8 BEST PRACTICES

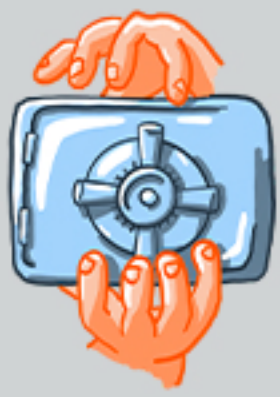
for Privileged Password Management

1 DISCOVER ALL PRIVILEGED ACCOUNTS

Identify where and how privileged credentials are being used and help reveal security blind spots across your on-premises and cloud infrastructure.

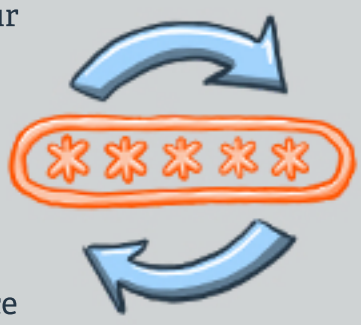
2 BRING PRIVILEGED CREDENTIALS UNDER CENTRALIZED MANAGEMENT

Automatically enforce your privileged password management policy by centrally storing and controlling all privileged credentials.



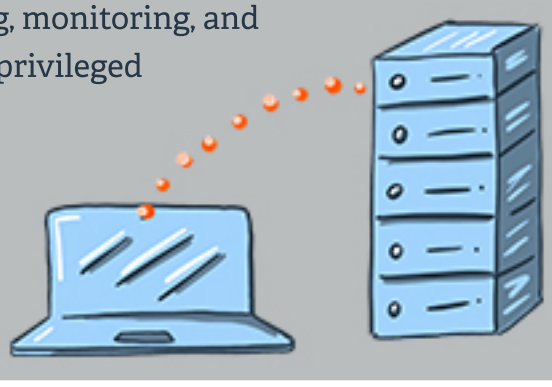
3 ENABLE PASSWORD ROTATION

Regularly rotate all of your privileged credentials at intervals set by your policy, and seamlessly synchronize the password changes to accounts, including service accounts and applications.



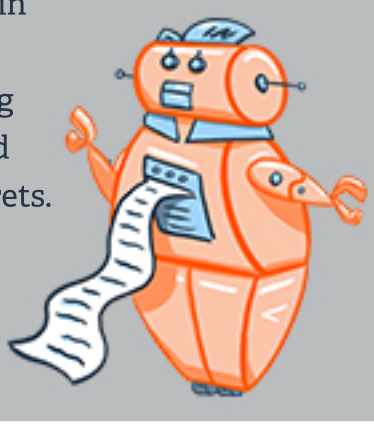
4 IMPLEMENT PRIVILEGED SESSION MANAGEMENT

Ensure complete oversight and accountability over privileged accounts and credentials by controlling, monitoring, and recording all privileged sessions.



5 ADDRESS NON-HUMAN & MACHINE CREDENTIALS

Implement API calls to gain control over scripts, files, code, and keys, eliminating hard-coded and embedded credentials and other secrets.



6 CONTROL SSH KEYS

Approach SSH keys as just another password — accompanied by a key pair that must also be managed — and regularly rotate private keys and passphrases to ensure each system has a unique key pair.

7 UTILIZE THREAT ANALYTICS

Continuously analyze privileged password, user, and account behavior to identify anomalies and potential threats, and accelerate awareness and mitigation.

8 AUTOMATE WORKFLOW MANAGEMENT

Streamline and optimize the entire credential management lifecycle and enable just-in-time (JIT) administration.

More Detailed Information:

"Privileged Password Management Explained"

GET THE WHITEPAPER