

Dimension Data's Managed Intrusion Detection and Prevention Service

A robust security infrastructure is essential to conduct business successfully in a networked

world. Firewalls and other barriers are a good start, but intrusion detection and prevention systems provide an extra layer of protection that improve the ability to respond to potential intrusions or unauthorised behaviour before they become serious security breaches. Intrusion detection and prevention systems are, however, complex technologies that are difficult to manage and maintain. They generate large volumes of complex data and alerts, which require rapid, accurate analysis and interpretation to truly reduce risk. This level of vigilance requires time, effort and specialised expertise... and focusing your internal IT department's energies on monitoring and managing intrusion detection and prevention systems means you have less time to execute strategic business activities.

If you're seeking to implement intrusion detection and prevention systems, without devoting costly internal resources to manage, maintain and monitor the systems, Dimension Data's Managed Intrusion Detection and Prevention Service can help. We offer a fully managed, 24/7/365 service that protects networks from attack and misuse, using network-based intrusion detection and prevention systems.

'If you're seeking to **implement intrusion detection** and **prevention systems**, without devoting costly internal resources to manage, maintain and monitor the systems, **Dimension Data's Managed Intrusion Detection and Prevention Service can help**.'

The service provides:

- Around-the-clock protection: true continuity of process and constant vigilance.
- Support for solutions from marketleading vendors: Cisco, McAfee, Juniper, Sourcefire, Tipping Point, Palo Alto, IBM, Fortinet, Industrial Defender and Snort.
- **Turnkey daily management:** including fine-tuning of filters, software upgrades and patches, and system configuration.
- Rapid intrusion identification, escalation and response using proven processes that ensure security events are responded to and escalated quickly.
- Client security portal: that provides the intelligence and analytics you need to easily understand your risks, demonstrate compliance and make better security decisions. The client security portal gives you full visibility into your security and compliance posture with advanced reporting functionality integrated across all of our Managed Security Services.

Benefits to you:

- **Improved security posture**, delivering a stronger return on investment than you'd achieve by managing the system internally.
- **Reduced costs** associated with hiring, training, managing and retaining high quality security engineering personnel.
- **Improved agility** by freeing up your internal resources to focus on your core business outcomes and requirements.
- Access to Security Operations Centre (SOC): for 24/7 support and escalated engineering.

- Certifications: AS/NZS 27001, ASIO T4, ISO/IEC 27001:2005, Defence Signals Directorate (DSD) certified gateway up to protected classification level and PCI DSS.
- Access to critical security data: including detailed analysis, summary overviews and customised query reports.
- Business intelligence: the client security portal features integrated business intelligence and analytics tools to help you gain the meaningful insights and new perspectives you need to answer these questions and make better security decisions. Highly customisable data visualisations and reports give you point-in-time snapshots as well as historical trending perspectives across multiple security metrics.
- Security reporting: To help demonstrate security effectiveness and reduce the burden of compliance reporting, client security portal provides you with an extensive set of pre-built reports for security and compliance. Reporting has been specifically designed to help clients demonstrate adherence to regulatory requirements and provide enterprisewide visibility into the performance of security controls.

The service elements include:

Service elements	Essential	Advanced
Client take-on	 ✓ 	 ✓
Event management		
Performance and availability monitoring and notification	 ✓ 	V
Security information and event management • Log collection • Log filtering • Log aggregation • Log categorisation • Log normalisation • Log forwarding • Log mining • Log correlation	×	V
Global intelligence correlation	×	V
Vulnerability scan data correlation	×	V
Content aware monitoring	×	V
Context aware monitoring	×	V
Predictive intelligence	×	V
Incident management		
Security incident management • Phase 1: security incident identification • Phase 2: security incident investigation • Phase 3: security incident response & containment • Phase 4: security incident rectification • Phase 5: restart • Phase 6: monitoring	×	V
Remote incident diagnosis and troubleshooting	V	V
Workaround or permanent resolution identification	V	V
Workaround or permanent resolution implementation	V	 ✓

data sheet | Dimension Data's Managed Intrusion Detection and Prevention Service

Service elements	Essential	Advanced
Service asset and configuration management		
Configuration and rule-base backup	V	V
Patch release notification	V	V
Asset inventory management	 ✓ 	
Role-based access control	V	
IDS/IPS policy tuning	×	V
Vulnerability scanning service	V	V
Change management		
Change request process	 ✓ 	
Configuration and rule-base administration	V	V
Release and deployment management		
Patch installations	V	
Configuration and rule-base restore	\checkmark	\checkmark
Signature update maintenance	\checkmark	\checkmark
Reporting		
Threat intelligence service	\checkmark	V
Online searching and reporting	×	V
Monthly reporting (system generated)	×	V
Report validation and review	×	Optional
Core service elements		
Service desk	<i>v</i>	v
Escalation management	<i>v</i>	
Request fulfilment	 ✓ 	V
Client security portal	×	V
MACD service units	 ✓ 	V
Service management • Client Services Manager • Service management reporting • Service review meetings	Optional	Optional

Why Dimension Data?

- Broad technical and integration expertise across a variety of IT disciplines, including networking, security, unified communications and collaboration, data centres, virtualisation, Microsoft and contact centres.
- **Strategic partnerships** with leading security technology vendors, including Cisco, Check Point, Blue Coat, RSA, McAfee, Zscaler, Juniper, Sourcefire, Imperva, Palo Alto, Fortinet and ArcSight.
- Proven track record: over 6,000 security clients across all industry sectors, including financial services, telecommunications, health care, manufacturing, government and education.
- Global footprint, local delivery: with over 14,000 employees and operations in 52 countries across five continents, Dimension Data manages more than USD12.5 billion of network infrastructure through five Global Service Centres on a 24x7 basis, in more than 15 languages.
- Real-time security information and event management **architecture:** an enterprise-wide risk management solution enabling our SOC analysts to centrally manage attacks, threats and exposures by correlating security information from firewalls, intrusion detectors, virus scanners, VPNs, operating systems, authentication solutions, vulnerability scanning tools and other security checkpoints. The solution enables our analysts to eliminate clutter such as false-positives, while quickly identifying the real security threats to help them respond with adaptive

security measures.

• Security Operations Centres:

our SOCs serve as the command, control and communications centre for all Dimension Data security operations and customer support centres. Staffed 24x7 with three teams, namely the Watch Team, Response Team and Forensic Team, dedicated to maintaining the highest quality of service. The SOCs utilise state-of-the-art equipment and technology for monitoring and managing the network and identifying and resolving problems.

- Security experts: our team of certified security experts brings a century of combined cyber security experience with organisations such as CERT, Department of Defence, IBM and Cisco, to augment the knowledge base of your IT organisation and provide peace of mind that skilled technicians are there to help you respond to and mitigate threats.
- Certifications: ISO9001, ISO 27001 Australian Signals Directorate (ASD) Protected Gateway, PCI DSS, Cisco MSCP, Information Security Manual (ISM) and ASIO T4.

Dimension Data creates, integrates and manages your security infrastructure in a way that supports your business goals. We offer a broad portfolio of security services coupled with proven technologies from a select group of innovative partners. Our security professionals are recognised for their depth of expertise and passionate client delivery. They're globally connected to bring you the best solutions for your security needs, delivered anywhere in the world.

Contact us

For more information, please contact your nearest Dimension Data office or visit http://www.dimensiondata.com



Middle East & Africa Algeria - Angola Botswana - Congo - Burundi Democratic Republic of the Congo Gabon - Ghana - Kenya Malawi - Mauritius - Morocco Mozambique - Namibia - Nigeria Oman - Rwanda - Saudi Arabia South Africa Tanzania - Uganda United Arab Emirates - Zambia

Asia China • Hong Kong India • Indonesia • Japan Korea • Malaysia New Zealand • Philippines Singapore • Taiwan Thailand • Vietnam

Australia Australian Capital Territory New South Wales • Queensland South Australia • Victoria Western Australia

Europe Belgium • Czech Republic France • Germany Italy • Luxembourg Netherlands • Spain Switzerland • United Kingdom

Americas Brazil • Canada • Chile Mexico • United States

For contact details in your region please visit www.dimensiondata.com/globalpresence

www.dimensiondata.com