Gartner Peer Community. | Bravura Security

Yes, Despite Rampant Breaches, Companies *Still* Manage Their Passwords with Old-School Spreadsheets

Even organizations with the most sensitive infrastructure suffer from catastrophically bad password management. Those not using privileged access management comprehensively and uniformly are resorting to poorly governed spreadsheets and personal password managers. These substandard solutions, combined with inadequate Joiner-Mover-Leaver user identity lifecycle means they are unable to catch rouge accounts in a timely manner, putting them at risk of being exploited for malicious purposes.

Organizations need a clear Joiner-Mover-Leaver plan that reflects the reality of fundamental security hygiene. Evaluating all points of the user identity lifecycle will ensure employees have the right access to get their job done while increasing security.

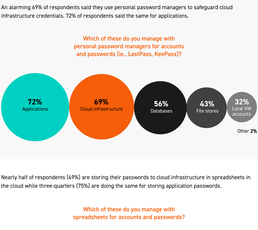
Bravura Security used the Gartner Peer Community platform to survey 100 security leaders to understand what the biggest concerns and risk in cloud security access management are today.

Data collection: August 16 - September 22, 2022

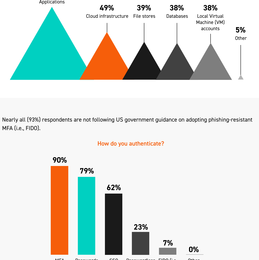
Respondents: 100 security and operations leaders

Privileged identities are at risk from inadequate password management

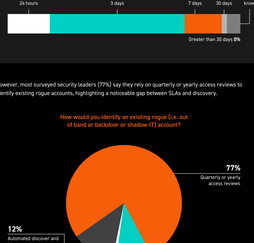
Surveyed security leaders say they manage cloud infrastructure (66%) and applications (66%) with privileged access platforms.



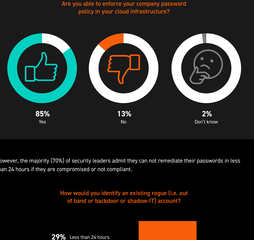
An alarming 69% of respondents said they use personal password managers to safeguard cloud infrastructure credentials. 72% of respondents said the same for applications.



Nearly half of respondents (49%) are storing their passwords to cloud infrastructure in spreadsheets in the cloud while three-quarters (75%) are doing the same for storing application passwords.



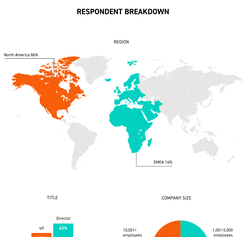
Nearly all (93%) respondents are not following US government guidance on adopting phishing-resistant MFA (i.e., FIDO).



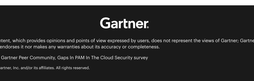
Organizations need to execute shorter turnarounds when revoking access and identifying rogue accounts

Over three-quarters of respondents (76%) say they can identify rogue access to their infrastructure within three days.

However, most surveyed security leaders (77%) say they rely on quarterly or yearly access reviews to identify existing rogue accounts, highlighting a noticeable gap between SLAs and discovery.



The vast majority (85%) of organizations are able to enforce their company password policy on their cloud infrastructure.



However, the majority (76%) of security leaders admit they can not remediate their passwords in less than 24 hours if they are compromised or not compliant.

Govern All Your Organization's Credentials with Bravura Security

Governance of enterprise accounts and credentials in identity lifecycle management, including Joiner-Mover-Leaver scenarios, remains largely lacking. Even in organizations which have adopted privileged access management solutions, coverage and pervasiveness appears to be inconsistent. The data suggests that these same organizations that are identifying Joiner-Mover-Leaver gaps often choose the wrong tools such as personal password managers and periodic audits to plug the holes.

Audits are intended to spot check that your processes, automation, workflow and governance are working correctly–they are reactive, not proactive. Instead, credentials should be vaulted, randomized, and stashed for all infrastructure and technology across the organization whether on-premises or in the cloud. In all cases these mechanisms should employ phishing-resistant authentication and enforce strong password policies.

As part of an organization's zero trust journey, Bravura Security provides the most comprehensive joiner, mover and leaver management solution for identity lifecycle management. Its enterprise solutions for privileged, end-user, and decentralized credentials ensures that you can swiftly enforce corporate password policy and safeguard against situations that are typically surfaced during audits.

RESPONDENT BREAKDOWN

Gartner