



Orchestrating a brighter world



Security Device Management

Lower risk exposure, protect your assets
and maximise technology investments

nec.com.au 

Lower risk exposure,
protect your assets and
maximise technology
investments



Why Security Device Management?

In today's ever evolving cybersecurity threat environment, managing security devices is essential for securing your businesses information, protecting data privacy and meeting compliance obligations.

Ensuring ICT security is strong and remaining vigilant to protect information assets, employees and customer data, and ultimately protecting the reputation of the business is paramount.

Security devices must be properly configured, updated, and patched to protect against internal and external threats. Simply deploying security devices is not enough to protect customer data and networking infrastructure.

We understand managing security devices can be challenging for organisations. From knowing what vulnerabilities exist; and if they do what updates to apply, what steps are involved, the urgency, the business risk, and having the skilled resources to protect your data requires expertise and can be costly.



Common Challenges

When facing security device management, your organisation can expect to encounter some, or perhaps all of these challenges. That's why NEC is here to guide you with its expertise.

NEC Security Device Management

Service Overview

NEC's highly skilled security experts today are actively assisting businesses, government, and enterprises to identify security device weaknesses and vulnerabilities before anyone attempts to exploit them. NEC delivers these services through our ISO 27001 certified Security Operations Centre (SOC). NEC's security experts have vendor certifications and experience in supporting technology that we manage, which can reduce security administration overheads and allowing your expensive

internal staff to focus on other core business functions. NEC Security Device Management service offerings are tiered, starting with our Essentials services that cater to low risk device deployments through to our Standard service packages for moderate risk environments through to our Premium service offerings for customers with highly available, multi-tiered, high-risk security deployments.



There are three services in the
Security Device Management portfolio

Available as standalone or bundled

Managed Firewall and Next-Generation Firewall Service

NEC's Managed Firewall and Next-Generation Firewall Service provides customers with a monitoring and management service to protect your organisations' private networks from unauthorised access. The service provides security policy enforcement across all the firewall capabilities that your organisation has enabled ensuring protection of your information systems, employees, business partners and connections to untrusted networks.

All our services deliver 24x7 proactive firewall configuration management, monitoring, systems support and reporting services. The service has been carefully designed to fit the diverse requirements of today's connected enterprises. From small and remote offices to large scale deployments, NEC has a managed firewall service designed to align with each individual organisation's security requirements and budgetary requirements.

The average cost of a data breach around the world is \$3.86 million*

Managed Intrusion Prevention Service (IPS)

NEC's Managed Intrusion Prevention Service (IPS) is a 24x7 availability monitoring and management service that ensures that your IPS device has its signature database updated regularly and is set to utilise vendor recommended settings. Through ongoing IPS tuning NEC security experts ensure that false positives are remediated and that relevant signatures are enabled to suit your business.

The service ensures that your intrusion prevention service is optimised and providing reliable and comprehensive protection for networks and servers against threats and unauthorised intrusions from both internal and external sources.

Managed Reverse Proxy and Load Balancer

NEC's Managed Reverse Proxy and Load Balancer application services provides customers with a 24x7 management service that includes security device systems administration, configuration, support, capacity management, availability monitoring, report generation and validation of security advisories.

The service ensures that your application performance is optimised enhancing user experience through providing a reliable, secure, and optimised application delivery. Our security device management service supports a wide range of technology platforms from vendors such as Cisco, Check Point, Juniper, Palo Alto, Fortinet, F5, Citrix, A10 Networks, Symantec, McAfee, and Tipping Point.

* Source: 2018 Cost of a Data Breach Study by Ponemon. \$ in USD.

What are the Benefits?

With NEC Certified Professionals watching over your network and devices, we give you peace of mind to get on with your day to day business.



Flexible service and tiered approach, only pay for the level of service you need



Reduced cost of ownership by leveraging NEC expertise. Save on FTE and training costs



Increased compliance as devices will be managed according to vendor specifications



Enhanced protection of staff and customer data



Reduced time to identify and remediate device weaknesses and vulnerabilities



Improved security posture by lowering risk exposure and maximise technology investments



Regular reporting facilitates improved planning and decision making



24x7 service option providing device availability and performance assurance



Reduction in potential damages / cost of breaches and un-necessary spend



Managed by experts. Leverage NEC's certified Security Operations Centre (SOC) team

Learn more

For more information on Security Device Management service package options, visit nec.com.au or if you are reading this on your preferred device; simply click on the service package buttons located on the right to download a datasheet for each service.



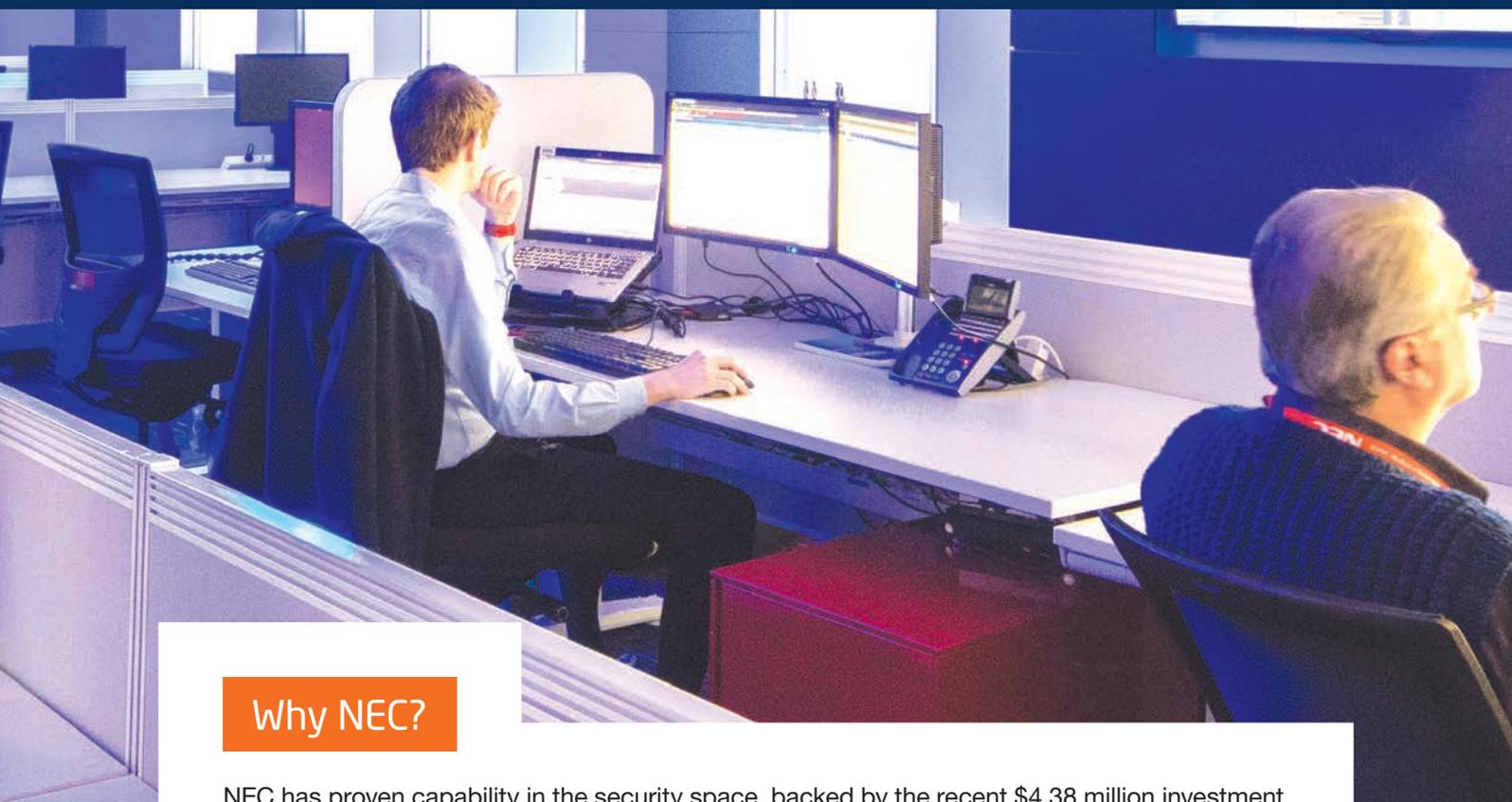
Managed Firewall
and Next Generation
Firewall Service



Managed Intrusion
Prevention Service



Managed Reverse Proxy
and Load Balancer Service



Why NEC?

NEC has proven capability in the security space, backed by the recent \$4.38 million investment in the new GSIC (Global Security Intelligence Centre) facility located in Adelaide.

This offers a wide range of security services delivered from the state of the art Security Operation Centre. It also offers extended benefits to clients and goes hand in hand with wider investments made globally that include Japan, Singapore, Europe, and the Americas to offer true global coverage.

NEC currently employs over 1600 staff across Australia and over 100,000 worldwide, offering local capability, national capacity and global coverage.



For more information:

 nec.com.au

 contactus@nec.com.au

 131 632

Corporate Headquarters (Japan)
NEC Corporation
www.nec.com

Australia
NEC Australia Pty Ltd
www.nec.com.au

North America (USA)
NEC Corporation of America
www.necam.com

Asia Pacific (AP)
NEC Asia Pacific
www.sg.nec.com

Europe (EMEA)
NEC Enterprise Solutions
www.nec-enterprise.com

NEC Australia Pty Ltd reserves the right to change product specifications, functions, or features, at any time, without notice. Please refer to your local NEC representatives for further details. Although all efforts have been made to ensure that the contents are correct, NEC shall not be liable for any direct, indirect, consequential or incidental damages resulting from the use of the equipment, manual or any related materials. The information contained herein is the property of NEC Australia Pty Ltd and shall not be reproduced without prior written approval from NEC Australia Pty Ltd.

©2021 NEC Australia Pty Ltd. All rights reserved. NEC and NEC logo are trademarks or registered trademarks of NEC Corporation that may be registered in Japan and other jurisdictions. All other trademarks are the property of their respective owners. All rights reserved. Printed in Australia. Note: This disclaimer also applies to all related documents previously published.

NEC