CYBERARK®

WHITEPAPER

Mitigate Risk with Privileged Access Management

Why Federal Agencies Should Implement the
Zero Trust Architecture with PAM

Table of Contents

Introduction

Cyber attacks are the new warfare. The rise in data breaches conducted by cybercriminals in recent years has exponentially grown and is now being treated by the U.S. Department of Justice as seriously as terrorism threats. Sensitive data into federal agencies ranging from the treasury and commerce departments, Office of Personnel Management and others have all had their fair share of data stolen from their databases.

Traditional security measures are not sufficient for today's new world. The sophistication and scale of cyber attacks is unlike any previous era. With 81% of breaches originating from compromised credentials and 95% of phishing attacks followed by malicious software installation, it is imperative to ensure all endpoints are integrated with identity and access management strategies.

These hacks often stem from breaking into privileged accounts and manipulating access, exposing highly sensitive data to cyber criminals. As a result, privileged accounts and the access they provide represent one of the largest security vulnerabilities all government agencies face today. These powerful accounts exist in every piece of hardware and software and on every U.S. network. Adversaries leverage stolen privilege accounts to gain access to confidential business data, personal identifiable information and disabled security systems, and take control of critical IT infrastructure. The General Services Administration (GSA) acknowledges the need to protect IT assets and data from external and internal threats by implementing strategic security approaches with appropriate access and controls to privileged accounts.

> Traditional security measures are not sufficient for today's new world. The sophistication and scale of cyber attacks is unlike any previous era.

Unfortunately, federal civilian data breaches have impacted millions of U.S. citizens, as well as state and local governments. These agencies have been held hostage to cyber criminals extorting them for millions of dollars to resolve the ransomware issues and prevent the leak of highly sensitive data and state secrets.

Hackers broke into the treasury and commerce departments in 2020 as a result of a global cyber espionage attack; cyber attacks on the Pulse Secure VPN impacted at least five federal civilian agencies. The list goes on.

In the spring of 2021, the White House issued an executive order putting into place guidelines on how to improve the nation's cybersecurity stance. This requires federal agencies to modernize their approach to cybersecurity by becoming more transparent about cyber threats and enhance their software supply chain security. Government agencies are required to move toward a **Zero Trust** architecture, which calls for an "assume-breach" mindset and secures all cloud services. Federal agency heads must develop a plan for implementing the ZT Architecture and incorporate guidelines from the National Institute of Standards and Technology (NIST) as appropriate.

With the cybersecurity **executive order** in place, the U.S. Department of Defense recently published its **Zero Trust Reference Architecture**. What's important to note is that the newly revised DISA Zero Trust Architecture now includes the addition of privileged account security.

This whitepaper will discuss the importance of privileged account security residing within the DISA Zero Trust reference architecture and why federal agencies need to follow the government's recommendations for implementing a Zero Trust framework.

Why Privileged Access Matters

The call to modernize federal government cybersecurity policies and procedures based on the new executive order is a critical move toward blocking the increase of sophisticated cyber threats from bad actors. With more and more ransomware attacks on the supply chain infrastructure, threats to public sectors, the healthcare industry and more, the U.S. government has now fully recognized the importance for implementing new cybersecurity best practices by including privileged access management (PAM) as a key tenet within the Zero Trust Architecture.

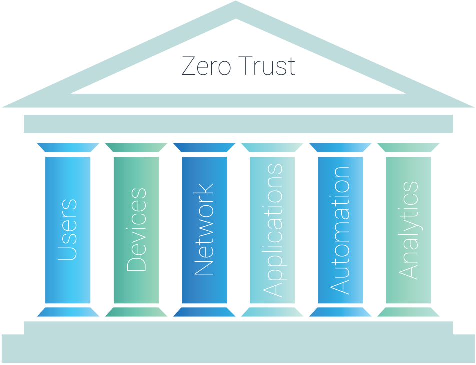
Adding privileged access management into the Zero Trust framework enables federal agency IT administrators to adopt the principle of least privilege and limit access to applications and data based on the user's role. Federal agencies are now armed with an extra layer of protection to limit break-ins at the perimeter.

Without the use of privileged access within federal agencies, the risk of advanced cyber attacks hitting not only the federal market but also other aspects of the public sector such as state and local governments will continue to become more and more prevalent. Agencies have responded by asking for budget increases for FY2022 with the White House, seeking nearly $10 billion to be allotted toward cybersecurity funding of federal civilian agencies. Other agencies have also requested budget increases to improve their cybersecurity posture, such as the Department of Defense that wants $10.4 billion for the cybersecurity budget in FY2022.[1]

[1] For IT, cyber policy goals, dig beneath the numbers of Biden's 2022 request, Federal News Network, June 1, 2021.

Privileged Access in the Zero Trust Security Model

Zero Trust can be thought of as a strategic initiative that, together with an organized framework, enables decision makers and security leaders to achieve pragmatic and effective security implementations. Zero Trust efforts need to incorporate, coordinate and integrate a challenging combination of policies, practices and technologies to succeed. A conceptual security model can be helpful to understand and organize these components.



Six Pillars of a Zero Trust Security Model

Pillar #1: Users

The ongoing authentication of trusted users is paramount to Zero Trust. This encompasses the use of technologies like identity, credential and access management (ICAM); multi-factor authentication; and continuous monitoring and validating user trustworthiness to govern their access and privileges. Technologies for securing and protecting users' interactions, such as traditional web gateway solutions, are also important.

Other capabilities, such as just-in-time (JIT), are equality important. For example, privileged access provides an "always-on" authorization, but users only need access for short periods of time. JIT supports the principle of least privilege (POLP) by decreasing standing access and offering the right access to the right user only for the time they need.

With PAM, federal agencies will reap the rewards of an improved time-to-value and risk mitigation simply because they govern the users POLP from the start.

Pillar #2: Devices

Device security, real-time cybersecurity posture and trustworthiness of devices are foundational attributes of the Zero Trust approach. Some "system of record" solutions, such as mobile device managers (MDM), provide data that can be useful for device-trust assessments. Additionally, other assessments should be conducted for each access request (e.g. examinations of compromise state, software versions, protection status, encryption enablement and more).

Devices act as gateways to company data and resources. It's critical that one only allows access to federal resources from trusted endpoints.

Pillar #3: Network

Some argue that perimeter protections are becoming less important for networks, workflows, tools and operations. This is not due to a single technology or use-case but rather a culmination of many new technologies and services that allows users to work and communicate in new ways. Zero Trust networks are sometimes described as "perimeter-less."

However, Zero Trust networks attempt to move perimeters in from the network edge and segment and isolate critical information from other data. The perimeter is still a reality, albeit in much more granular ways. The traditional infrastructure firewall perimeter, or "castle and moat" approach, is not sufficient.

The perimeter must move closer to the data in concert with micro-segmentation to strengthen protections and controls. Network security must expand as agencies grow their networks to transition partially or fully to Software Defined Networks (SDN), Software Defined Wide Area Networks (SD-WAN), and internet-based technologies. It is critical to:

1. control privileged network access,
2. manage internal and external data flows,
3. prevent lateral movement in the network,
4. have visibility to make dynamic policy and trust decisions on network and data traffic.

Being able to segment, isolate and control the network continues to be a pivotal point of security and is essential for a Zero Trust network.

Pillar #4: Application

Securing and properly managing the application layer, as well as computing containers and virtual machines, is central to Zero Trust adoption. Being able to identify and control the technology stack facilitates more granular and accurate access decisions. Multi-factor authentication is an increasingly critical part of providing proper access control to applications in Zero Trust environments.

Pillar #5: Automation

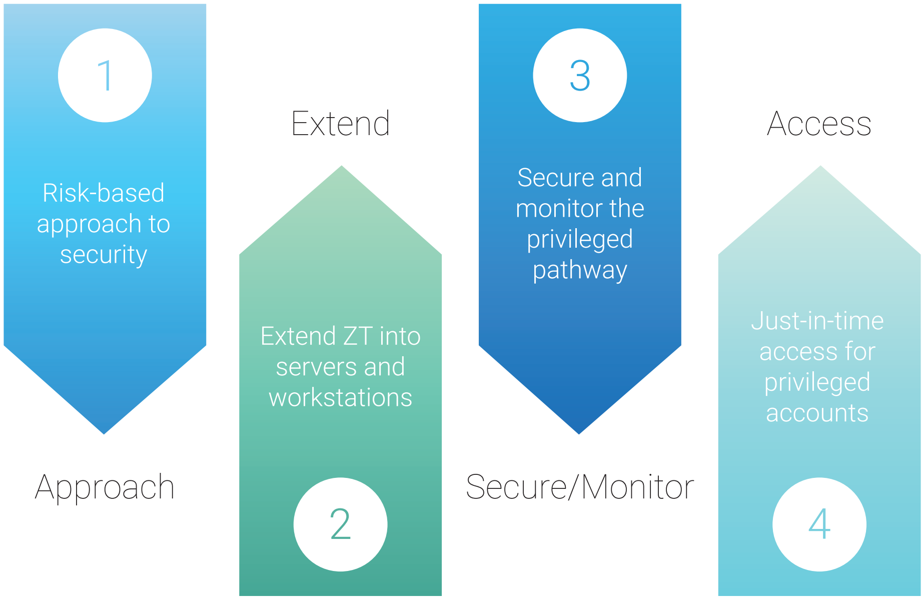
Security automation and orchestration must play together in a harmonious fashion. Zero Trust makes full use of security automation response tools that automate tasks across products through workflows, while allowing for end-user oversight and interaction. Security Operation Centers (SOC) commonly use other automated tools for security information, event management and user and entity behavior analysis. Security orchestration connects these security tools and assists in managing disparate security systems. When integrated, these tools can greatly reduce manual effort and event reaction times, while reducing costs.

Pillar #6: Analytics

Combatting an invisible threat can seem like an impossible feat. Zero Trust leverages tools like security information management (SIEM), advanced security analytics platforms, security user behavior analytics and other analytics systems to enable security experts to observe in real time what is happening and orient defenses more intelligently. The focus on the analysis of cyber-related event data can help develop proactive security measures before an actual incident occurs.

Securing the Network

With identity security functioning as the new perimeter, there are many best practices federal agencies can follow to implement a secure, Zero Trust approach to support privileged account security.


1
Risk-based approach to security
Approach
Extend
Extend ZT into servers and workstations
2
3
Secure and monitor the privileged pathway
Secure/Monitor
Access
Just-in-time access for privileged accounts
4

Implement a Risk-based Approach to Security

Insider threat and external attacks continue to persist, affecting every industry and often involve the misuse of privilege.[1]

The first step in implementing a risk-based approach is to secure the last line of defense, or privileged access. It's the road most traveled by both internal and external nefarious actors, as one break-in can lead to a payload of data.

Extend ZT into Servers and Endpoints

If an attacker or malicious insider gains access to a privileged account and its associated credential, the attacker will become indistinguishable from a fully validated and trusted user. This makes it difficult to detect high-risk activity and behavior.

Application control becomes an important factor in the "trust but verify and reverify" methodology. Organizations should implement restriction models. These restriction models should only trust certain applications that are run by specific accounts and under specific circumstances. Application control helps mitigate the risk of ransomware attacks and code injections, as examples, and is a foundational component of a Zero Trust strategy.

Beyond identifying all human and machine users, discovering and classifying all assets, both software and hardware, across the enterprise is critical. Federal agencies must understand and know which software versions are running on devices and establish security configurations, such as screen lock and disk encryption. This step is critical to ensure trustworthy devices.

Zero Trust is just the beginning. Start by providing “initial trust’” and continue to verify, reverify and put controls in place to mitigate risk. Introducing controls on the endpoint provides some level of trust, but it is just one piece to the Zero Trust puzzle. Federal agencies must secure and monitor the privileged pathway.

Secure and Monitor the Privileged Pathway

Trust, verification and monitoring network traffic are three main elements of both Zero Trust and BeyondCorp, Google’s implementation of the Zero Trust model. Key indicators of malicious activity are often overlooked or mischaracterized as benign because of an implicit trust that malicious activity will be flagged by detection mechanisms.[2]

Traditional perimeter models allow for an easy means of moving in and out of a network, which is why network visibility is critical. Detection, response, remediation and recovery are even more important. Monitoring the privileged access pathway prevents malicious insiders and external attackers from moving their attack forward. Organizations must place tight controls around the applications end users are accessing. Additionally, they must monitor, detect, respond and remediate before the business suffers irreparable damage.

There must be isolation layers between endpoints, users and target systems, and access must be monitored — specifically the “who, what and when.” It is important to create secure connections for end users connecting to critical assets and resources and to confirm an end user’s ability to review the session in real time. The key indicators of malicious activity should be predefined and automated controls to respond, when necessary, and take action must be implanted. As more and more employees work remotely — often from uncontrolled devices — organizations should provide application isolation layers to protect corporate resources from these devices — a critical aspect of Zero Trust.

[2] For IT, cyber policy goals, dig beneath the numbers of Biden’s 2022 request, Federal News Network, June 1, 2021.

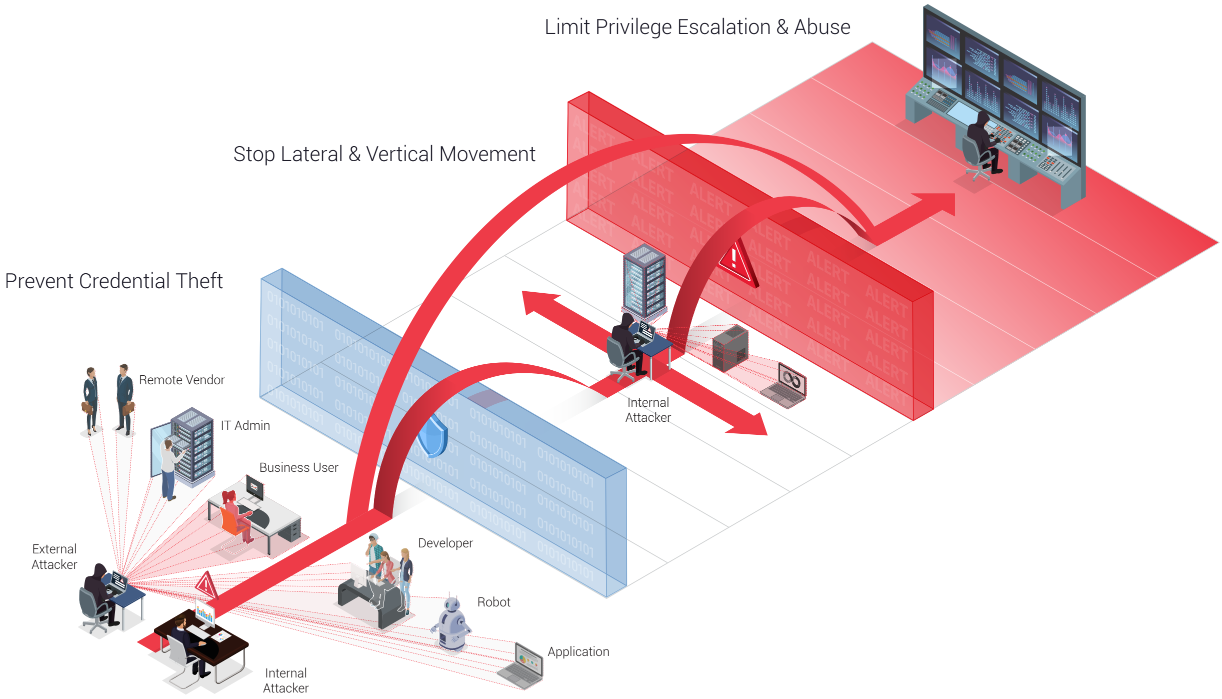
The CyberArk Identity Security Platform

The call to action for federal agencies to incorporate cybersecurity measures is an imperative — not an option. They must work toward securing their data and implement identity security methods for Zero Trust.

CyberArk has established itself as the leader in the **privileged access management industry**, protecting privileged accounts and ensuring data and sensitive credentials are not compromised — on-premises and in the cloud. CyberArk has developed a prescriptive approach designed to help organizations and government agencies improve security and reduce risk by establishing and maintaining strong privileged access management hygiene. The CyberArk Blueprint framework aligns with the DISA Zero Trust pillars today by incorporating a thorough understanding of the security risks and challenges organizations face daily by implementing three guiding principles:

- Prevent credential theft.
- Stop lateral and vertical movement.
- Limit privilege escalation and abuse.

CYBERARK BLUEPRINT: THREE GUIDING PRINCIPLES



The CyberArk solution includes a family of products designed for the Identity Security Platform and supports Zero Trust with the following family of solutions.

Privileged Access

CyberArk's Privileged Access Manager provides federal agencies the foundational controls to mitigate the risks and defend against attacks. The solution can be deployed as both an on-premises or PAM as a Service offering to secure privileged identities for both human and machine to keep unauthorized users out of the network. Core capabilities include:

- **Credential Protection and Management:** The solution centrally secures and controls access to privileged credentials based on privileged access security policies. Automated password and SSH key rotation reduces the timeconsuming and error-prone task of manually tracking and updating privileged credentials to easily meet audit and compliance standards.

> CyberArk's C3 Alliances supports over 300 integrations with it's technology ecosystem, providing the ability to manage privilege credentials for the most critical applications.

- **Session Isolation and Monitoring:** The solution isolates and secures privileged user sessions, protects target systems from malware on endpoints, and enables privileged access without exposing sensitive credentials. Monitoring and recording capabilities enable federal agencies to view privileged sessions in real-time, automatically suspend and remotely terminate suspicious sessions, and maintain a searchable audit trail of privileged user activity.
- **Privileged Threat Detection and Response:** The solution delivers advanced analytics to detect anomalies when they occur. The out-of-the-box analytics combines deterministic algorithms, statistical modeling, machine learning and behavior profiling to enable federal agencies to make calculated decisions based on both trust and risk. Combining intelligent analytics and response results in a force multiplier that inherently scales security proficiency, especially with resource constraints, present risk to federal agencies.

With CyberArk's Endpoint Privilege Manager's application control, least privilege and Zero Trust capabilities, IT operations and security teams can allow approved applications to run, while blocking malware, including ransomware. Unknown applications can run in "Restricted Mode," which prevents them from accessing corporate resources, sensitive data or the Internet. These applications can also be sent to Endpoint Privilege Manager's cloud-based application analysis service, which integrates with data feeds from CheckPoint, FireEye, Palo Alto Network and other services for additional analysis. The solution lowers security risk and configuration drift on endpoints, while reducing help desk calls from end users. Based on testing by CyberArk Labs, the removal of local administrator rights — combined with application control — is extremely effective in preventing ransomware from encrypting files.

Access

CyberArk Identity delivers next-gen access, protecting organizations with single sign-on and multifactor authentication. With CyberArk Identity, federal agencies experience secure access everywhere, with reduced complexity and newfound confidence to adopt modern business models and deliver exceptional customer experiences.

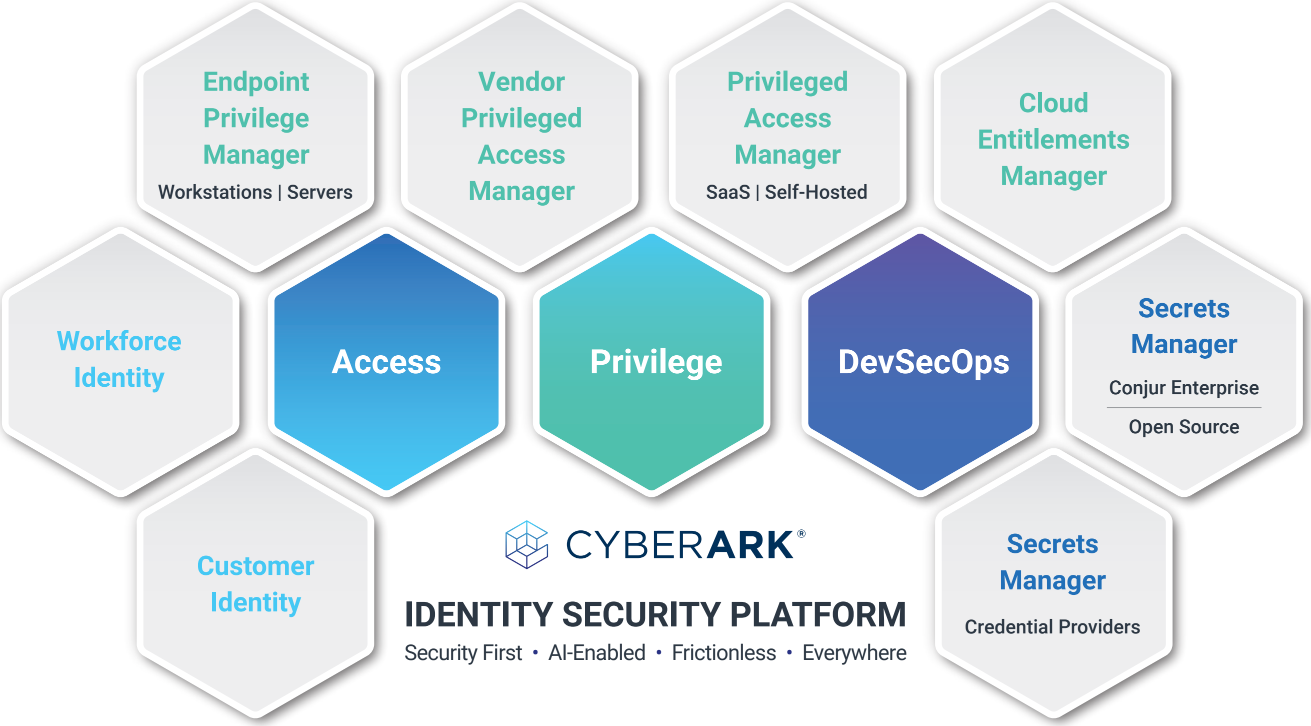
Organizations can take a step toward Zero Trust architecture by strengthening access controls with frictionless secondary authentication using CyberArk's Privilege Access Manager for end users.

Multi-factor authentication (MFA) adds an extra layer of protection before access to corporate applications is granted. Leveraging device, network and user behavior context, CyberArk Identity intelligently assigns risk to each access event and allows you to create dynamic access policies that are triggered when anomalous behavior is detected.

The CyberArk Identity App Gateway is available as an add-on to the CyberArk Identity Single Sign-On service. It provides an easy and secure way to access on-premises applications without requiring configuration of VPN clients, modification of firewall policies or changing of on-premises code. With CyberArk Identity, IT teams can provide users SSO access to applications required to perform responsibilities and manage user identities across all applications and endpoints from a single console. CyberArk Identity enforces Zero Trust by securing access to legacy applications with CyberArk Identity Adaptive Multi-Factor Authentication and configures per-application access based on user roles. CyberArk Identity App Gateway enables you to prevent both inadvertent and intentional identity–related security breaches and manage access policies for all applications in one management interface

DevSecOps

Enterprises are increasingly adopting DevOps methodologies and automation to improve business efficiency and accelerate innovation, while also leveraging commercial and internally developed applications. However, each application, automation tool and other non-human identity relies on some form of privileged credential to access sensitive resources. Additionally, application and IT environments can vary significantly within the organization — from highly dynamic native cloud to largely static and even mainframe based. The privileged credentials used by applications need to be secured by a solution such as the CyberArk Secrets Manager, regardless of the application type and compute environment. These credentials pose a variety of challenges for IT security, operations and compliance teams. Application and other non-human credentials must be managed. In addition to eliminating hard-coded credentials in code and scripts, approaches and techniques — including strong authentication, least privilege, role-based access controls, credential rotation and audit — should also be used in a Zero Trust environment


Endpoint Privilege Manager
Workstations | Servers
Vendor Privileged Access Manager
Privileged Access Manager
SaaS | Self-Hosted
Cloud Entitlements Manager
Workforce Identity
Access
Privilege
DevSecOps
Secrets Manager
Conjur Enterprise
Open Source
Customer Identity
CYBERARK
IDENTITY SECURITY PLATFORM
Security First • AI-Enabled • Frictionless • Everywhere
Secrets Manager
Credential Providers

Conclusion

Zero Trust is a journey — not a destination.

As federal agencies put the requirements of the cybersecurity executive order into place, there's no question that Identity Security has become the first line of defense to keep the bad threat actors out. Identity is the new security perimeter, and any compromise to privilege accounts will only result in untold dire consequences for citizens and the nation.

LEARN MORE

Top 5 Reasons to Prioritize Privileged Access Management as-a-Service

Dive into why Privileged Access Management as a Service is a requirement for federal agencies to comply with the new Zero Trust Architecture with this eBook.

GET THE EBOOK

Achieve Zero Trust with Identity Security

Read more about how to reach Zero Trust in this whitepaper.

GET THE WHITEPAPER

Request a demo of CyberArk's Privileged Access Manager and find out how the solution can manage credentials for privileged users and application accounts.

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.

CYBERARK®

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. U.S., 03.22 Doc. TSK-1080 (280401)

THIS PUBLICATION IS FOR INFORMATIONAL PURPOSES ONLY AND IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER WHETHER EXPRESSED OR IMPLIED, INCLUDING WARRANTY OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, NON-INFRINGEMENT OR OTHERWISE. IN NO EVENT SHALL CYBERARK BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND IN PARTICULAR CYBERARK SHALL NOT BE LIABLE FOR DIRECT, SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE OR LOSS OF USE, COST OF REPLACEMENT GOODS, LOSS OR DAMAGE TO DATA ARISING FROM USE OF OR IN RELIANCE ON THIS PUBLICATION, EVEN IF CYBERARK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.