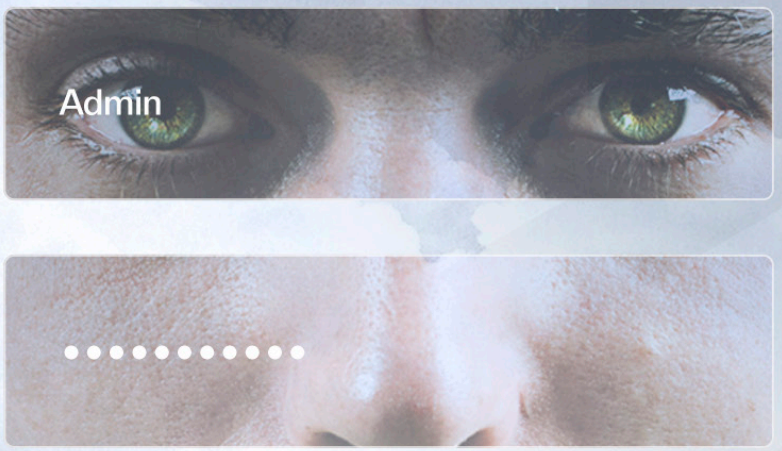
CYBERARK



5 top reasons
to prioritize privileged account security today

Privileged accounts represent the gateway to an organization's most valuable assets. That's why cyber attackers covet them. It's also why nearly all serious security breaches involve privileged accounts that attackers acquire, compromise and exploit.

CYBERARK

Today's reality is that the IT infrastructure is not fully protected unless privileged accounts and their credentials are secured. Privileged accounts should be secured regardless of where they reside—whether they are accessed by humans or applications:

· Across the IT landscape in endpoints, servers and domain controllers
· On premises or in the cloud

Simply put, protection from advanced threats requires a complete layer of privileged account security. But establishing cyber security priorities is difficult for security practitioners because of competing ideas from internal teams and conflicting messages from vendors.

There is confusion around what to do to get the most effective protection against cyber attacks.

Privileged account security is the logical choice when it comes to what should come first. It's time businesses prioritize privilege. Here are five reasons why:

1.

Privilege is the road most traveled.

Privilege is the one constant in the cyber attack lifecycle. In fact, 100% of advanced cyber attacks involve the escalation of privilege.[1] It is the common denominator in nearly every serious attack, and the reason is clear: Attackers need the credentials of an insider to move around and achieve their goals. Without credentials, an attacker's ability to move across the network is blocked.

Credentials—and, in particular, privileged credentials—give attackers the permissions necessary to access servers and steal data or go after the domain controllers and take control of the IT environment. If you block privilege escalation, you block the attack.

CYBERARK

2.

Privileged accounts represent the express lane to your domain controllers.

If an attacker reaches the domain controllers, they own every piece of the infrastructure. They can create their own credentials and therefore, go anywhere they want. This means they can access any server, any controller and any endpoint—any asset or data on your network. They will own the environment.

Cyber attacks can move rapidly from the point of infection, when an end user clicks on a link from a phishing attack and downloads malware. As quickly as 12 minutes later, the domain controller can essentially belong to the attackers.[2] With privileged credentials, attackers can get there that quickly.

Effective privileged account security is an important tool to protect domain controllers. Once you lose control of your domain controllers, you've essentially lost control of your business. Game over.[2]

3.

Your security systems need to be secure.

Organizations need layers of security, including proactive controls such as encryption and detection systems to identify malicious behavior. Privileged account security is not a silver bullet, but security systems are largely ineffective without privileged account security in place.

Privileged accounts are embedded within every piece of security, database and network technology for them to be installed and managed. If you deploy a million dollars' worth of next-gen firewalls and don't secure their privileged accounts, it's easy for the attacker to get those credentials and go right through your firewall. That will make your million-dollar investment nearly worthless.

The point can't be mistaken: Protect your security systems. To maintain the credibility and efficacy of your security solutions, put privileged account security in place before you deploy any other security controls or detection solutions.

All security systems are ineffective without privileged account security in place.

CYBERARK

4.

A single solution to protect against insider threats and external attackers.

A single solution that will protect against insider threats as well as external attackers should be at the top of every list of security needs. Privileged account security protects against both—whether it's a malicious insider who already has access to the credentials, insiders who make an error or do something they shouldn't because of inappropriate access rights or external attackers who break in and steal those credentials. In any case, privileged credentials should be locked down.

Privileged account security combines proactive controls with real-time detection on privileged activity. It's important to know immediately when rogue insiders are misusing their privileged access to sensitive information.

5.

Securing privileged accounts is the first action following a breach.

If the infection is serious, or if the domain controller has fallen, organizations may choose not to trust the rest of the infrastructure—so they will have to rebuild with new hardware and new systems. Then they need to add in a layer of privileged account security—before loading applications and before connecting to any other network device.

Organizations should want privileged account security in place—from Day 1, Minute 1—in order to maintain control of privileged access on any particular machine or asset. If they lose control of privileged access, they've essentially lost control of their IT systems and structure.

Wouldn't you rather address privileged account security now, as opposed to doing it in the heat of battle when you're trying to recover from a breach and your business has been crippled? Be proactive when there is time to plan. If it's the first thing you're going to do after an attack, it really should be done today.

The CyberArk Privileged Account Security Solution reduces an enterprise's cyber security risk profile by protecting against advanced threats that exploit privileged credentials. Customers can achieve rapid ROI—complete payback within six months or less—as the CyberArk platform is used over time.[3]

CYBERARK

Being proactive is the ultimate protection. It's time to put privilege first.

About CyberArk

CyberArk is dedicated to protecting enterprises against the most advanced cyber threats: those that use insider privileges to attack the heart of the enterprise and bring business to a halt.

Are you protecting your business by prioritizing privileged account security?

Take the free risk assessment with CyberArk Discovery & Audit™

[1]"Privileged accounts are on their critical path to success 100% of the time in every attack, regardless of the threat."—The role of privileged accounts in high profile breaches, CyberSheath Services International, 2014

[2]CyberArk press release: http://www.cyberark.com/press/gone-12-minutes-cyberark-announces-real-time-detection-automatic-containment-cyber-attacks-targeting-active-directory/

[3]Nucleus Research Guidebook: CyberArk Privileged Account Security Solution