How to secure your networks for a hybrid everything world.

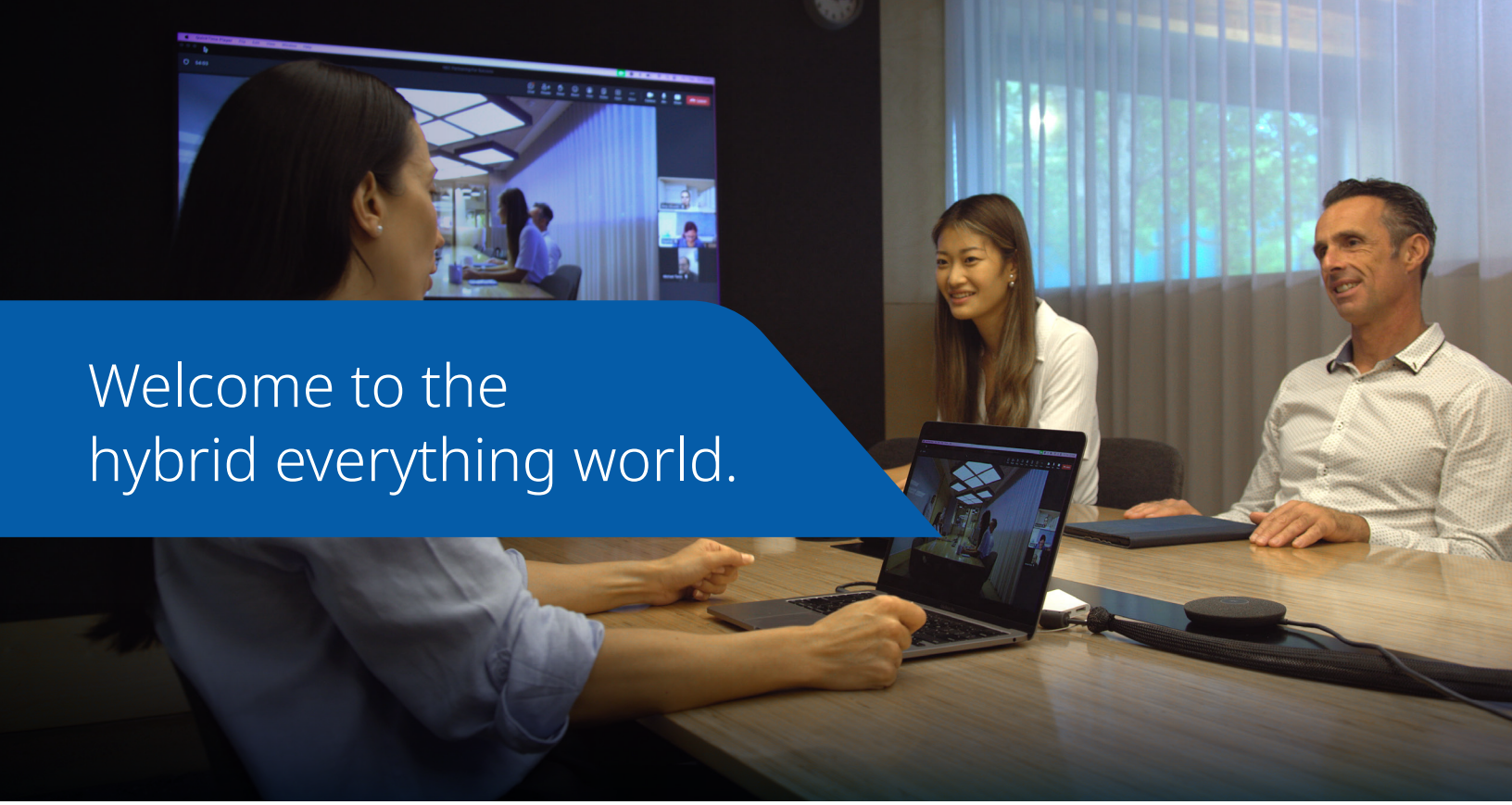
NEC

cisco Partner

Balancing connectivity and security in today's work-from-anywhere world

No one wants to make news headlines because of a security breach. But as IT leaders strive to secure the enterprise, they must also support connectivity and access to support remote work and cloud capabilities. By harmonising these twin priorities of security and connectivity, business leaders can keep pace in a hybrid world.

Contents



Welcome to the hybrid everything world.

We're officially in a world where people work from the office some days, from home others — plus the airport, the coffee shop, and points in between. A world where people use managed and unmanaged devices to access SaaS applications, internal applications, and external applications hosted on a public cloud.

The hybrid world is interconnected and dynamic. Remote access and cloud computing create opportunities for people to work from anywhere and for companies to tap into a broader pool of talent. Cloud computing means greater flexibility and scale, making it easier for business leaders to innovate and adapt to shifts in the marketplace.

But with those opportunities come challenges. In a hybrid world, the proliferation of endpoints and reliance on cloud creates a greater surface area for cyber attacks. Threat actors are more prominent and active than ever, making headlines — and making boards and business leaders take a closer look at their security posture.

And in a world that's moving faster than ever, tech becomes legacy in the blink of an eye. The architecture that allowed companies to pivot to remote work just two years ago? Outdated. The on-premises firewall installed just five years ago? Might as well be from the ice age.

Given these competing challenges, what can business leaders do?

Navigating this hybrid world means enabling the twin peaks of connectivity and security.

- **Connectivity,** because when people have the devices, access, and applications they need, at a level on par with what they'd get in the office, they can work productively.
- **Security,** because the cost of a breach goes far beyond remediation or potential fines — the reputational damage from a data breach can be immeasurable.

Importantly, connectivity and security are intertwined. To focus on one without the other is to minimise your people's ability to do their best work, and to hamper your organisation's growth and competitiveness.

Balancing the three critical hybrid priorities

While it's true, every business is different, the considerations for secure networks are the same — Workforce, Cloud and On-Premise. Let's look at each.

1. Workforce

94%

of Australian workers would like to work at home some of the time [1]

64%

of Australian workers would like a hybrid arrangement of work-from-home and in-office work [2]

60%

of workers report their employers permit hybrid work [3]

Australians have gotten used to hybrid work, and business leaders are having to account for these shifts in worker expectations. That's a challenge because whilst workers are in the office, things seem simpler. They operate from behind the company's network and are subject to the security policies set on managed computers.

But outside the office, things are much less predictable.

Consider the divergent needs of these three:

- Jo in accounting works from her dining table behind a home broadband router with a flimsy password.
- Steve in sales is tethered to his phone while his son plays cricket at a local oval.
- Issy in product development is working from the airport after a client presentation.

How can their employer provide them with secure, reliable access to the applications they need, whether they're working remotely or in the office?

[1] https://melbourneinstitute.unimelb.edu.au/data/taking-the-pulse-of-the-nation-2022/2023/ttpn-july-2023
[2] Ibid.
[3] Ibid.

VPNs are common tools to support remote work. However, they raise several issues. Specifically:

- **VPNs make it hard to manage demand:** If the number of remote users exceeds the expected load for the VPN, there can be impediments to performance of the network — which, in turn, affects people's productivity.
- **Manual work limits scale:** Given the proliferation of users and devices, it can be challenging to install and configure VPN software on all the devices that need to be connected. Changes in people's work, business objectives or access policies must also be done manually.
- **Access to the entire system is risky:** Once a user gains access to the VPN, they have access to the entire system. This increases the surface area for cyber attack and increases the blast radius of attack, should one occur.

Provide secure and reliable access – at any time, from anywhere.

NEC's Secure Access Service Edge (SASE) service supports the dynamic needs of the modern remote workforce. As network and security technologies converge and move to a cloud-based model, SASE offers the connectivity people need — with the security that the company needs. SASE provides:

- **Enhanced security:** Zero-trust protection from endpoint to application, for protection 24x7. That means better visibility, overall security awareness, and reduced risk.
- **Cost effectiveness:** A single platform dramatically reduces costs and IT resources and is offered as a composable service with flexible pricing.
- **Improved performance:** Support your increasingly mobile workforce by ensuring they can easily access applications, the internet, and corporate data, wherever they are.
- **Leverage expertise:** NEC's end-to-end service can be customized for your business's specific needs, and our deep and long-standing partnership with leading vendors like Cisco allows us to offer best-in-breed solutions.

2. Cloud

72%
of Australian organisations use one to five public clouds [4]

23%
of Australian organisations use more than five public cloud environments [5]

72%
of global organisations use a hybrid, multi-cloud strategy that includes private and public clouds [6]

79%
of global organisations say security is a top cloud challenge [7]

Cost savings, faster innovation, and greater agility are common reasons for cloud investment. Cloud capabilities are also essential for supporting a remote workforce and maintaining business continuity.

But with speed, agility, and flexibility come challenges:

- How do you support Jo in accounting to access several SaaS applications, hosted on a mixture of internal and public clouds, when she's dealing with sensitive financial information?
- How do you help Steve in sales, working from the side of the cricket pitch, as he combs through the quarter's sales data on his work laptop?
- How do you assist Issy in product development, hunkering down in Gate 36, as she navigates several applications on private clouds, public clouds and SaaS?

Again, these scenarios raise questions about how to achieve both security and connectivity in our hybrid world.

Where does your data live?

Our world may be global but borders still matter. Data stored, collected, and processed in Australia is subject to the laws and governance of Australia — and accordingly, data sovereignty has implications for compliance, data privacy, and trust.

Data sovereignty should be part of your cloud and network considerations, if it hasn't already been. NEC has been providing local support to Australian organisations and governments for over 50 years, and we're happy to support these conversations in your business.

4 https://adapt.com.au/resources/articles/cloud-infrastructure/55-of-australian-organisations-workloads-in-public-cloud-by-2025
5 Ibid
6 https://info.flexera.com/CM-REPORT-State-of-the-Cloud
7 Ibid

3. On-premises

Many business leaders perceive on-premises capabilities as being more secure than the others. There's a perception that the physical location is easier to secure because it's within the company's physical infrastructure.

That is, until you start to examine the state of the network. Consider these common use-cases:

- Networks that have accommodated ad hoc growth as new verticals or divisions were created, or as mergers and acquisitions happened.
- Networks with competing network devices with varying capabilities, or smaller capabilities bolted onto larger ones.
- Networks that started off well-designed but are now out of date with business needs, with no simple way to make updates.

More issues arise because traditional IP-based processes:

- Were designed for an in-person workforce, and don't work as well when users can connect remotely from multiple device types.
- Make it challenging to configure and troubleshoot user access and maintain a consistent security and connectivity posture across the network.
- Make it hard to know who and what is connecting, which makes it difficult to map and control the network.

Things are changing faster than humans can keep up — and a business that relies on manually updated, legacy on-premises solutions may be hindering itself. It's reducing its ability to adapt to market changes and deliver the connectivity and security required in a hybrid world.

Connect the modern workforce with NEC's Software-Defined Network (SDN)

Leave behind your IT complexity — and the manual configuration, lack of visibility, and limited scalability that comes with traditional network solutions. NEC's SDN solution helps businesses manage intricate environments and adapt to changing business needs:

- Flexible network solutions that seamlessly connect organisation, employee, and customer.
- Agility to support the proliferation of mobile and data-reliant devices, while ensuring data security.
- Drive flexibility and scalability in business systems, processes, and transformations.

NEC is proud to have received Cisco's Secure Access Designation for our SDN solution, and to be only the second Australian partner to have done so.

Traditional solutions aren't up to hybrid world challenges.

The perimeter used to be defined by the on-premises network. But today, the perimeter has been pixelated by remote work and cloud computing. So, thinking about connectivity and security means thinking about this wider hybrid world, and the more diffuse perimeter your organisation needs to secure.

Traditional solutions simply aren't up to the new challenges. Notably, the proliferation of users and devices means traditional solutions aren't flexible or scalable enough to support the needs of users or the business.

- **Manual configurations.** Legacy approaches to onboarding devices, such as setting up access through firewalls and access control lists, simply aren't feasible to keep up with the scale and speed required to be competitive.
- **Access control policies based on IP addresses or user locations.** Given the increase in user mobility and the number of devices, it's neither manageable nor scalable to manage access this way.
- **Granting access to the entire network.** Legacy solutions authenticate a user once, then grant access to the entire network — including applications or parts of the network an individual user doesn't need. This increases the potential surface area for cyber attack and the likelihood that a breach can spread laterally.

Instead, the hybrid world demands a more unified, digital, and automated approach that can provide consistent service and security across the network — wherever users or devices are located..

- **Automated capabilities**. Modern solutions allow enterprises to connect the endpoints to understand how users and devices are using the network — and then segment them into groups so you can define their access at scale.
- **Access control policies based on group rules and need.** Group-based network policies provide an intuitive and easier way to define access control policies, at scale and at the speed of business.
- **Zero trust policies.** Zero-trust security gives the minimum level of access to people and technology that a user needs to get their work done. By granting access only to what's needed — and nothing that isn't — the surface area for attack is dramatically reduced and any breaches can be more easily contained.

The increasing cost of legacy solutions.

No one wants to be at the centre of a highly publicised security breach. Equally, no one has an unlimited budget. But just as the hybrid world has changed how we look at network security and connectivity, new solutions can make it easier and more cost-effective to maintain a consistent security and connectivity posture.

Consider the hypothetical example of a company with 100 offices around Australia. Traditional solutions would include capital investments in hardware, sending technicians to each site to install and configure the hardware — never mind the time and cost of maintenance, or manual updates to try to keep up with shifting business priorities.

Instead, a cloud-based firewall would be far more feasible, cost-effective, and less disruptive. Importantly, it would allow a consistent security posture across the enterprise, without the logistical nightmare of coordinating 100 physical installs of a firewall.

While many business leaders will first consider cost and then security posture, perhaps it's instructive to flip the order. Without thoroughly considering network security, the company is at greater risk of a breach, with a price tag covering business losses, fines, class-action lawsuits, insurance-related costs, containment costs, and remediation costs.

Reputational damage wreaks damage long after the bills have been paid, negatively affecting customer retention and churn. Companies work very hard to win their customers' trust; that trust, once broken, is difficult to restore.

Importantly, options are available today which shift IT spend from up-front capital investments to more cloud-based subscription solutions that provide scale and flexibility — and much-needed security.

Simplify your network operations with Network as a Service (NaaS)

Did you know? 70% of enterprises will face a 15% rise in OpEx within five years, and 75% of annual hours are spent on maintaining network operations. NEC NaaS delivers the performance you need, with the secure and dependable connection that you expect.

- Take the hassle out of managing IT capital expenditures and ongoing network administration.
- Ensure that network performance remains at its peak.
- Streamline network operations with a secure, scalable, and simplified way to manage your network.

Keys to secure networks in a hybrid everything world.

The genie's out of the bottle. We can't put remote work or cloud computing back in. So how can business leaders design a workplace that provides connectivity and security, enables them to keep up with market shifts, and drives their business goals?

1. Limit the lateral movement of threats.

When it comes to cyber security, best practice is to assume that you've already been breached. Given that mindset, think about what would happen in such a case. With legacy solutions that provide network access to an authenticated user, the blast radius of a breach would be extensive. On the other hand, using zero-trust policies, which provide minimum-level access to users and devices, a breach could be quarantined without it moving laterally across the organisation.

2. Aim for a consistent security and connectivity posture.

Operating in a hybrid world means having a consistent posture across the organisation. Cloud-based solutions provide that consistent posture across the hybrid business environment, in a way that physical solutions can't. And having a consistent security and connectivity posture doesn't just help enterprises to deliver the same service and security when someone is working remotely as when they're in the office. It also helps to mitigate the likelihood of a vulnerability that can be exploited by a threat actor.

3. Balance your budget with your priorities.

Cost will always be a top consideration, but it shouldn't come at the expense of security. As with other business decisions, it's important to have a clear understanding of your objectives and needs. Some organisations prioritise connectivity and security of their central location — while others with remote workforces in rural areas may privilege connectivity for the field force. Also make sure the services you procure are in line with your needs. Everyone wants top-of-the-line services, but if you only need a Ford, don't buy a Ferrari. A reputable service provider will work with you to determine what you need – without the bells and whistles you don't.

4. Know how quickly things change.

Things are moving faster than ever. It's not enough to run with the blueprint of a three-year-old plan – that blueprint is already out of date. Effective partnerships with technology providers can help business leaders stay abreast of key issues, while allowing them to focus on the core competencies of the business.

NEC and Cisco can keep everyone securely connected.

NEC has a century-long history of innovation. From its cornerstone ideal – "Orchestrating a brighter world" - NEC integrates technologies, expertise, and ideas from around the world. With this global expertise, NEC Australia can bring global experience to our local clients.

For over 50 years, we've been providing local support to Australian organisations, bringing together the best tech and the best people.

Through value co-creation with customers and partners, NEC Australia innovates to design and deliver end-to-end technology solutions which meet customers' needs throughout their entire business lifecycle.

Cisco delivers integrated solutions to develop and connect networks around the world. As a global market leader, Cisco is changing the way the world works, lives, plays, and learns. NEC is proud to be a Cisco Gold Certified Partner, and to be only the second partner in Australia to receive Cisco's Secure Access Designation for our Software Defined Network (SDN) solution.

To start a conversation about how NEC and Cisco can help you embrace the hybrid world,
visit nec.com.au/secure-networks

\Orchestrating a brighter world

NEC

cisco Partner