Privileged access represents the single largest threat to any organisation

Now you can easily protect, monitor and control privileged access across on-premises, cloud, and hybrid infrastructure.

Privileged accounts are used to maintain systems, facilitate automated processes, safeguard sensitive information, and ensure business continuity. But in the wrong hands they can be used to steal sensitive data and damage your business.

In fact, Forrester estimates that at least 80% of data breaches have a connection to compromised privileged credentials[1].

Why are privileged accounts so attractive?

Privileged access is everywhere, in every networked device, database and application, as well as your servers, Industrial Control System environments, and even through the DevOps pipeline.

Used by both human and machine identities with all-powerful access to confidential data and systems, privileged accounts:

- have shared administrative access making their users anonymous
- grant broad access rights, far beyond what is needed for the user to perform their job function
- go unmonitored and unreported and therefore unsecured

A better way: Privileged Access Management

Our Privileged Access Management service, provided in association with CyberArk, is a complete solution for protecting, controlling, and monitoring privileged access across on-premises, cloud, and hybrid infrastructure. Designed from the ground up for security, Privileged Access Management will help you:

- efficiently manage privileged account credentials and access rights
- proactively monitor and control privileged account activity
- intelligently identify suspicious activity
- quickly respond to threats.

Challenges with privileged access

Managing account credentials.
Many organisations rely on manually intensive, error-prone administrative processes to rotate and update privileged credentials – an inefficient, risky and costly approach.

Tracking privileged activity.
Many enterprises cannot centrally monitor and control privileged sessions, exposing the business to security threats and compliance violations.

Monitoring and analysing threats.
Many organisations lack comprehensive threat analysis tools and are unable to proactively identify suspicious activities and remediate security incidents.

Controlling user access to cloud resources.
Organisations often struggle to effectively control privileged user access to cloud platforms (IaaS / PaaS), SaaS applications, social media and more, creating compliance risks and operational complexity.

Protecting Windows domain controllers.
Attackers can exploit vulnerabilities to impersonate authorised users and gain access to critical IT resources and confidential data.

All identities can become privileged under certain conditions, based on the systems, environments, applications or data they are accessing, or the types of operations they are performing.

1. The Forrester Wave: Privileged Identity Management, Q4 2018

A comprehensive privileged identity management service

Credential discovery and management

Discover
Continually scan the IT estate to detect privileged credentials and accounts

Onboard
Automatically add discovered privileged accounts to the CyberArk Digital Vault

Manage
Automatically rotate credentials and govern access according to policy

Privileged session management

Isolate
Isolate credentials from end users and workstations

Record and audit
Support forensic analysis and audit with detailed logs of privileged activity

Monitor
Monitor, track and detect suspicious privileged activity in real time

Key features

- **Centrally secure and control access** to privileged credentials based on administratively defined security policies. Automated privileged credential rotation for both human and non-human users eliminates manually intensive, time consuming and error-prone administrative tasks, safeguarding credentials.
- **Isolate and monitor privileged sessions.** Establish secure, isolated remote sessions and record all activity. Credentials are retrieved by the solution and sent directly to the target system, so both end users and machines are not exposed to credentials. Meanwhile, session isolation prevents the spread of malware.
- **Loosely connected devices.** Enforce security policies and rotate credentials of accounts on endpoints that are not always connected to the enterprise network.
- **Remote Access to Privilege Cloud.** Enable secure access for remote employees no matter where they are, without the need for VPNs, passwords or agents. Enable offline access in air-gapped and offline environments.
- **Secure credentials for applications** and non-human users. You can remove and manage hard-coded credentials used in homegrown applications. The solution also integrates with other leading security vendors to remove hard-coded credentials from apps when they require privileged access.

Why work with us?

A fully managed service – identity management can be complex; we provide you with a fully managed privileged access management as a service underpinned with CyberArk's Privilege Cloud solution.

A skilled team – we have accredited CyberArk experts with many years' experience of deploying and managing privileged identity solutions.

24x7x365 coverage – our SOCs provide you with 24x7 support, every day of the year.

Economies of scale – managing privileges is a full time job – our scale saves you the cost of employing your own resources.

What could Privileged Access Management do for you?

Visit bt.com/security

November 2022