CYBERARK®

WHITE PAPER

CYBERARK BLUEPRINT FOR IDENTITY SECURITY SUCCESS

www.cyberark.com

Table of Contents

Summary 3

Introduction – Any identity can become privileged under certain conditions 3

CyberArk Blueprint Helps Reduce Identity Security Risks 4

Three Guiding Principles for Identity Security Success 4

- Guiding Principle One: Prevent Credential Theft 5
- Guiding Principle Two: Stop Lateral and Vertical Movement 6
- Guiding Principle Three: Limit Privilege Escalation and Abuse 7

Phased Implementation Plan Aligns Prescriptive Actions with Risk Reduction 8

- Stage One – Rapid Risk Mitigation 8
- Stage Two – Core Security 8
- Stage Three – Enterprise Program 9
- Stage Four – Mature the Program 9
- Stage Five – Advanced Security 9

Conclusion 9

Next Steps 9

About CyberArk 10

Summary

In today's hybrid and multi-cloud world, Identity is the new perimeter. Physical and network barriers have dissolved, and all identities can be an attack path to an organization's most valuable assets. Businesses must strengthen the security of their identities but implementing an effective Identity Security program is a challenge for many organizations as the identity landscape is large, complex and continuously evolving.

CyberArk has developed a compressive blueprint to help organizations assess and prioritize identity vulnerabilities, strengthen security and reduce risks. Leveraging CyberArk's vast experience and deep subject-matter expertise, the CyberArk Blueprint for Identity Security Success lays out a prescriptive, risk-aligned plan for establishing and maintaining an effective Identity Security program.

This paper reviews common Identity Security challenges and explains how the CyberArk Blueprint can help organizations improve Identity Security systems and practices, reduce security vulnerabilities and mitigate risk.

Introduction – Any identity can become privileged under certain conditions

Identities represent one of the largest security vulnerabilities any organization faces today. According to Verizon's 2020 Data Breach Investigation Report, 80% of breaches tied to hacking involve brute force or lost or stolen credentials.[1] And the reasons why they are so attractive to attackers are simple. Identities exist throughout the entire IT spectrum of a business and they help authenticate and authorize access to an enterprise sensitive data, business processes and systems.

Furthermore, with the physical and network barriers dissolved due to an accelerated adoption of cloud and automation services alongside with a growing remote workforce, any identity can become privileged under certain conditions.

- Developers or DevOps engineers often require access to source code to create products and services.
- Applications or RPAs need high privileges to access corporate resources to perform their tasks.
- Workforce team members need to execute sensitive business processes or access sensitive data.
- Third party vendors need access corporate resources remotely in order to perform their duties.

All these types of privileged access represent high risk to the organization and therefore require high level of security controls.

IT and security teams can overcome these challenges and minimize the growing risks tied to identities by:

- Taking a close look at how attackers exploit privileged identities. What are the most common privileged access attack vectors? How does the perpetrator think and behave in each case?
- Taking a practical, phased approach to Identity Security. Identifying the most-sensitive identities and their related accounts. Zeroing in on identities that could jeopardize mission-critical infrastructure or expose confidential data.
- Developing a prioritized plan to reduce vulnerabilities and strengthen security. Which actions are most important? Which items can be achieved quickly and with minimal resources? Which require significant time and effort?
- Continuously reassessing and improving the Identity Security plan to address evolving threats and new technologies.

CyberArk Blueprint Helps Reduce Identity Security Risks

CyberArk has developed a prescriptive blueprint framework to help organizations establish and evolve an effective Identity Security program. The CyberArk Blueprint for Identity Security Success (or CyberArk Blueprint for short) is designed to defend against three common attack chain stages used to steal data and wreak havoc. Simple, yet comprehensive, the CyberArk Blueprint provides a prioritized, phased security framework that closely aligns Identity Security initiatives with potential risk reduction, helping organizations address their greatest liabilities as quickly as possible. It should be used as a tool to help guide your own Identity Security program roadmap development, in combination with your current state, internal priorities and desired business outcomes.

The CyberArk Blueprint was built with contemporary organizations and extensibility in mind. It prescribes Identity Security controls and best practices for organizations using conventional on-premises infrastructure and software development methods, as well as for organizations embarking on digital transformation projects such as migrating infrastructure to the cloud, adopting CI/CD practices, optimizing processes through robotic process automation or implementing SaaS solutions for business-critical applications.

The CyberArk Blueprint reflects the combined knowledge and experience of CyberArk's global Sales, Sales Engineering, Security Services and Customer Success organizations. As a recognized leader, CyberArk is uniquely positioned to deliver a thorough and effective Identity Security plan:

- CyberArk solutions are trusted by 6,300+ customers, including more than 50% of the Fortune 500, across a wide range of industries including financial services, insurance, manufacturing, healthcare and tech.
- CyberArk's Remediation and Red Team have been front and center in helping companies recover from some of the largest breaches of the 21st century. Additionally, CyberArk draws on the insights of its Threat Research and Innovation Lab.
- CyberArk Security Services and Customer Success organizations have decades of real-world implementation and support experience, and have a detailed, first-hand understanding of the risks present within human and non-human identities and best practices.
- Leading research and advisory firms recognize CyberArk as a privileged access management leader for both completeness of vision and ability to execute.[2]

Three Guiding Principles for Identity Security Success

While every organization's IT environment is unique, perpetrators can attack virtually any business by following well established steps in the attack chain: 1) gain unauthorized access to privileged identities, 2) traverse the network looking for high-value targets, and 3) use elevated privileges to steal confidential information or disrupt services. The CyberArk Blueprint helps organizations strengthen their security posture by thinking like an attacker and defending against the three techniques adversaries typically use to access privileged identities, steal data and take down systems.

More specifically, the CyberArk Blueprint for Identity Security Success is based on three guiding principles:

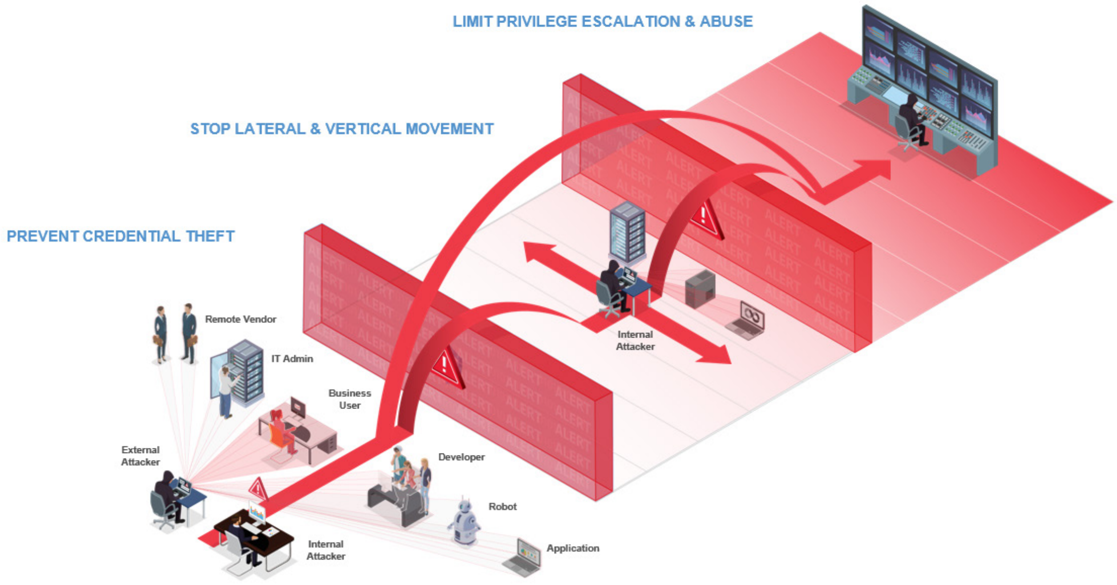
1. Prevent credential theft
2. Stop lateral and vertical movement
3. Limit privilege escalation and abuse

The Blueprint is designed to protect any customer environment, strengthening Identity Security for on-premises, cloud or

[3] Magic Quadrant for Privileged Access Management, Gartner, 2018

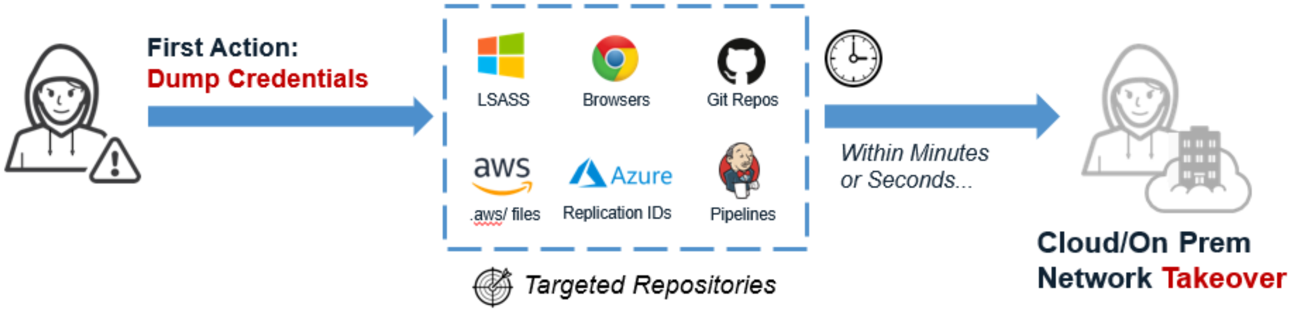
hybrid infrastructure. It lays out a pragmatic, risk-based implementation plan that introduces security controls in stages, helping businesses address their most pressing needs in the short-term, while providing a long-term plan to address the more advanced security use cases.

CYBERARK BLUEPRINT: 3 GUIDING PRINCIPLES



Guiding Principle One: Prevent Credential Theft

Many organizations rely on inefficient manual processes to assign and track privileged identities and their corresponding privileged accounts. Passwords and keys sometimes remain unchanged for months or even years after they are issued. Former employees, contractors and business partners often maintain access to critical applications and systems long after termination, exposing the business to data breaches and malicious attacks. Disgruntled employees or external attackers can exploit dormant accounts or stale passwords to mount sophisticated attacks.



In addition, attackers can obtain non-human credentials (secrets used by applications, machines, bots, etc.) from public source code repositories like GitHub (developers often hard-code secrets into applications and scripts in clear text), from credential files used for cloud services like AWS and from configuration or pipeline files used by CI/CD platforms like Jenkins or Ansible.

Once a savvy attacker gains access to privileged account credentials they can breach other critical enterprise resources in just minutes. CyberArk security professionals have seen adversaries go from penetrating a workstation to gaining full domain admin rights on a domain controller in less than 20 minutes!

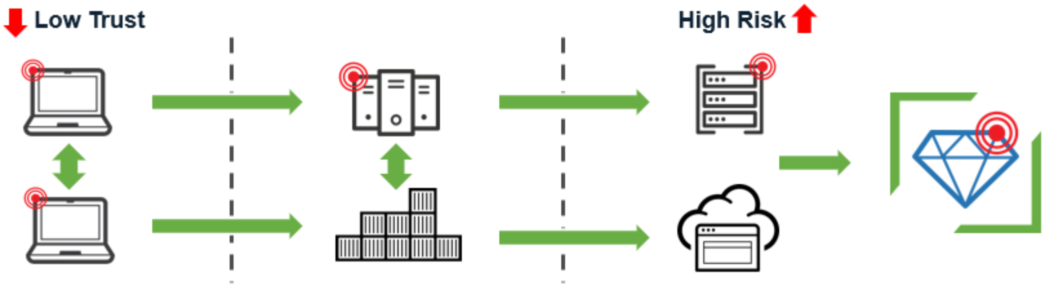
To prevent credential theft, CyberArk recommends organizations:

1. **Discontinue disjointed, manual credential and secrets management processes.** Introduce a hardened and secure digital vault to centrally store and track privileged account credentials. Automatically rotate passwords and keys based on policies.
2. **Isolate privileged sessions.** Use a secure proxy server to decouple endpoints from target systems, segregate privileged session traffic and avoid transmitting credentials and revealing them to end users. With this approach, users authenticate to the proxy server and then gain privileged access to target systems via a separate session.
3. **Remove hard-coded credentials from applications, robotic process automation platforms, CI/CD tools and other non-human entities.** Introduce a centralized, automated application access management solution to keep secrets out of repositories, source code and hard drives. With this approach, authorized applications automatically retrieve secrets from the secure digital vault in real-time.
4. **For an additional layer of protection, implement credential theft blocking controls directly at the OS level.** Actively monitor common credential stores such as the LSASS process, browser caches, remoting tools like WinSCP or VNC, service accounts, and SAML key repositories. Proactively block unauthorized access to these repositories. Cutting off access to these well-known credential sources makes it more difficult for attackers to make headway.

Guiding Principle Two: Stop Lateral and Vertical Movement

With credentials in hand, an adversary will often pivot from lower-value systems to higher-value targets that contain sensitive information or can be used to control an environment. This can take two forms:

1. Moving laterally within the same "risk tier" in the hopes of finding better, more useful credentials, or
2. Moving vertically from one risk tier to another (move from workstations to servers for example) to get ever closer to the "crown jewels."



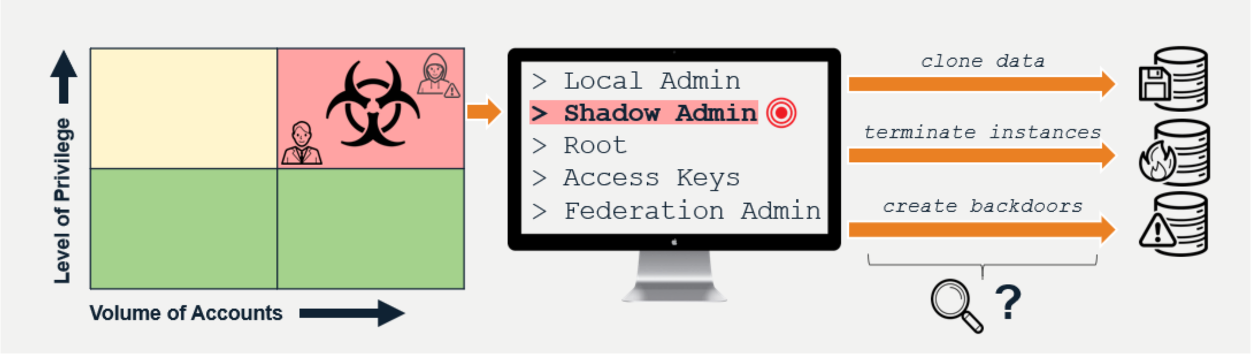
To prevent lateral or vertical movement, CyberArk recommends organizations:

1. **Rotate and randomize credentials to stop lateral and vertical movement.** Rotating credentials limits an attacker's window of opportunity. While eliminating shared common credentials across endpoints prevents traversal.
2. **Move to a *Zero Trust* model.** Enable just-in-time privilege elevation, allowing users to access privileged accounts or run privileged commands on a temporary, as needed basis, only when required.

3. **Implement session isolation (with credential boundaries where appropriate) to limit an attacker's range of motion. .** For example, don't grant a single-domain account access. Instead split up access, using distinct accounts for datacenter administration and server administration.

Guiding Principle Three: Limit Privilege Escalation and Abuse

Identities exist everywhere, and the privileged accounts tied to them are pervasive. Every host, application, database and platform have its own built-in administrative credentials. Many organizations administer credentials manually and have limited visibility and control over the privileged activities being performed. And to make matters worse, many organizations over-privilege end-users and application processes, granting them full admin rights, regardless of their actual requirements. The proliferation of privileged identities, and lack of administrative visibility and control create a wide attack surface for malicious insiders and external attackers to exploit.

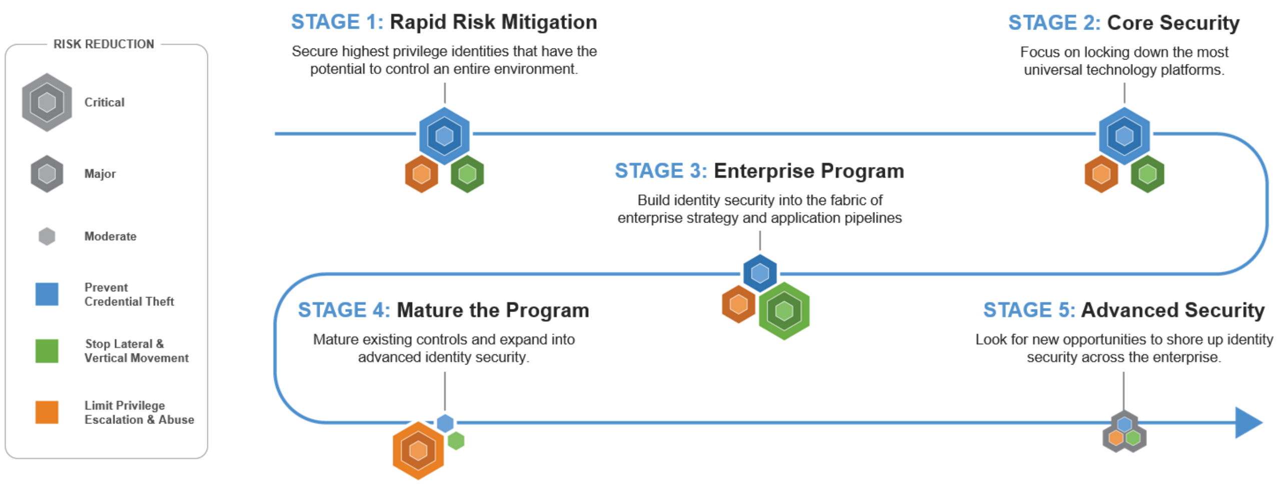


To limit privilege escalation and abuse, CyberArk recommends:

1. Embrace the principle of least privilege to reduce attack surfaces and contain bad actors. Implement least-privileged access controls at the OS level in the most widely deployed platforms: Windows, Unix and Mac endpoints. Introduce just-in-time security controls, granting users access to specific systems, applications or functions for finite periods of time, on an as-needed basis.
2. Use a privileged threat analytics solution to automatically analyze privileged session activity, identify suspicious actions and detect in-progress attacks. Analytics solutions collect and analyze data from multiple sources, using advanced algorithms to intelligently establish baselines, evaluate threats and assess risks.
3. Privileged threat analytics solutions provide alert notifications of attacks and data breaches, assigning a risk score to each incident. Best-of-breed solutions automatically respond to high-severity incidents taking remedial actions to thwart in-progress attacks.

Phased Implementation Plan Aligns Prescriptive Actions with Risk Reduction

CyberArk recommends a phased Identity Security implementation plan that aligns program milestones with risk reduction potential and aligns cybersecurity investments with benefits. Each stage of the implementation plan is formulated with the three guiding principles in mind. The prioritized plan targets the threats that pose the greatest potential risk in the preliminary stages, while shoring up other vulnerabilities over time. Stages one and two have a major impact on credential theft risk, stage three has a major impact on lateral and vertical movement risk, stage four has a major impact on privilege escalation and abuse risk, and stage five is all about mitigating any remaining vulnerability.


RISK REDUCTION
Critical
Major
Moderate
Prevent Credential Theft
Stop Lateral & Vertical Movement
Limit Privilege Escalation & Abuse

STAGE 1: Rapid Risk Mitigation
Secure highest privilege identities that have the potential to control an entire environment.

STAGE 2: Core Security
Focus on locking down the most universal technology platforms.

STAGE 3: Enterprise Program
Build identity security into the fabric of enterprise strategy and application pipelines

STAGE 4: Mature the Program
Mature existing controls and expand into advanced identity security.

STAGE 5: Advanced Security
Look for new opportunities to shore up identity security across the enterprise.

Stage One – Rapid Risk Mitigation

In the first stage of the plan, secure the highest privileged identities that represent the greatest potential risk as they can be exploited to control an entire environment, with entitlements such as Cloud admin, domain admin or system admin.

Prevent unauthorized access and reduce risk for human users by leveraging adaptive multi-factor authentication, isolating privileged sessions, rotating passwords and intelligently monitoring and analyzing privileged session activity for domain admins, hypervisor admins and Windows local admins. Apply adaptive multi-factor authentication, single sign-on (SSO) and least privilege controls to role-based Cloud Admins and Shadow admins. For non-human consumers of high privilege secrets, such as third-party security tools, remove their hard-coded credentials and replace that with an API call to retrieve on demand credentials. For any embedded OS services that are running as domain admin, reduce the permission and/or manage the associated service account.

Stage Two – Core Security

In stage two, lock down the most universally deployed technology platforms. Secure privileged access to CI/CD platforms (consoles and CLIs), PaaS admins and other cloud privileged entities by applying adaptive multi-factor authentication and applying least privilege controls. Secure workstation local admins, privileged active directory users, NIX* root account IDs (passwords and SSH Keys) by isolating sessions and protect third party business tools and application servers by removing hardcoded credentials.

Stage Three – Enterprise Program

In stage three, incorporate Identity Security solutions and best practices into the overall enterprise security strategy and throughout application pipelines. Implement adaptive multi-factor authentication and SSO for mission critical web applications. Remove hard-coded secrets from dynamic applications (e.g. containerized apps, microservices) to prevent credential theft. Secure root-similar accounts on *NIX systems, and secure default built-in database admin accounts. Implement OS-level least privileged access controls for IT admin workstations. Introduce a just-in-time authentication and authorization solution to give remote third-party IT service organizations temporary, secure privileged access without requiring VPNs or special-purpose agent software.

Stage Four – Mature the Program

In stage four, further strengthen the organization's security posture by expanding into advanced Identity Security controls. Go deeper by applying adaptive multi-factor authentication and SSO controls to the core web applications and by removing hard-coded credentials from static applications (e.g. legacy client/server applications). Secure named database admin accounts. Implement OS-level least privileged access controls on additional endpoints—Windows servers, Windows desktops, Macs.

Go wider by extending identity security controls to other IT infrastructure such as switches, routers and storage arrays. Implement privileged access controls for business applications and web apps with the greatest risk potential such as CRM and ERP solutions.

Stage Five – Advanced Security

In stage five, shore up any remaining vulnerabilities. Implement Identity Security controls for all remaining business applications and web apps. Apply adaptive multi-factor authentication to the pending web applications, extend session isolation and threat analytics to legacy mainframe systems and applications. Secure any remaining *NIX or Windows server privileged accounts.

Introduce advanced security practices. Automatically rotate credentials used in embedded OS services such as Windows Services, Scheduled Tasks or COM Objects. Ensure applications are strongly authenticated using multiple attributes when requesting secrets. Apply least privilege controls to all *NIX servers.

Conclusion

Malicious insiders and external attackers can exploit identities to steal confidential data or disrupt critical applications. The CyberArk Blueprint helps organizations formulate and maintain an effective risk-based Identity Security program that takes full advantage of CyberArk's vast knowledge and expertise. Designed to defend against the three most common attack scenarios, the CyberArk Blueprint provides a prioritized framework that closely aligns prescriptive actions with risk reduction, helping organizations address the vulnerabilities that pose the greatest potential threat, as quickly as possible.

By following the recommendations and guidelines laid out in the CyberArk Blueprint organizations can strengthen their security posture, reduce risks and make the most of their Identity Security technology investments.

Next Steps

Developing and executing an effective Identity Security program can be a complex undertaking. CyberArk has the experience, solutions and security services to help you succeed. To begin your Blueprint journey, visit www.cyberark.com/blueprint and sign up for a Blueprint session to learn about how Blueprint can help you achieve Identity Security success!

Once you have completed a Blueprint session and have a roadmap, CyberArk and our partners offer a wide range of professional services and customer success services to help you with every facet of your Identity Security program. For more information on the CyberArk Security Services Identity Security Program Development Package visit www.cyberark.com/blueprint. The package includes a focused approach based on the CyberArk Blueprint and helps you set and meet goals to achieve the highest level of protection against the most common attacks missing identities and their related accounts, credentials and secrets.

About CyberArk

CyberArk (NASDAQ: CYBR) is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security solutions for any identity – human or machine – across business applications, distributed workforces, hybrid cloud workloads, and throughout DevOps pipelines. The world's leading organizations trust CyberArk to help secure their most critical assets. To learn more about CyberArk, visit www.cyberark.com.

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., 02.20 Doc. 47303

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.

CYBERARK®