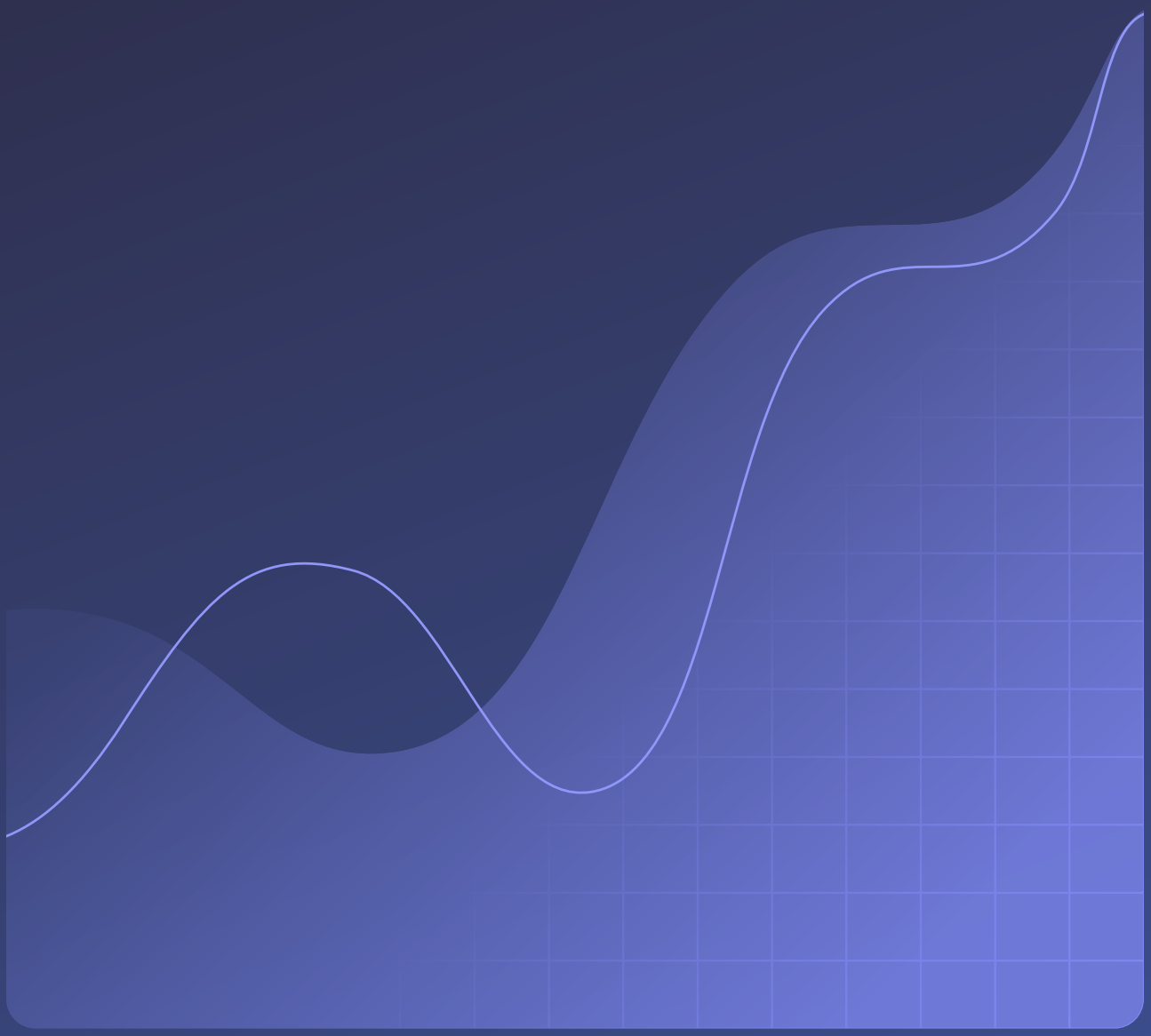
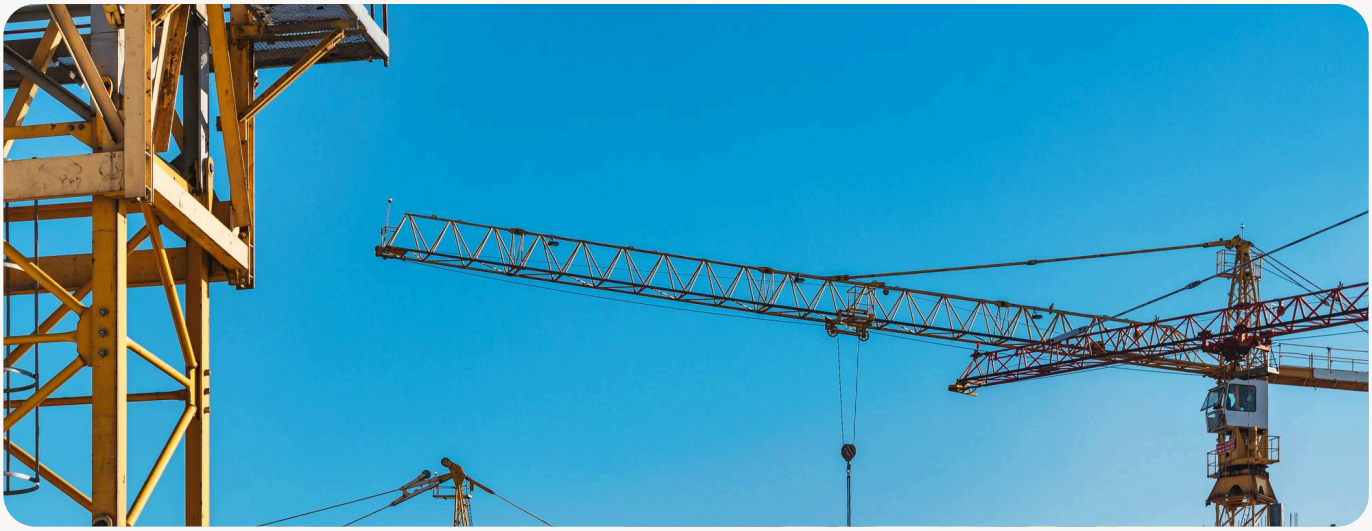
DASHLANE

CASE STUDY

How a Critical Infrastructure Services Provider Safeguards Privileged Access





Downer

Company description

Founded in 1933, Downer Group is the leading provider of integrated infrastructure services across Australia and New Zealand.

Industry

Critical infrastructure services

Company size

26,000 employees across 700+ sites

The challenge: Protecting against unauthorized access to critical infrastructure

Downer Group offers diverse services that are essential to building, managing, and maintaining assets, infrastructure, and facilities across Australia and New Zealand. The company serves transportation, telecommunications, and energy and utilities companies. Prominent projects include building and maintaining the fleet of trains that will support the 2032 Summer Olympics in Brisbane, Australia. They also serve high-profile facilities like hospitals, defense bases, and prisons.

Over half of Downer's workforce is frontline employees across more than 700 sites, including remote areas. The vendors supporting them are spread throughout multiple countries, and many of these vendors are privileged users. They have access to what Aidan Turner, Downer's Identity and Access Management Manager, describes as "the crown jewels."

"Downer, like every other organization, is constantly under attack, and increasingly, attackers are logging in and not breaking in," Aidan explains. "Whenever those privileged user credentials are exposed, it puts the reputation of our business on the line."

An even bigger concern is that an attack on Downer could have devastating results if customer operations were disrupted or data were lost.

"If we don't protect our systems correctly and an attacker were to gain access to those credentials, they could potentially infiltrate or disrupt systems that support essential services," Aidan says.

> “The last thing you want to hear is that your company was under a breach that led to the loss of customer data—that would absolutely be catastrophic.”
>
> **Aidan Turner**, Identity and Access Management Manager, Downer Group

The consequences of a disruption could amount to significant financial cost. Downer’s agreements with some customers include severe abatements for downtime, such as six-figure penalties for every 15 minutes of interruption.

“If something were to be breached and a credential brought down a system, which is very feasible, it’s of utmost importance to contain it quickly and lessen the financial impact,” shares Aidan.

Mergers and acquisitions in recent years have brought new businesses under the Downer umbrella. Each of them came with separate technical standards and procedures. The result was a complex infrastructure with multiple Active Directory (AD) domains. Technology services outsourced to various providers added further challenges.

“Because of our large mix of suppliers who have different internal processes, there was a lot of shadow IT and mismanagement of privileged identities,” Aidan says.

Downer needed a credential risk management solution that would provide:

- Secure credential storage for critical accounts
- Standardization of the IT-approved security stack
- A simple and easy-to-use interface for admins
- Proactive, real-time credential risk mitigation for admins and employees

The solution: A standardized, easy-to-use tool for securing privileged accounts

Some of Downer's privileged users stored their passwords in unsupported credential managers. Others used spreadsheets.

"There were too many instances of people inappropriately using their credentials," Aidan says. "We needed to take a stand and redevelop the standard, and we picked and implemented Dashlane."

He says they chose Dashlane because the solution was well-positioned for their use case and "extremely competitive," a significant advantage when IT budgets are stretched thin. Other differentiating features included Dashlane's easy onboarding, simple administration, and SSO integration.

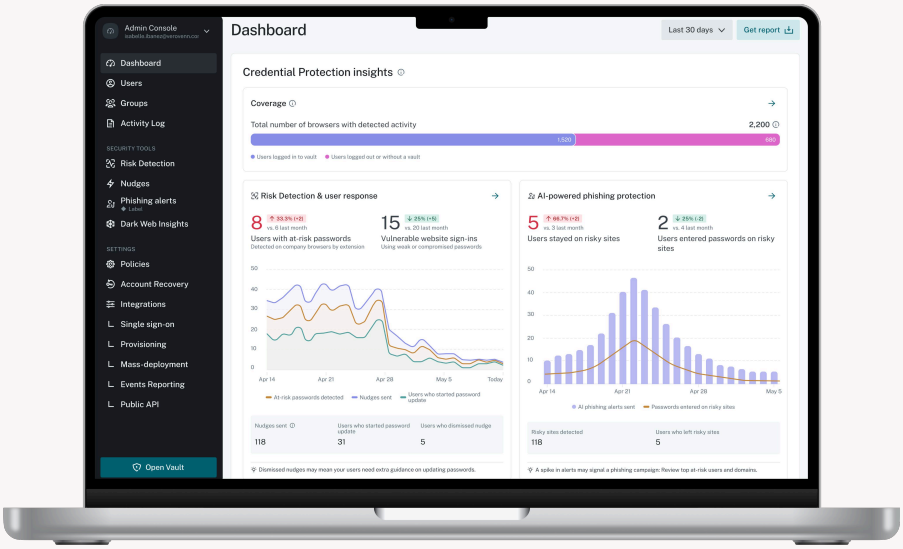
The initial goal was to implement the credential manager for the security team. However, the team recognized a bigger opportunity as they onboarded more users and more people used the tool. They decided to adopt Dashlane as a sanctioned solution to provide secure credential management and proactive risk detection, starting with critical credentials.

> "Over time, for our crown jewels, we've required privileged users to onboard Dashlane so they can vault and store their credentials there for extremely critical applications."
>
> **Aidan Turner**, Identity and Access Management Manager, Downer Group

With Dashlane, Downer Group benefits from:

- A password vault that securely stores credentials for critical accounts
- Dark Web Monitoring that enables employees to mitigate their risks proactively
- An admin dashboard that's simple and easy to use
- Seamless integration with SSO and Active Directory
- Credential Risk Detection that allows the admin to manage the risk of privileged identities in real time

Aidan also notes that Dashlane's support team is very helpful and responsive.



Admins get actionable insights with Credential Risk Detection, including the number of employees who entered at-risk credentials while not logged in and risks detected over time.

The results: Robust credential risk management that's not burdening the security team

As a busy security practitioner, Aidan appreciates that he can use and manage the Dashlane platform easily and effectively.

"And I know for sure that there are other platforms where that wouldn't be the case," he says.

His team is deploying the solution within multiple business unit IT teams. He notes that Dashlane's seamless user onboarding and SSO integration are especially valuable for admins.

"When my teams are managing Dashlane, we don't need an army of people to manage the system on the back end; we can do it relatively lightweight," adds Aidan.

The adoption rate is high among Downer's centralized teams that were part of the initial Dashlane rollout. This speaks to Dashlane's simplicity and ease of use for employees.

> "From a historic low Password Health score of 59.9%, we are now sitting comfortably above 85%."
>
> **Aidan Turner**, Identity and Access Management Manager, Downer Group

In addition, he explains, "Dark Web Insights and compromised password monitoring are excellent features that my team is utilizing to further protect credentials for our critical applications."

Aidan says that having Dark Web Monitoring and Insights built into Dashlane is a big advantage because it enables the company to strengthen security proactively.

“We don’t want to have compromised credentials stuck in the vault. Once we see that passwords associated with a particular email address are compromised or weak, we want to proactively notify users so they can take appropriate action to strengthen their account,” he says.

“To have Dark Web Monitoring directly in the tool is quite useful, and we can also tie it into our security awareness plan.”

With Password Health scores greatly improved, Aidan and his team can confidently report to the board of directors that Downer can better prevent unauthorized access to international systems and mitigate risk.

“Our key risks were the privileged passwords that would give away the keys to the kingdom," shares Aidan. “With Dashlane, we’re helping reduce that key risk and can report better to the board that we’re driving down the number of breaches associated with credentials.”

Based on Dashlane’s initial success, Downer is considering a rollout for all regular business users across the enterprise.

“In the future, we want to give vaulting to everybody,” Aidan says.

> “We're looking at some point to adopt Dashlane organization-wide, especially as we continue to expand our services.”
>
> **Aidan Turner**, Identity and Access Management Manager, Downer Group

See for yourself how Omnix delivers proactive credential security.
Request a demo