Centrify warns Password Vaults alone not enough to stop data breaches

Submitted by: Origin Comms Ltd
Wednesday, 26 April 2017

Innovative new capabilities help organisations implement privileged identity management (PIM) best practices and greatly reduce risk of a breach

Centrify (https://www.centrify.com), the leader in securing hybrid enterprises through the power of identity services, today announced significant enhancements to its best-in-class privileged identity management (PIM) solution to stop breaches that abuse privilege. By minimising the attack surface and controlling privileged access to the hybrid enterprise, Centrify's new capabilities enable organisations to move from static, long-lived privilege assignments to a just-in-time model where advanced monitoring detects and alerts in real-time on the creation of backdoor accounts that make it easy to bypass a password vault.

Securing privileged access in today's hybrid enterprise is mandatory in achieving a mature risk posture. According to the The Forrester Wave: Privileged Identity Management, Q3 2016, 80 per cent of breaches leverage privileged credentials to gain access to the organisation. The increasingly hybrid nature of infrastructure, driven by the adoption of cloud-based workloads, is driving the need to secure privileged access across on-premises, private-cloud and public cloud infrastructure and apps with a single solution. And while most PIM solutions have traditionally focused on vaulting the credentials for shared accounts on-premises, password vaults alone do not provide the level of privileged access security required to stop the breach.

"Data breaches are happening at an alarming rate and to stop them Centrify is taking a unique approach to controlling privileged access in the hybrid enterprise that simplifies the implementation of PIM best practices and strengthens an organisation's risk posture," said Bill Mann, chief product officer at Centrify. "By contrast, password vaults alone are not enough, best practices require organizations add and integrate point products to the vault, which leaves gaps in security and increases risk. We've closed those gaps with an integrated solution that combines password vaulting with brokering of identities, MFA enforcement and just-enough privilege, all while securing remote access and monitoring all privileged sessions."

Only a Full PIM Solution Can Stop the Breach

A recent Forrester study examined four levels of Identity Access Management (IAM) maturity. It found a direct correlation between the number of PIM best practices an organisation has implemented and the number of security incidents it encounters. Centrify's new PIM capabilities enable these best practices, adding to Centrify's already comprehensive set of integrated services that help organisations increase their IAM maturity level and security posture.

1. Establish Identity Assurance. Centrify ensures accountability by having users log in as themselves and attributing all activity to the individual. Its advanced host-based auditing capabilities now include process-level monitoring in addition to existing shell-based monitoring to attribute all activity to the individual instead of a shared account or alias. This new advanced monitoring adds a layer of security that is virtually impossible to spoof.

2. Limit Lateral Movement: Centrify enables organisations to reduce the attack surface by governing privileged access and ensuring users' privileges only apply on the approved server. Now you can require access approvals for role assignment and make them short-lived. Centrify's proven host-based privilege management ensures that the user's approved privileges apply only to the target system, and cannot be used across the network on other computers. And if credentials are compromised, hackers and malware will not have the privileges that would allow them to wreak havoc within your network.

3. Institute Least Privilege: Centrify now uniquely governs access to both privileged accounts and privilege elevation via roles enabling organisations to implement true cross-platform least privilege access. Centrify lowers the risk of a security breach by granting just-in-time privilege and just-enough-privilege through temporary and time-bound access that leverages request and approval workflows. Audit trails and compliance reporting capabilities now include who has access, who approved that access and how that access was used across privileged accounts and privileged roles.

4. Monitor Privileged Use: Centrify now monitors for the creation of backdoors whose existence make privileged access to infrastructure convenient instead of secure. Centrify's advanced monitoring capabilities detect the growing threatscape and alert in real time through SIEM integration on rogue creation of SSH keys that enable privileged access that bypasses the password vault.

According to the Forrester study, organisations that reach the highest levels on the maturity scale are 50 per cent less likely to have a breach. In addition, these organisations save 40 per cent in security costs over their less mature counterparts, and spend $5 million less in breach costs.

See how Centrify Stops the Breach.

About Centrify (https://www.centrify.com)

Centrify redefines security from a legacy static perimeter-based approach to protecting millions of scattered connections in a boundaryless hybrid enterprise. As the only industry recognised leader in both Privileged Identity Management and Identity-as-a-Service, Centrify provides a single platform to secure each user's access to apps and infrastructure through the power of identity services. This is Next Dimension Security in the Age of Access. Centrify is enabling over 5,000 customers, including over half the Fortune 50, to defend their organisations. To learn more visit www.centrify.com.
The Breach Stops Here.

Media contact:
Amanda Hassall
Consultant
T:+44 (0) 16 2882 2741
M: +44 (0) 78 5535 9889
E: amanda@origincomms.com