ISG Provider Lens™

Cyber Security – Solutions & Services

Australia 2021

Quadrant Report

A research report comparing provider strengths, challenges and competitive differentiators

Customized report courtesy of:

CyberCX

June 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 June 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. The Quality and Consistency Advisor is Michael Gale and Anand Balasubramanian.

ISG Provider Lens™

ISG Provider Lens™

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 our studies, please email ISGLens@isg-one.com, call +49 (0) 561-50697537, or visit ISG Provider Lens™ under ISG Provider Lens™.

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, call +49 (0) 561-50697537 or visit research.isg-one.com.

EXECUTIVE SUMMARY

Key trends in Australia

The cyber security landscape in Australia continues to evolve rapidly. Digital transformation initiatives that leverage cloud technologies and enable remote working are driving the demand for more cyber security 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 cyber security providers.

Australia-based organisations are demanding both simplicity and flexibility in cyber security 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 cyber security is changing the way Australia-based enterprises are procuring related services. Senior management is increasingly being included in the decision making on cyber security 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 Gateway, Identity Access Management, Secure Access Service Edge (SASE) and Web Application Firewall. 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 expecting to grow strongly in Australia.

Strong Growth Predicted in Cyber Security Space in Australia by 2024

In 2021, over 26,500 people were employed in the Cyber sector in Australia. The Australian Cyber Security Centre (ACSC) estimates that over 7,000 new jobs need to be created by 2024, to support the rising demand for cyber security 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 Cyber Security market in Australia is expected to maintain its growth trajectory over the next few years.

The use of AI in cyber security 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-gen identity and access management, messaging and network security will be the key cyber security investment areas for enterprises in 2021 and 2022. Mobile device security is also likely to be a fast-growing cyber security priority.

As an increasing number of critical resources are being stored in the cloud, the number of cyberattacks 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 cyber security 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 Cyber Security Strategy

The Government of Australia launched its Cyber Security 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 cyber security to AUS$1.66 billion over the next decade. It is also strongly focused on enforcement of regulations and on strengthening Australia's national cyber security 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 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 cyber security baseline for Australia, including sector by sector guidance on cyber security standards and best practices.

Australia-Based Companies Concerned About Cyber Security 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 cyber security incident would cost the region's economy around AU$30 billion, or about 1.5 per cent of GDP, and would result in the loss of over 160,000 jobs. The increased number of cyber security breaches is driving the demand for cyber security services amongst companies in Australia. There is also widespread public uncertainty and distrust around how organisations handle their data. Cyber security 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 cyber security.

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. Organizations 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 analyze, 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.

ISG Provider Lens™

Technical Security Services Market Trends

Cyber security 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 cyber security 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 cyber security 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 cyber security 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 cyber security 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 enterprise, in particular, to retain cyber security 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 this ISG Provider Lens™ quadrant study, we are introducing the following six quadrants under Network — Software-defined Solutions and Services 2021.

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)	✓	✓	✓	✓	✓	✓	✓	✓
Managed Security Services (MSS)	✓	✓	✓	✓	✓	✓	✓	✓
Technical Security Services (TSS)	✓	✓	✓	✓	✓	✓	✓	✓
Strategic Security Services (SSS)	✓	✓	✓	✓	✓	✓	✓	✓

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 more than 5,000 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

The Leaders among the vendors/providers have a highly attractive product and service offering and a very strong market and competitive position; they fulfill all requirements for successful market cultivation. They can be regarded as opinion leaders, providing strategic impulses to the market. They also ensure innovative strength and stability.

Product Challenger

The Product Challengers offer a product and service portfolio that provides an above-average coverage of corporate requirements, but are not able to provide the same resources and strengths as the Leaders regarding the individual market cultivation categories. Often, this is due to the respective vendor's size or weak footprint within the respective target segment.

Market Challenger

Market Challengers are also very competitive, but there is still significant portfolio potential and they clearly fall behind the Leaders. Often, the Market Challengers are established vendors that are somewhat slow to address new trends due to their size and company structure, and therefore have some potential to optimize their portfolio and increase their attractiveness.

Contender

Contenders still lack mature products and services or sufficient depth and breadth in their offering, but also show some strengths and improvement potential in their market cultivation efforts. These vendors are often generalists or niche players.

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

Companies that receive the Rising Star award have a promising portfolio 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. This award is only given to vendors or service providers that have made significant progress toward their goals in the last 12 months and are expected to reach the Leader quadrant within the next 12-24 months due to their above-average impact and strength for innovation.

Not In

The service provider or vendor was not included in this quadrant. There might be one or several reasons why this designation is applied: 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 qualify due to market share, revenue, delivery capacity, number of customers or other metrics of scale to be directly compared with other providers in the quadrant. Omission from the quadrant does not imply that the service provider or vendor does not offer this service or solution, or confer any other meaning.

Cyber Security – 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

Cyber Security – 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		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

Cyber Security – 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

Cyber Security – 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

Cyber Security – 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

Cyber Security – 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		Leader	Product Challenger	Leader
Tesserent	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	Rising Star
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

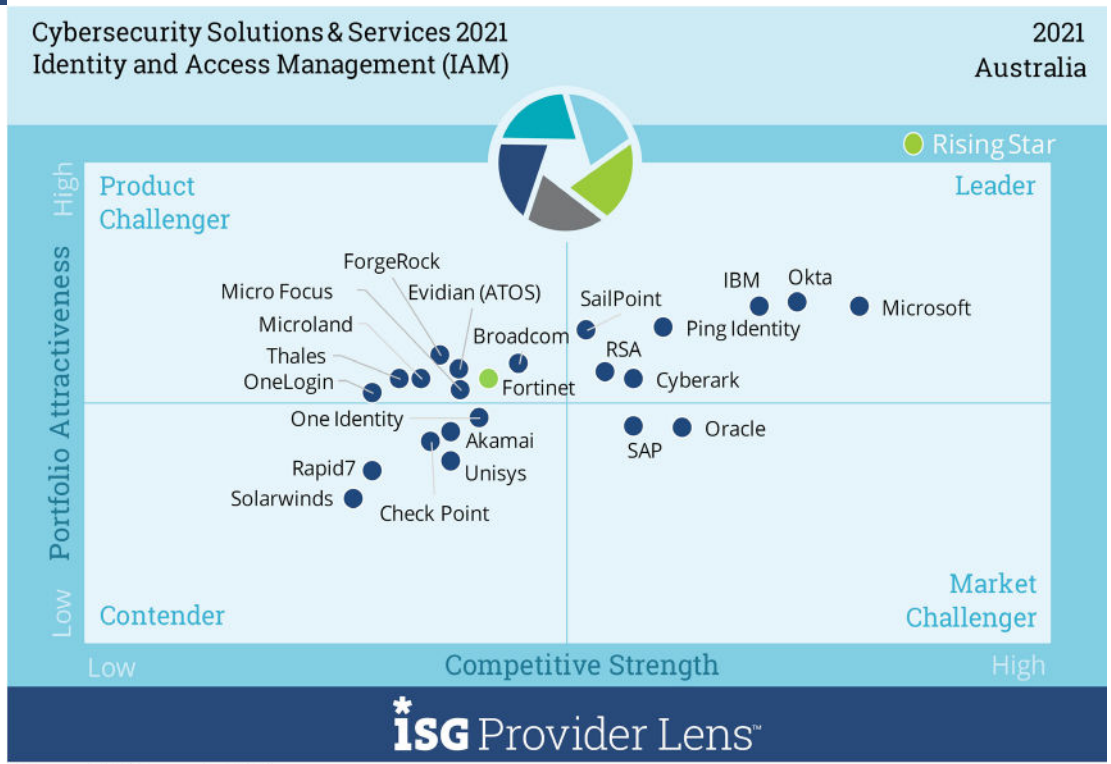
Cyber Security – Solutions & Services Quadrants

IDENTITY & ACCESS MANAGEMENT (IAM)

Definition

IAM vendors and solution providers are characterized by their ability to offer proprietary software and associated services to meet unique demands for securely managing enterprise user identities and devices. This quadrant also includes SaaS based on proprietary software. Pure service providers that do not offer an IAM product (on-premises and/or cloud) based on self-developed software are not included here. Depending on organizational requirements, these solutions could be deployed on-premises or on cloud (managed by customer) or as an As-a-Service model or a combination thereof.

IAM solutions are aimed at collecting, recording and administering user identities and related access rights, as well as specialized access to critical assets, and include privileged access management (PAM). They ensure that access rights are granted based on defined policies. To handle existing and new application requirements, IAM solutions are increasingly embedded with secure mechanisms, frameworks, and automation (for example, risk analyses) within their management suites to provide real-time user and attack profiling functionalities. Solution providers are also expected to provide additional features related to social media and mobile users to address security needs that go beyond traditional web and context-related rights management.



Source: ISG Research 2021

IDENTITY & ACCESS MANAGEMENT (IAM)

Eligibility Criteria

- Relevance (revenue and number of customers) as an IAM product vendor in the respective country
- IAM offerings should be based on proprietary software and not on third-party software.
- The solution should be capable of being deployed individually or as a combination of on-premises, cloud, IDaaS and a managed (third-party) model.
- The solution should be capable of supporting authentication individually or by way of a combination of SSO, MFA, risk-based and context-based models.
- The solution should be capable of supporting role-based access and privileged access management.
- 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.
- 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.
- To support through secure access, 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 & ACCESS MANAGEMENT (IAM)

Observations

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

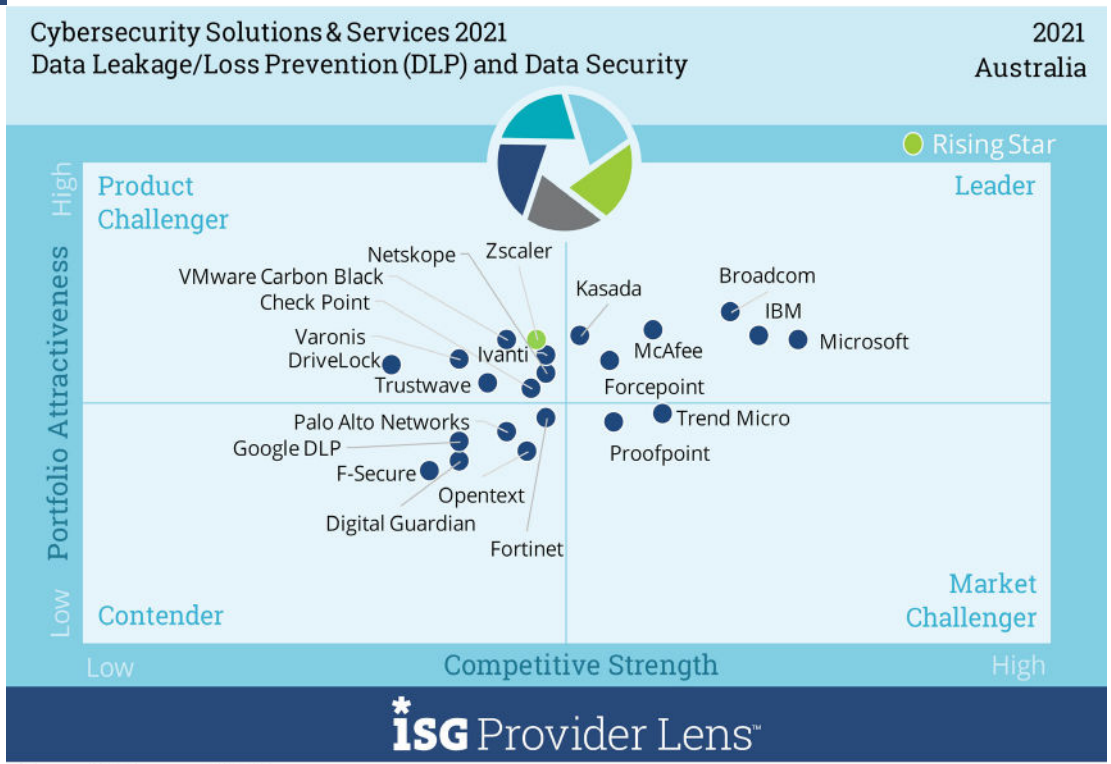
- **CyberArk** is global leader in PAM and a security partner to more than 6,770 global businesses. It has offices in the U.S, Israel, the U.K., Canada, France, Germany, Australia (Sydney) and India. CyberArk is rapidly expanding in Australia, within the small and medium enterprise (SME) market.
- **IBM** has expanded its security services offering with the acquisition of over 20 security vendors and service providers over the years. IAM is a core part of this offering. It has more than 8,000 security experts, who share knowledge globally, and 5,000 employees in Australia, with offices in every state and territory.
- **Microsoft** is one of the leading software companies in the world and has a large office in Australia, with around 1,500 employees. Azure Active Directory (Azure AD) is Microsoft's cloud-based IAM service. Microsoft recently expanded its IAM product suite in Australia. The company invests over US$1 billion, annually, in cyber security R&D.
- **Okta** offers fully functional cloud-based IAM management products. It has over 6,000 employees globally and an established presence in Australia. Its IAM products are Okta Cloud Connect and Okta Lifecycle Management. The company operates through a global network of more than 2,000 integrators and partners, including many in Australia.
- **Ping Identity's** Intelligent Identity platform provides access to cloud, mobile, SaaS across on-premises and cloud applications. Ping has a significant presence in Australia and a local instance in cloud infrastructure. This presence is expected to grow significantly over the next few years.
- **RSA** developed the world's first public key cryptographic algorithm. The company was acquired by Dell in 2016, which sold it to a consortium led by Symphony Technology Group in 2020. Cyber security services include implementation and optimisation, incidence response and cyber defence.
- **SailPoint** has a small, but growing, presence in Australia, with a strong base of resellers and channel partners. The company has a strong partner network, with major consultancies and security implementation specialists. It has a strategic alliance with EY and works closely with PwC Australia, which has helped win accounts in the Australian government sector.
- **Fortinet** (Rising Star) is a cyber security specialist that provides a full suite of security solutions, including IAM and AEDTPR, and provides lifecycle management and centralised operations, administration, and maintenance. Fortinet has had a strong presence in Australia for over 10 years through a strong partner ecosystem. The key verticals for Fortinet, in Australia, include IT services, Cloud Computing, Telecommunications and Retail.

DATA LEAKAGE/LOSS PREVENTION (DLP) AND DATA SECURITY

Definition

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

These solutions should be able to identify sensitive data, enforce policies, monitor traffic and improve data compliance. They are gaining considerable importance as it has become increasingly difficult for companies to control data movements and transfers. The number of



Source: ISG Research 2021

DATA LEAKAGE/LOSS PREVENTION (DLP) AND DATA SECURITY

Definition (cont.)

devices, including mobile, that are used to store data is increasing in companies. These are mostly equipped with an Internet connection and can send and receive data without passing it through a central Internet gateway. The devices are supplied with a multitude of interfaces, such as USB ports, Bluetooth, wireless local area network (WLAN) and near-field communication (NFC), which enable data sharing. Data security solutions protect data from unauthorized access, disclosure, or theft.

Eligibility Criteria

- Relevance (revenue and number of customers) as a DLP product vendor in the respective country
- The DLP offering should be based on proprietary software and not on a third-party software.
- The solution should be capable of supporting DLP across any architecture such as the cloud, network, storage, or endpoint.
- The solution should be able to protect sensitive data across structured or unstructured data, text or binary data.
- 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.

DATA LEAKAGE/LOSS PREVENTION (DLP) AND DATA SECURITY

Observations

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

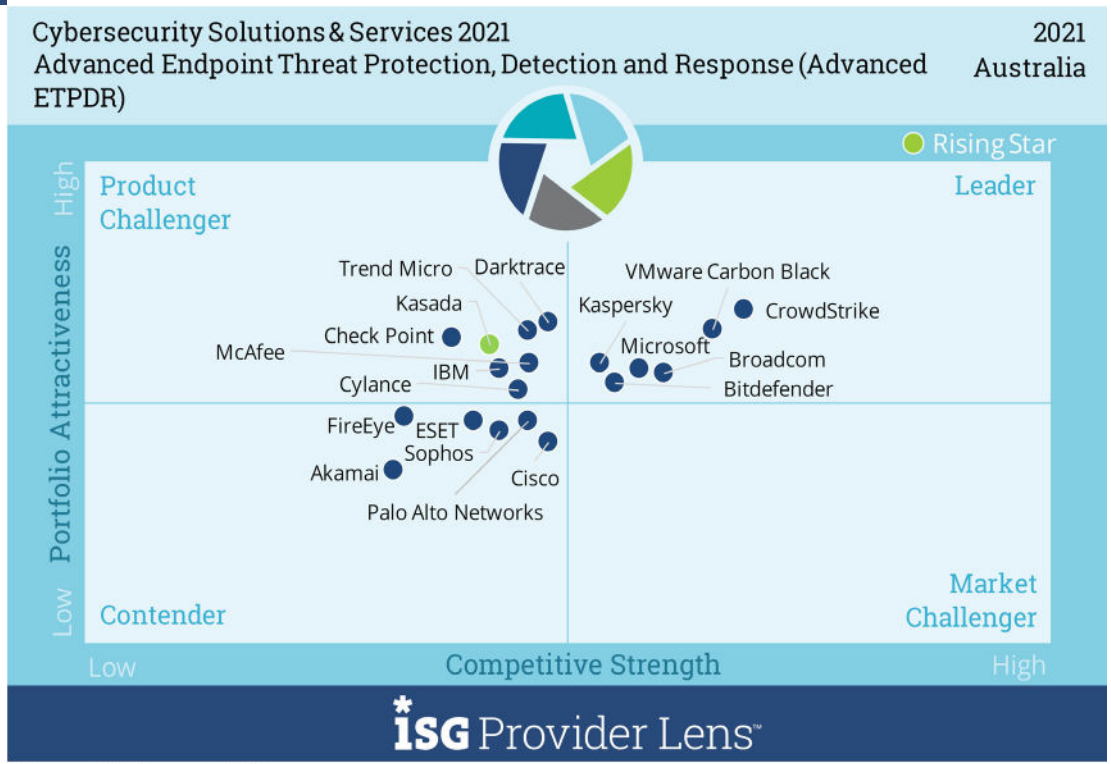
- **Broadcom** provides DLP through its Symantec brand and cross-sells its broad security portfolio directly to existing customers through an extensive partner program. It runs a large operation in Australia, but lost a considerable number of employees after it lost Symantec's Cyber Security Services to Accenture through an acquisition.
- **Forcepoint** is a global security solutions vendor with a large client base. Forcepoint Australia hired many senior staff from Symantec after the latter was acquired by Broadcom in late 2019. It made four new key appointments in 2020 to its leadership team for strengthening its channel, strategy and sales lineup across Australia.
- **IBM** has evolved its business focus in the past four years, with services that address data, AI, cloud, analytics and cyber security now representing more than half its revenue. IBM Security Guardium is its main DLP product, offering data protection, activity monitoring and compliance reporting.
- **Kasada** is an Australia-based cyber security company. Its anti-bot technology, as a part of its DLP offering, works by using client-side detection and mitigation, and is offered through a subscription model. Core clients are large enterprises in the Retail, Payments, Hospitality, Financial Services, Gaming, and Gambling/Casinos industries.
- **McAfee** offers a comprehensive range of DLP and endpoint protection security products. The company has 7,000 employees globally, including 150 in Australia. It has around 70,000 corporate clients, globally. It is expanding its presence in Australia and has recently signed a contract with a major Australian government department.
- **Microsoft** is one of the leading software companies in the world and has a large office in Australia, with around 1,500 employees. Microsoft invests over US$1 billion, annually, in cyber security R&D. Microsoft has a comprehensive set of DLP tools for end user, workplace and cloud users.
- **Zscaler (**Rising Star), founder in 2007, is a specialist DLP provider. Zscaler's platform infrastructure is distributed across more than 100 data centers globally. It has a fast-growing presence in the Australian market, where it is particularly strong in the government sector.

ADVANCED ENDPOINT THREAT PROTECTION, DETECTION, AND RESPONSE (ADVANCED ETPDR)

Definition

Advanced ETPDR vendors and solution providers are characterized by their ability to offer proprietary software and associated services. This quadrant also includes SaaS based on proprietary software. Pure service providers that do not offer an advanced ETPDR product (on-premises or cloud-based) based on self-developed software are not included here. This quadrant evaluates providers offering products that can provide continuous monitoring and complete visibility of all endpoints, and can analyze, prevent, and respond to advanced threats.

These solutions go beyond plain signature-based protection and offer protection from adversaries such as ransomware, 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/remediation. Such solutions comprise a database, wherein the information collected from network and endpoints is aggregated, analyzed, and investigated, and an agent that resides in the host system offers the monitoring and reporting capabilities for the events.



Source: ISG Research 2021

ADVANCED ENDPOINT THREAT PROTECTION, DETECTION, AND RESPONSE (ADVANCED ETPDR)

Eligibility Criteria

- Relevance (revenue and number of customers) as an advanced ETPDR product vendor in the respective country.
- The advanced ETPDR offering should be based on proprietary software and not on a third-party software.
- The provider's solutions should provide comprehensive and total coverage and visibility of all endpoints in the network.
- The solution should demonstrate effectiveness in blocking sophisticated threats such as APTs, ransomware and malware.
- The solution should leverage threat intelligence, analyze, and offer real-time insights on threats across endpoints.

Observations

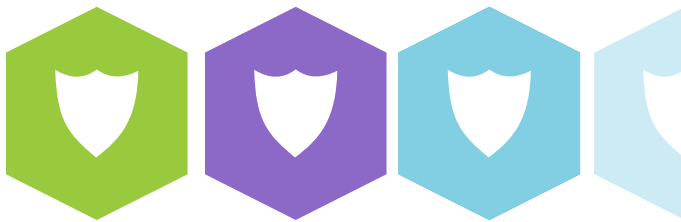
Of the 19 providers in Australia in this quadrant, six are Leaders and one is a Rising Star:

- **Bitdefender** is a cyber security technology company headquartered in Romania, with offices in the U.S., Europe, the Middle East and Australia. Bitdefender's office in Melbourne, Australia, was established in 2019, when it began offering its global partner program to local resellers in the ANZ market.
- **Broadcom** utilises Symantec's platform to protect all traditional and mobile endpoint devices for on-premises, hybrid, or cloud-based solutions. It provides advanced endpoint protection, pre-attack and attack surface reduction, breach prevention and response and remediation functionality. It runs a large operation in Australia.
- **Carbon Black** is a cyber security company with headquarters in the U.S. It develops cloud-native advanced endpoint security software. Carbon Black has over 1,000 employees, serving has than 6,000 global customers. It has a growing presence in Australia and launched a data centre in the region in 2020.
- **CrowdStrike** is a cyber security specialist company headquartered in the US. It has been operating in the Australian market since 2016 and continues to grow strongly in Australia, supported by its expanding channel partner network.

ADVANCED ENDPOINT THREAT PROTECTION, DETECTION, AND RESPONSE (ADVANCED ETPDR)

Observations (cont.)

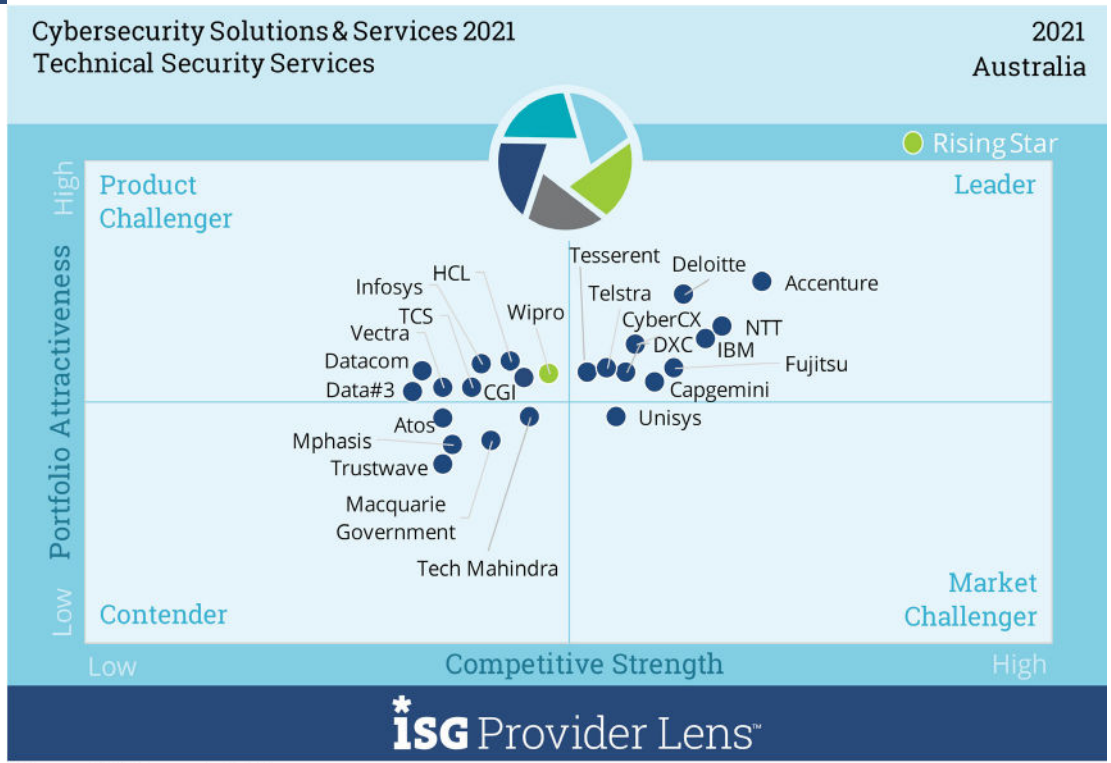
- **Kaspersky** is multinational cyber security and anti-virus provider based in Russia. It targets both SME and enterprise markets. Kaspersky services the Australian market via a localised website. In 2020 it moved its Australian related data to Switzerland as part of a global transparency project.
- **Microsoft** is one of the leading software companies in the world and has a large office in Australia, with around 1,500 employees. The company invests over US$1 billion, annually, in cyber security R&D. Microsoft Defender for endpoint provides advanced attack detections and enables security analysts to prioritise alerts.
- **Kasada** (Rising Star) is an Australia-based cyber security company founded in 2015, with offices in Australia, the U.S and the UK. The company is focused on preventing malicious bot-based attacks and offers its solution through a subscription model. Core clients are large enterprises in the Retail, Payments, Hospitality, Financial Services, Gaming and Gambling/Casinos industries.



TECHNICAL SECURITY SERVICES

Definition

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. TSS covers integration, maintenance and support for IT security products or solutions. TSS addresses all security products, including anti-virus, cloud, and data center security, IAM, DLP, network security, endpoint security, unified threat management (UTM) and others.



Source: ISG Research 2021

TECHNICAL SECURITY SERVICES

Eligibility Criteria

- Demonstrate experience in implementing security solutions for companies in the respective country
- Not exclusively focused on proprietary products
- Authorized by vendors to distribute and support security solutions
- Certified experts to support its security technologies
- Ability to participate (desirable, not mandatory) in local security associations and certification agencies

Observations

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

- **Accenture** has a highly comprehensive TSS offering as a part of its professional security services offering. Accenture has been operating in Australia for over 40 years, with around 5,000 employees in six Australian cities. In addition to offering its services to local clients, Accenture's Australian offices support clients worldwide.
- **Capgemini** is a leading global security service provider and its TSS offering includes solutions that address business goals, while protecting critical data, systems and users. Capgemini has a significant presence in the MSS space in Australia and has an SOC in Melbourne.
- **CyberCX** is an Australia-based cyber security specialist with headquarters in Melbourne. It was established in 2019 by aggregating 14 Australia and New Zealand based niche cyber security companies. Through its TSS, CyberCX acts as an independent cyber security partner for clients through end-to-end consultations.

TECHNICAL SECURITY SERVICES

Observations (cont.)

- **Deloitte** offers a broad range of technical cyber security services to Australia-based organisations. The global consultancy firm has over 100 cyber security experts located in Australia that conduct security audits for major local enterprises and large enterprise located in the APAC.
- **DXC** employs 10,000 people in Australia. Its TSS are supported by 12 SOCs worldwide, including one in Australia. The company also has over 30 security solution partners. DXC has a strong pipeline of cyber security services for the next few years.
- **Fujitsu** has a significant security services presence in Australia and New Zealand. Its TSS cover project deployment and technical support for third-party solutions. The key industries for its cyber security services in Australia include the Public Sector, Defense, Health, 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 cyber security now representing more than half its revenue. IBM's TSS offering has full-stack cyber security portfolio, including technology transformation.
- **NTT** offers managed cloud services and IT support services to over 450 global customers that comprise a revenue of US$1 trillion. Its TSS are supported by two SOCs in Australia — one in Sydney and the other in Canberra. NTT Australia has seen very strong recent growth.
- **Telstra's** TSS offering is called Telstra Purple Cyber Security Architecture and Solutions. The services are grouped into 4 domains, namely, Network Security, Endpoint Security, Cloud Security, and Analytics and Automation. Telstra has set an ambitious target of AU$500 million, from these services, by 2025.
- **Tesserent** is a one-stop-shop for cyber security solutions in Australia, including managed security through its SOCs and an NOC. Over the next few years, Tesserent will continue to deliver its Cyber 360 capabilities to an increasing number of Australia-based organisations.
- **Wipro** (Rising Star) is a leading global IT, consulting and business process services provider, headquartered in India. In Australia, the key industries it supports are Retail, Utilities, Government and Education. It has an SOC in Melbourne and development centres in Sydney, Canberra and Perth.

CYBERCX

Overview

CyberCX is an Australia-based cyber security specialist with headquarters in Melbourne, providing end-to-end cyber security services. It was established in 2019 by aggregating 14 Australia and New Zealand based niche cyber security companies. CyberCX has a workforce of over 700 (mostly cyber security) professionals, with offices in Australia and New Zealand that are being consolidated. CyberCX also has a presence in the U.K. Through its TSS, CyberCX acts as an independent cyber security partner for clients through a consultative end-to-end approach.

Strengths

Highly experienced and strong management team: CyberCX is backed by a very strong and highly experience management team. The company provides strategic guidance from multi-disciplined experts and industry leaders in the Cyber security market in Australia and New Zealand. It has decades of experience protecting industry and government in Australia and New Zealand. The companies they brought together to form CyberCX have many cyber security experts with considerable experience in government and private enterprises.

Wide expertise brought in by players involved in company formation: The firms that initially formed CyberCX, are Alcorn, Assurance, Asterisk, CQR, Diamond, Enosys, Gen2, Identity Solutions, Klein & Co, Phriendly Phishing, Sense of Security, Shearwater, Trusted Security Services and Yell IT. This brought to CyberCX a wide range of cyber security services that include consulting and advisory, risk and compliance, security assurance, integration and engineering, training and education, incident response, digital forensics and MSS.

Comprehensive range of services: CyberCX offers a comprehensive range of cybersecurity services, including consulting and advisory; governance, risk and compliance; incident response; penetration testing and assurance; security integration and engineering; cloud and identity security; MSS; and cyber security training. CyberCX has strong knowledge and experience in high security environments, particularly with respect to the Australian Federal Government, through its protected SOC offering. It also has the ability to develop capability and integration solutions to save customers time and additional vendor licensing costs.

Caution

CyberCX lacks the global reach of many of its competitors. In the near future, this potentially increases the risk of it losing market share to a larger competitor that directly targets its product set or makes it a prime target for acquisition.

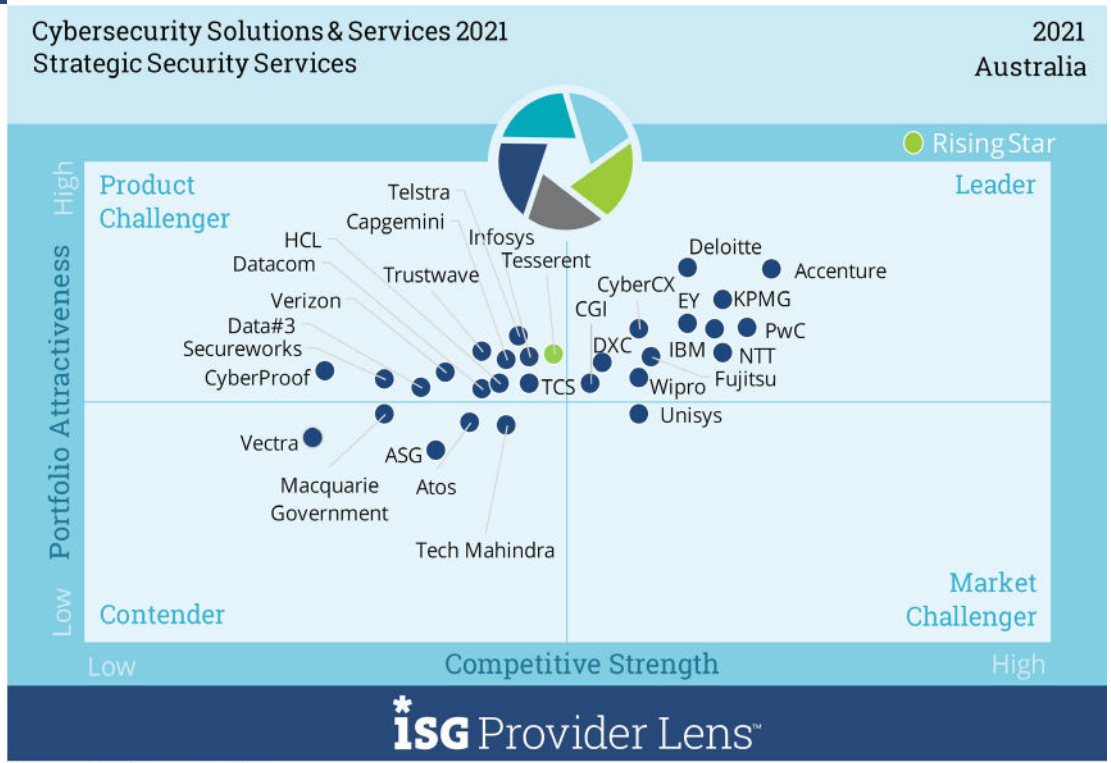
2021 ISG Provider Lens™ Leader

CyberCX is backed by a very strong and highly experience management team. The company provides strategic guidance from multi-disciplined experts and industry leaders in the Cyber Security market in Australia and New Zealand.

STRATEGIC SECURITY SERVICES

Definition

SSS primarily covers consulting for IT security. Some of the 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, risk posture, and define cybersecurity strategy for enterprises. This quadrant examines service providers that do not have an exclusive focus on proprietary products or solutions. The services analyzed here cover all security technologies.



Source: ISG Research 2021

STRATEGIC SECURITY SERVICES

Eligibility Criteria

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

Observations

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

- **Accenture** has a highly comprehensive SSS offering as a part of its professional security services offering. It has been operating in Australia for over 40 years and employs around 5,000 people in six Australian cities, of which half are 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. It has been in Australia for over 40 years, offering services to over 115 clients across Energy, Telecommunications, Government, and Utilities sectors. CGI has nine 24/7 Global Security Operations Centres, including one in Southbank, Melbourne.
- **CyberCX** is an Australia-based cyber security specialist with headquarters in Melbourne. It has a large, highly trained, certified, and experienced onshore national team of security testers, with a physical presence in every major state of Australia. CyberCX has developed a detailed testing process and cyber security methodology.
- **Deloitte** is a major global consultancy with over 8,000 employees and 880 partners in Australia. Sydney is the largest of Deloitte Australia's 14 offices. Deloitte offers a broad range of strategic cyber security services to local organisations, spanning strategic consulting, risk advisory, cyber intelligence information, and vulnerability management services.

STRATEGIC SECURITY SERVICES

Observations (cont.)

- **DXC** employs 10,000 people in Australia. Its SSS are supported by 12 SOCs worldwide, including one in Australia. DXC also has over 30 security solution partners. It has a strong pipeline of cyber security services for the next few years.
- **EY** is a major global consultancy with 299,000 employees worldwide, including more than 6,000 in Australia. It has more than 25 years of experience in cyber security with a large practice, globally. The company has a strong cyber security offering in Australia and maintains an SOC in Melbourne.
- **Fujitsu** has a large MSS practice in Australia and has been operating here for 40 years. Australia is now its most strategic international operation outside Europe and the U.K.
- **IBM** has expanded its MSS offering with the acquisition of over 20 security vendors and service providers over the years. It has more than 8,000 security experts, who share knowledge globally, and 5,000 employees in Australia, with offices in every state and territory.
- **KPMG** Australia has extensive cyber security operations. It recently acquired Ferrier Hodgson, a major Australian management consultancy, and CyberHat, a cyber security solutions company. In Australia, KPMG is particularly strong in Financial Services and the Public sector, and in asset intensive industries such as Mining.
- **NTT's** managed cloud services and IT support services encompass over 450 global customers that contribute US$1 trillion in revenue. Its SSS are supported by two SOCs in Australia — one in Sydney and the other in Canberra. NTT Australia has seen very strong recent growth.
- **PwC** Australia is a global consulting group that delivers audit, assurance, consulting and tax services to more than 5,000 clients in 158 countries, with over 250,000 employees. In Australia, it has a workforce of 8,000, generating AU$2.6 billion in revenue in 2020. It has a large cyber security and privacy practice in Australia. It provides scale and a broad range of cyber, digital risk and related legal services to clients.
- **Wipro** is a leading global IT, consulting and business process services provider, headquartered in India. Wipro's TSS include IAM solutions, data and cloud security and forensic services. It has an SOC in Melbourne and development centres in Sydney, Canberra and Perth.
- **Tesserent (Rising Star)** is the largest cyber security company listed on ASX. It is strategically focused on growing its market share in three verticals, namely, Government Departments and Agencies, Critical Infrastructure and Smart Infrastructure/IoT, and Financial Services.

CYBERCX

Overview

CyberCX is an Australia-based cyber security specialist, with its headquarters in Melbourne. As a part of its strategic services, it has dedicated R&D and capability functions focused on pioneering and improving techniques and practices. In addition to internally developed capabilities, CyberCX security tester's techniques and tools are also informed by interaction with real-world adversaries via its collaboration with CyberCX SOC and Digital Forensics and Incident Response (DFIR) staff.

Strengths

Broad and comprehensive SSS offering: CyberCX's SSS include Cyber Strategic Policy Advice, as well as Cyber Security: Strategic Review, Strategy Design, Target Operating Model and Transformation Roadmap. It also includes CISO as a Service (CISOaaS), Cyber Metrics Board Reporting, Cyber Security Rationalisation and Executive Incident Response Planning and Simulations. Cyber Security Program Development, OT Security Uplift Strategy, Enterprise Cybersecurity Architecture and Due Diligence Assessments are also a part of its SSS.

Highly trained staff: CyberCX has a large, highly trained, certified, and experienced onshore local team of security testers, with a physical presence in every major state of Australia; most of the team has over 25 years of experience in cyber security and IT. The CyberCX team actively maintains a variety of cyber security industry certifications, including Offensive Security Certified Professional, Offensive Security Certified Expert, Offensive Security Web Expert and Certified Ethical Hacker.

Detailed testing process and methodology: CyberCX has developed a detailed testing process and cyber security methodology that aligns with best practices and technical standards, utilising its proprietary knowledge base built through prior security testing engagements and research. All deliverables are peer reviewed and undergo a management review to ensure that they meet strict CyberCX quality standards and are suitable for the intended audience.

Caution

In common with a number of other providers in the Australian market, leadership in the SSS market is increasingly important for taking the high ground in any cybersecurity project. CyberCX faces continued robust competition in this area for local and global players and must continue with its concentrated efforts to maintain its leadership position.

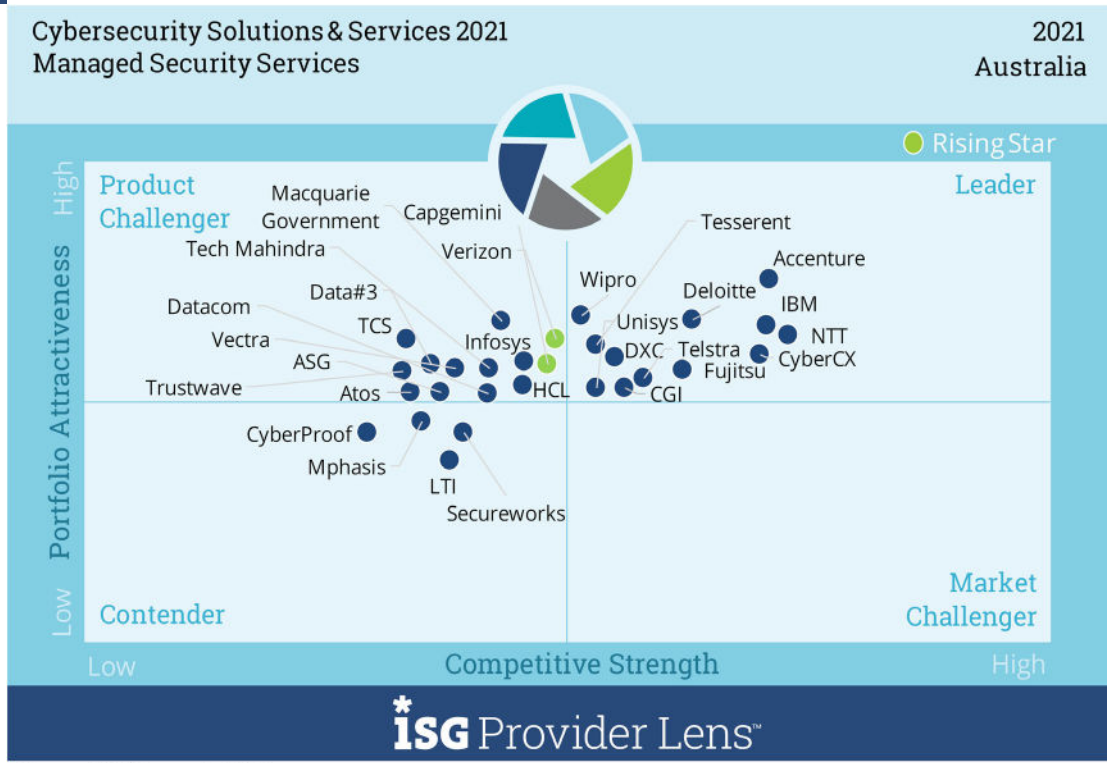
2021 ISG Provider Lens™ Leader

CyberCX is one of the leading end-to-end cyber security service providers. It has a large, highly trained, certified, and experienced onshore local team of security testers, with a physical presence in every major state of Australia.

MANAGED SECURITY SERVICES

Definition

MSS comprises the operations and management of IT security infra-structures for one or several customers by an SOC. 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.



Source: ISG Research 2021

MANAGED SECURITY SERVICES

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

- 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
- Relevance (revenue and number of customers) as an MSS provider in the respective country
- Not exclusively focused on proprietary products but can manage and operate best-of-breed security tools
- Possess accreditations from vendors of security tools.
- SOCs ideally owned and managed by the provider and not predominantly by partners
- 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

Observations

Of the 29 providers in Australia in this quadrant, 12 are Leaders and 2 are Rising Stars:

- **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 Cyber Security industry in Australia.
- **CyberCX** is an Australia-based cyber security 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 cyber security services to Australian organisations, spanning strategic consulting, risk advisory, cyber intelligence information and vulnerability management services.
- **DXC** 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 12 SOCs 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 cyber security 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 cyber security now representing more than half of its revenue. It offers security services for data centre, network, digital workplace, security access and cloud cyber security. It has 5,000 employees in Australia, with offices in every state and territory.

MANAGED SECURITY SERVICES

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 SOCs 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 cyber security company listed on the Australian Securities Exchange (ASX). It is a one-stop-shop for cyber security solutions, including managed security throughout its SOCs and an NOC. 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 cyber security big data platform. Telstra delivers SOC 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 cyber security space in Australia; it generates over 50 percent of its global cyber security revenue from the region. It has offices in Sydney, Melbourne and Canberra, and an SOC in Bangalore.
- **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, cyber security platforms and managed security infrastructure and operations. Wipro has an SOC 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 SOC delivery models. Capgemini has a significant presence in offering MSS in Australia, and has an SOC in Melbourne.
- **Verizon's** (Rising Star) 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.

CYBERCX

Overview

CyberCX is an Australia-based cyber security specialist, with headquarters in Melbourne, that is recognized as one of the leading end-to-end cyber security service providers. in the Southern Hemisphere. It responds to over 200 security incidents, per year, and over 500 cyber security baseline assessments, per year. As a part of its MSS offering, CyberCX utilises its Australia or New Zealand Sovereign (onshore) SOCaaS offering, as well as a "follow the sun" coverage model, leveraging three countries.

Strengths

Industry leading SOCaaS offering: CyberCX offers a 24x7 SOCaaS solution, including management and monitoring of managed SIEM (cloud, on-premises and hybrid), vulnerability management, endpoint detection and response, digital brand protection and breach and attack simulation. These are offered as fully onshore services in Australia/ New Zealand via continuous staff monitoring during business hours and out of hours by an automated alerting and pager system. CyberCX also offers these services via 24/7 staff monitoring services, as a "follow the sun" model between the U.K., Australia and New Zealand. In addition, it offers managed SD-WAN, firewall, proxy, CASB, DLP, storage, server and endpoint security solutions.

Strong cyber intelligence offering: CyberCX's dedicated cyber intel team synthesises learnings from its local practice to create unique threat identifying packages for its SOC analyst teams. It has a strong ethos of partnering with its customers, and the ability to blend traditional managed security services with a broad range of offerings, including digital forensics, GRC, strategy and consulting, penetration testing, red teaming, IAM, cloud security and professional services (design and build).

Scale and breadth of offering: CyberCX has over 150 employees in its Security Testing and Assurance practice. This makes CyberCX's security testing, application security and training team one of the largest in the APAC. It has undertaken thousands of security tests in the past year in Australia, discovering many security vulnerabilities. Many of these vulnerabilities were discovered for the first time by its consultants and disclosed to customers, vendors and appropriate parties for remediation. These tests and resulting security recommendations have led to significant security improvements for CyberCX clients across its systems, applications, infrastructure and operations.

Caution

CyberCX has made great progress in integrating a broad range of technical solutions services providers and capabilities, however, needs to do more work to differentiate its portfolio in the market.

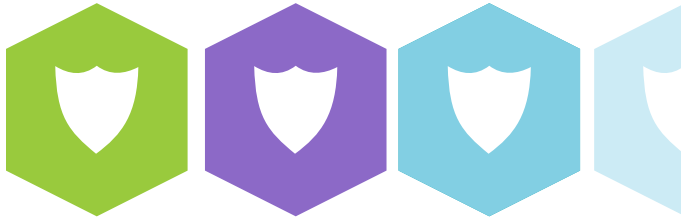
2021 ISG Provider Lens™ Leader

CyberCX provides a packaged best-of-breed offerings from leading global security vendors such as Splunk, CrowdStrike, Tenable. It also provides vendor-agnostic offerings that have the ability to service legacy SIEM tools.

Methodology

METHODOLOGY

The research study "2021 ISG Provider Lens™ Cyber Security – Solutions & Services Australia" 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. The study was divided into the following steps:



1. Definition of 2021 ISG Provider Lens™ Cyber Security – 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

Distinguished 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).

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
June 2021

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.