

BUPA

CASE STUDY



Company: Bupa

Bupa is a diverse health and care group which has been committed to a purpose of helping people live longer, healthier, happier lives for close to 70 years.

Industry: Healthcare

Annual Revenue: USD 16.78 billion (Worldwide)

Employees: 22,000

CyberArk Product & Services:

CyberArk Core Privileged Access Security Solution

CyberArk Discovery and Audit

Bupa Mitigates Risks With CyberArk Privileged Access Management Solutions

“One of the key benefits we get from CyberArk is control: Once an account is in CyberArk you immediately have that control,” stated Michael Freeman, security manager for identity and access for the Australian and New Zealand regions of his company, Bupa.

In Australia and New Zealand, Bupa supports more than 6 million customers through a broad range of health and care services including health insurance, aged care, rehabilitation, dental, optical, medical, hearing and medical visa services. The company employs more than 22,000 people and has reinvested approximately AUD \$6 billion in Australia and New Zealand, while the Bupa Health Foundation has invested over \$35 million to support more than 100 health and care projects.

The nature of Bupa’s business means that the company is entrusted with holding copious amounts of highly sensitive information, covering the personal, financial and medical records of millions of its customers.

Managing Expanding Entitlements

As with many large enterprises, one of the issues facing Freeman and his team was the widespread proliferation of privileged credentials on both administrative and standard accounts. Once identified as being a tangible risk, a project was launched that focused on reducing the sheer number of privileged entitlements throughout the environment.

Freeman described his philosophy, “Governance and segregation of duties are among the most powerful controls we have for effectively managing privilege access across the organisation. Role-based access security, designed with the principle of least privilege, provides us with an objective basis for mitigating risk and consistently enforcing rules.”

“Being able to manage all users from a centralized console is a massive benefit for us.”

Michael Freeman,
Security Manager for Identity and Access
Bupa

KEY BENEFITS

- Visibility and control over every step of an application user's journey
- Low-level granularity enables precise allocation of user access entitlements
- Unified view delivers resource efficiencies
- Access credentials managed equally effectively across on-prem, cloud, and hybrid domains

To help in prioritising the rollout of privileged access controls, the team met with stakeholders to identify Bupa's 'crown jewels' – the company's most critical data and highest risk applications.

Initially, as is commonplace, there was a level of resistance to surrendering any elevated credentials. "We overcame people's concerns by approaching the subject in a calm, collaborative manner," recalled Freeman. "Then we applied a role-based lens to really understand what permissions were needed to perform each activity."

CyberArk Brings Control

CyberArk had previously been used on a limited basis at Bupa but managing privileged credentials on an enterprise-wide basis had never been an imperative. "I already knew how good CyberArk was and it was an easy decision to utilise the CyberArk Core Privileged Access Security Solution for this company-critical project," remarked Freeman.

He continued, "Deploying CyberArk is much simpler than other privileged access apps that I've worked with; it's a very clean product that just works as sold."

To support the rollout, an onboarding guide was written for standard account users that discussed privilege access management best-practices. For users needing elevated privileges or employees requiring access to data in the crown jewel category, a series of short workshops was put together to cover activities such as logging-in and establishing a session through CyberArk.

The CyberArk Core Privileged Access Security Solution is architected to deliver a unified, single pane of glass view, coupled with the granularity needed to implement access governance accurately and efficiently. "Being able to manage all users from a centralised console is a massive benefit for us," noted Freeman. "The precision and control we have with CyberArk enabled us to accurately distill down each role to assign the least amount of privilege for any user in the organisation."

Freeman also makes extensive use of CyberArk Discovery and Audit (DNA) to conduct detailed privileged access risk assessments. As the Bupa environment expands and evolves, DNA account discovery scans are regularly performed to identify risk and bring privileged access accounts under CyberArk. He commented, "CyberArk delivers a level of visibility and management that we previously never had: This is just fantastic."

Setting the Standard for Security

Bupa's internal Global Information Security Office (GISO) defines governance standards for the whole company. These controls are designed to meet or exceed prevailing industry and regulatory requirements. When new platforms are being developed, accounts are registered in CyberArk and evaluated for compliance against the GISO standards.

“CyberArk is a great solution – the company is a clear leader in the privileged access management space for both cloud and on-prem environments. We now have visibility and control over every aspect of an application user’s journey.”

Michael Freeman,
Security Manager for Identity and Access
Bupa

“Once we onboard an account in CyberArk we can record and report against usage of those credentials from a single location, rather than having to rely on an application owner,” Freeman explained. “With increased usage it gets progressively more accurate and evolves in parallel with our privileged access strategy. It’s a dramatic step-up in efficiency and resource effectiveness for us.”

Bupa is undergoing a significant transition to a predominantly cloud-based infrastructure. The multi-year initiative is creating a constantly changing mix of on-prem, cloud and hybrid domains. “Even though each environment involves completely different technologies, CyberArk has been able to handle all the use cases we’ve thrown at it without issue,” reflected Freeman.

A standout for Freeman has been the relationship he enjoys with CyberArk: “The people on our CyberArk account team feel like they’ve got a real stake in the work they’re doing: They truly care about our success.”

The impact of the project has been significant: Many thousands of privileged accounts have been eliminated. However, for Freeman, the true measure of success has come at an application-specific level: “Over the years, some of our more mature crown jewel applications have accumulated large numbers of standard accounts with privileged access credentials. Without a role-based access approach, it would be have been impossible to untangle the mess. Leveraging CyberArk has enabled us to achieve massive reductions in the quantity of elevated privileges associated with each application.”

He concluded, “CyberArk is a great solution – the company is a clear leader in the privileged access management space for both cloud and on-prem environments. We now have visibility and control over every aspect of an application user’s journey.”