

Australia and New Zealand Digital Trust and Security

AN IDC REPORT SERIES

IDC's *Australia and New Zealand Digital Trust and Security* series provides a comprehensive look at the full breadth of the cybersecurity market that includes professional security services, managed security services, security software, security appliances, security support, and security training/education services markets. In addition, it also covers topics related to blockchain, or distributed ledger technology, which has recently emerged in several businesses beyond the financial services industry.

Markets and Subjects Analyzed

- This research examines market trends, customer preferences and buying behavior, and emerging new security software/services opportunities such as predictive security, cyberinsurance, mobile security, IoT security, blockchain/DLT, and security as a service.
- The service also provides an analysis of existing and emerging players for the Australian cybersecurity/blockchain market.

Core Research

- Australia and New Zealand Threat Life-Cycle Services
- Australia and New Zealand Managed Security Services, 2018
- State of Blockchain and Cryptocurrency Legislation in Australia and New Zealand
- Distributed Ledger Use Cases in Australia and New Zealand
- Managed Security Services: Vendor Assessment Criteria

In addition to the insight provided in this service, IDC may conduct research on specific topics or emerging market segments via research offerings that require additional IDC funding and client investment. To learn more about the analysts and published research, please visit: [Australia and New Zealand Digital Trust and Security](#).

Key Questions Answered

1. What are the key areas of growth by country, industry, and functional markets for security (services/software/appliances)? What are the market shares and competitive positioning of the leading vendors?
2. What are IT buyers' priorities, challenges, and spending plans for security (services/software/appliances) in Australia, and how can vendors address them?
3. How is the security services/security software/blockchain competitive space evolving, and what are the key recommendations for vendors?
4. How can end users leverage security services/security software/blockchain? Which are the key buyer use cases in Australia? Which are the top solutions?
5. How will blockchain, or distributed ledger technology, change what we do? What are some use case examples of where blockchain can be or is being used in Australia?

Companies Analyzed

This service reviews the strategies, market positioning, and future direction of several providers in the Australian cybersecurity market, including: Accenture, Check Point, Cisco, Fortinet, Hewlett Packard Enterprise, IBM, Intel, Juniper, Microsoft, Palo Alto Networks, SonicWall, Symantec, and WatchGuard.