PREVENT PRIVILEGED CREDENTIAL ABUSE WITH RSA SECURID® ACCESS & CYBERARK PRIVILEGED ACCOUNT SECURITY SOLUTION
THE CHALLENGE
Today, more than ever, organizations need to be aware that compromised identities represent the single biggest attack vector for adversaries. The ease with which passwords can be harvested and packaged together with very sophisticated tools and techniques to exploit them can lead to devastating consequences.

While any compromised identity can have real consequences for organizations, it’s widely recognized that privileged accounts pose the largest security threat. In the wrong hands, privileged credentials can allow attackers to take control of IT infrastructure, disable security controls, steal confidential information and commit fraud. In order to help prevent a potentially catastrophic breach, organizations must know who privileged users are, what they have access to and what they are doing once logged in to sensitive systems and applications.

KEY BENEFITS
- **Mitigate** privileged credential abuse with multi-factor authentication for privileged access.
- **Protect** privileged access across cloud, web and on-premises applications, and enforce consistent policies regardless of where the data lives.
- **Simplify** user access and deliver a high level of identity assurance with RSA behavioral analytics and mobile push and biometric authentication.
- **Balance** security and convenience with RSA assurance levels and easily define unique authentication requirements based on policy.

The combined solution further enables organizations to easily tailor different levels of assurance, based on user privileges, their roles and the sensitivity of the resources they are trying to access. This gives organizations the flexibility to provide privileged users with more than one multi-factor authentication option, allowing users to choose what’s most convenient, but still be secure.

Moreover, RSA and CyberArk together can be deployed to protect SSH administrative access to remote computers for performing administrative tasks like troubleshooting and configuring updates, as well as for admin access to infrastructure equipment such as routers, switches and Unix servers.
Current RSA SecurID customers can easily leverage their existing deployment of hardware or software tokens, or add other mobile multi-factor authentication options, including push or biometrics, for accessing the CyberArk Enterprise Password Vault. In addition, larger enterprises that may have hundreds or even thousands of RSA SecurID agents deployed on Linux machines could use the CyberArk Enterprise Password Vault as an authentication gateway—to enforce RSA SecurID Access multi-factor authentication—and reduce complexity by eliminating the need to manage native RSA agents deployed across these endpoint systems.

**HOW IT WORKS**

![Diagram of RSA and CyberArk integration](image)

**CLOUD-TO-GROUND PRIVILEGE PROTECTION**

The elastic nature of cloud computing can create unique challenges and potentially new unmanaged and unsecured privileged accounts. Similar to the need for managing privileges on-premises, organizations must also control and monitor privileged users in the cloud. The combined solution of RSA SecurID Access and the CyberArk Privileged Account Security Solution solves this challenge.

With CyberArk, privileged accounts for cloud management tools, infrastructure and APIs are secured, monitored and managed. And with RSA, organizations get the identity assurance they need to protect privileged access in the cloud, as well as secure access to all their cloud provider consoles, while also providing a consistent and consumer-friendly access experience for privileged users.
CENTRALLY GOVERN PRIVILEGED IDENTITIES
For complete identity protection, RSA Identity Governance and Lifecycle has also been tightly integrated with the CyberArk Privileged Account Security Solution to provide a unified view of user access, driven by centralized, policy-based identity management for all privileged users and applications, and their entitlements, to ensure access is appropriate and adheres with security best practices guidelines.

Centralizing and automating identity and access governance of privileged identities ensures that privileges are accurately managed throughout their lifecycles, revoking or decrementing privileges appropriately as employees leave organizations or change roles within them.

ABOUT RSA
RSA offers business-driven security solutions that uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and, reduce business risk, fraud, and cybercrime. RSA protects millions of users around the world and helps more than 90% of the Fortune 500 companies thrive in an uncertain, high risk world. For more information, go to rsa.com.

ABOUT CYBERARK
CyberArk is the global leader in privileged account security, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. CyberArk delivers the industry’s most complete solution to reduce risk created by privileged credentials and secrets. The company is trusted by the world’s leading organizations, including more than 50 percent of the Fortune 100, to protect against external attackers and malicious insiders. For more info, visit cyberark.com.