





CyberArk Identity Security Platform

Secure All Identities With Intelligent Privilege Controls


Thank you for downloading this CyberArk Solution Brief. Carahsoft is the distributor for CyberArk cybersecurity solutions available via GSA, CMAS, MHEC, and other contract vehicles.


To learn how to take the next step toward acquiring CyberArk's solutions, please check out the following resources and information:


 For additional resources:
carah.io/CyberArkResources

 For upcoming events:
carah.io/CyberArkEvents

 For additional CyberArk solutions:
carah.io/CyberArkSolutions

 For additional cybersecurity solutions:
carah.io/cybersolutions

 To set up a meeting:
Cyber-Ark@carahsoft.com
703-871-8548

 To purchase, check out the contract vehicles available for procurement:
carah.io/CyberArkContracts



CYBERARK[®]
The Identity Security Company

SOLUTION BRIEF

CyberArk Identity Security Platform

Secure All Identities With Intelligent Privilege Controls

Security teams are facing the perfect storm as three variables grow in volume and velocity:

- The cloud and digital initiatives your enterprise is spearheading.
- The identities of your users and machines powering these initiatives.
- The innovation today's attackers employ to exploit your identities.

Compromised identities — whether privileged or not — are a gateway to the sensitive resources today's sophisticated attackers are targeting. Compounding the security challenge: internal users and third parties who may abuse or misuse the access they've been granted — which is often far beyond what they actually need.

Digging deeper into the problem, enterprises are dealing with several shifts happening at once:

- **Explosion of identities:** We live in a digital world with no boundaries. There are 45 machine identities for every human identity,¹ and the total number of identities is growing at an accelerated rate of 3x per year,² according to CyberArk research. There is no longer a perimeter to protect; identities are the new perimeter.
- **All identities can become privileged:** "Privileged users" are no longer just IT admins. Fifty-two percent of all employee identities have access to sensitive systems and data that attackers can easily exploit.³ In this environment, every identity at any access point is a gateway to an organization's most valuable resources. Privilege is now everywhere, and so are the risks associated with it.
- **Cyberattackers continue to innovate:** Attackers are using more sophisticated techniques to impersonate users, launch targeted phishing campaigns and compromise identities. Sixty-three percent of organizations have faced a successful cybersecurity attack due to an Identity Security-related issue.⁴
- **IT landscape complexity:** Organizations embracing digital transformation leverage hybrid and multi-cloud environments and have a proliferation of endpoints, both managed and non-managed, across their infrastructures. This complexity makes it even more challenging for security teams to have visibility, control and management of identities. Eighty percent of organizations expect to leverage three or more public cloud providers in 2023, and 57% have separate teams to secure identities on-premises and in the public cloud.⁵
- **Complexity in risk reduction:** Security leaders recognize that achieving and maintaining control of every identity is the key to stopping most modern attacks. But they are struggling to implement a security-first approach. Every new digital initiative brings new identity-related challenges and requirements. In an effort to keep up, enterprises often implement new security tools ad hoc.

^{1,3} CyberArk, "2022 Identity Security Threat Landscape Report," 2022

^{2,4,5} Enterprise Strategy Group, "The Holistic Identity Security Maturity Model," February 2023

- **Operational inefficiencies:** An accumulation of overlapping tools has created an unwieldy situation for security teams. Teams are juggling multiple solutions – from identity and access management (IAM) to identity governance and administration (IGA) and privileged access management (PAM) – that don't necessarily integrate with each other. This limits security teams' visibility and control of identities across the enterprise and strains tight resources.
- **Security vendor sprawl:** With the average enterprise using 75 security vendors,⁶ the cost and complexity of today's siloed security solutions is top of mind. These tools may not approach security issues the same way, making it difficult for security teams to realize the value of each standalone solution. It's no wonder CyberArk research showed that 54% of organizations favor unified platforms from fewer vendors.⁷ Vendor consolidation across Identity Security tools can provide security benefits, operational efficiencies and a better ROI.

SOLUTION

Identity Security is a strategic approach to enable Zero Trust and enforce least privilege. It requires a core set of technology, people and processes that organizations need to secure the access of human and machine identities to their most critical assets and data across any environment or devices.

Identity Security controls are dynamic and adaptive in nature, designed to ensure the right level of access is given based on risk. Privilege controls such as session isolation and monitoring, elevation, endpoint privilege management and delegation management are at the core of Identity Security and access, especially as the definition of who has privileged access has evolved. In today's environment, almost any identity can have high-value or high-level privileged access, depending on what activity they are carrying out.

As a result, privilege controls and processes are increasingly being integrated with IAM capabilities such as lifecycle and entitlements management, secure single sign-on, authentication, password management and automated orchestration. Through a unified Identity Security approach, privilege controls are applied to:

- All types of identities, from employees to vendors and from DevOps teams to the automated tools they use.
- All IAM controls, such as access reviews, certifications and lifecycle management workflows.

With Identity Security, access is monitored on an ongoing basis for all identities across all environments with continuous identity threat detection so that the appropriate Identity Security controls and responses – such as session suspension and step-up authentication – can be applied based on a real-time analysis of risk.

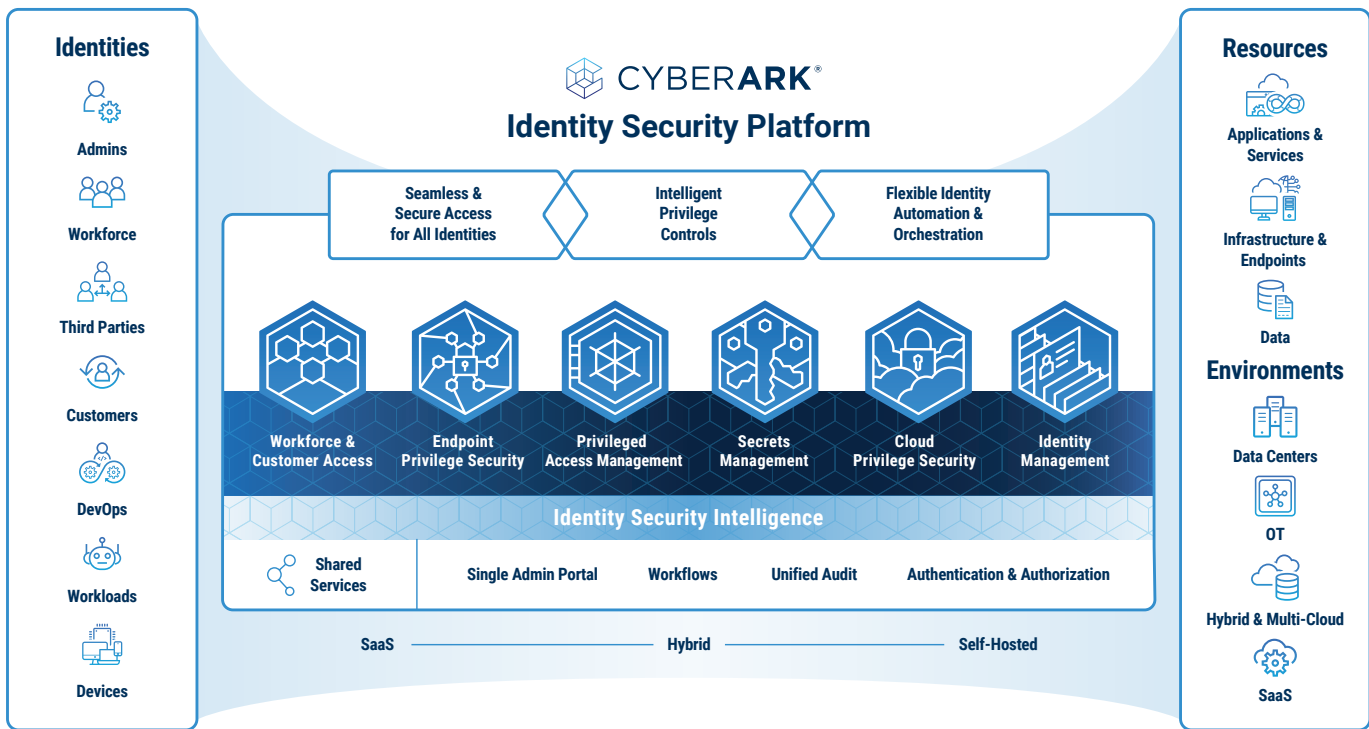
CyberArk Identity Security Platform

Centered on intelligent privilege controls, the CyberArk Identity Security Platform seamlessly secures human and machine identities accessing workloads from hybrid to multi-cloud and flexibly automates the identity lifecycle – all with a unified approach. CyberArk offers the most complete and extensible Identity Security Platform across workforce and customer access, endpoint privilege security, privileged access management, secrets management, cloud privilege security and identity management to enable Zero Trust and enforce least privilege.

The CyberArk Identity Security Platform is based on a set of foundational shared services – including AI-powered Identity Security Intelligence – that delivers a unified user experience through a single admin portal and enhances value with robust automation and analytics. Through our vast partner network and more than 300 out-of-the-box integrations, CyberArk supports each organization along every step of their Identity Security journey, while helping them maximize existing security investments.

⁶ Panaseer, "2022 Security Leaders Peer Report," 2022

⁷ Enterprise Strategy Group, "The Holistic Identity Security Maturity Model," February 2023



KEY FEATURES: CYBERARK IDENTITY SECURITY PLATFORM

- **Unified Identity Security Platform:** Use a consolidated platform that provides multiple capabilities to enable security of all individual identities, both human and non-human, throughout the cycle of accessing any resource across any infrastructure by applying privileged controls.
- **Intelligent privilege controls:** Apply least privilege security controls across identities, infrastructure and apps, from the endpoint to the cloud. Gain intelligence to detect anomalous behavior that – on its own or in combination with privileged access misuse – could be a potential threat.
- **Strong authentication:** Enable contextual, risk-based and adaptive access management for employees, partners, vendors and customers. Strong passwordless authentication factors including biometric, QR codes, mobile push and USB tokens.
- **Contextual authorization:** Secure privileged access for human users and machine identities, such as applications. Enforce least privilege and just-in-time access principles across platforms, endpoints and applications.
- **Frictionless access:** Employ a single pane of glass designed to administer, provision, enable access and secure all identities and resource types with automated workflows to provide self-service to user provisioning, account and password resets, application access and more. Seamlessly work with thousands of SaaS, mobile and custom applications.
- **Audit and accountability:** Gain visibility and control by securing brokered sessions to ensure accountability, monitoring and identifying risky behaviors and providing tamper-proof audit trails. Use risk analytics to monitor access activity and act on suspicious behavior in real time.
- **Seamless integration:** Experience seamless integration with existing technology tools, including third-party threat intelligence and DevOps tools.

CONCLUSION

Organizations adopting Identity Security can realize significant security benefits and operational efficiencies by consolidating vendors into a unified platform. However, the CyberArk Identity Security Platform is modular, so organizations can start with one or more of our best-in-class capabilities or the whole platform. Regardless of the approach, what is most important is that organizations build strong Identity Security programs that deliver measurable cyber risk reduction.

With CyberArk, organizations can enable Zero Trust and enforce least privilege with complete visibility, ensuring that every identity can securely access any resource, located anywhere, from everywhere – with a single Identity Security Platform.

About CyberArk

CyberArk is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security offering for any identity – human or machine – across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets.



©Copyright 2023 CyberArk Software. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners. U.S., 02.23. Doc. TSK-3119

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.