

blueAPACHE Improves Efficiency in Security Management - blueAPACHE

Canonical: <https://www.blueapache.com/case-studies/blueapache-security>

Details:

Summary

This case study, authored by CyberArk, describes how we deployed the CyberArk Identity Security Platform to protect our own business and to offer identity security as a managed service. We are the customer in this account. CyberArk describes our management of privileged access across hundreds of customer environments and the move from password vaulting without rotation or session recording to privileged access management, workforce identity, password management and vendor privileged access. It also describes our becoming a CyberArk MSP partner. The account records the deployment described at publication; confirm current access arrangements for a particular engagement.

Key facts

Label	Value
Customer	blueAPACHE (also becoming a CyberArk MSP partner)
Vendor and author	CyberArk; the case study is written in CyberArk's voice
Problem	Password vaulting without automated rotation or session recording; risk of credentials left behind in customer directories after staff departures
Products deployed	CyberArk Privilege Cloud, CyberArk Workforce Identity (SSO, adaptive MFA, Workforce Password Management), CyberArk Vendor PAM; next phase Credential Providers and Conjur Secrets Manager Enterprise
Scope	Deployed across emPOWER Cloud, emPOWER Connectivity, emPOWER Collaboration and emPOWER Managed Services, and our internal IT
Scale stated	Over 200 users in Privilege Cloud, over 250 in Workforce Identity, hundreds in Vendor PAM; CyberArk manages all customer support and administration access
Implementation	CyberArk Jump Start Service Package and Strategic Consulting Services, chosen because of the multi-tenanted environment

Stated efficiency outcome	A ten-fold efficiency increase; doing the same without CyberArk estimated to require four times more staff
Service offer to customers	Dedicated CyberArk tenants for large businesses; a multi-tenanted platform for smaller organisations
Named executive	Michael Zuppa, General Manager of Technology at the time of publication

Customer

blueAPACHE, described in the case study as a managed services provider offering IT management, IT strategy and converged IT services to clients across Australia, the UK, Asia and North America since 1998, headquartered in Melbourne with offices in Sydney and Brisbane. The case study frames the MSP position as the frontline: MSPs are trusted with access to client systems and data, so compromised or fake identities are the standard route for attackers.

Sector

Managed services and cyber security. The case illustrates privileged-access practices described for our own operations and a managed identity-security offering. It is not an independent compliance assessment or proof of the controls included in every current customer engagement. Related sector guidance is available for financial services , government and public sector and utilities .

Challenge

Our General Manager of Technology describes identity security as extremely challenging for an MSP with hundreds of employees serving customers: creating hundreds of identities in each customer directory is a risk because the organisation is only as strong as its onboarding and offboarding, and with a dynamic workforce credentials can be left behind when someone leaves. The previous password vaulting tools lacked automated rotation and session recording, which made it hard to enforce identity and role controls, particularly during onboarding and offboarding. We also wanted stronger workforce access controls for all staff, alignment with government standards, and a platform that could extend to endpoints and non-human identities.

Solution

After a review of potential providers, we selected the CyberArk Identity Security Platform and used the CyberArk Jump Start Service Package and Strategic Consulting Services to implement it across a multi-tenanted environment.

CyberArk Privilege Cloud secures privileged access to customer and internal systems with session isolation and monitoring; the platform now manages all customer support and administration access.

CyberArk Workforce Identity gives staff single sign-on, adaptive multi-factor authentication and Workforce Password Management, so applications that do not support SSO are accessed the same way while their credentials are vaulted, encrypted and centrally managed.

CyberArk Vendor PAM provides passwordless, VPN-less and agent-less access for remote users with privileged access, authenticating with biometric adaptive MFA and receiving just-in-time access.

Centralised password rotation removed password ownership from individuals and eliminated credential re-use across the hundreds of credentials we control internally and for customers.

The next phase is Credential Providers (CP/CCP) and CyberArk Conjur Secrets Manager Enterprise.

At the same time we became a CyberArk MSP partner: large customers get a dedicated CyberArk tenant set up and managed by us; smaller organisations use a multi-tenanted platform. Services include provisioning and deprovisioning IT and workforce users, onboarding infrastructure and business applications into Privilege Cloud or Workforce Identity, and configuring remote privileged access with Vendor PAM.

Services used

emPOWER Security and emPOWER Security overview : the pillar under which identity security is delivered as a managed service.

Governance, Risk and Compliance : the control assessment and policy work that sits around privileged access.

emPOWER Managed Services , emPOWER Cloud , emPOWER Connectivity and emPOWER Collaboration : the four service lines the platform is deployed across.

Outcomes

Outcome	Result
Credential control	All customer support and administration access managed by CyberArk; passwords rotated automatically; credential re-use removed
Auditability	We can show customers audited records of automatically rotated passwords used to manage their services and share session recordings
Offboarding	"If an employee leaves blueAPACHE tomorrow, they would have no idea of passwords or credentials used to access customer services"
Efficiency	A ten-fold efficiency increase; doing the same without CyberArk estimated to need four times more staff
Incident response	Time saved because logs from multi-tenanted environments are in one place
Commercial	Builds credibility and strengthens the value proposition to organisations that trust blueAPACHE to manage their environments; enterprise-level identity security made accessible to mid-market businesses
Supply chain	Increased defence against supply chain attacks (listed under key benefits)

Our General Manager of Technology provided these efficiency and staffing estimates for this case study. They describe that engagement and are not a guarantee of results for other environments.

Distinguishing internal practice from customer scope

The case describes blueAPACHE using security technology internally. It is evidence of the described approach to privileged access, not an inclusion statement for every customer security service. Identify which accounts and systems the proposal covers, who approves access and what evidence follows a change or incident. For purchased MDR, exposure management or governance work, the relevant Service Description establishes actual deliverables and responsibilities.

Related

emPOWER Security

Managed Detection and Response

Governance, Risk and Compliance

Exposure Management

Human Risk Management

Our partners

Financial services

Government and public sector

Blog: Exclusive: why we chose to partner with CyberArk

Blog: we were named ARN Mid-Market Partner of the Year in the 2020 Innovation Awards

Blog: we ranked among the world's most elite 501 managed service providers

All case studies

Contact

Who wrote this case study and who is the customer?

CyberArk wrote it, and we are the customer. It describes our deployment of the CyberArk Identity Security Platform across our own business and emPOWER services, and our parallel move to become a CyberArk MSP partner offering identity security to customers.

What engineer-access controls does this case describe?

The account describes customer support and administration access through CyberArk Privilege Cloud with session isolation and monitoring, automatic password rotation and just-in-time remote access through Vendor PAM. It also describes audited records and session recordings. Confirm which controls, systems and evidence apply to your current engagement.

What happens to credentials when a blueAPACHE engineer leaves?

Because password ownership was removed from individuals and credentials are rotated centrally, the General Manager of Technology states that an employee leaving tomorrow would have no knowledge of the passwords or credentials used to access customer services. This was the offboarding risk that drove the project.

Which CyberArk products did we deploy?

CyberArk Privilege Cloud, CyberArk Workforce Identity with single sign-on, adaptive multi-factor authentication and Workforce Password Management, and CyberArk Vendor PAM. The stated next phase is Credential Providers and Conjur Secrets Manager Enterprise for application and machine secrets.

Can I buy CyberArk through you?

The case describes a managed CyberArk offering with dedicated tenants for larger businesses and a multi-tenanted platform for smaller organisations, covering user provisioning, application and infrastructure onboarding, and remote privileged access. Contact us to confirm current availability and scope.

How many blueAPACHE users are on the platform?

The case reports over 200 users in CyberArk Privilege Cloud, over 250 in Workforce Identity and hundreds in Vendor PAM, across the named emPOWER service lines and internal IT. These are the figures reported for that deployment, not current user counts.

How does this relate to your compliance claims?

The case describes access-control practices and available audit evidence; it does not establish compliance with a particular regulatory framework. The supplied ISO/IEC 27001:2022 certificate 202507-118 concerns blueAPACHE's ISMS and states dates from 1 August 2025 to 1 August 2028. Confirm current certification standing, scope and the evidence required for your organisation separately.

What is this blueAPACHE case study about?

Our case study, titled 'blueAPACHE Improves Efficiency in Security Management,' describes how we strengthened our security posture by implementing CyberArk, adding enterprise-level identity controls across our business and managed services.

Which security vendor did you use to improve your security posture?

We used CyberArk to strengthen our security posture.

What kind of controls did you add as part of this security improvement?

We added enterprise-level identity controls across our business and managed services, as described in the case study.

What industry do you operate in, according to this case study page?

According to the case study page, we operate in the Professional Services industry.

How is the original case-study page titled?

The original blueAPACHE page identifies the case study as 'blueAPACHE - Security.' Its summary describes adding enterprise-level identity controls across the business and managed services.