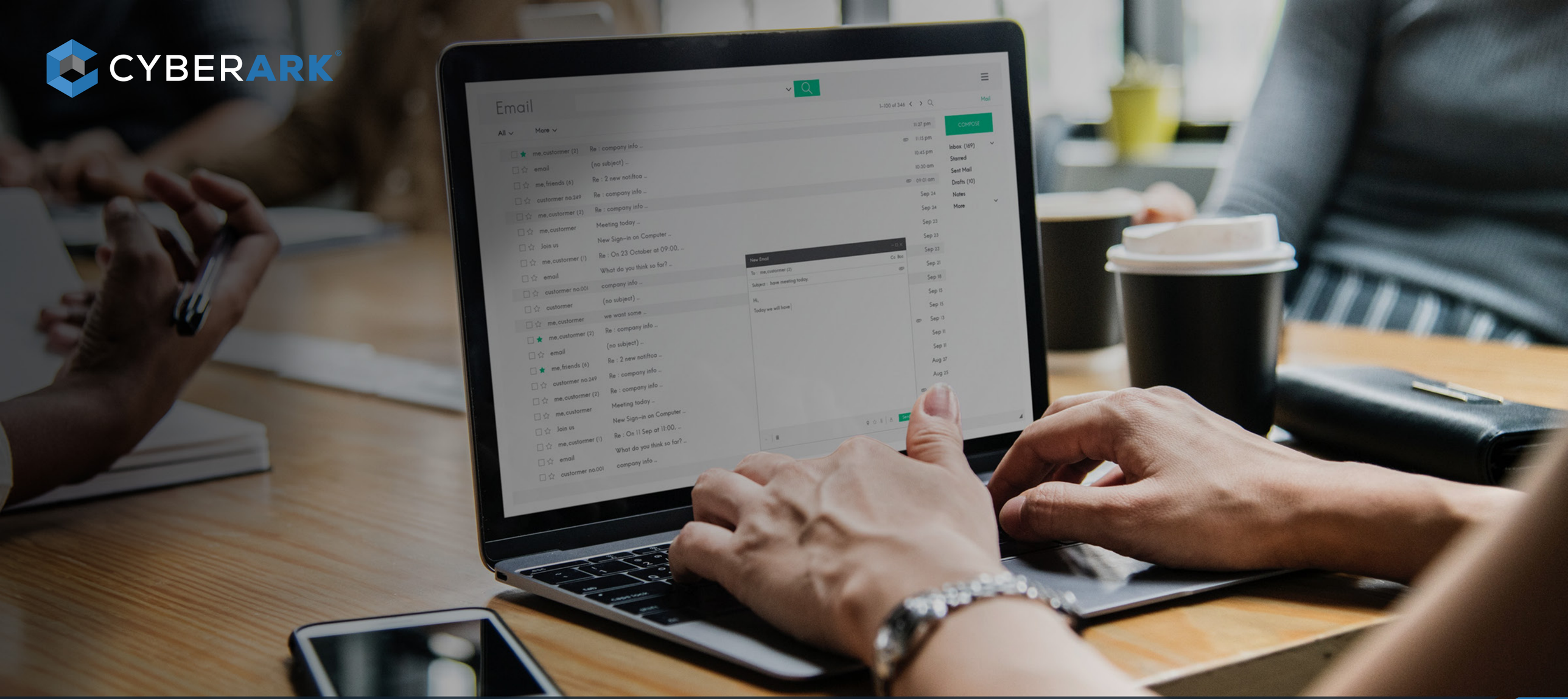
CYBERARK



TOP 5 REASONS TO PUT PRIVILEGE FIRST

INTRODUCTION

Privileged access is the gateway to an organization's most valuable assets and is at the core of nearly every major security breach. Organizations must have a strategy in place to manage and monitor privileged access, as well as detect and respond to threats if they'd like to mitigate risk from today's advanced attacks.

Your application stack and infrastructure is likely quite complex and it can be hard to identify which assets are the most sensitive. And there is a never-ending supply of vendors knocking down your door competing for your time and attention. These two realities make it increasingly difficult to identify which security project to tackle next. When thinking about how to prioritize, it is advantageous to take a step back and think about your businesses goals, albeit in a slightly different way: try to envision what you would be looking for if you were an external attacker or malicious insider looking to steal sensitive data, commit Ransomware, or use your infrastructure for illicit cryptomining.

Forrester estimates that 80% of security breaches involve privileged credentials.[1] Privilege is THE common denominator in virtually every serious attack, and the reason is clear: Attackers need privileged accounts, credentials and secrets to gain the permissions or tools allowing them to pose as an insider and gain access to privileged information or assets. Privileged access is needed in order to access network infrastructure and steal data. However, without privileged access, an attacker is severely limited.

The harsh reality is that no organization can ever fully secure all of their applications and infrastrucuture, whether their data center is on-premises, in the cloud, or hybrid. Protection from all of the various methods that attackers may use is impossible; they will get in, it's what they do. There is no single solution available in the market today that will prevent every advanced cyber-attack. But prioritizing what matters most first – privileged access – needs to be at the core of every enterprise organization's strategy. Here's why:

Contents

[1] **The Forrester Wave™:** Privileged Identity Management, Q4 2018

1. PRIVILEGE IS THE ROUTE TO YOUR MOST CRITICAL ASSETS

"Privileged access security is the preeminent tool to protect your Tier0 assets."

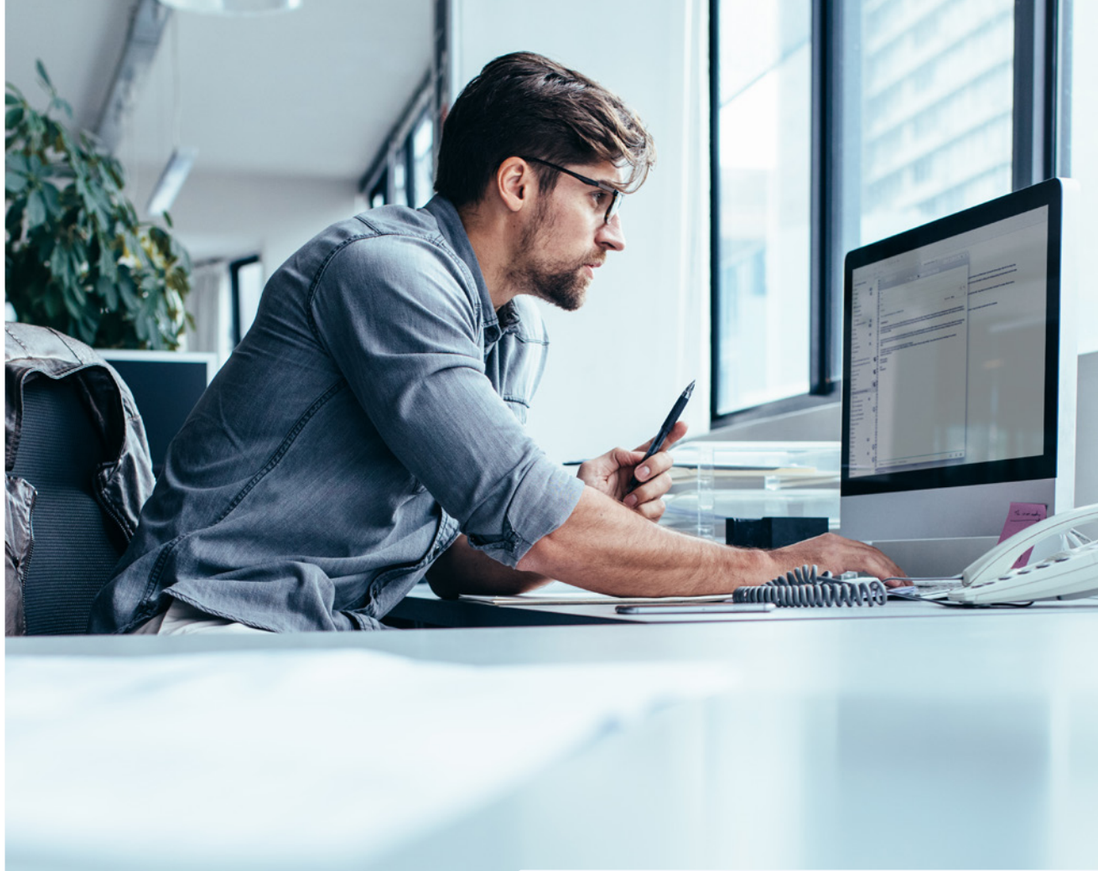
It's well known that if an attacker reaches your domain controllers, they essentially have complete access your entire organization and can bring down your network without any restrictions. What's lesser known, but becoming increasingly popular, is that newer systems like cloud consoles or orchestration tools (i.e. k8s, Docker Swarm) are also becoming primary targets for attackers as they seek out how to own every piece of your infrastructure, so that they can perform reconnaissance undetected. Once someone (or something) obtains this level of access, be it domain controllers or cloud consoles, they can access any server, controller, endpoint or piece of data, anywhere in your network. Not only this, but they can run any commands, or download/install anything they want. They essentially have complete control over your entire domain.

Privileged access security is the preeminent tool to protect your Tier0 assets. Especially as companies adopt the DevOps methodology and mindset, additional tools are then introduced to support the agility that comes along with that digital transformation. Every one of these tools requires a human to perform some level of privileged administrative tasks and should be protected as you would with other Tier0 and revenue generating assets. Care should be taken to not introduce constraints, slow-downs, or radical shifts to the native user experience when extending security to these platforms. Without the appropriate controls and privilege in place, domain controllers will be left vulnerable; and as mentioned, there's no bigger single threat to an organization's wellbeing than attacks on domain controllers.

2. HUMANS ARE, WELL, HUMAN

It is human nature to take the path of least resistance, and as such, humans are often times the weak link in the attack vector. Shortcuts are dangerous for a variety of reasons. When steps are skipped and processes circumvented, big mistakes often follow. Moreover, insiders can create shortcuts to connect to systems in their regular routines, which creates unmonitored pathways for insiders or outsiders to gain access where they shouldn't. Hackers too, are human, and are looking for the easiest way in – they can follow a trail of bread crumbs until the reach something that they can exploit in a variety of ways.

While external attackers will either seek out users with privilege so they can masquerade as a privileged insider or gain access directly to sensitive information, and internal users either knowingly or unknowingly access information they shouldn't, it's clear that to protect people from themselves, having a privileged access program in place is paramount. Privilege is the control to make sure that the right people have only the necessary levels of access to sensitive applications and infrastructure to do their jobs, and nothing more. Privileged controls also provide the ability to ensure that the activities occurring within an environment aren't malicious, or if they are, they're quickly addressed by the necessary security operations teams to take action.



Humans always are looking for the easy way out (or in)

3. PRIVILEGE DOESN'T STOP WITH PEOPLE

The number of machines and applications that require privileged access to run routine and important tasks vastly outnumber the number of people. A general rule of thumb is that for every person at an organization, there are 3-5x that number of privileged accounts; and the landscape of non-human privileged users is even larger. These non-human entities are often times harder to monitor, keep track of, or even identify.

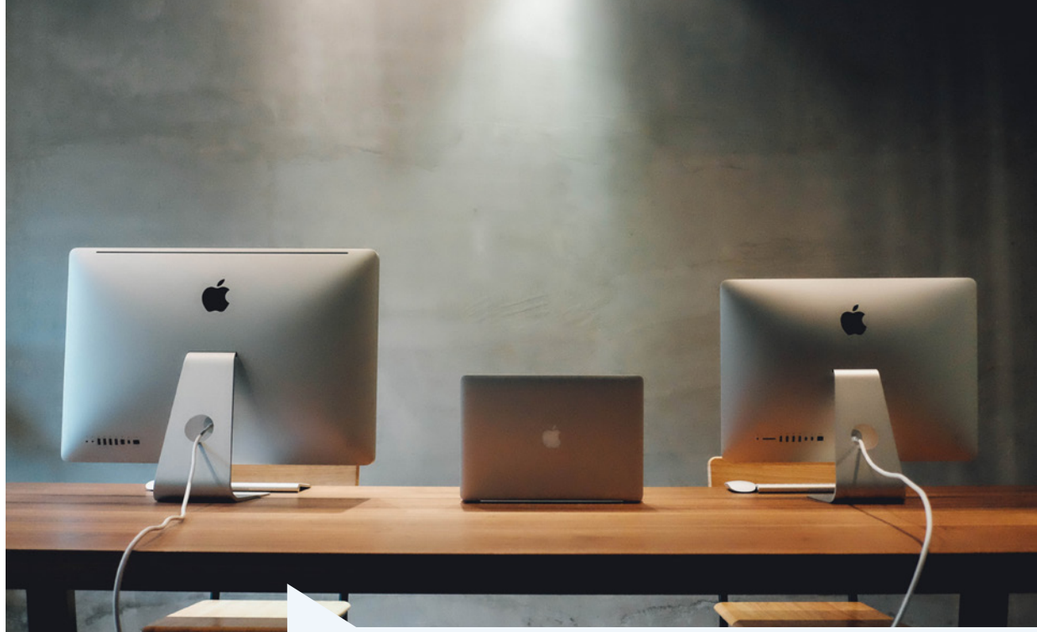
"Traditional" commercial applications that are deployed currently like CMDB, Enterprise ticketing, vulnerability scanners, etc., all require access to varying parts of the network in order to complete their tasks. However, because they require access throughout the domain, these applications (and many more) essentially have sweeping access throughout your environment, and need to be secured. Attackers are also targeting high visibility / high value targets like orchestration platforms (e.g. Puppet and Ansible) and automation servers (e.g. Jenkins) in addition to more traditional, legacy Tier0 applications. Additionally, with the advent of Robotic Process Automation (RPA), software bots are taking the place of human operators for repeatable tasks with or without DevOps adoption, hardcoded credentials and secrets have never been more prevalent.

Sorting out your privilege strategy will allow your organization to monitor where the various layers of privilege live, and detect when anomalous activities are occurring.

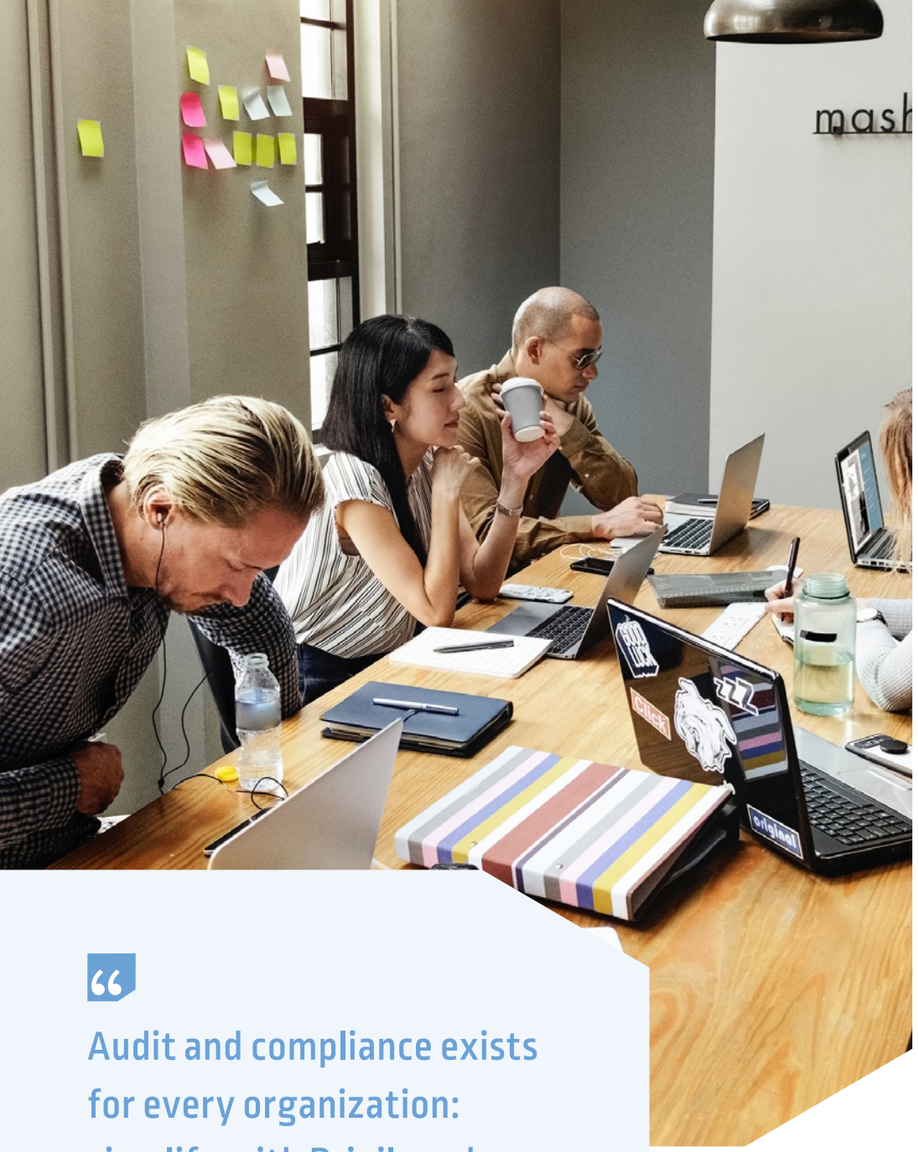
4. PRIVILEGE EXISTS ON ALL OF YOUR EMPLOYEES' WORKSTATIONS

When organizations first think about how to secure their environments, it's common to think about things like servers, databases, switches, routers and firewalls. However it's important to remember that every single workstation contains privilege by default. Every. Single. One. All workstations have built-in administrator accounts that can be used by internal IT users to fix issues occurring locally. However, this creates a massive security gap, as these admin accounts are located via shared accounts that can be difficult to monitor, and also provides unnecessary access. In that same vein, often time's users are granted default local administrator access, which dramatically widens the attack surface, but has little operational benefit.

When granted unneeded access, end users are given free rein to do things like install applications and software that are potentially dangerous. Hackers can exploit these risky systems by getting in and then jumping laterally from workstation to workstation until they reach what they are looking for. Putting forth a plan to secure your environment has to include a step to prioritize privilege and remove local administrative rights on workstations. Without this step, it becomes much easier to move laterally within your network, and much harder to pinpoint each user's behavior and activities.



It's important to remember that every single workstation contains privilege by default.



> “Audit and compliance exists for every organization: simplify with Privileged Access Security.”

5. PASSING AUDITS AND MEETING COMPLIANCE REVOLVES AROUND PRIVILEGE

Audits are a fact of life for every organization in some fashion. Additionally, with more and more legislation and regulations being passed on how organizations secure their and their customers’ data, it’s crucial to identify security tools and programs that will help stay up to date. Auditors often times require extensive logs, records, and proof that organizations are securing their most sensitive data, and meeting compliance can be an ongoing struggle for any organization as they face harsh penalties like fines and future restrictions. Organizations need to be totally committed when it comes to securing their privileged data, be it related to customers, personal health information, finances, credit card information, or otherwise.

By putting privilege at the forefront of your organization’s strategy, you can automatically record and log all activities that relate to your critical IT infrastructure and/or sensitive information. Prioritizing privilege grants your organization granular visibility deep into what is occurring with your most critical assets. Moreover, the ability to monitor and detect suspicious events in your environment is very important, but without a clear focus on what presents the most amount of risk to your business, you’ll be unable to prove to auditors and regulators that you’re compliant, and able to respond to dangerous activity.

Privileged access controls have been identified as being mission critical initiatives to help mitigate risk from advanced attacks. In fact, its among top five CIS basic controls.

According to Gartner, privileged account management was identified as the No. 1 security project in 2018 for CISOs.[2] Privileged access security not only reduces risk, but has business-wide benefits, that keep organizations safe, operational and productive.

Although privileged access has been identified as a top security control by multiple experts, some organizations are still hesitant about moving forward since they view undertaking a Privileged Access Security project as being overly complex, and/or a drain on resources. In certain circumstances, like when organizations attempt to do too much too soon, this can certainly be the case. It is always advisable to start slow, and begin any security project with a clear focus and a finite list of objectives: set goals, accomplish goals, rinse and repeat.

It bears repeating that no one part of your security stack will fully protect your organization from the endless types of cyberattacks that are present today. However, by prioritizing privileged access, you can implement strong controls around your most sensitive assets.

CyberArk is the #1 global solution for Privileged Access Security, and is responsible for securing the most critical layers of organizations' infrastructure, data and assets; in on-premises, cloud, and DevOps environments. CyberArk is trusted by the world's leading organizations, including more than 50% of the Fortune 100, to protect against external hackers as well as insider threats.

FIND OUT MORE

Visit cyberark.com to learn more.

[2] Gartner, Smarter with Gartner, Gartner Top 10 Security Projects for 2018, June 6, 2018