ISG Provider Lens™

Cybersecurity – Solutions and Services

A research report comparing provider strengths, challenges and competitive differentiators

Customized report courtesy of:

AC3

SWEET SPOT | JUNE 2023 | AUSTRALIA

Table of Contents

© 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Report Author: Andrew Milroy

Recent high-profile attacks in Australia led to a reevaluation of cybersecurity postures

Australian consumers and companies have recently been exposed to enormous and damaging data leaks. These leaks have made headline news and various perspectives have been shared by diverse groups of people — ranging from customers of the affected companies to government officials.

It is probable that too many large organisations — not only in Australia but around the globe — have similar vulnerabilities as those exposed in the recent criminal cyber attacks. No organisation can be completely safe from breaches. There is always a privileged user falling for a phishing attack, or a dishonest insider or a negligent employee making a mistake, exposing their organisations to breaches.

Indeed, insider threats such as developers not securing API endpoints — or employees with access to sensitive data falling prey to phishing attacks and sharing credentials — are thought to have played a major role in recent data leaks in Australia and elsewhere.

The growing importance of cybersecurity changes the way Australian enterprises procure cybersecurity services. Senior management gets increasingly involved in the decision-making on cybersecurity products and strategies and expresses interest in understanding all the aspects of cyber risks. Increased awareness of cyberattacks and strict regulations and legislation further raise cybersecurity standards.

Organisations now take an "assume breach" approach to cybersecurity. They recognize that not all breaches can be prevented. Hence, they place greater focus on detecting and responding to breaches as rapidly as possible.

Due to the far-reaching consequences of cyberattacks for an organisation's reputation, brand and shareholder value, security has transitioned from solely an IT concern

Australian organisations place greater focus on **detection and response** capabilities.

 © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

to an enterprise risk challengethat now is more closely monitored at the top level of an organisation.

In the post-COVID world, customers move more aggressively to a cloud-first environment. They re-evaluate their operational priorities and place security and privacy at the top of their digital transformation agendas.
As a result, there is an increasing need for security organisations to demonstrate positive returns on investment for cybersecurity spending and initiatives.

Recent high-profile attacks have shown that Australian organisations face an escalating and sophisticated threat environment. Criminals now target businesses and government organisations with the most advanced protections and controls. This forces Australian businesses and government organisations to make cybersecurity a strategic imperative.

The Notifiable Data Breaches (NDB) scheme has been implemented in Australia, requiring organisations to report data breaches to affected individuals and the Office of the Australian Information Commissioner (OAIC). This has led to an increased focus on data privacy and security and a greater emphasis on implementing robust security measures against data breaches.

The Australian Cyber Collaboration Centre has been established in Adelaide's Lot Fourteen as a not-for-profit, mission-driven organisation to make cyberspace a safe arena to conduct business. Adelaide's Lot Fourteen is the largest innovation precinct in the southern hemisphere, with over $1 billion in federal and state government and industry funding. The Centre aims to leverage resources and expertise from businesses of all sizes, the government and research institutions, incubate solutions and initiatives, and develop offerings to drive a more cybersecure digital economy. Cybersecurity is one of the many high-tech sectors getting focus within the precinct.

Australian is one of the many countries that have issued cybersecurity mandates and guidelines to protect critical infrastructure, many of which are grounded in a zero-trust cybersecurity model.

Australian organisations demand simple and flexible cybersecurity solutions. Cybersecurity providers should focus on developing more comprehensive offerings targeting an increasingly diverse customer base while adapting to their rapidly changing needs.

Digital transformation initiatives leveraging cloud technologies and enabling remote working are driving demand for more cybersecurity solutions in Australia. Over the next few years in Australia, there will likely be a strong demand for cloud-based detection and response solutions, such as extended detection and response (XDR).

The Australian Security market is expected to grow strongly over the next five years to 2025. More jobs are needed to support Australia's rising demand for cybersecurity services over the next five years. In addition, many roles across businesses and the government will need increased cyber awareness and skill levels. Due to cyber threats and data privacy concerns and regulations, AI in cybersecurity is likely to grow exponentially with the adoption of IoT. Next-gen Identity and Access Management, messaging and network security will be key for enterprise cybersecurity investments over the next one to two years.

Recent attacks have shown that Australian companies' cyber maturity is very low. Given the increased frequency and impact of attacks, Australian companies need to assess their risk tolerance and existing controls and seek more mature postures, which can offer greater risk mitigation. Typically, Australian companies have already invested heavily in cybersecurity controls. But these investments are focused only on preventing breaches, have limited access controls and are based on the assumption that sensitive data is accessed from office locations.

Increased digital engagement, widespread remote working and greater use of IoT collectively expand attack surfaces and expose many cybersecurity postures as inadequate. Companies often combat threats with multiple cybersecurity tools, often with separate dashboards. Too many false-positives are generated across these tools, often requiring manual intervention. High automation and interoperability between tools are urgently required to take the pressure off

© 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

security operations centres (SOCs) and address burgeoning cybersecurity skill shortages.

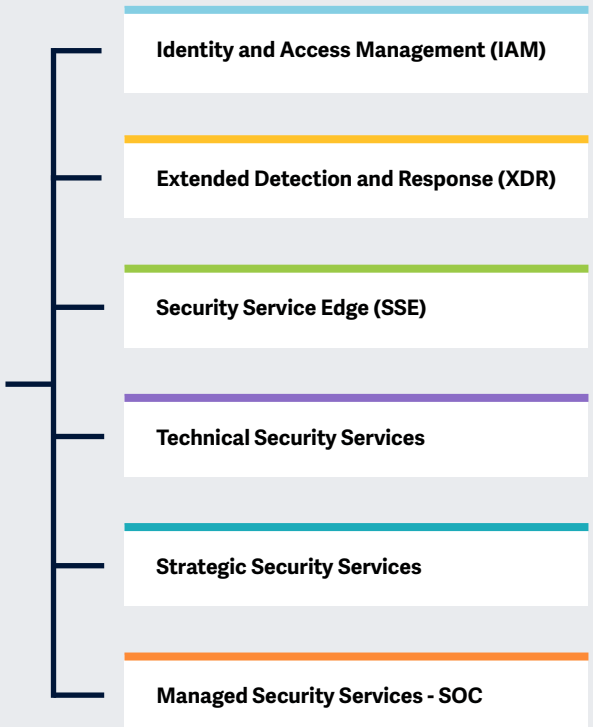
These challenges can be addressed by gradually developing a cybersecurity posture that allows continuous monitoring of internal assets, combined with the ability to adapt to changing threats and regulatory environments.

Australian cybersecurity decision-makers are aware that progress in the cyber maturity journey is not easy. Perhaps now is the time for companies to step back, assess risks and risk tolerance, evaluate current controls, identify the gaps and put people and processes in place to implement an adaptable posture — aligned with acceptable risk levels and new more distributed technology environments. Establishing cybersecurity policies and processes should precede cybersecurity technology investments. After all, the role of technology is to implement these policies and processes. Companies often buy technology reactively when they encounter a threat and pay insufficient attention to policies, people and processes.

Increases in digital engagement, remote working and IoT expand attack surfaces and expose inadequacies in cybersecurity postures. Australian companies use multiple cybersecurity tools, with separate dashboards, to fight threats. Too many false-positives are generated across these tools, often requiring manual intervention. High automation and tool interoperability are urgently required to relieve security operations centres and address skill shortages.

© 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

This study focuses on what ISG perceives as most critical in 2023 for **Cybersecurity decision-makers**



Simplified Illustration; Source: ISG 2023

Definition

The year 2022 could be termed as tumultuous from a cybersecurity perspective; although there was a decrease in data breach incidents, the year saw significantly increased sophistication and severity in the attacks. In 2022, enterprises increased their investment in cybersecurity and prioritized relevant initiatives to prevent attacks and improve their security posture. The continued learnings from the 2021 attacks led to executives and businesses of all sizes and across industries investing in measures to respond to and survive cybersecurity threats and cyberattacks.

From an enterprise perspective, even small businesses understood the impact of cyber threats and realized that they are actively targeted and are highly vulnerable to cyberattacks. This reinforced the need for (managed) security services and cyber resiliency services that would enable businesses to recover and resume operations quickly after a cyber incident. Service providers and vendors are, therefore, offering services and solutions that help in recovery and business continuity.

From the perspective of the cybercriminals, they began exploiting large-scale vulnerabilities, such as Log4shell, and continued using ransomware to disrupt business activities, specifically targeting healthcare, supply chain and public sector services.

These prompted businesses to invest in capabilities such as identity and access management (IAM), managed detection and response (MDR) and securing cloud and endpoints. The market is shifting toward integrated solutions, such as security service edge (SSE) and extended detection and response (XDR), which leverage the best tools and human expertise and are augmented with behavioral and contextual intelligence and automation to deliver a superior security posture.

© 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Sweet Spot

AC3

Overview

AC3, established in 1999 and based in Sydney, has approximately 400 employees. The company offers a range of cybersecurity capabilities across cloud, infrastructure and application platforms for clients in Australia. It has a strong history of serving the government sector and not-for-profit clients. It also has a growing enterprise business that is expected to help drive the next generation of growth.

Key Provider Capabilities

Managed detection and response

Modern attacks such as ransomware and advanced phishing are common and becoming increasingly complex. These attacks require next-generation services such as endpoint detection and response, SIEM and XDR to provide a holistic approach to security monitoring, which can identify more threats and help you close more security gaps than traditional technologies. AC3's solutions are designed to use cloud-based analytics to enable a more dynamic and proactive approach to security and ensure total coverage.

Perimeter protection

In today's hybrid cloud world, where much of the workforce works remotely, protecting your businesses from security breaches is getting more complex. AC3's managed perimeter protection services protect an ever-changing perimeter.

Email and web security

Protecting employees from threats via email and websites is critical. The weakest link in security chains is often the endpoint, so working with AC3 to provide best-of-breed email and web security platforms can keep employees and corporate reputations safe, regardless of device or location.

Vulnerability assessment and management

Identifying weaknesses in security posture is essential. AC3 provides simulated cyberattacks by ethical security experts, identifying improvement areas. This can help organisations meet compliance requirements and/or reduce risk substantially.

Benefits Delivered

- **Extensive government expertise**
- **Focus on compliance and best practices**
- **Deep knowledge transfer with certified experts and cross-industry expertise**
- **Ability to provide end-to-end services, over and above typical MSSP offerings, because of closely coupled cloud business**
- **Precleared staff due to defence industry security program membership**

© 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

AC3

Sweet Spot

AC3's sweet spot is its government heritage. It acquired a large portion of its business and people from the New South Wales State Government in 2013. This gives the company the rigour of process, security clearances, qualifications and compliance that government requires. As regulatory pressure intensifies in the Australian market, these capabilities are critical to all Australian organisations.

The company is Australian-owned and operated, addressing growing concerns around data sovereignty and nation-state attacks. All security staff are Australian citizens or permanent residents, and the staff that holds security clearance are all Australian citizens.

Specific dimensions of AC3's approach include the following:

- **Customised threat intelligence:** Rather than provide an *off-the-shelf* threat intelligence solution, AC3 customises threat intelligence to meet specific customer requirements and further bolsters this with indicators of compromise (IOCs) identified as part of incident response or threat hunting, providing a form of herd immunity.
- **Transparency and focus on customer outcomes:** The customer's view is the same as that of SOC analysts. The customer has full ownership of data giving it more control of MSS activities.
- **Culture of accountability:** Customers can access someone with authority to make decisions when a requirement emerges. AC3 has a deep understanding of its customers and can offer high levels of customer intimacy.
- **Strong cloud expertise, particularly around AWS and Azure:** This strengthens the company in all aspects of cloud security and threat detection.

Future roadmap

AC3 expects its strong growth to continue in 2024. It is expanding its MSS offerings by introducing both platforms and managed services for:

- Dark web and data breach monitoring
- Hybrid and multicloud workload protection and cloud-native application protection
- Microsoft Defender threat intelligence and external attack surface management

© 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Appendix

The ISG Provider Lens™ 2023 – Cybersecurity Solutions and Services report analyzes the relevant software vendors/service providers in the Australian market, based on a multi-phased research and analysis process, and positions these providers based on the ISG Research™ methodology.

Lead Authors:
Andrew Milroy and Phil Harpur

Editors:
Kondappan S and John Burnell

Research Analyst:
Angie Koh

Data Analysts:
Rajesh Chillappagari and Shilpashree N

Consultant Advisor:
Anand Balasubramanium

Project Manager:
Donston Sharwin

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 April 2023, for providers who actively participated as well as for providers who did not. ISG recognizes that many mergers and acquisitions have taken place since that time, but those changes are not reflected in this report.

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

The study was divided into the following steps:

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

 © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Author

Andrew Milroy
Lead Analyst

Andrew is a well-known and respected thought leader and speaker in the APAC region. He is currently part of the DataDriven team, which is the Asia Pacific research partner for ISG. With more than two decades of experience in the technology sector, Andrew has worked with clients in a variety of tech domains including cybersecurity, telecoms strategies, cloud computing, IoT, AI, intelligent automation and customer experience. His most recent work has been focused on advising clients on cybersecurity transformation.

Since moving to Singapore in 2011, he has held regional leadership roles with Frost & Sullivan and Ovum (now Omdia). Prior to working in Singapore, Andrew gained invaluable technology knowledge and insights while working in Europe, the United States and Australia.

Andrew is the founder of cybersecurity advisory firm Veqtor8.

Co-author

Phil Harpur
Principal Analyst

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

Phil is currently part of the DataDriven team, which is the Asia Pacific research partner for ISG, and has contributed to the creation of nine ISG Provider Lens™ reports. Prior experience includes work with Gartner, Frost & Sullivan, and BuddeComm.

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

© 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Author

Gowtham Kumar Sampath

Assistant Director and Principal Analyst

Gowtham Sampath is a Senior Manager with ISG Research, responsible for authoring ISG Provider Lens™ quadrant reports for Banking Technology/Platforms, Digital Banking Services, Cybersecurity and Analytics Solutions & Services market. With 15 years of market research experience, Gowtham works on analyzing and bridging the gap between data analytics providers and businesses, addressing market opportunities and best practices. In his role, he also works with advisors in addressing enterprise clients' requests for ad-hoc research requirements within the IT services sector, across industries.

He is also authoring thought leadership research, whitepapers, articles on emerging technologies within the banking sector in the areas of automation, DX and UX experience as well as the impact of data analytics across different industry verticals.

Research Analyst

Angie Kho

Regional Support Analyst

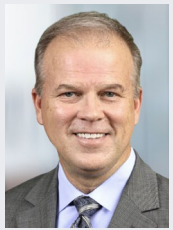
Angie Kho is a regional support analyst at ISG and is responsible for supporting and contributing to Provider Lens™ studies for the APAC markets.

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

Her areas of expertise lie in IT services management and enterprise planning services. Angie develops content from an enterprise perspective and writes Global Summary reports for Provider Lens studies. She also supports the lead analysts in the research process and ad hoc research assignments.

© 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

IPL Product Owner



Jan Erik Aase

Partner and Global Head – ISG Provider Lens™

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

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

© 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

ISG Provider Lens™

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

For more information about ISG Provider Lens™ research, please visit this webpage.

ISG Research™

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

ISG offers research specifically about providers to state and local governments (including counties, cities) as well as higher education institutions. Visit: Public Sector.

For more information about ISG Research™ subscriptions, please email contact@isg-one.com, call +1.203.454.3900, or visit research.isg-one.com.

ISG

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 900 clients, including more than 75 of the world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis.

Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,600 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 isg-one.com.

© 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

ISG Provider Lens™

JUNE, 2023

REPORT: CYBERSECURITY – SOLUTIONS AND SERVICES

© 2023 Information Services Group, Inc.
All Rights Reserved