Why we chose to partner with CyberArk - blueAPACHE

Canonical: https://www.blueapache.com/blog/exclusive-why-blueapache-chose-to-partner-with-cyberark

Details:

Summary

This blog post, "Security Brief Australia: Why blueAPACHE chose to partner with CyberArk", is a blueAPACHE article from 2023 covering security. JUNE 23, 2023: CyberArk is an identity security company that enables organisations to secure access to critical assets and data while enforcing least privilege and enabling Zero Trust. To learn more about the company and how its solutions are helping its customers, TechDay spoke with Olly Stimpson, Strategic Business Development Manager for ANZ at CyberArk and Michael Zuppa, GM of Technology at blueAPACHE. It is written for readers evaluating emPOWER Security, Managed Detection and Response. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2023
Topic	Security Brief Australia: Why blueAPACHE chose to partner with CyberArk
Services referenced	emPOWER Security, Managed Detection and Response, Advanced Infrastructure Managed Services
Named products or vendors	CyberArk, Gartner

Article

JUNE 23, 2023: CyberArk is an identity security company that enables organisations to secure access to critical assets and data while enforcing least privilege and enabling Zero Trust. To learn more about the company and how its solutions are helping its customers, TechDay spoke with Olly Stimpson, Strategic Business Development Manager for ANZ at CyberArk and Michael Zuppa, GM of Technology at blueAPACHE. What does CyberArk do? Through its unified Identity Security Platform, CyberArk provides a comprehensive security offering for any identity – human or machine – across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. With a presence in 110 countries and over 8000 customers, CyberArk is a global company. Listed on the NYSE, it established its Australian operations in April 2016. The company was also recently recognised as a leader in the Gartner Magic Quadrant Reports for both Access Management and Privileged Access Management. What are the challenges facing Australian organisations? Australia is currently experiencing a concerning rise in cyberattacks, with its frequency and severity rapidly intensifying over the last six months. Given the evolving threat landscape, this escalation highlights how crucial it is for

Managed Service Providers (MSPs) to prioritise their security measures and strengthen their security posture. As threat actors are relentlessly focusing on targeting supply chains, having robust security practices in place within these networks will be essential. Identities are becoming the standard route for initiating and spreading attacks. This indicates that attackers are leveraging compromised or fake identities as a preferred avenue to infiltrate systems and carry out their malicious activities. Implementing comprehensive security measures across the whole supply chain ecosystem will help mitigate the risk of attacks and safeguard critical infrastructure and data. Last year, The Australian Cyber Security Centre (ACSC) issued a warning about threat actors employing a 'one to many' approach to target organisations through their MSPs. The recent breach of Latitude Financial is a prime example of this type of exploitation through the supply chain network. Australia has become an attractive target for cybercriminals, and there is a need to acknowledge the significance of MSPs in the security landscape and why it's more important than ever to adopt robust identity-centric security practices. MSPs are now at the frontline and will play a crucial role in safeguarding Australia's digital landscape and critical infrastructure. By taking a closer look at the current threat landscape, identity has emerged as the primary pathway for attackers to breach organisations, regardless of their size. Relying solely on basic Multi-Factor Authentication (MFA) and commercial password managers without enterprise-grade controls is no longer sufficient. Recent attacks have demonstrated how a single oversight can result in a complete network takeover, underscoring the importance of a robust security strategy. How does CyberArk's MSP strategy address these challenges and assist its partners? The role of MSPs is undergoing rapid transformation as they adapt to the evolving threat landscape. They are now required to enhance their own security measures while also providing advanced security capabilities to their customers. As a result, in today's environment, an MSP's security offering has become a crucial competitive differentiator. Services such as Managed Identity, Chief Information Security Officer as a Service (CISOaaS), and security consulting are now commonplace. As the Australian Government seeks to strengthen and mature the nation's security posture, the responsibility for delivering the advantages of one-to-many security offerings to customers increasingly rests on MSPs. MSPs are well-positioned to provide comprehensive, scalable and efficient security services to a broad range of organisations, helping them enhance their resilience against cyber threats while focusing on their core operations and without having to build and maintain such capabilities in-house. CyberArk's strategic approach is two-fold. Firstly, CyberArk collaborates with MSPs to enhance their identity security managed services – leveraging CyberArk's expertise and technology to help MSPs strengthen their offerings in managing and securing identities within their customers' environments. By integrating CyberArk's solutions into their portfolio, MSPs can provide advanced identity security capabilities to their customers, bolstering their overall security posture. Secondly, CyberArk recognises the importance of MSPs securing their own operations. Cybersecurity threats can target MSPs directly, making it crucial for these service providers to implement robust security measures internally. CyberArk assists MSPs in safeguarding their own infrastructure and systems by offering comprehensive security solutions tailored to their specific needs. By protecting their own operations with CyberArk's technology, MSPs can gain firsthand experience and insights into the effectiveness of these solutions. This two-fold approach benefits both the MSPs and their customers. MSPs not only enhance their internal security practices but also gain valuable expertise in deploying CyberArk's technology. Combining these two allows MSPs to effectively build and market their expertise and knowledge as unique IPs, positioning them as trusted advisors and experts in the market. It enables them to deliver differentiated services that leverage CyberArk's technology and best practices to their customers, providing enhanced security and mitigating the risks associated with identity-related attacks.

"Many MSPs are looking to expand both their internal and external identity security practice as the evolving threat landscape demands this. Security technologies like MDR, Email Threat Protection and Managed SIEM are now common place in MSPs' security offering, but the market is demanding an evolution," says Olly Stimpson, Strategic Business Development Manager, ANZ, CyberArk. "With a need to drive a rapid uplift in security, MSPs with mature, secure offerings, including identity security, are reaping the rewards in a crowded space." How and why did blueAPACHE partner with CyberArk? blueAPACHE chose to partner with CyberArk for several reasons. Firstly was the opportunity to work

with CyberArk on leading identity security solutions and services that met blueAPACHE's complex requirements, but also solutions that could be packaged as easy-to-consume outcome-based offerings for the company's customers. With CyberArk's focus on serving MSPs in the mid-market and blueAPACHE's ongoing recognition as the leading Midmarket Service Provider, the company has firmly established itself as the go-to provider in the mid-market landscape and solidified its position as a trusted leader in the industry. blueAPACHE initially sought a PAM solution, but what truly resonated with the company was CyberArk's strategy of securing all identities through its Identity Security Platform approach. This comprehensive approach not only addressed blueAPACHE's current needs, but also positioned the company for continuous evolution in securing the identities of humans, applications, and machines. "A strong channel and managed service offer is an essential part of CyberArk's growth plans in Australia and New Zealand," adds Stimpson. "With ever more organisations recognising the need to improve their security posture, our managed service partnerships are prospering by allowing organisations of all sizes to secure identities while reducing cost, time to value and boosting program success." Before partnering with CyberArk, blueAPACHE was using common password vaulting solutions that lacked automated password rotation or session recording capabilities, making it challenging to maintain strong and consistent enforcement of identity and roles, especially during onboarding and offboarding processes. Additionally, there was a risk of credentials being locally saved or cached in remote management toolsets or even stored in spreadsheets. With CyberArk's unified Identity Security Platform, blueAPACHE was able to implement access management controls that forced all sessions through a secure vaulted platform. The platform requires multi-factor authentication for accessing templated least privileged role accounts across various technologies. Each account has unique passwords that are rotated after each access, and all sessions are recorded and analysed in real-time to detect risky or anomalous activity. The company further enhanced its solution by integrating a remote management toolset that automates the syncing of nodes from its monitoring platforms, driving efficiencies and enabling blueAPACHE's engineers to work natively without encountering friction. What is different about blueAPACHE's current security strategy solutions compared to 6 months ago? blueAPACHE's security strategy solutions have remained consistent over the past six months, focusing on maintaining its ISO 27001 certification and expanding coverage across ISM and MITRE ATT&CK framework controls. This approach has brought several benefits, including assurance to the company's customers regarding data security and adherence to industry best practices. By continuously improving its security measures, blueAPACHE stays ahead of emerging threats and vulnerabilities, ensuring a secure environment for its customers' data. The company's commitment to a robust security posture, demonstrated through its ISO 27001 certification and expanded coverage, instils confidence in its customers and reinforces its dedication to delivering a secure and reliable service. Additional information: Click here to view the full article

Related

emPOWER Security

emPOWER Security (pillar hub)

Managed Detection and Response

Advanced Infrastructure Managed Services

emPOWER Managed Services (pillar hub)

blueAPACHE Security (case study)

Frequently asked questions

When did CyberArk establish its Australian operations, and how many countries and customers does it serve, per this article?

CyberArk established its Australian operations in April 2016, and the article states it has a presence in 110 countries and over 8,000 customers, listed on the NYSE.

Which two Gartner Magic Quadrant categories does the article say CyberArk was recognised as a leader in?

Access Management and Privileged Access Management.

Who are the two people interviewed for this article, and what are their roles?

Olly Stimpson, Strategic Business Development Manager for ANZ at CyberArk, and Michael Zuppa, GM of Technology at blueAPACHE.

What security gaps did blueAPACHE have before adopting CyberArk's platform, according to the article?

blueAPACHE was using common password vaulting solutions that lacked automated password rotation or session recording, creating risk that credentials could be locally saved or cached in remote management toolsets or stored in spreadsheets.

What breach does the article cite as an example of supply-chain exploitation through an MSP?

The Latitude Financial breach is named as a prime example of the 'one to many' MSP-targeting approach the ACSC had warned about the previous year.

What security controls did blueAPACHE implement using CyberArk's platform, per the article?

Access management controls forcing all sessions through a secure vaulted platform, multi-factor authentication for templated least-privilege role accounts, unique passwords rotated after each access, and real-time recording and analysis of sessions for anomalous activity.

What solution was blueAPACHE initially seeking before choosing CyberArk's broader platform?

blueAPACHE initially sought a PAM (Privileged Access Management) solution, but was drawn to CyberArk's broader Identity Security Platform approach covering all identities.

What certification and frameworks does the article say blueAPACHE's security strategy has focused on maintaining?

Its ISO 27001 certification and expanding coverage across ISM and MITRE ATT&CK framework controls, unchanged in focus over the six months before the article's publication.

Source

origin post (2023)

Knowledge Base

What does CyberArk do?

CyberArk is an identity security company that provides a comprehensive security offering for any identity—human or machine—across business applications, distributed workforces, hybrid cloud workloads, and the DevOps lifecycle through its unified Identity Security Platform. It enables organisations to secure access to critical assets and data while enforcing least privilege and enabling Zero Trust.

How large is CyberArk's global presence?

CyberArk operates in 110 countries with over 8,000 customers, is listed on the NYSE, and established our Australian operations in April 2016. It was also recently recognised as a leader in the Gartner Magic

Quadrant Reports for both Access Management and Privileged Access Management.

Who were the interviewees discussing the blueAPACHE-CyberArk partnership?

TechDay spoke with Olly Stimpson, Strategic Business Development Manager for ANZ at CyberArk, and Michael Zuppa, GM of Technology within our business.

Why did you choose to partner with CyberArk?

We partnered with CyberArk for the opportunity to work on leading identity security solutions and services that met its complex requirements while also being packaged as easy-to-consume, outcome-based offerings for customers. CyberArk's focus on serving MSPs in the mid-market aligned with our position as the leading Midmarket Service Provider, and CyberArk's Identity Security Platform approach to securing all identities resonated beyond our initial search for just a PAM solution.

What security setup did you have before partnering with CyberArk?

Before partnering with CyberArk, we used common password vaulting solutions that lacked automated password rotation or session recording capabilities, making it difficult to maintain strong, consistent enforcement of identity and roles, especially during onboarding and offboarding. There was also a risk of credentials being locally saved or cached in remote management toolsets or stored in spreadsheets.

How did CyberArk's platform improve your security controls?

With CyberArk's unified Identity Security Platform, we implemented access management controls that force all sessions through a secure vaulted platform, requiring multi-factor authentication for templated least-privileged role accounts across various technologies. Each account has unique passwords rotated after each access, and all sessions are recorded and analysed in real-time to detect risky or anomalous activity. blueAPACHE further enhanced this by integrating a remote management toolset that automates syncing of nodes from its monitoring platforms, driving efficiencies for engineers.

What is CyberArk's two-fold strategic approach for MSPs?

CyberArk's strategy is two-fold: first, it collaborates with MSPs to enhance their identity security managed services by integrating CyberArk's expertise and technology into their portfolios; second, it helps MSPs secure their own operations by offering security solutions tailored to their needs, since MSPs themselves can be direct targets of cyber threats.

What cybersecurity challenges are Australian organisations facing, ?

Australia has experienced a concerning rise in cyberattacks, with frequency and severity intensifying over the last six months, and threat actors increasingly targeting supply chains. Identities have become the standard route for initiating and spreading attacks, with attackers leveraging compromised or fake identities. The Australian Cyber Security Centre (ACSC) warned about threat actors using a 'one to many' approach to target organisations through their MSPs, with the Latitude Financial breach cited as a prime example.