SOLUTION BRIEF
CyberArk Privileged Access Security Solution with SafeNet Luna HSM and HSM On Demand for CyberArk

Securing and Managing Privileged Account Credentials

Protecting privileged access management credentials presents one of the largest security risks an organization faces today. These access accounts allow control of an organization’s resources, disable security systems, and enable access to vast amounts of sensitive data. Forrester estimates that 80 percent of security breaches involve privileged credentials. These breaches can come from external attackers and malicious insiders seeking a way to gain direct access to the heart of the enterprise. The fast adoption of “everything to the cloud” has increased the IT footprint, creating an increasingly porous enterprise perimeter. Protecting this widely dispersed corporate and customer data, along with their associated user credentials, is paramount to a corporation’s reputation, and their success.

The Challenge
At the same time the adoption of the cloud increases business opportunities, it also drives the growth of a wide range of users that require these powerful Privilege Access Credentials, including:

- Senior-level executives and IT personnel to access sensitive data
- Hypervisor or cloud server managers to administer cloud applications
- Systems, Applications or Database administrators to access operating systems, servers, and databases
- DevOps or SecOps teams building IT applications for the enterprise
- Third-party providers to enable contractors to perform a job function
- End users are given short-term local admin access allowing them to install software or printers

As the threat landscape increases, compliance regulations and internal policy requirements to control, manage and monitor these privileged access accounts have also increased. These compliance regulations, like GDPR, offer significant guidance in attempting to limit the impact of breaches. While these regulations provide guidance on securing data, they also require an organization to provide improved audit and control over their IT security systems, representing an increasing challenge to organizations.

Businesses must develop methods to secure these access privileges while not impacting day-to-day operations. Processes must be implemented that identifies security weaknesses, automates key storage, retrieval and rotation, and simplifies compliance with policies and regulations.

The Solution
Privileged Account credentials are the “keys to the IT kingdom”. External attackers and malicious insiders know this is the most effective way to gain access to your critical data. Safely generating and storing the keys used for these access credentials is a critical part of the security solution.

Gemalto offers two solutions that can generate and store the server keys, providing private key protection and strong entropy for key generation for CyberArk Privileged Access Security Solution system.

- SafeNet Data Protection On Demand is a cloud based hardware security module (HSMoD) as a service that offers a CyberArk specific key management capability (HSM On Demand for CyberArk) that can be deployed within minutes with no need for specialized hardware or associated skills
- SafeNet Luna HSMs store, protect and manage sensitive cryptographic keys on-premises in FIPS 140-2 Level 3, tamper-resistant hardware appliances, providing high-assurance key protection within an organization’s own IT infrastructure

Key Features
- Protecting privileged access management credentials presents one of the largest security risks an organization faces today. These access accounts allow control of an organization’s resources, disable security systems, and enable access to vast amounts of sensitive data. Forrester estimates that 80 percent of security breaches involve privileged credentials. These breaches can come from external attackers and malicious insiders seeking a way to gain direct access to the heart of the enterprise. The fast adoption of “everything to the cloud” has increased the IT footprint, creating an increasingly porous enterprise perimeter. Protecting this widely dispersed corporate and customer data, along with their associated user credentials, is paramount to a corporation’s reputation, and their success.

The Challenge
At the same time the adoption of the cloud increases business opportunities, it also drives the growth of a wide range of users that require these powerful Privilege Access Credentials, including:

- Senior-level executives and IT personnel to access sensitive data
- Hypervisor or cloud server managers to administer cloud applications
- Systems, Applications or Database administrators to access operating systems, servers, and databases
- DevOps or SecOps teams building IT applications for the enterprise
- Third-party providers to enable contractors to perform a job function
- End users are given short-term local admin access allowing them to install software or printers

As the threat landscape increases, compliance regulations and internal policy requirements to control, manage and monitor these privileged access accounts have also increased. These compliance regulations, like GDPR, offer significant guidance in attempting to limit the impact of breaches. While these regulations provide guidance on securing data, they also require an organization to provide improved audit and control over their IT security systems, representing an increasing challenge to organizations.

Businesses must develop methods to secure these access privileges while not impacting day-to-day operations. Processes must be implemented that identifies security weaknesses, automates key storage, retrieval and rotation, and simplifies compliance with policies and regulations.

The Solution
Privileged Account credentials are the “keys to the IT kingdom”. External attackers and malicious insiders know this is the most effective way to gain access to your critical data. Safely generating and storing the keys used for these access credentials is a critical part of the security solution.

Gemalto offers two solutions that can generate and store the server keys, providing private key protection and strong entropy for key generation for CyberArk Privileged Access Security Solution system.

- SafeNet Data Protection On Demand is a cloud based hardware security module (HSMoD) as a service that offers a CyberArk specific key management capability (HSM On Demand for CyberArk) that can be deployed within minutes with no need for specialized hardware or associated skills
- SafeNet Luna HSMs store, protect and manage sensitive cryptographic keys on-premises in FIPS 140-2 Level 3, tamper-resistant hardware appliances, providing high-assurance key protection within an organization’s own IT infrastructure

Key Features
- Protecting privileged access management credentials presents one of the largest security risks an organization faces today. These access accounts allow control of an organization’s resources, disable security systems, and enable access to vast amounts of sensitive data. Forrester estimates that 80 percent of security breaches involve privileged credentials. These breaches can come from external attackers and malicious insiders seeking a way to gain direct access to the heart of the enterprise. The fast adoption of “everything to the cloud” has increased the IT footprint, creating an increasingly porous enterprise perimeter. Protecting this widely dispersed corporate and customer data, along with their associated user credentials, is paramount to a corporation’s reputation, and their success.

The Challenge
At the same time the adoption of the cloud increases business opportunities, it also drives the growth of a wide range of users that require these powerful Privilege Access Credentials, including:

- Senior-level executives and IT personnel to access sensitive data
- Hypervisor or cloud server managers to administer cloud applications
- Systems, Applications or Database administrators to access operating systems, servers, and databases
- DevOps or SecOps teams building IT applications for the enterprise
- Third-party providers to enable contractors to perform a job function
- End users are given short-term local admin access allowing them to install software or printers

As the threat landscape increases, compliance regulations and internal policy requirements to control, manage and monitor these privileged access accounts have also increased. These compliance regulations, like GDPR, offer significant guidance in attempting to limit the impact of breaches. While these regulations provide guidance on securing data, they also require an organization to provide improved audit and control over their IT security systems, representing an increasing challenge to organizations.

Businesses must develop methods to secure these access privileges while not impacting day-to-day operations. Processes must be implemented that identifies security weaknesses, automates key storage, retrieval and rotation, and simplifies compliance with policies and regulations.
CyberArk Privileged Access Security Solution with SafeNet Luna HSM and HSM On Demand for CyberArk - Solution Brief

Solution Benefits

- Enhanced key protection significantly enhance security and reduce risk
- Automated password system, with role-based credential management system
- Reporting and audit features for easier adherence to compliance regulations
- Cloud-based, hybrid and on-premises support is flexible and scalable for a global solution

About Gemalto SafeNet Identity and Data Protection Solutions

Gemalto’s portfolio of Identity and Data Protection solutions offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions – from the edge to the core. Gemalto’s SafeNet Identity and Data Protection solutions enable enterprises across many verticles, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters.

Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation to protect customer trust in an increasingly digital world.

About CyberArk

CyberArk is 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. CyberArk delivers the industry’s most complete solution to reduce risk created by privileged credentials and secrets. The company is trusted by the world’s leading organizations, including more than 50 percent of the Fortune 100, to protect against external attackers and malicious insiders. A global company, CyberArk is headquartered in Petach Tikva, Israel, with U.S. headquarters located in Newton, Mass. The company also has offices throughout the Americas, EMEA, Asia Pacific and Japan.

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com/contact-us
Follow Us: blog.gemalto.com/security

©Gemalto 2019. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries. SB (EN)-Feb.05.2019 - Design: ELC

1 The Forrester Wave™: Privileged Identity Management, Q3 2016 by Andras Cser, July 8, 2016