

# Managed Intrusion Prevention Service

## Optimised IPS that provides reliable and comprehensive protection

Intrusion Protection technologies help protect you from known and zero-day threats using signature analysis, threat feeds applying AI and ML, to secure your networks, on-premises and or public cloud infrastructure.

### NEC's 24x7 Managed Intrusion Prevention Service (IPS):

- ✓ monitors your networks, on-premises and or public cloud infrastructure at the edge
- ✓ ensures your signature database is updated regularly and is configured correctly to utilise your vendor recommended settings
- ✓ applies global threat intelligence, automation, and machine learning to detect threats
- ✓ defines and applies security policies aligned to your specific environment

Our intrusion prevention service will continually optimise your IPS device to provide reliable and comprehensive protection for your networks and servers against threats and unauthorised intrusions from both internal and external sources.

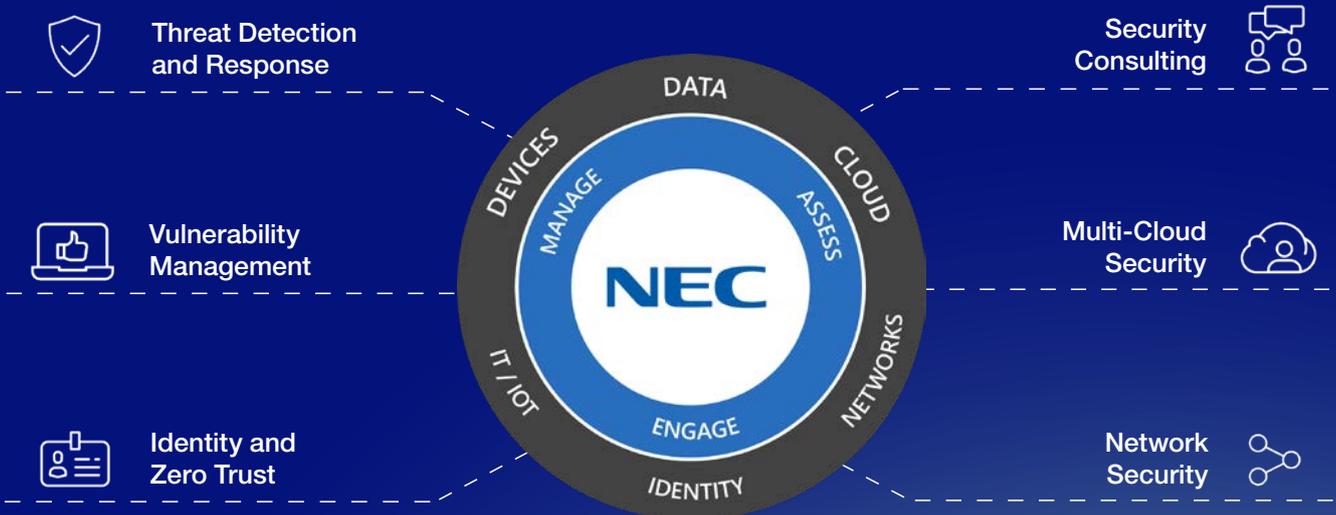
## Key customer benefits

- ✓ **Improve your reaction time to threats** - reduce the time to identify and remediate device weaknesses and vulnerabilities leveraging NEC's certified Security Operations Centre (SOC) team
- ✓ **Decrease your cost of ownership** – options are available to manage your security spend from adopting either an Opex model or NEC can manage your existing devices
- ✓ **Leverage onshore security experts** – our security analysts are certified and experienced across a range of IPS technologies to provide support from design, implementation and operating.
- ✓ **Enhance your data security and compliance** – robust and regular reporting to assist you with responding to audits and meeting compliance requirements
- ✓ **24x7 monitoring** - regular monitoring, optimised for your device, focusing on device availability and performance assurance to support better decision making

NEC Australia has been providing local support to our customers since 1969. We have proven long-term network monitoring and management experience across large enterprise and state government departments.

With over 1,500 dedicated employees across Australia and partnerships with best-of-breed technology companies, NEC helps our customers drive flexibility and scalability in business systems, processes, and transformations.

We deliver a wide range of security services from our Australian-based Security Operation Centre (SOC). The state-of-the-art facility connects with our global SOC's that include Japan, Singapore, Europe, and the Americas to offer local capability, global coverage and sharing of threat intelligence.



For more information visit:

[nec.com.au](http://nec.com.au)

Speak to a Cyber Security expert:

[Contact Us](#)

**Japan (Corporate HQ)**  
NEC Corporation  
[www.nec.com](http://www.nec.com)

**Australia**  
NEC Australia Pty Ltd  
[www.nec.com.au](http://www.nec.com.au)

**North America (USA)**  
NEC Corporation of America  
[www.necam.com](http://www.necam.com)

**Asia Pacific (AP)**  
NEC Asia Pacific  
[www.sg.nec.com](http://www.sg.nec.com)

**Europe (EMEA)**  
NEC Enterprise Solutions  
[www.nec-enterprise.com](http://www.nec-enterprise.com)

v.22.11.24 | Managed Intrusion Prevention Service

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.

©2022 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.