Moving financial services to the cloud:
How National Australia Bank transitioned to working remotely

Excerpted from Securing Remote Work – Safeguarding Business Continuity with Zscaler™ ©2020, all rights reserved.
“To go from where we were, to almost the entire bank working from home within four weeks...people are quite astounded. We’re looking forward now, and I’m appreciative of this partnership.”

Steve Day, Executive for Enterprise Technology, National Australia Bank

With more than nine million customers, National Australia Bank (NAB) is the largest business bank in Australia, not to mention a 160-year-old institution and a national icon.

Like most banks, NAB has adapted to new ways of doing business. “Cash is becoming less and less relevant in today’s society,” explains Steve Day, NAB executive for enterprise technology. “Transactions used to be performed within a branch, but now people are expecting a Google or Amazon-type experience when they work with their bank.”

Day and his IT team have shepherded NAB towards an operational future that integrates online-transaction convenience with a relationship-driven development approach. Some transactions, large ones primarily, require “personal, direct engagement,” notes Day, who observes that few people want to go online for say, “the biggest investment you make in your life.” For Day, finding a balance between in-person and online communication is an ongoing objective.

In practice, it means “moving to a business model where day-to-day online activities become seamless and easy while maintaining that personal relationship on bigger transactions.”

Moving financial services forward in the cloud

When it comes to business evolution, the financial services industry can be staid: Strict data-privacy requirements, low risk tolerance, and regulatory constraints can all foster resistance to change. But NAB hasn’t let operating pressures slow its progressive approach to infrastructure innovation.

In the mid 2010s, NAB’s leadership recognized the potential and value in migrating to the cloud, in particular to help strengthen its security posture. The company invested in Zscaler Internet Access (ZIA), rolling out local internet breakouts for users, and taking advantage of ZIA’s Cloud Sandbox security technology.
The third adjustment was sudden: An employee reported contracting coronavirus. To safeguard the health of the employee and the employee’s coworkers, NAB immediately evacuated the building, meaning 4,500 people had to work remotely, though some were not yet enabled to do so.

Moving a high-touch business to a work-from-anywhere model

NAB’s shift to the cloud was driven by security priorities. “Part of the initial motivation was to get to Zero Trust,” says Day. “We didn’t need to run a separate corporate network, since that increases the number of places you can be attacked from.”

“Many of our older financial systems were not designed for working anywhere but in an office, and on a low-latency connection,” comments Day. With a dual focus on securely enabling the business and improving user experience, Day and team began evaluating Zscaler Private Access (ZPA) as a solution for connecting employees to internal resources.

And then in early 2020, the coronavirus outbreak hit. The first necessary adjustment NAB had to make was scaling to accommodate higher-than-normal customer call volumes. In the space of a few days, NAB found itself having to transact three-to-four times its normal commercial and consumer banking volume.

“The bank must play a role in enabling and sustaining the Australian economy through a crisis,” explains Day. “We play a part in enabling the stimulus packages and support programs.”

The second adjustment was a practical challenge: To ensure the safety of its employees and enable teams to be able to serve customers in a time of need, NAB had to enable its call-center staff employees to work remotely.

The third adjustment was sudden: An employee reported contracting coronavirus. To safeguard the health of the employee and the employee’s coworkers, NAB immediately evacuated the building, meaning 4,500 people had to work remotely, though some were not yet enabled to do so.

Moving from constrained VPNs to scalable cloud

Day and the NAB IT team shifted into overdrive: “The amount of logistics that went over the days following...we worked 24/7 for four days to enable remote access for thousands of employees.”

![NAB: ZPA Active Users](image)

**Figure 6-4.** National Australia Bank (NAB) deployed ZPA to more than 15,000 users in only two weeks, enabling its workforce to work remotely during the COVID-19 crisis.
Day’s original intent with implementing ZIA and ZPA for local internet breakouts was to get to a Zero-Trust environment. Ultimately, COVID became the catalyst for accelerating scale up. According to Day, ZPA’s ease of use and flexibility made fast rollout possible. He also credits the efforts and insourcing work of internal teams for the successful deployment.

“Zscaler enables us to save costs and reduce threat surface area,” says Day. “Because Zscaler is a cloud-based service, it scales beautifully…we didn’t need to build out additional infrastructure — It was the obvious solution.”

The alternative? An accelerated — *a very accelerated* — ZPA rollout

“We needed to pivot quickly,” says Day, with unintentional understatement. Over the course of the next few weeks in March 2020, NAB shifted to a remote-access model, with only those required to work on premise remaining to do so. Day and his colleagues deployed ZPA for thousands of employees, enabling their access to corporate resources from remote locations.

Those ZPA-enabled employees included NAB’s call-center staff around the world. “Before March 2020,” comments Day, “we had never had a single customer call handled by someone working outside of one of our offices.”

Moving away from a corporate network

“Today, we are happily working with 22,500 users on ZPA,” says Day, who notes that NAB went from fewer than 150 users to full deployment in less than three weeks. “ZPA offered a seamless experience,” he says. “Users would turn on their PCs and they connected exactly the same way as they did in the office. That was a real benefit for us.”

“We had been looking at modernizing our internal capabilities,” says Day, “and as we moved applications to the public cloud, we could see that the current VPN wasn’t providing the right outcomes.”

He and team realized they wouldn’t be able to procure legacy connectivity hardware affordably, let alone expediently. “We couldn’t scale up our existing VPN solution rapidly,” explains Day. “We’d have to order equipment, and wait for it to be delivered, but you don’t know when you’re going to get anything since everything’s clogged up in customs right now.”
About Zscaler

Zscaler was founded in 2007 on a simple but powerful concept: As applications move to the cloud, security needs to move there as well. Today, we are helping thousands of global organizations transform into cloud-enabled operations.

© 2021 Zscaler, Inc. All rights reserved. Zscaler™ is either (i) a registered trademark or service mark or (ii) a trademark or service mark of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.