CYBERARK

SOLUTION BRIEF

ADDRESSING GAPS IN GDPR COMPLIANCE WITH CYBERARK PRIVILEGED ACCOUNT SECURITY

Applying CyberArk Privileged Account Security can do more than protect penalties and liability. CyberArk solutions can help you enable your organization to securely leverage personal data so you can advance in an increasingly dynamic, competitive business environment.

For more information, please contact your CyberAark representative and check out our resources online.

Operational control over who has access to personal data is at the heart of complying with the General Data Protection Regulation (GDPR). Essential to gaining that operational control is having a strong Privileged Account Security (PAS) solution. In completing ***Get Your Enterprise Ready for GDPR*** you identified specific areas in your organization's PAS that you need to improve.

The matrix below maps specific CyberArk solutions to areas of personal data protection that may need improvement. You can use this matrix to help those within your organization who are responsible for GDPR compliance. Additional detail, including a GDPR Solution Brief and the official text of the regulation itself, can be found at www.cyberark.com/GDPR.

Can you implement these solutions before GDPR is enforced May 25, 2018? Absolutely. But you need to start taking action now.

Protecting access to personal data	
GDPR Article 25: Data protection by design and by default **GDPR Article 32 (2):** Accidental or unlawful destruction, loss, alteration or access to personal data	**How CyberArk can help**
Manage accounts by the "least privilege principle," e.g., Use admin accounts for administrative tasks only; delegate only those permissions needed for a user to do his/her job.	Endpoint Privilege Manager enforces least privilege policies on Windows endpoints and servers, enabling granular segregation of duties for IT administrators. Application Identity Manager™ eliminates hard-coded credentials, including passwords and encryption keys from applications, service accounts and scripts with no impact on application performance Core Privileged Account Security • Allows organizations to control and monitor the commands super-users can run based on their role and task at hand to help support the enforcement of least privilege • Fully protect privileged passwords based on privileged account security policies and control who can access which passwords when • Securely store, rotate and control access to SSH keys to prevent unauthorized access to privileged accounts • Isolate, control, and monitor privileged user access as well as activities for critical Unix, Linux, and Windows-based systems, databases, and virtual machines
Remove plain-text application credentials, such as embedded passwords and locally stored SSH keys.	
Segregate accounts used to manage domain controllers, servers and workstations.	
Automatically select and rotate unique passwords for all admin accounts.	
Use a password vault which automatically enforces strong password policies.	
Enforce multi-factor authentication for users to access credentials in the vault.	
Force all privileged sessions through a secure jump server.	
Isolate administrative access to personal data from Internet-connected workstations.	
Restrict application accounts to "least privilege", e.g. not allow applications to have domain administrator privileges.	

Responding rapidly to a breach

GDPR Article 33: Notification of a personal data breach to the supervisory authority	**How CyberArk can help**
Detect the misuse of credentials leading to a breach of personal data early in the attack lifecycle.	Core Privileged Account Security • Isolate, control, and monitor privileged user access as well as activities for critical Unix, Linux, and Windows-based systems, databases, and virtual machines • Analyze and alert on previously undetectable malicious privileged user behavior enables incident response teams to disrupt and quickly respond to an attack.
Perform live monitoring and recording of user activity during privileged sessions.	
Detect credential theft—for example, by monitoring administrative activities associated with a password vault.	
Isolate privileged sessions, especially those originating from outside the network and from unmanaged devices, e.g. third parties.	
Account for who accessed what personal data on which systems when, including third party accounts who process personal data for you.	
Identify all locations of malware that may have been used to facilitate the breach.	

Assessing risk to your personal data

GDPR Article 35: Data protection impact assessment	**How CyberArk can help**
Exercise regular discovery processes to identify privileged accounts and credentials, including passwords and SSH keys.	Discovery & Audit™ (DNA) scans your network to discover all your privileged accounts, including third party accounts with access to personal data. CyberArk Red Team specializes in adversary simulation and uses a variety of tactics, techniques and procedures that are used in real world attacks to help clients safely uncover vulnerabilities, test security procedures and identify areas for improvement. Core Privileged Account Security Solution analyzes and alerts on previously undetectable malicious privileged user behavior enabling incident response teams to disrupt and quickly respond to an attack. The CyberArk Shared Technology Platform supports protecting access to personal data by design and default. Extend Privileged Account Security to new systems as business needs expand.
Map trust relationships between accounts and systems that have access to personal data.	
Limit the proliferation of administrative accounts by minimizing the use of personal privileged accounts.	
Conduct “ethical hacking” attacks to determine areas of privileged access vulnerability.	
Look for signs of suspicious lateral movement or privilege escalation in real time.	
Leverage behavioral analytics to detect suspicious user and account activity that could indicate a compromised privileged account?	
Evaluate the processes for securely adding new users and assets to the system and de- provisioning obsolete ones.	

Demonstrate GDPR compliance

GDPR Article 82: Right to compensation and liability	How CyberArk can help
Provide audit logs of who and what (e.g. applications) accessed personal data, including third party access to personal data.	Core Privileged Account Security • Securely audit and log all privileged access to systems and applications containing personal data to defend against claims. • Global analytic reporting capabilities help demonstrate adequate security controls to GDPR supervisory authorities • Isolate, control, and monitor privileged user access as well as activities for critical Unix, Linux, and Windows-based systems, databases, and virtual machines
Enforce access controls to ensure that only the right users are able to access – or request access to – authorized credentials.	
Monitor access to privileged accounts and require users to "check-out" shared account credentials to establish individual accountability.	
Quickly and easily generate reports that verify you have these privileged account controls in place.	
Automatically and regularly scan the network to identify accounts needing better protection, and show the reduction in vulnerable accounts.	
Provide tamper-proof audit logs and session recordings to demonstrate audit integrity.	
Assess environmental risks and distinguish between normal and abnormal behavior.	
Define high-risk activity and alert the necessary incident response teams.	
Conduct impact assessments to measure the effectiveness of security controls you have in place.	