

***ISG** Provider Lens™

Cybersecurity – Solutions & Services

Managed Security Services (MSS)

Australia 2021
Quadrant
Report



A research report
comparing provider
strengths, challenges
and competitive
differentiators

Customized report courtesy of:

CGI

August 2021

About this Report

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 August 2021, 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 lead author for this report is Craig Baty. The editor is Ipshita Sengupta. The research analyst is Monica K and the data analyst is Rajesh C. The quality and consistency advisors are Michael Gale and Anand Balasubramanian.





ISG Provider Lens™ delivers leading-edge and actionable research studies, reports and consulting services focused on technology and service providers' strengths and weaknesses and how they are positioned relative to their peers in the market. These reports provide influential insights accessed by our large pool of advisors who are actively advising outsourcing deals as well as large numbers of ISG enterprise clients who are potential outsourcers.

For more information about ISG Provider Lens™ studies, please email ISGLens@isg-one.com, call +1.203.454.3900, or visit ISG Provider Lens™ under [ISG Provider Lens™](#).




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, call +1.203.454.3900 or visit research.isg-one.com.



1	Executive Summary
6	Introduction
19	Managed Security Services (MSS)
24	Methodology

© 2021 Information Services Group, Inc. All rights reserved. Reproduction of this publication in any form without prior permission is strictly prohibited. Information contained in this report is based on the best available and reliable resources. Opinions expressed in this report reflect ISG's judgment at the time of this report and are subject to change without notice. ISG has no liability for omissions, errors or completeness of information in this report. ISG Research™ and ISG Provider Lens™ are trademarks of Information Services Group, Inc.



EXECUTIVE SUMMARY

Key trends in Australia

The cybersecurity landscape in Australia continues to evolve rapidly. Digital transformation initiatives that leverage cloud technologies and enable remote working are driving the demand for more cybersecurity solutions in Australia. Concurrently, both small and large providers in this space are expanding their service offerings and packaging them as platforms. Smaller providers are also often merging with or acquiring other providers of similar size to become end-to-end cybersecurity providers.

Australia-based organisations are demanding both simplicity and flexibility in cybersecurity solutions. Therefore, providers should look to developing more comprehensive offerings that target an increasingly diverse customer base, while also adapting to their rapidly changing needs.

The growing importance of cybersecurity is changing the way Australia-based enterprises are procuring related services. Senior management is increasingly being included in the decision making on cybersecurity products and strategies and are keen to understand all aspects of cyber risks. Increased awareness of cyberattacks and stricter regulations and legislations are further raising the maturity of these services.

A broad range of cybersecurity providers are expanding their consulting divisions, with customers increasingly preferring to purchase solutions from their existing providers,

rather than engaging in new consultations. The interest in on-demand solutions is growing significantly among customers in Australia.

There is a growing demand for technologies that can support remote working. These include endpoint protection, secure web gateways, identity access management, secure access service edge (SASE) and web application firewalls. In the next few years, the demand for cloud-based detection and response solutions, such as endpoint detection and response (EDR) and managed detection and response (MDR), is expected to grow strongly in Australia.

Strong growth predicted in cybersecurity space in Australia by 2024

In 2021, over 26,500 people were employed in the cyber sector in Australia. The Australian Cybersecurity Centre (ACSC) estimates that over 7,000 new jobs need to be created by 2024, to support the rising demand for cybersecurity services. In addition, many roles across enterprises and government entities will need increasing awareness about the evolving nature of cyber risks, with the skill levels to deal with such threats. The cybersecurity market in Australia is expected to maintain its growth trajectory over the next few years.

The use of AI in cybersecurity is also expected to grow, rapidly driven by the adoption of IoT, increase in cyber threats, concerns over data privacy and stringent data-related regulations. Next-generation identity and access management, messaging and network security will be the key cybersecurity investment areas for enterprises in 2021 and 2022. Mobile device security is also likely to be a fast-growing cybersecurity priority.

As an increasing number of critical resources are being stored in the cloud, the number of cyber attacks are, correspondingly, on the rise. Enterprises are ramping up their strategies to leverage cloud, enable remote working and optimise cost structure. This is driving the high demand for cybersecurity services. Demand for cloud-based detection and response solutions and web access management is anticipated to accelerate in the next few years as companies need to safely access large volumes of information and applications online.

Government of Australia launches new cybersecurity strategy

The government of Australia launched its Cybersecurity Strategy in 2020, in an effort to protect Australia's critical infrastructure from persistent and significant cyber threats. This strategy will trigger an increase in federal spending on cybersecurity to AUS\$1.66 billion over the next decade. It is also strongly focused on enforcement of regulations and on strengthening Australia's national cybersecurity organisations such as the ACSC and the Australian Signals Directorate (ASD). Under this strategy, initiatives are expected to boost community awareness and preparedness, and help critical infrastructure providers assess

vulnerabilities in their networks. It also includes additional funding for the Australian Federal Police (AFP) to investigate and counter cyber threats and measures to strengthen the security defences of small and medium-sized businesses (SMBs), universities and households. The government will also work with large businesses and managed service providers to improve the tools available to ensure companies have the capacity to combat cyber threats. Key segments of Australia's national critical infrastructure will be required to meet a new "positive security obligation" (PSO), under the government's proposed security of critical infrastructure (SoCI) reforms. The PSO will set a minimum cybersecurity baseline for Australia, including sector-by-sector guidance on cybersecurity standards and best practices.

Australia-based companies concerned about cybersecurity with growth in cyberattacks

The AustCyber Digital Trust Report 2020 estimates that a four-week disruption to the nation's digital infrastructure due to a significant cybersecurity incident would cost the region's economy around AU\$30 billion, or about 1.5 percent of GDP, and would result in the loss of over 160,000 jobs. The increased number of cybersecurity breaches is driving the demand for cybersecurity services amongst companies in Australia. There is also widespread public uncertainty and distrust around how organisations handle their data. Cybersecurity is becoming a major challenge for local organisations with a growth in number of sophisticated cyberattacks. The COVID-19 pandemic has put an even greater

strain on security systems that are already under significant amounts of pressure. Australian organisations can be better equipped to respond effectively to attacks, by utilising threat intelligence and adopting more strategic approaches to cybersecurity.

Identity and Access Management Software Market Trends

An identity and access management (IAM) platform has become one of the most important technology investments for organizations due to the continued global market tailwinds of cloud and hybrid IT, digital transformation and zero-trust security. These trends have accelerated in 2020 and 2021 as companies of all sizes, and in all industries, have had to quickly adjust their delivery models to engage with more customers online.

Cloud computing is driving two important trends that are changing the competitive IAM landscape. Many providers are moving IAM from on-premises to the cloud, or are building solutions that straddle both. Customers are also increasingly demanding pay-as-you-go (PAYG) models or IAM as a service, which some providers refer to as identity as a service (IDaaS).

Australia-based enterprises procuring IAM should take a balanced decision based on their unique needs. Factors such as provider support, partner networks and a vendor's product development roadmap should be strictly assessed. IAM technology is evolving rapidly in the face of novel IAM-as-a-Service offerings, and the growing need to include IAM functionality in DevOps and containers as well as for securing IoT devices.

Of the 23 providers in Australia in this quadrant, seven are Leaders and one is a Rising Star.

Data Loss Prevention Software Market Trends

Advanced data loss prevention (DLP) tools can scan files and databases to identify private data, tag those assets and raise alerts for intervention. Organisations can define guidelines to process those assets, deciding between deleting the sensitive information, obfuscating, replacing, encrypting or moving files to safe storage. They can use these tools to fix old data and comply with new business processes.

DLP has become a 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 a part of the new legislation, have increased the importance of data protection measures. Europe's General Data Protection Regulation (GDPR) has also received wide attention in the region, creating a significant impact, as most large Australia-based enterprises do business with Europe and need to comply with it.

The Australian Privacy Act contains the 13 Australian Privacy Principles that apply to most government agencies and all private sector organisations having an annual turnover of more than AU\$3 million. The privacy act also regulates the privacy component of the consumer reporting system, tax file numbers, and health and medical research.

Of the 22 providers in Australia in this quadrant, five are Leaders and one is a Rising Star.

Advanced Endpoint Threat Protection, Detection and Response Market Trends

With an increasingly number of employees in Australia working remotely from unsecure networks, the adoption of advanced Endpoint Threat Protection, Detection and Response (ETPDR) solutions has increased significantly. The increased demand for security solutions and services is being driven by external threats. Demand is also being triggered by legacy technology and an explosion of Internet-facing endpoints and services that are creating technical complexity, leading to configuration errors. The configuration errors caused by humans, is now one of the leading causes for breaches.

Enterprises need continuous monitoring and complete visibility of all endpoints, and a tool that can analyse, prevent, and respond to advanced threats, isolating the compromised endpoint. Many enterprises are already using endpoint protection solutions, but ETPDR solutions are more advanced and provide automation and orchestration of multiple threat protection, detection, and response capabilities in a single product. The best ETPDR solutions include behavioral detection with automatic response. Also, to cover the entire enterprise endpoint landscape, the solution should offer threat protection and detection capabilities across all operating systems (OSes). Finally, the most mature solutions use risk-based approaches to policy architecture and enforcement to help support a zero-trust device posture.

Of the 19 providers in Australia in this quadrant, six are Leaders and one is a Rising Star.

Technical Security Services Market Trends

Cybersecurity software vendors rely on service partners to install, configure and integrate their solutions. It is often the service partner that closes the sale through the vendor's pre-sales team to support product information. Service partners retain client relationships and are considered as trusted consultants that estimate capacity and system requirements.

The Australian Privacy Act was significantly strengthened in 2018, particularly with the introduction of the NDB scheme. Although these regulations are not technical in nature, they guide enterprises to ensure that their cybersecurity implementations meet certain minimal standards. Enterprises procuring technical security services should first check which service partners are available locally to provide the necessary engineering, architecture and integration.

The procurement process must bundle software, hardware and service partners in a balanced manner to ensure long-term service support. They may require immediate support from a robust service partner to address a data breach or cyberattack.

Of the 22 providers in Australia in this quadrant, 10 are leaders and one is a Rising Star.

Strategic Security Services Trends

The strategic security services market is largely driven by Australia's new privacy laws, growing awareness about security issues, and an increasing number of cyberattacks, driven by the COVID-19 pandemic.

Enterprises in Australia are becoming more aware of the repercussions of a cybercrime on their finances and reputation. Governance, risk and compliance (GRC) practices, which were once focused solely on business factors, now cover cybersecurity because of the cost implications as well as the impact on brand credibility, following a data breach or ransomware attack. Since the introduction of stringent data privacy laws and the NDB scheme, many organisations have employed a data security officer or compliance officer.

In this highly regulated environment, consulting firms operating in Australia have built additional expertise to help clients with compliance. Most major system and software providers as well as consultancy firms have established or expanded their cybersecurity practices, and are aggressively marketing them to Australia-based enterprises.

Of the 29 providers in Australia in this quadrant, 12 are Leaders and one is a Rising Star.

Managed Security Services Market Trends

The managed security services 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 deep specialization that compensates for scale to provide more client proximity.

Cyber criminals around the world are using AI tools to automate threat creation, web scanning and malware distribution. Enterprises are thus required to adopt more sophisticated tools as defence. Cyber defence centres (CDCs) have emerged, not to replace SOCs, but to expand security operations. These centres leverage advanced machine learning (ML) tools that can ingest large volumes of data to provide smart analytics, giving insights into how threats morph, move and spread. They share information dynamically with other CDCs to stay abreast with new developments in cybercrime. New tools such as micro-segmentation enable experts to isolate hackers or bots when they break into an enterprise network.

Managed cybersecurity services have become essential for enterprises. As security requires significant expertise, staff shortage is a challenge for enterprises in Australia. It is difficult for midsize enterprises, in particular, to retain cybersecurity experts. Service providers address this concern by offering the expertise of highly skilled practitioners to this enterprise segment.

Of the 29 providers in Australia in this quadrant, 12 are Leaders and two are Rising Stars.

Introduction

Simplified illustration



Source: ISG 2021

Definition

Enterprises are rapidly adopting new technologies to embark on digital transformation journeys to stay competitive and align with ever-evolving end-user needs. The growing adoption of these technologies, along with new tools to deliver efficiency and speed, has made enterprises vulnerable by expanding threat attack surface. Ransomware, advanced persistent threats (APTs), and phishing attacks emerged as some of the leading cyberthreats in 2020. Experian, SolarWinds, Zoom, Magellan Health, Finastra and Marriott were some of the leading entities that faced cyberattacks from hacking, malicious code, and ransomware last year.

Definition (cont.)

Scope of the Report

As part of the ISG Provider Lens™ Quadrant Study, we are introducing the following six quadrants (market) research on Cybersecurity - Solutions & Services 2021 by region:

Scope of the Study – Quadrant and Geography Coverage

	USA	UK	Nordics	Germany	Switzerland	France	Brazil	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)	✓	✓	✓	✓	✓	✓	✓	✓

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 classes 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 5,000 or more employees or revenue above US\$1 billion, with activities worldwide and globally distributed decision-making structures.

Provider Classifications

The ISG Provider Lens™ quadrants are created using an evaluation matrix containing four segments (Leader, Product & Market Challenger and Contender), and the providers are positioned accordingly.

Leader

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.

Product Challenger

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.

Market Challenger

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.

Contender

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 both products and services and a sensible market approach with a goal of becoming a Product or Market Challenger within 12 to 18 months.

Provider Classifications (cont.)

Each ISG Provider Lens™ quadrant may include a service provider(s) which 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 (exceptions are possible).

Rising Star

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

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.

Cybersecurity – Solutions & Services - Quadrant Provider Listing 1 of 6

	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	● Product Challenger
Atos	● Not in	● Not in	● Not in	● Contender	● Contender	● Product Challenger
Bitdefender	● Not in	● Not in	● Leader	● 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	● Rising Star
CGI	● Not in	● Not in	● Not in	● Product Challenger	● Leader	● Leader
Check Point	● Contender	● Product Challenger	● Product Challenger	● Not in	● Not in	● Not in
Cisco	● Not in	● Not in	● Contender	● Not in	● Not in	● Not in
CrowdStrike	● Not in	● Not in	● Leader	● Not in	● Not in	● Not in
Cyberark	● Leader	● Not in	● Not in	● Not in	● Not in	● Not in
CyberCX	● Not in	● Not in	● Not in	● Leader	● Leader	● Leader

Cybersecurity – Solutions & Services - Quadrant Provider Listing 2 of 6

	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
CyberProof	● Not in	● Not in	● Not in	● Not in	● Product Challenger	● Contender
Cylance	● Not in	● Not in	● Product Challenger	● 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	● Product Challenger	● Product Challenger	● Product Challenger
Datacom	● Not in	● Not in	● Not in	● Product Challenger	● Product Challenger	● Product Challenger
Deloitte	● Not in	● Not in	● Not in	● Leader	● Leader	● Leader
Digital Guardian	● Not in	● Contender	● Not in	● Not in	● Not in	● Not in
DriveLock	● Not in	● Product Challenger	● Not in	● Not in	● Not in	● Not in
DXC	● Not in	● Not in	● Not in	● Leader	● Leader	● Leader
ESET	● Not in	● Not in	● Contender	● Not in	● Not in	● Not in
Evidian (ATOS)	● Product Challenger	● Not in	● Not in	● Not in	● Not in	● Not in
EY	● Not in	● Not in	● Not in	● Not in	● Leader	● Not in
FireEye	● Not in	● Not in	● Contender	● Not in	● Not in	● Not in

Cybersecurity – Solutions & Services - Quadrant Provider Listing 3 of 6

	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
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	● Rising Star	● 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
Google DLP	● Not in	● Contender	● Not in	● Not in	● Not in	● Not in
HCL	● Not in	● Not in	● Not in	● Product Challenger	● Product Challenger	● Product Challenger
IBM	● Leader	● Leader	● Product Challenger	● Leader	● Leader	● Leader
Infosys	● Not in	● Not in	● Not in	● Product Challenger	● Product Challenger	● Product Challenger
Ivanti	● Not in	● Product Challenger	● Not in	● Not in	● Not in	● Not in
Kasada	● Not in	● Leader	● Rising Star	● Not in	● Not in	● Not in
Kaspersky	● Not in	● Not in	● Leader	● Not in	● Not in	● Not in
KPMG	● Not in	● Not in	● Not in	● Not in	● Leader	● Not in

Cybersecurity – Solutions & Services - Quadrant Provider Listing 4 of 6

	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 Government	● Not in	● Not in	● Not in	● Contender	● Contender	● Product Challenger
McAfee	● Not in	● Leader	● Product Challenger	● Not in	● Not in	● Not in
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
Mphasis	● Not in	● Not in	● Not in	● Contender	● Not in	● Contender
Netskope	● Not in	● Product Challenger	● Not in	● 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	● Contender	● Not in	● Not in	● Not in	● Not in	● Not in
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

Cybersecurity – Solutions & Services - Quadrant Provider Listing 5 of 6

	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
Proofpoint	● Not in	● Market Challenger	● Not in	● Not in	● Not in	● Not in
PwC	● Not in	● Not in	● Not in	● Not in	● Leader	● Not in
Rapid7	● Contender	● Not in	● Not in	● 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
SAP	● Market Challenger	● Not in	● Not in	● Not in	● Not in	● Not in
Secureworks	● Not in	● Not in	● Not in	● Not in	● Product Challenger	● Contender
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	● Product Challenger	● Product Challenger	● Product Challenger

Cybersecurity – Solutions & Services - Quadrant Provider Listing 6 of 6

	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
Tech Mahindra	● Not in	● Not in	● Not in	● Contender	● Contender	● Product Challenger
Telstra	● Not in	● Not in	● Not in	● Leader	● Product Challenger	● Leader
Tesseract	● Not in	● Not in	● Not in	● Leader	● Rising Star	● Leader
Thales	● Product Challenger	● Not in	● Not in	● Not in	● Not in	● Not in
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	● Contender	● 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	● Not in	● Product Challenger	● Leader
VMware Carbon Black	● Not in	● Product Challenger	● Leader	● Not in	● Not in	● Not in
Wipro	● Not in	● Not in	● Not in	● Rising Star	● Leader	● Leader
Zscaler	● Not in	● Rising Star	● Not in	● Not in	● Not in	● Not in



Cybersecurity – Solutions & Services Quadrants

ENTERPRISE CONTEXT

Managed Security Services (MSS)

This report is relevant to enterprises across industries in Australia for evaluating providers of managed security services.

In this quadrant report, ISG highlights the current market positioning of providers of managed security to enterprises in Australia, and how each provider addresses the key challenges faced in the region.

Without the appropriate managed IT support, IT systems are vulnerable to exploitation. As more crucial processes move onto the cloud and cybercriminals become even more sophisticated, there is an even greater need for a smarter way to improve security. As a result, the demand for cloud security, security operations center (SOC) services, Internet of Things (IoT) and operational technology (OT) security and zero trust security have been increasing among the enterprises over the past few years.

Managed security service providers (MSSPs) have established their own, dedicated, co-managed or virtual SOCs within the region to serve enterprises. The managed security services (MSS) market in Australia is mainly driven by the growing need for security solutions across various end-user industries. Additionally, increased spending by the government on security solutions and growing concerns over breaches of intelligence data are further expected to foster the market growth. Regulation and compliance pressure will create new demands for managed security services in the region.

Due to a shortage of skilled cybersecurity personnel in the region, there is a high rate of security management outsourcing, which, in turn, drives the MSS market. Australia has emerged as a strategic market for global MSSPs with a presence in the Asia Pacific region.

The following can use this report to identify and evaluate different service providers:

Chief information officers (CIOs) should read this report to better understand how the current processes and protocols impact an enterprise's existing systems as well as the security needs for the adoption and integration of new capabilities.

Chief technology officer (CTOs) handling operations and services should read this report to acquire in-depth knowledge on emerging technologies and solutions to gain strategic directions as well as partnership options with relevant service providers. CTOs can also ensure the deployment of appropriate security platforms and solutions, enabling competitive advantage.

Security leaders should read this report to understand the relative positioning and capabilities of MSSPs. The report also compares the technical capabilities of various service providers in the market.

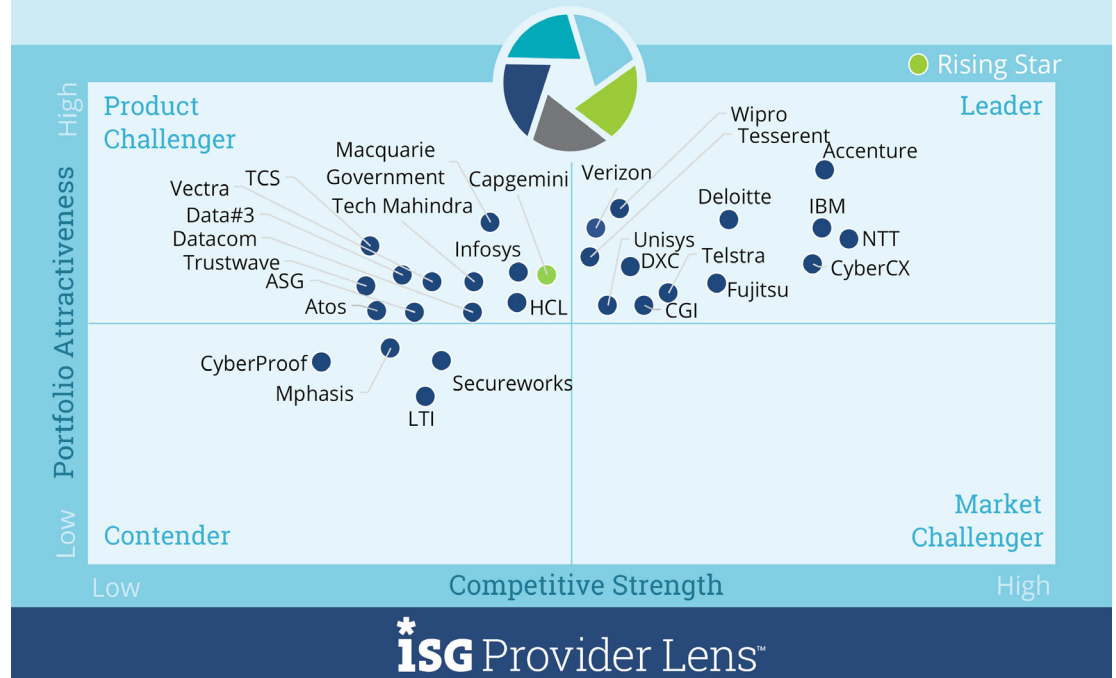
MANAGED SECURITY SERVICES (MSS)

Definition

MSS comprises the operations and management of IT security infrastructures for one or several customers by a security operations centre. Typical services include security monitoring, behaviour analysis, unauthorised access detection, advisory on preventive measures, penetration testing, firewall operations, anti-virus operations, IAM operation services, DLP operations and all other operating services to provide ongoing, real-time protection, without compromising business performance. This quadrant examines service providers that are not exclusively focused on proprietary products but can manage and operate the best-of-breed security tools. These service providers can handle the entire security incident lifecycle, starting from identification to resolution.

Cybersecurity Solutions & Services 2021
Managed Security Services

2021
Australia



Source: ISG Research 2021

MANAGED SECURITY SERVICES (MSS)

Definition (cont.)

This quadrant assesses a service provider's ability to provide ongoing management services for large enterprise clients. These clients usually run operations in many countries and have a broad network with a vast number of secure endpoints. They are the preferred targets for hackers and data breaches because of the value of their assets and their financial capacity to pay for ransomware. This group also includes banking, financial services, insurance, health organizations and other enterprises that must comply with strict regulations. To support this select group of companies, service providers in this space provide many security tools and superior threat identification technologies.

Eligibility Criteria

- Providers should have the 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 site.
- Providers should be relevant, in terms of revenue and number of customers, as an MSS provider in the respective country.
- The provider should not be exclusively focused on proprietary products but can manage and operate best-of-breed security tools.
- The provider should possess accreditations from vendors of security tools.
- Security operations centres are ideally owned and managed by the provider and not predominantly by partners.
- The provider should maintain certified staff, for example, in Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC).

MANAGED SECURITY SERVICES (MSS)

Observations

Of the 29 providers in Australia in this quadrant, 13 are Leaders and one is a Rising Star:

- **Accenture** has a highly comprehensive managed security services offering as a part of its professional security services offering. The company has been operating in Australia for over 40 years and employs around 5,000 staff in six Australian cities — half of them dedicated to technology.
- **CGI** is one of the largest IT and business consulting services firms in the world, with 76,000 consultants across 40 countries. CGI has been in Australia for over 40 years, offering its services to over 115 clients across energy, telecommunications, government, and utilities sectors. CGI is highly active in the cybersecurity industry in Australia.
- **CyberCX** is an Australia- and New Zealand-based cybersecurity specialist, with headquarters in Melbourne. CyberCX utilises its Australia or New Zealand Sovereign (onshore) Security Operation Centre as-a-service (SOCaaS) offering, as well as a “follow the sun” coverage model, leveraging three countries.
- **Deloitte's** annual revenue in 2020 was US\$48 billion. Australia contributed just over AU\$2 billion in revenue. Deloitte offers a broad range of managed cybersecurity services to Australian organisations, spanning strategic consulting, risk advisory, cyber intelligence information and vulnerability management services.
- **DXC Technology** employs 10,000 people in Australia and has revenues of more than US\$1.4 billion in 2020. DXC's managed security services are supported by nine security operations centres worldwide, including one in Australia. It also has over 30 security solution partners.
- **Fujitsu** has a large presence in the managed security services space in Australia, and has been operating in the region for 40 years. Australia is now its most strategic international operation outside Europe and the U.K. Key industries for cybersecurity services in Australia include the public sector, defence, healthcare, retail, public safety and commercial.
- **IBM** has evolved its business focus in the past four years, with services that address data, AI, cloud, analytics and cybersecurity now representing more than half of its revenue. It offers security services for data centres, networks, digital workplaces, security access and the cloud. It has 5,000 employees in Australia, with offices in every state and territory.

MANAGED SECURITY SERVICES (MSS)

Observations (cont.)

- **NTT** offers managed cloud services, and IT support services encompass over 450 global customers, generating US\$1 trillion in revenue. Its managed security services are supported by two security operations centres in Australia — one in Sydney and the other in Canberra. NTT Australia has seen very strong recent growth. In 2020, it saw bookings grow by 300 percent.
- **Tesserent** is the largest cybersecurity company listed on the Australian Securities Exchange (ASX). It is a one-stop-shop for cybersecurity solutions, including managed security throughout its security operations centres and a network operations center. Tesserent has recently restructured into three new company divisions to realize its rapid expansion plan over the next few years.
- **Telstra** offers managed security services for a range of a range of local and global products. These services are centred around a custom developed and public cloud hosted OpenMSS cybersecurity big data platform. Telstra delivers security operations centre services to approximately 400 customers.
- **Unisys'** portfolio is based on a number of service platforms, including Unisys Stealth™ and TrustCheck. Unisys has a significant presence in the cybersecurity space in Australia; it generates over 50 percent of its global cybersecurity revenue from the region. It has offices in Sydney, Melbourne and Canberra, and a security operations centre in Bangalore.
- **Verizon's** global managed security solution offering includes advanced security operations and managed threat protection services, threat intel and response services, forensic investigations, and identity management. The offerings remotely monitor and manage IT security assets and technology across a broad set of security vendors.
- **Wipro** is a leading global IT, consulting and business process services provider, headquartered in India. Wipro's managed security services include advanced cyber defense centres, cybersecurity platforms and managed security infrastructure and operations. Wipro has a security operations centre in Melbourne and development centres in Sydney, Canberra and Perth.
- **Capgemini** (Rising Star) is a leading global security service provider. Its managed security service offerings are delivered through a variety of options, including managed, dedicated, satellite and hybrid security operations centre delivery models. Capgemini has a significant presence in offering MSS in Australia, and has a security operations centre in Melbourne.

CGI



Overview

Founded in 1976, CGI is one of the largest IT and business consulting services firms in the world, with 76,000 consultants across 40 countries, offering services to 5,500 clients. Its emerging technology practice, including MSS, is offered across 17 countries, and includes dedicated and virtual teams in Australia. CGI has been in Australia for over 40 years, with offices in Sydney, Melbourne, Brisbane and Hobart, offering services to over 115 clients, across a range of industries, including energy, telecommunications, government, and utilities. CGI is highly active in the cybersecurity industry in Australia.



Strengths

Highly comprehensive MSS offerings: CGI's MSSes range from technical services — maintaining security controls such as firewalls, anti-virus solutions, EDR solutions and cloud security controls — to security operations centre services — detecting, analysing and remediating security incidents in client IT and operational technology environments. CGI has nine security operations centres, globally. CGI's MSS services also include incident management and coordination services, vulnerability assessment and management, as well as sophisticated IT forensics and security architecture planning services. CGI's Australian security operations are certified for Information Security Management System (ISMS) ISO 27001:2013 and Business Continuity Management Systems (BCMS) ISO 22301:2019 standards.

Comprehensive cybersecurity services in Australia: CGI's Australian Security Practice operationalises cybersecurity services across the lifecycle of its Utilities clients' IT & OT operations, aligning business and regulatory objectives. It has a security operations centre in Melbourne that continuously monitors and improves its client's security posture, while detecting, analysing and responding to cybersecurity incidents. Australian cyber services include Vulnerability Management Services and Infrastructure Protection Services that include IAM, endpoint protection, application cloud and data protection, and messaging and mobile protection.

IBroad range of security services: CGI's security services range from consulting and staff augmentation to fully managed services, as well as from enterprise risk management to secure software lifecycle management, penetration testing, audits and assessments. It also includes managed detection and response services, with capabilities ranging from detection to forensic investigation and breach response services.



Caution

CGI has strong capabilities in the Australian market and is well recognized, however, several of its more advanced offerings, especially in the IoT area, remain under communicated.



2021 ISG Provider Lens™ Leader

CGI is highly active in the cybersecurity industry in Australia and has a security operations centre in Melbourne. Australian cyber services include Vulnerability Management Services and Infrastructure Protection Services that include IAM and endpoint protection.



Methodology

METHODOLOGY

The research study “2021 ISG Provider Lens™ Cybersecurity – Solutions & Services Australia” analyses 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. The study was divided into the following steps:



1. Definition of 2021 ISG Provider Lens™ Cybersecurity – Solutions & Services Australian market
2. Use of questionnaire-based surveys of service providers/vendor across all trend topics
3. Interactive discussions with service providers/vendors on capabilities and use cases
4. Leverage ISG’s internal databases and advisor knowledge and experience (wherever applicable)
5. Detailed analysis and evaluation of services and service documentation-based on the facts and figures received from providers and other sources.
6. Use of the following key evaluation criteria:
 - Strategy & vision
 - Innovation
 - Brand awareness and presence in the market
 - Sales and partner landscape
 - Breadth and depth of portfolio of services offered
 - Technology advancements

Author and Editor



Craig Baty, Author

Lead Analyst

Distinguished lead analyst and author Craig Baty has extensive research and thought leadership experience in the Asia Pacific and Japan ICT markets. Craig is Principal and Founder 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 ICT industry, including as a Group VP and Head of Gartner Research AP/J, CEO of Gartner Japan, Global VP Frost & Sullivan, EGM Marketing and CTO Fujitsu ANZ, GM Marketing Strategy and Alliances at BT Syntegra Australia, and more recently as VP Global Strategy and VP Digital Services in Fujitsu Tokyo HQ. As a well-known ICT commentator and analyst, Craig has written more than 200 research pieces and presented at over 1,500 events globally. He is also regularly quoted in the media. Craig is actively involved in the ICT community as a board member of the Australian Information Industry Association (AIIA) and other appointments. He is currently pursuing a Doctor of Business Administration by Research (DBA) in the area of national culture and its influence on IT strategic use and investment and is a former Advisor to the Japanese PM & Cabinet Next-Gen Global Leadership Program (Cross Cultural Communications).



Monica K, Enterprise Context and Global Overview Analyst

Senior Analyst

Monica K is a senior analyst at ISG. She is responsible for supporting and co-authoring Provider Lens™ studies on Digital Business Transformation, Enterprise Application aaS and Cybersecurity. Her area of expertise includes cybersecurity, IoT, robotic process automation (RPA), blockchain and artificial intelligence (AI). She is also responsible for authoring the enterprise content and the global summary report. Additionally, she engages in delivering ad-hoc vendor selection project requests from providers and advisors.

Author and Editor



Jan Erik Aase, Editor

Partner and Global Head – ISG Provider Lens/ISG Research

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™ | Quadrant Report

August 2021

© 2021 Information Services Group, Inc. All Rights Reserved



ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 700 clients, including more than 75 of 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.