaders also represent innovative strength and competitive stability.

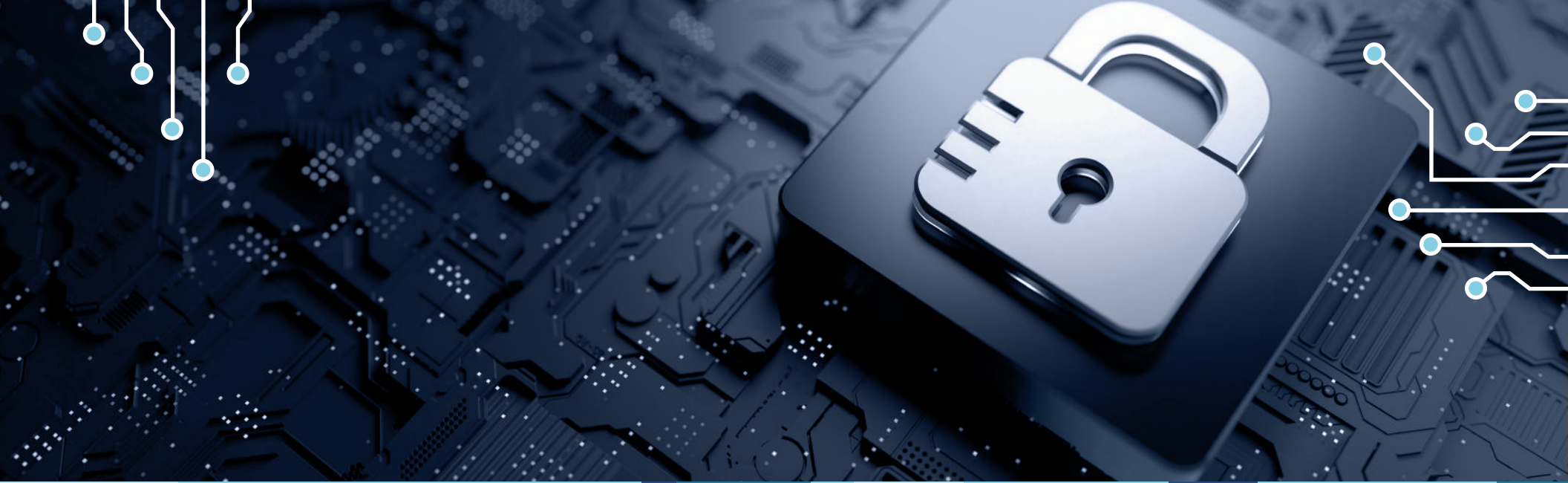
**Market Challengers** have a strong presence in the market and offer a significant edge over other vendors and providers based on competitive strength. Often, Market Challengers are the established and well-known vendors in the regions or vertical markets covered in the study.

★ **Rising Stars** have promising portfolios or the market experience to become a Leader, including the required roadmap and adequate focus on key market trends and customer requirements. Rising Stars also have excellent management and understanding of the local market in the studied region. These vendors and service providers give evidence of significant progress toward their goals in the last 12 months. ISG expects Rising Stars to reach the Leader quadrant within the next 12 to 24 months if they continue their delivery of above-average market impact and strength of innovation.

**Not in** means the service provider or vendor was not included in this quadrant. Among the possible reasons for this designation: ISG could not obtain enough information to position the company; the company does not provide the relevant service or solution as defined for each quadrant of a study; or the company did not meet the eligibility criteria for the study quadrant. Omission from the quadrant does not imply that the service provider or vendor does not offer or plan to offer this service or solution.







# Identity and Access Management (IAM)

## Identity and Access Management (IAM)

### Who Should Read This

This report is relevant to enterprises across industries in Australia for evaluating providers offering solutions that integrate multiple features, addressing the security concerns arising from changes in work patterns and increased digitalisation.

In this quadrant report, ISG highlights the current market positioning of identity and access management (IAM) solution providers that help mitigate security threats for enterprises in Australia, and how each provider addresses the key challenges.

IAM platform investments continue to grow in tandem with the trend of cloud adoption and hybrid digital transformation. Security service providers are offering IAM solutions with a combination of single –

sign-on (SSO), multifactor authentication (MFA) and risk-based and context-based models.

Australia-based enterprises are procuring IAM solutions capable of role-based access and privileged access management (PAM), and able to support one or more legacy and new IAM standards. While considering IAM tools either as a pay-as-you-go (PAYG) model or as IAM as a service, Australian enterprises need to consider their unique business requirements and how IAM can be leveraged to drive growth, streamline processes, reduce costs and maintain high levels of security.



**Chief information security officers** should read this report to understand how IAM solution providers address the significant challenges of compliance and security, while maintaining seamless experience for enterprise clients.



**Chief strategy officers** should read this report to understand the vast potential of solution providers to differentiate themselves by better meeting evolving customer demands.



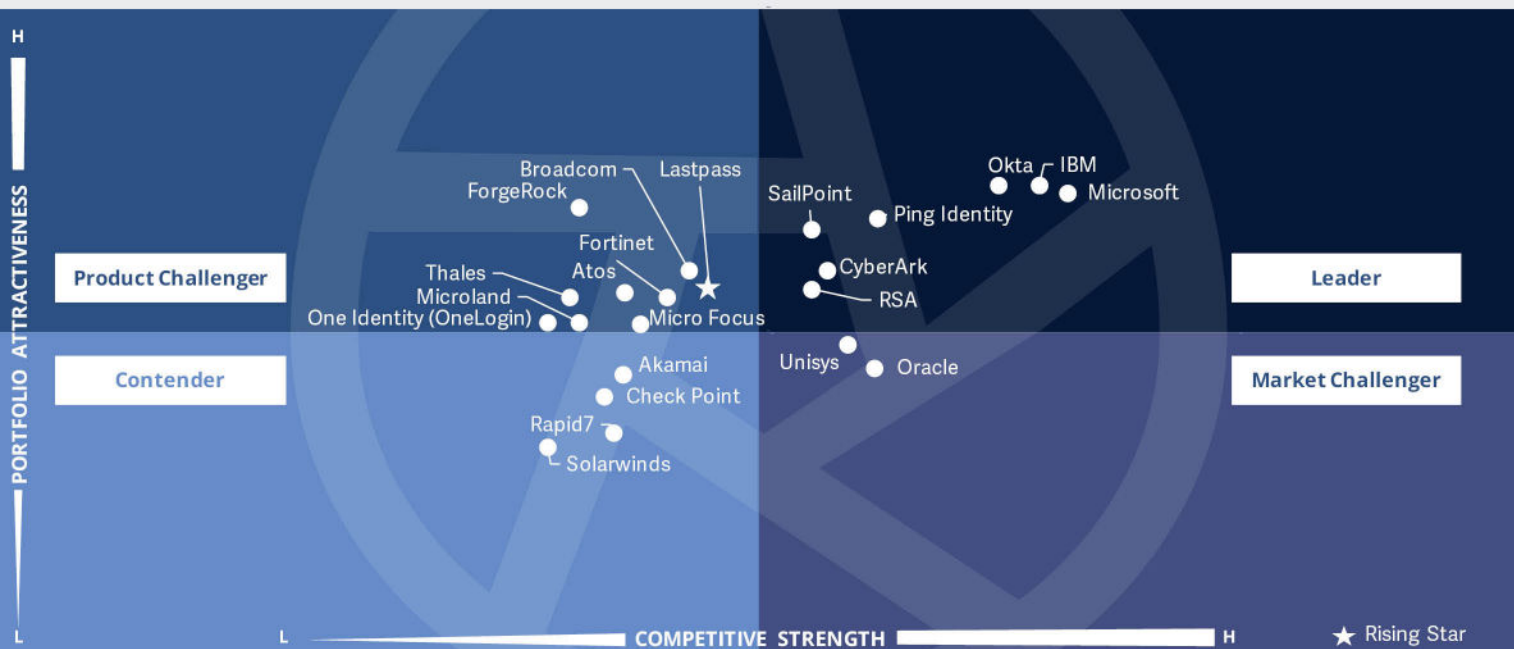
**Chief data officers and data privacy officers** should read this report to understand how a provider offers information protection and privacy, information governance, data quality and data lifecycle management.



**ISG** Provider Lens™  
 Cybersecurity - Solutions and Services  
 Identity and Access Management (IAM)

Source: ISG RESEARCH

Australia 2022



This quadrant assesses IAM software providers that are characterised by their **ability to offer proprietary software** and associated services for securely **managing enterprise user identities** and devices.

Craig Baty



## Identity and Access Management (IAM)

### Definition

IAM vendors and solution providers are characterised by their ability to offer proprietary software and associated services for securely managing enterprise user identities and devices. This quadrant also includes software as a service (SaaS) based on proprietary software.

**Pure service providers that do not offer an IAM product (on-premises or in the cloud) based on proprietary software are not included here.** Depending on organisational requirements, these solutions could be deployed in several ways such as on-premises, in the cloud (managed by the customer), in an as-a-service model or a combination thereof.

### Eligibility Criteria

1. The solution should be **capable of being deployed** in combination with an **on-premises, cloud, identity as a service (IDaaS)**, and managed third-party model.
2. The solution should be **capable of supporting authentication** by a combination of single sign-on (SSO), multifactor authentication, risk-based, and context-based models.
3. The solution should be capable of **supporting role-based access** and PAM.
4. The IAM vendor should be able to provide **access management for one or more enterprise needs** such as cloud, endpoint, mobile devices, application programming interfaces (APIs) and web applications.
5. The solution should be capable of **supporting one or more legacy and newer IAM standards**, including, but not limited to, SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust, and SCIM.
6. To support via secure access methods, the portfolio **should offer one or more of the following**: directory solutions, dashboard or self-service management, and lifecycle management (migration, sync and replication).



## Identity and Access Management (IAM)

### Observations

Cloud-based services are breaking down the traditional enterprise defence perimeter and posing new risks, which is causing many organisations to rethink traditional approaches to managing digital identities. Cyber-resilient enterprises need to govern access to critical data and gain control of digital identity management across customers, employees, partners and devices. However, they need to do this while delivering personalised, engaging, and secure customer experiences. Organisations are increasingly relying on IAM platforms to streamline processes, reduce costs, maintain high levels of security, and improve customer experiences to drive further growth. Australian enterprises purchasing IAM-related tools should make a balanced decision based on their individual requirements. Factors that

need to be rigorously assessed include vendor support, partner networks and the vendor's product development roadmap.

From the 167 companies assessed for this study, 25 have qualified for this quadrant, with seven being Leaders and 1 Rising Star.

### CyberArk

**CyberArk** is a cybersecurity provider and a global leader in privileged access management (PAM). It is rapidly expanding in Australia in the small and midsize enterprises market and has an office in Sydney.

### IBM

**IBM** offers cybersecurity solutions to customers in over 130 countries. It has 5,000 employees in Australia, with offices in every state and territory. Data, AI, cloud, analytics, and cybersecurity now represent more than half of IBM's revenue.

### Microsoft

**Microsoft** is one of the world's leading software companies, with 181,000 employees in 150 offices across over 90 countries. Microsoft has comprehensive IAM functionality and an expanding product suite expansion in Australia.

### Okta

**Okta** is a global specialist in IAM services, through its Okta Identity Cloud, and has a fast-growing presence in Australia. It services more than 15,000 organisations across a broad range of industries.

### Ping Identity

**Ping Identity** is an IAM provider, headquartered in Denver, U.S., that has been in operation for two decades and has a growing presence in Australia. Its investment in identity standards enables it to create innovative product features.

### RSA

**RSA** is a global cybersecurity specialist with headquarters in Bedford, U.S. Its services include implementation and optimisation, incident response, and cyber defence. It has robust technology supporting the identity needs of Australian organisations of all sizes.

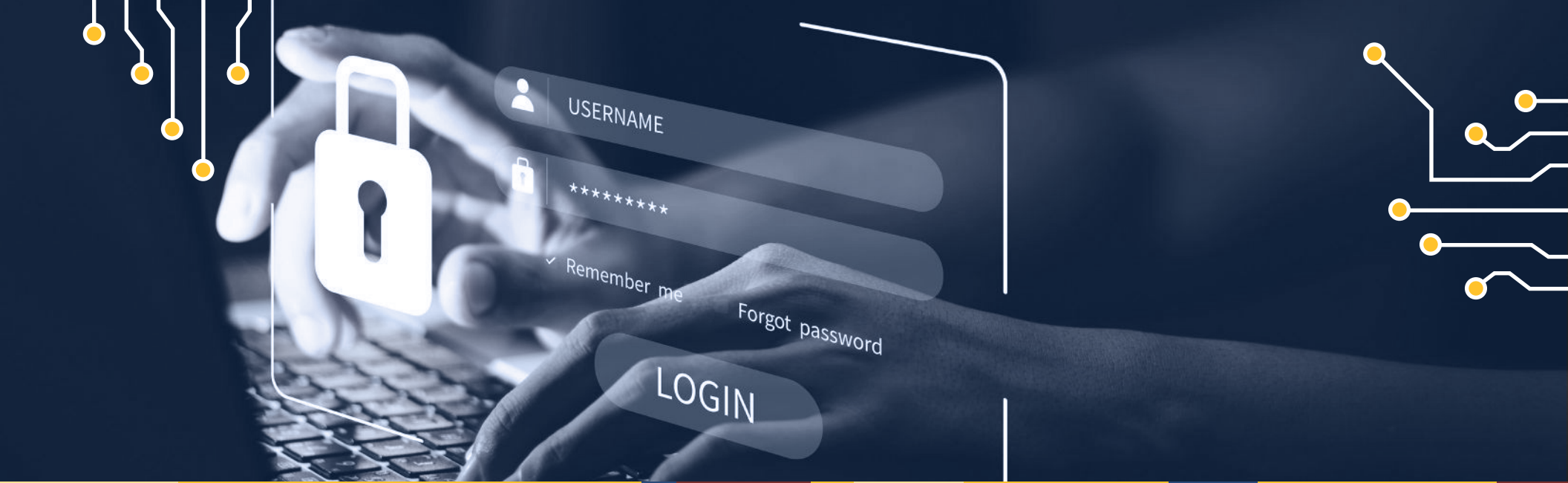
### SailPoint

**SailPoint** is an enterprise IAM specialist provider with 1,500 employees globally. SailPoint has a small but growing presence in Australia, supported by an expanding base of resellers and channel partners.

### LastPass

**LastPass** provides password and identity management solutions and is headquartered in Boston, U.S. Until recently, LastPass was part of GoTo (which includes LogMeIn), and recently, it separated from the parent organisation.





# Data Leakage/Loss Prevention (DLP) and Data Security

### Who Should Read This

This report is relevant to enterprises across industries in Australia for evaluating providers offering solutions that integrate multiple features addressing security concerns arising from changes in work patterns and increased digitalisation.

In this quadrant report, ISG highlights the current market positioning of data leakage/loss prevention (DLP) and data security solution providers that help circumvent security threats for enterprises in Australia, and how each provider addresses the key challenges in the region.

DLP solutions are gaining considerable importance in Australia due to the increase of IoT adoption and the movement of a large volume of data between various platforms (cloud, network, storage and endpoint).

Enterprises with more critical data movement procure more complex and expensive DLP solutions, while others with few applications opt for a less sophisticated DLP strategy to protect their data. Besides assessing the level of complexity of DLP solutions that providers offer, enterprises also take into consideration factors such as price, implementation capabilities, after-sales support and licensing models.



**Chief information security officers** should read this report to understand how DLP solution providers address the significant challenges of compliance and security while maintaining a seamless experience for enterprise clients.



**Chief executive officers** should read this report to understand the vast potential of solution providers to differentiate themselves by better meeting evolving customer demands.



**Chief data officers and data privacy officers** should read this report to understand how a provider offers information protection and privacy, information governance, data quality and data lifecycle management.



**ISG** Provider Lens™  
 Cybersecurity - Solutions and Services  
 Data Leakage/Loss Prevention (DLP) and Data Security

Source: ISG RESEARCH

Australia 2022



This quadrant assesses **DLP software providers' offerings** that can identify and monitor sensitive data, provide access for only authorized users, and **prevent data leakage**.

Craig Baty





### Definition

DLP vendors and solution providers are characterised by their ability to offer proprietary software and associated services. This quadrant also includes software as a service, based on proprietary software. Pure service providers that do not offer a DLP product (on-premises or cloud-based) based on proprietary software are not included here. DLP solutions are offerings that can identify and monitor sensitive data, provide access for only authorised users, and prevent data leakage. Vendor solutions in the market are characterised by a mix of products capable of providing visibility and control over sensitive data residing in cloud applications, endpoints, networks, and other devices.

These solutions are gaining considerable importance as it has become increasingly difficult for companies to control data movements and transfers. The number of

devices, including mobile devices, which are being used to store data is growing rapidly in companies. These are mostly equipped with an internet connection and can send and receive data without passing it through a central internet gateway. Data security solutions protect data from unauthorised access, disclosure or theft.

### Eligibility Criteria

1. The DLP offering should be **based on proprietary software** and not on third-party software.
2. The solution should be capable of **supporting DLP across any architecture**, including the cloud, network, storage or endpoint.
3. The solution should be capable of **handling sensitive data protection** across structured or unstructured data, text, or binary data.
4. The solution should be offered **with basic management support** – including, but not limited to, reporting, policy controls, installation and maintenance – and advanced threat detection functionalities.
5. The solution should be able to **identify sensitive data, enforce policies, monitor traffic and improve** data compliance.



### Observations

Some DLP solutions are highly efficient and sophisticated and are designed to support high-volume transactions in enterprises such as large financial institutions. However, these may be too expensive and complex for many more limited applications. The initial factor to consider when procuring DLP products and services is the frequency of changes in critical data held by an organisation. If this data changes often or is very fluid, more stringent measures are required.

From the 167 companies assessed for this study, 21 have qualified for this quadrant, with seven being Leaders and one Rising Star.

### Broadcom

**Broadcom** is a U.S. provider of semiconductor and infrastructure software products, including a broad range of cybersecurity software solutions that it offers to Australian clients.

### Forcepoint

**Forcepoint** is a global security solutions vendor that has been in operation for 28 years. It has over 2,700 employees and 14,000 clients across 150 countries. Forcepoint has strengthened its channel, strategy and leadership, and sales teams across Australia.

### IBM

**IBM** offers cybersecurity solutions to customers in over 130 countries. It has 5,000 employees in Australia, with offices in every state and territory. IBM recently

expanded its security services through the acquisition of over 20 security vendors.

### Kasada

**Kasada**, an Australian cybersecurity company founded in 2015, is based in New York and Sydney, with offices in Melbourne, San Francisco, and London. Kasada has regional expansion plans, supported by strong investment backing.

### Microsoft

**Microsoft** is one of the world's leading software companies, with over 181,000 employees in 150 offices across over 90 countries. Microsoft continues to invest in developing cutting-edge information DLP protection solutions.

### Trellix

**Trellix** was formed from the merger of McAfee Enterprise and FireEye in 2022. The company has an extensive partner ecosystem, over 40,000 business and government customers, and a growing presence in Australia.

### VMware

**VMware Carbon Black**, a global cybersecurity company, develops cloud-native endpoint security software. Carbon Black pioneered endpoint security categories, including endpoint detection and response.

### Check Point

**Check Point** is headquartered in Israel and has a fast-growing presence in Australia. It offers a highly comprehensive endpoint solution and advanced DLP functionality.





# Advanced Endpoint Threat Protection, Detection, and Response (Advanced ETPDR)

## Advanced Endpoint Threat Protection, Detection, and Response (Advanced ETPDR)

### Who Should Read This

This report is relevant to enterprises across industries in Australia for evaluating providers offering solutions that integrate multiple features, addressing security concerns arising from changes in work patterns and increased digitalisation.

In this quadrant, ISG focuses on the current market positioning of providers of advanced endpoint threat products to enterprises in Australia, and how each provider addresses the key challenges faced in the region.

The increasingly distributed work environment in Australia has expanded the threat surface. In addition, some enterprises are still operating with a combination of legacy technology, Internet-facing endpoints and services and technical complexity, and data security challenges are inevitable.

Many enterprises that are already using endpoint protection solutions are deploying or in the process of procuring advanced ETPDR solutions as a protection against complex data security threats.



#### **Chief information security officers**

should read this report because it presents a broad view of the latest trends in the security landscape. Also, it provides a comprehensive understanding of immediate threats and the security capabilities needed to combat them, and it assists in taking strategic business decisions to address existing security concerns. This report also provides valuable insights on enhancing productivity and reducing complexity in enterprise security



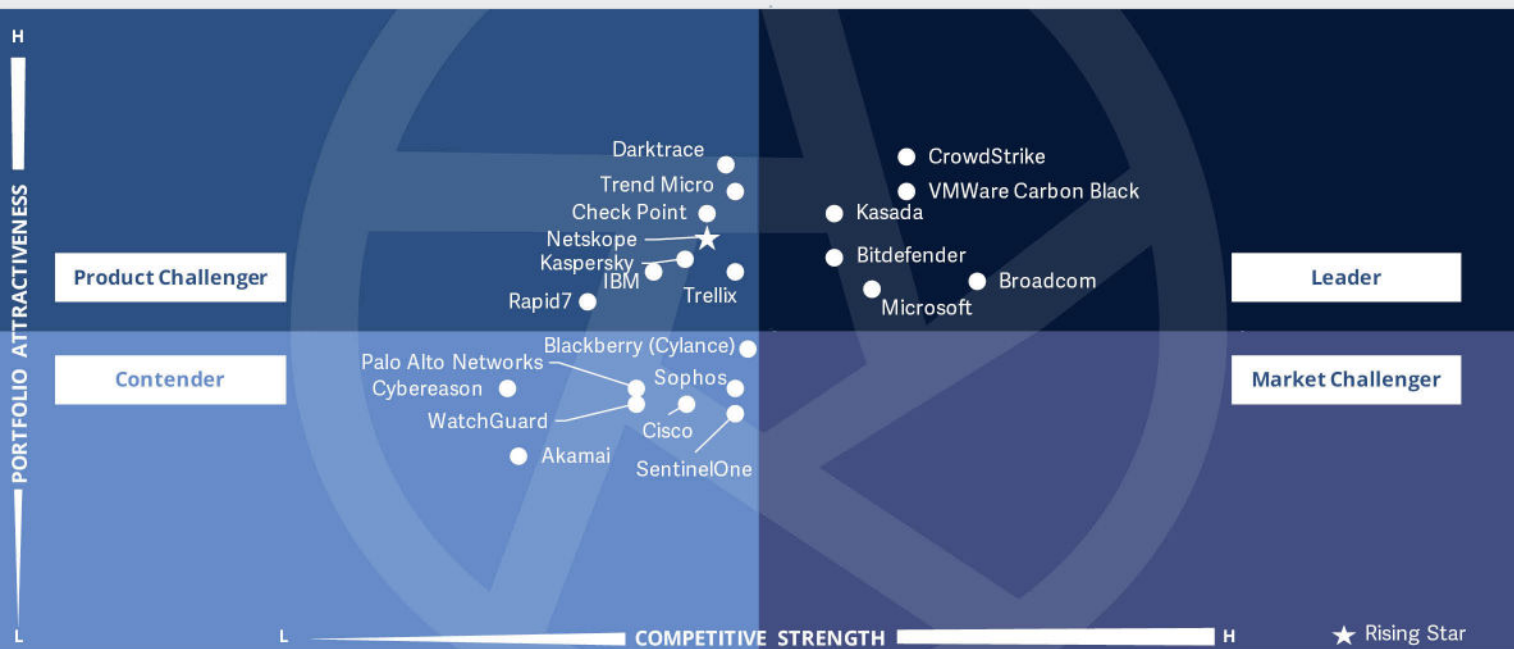
**Chief technology officers** should read this report because it provides the latest trends for CTOs to stay apace with the changing security landscape. In addition to setting

strategic objectives and adopting security platforms in accordance with marketing needs, CTOs can improve competitive advantages to attract more employee prospects.



**Chief strategy officers** should read this report because it examines the relative positioning and capabilities of advanced endpoint solution providers in Australia. This report is relevant to enterprises across all industries in Australia for evaluating solutions that integrate multiple cybersecurity features addressing security concerns caused by changes in work patterns and increased digitalisation.





This quadrant assesses the **providers of advanced endpoint threat** protection, detection, and response software that can provide **continuous monitoring** and total visibility of all endpoints and also analyse, prevent, and respond to advanced threats.

Craig Baty



## Advanced Endpoint Threat Protection, Detection, and Response (Advanced ETPDR)

### Definition

Advanced ETPDR vendors and solution providers are characterised by their ability to offer proprietary software and associated services. This quadrant also includes software as a service, based on proprietary software. Pure service providers that do not offer an Advanced ETPDR product (on-premises or cloud-based) based on proprietary software are not included here. This quadrant evaluates providers offering products that can provide continuous monitoring and complete visibility of all endpoints and can analyse, prevent, and respond to advanced threats. Endpoint security solutions that integrate secure access service edge (SASE) are also included here. In our consideration, endpoint security also includes the corresponding protection of operational technology (OT) solutions.

These solutions go beyond plain, signature-based protection and encompass protection from risks such as ransomware, advanced persistent threats (APTs), and malware by investigating the incidents across the complete endpoint landscape. The solution should be able to isolate the compromised endpoint and take the necessary corrective action or remediation. Such solutions make up a database, wherein the information collected from a network and endpoints is aggregated, analysed, and investigated, and the agent that resides in the host system offers the monitoring and reporting capabilities for the events.

### Eligibility Criteria

1. The solution provides **comprehensive coverage and visibility of all endpoints** in a network.
2. The solution demonstrates effectiveness in **blocking sophisticated threats** such as advanced persistent threats, ransomware and malware.
3. The solution leverages threat intelligence and analyses and **offers real-time** insights on threats emanating across endpoints.
4. The solution includes automated response features that include, but are not limited to, deleting malicious files, sandboxing, ending suspicious processes, isolating infected endpoints and blocking suspicious accounts.



## Advanced Endpoint Threat Protection, Detection, and Response (Advanced ETPDR)

### Observations

Demand for security solutions and services in this segment is being driven by a rising number of external security threats. In addition, the combination of legacy technology and a significant increase in Internet-related endpoints and services are generating additional technical complexity, often results in configuration errors. Configuration errors caused by humans are now one of the leading causes for breaches.

From the 167 companies assessed for this study, 21 have qualified for this quadrant, with 6 being Leaders and one Rising Star.

### Bitdefender

**Bitdefender** is a global cybersecurity technology company headquartered in Romania. Its Australian office in Melbourne was opened in 2019. Bitdefender continues to grow its presence in Australia through a strong partner network.

### Broadcom

**Broadcom** is a U.S. provider of a wide range of semiconductor and infrastructure software products. It has strong EDR capabilities and functionality.

### CrowdStrike

**CrowdStrike** is a fast-growing cybersecurity specialist that offers cloud workload and endpoint security, as well as threat intelligence services. CrowdStrike is growing steadily in Australia, supported by its expanding channel partner network.

### Kasada

**Kasada**, an Australian cybersecurity company founded in 2015, is based in New York and Sydney, with offices in Melbourne, San Francisco, and London. Kasada has an innovative advanced ETPDR platform and an extensive local partner alliance ecosystem.

### Microsoft

**Microsoft** is one of the world's leading software companies, with 181,000 employees in 150 offices across over 90 countries. Microsoft's Advanced ETPDR offering uses behavioural cyber telemetry and modern workplace functionality.

### VMware Carbon Black

**VMware Carbon Black**, a global cybersecurity company, develops cloud-native endpoint security software. Carbon Black has advanced endpoint functionality with a comprehensive range of features.





# Technical Security Services



### Who Should Read This

This report is designed to help companies across industries in Australia evaluate providers that are not exclusively focused on their respective proprietary products but can implement and integrate other vendors' products or solutions. The report covers integration and implementation of IT security services.

In this quadrant, ISG defines the current market positioning of technical security service providers offering implementation and integration services and highlights how each provider addresses the key challenges in Australia. By leveraging the services offered by providers, organisations can prepare for attacks and respond swiftly to threats perpetrated with the intent of misusing sensitive information.

Government guidelines in Australia have compelled enterprises to comply with certain minimal cybersecurity standards.

Because most of the security implementation bundles comprise proprietary tools, complemented with hardware and software from third-party providers, enterprises should look for a robust TSS vendor that has the capability to provide the necessary integration and timely local support in case of a data breach. The evolving ransomware landscape is also driving enterprises to consider a scalable arrangement with their TSS vendors.



**Chief information security officers** should read this report to find a balance between data security, customer experience and privacy in their pursuit of digital transformation. This report provides a deep insight into these topics and assists in the selections of IT security

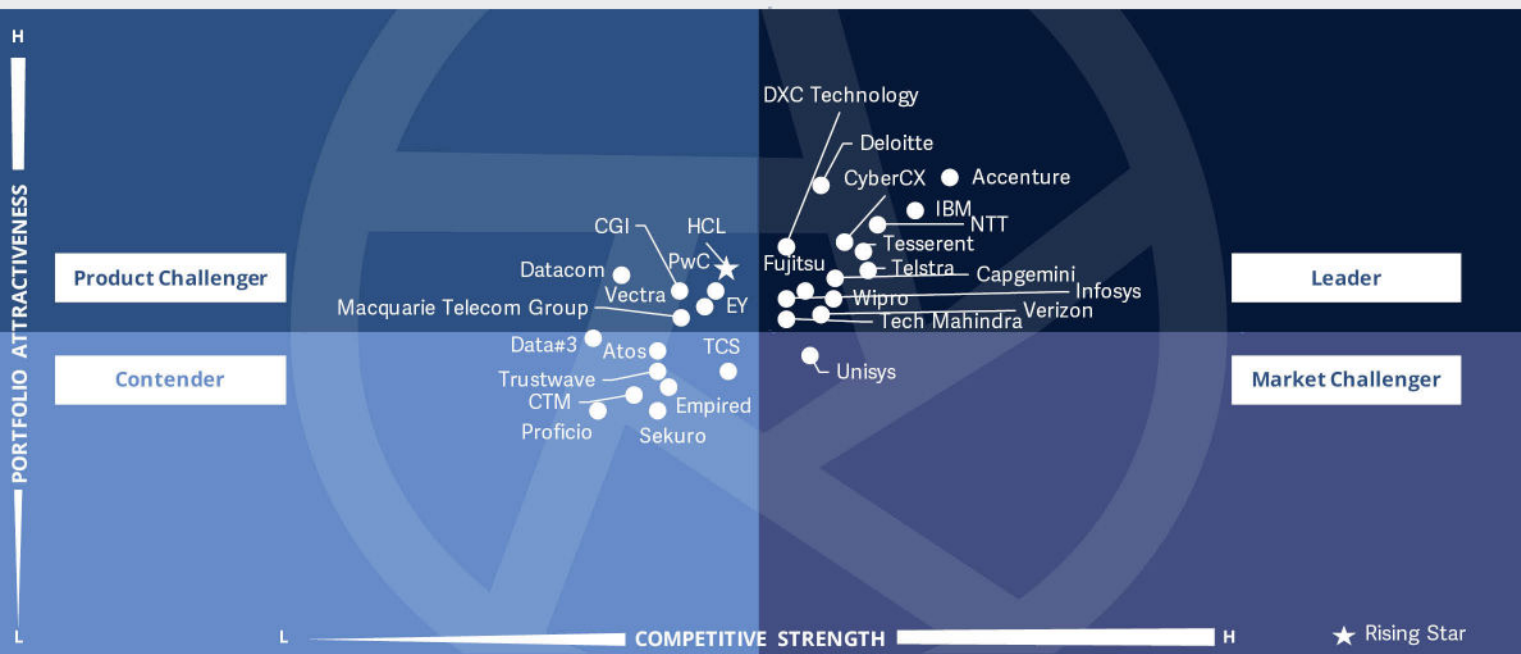


**Chief Strategy Officers** should read this report to understand the relative positioning and capabilities of service providers and collaborate with them to develop an effective cybersecurity service. This report contains information that can be used to implement a security solution.



**Security analysts** should read this report to understand how providers adhere to the security and data protection regulations in Australia to stay apace with market trends and prepare themselves to leverage all available services.





This quadrant assesses the technical security service providers that offer **integration, maintenance, and support services** for IT security products or solutions.

Craig Baty



### Definition

TSS covers integration, maintenance and support for both IT and operational technology (OT) security products or solutions. DevSecOps services are also included here. TSS addresses all security products, including antivirus, cloud and data centre security, IAM, DLP, network security, endpoint security, unified threat management (UTM), OT security, and secure access service edge (SASE). This quadrant examines service providers that do not have an exclusive focus on their respective proprietary products and can implement and integrate other vendor products or solutions.

### Eligibility Criteria

1. Demonstrate experience in **implementing cybersecurity solutions** for companies in the respective country
2. **Authorised by security technology vendors** (hardware and software) to distribute and support security solutions
3. Providers should **employ certified experts** (vendor-sponsored, association- and organisation-led credentials, government agencies) capable of supporting security technologies



## Technical Security Services

### Observations

Cybersecurity software vendors depend on service partners to install, configure, and integrate their solutions. Service partners provide a range of TSS and is often the key party that closes the sale through the vendor's presales team to support product information. Service partners often are key in maintaining client relationships and are considered trusted consultants that are involved in estimating capacity and other system requirements.

The cybersecurity product procurement process should correctly balance and bundle software, hardware, and service partners to ensure the appropriate long-term service support. Many enterprises, and in particular their security solutions, will require immediate support from a robust security partner in case of a data breach or cyberattack.

From the 167 companies assessed for this study, 30 have qualified for this quadrant, with 14 being Leaders and 1 Rising Star.



**Accenture** is one of the world's largest professional service providers, with leading capabilities in digital technologies, cloud, and security. Accenture has a highly innovative and well-developed cybersecurity research and development program.



**Capgemini** is a leading global security service provider headquartered in Paris. It has a significant cybersecurity presence in Australia and a security operations centre (SOC) in Melbourne.



**CyberCX**, an Australian cybersecurity specialist, is one of the leading end-to-end cybersecurity service providers in the Southern Hemisphere. CyberCX has a highly experienced cybersecurity management team.

### Deloitte

**Deloitte** is a major global consultancy that offers a range of technical cybersecurity services. It provides Australian clients with deep cybersecurity expertise for data privacy compliance.

### DXC

**DXC** is a global ICT service provider operating with more than 130,000 people in over 70 countries. The company offers a range of cybersecurity services in Australia delivered via its SOC.

### Fujitsu

**Fujitsu** is a large global IT managed service provider headquartered in Tokyo, Japan, with strong cybersecurity capabilities. Fujitsu offers Australian clients a range of local technical security capabilities.

### IBM

**IBM** delivers cybersecurity solutions to customers in over 130 countries. It has 5,000 employees in Australia, with offices in every state and territory. IBM has made multiple recent acquisitions to enhance its cloud and security portfolio.



**Infosys** is headquartered in Bengaluru, India, and provides business consulting, information technology, and outsourcing services. It has a strong presence in Australia, which is the third-largest market for Infosys globally.



## Technical Security Services

### NTT

**NTT** is a global IT service provider that offers network, infrastructure, security, cloud, and managed solutions to clients throughout Australia. NTT's technical security capabilities complement its existing cybersecurity services portfolio.

### Tech Mahindra

**Tech Mahindra** is a leading technology provider of digital transformation, consulting, and business reengineering services across 90 countries. Tech Mahindra aims to grow its cybersecurity business to over \$500 million within five years.



**Telstra** is Australia's largest telecommunications provider, with headquarters in Melbourne and operations across Southeast Asia. It has a strong consulting-led security services offering and is ramping up its cybersecurity expansion plans.



**Tesserent** provides enterprise-level managed cybersecurity and network services across Australia and Asia-Pacific. It continues to expand its Cyber 360 capabilities and to integrate acquisitions.



**Verizon** is a multinational telecommunications conglomerate with global headquarters in New York and Australian headquarters in Sydney. Verizon's cyber presence in Australia includes two SOCs and a forensic laboratory.



**Wipro** is a leading global IT, consulting, and business process services provider headquartered in Bengaluru, India. Wipro has a strong and growing cybersecurity presence in Australia after its acquisition of Ampion.



**HCL Technologies** is an India-based, multinational IT services and consulting technology company. HCL continues to expand its cybersecurity presence in Australia with major recent client wins.



# CyberCX



“CyberCX has a strong and highly experienced cybersecurity management team.”

*Craig Baty*

## Overview

CyberCX, an Australian cybersecurity specialist with headquarters in Melbourne, is one of the leading end-to-end cybersecurity service providers in the Southern Hemisphere. It was established in 2019 by integrating 14 niche cybersecurity companies based in Australia and New Zealand. CyberCX has a workforce of over 1,000 professionals. Through its TSS, CyberCX acts as an independent cybersecurity partner for clients through a consultative end-to-end approach.

## Strengths

**Comprehensive offerings:** CyberCX’s cybersecurity services include consulting and advisory; governance, risk, and compliance (GRC); incident response; penetration testing and assurance; network and infrastructure solutions; identity and access management and cloud security solutions. It also has the ability to develop bespoke and integration solutions.

**Highly experienced management team:** CyberCX has decades of experience protecting industries and governments in Australia and New Zealand. The management teams from

companies were brought together to form CyberCX, which has many cybersecurity experts with a wealth of experience in government and private enterprises.

**Wide expertise resulting from initial company formation:** The firms that initially formed CyberCX brought extensive expertise across a range of cybersecurity capabilities. This includes consulting and advisory, risk and compliance, security assurance, integration and engineering, training and education, incident response, digital forensics, and MSS.

## Caution

CyberCX is becoming increasingly recognised as a preeminent Australian provider of TSS. However, there is still a perception in some sectors that the level of TSS services is not yet as integrated as it could be.





# Strategic Security Services

### Who Should Read This

This report is relevant to enterprises across industries in Australia for evaluating providers offering services that integrate multiple features that address security concerns arising from changes in work patterns and increased digitalisation.

In this quadrant, ISG focuses on the current market positioning of strategic security service providers that help enterprises mitigate security threats in Australia, and it highlights how each provider addresses the key challenges.

The repercussion of any data breach is too significant for an enterprise to ignore. The strategic security services market is being driven by Australia's privacy laws, high awareness about security issues and increasingly complex ransomware activities.

Enterprises must stay on top of the governance, risk, and compliance (GRC) practices to protect their digital assets and minimise the cost implications of a breach. In this highly regulated environment, consulting firms operating in Australia have built additional expertise to help enterprises with compliance. Most major system and software providers and consultancy firms have established or expanded their cybersecurity practices and are aggressively marketing them to Australia-based enterprises.



#### Chief information security officers

should read this report because it presents a broad view of the latest trends in the security landscape. Also, it provides a comprehensive understanding of immediate threats and the security capabilities needed to combat them, and it assists in making strategic business decisions to address security concerns. This report provides valuable insights on enhancing productivity and reducing complexity in enterprise security operations.



**Chief technology officers** should read this report because it highlights the latest trends for CTOs to stay apace with the changing security landscape. In addition to setting

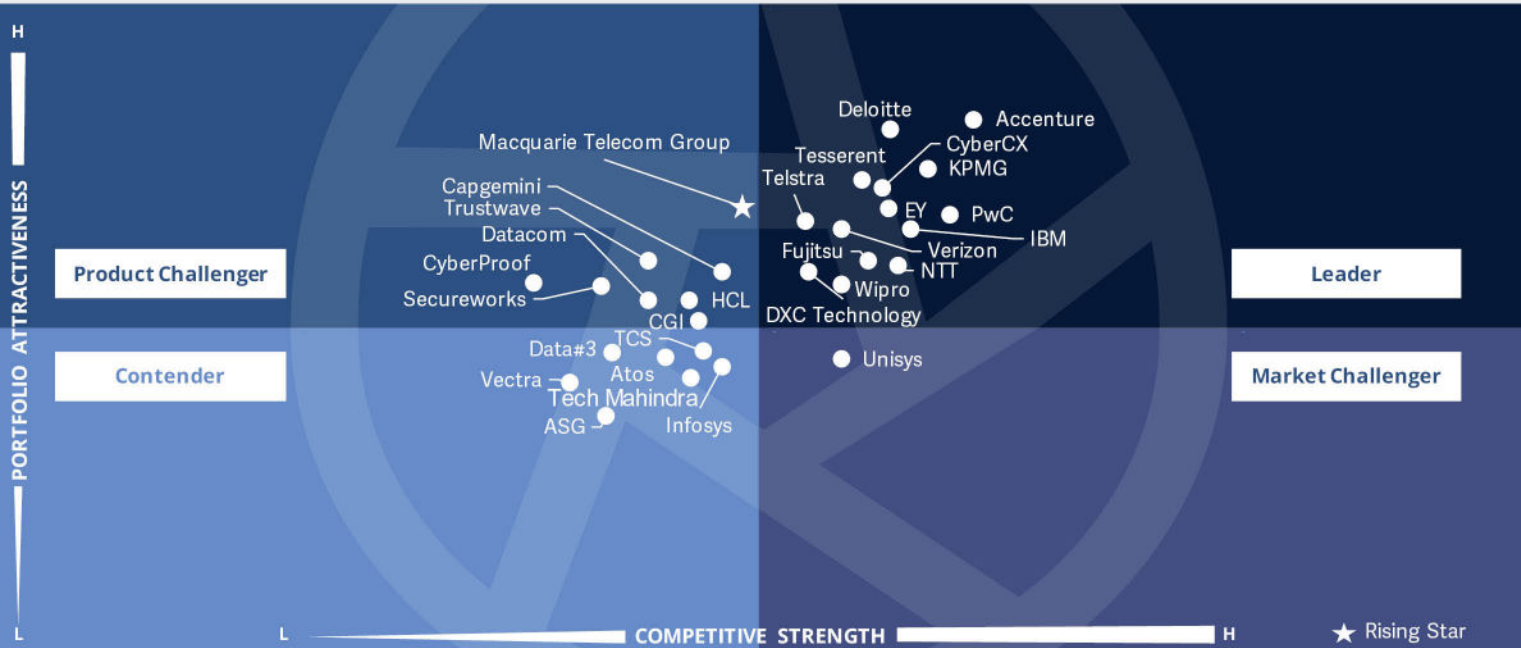
strategic objectives and developing security platforms in accordance with marketing needs, CTOs can improve competitive advantages to attract more employee prospects.



**Chief strategy officers** should read this report because it examines the relative positioning and capabilities of strategic security service providers in the the market. It helps a company set its vision and strategy for security. Additionally, it supports decision-making on collaborations, partnerships and cost-reduction initiatives.







This quadrant assesses the **strategic security service providers** that offer security audits, compliance and risk advisory services, security assessments, security solution architecture consulting, and awareness and training services.

Craig Baty



## Strategic Security Services

### Definition

Strategic security services (SSS) primarily covers consulting for IT and OT security. Services covered in this quadrant include security audits, compliance and risk advisory services, security assessments, security solution architecture consulting, and awareness and training. These services are used to assess security maturity and risk posture and define cybersecurity strategy for enterprises (tailored to specific requirements). This quadrant examines service providers that are not exclusively focused on proprietary products or solutions. The services analysed here cover all security technologies, especially OT security and SASE.

### Eligibility Criteria

1. Service providers should **demonstrate abilities in SSS** areas such as evaluation, assessments, vendor selection, architecture consulting, and risk advisory.
2. Service providers should **offer at least one of the above** SSS in the respective country.
3. Execution of security consulting services using frameworks will be an advantage.
4. **No exclusive focus** on proprietary products or solutions.



## Strategic Security Services

### Observations

The SSS market is being significantly impacted by the COVID-19 pandemic, which has resulted in many security managers (CISOs) reevaluating their capability to tackle future systemic risk events. CISOs are broadening the aperture of external events within a risk management plan. Risk quantification becomes a tool for CISOs to prioritise what to do and where to invest to manage risks and protect the enterprise.

From the 167 companies assessed for this study, 30 have qualified for this quadrant, with 13 being Leaders and 1 Rising Star.



**Accenture** is one of the world's largest professional service providers, with leading capabilities in digital technologies, cloud, and security. Accenture's

cybersecurity capabilities have been strengthened by a number of recent acquisitions.



**CyberCX**, an Australian cybersecurity specialist, is one of the leading end-to-end cybersecurity service providers in the Southern Hemisphere. CyberCX has a large, highly trained, and experienced onshore national team of security testers.

### Deloitte

**Deloitte** is a major global consultancy that provides a range of strategic cybersecurity services. The company offers Australian clients an industry-leading security audit and compliance offering.

### DXC

**DXC** is a global ICT service provider operating with more than 130,000 people in over 70 countries. It offers comprehensive security advisory services and strong risk management capabilities.

### EY

**EY** is a major international consultancy with more than 25 years' experience in cybersecurity. It has a large global cybersecurity practice in Australia and a comprehensive range of cybersecurity services.

### Fujitsu

**Fujitsu** is a large global IT managed service provider headquartered in Tokyo, Japan, with strong cybersecurity capabilities. Fujitsu has an expanding cybersecurity consultancy practice both in Australia and globally.

### IBM

**IBM** offers cybersecurity solutions to customers in over 130 countries. It has 5,000 employees in Australia, with offices in every state and territory. IBM delivers Australian organisations a holistic end-to-end portfolio of SSS.

### KPMG

**KPMG** is a major international consultancy headquartered in Amsterdam. Recent acquisitions have significantly strengthened KPMG's Australian cybersecurity portfolio.

### NTT

**NTT** is a global IT service provider that offers network, infrastructure, security, cloud and managed solutions to clients throughout Australia. NTT has a broad portfolio of cyber services and an advanced compliance assurance security offering.



## Strategic Security Services

### PwC

**PwC** is a global consulting group that delivers audit, assurance, consulting, and tax services. It collaborates with business leaders, governments, and regulators to develop its cyber strategy.



**Telstra** is Australia's largest telecommunications provider, with headquarters in Melbourne and operations across Southeast Asia. Telstra has strong cybersecurity intelligence capabilities and strong cyber thought leadership.



**Tesseract** is the largest cybersecurity company listed on the Australian Securities Exchange and one of the two largest locally based cybersecurity

providers. Tesseract is focusing on capturing market share in government, critical infrastructure, and finance.



**Verizon** is a multinational telecommunications conglomerate with global headquarters in New York and Australian headquarters in Sydney. The company offers Australian clients a broad, advanced range of SSS.



**Wipro** is a leading global IT, consulting, and business process services provider headquartered in Bengaluru, India. It has more than 20 years of consulting and IT transformation experience in Australia.



**Macquarie Telecom Group** is an ASX-listed Australian company that operates across four businesses: Macquarie Telecom, Cloud Services, Government, and Data Centres. It has offices in Sydney, Melbourne, Canberra, Brisbane, and Perth.



# CyberCX



“CyberCX has a large, highly trained, and experienced onshore national team of security testers and strategic consultants.”

*Craig Baty*

## Overview

CyberCX, an Australian cybersecurity specialist with headquarters in Melbourne, is one of the leading end-to-end cybersecurity service providers in the Southern Hemisphere. CyberCX has a workforce of over 1,000 professionals. It was established in 2019 by integrating 14 niche cybersecurity companies based in Australia and New Zealand. As part of its strategic services offering, it has dedicated R&D and capabilities for pioneering tactics, techniques, and practices.

## Strengths

**Broad SSS offering:** Services include cybersecurity strategic policy advice, strategy design, and transformation roadmap. It includes CISO as a service, cyber metrics board reporting, cybersecurity rationalisation, and executive incident response planning and simulations.

**Staff expertise:** CyberCX’s onshore national team of security testers is highly trained and certified. The company has a physical presence in every major state of Australia, and most members of its leadership team have over 25 years of experience in cybersecurity. They actively maintain

a variety of cybersecurity industry certifications, and many have government security clearances.

**Advanced testing process and methodology:** CyberCX leverages advanced testing processes and cybersecurity methodologies that align with best practice approaches and technical standards. It utilises known issues and techniques drawn from its proprietary knowledge base, which is built through a large volume of security testing engagements and research, and collaborative intelligence sharing across business units and its dedicated cyber intelligence team.

## Caution

CyberCX has several large, well-known clients and is very successful with this segment. However, it needs to expand its midmarket client base.





# Managed Security Services

### Who Should Read This

This report is relevant to enterprises across industries in Australia for evaluating providers offering services that integrate multiple features, addressing security concerns arising from changes in work patterns and increased digitalisation.

In this quadrant, ISG focuses on the current market positioning of managed security service providers that help mitigate security threats for enterprises in these regions, and how each provider addresses key challenges.

In the rapidly evolving threat landscape, Australian enterprises are increasingly leveraging managed security services to gain the required expertise and reduce the workload of their in-house security staff. MSS providers are incorporating threat intelligence in the conventional service offerings. Security operations centres are evolving into more complex AI-powered

cyber defence organisations that can offer operational management, vulnerability management, centralised threat advisory services and virtual security operations.



#### **Chief information security officers**

should read this report because it presents a broad view of the latest trends in the security landscape. Also, it provides a comprehensive understanding of immediate threats and the security capabilities needed to combat them, and it assists in making strategic business decisions to address existing security concerns. This report also provides valuable insights on enhancing productivity and reducing complexity in enterprise security operations.



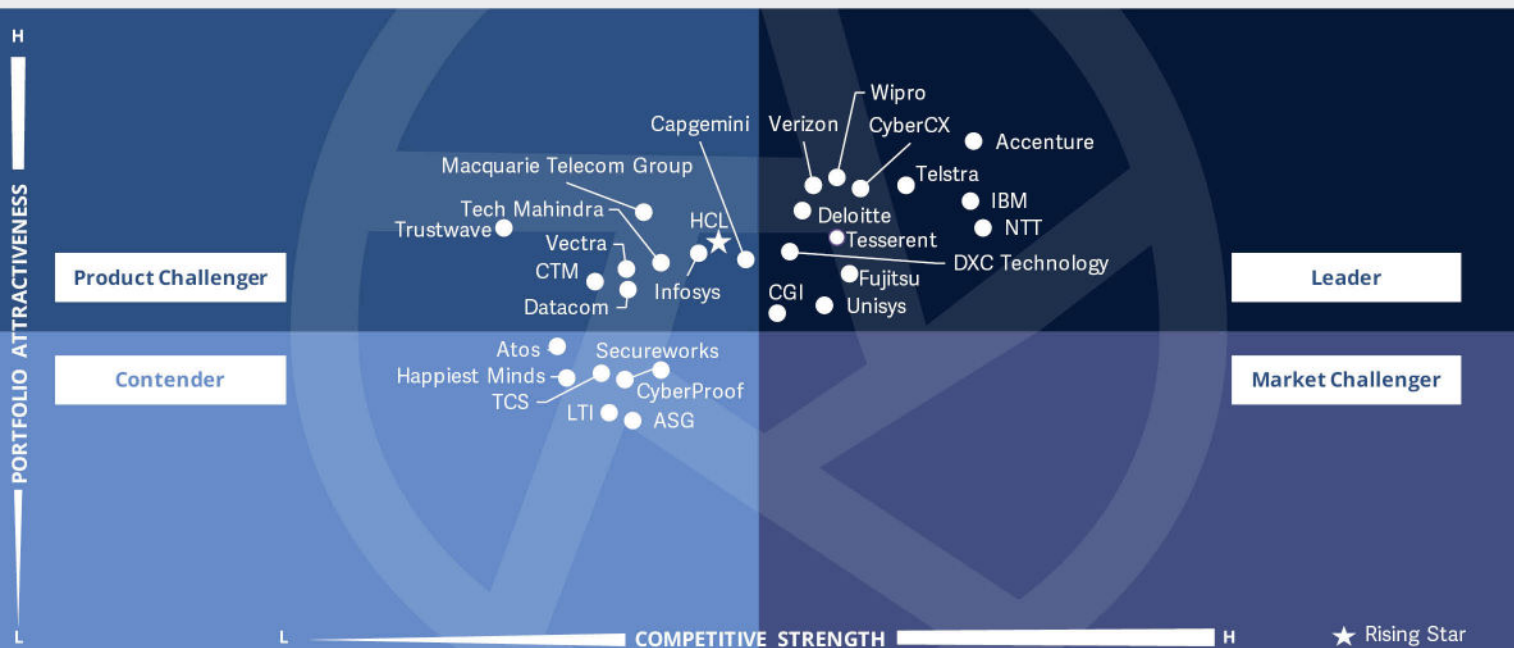
**Chief technology officers** should read this report because it highlights the latest trends for CTOs to stay apace with the changing security



**Chief strategy officers** should read this report because it examines the relative positioning and capabilities of managed security services providers in the market. It helps a company set its vision and strategy for security. Additionally, it supports decision-making on collaborations, partnerships and cost-reduction initiatives.

landscape. In addition to setting strategic objectives and developing security platforms in accordance with marketing needs, CTOs can improve competitive advantages to attract more employee prospects





This quadrant assesses the **managed security service** providers that operate and manage IT security infrastructure for one or several clients through **a security operations centre (SOC)**.

Craig Baty





### Definition

Managed security services comprises the operations and management of IT and OT security infrastructures for one or several customers by a security operations centre (SOC). This quadrant examines service providers that are not exclusively focused on proprietary products but can manage and operate best-of-breed security tools. These service providers can handle the entire security incident lifecycle, from identification to resolution.

### Eligibility Criteria

#### 1. Typical services include

security monitoring, behaviour analysis, unauthorised access detection, advisory on prevention measures, penetration testing, firewall operations, antivirus operations, identity and access management (IAM) operation services, data leakage/loss prevention (DLP) operations, and all other operating services to provide ongoing, real-time protection, without compromising business performance; secure access service edge (SASE) is also included

#### 2. Ability to provide security services

such as detection and prevention; security information and event

management (SIEM); and security advisor and auditing support, remotely or at the client's site

#### 3. Possesses **accreditations from vendors** of security tools

#### 4. **SOCs are ideally owned and managed** by the provider and not predominantly by partners

#### 5. **Maintains certified staff** who are, for example, a Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager (CISM), or who have earned a Global Information Assurance Certification (GIAC)



### Observations

The MSS market both in Australia and globally is evolving from SOCs to complex, AI-powered cyber defence organisations. Many service providers in this space have a strong specialisation. Managed cybersecurity services have become a continuous and essential process for enterprises.

Enterprises are required to adopt more sophisticated tools to defend themselves as cybercriminals around the world are using AI tools to automate threat creation, web scanning, and malware distribution.

New tools have emerged, such as micro-segmentation that can isolate hackers or bots when they break into an enterprise network. XDR platforms use analytics and automation to accelerate and simplify detection and response. Services around governance and data protection help clients audit access, manage the

segregation of duties, and produce evidence of implementing protection measures prior to a data breach, thus helping reduce the consequences and any subsequent penalties. It can sometimes be challenging for Australian midsize enterprises to retain cybersecurity experts. Service providers can tackle this issue by allowing midmarket clients to resource highly skilled practitioners.

From the 167 companies assessed for this study, 29 have qualified for this quadrant, with 13 being Leaders and 1 Rising Star.



**Accenture**, one of the world's largest professional service providers, has leading capabilities in digital technologies, cloud, and security. It has a large cybersecurity practice in most major economies, including Australia, called Accenture Security.

### CGI

**CGI** is one of the largest IT and business consulting services firms in the world. It has been in Australia for over 40 years, with offices in Sydney, Melbourne, Brisbane, and Hobart. CGI is highly active in the cybersecurity industry in Australia.



**CyberCX**, an Australian cybersecurity specialist, is one of the leading end-to-end cybersecurity service providers in the Southern Hemisphere. CyberCX has a workforce of over 1,000 professionals, most of whom are cybersecurity professionals.

### Deloitte

**Deloitte** is a major global consultancy that offers a broad range of managed cybersecurity services. The company has a strong and well-established cybersecurity presence in Australia.

### DXC

**DXC** is a global ICT service provider operating with more than 130,000 people in over 70 countries. It has a strong cyber presence in Australia and a highly comprehensive cyber solution portfolio.

### Fujitsu

**Fujitsu** is a large global IT managed service provider headquartered in Tokyo, with strong cybersecurity capabilities. Fujitsu has highly developed, Australian-based SOC capabilities and strong experience working with the Australian Government.

### IBM

**IBM** offers cybersecurity solutions to customers in over 130 countries. It has 5,000 employees in Australia, with offices in every state and territory. IBM has been one of the leaders in the MSS sector since the early 2000s.



## Managed Security Services

### NTT

**NTT** is a global IT service provider that offers network, infrastructure, security, cloud, and managed solutions to clients throughout Australia. The company continues to expand its presence in Australia with recent growth.



**Telstra** is Australia's largest telecommunications provider, with headquarters in Melbourne and operations across Southeast Asia. Telstra has fully integrated vulnerability management, threat intelligence and detection, and analytics capabilities.



**Tesserent** is the largest cybersecurity company listed on the Australian Securities Exchange and one of the two largest locally based cybersecurity providers. Recent acquisitions have broadened Tesserent's customer base across both enterprises and governments.

### Unisys

**Unisys** is a global systems and services company that has a significant cybersecurity presence in Australia. It generates over 50 percent of its global cybersecurity revenues in the country.



**Verizon** is a multinational telecommunications conglomerate with global headquarters in New York and Australian headquarters in Sydney. Verizon has a highly comprehensive SOC solutions offering.



**Wipro** is a leading global IT, consulting, and business process services provider headquartered in Bengaluru, India. It has a well-developed and expanding cybersecurity presence in Australia.



**HCL** has a strong cybersecurity presence in Australia and is headquartered in Noida, India. HCL has a very large cybersecurity practice with over 25 years' experience, 5,500 certified engineers, and 40 collaborative partners and alliances.



# CyberCX



“CyberCX provides tightly packaged, best-of-breed offerings from leading global security vendors.”

*Craig Baty*

## Overview

CyberCX, an Australian cybersecurity specialist with headquarters in Melbourne, is one of the leading end-to-end cybersecurity service providers in the Southern Hemisphere. It was established in 2019 by integrating 14 niche cybersecurity companies based in Australia and New Zealand. CyberCX has a workforce of over 1,000 professionals, most of whom are cybersecurity professionals. It has offices in Australia and New Zealand, which are being consolidated, and also has a presence in the U.K.

## Strengths

### Industry-leading SOC as a service:

This solution includes management and monitoring security information and event management (SIEM), vulnerability management, and endpoint detection and response. These services are offered fully onshore in Australia or New Zealand. CyberCX also offers these services via 24x7 monitoring services.

### Cyber intelligence-led offering:

CyberCX's dedicated cyber intel team synthesises lessons learned to create unique threat-hunting packages. It has the ability to blend traditional MSS with offerings such as digital forensics;

governance, risk, and compliance; penetration testing; red teaming; and identity and access management.

### Large and experienced cyber team:

CyberCX has over 150 staff employed in its Security Testing and Assurance practice, making its team the largest in the Asia-Pacific region. Recent tests and resulting security recommendations have led to significant security improvements for CyberCX clients across its internal systems, applications, infrastructure, and operations.

## Caution

CyberCX offers managed services to all major states across Australia and New Zealand. However, because this network was created from the combination of different acquisitions, CyberCX should help customers understand exactly what levels of standardisation and integration have been achieved and what the future plans are for their managed services network.





# Appendix

The ISG Provider Lens 2022 – Cybersecurity - Solutions and Services research study analyzes the relevant software vendors/service providers in the Australian market, based on a multi-phased research and analysis process, and positions these providers based on the ISG Research methodology.

**Lead Authors:**

Craig Baty, Phil Harpur

**Editors:**

Jack Kirshbaum, Dona George

**Research Analyst:**

Angie Kho

**Data Analyst:**

Rajesh Chillappagari

**Consultant Advisor:**

Anand Balasubramaniam

**Project Manager:**

Ridam Bhattacharjee

Information Services Group Inc. is solely responsible for the content of this report. Unless otherwise cited, all content, including illustrations, research, conclusions, assertions and positions contained in this report were developed by, and are the sole property of Information Services Group Inc.

The research and analysis presented in this report includes research from the ISG Provider Lens program, ongoing ISG Research programs, interviews with ISG advisors, briefings with services providers and analysis of publicly available market information from multiple sources. The data collected for this report represents information that ISG believes to be current as of June 2022, for providers who actively participated as well as for providers who did not. ISG recognizes that many mergers and acquisitions have taken place since that time, but those changes are not reflected in this report.

All revenue references are in U.S. dollars (\$US) unless noted.

The study was divided into the following steps:

1. Definition of Cybersecurity – Solutions and Services market
2. Use of questionnaire-based surveys of service providers/ vendor across all trend topics
3. Interactive discussions with service providers/vendors on capabilities & use cases
4. Leverage ISG's internal databases & advisor knowledge & experience (wherever applicable)
5. Use of Star of Excellence CX-Data
6. Detailed analysis & evaluation of services & service documentation based on the facts & figures received from providers & other sources.
7. Use of the following key evaluation criteria:
  - \* Strategy & vision
  - \* Tech Innovation
  - \* Brand awareness and presence in the market
  - \* Sales and partner landscape
  - \* Breadth and depth of portfolio of services offered
  - \* CX and Recommendation



## Author & Editor Biographies

Author



**Craig Baty**  
**Lead Analyst**

Craig Baty has extensive research and thought leadership experience across the Asia Pacific and Japanese ICT markets. Craig is principal of DataDriven, an Asia Pacific-based research and advisory firm that is an ISG Research partner. Craig has over 30 years of executive and board-level experience in the industry, including as group vice president and head of Gartner Research Asia Pacific and Japan; CEO of Gartner Japan; global vice president of Frost & Sullivan; executive general manager for marketing and CTO of Fujitsu Australia New Zealand & Asia; and general manager for marketing, strategy and alliances at BT Syntegra. More recently he was vice

president of global strategy and vice president of digital services at Fujitsu's Tokyo headquarters.

As a well-known ICT commentator and analyst, Craig has written more than 200 research pieces, has presented at over 1,500 events globally and is regularly quoted in regional media. Craig is actively involved in the ICT community as board member of the Australian Information Industry Association (AIIA). He is currently pursuing a Doctor of Business Administration degree on the national culture impact on IT strategy/investment (Japan compared to Australia).

Co-Lead Author



**Phil Harpur**  
**Principal Analyst**

Phil Harpur is an Australian-based technology analyst and consultant with over 25 years of experience across telecommunications, the cloud, data centres and digital media. His expertise spans over 35 countries across Asia. He also works as an analyst/writer in the financial services industry with a focus on the technology sector.

Phil is currently part of the DataDriven team, which is the Asia Pacific research partner for ISG, and has contributed to the creation of nine ISG Provider Lens™ reports. Prior experience

includes Gartner, Frost & Sullivan and BuddeComm. He has been quoted in multiple global publications and appeared on business TV programs including Bloomberg, CNBC, Fox Business and ABC. He has also presented at numerous local and international conferences. Phil has a Bachelor of Science degree, with majors in computing and statistics from Macquarie University and holds a graduate certificate in applied finance and investment from the Securities Institute of Australia.



## Author & Editor Biographies



*Research Analyst*

**Angie Kho**  
**Regional Support Analyst**

Angie Kho is a regional support analyst at ISG and is responsible for supporting and contributing to Provider Lens™ studies on Microsoft Ecosystem for the Singapore and Malaysia markets.

Angie is part of the DataDriven team, which is the Asia Pacific research partner for ISG and has contributed to seven IPL reports.

Her areas of expertise lie in IT services management and enterprise planning services. Angie develops content from an enterprise perspective and authors

the global summary report. Along with this, she supports the lead analysts in the research process and ad hoc research assignments.



*IPL Product Owner*

**Jan Erik Aase**  
**Partner and Global Head – ISG Provider Lens™**

Mr. Aase brings extensive experience in the implementation and research of service integration and management of both IT and business processes. With over 35 years of experience, he is highly skilled at analyzing vendor governance trends and methodologies, identifying inefficiencies in current processes, and advising the industry. Jan Erik has experience on all four sides of the sourcing and vendor governance lifecycle - as a client, an industry analyst, a service provider and an advisor. Now as a research

director, principal analyst and global head of ISG Provider Lens™, he is very well positioned to assess and report on the state of the industry and make recommendations for both enterprises and service provider clients.





### \*ISG Provider Lens™

The ISG Provider Lens™ Quadrant research series is the only service provider evaluation of its kind to combine empirical, data-driven research and market analysis with the real-world experience and observations of ISG's global advisory team. Enterprises will find a wealth of detailed data and market analysis to help guide their selection of appropriate sourcing partners, while ISG advisors use the reports to validate their own market knowledge and make recommendations to ISG's enterprise clients. The research currently covers providers offering their services across multiple geographies globally.

For more information about ISG Provider Lens research, please visit this [webpage](#).

### \*ISG Research™

ISG Research™ provides subscription research, advisory consulting and executive event services focused on market trends and disruptive technologies driving change in business computing. ISG Research delivers guidance that helps businesses accelerate growth and create more value.

For more information about ISG Research subscriptions, please email [contact@isg-one.com](mailto:contact@isg-one.com), call +1.203.454.3900, or visit [research.isg-one.com](http://research.isg-one.com).

### \*ISG

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 800 clients, including more than 75 of the world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis.

Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,300 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data. For more information, visit [www.isg-one.com](http://www.isg-one.com).



**JULY 2022**

---

**REPORT: CYBERSECURITY — SOLUTIONS AND SERVICES**