NATIONAL AUSTRALIA BANK

CASE STUDY

CYBERARK®

Company: National Australia Bank

Headquarters: Australia

Website: www.nab.com.au

Industry: Financial Services

CyberArk Products & Services:
CyberArk Privileged Access Manager Solution

"This isn't just a compliance check-box exercise, we're actively designing and aligning policies to cybersecurity best practices to strengthen overall security posture and align internal teams."

Joel Harris, Manager
National Australia Bank

Taking a Phased Approach, National Australia Bank Implements PAM Across Multiple Operation Areas

OVERVIEW

National Australia Bank (NAB) is a financial services organisation that provides a comprehensive and integrated range of banking and financial products and services, with operations in Australia, New Zealand, parts of Asia, the United Kingdom, and the United States. A long-time CyberArk customer NAB has prioritised privileged access management (PAM) within the Enterprise Security division to help protect against growing external and internal threats to personal and proprietary information.

THE CHALLENGE

Changing customer expectations, greater digital use and the ever-evolving cyber threat landscape is changing the way financial institutions balance innovation with effective security practices to safeguard reputation and attempt to future-proof success.

To achieve this balance, privileged access management is critical to enable flexible — yet strictly controlled — access to critical systems that hold sensitive customer PII and other valuable organisational information. Privileged access can be given to system admins and other users, but also be granted to applications and machines. As financial systems grow in size and complexity, privilege is everywhere — in administration accounts, in business applications, in the software development pipeline and in many areas of operational technology as well.

Now more than ever, strong PAM is key to allowing banks to move with agility to capture new opportunities without jeopardising their brand or regulatory compliance.

THE SOLUTION

NAB's PAM team, led by manager Joel Harris, uses CyberArk to protect privileged access, while also helping guide and further develop the organisation's enterprise-wide PAM program across people, process and technology domains.

With privileged accounts throughout the expansive enterprise, the team is taking a phased, programmatic approach to PAM — beginning with managing and securing the privileged accounts that pose the most risk. This involves migrating all privileged credentials associated with critical infrastructure and high priority business applications— into CyberArk.

The CyberArk Privileged Access Manager Solution assists the PAM team to enforce least privilege principles by centrally vaulting and rotating credentials in an encrypted repository, isolating credentials and sessions, recording and storing privileged sessions. With CyberArk, the team can lock down powerful privileged accounts and access to defend against both internal and advanced persistent threats.

THE RESULTS

NAB has on-boarded hundreds of business critical applications and tens of thousands of accounts into CyberArk to date. With a strong PAM foundation in place, the team is expanding coverage to new areas of the organisation.

Using CyberArk Discover and Audit (DNA), a privileged access risk-assessment tool, the NAB PAM team is working with numerous infrastructure and application teams within the business to inventory privileged accounts and technology assets across their operating environments — and evaluate the strength of existing controls — to create an actionable plan to attempt to reduce risk. This approach also helps the team demonstrate remediation activities against the organisation's risk framework.

Taking a policy-first approach has helped Harris and his team to achieve some initial wins. "This isn't just a compliance check-box exercise, we're actively designing and aligning policies to cybersecurity best practices to strengthen overall security posture and align internal teams," he says.

"We've found CyberArk can centrally manage, collect and report on privileged access activity for us. With Policy and Architecture teams on our side, we're collaboratively designing controls and evolving policies — bringing them into close alignment to drive internal adoption, and potentially, better protect the organization," he continues.

As NAB continues on their cloud first, multi-cloud strategy the PAM team has also extended its CyberArk deployment to the cloud. "We're focused on architecting the most resilient service possible," says Harris. "By moving CyberArk to the cloud, we're empowering our users with higher levels of availability and scalability, while paving the way for advanced PAM use cases to help secure the business as it grows."