



THE AGE OF DIGITAL TRANSFORMATION: 5 KEYS TO SECURING YOUR BUSINESS CRITICAL APPLICATIONS

INTRODUCTION

The digital transformation of enterprise IT has dramatically increased the challenge of protecting business critical applications. CyberArk research has found gaps between how well business leaders believe they are securing their business-critical applications – and the reality.

Learn the 5 key requirements to better protect your business critical applications on endpoints in on-premises data centers, the cloud and via SaaS. Meeting these requirements ensures only the right people have the right access to your most valuable applications and business data.

Contents

- Business Critical for a Reason 3
- Protecting Business Critical Applications 5
- Most Attacks are Connected to Compromised Privileged Credentials..... 7
- 5 Keys to Securing Business Critical Applications 9
- Summary 11
- Learn More 13

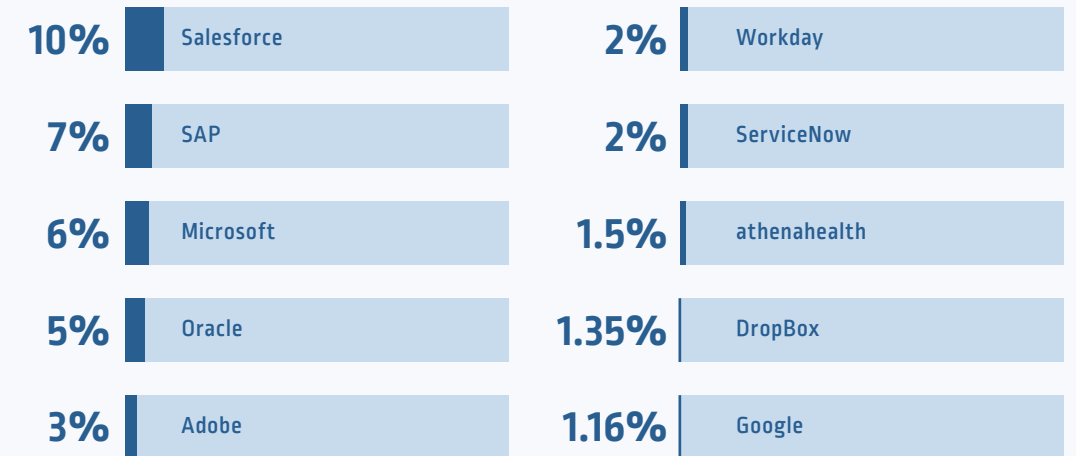
BUSINESS CRITICAL FOR A REASON

Business critical applications are key to getting daily business done. Of course, what is considered critical can vary by industry and organization, from Office 365 to enterprise resource planning (ERP) applications. But one thing is clear: their disruption immediately impacts the bottom line with continuing business and fiscal risks from compromised data.

Common scenarios for the disruption of business critical applications include:

- **Compromised ERP** applications can make it difficult for manufacturers to source critical components, for retailers to stock stores, for hospitals to have medicine, etc.
- **Unavailable eCommerce** applications mean immediate lost sales – and potentially angry customers.
- **Broken financial transaction** applications, from customer-facing (e.g. ATMs) to B2B (e.g. Swift) can mean direct financial losses, lost credibility and regulatory penalties.
- **Compromised healthcare** applications, such as patient portals or Electronic Healthcare Records software, can result in the inability to deliver care and financial penalties due to the breach of Electronic Personal Health Information (ePHI).
- **Disrupted Customer Relationship Management (CRM) systems** can hurt on-going sales, customer loyalty and provide an entrée for competition.

Market Share of Top 10 Enterprise Apps (40% total market share)



Source: Apps Run the World Apps Top 500 Report, Market Share Data, 2017



“

The need to secure data and critical workloads, such as business-critical applications, has become a board-level initiative in organizations world-wide.”

The Impact of Cloud on ERP: A Survey Report on the Migration of ERP to Cloud Environments, Cloud Security Alliance, 2018.

“

“In the past, when the majority of enterprises’ data was located on premises, organizations placed a great amount of security focus on network and device security. The idea was that **having a hard outer perimeter, backed up by device-level defenses within the firewall, was the best approach to securing sensitive data.**”

2019 Thales Data Threat Report

PROTECTING BUSINESS CRITICAL APPLICATIONS: PERCEPTION VS. REALITY

A recent CyberArk survey of EMEA organizations¹ found 72% of respondents believe they can protect their business-critical applications and stop data breaches at the perimeter.

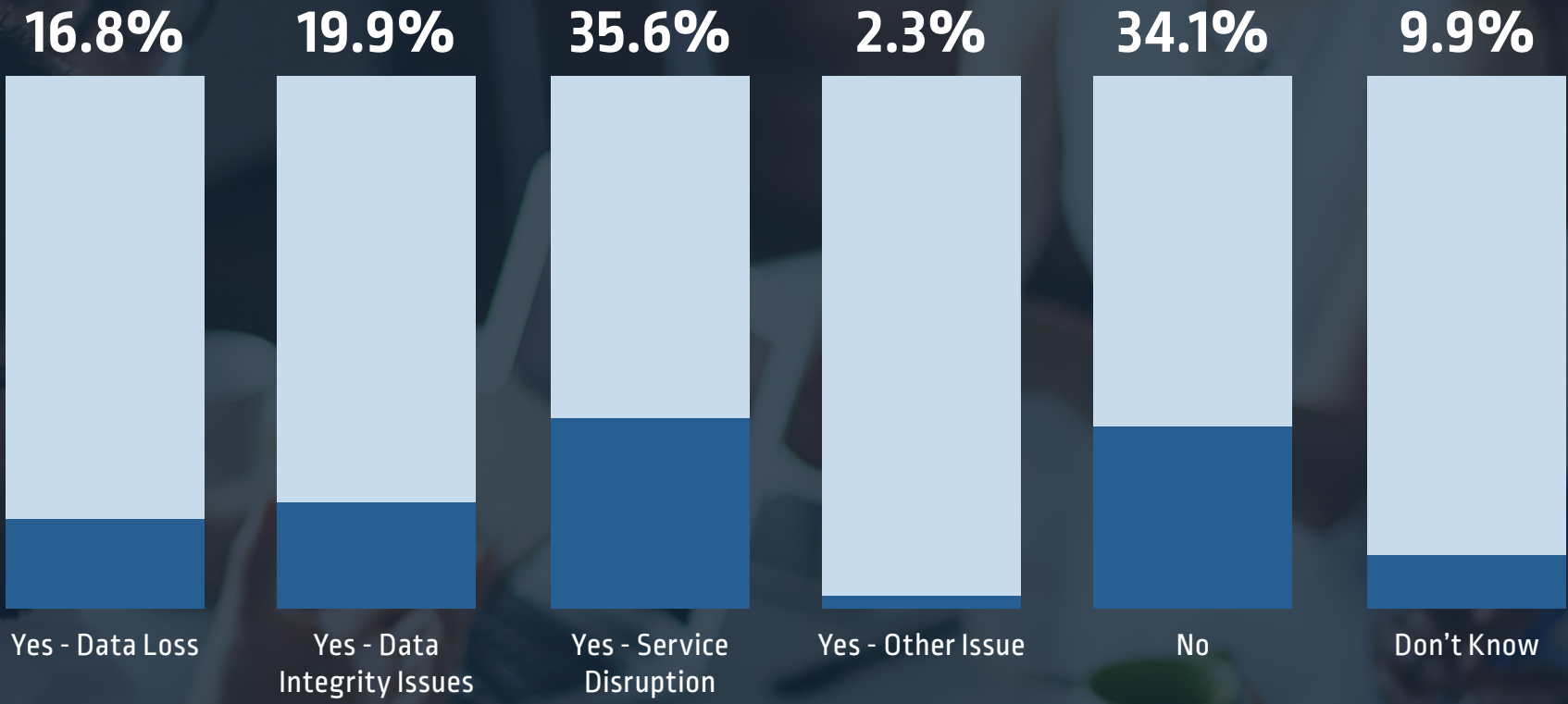
Even with the acknowledged importance of business critical applications to the bottom line, 69% of respondents in our survey said that either their cyber security measures did not give priority to protecting business critical applications—or (worse) they didn’t know.

And yet, the threat from increasingly advanced and fast external cyber-attacks (and malicious insiders) has never been higher. In fact, the same CyberArk research found fully 56% of these respondents had some kind of security incident involving business critical applications within the last 24 months.

Clearly there is a disconnect between organizations believing they can protect their business critical applications and the reality of the incidents reported.

¹ CyberArk EMEA Business Critical Application Survey 2019

Has your organization faced any incidents over the last 24 months that have resulted in any of the following outcomes to business critical apps?



Respondents: 1,450 | CyberArk EMEA Business Critical Application Survey, 2019; question allowed for the selection of more multiple responses.

“

Privileged accounts represent the largest security threat an organization faces today. Forrester estimates that at least 80% of data breaches have a connection to compromised privileged credentials, such as passwords, tokens, keys and certificates.”

The Forrester Wave™: Privileged Identity Management, Q4 2018

MOST ATTACKS ARE CONNECTED TO COMPROMISED PRIVILEGED CREDENTIALS

Securing business-critical applications means access must be reserved for individuals or machines (application-to-application) with the proper credentials and permissions.

Cybercriminals and malicious insiders take advantage of complexity and the business-critical application environment is becoming increasingly complex. Business critical applications now run on-premises, in the cloud and via SaaS applications – many times a combination of the three.

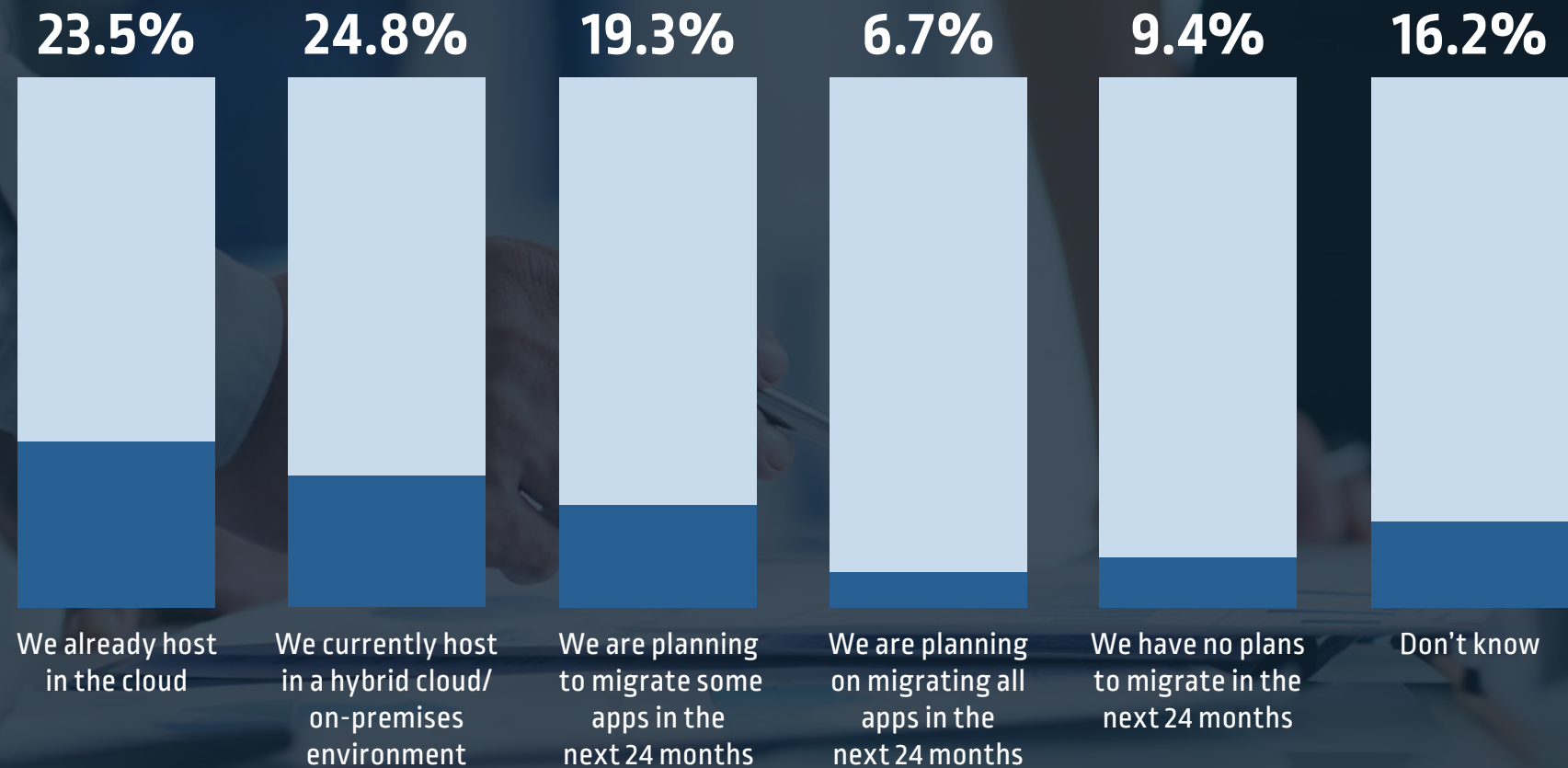
Throughout that environment, there are a wide variety of privileged users who require access: employees working both on-premises and at remote endpoints, third party partners and vendors and developers making changes to business critical applications.

Privileged credentials are also embedded in machine-to-machine interactions. More complex business-critical applications increasingly require application-to-application access; for instance, this could be a script or API that automatically loads data into a CRM system or, alternatively, an in-house application that processes financial transactions and connects to a CRM system with an API to push and pull transaction and customer data.

As with human users, change is constant as new applications are acquired or licensed, connected, disconnected, moved to the cloud and retired.

How do you effectively manage and track privileged access in this complex environment without breaking the bank?

How would you describe your organization's plan to migrate business critical applications to the cloud?



Respondents: 1,450 | CyberArk EMEA Business Critical Application Survey, 2019

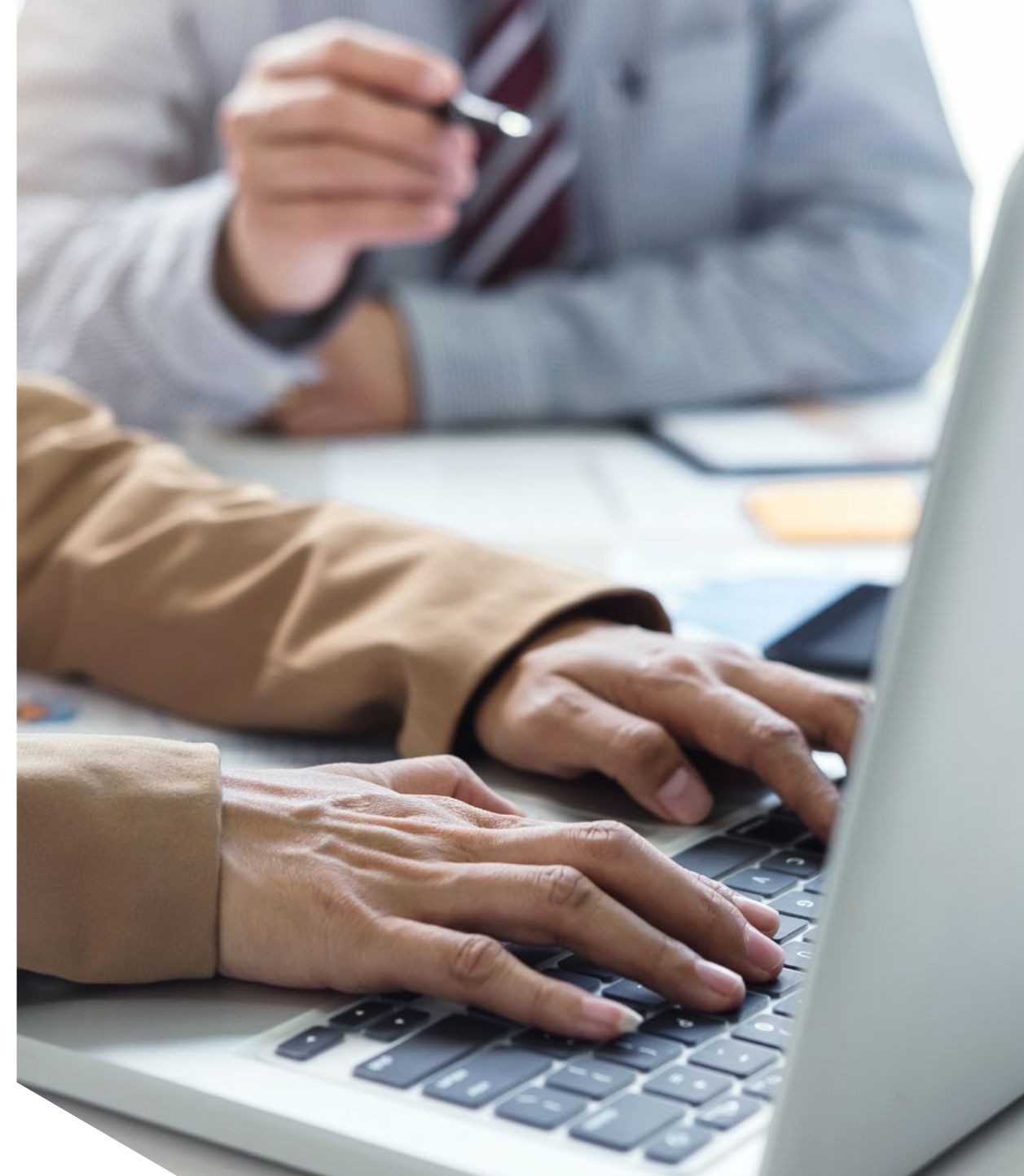
5 KEYS TO SECURING BUSINESS CRITICAL APPLICATIONS

Privileged access security solutions are designed to control and protect privileged credentials across all environments.



Identify what apps are truly business critical

As a security leader, it goes without saying that you need to be close to the business. Get to know your line of business leaders and the leaders of key functions such as finance, human resources, and marketing. Once you have a handle on important business initiatives, you will be in a better place to identify the business apps that are truly critical. These could be SaaS applications or even custom applications that are being built using DevOps tools and methodologies. You will also have a better understanding of who is using the applications and for what, which will enable you to prioritize which applications need privileged access security most urgently.





Get comfortable with the Cloud (and Securing It)

Understand what your cloud strategy, migration plan and timelines are for on-premises applications that are moving to the cloud or new cloud-native applications. Partner with cross-functional stakeholders to ensure privileged access security is a front-and-center consideration when looking to migrate applications to the cloud or to adopt new cloud applications.



Secure the access of the admins who manage your business critical applications

Once business critical applications are identified, vault and rotate all admin credentials associated with these apps, including the underlying infrastructure. Also isolate sessions to prevent credential theft and provides a full audit trail of all privileged activity involving your business-critical applications. Bear in mind that in many cases, the admins for your these apps will sit outside IT as part of a line of business or within a functional organization such as Finance, HR, or Marketing.



Don't forget the machines

Secure the human and application-to-application privileged credentials and service accounts used by your business-critical on-premises applications, SaaS applications as well as your cloud-native applications built using DevOps tools and methodologies. The use of hard-coded credentials represents a significant security risk to your business critical applications and should be eliminated.



Limit the risk to your business critical applications from unmanaged end user workstations

Prevent attacks against your business critical apps that start on Windows and Mac workstations by removing local admin rights to prevent the download of malware. Also invest in anti-phishing protection and security education and awareness to educate end users so they can recognize phishing attacks as well.

Privileged access security solutions offer you the opportunity to take a holistic approach to protecting your business-critical applications. No matter how your environment and users change, you can prioritize and protect your most valuable applications and data.


SUMMARY

Everyone Wins Securing Business Critical Applications

The downside of compromised business critical applications is pretty clear: negative impact to the bottom line, soured customer relations and continuing business risks from compromised data. Conversely, the upside of implementing a strong privileged access security solution does more than secure applications, it also offers business benefits to the entire organization.

CISOs can spend their security dollars prioritizing the protection of applications and data critical to the business. It also allows them to assure fellow executives that they have the best possible protection against new vulnerabilities and changing threats.

CIOs can securely support digital transformation, taking advantage of game-changing IT services, without worrying about significant outages or compromised critical applications. As the ultimate owner of business critical applications, CIOs can be more confident that they can “keep the lights on” and deliver fully developed, key services even in the event of an orchestrated attack.



CFOs and Executives responsible for managing the company’s finances and risk profile can show regulators, auditors, government agencies and rule-makers that they have done everything possible to protect high-value company assets, minimizing the risk of financial losses, penalties and damage to the brand.

CMOs and other line-of-business leaders can concentrate on adding value to their core product/service areas, knowing the services and data that only a privileged few should be able to access are fully protected.

By protecting business critical processes through privilege account security, everyone responsible for the success of the business wins.

LEARN MORE

You can get started evaluating how well you are protecting your business critical applications today. Visit us at www.cyberark.com.

About CyberArk

CyberArk is widely recognized as the global leader in privileged access security, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. The company is trusted by the world's leading organizations, including over half of the Fortune 500, to protect against external attackers and malicious insiders.

CyberArk offers Conjur Open Source, a secrets management solution tailored specifically to the unique infrastructure requirements of native cloud and DevOps environments. The solution helps developers work with IT and information security organizations to secure and manage secrets used by non-human users (applications, microservices, CI/CD tools, APIs, scripts, etc.) throughout the DevOps pipeline.

An enterprise version, built on the Conjur Open Source core, integrates with existing Active Directory, LDAP, and SIEM systems to help protect and extend the organization's previous investments, and preserve established security models and practices. CyberArk solutions enable organizations to consistently manage privileged access for both human and on-human users.



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.

3.19. Doc. 329388347

