Enabling remote working at scale with zero trust network access

Case Study +

Established in 2013 and headquartered in Sydney, Australia, Zip is one of the fastest growing "buy now, pay later" fintech firms in the world. The company, which currently operates on a global scale, with core markets in Australia, New Zealand and the US has approximately 90.7k retail partners and over 11.4m customers and 1,000 employees.

How does a leading fintech enable secure, high-performance remote working for its entire workforce?

In March 2020, the COVID-19 pandemic got underway. Almost overnight, Zip had to contend with lockdowns across its global operations. The impact was immense. In its Sydney headquarters alone, the company had to rapidly adapt to cater to a workforce that had previously been operating across five floors of dedicated office space to one that would be working entirely remotely.

Charbel Boutros, Senior Security Engineer at Zip, recalls the time: "I had started worked at Zip in January that year, then all of a sudden, we needed to find a way to secure a completely different way of working. One thing was clear: we needed to find something different to the traditional virtual private network (VPN)."

As Boutros explains, VPNs were simply not practical in this case. "The cost for the VPN licenses alone ruled this option out immediately," says Boutros. "But there were performance considerations too: we would have had a situation where our 500 Sydney-based employees would have been sharing a single 50 meg link. It would also have been a significant drain on IT resources, as we would have needed to whitelist all employee devices to get them on the network."

In a hurry to get the remote working capability up and running, Boutros decided to take a closer look at the company's existing investments in Netskope's Intelligent Security Service Edge.

Profile

Industry	Region	Employees	Yearly Revenue
Financial technology	Global, HQ Australia	1,000	$620M

Click here to visit the Zip website

Challenges

- Enable secure remote working at the onset of the COVID-19 pandemic
- Overcome limitations of traditional VPN-based approaches
- Enable workers unfettered access to AWS services

Solutions

- Netskope NPA for secure ZTNA to corporate apps

Results

- Secure and rapid onboard new team members worldwide
- Immediate least-privilege remote access
- Integration with analytics apps for enhanced security

> "I started working at Zip in January 2020, then all of a sudden, we needed to find a way to secure a completely different way of working. One thing was clear: we needed to find something different to the traditional virtual private network."
>
> – Charbel Boutros, Senior Security Engineer, Zip

netskope

Enabling Netskope Private Access for zero-trust networking

Zip is fearless in its adoption of cutting-edge technology, a true industry cloud trailblazer and one of the earliest production adopters of Netskope Private Access (NPA) in the APAC region. Boutros explains: “Zip had already fully adopted a Secure Access Service Edge (SASE) architecture when COVID hit, which put us in a great position. All we needed to do was enable the NPA solution and we were ready to go. NPA turned out to be our cure for COVID’s business ills.”

The rollout of NPA proceeded at extreme pace proportionate to the challenges of lockdown. NPA was enabled on a Wednesday and fully configured and tested against a pilot by Friday of that week. By the following Monday it was successfully and seamlessly deployed to all users, enabling zero trust network access (ZTNA) for its Sydney staff to more than 300 private applications. “The process was so seamless that none of our end users were even aware that they’d been moved off of our legacy VPN,” says Boutros.

Today, the NPA solution lies at the heart of Zip’s ongoing remote working capability and is fully integrated with Zip’s Netskope alliance partners, including Crowdstrike, Mimecast, and Sumologic, for a robust security infrastructure.

> “Thanks to the flexibility of NPA, we can stream alerts into our analytics dashboard and run behavioral analysis, which provides a real boost to our ability to detect threats.”
>
> – Charbel Boutros, Senior Security Engineer, Zip

Immediate, secure, and least-privilege remote access to resources

NPA now enables Zip to securely and rapidly onboard new team members anywhere in the world. A new user receives credentials to authenticate against Zip’s cloud identity provider, access a Netskope client enabled virtual desktop (Windows365 VMS) or a Windows/Mac device (deployed via Autopilot) and have immediate secure and least-privilege access to exactly what they need to perform their role without any impact to the user experience.

“The ability to run AWS Workspaces through the NPA is critical,” comments Boutros. “Our engineers use AWS for pretty much everything, so it’s great we can send that traffic through Netskope. The control provided by NPA is also key. It means we can give our developers the right to disable NPA, which they need to do to use Docker, without disabling it for other groups.” Soon, Zip plans to use the NPA to provide conditional access to applications based on devices’ compliance with its security policies.

The usability of NPA is another benefit. Boutros reports that no tickets have been raised for support issues with NPA. “Most people don’t even know the NPA is there,” he says, “they just turn on their workstations and they have access to what they need—no more, no less. This is helped by an incredible partnership with Netskope. Its team goes the extra mile to help us try out new things and get the most out of its systems.”

From a security perspective, Zip benefits by being able to link the NPA’s backend API to its analytics systems. “Thanks to the flexibility of NPA, we can stream alerts into our analytics dashboard and run behavioral analysis, which provides a real boost to our ability to detect threats.”

netskope

Netskope, a global cybersecurity leader, is redefining cloud, data, and network security to help organizations apply zero trust principles to protect data. The Netskope Intelligent Security Service Edge (SSE) platform is fast, easy to use, and secures people, devices, and data anywhere they go. Learn how Netskope helps customers be ready for anything, visit netskope.com.