TOP 5 REASONS TO PRIORITIZE PRIVILEGED ACCESS MANAGEMENT AS A SERVICE

Privileged access is the gateway to an organization's most valuable assets and is at the core of nearly every major security breach. Privileged Access Management (PAM) as a Service is a good way for organizations to get their PAM programs up and running, faster and easier than ever.

As enterprise, IT and business standards evolve with more focus on digital transformation such as migrating applications to the cloud, adopting Robotic Process Automation, and embracing DevOps methodologies for software development, organizations continue to look for easy to use and quick to deploy solutions that solve critical business needs. This is summarized neatly as organizations move to the cloud for a variety of reasons including security, cost savings and ease of management.

Likewise, in cybersecurity, organizations are starting to turn more and more to Security as a Service to capitalize on the operational ease of use and improve their security postures. In CyberArk's Global Advanced Threat Landscape Report: Where Security Accountability Stops and Starts in the Public Cloud, we found that the **number 1 reason organizations are moving to the cloud is security**.

Ensuring that privileged access to sensitive applications and systems is secured is something that organizations of all shapes and sizes are challenged to achieve. There is no single solution available in the market today that will prevent every advanced cyber-attack. But prioritizing securing controls that deliver the most risk reduction, such as privileged access management, and taking advantage of all the benefits a SaaS solution can provide is increasingly becoming the option of choice for many organizations. Here are the top five reasons:

Table of Contents

1. PRIVILEGED ACCESS PROVIDES THE KEYS TO THE IT KINGDOM

Privileged access is the gateway to an organization's most valuable assets and is at the core of nearly every major security breach today. It is well known that if an attacker reaches your domain controllers in a traditional on-premises environment, they essentially have complete access your entire organization and can bring down your network without any restrictions. What's lesser known is that newer systems like public cloud and SaaS admin consoles are also becoming primary targets for attackers. Once someone (or something) obtains this level of access, they can then move laterally until they can escalate privileges to the application or system they aim to reach to steal sensitive data, install ransomware, or use your infrastructure for illicit purposes such as cryptomining.

Forrester estimates that 80% of security breaches involve compromised privileged credentials.[1] Relying on spreadsheets, manual processes or scattershot solutions to secure privileged credentials just won't cut it. Organizations of all shapes and sizes need to prioritize managing privileged access to maintain and safeguard business critical information.

Forrester estimates that 80% of security breaches involve compromised privileged credentials.[1]

[1] The Forrester Wave™: Privileged Identity Management, Q3 2018

2. PRIVILEGED ACCESS EXISTS FOR ALL HUMANS

Nearly three in four CFOs plan to shift at least 5% of previously on-site employees to permanently remote positions post-COVID 19.[2]

Privileged access doesn’t just lie with IT super users and cloud administrators. Developers that build applications, HR leaders who possess sensitive employee information, sales leaders with revenue goals and more all possess privileges. In addition, every single workstation has a built-in administrator accounts that can be used by device owners to make changes such as installing software and more. Furthermore, as more and more employees work remotely and on-the-go, using “Bring Your Own Devices,” this creates a massive security gap, as the spread of privilege and new devices can be difficult to account for and thus creates easy targets for attackers. This challenge is not likely to go away anytime soon. Nearly three in four CFOs plan to shift at least 5% of previously on-site employees to permanently remote positions post-COVID 19.[2]

Managing privileges for all human users and ensuring that they only have the privileges needed to do their jobs dramatically shrinks the attack surface. Putting forth a plan to secure your environment should include removing local administrator rights from end user workstations and securing any users with privileged access with controls such as multi-factor authentication, credential rotation, and session management. With a strong Privileged Access Management program in place, it becomes much harder for attackers to gain entry via unsecured workstations, jump laterally from system to system, escalate privileges to steal data, encrypt files with Ransomware, and cause general business disruption.

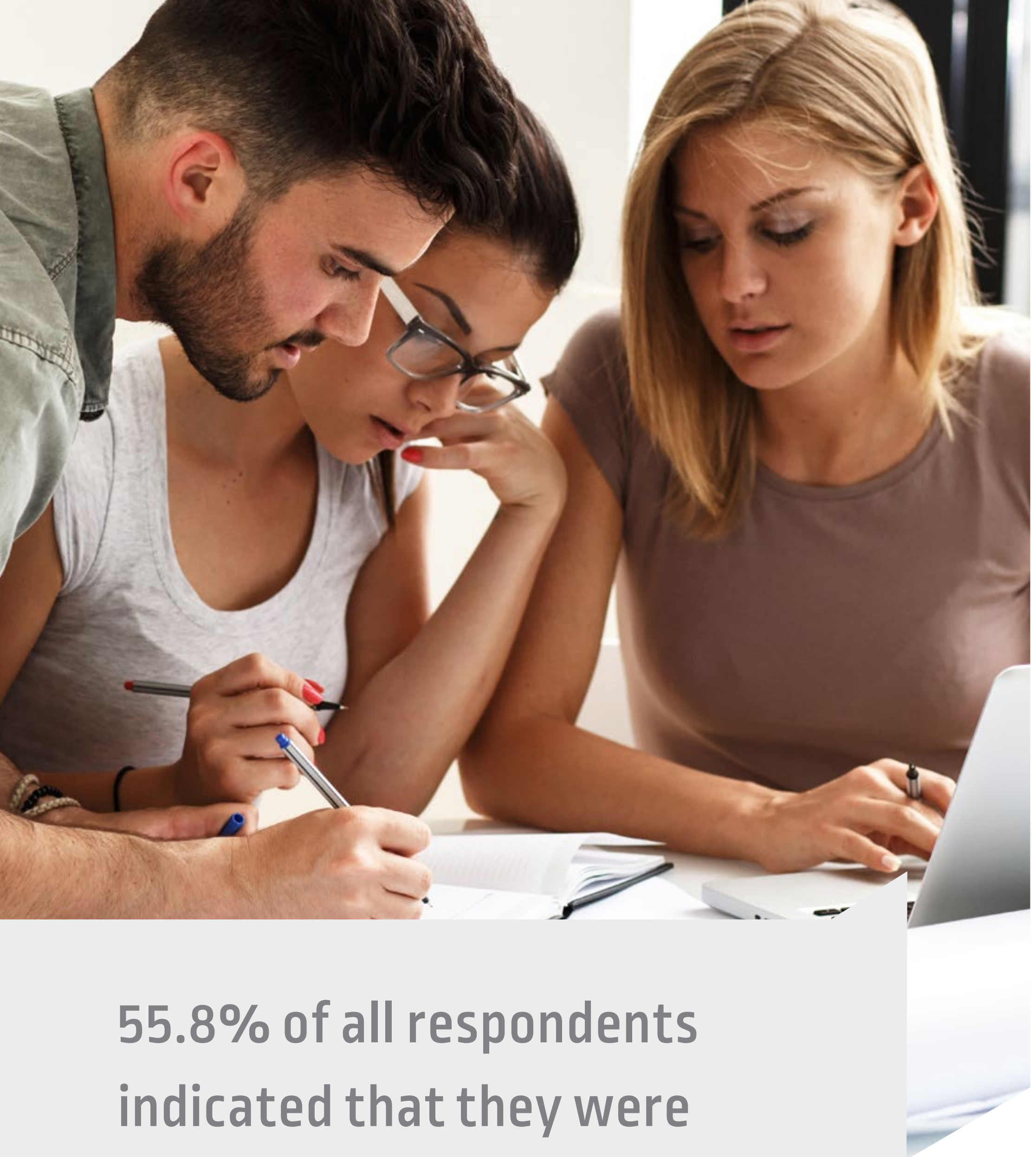
[2] Gartner Press Release, Gartner CFO Survey Reveals 74% Intend to Shift Some Employees to Remote Work Permanently, April 3, 2020

3. PRIVILEGE ACCESS EXISTS ON APPLICATIONS TOO

In a typical organization, whether it is big, medium or small, the machines and applications that require privileged access to run various routine and important tasks vastly outnumber the number of human users that require privileged access. This includes things like service accounts, Commercial Off the Shelf (COTS) applications, security software like vulnerability scanners, SIEM and RPA tools, application servers, CI/CD tool chains and more. With more users, devices and applications than ever before in digital-first organizations, many security teams struggle with maintaining security for applications and manually rotating credentials for applications can be an impossible task.

By adopting PAM as a Service, organizations can ensure that no matter who or what is accessing your most critical systems, they can do so securely. PAM as a Service can be quickly adopted and scaled to remove hardcoded credentials and secrets from applications, integrate with other solutions in the security stack to enable these applications to perform critical business tasks and operations, while remaining secure.

Machines and applications that require privileged access to run various routine and important tasks vastly outnumber the number of human users that require privileged access.



55.8% of all respondents indicated that they were already, using or planning to deploy PAM as a Service.

4. GET PAM CHECKED OFF YOUR TO-DO LIST

Gartner has identified privileged access management as being mission critical initiatives as shown in its Top 10 Cybersecurity Projects for 2019.[3] The most recent CIS Controls report notes privileged access controls as a mission critical initiative. Securing privileged access not only reduces risk, but has business-wide benefits, that keep organizations safe, operational and productive. However, organizations are too frequently tabling their PAM programs due to resource constraints.

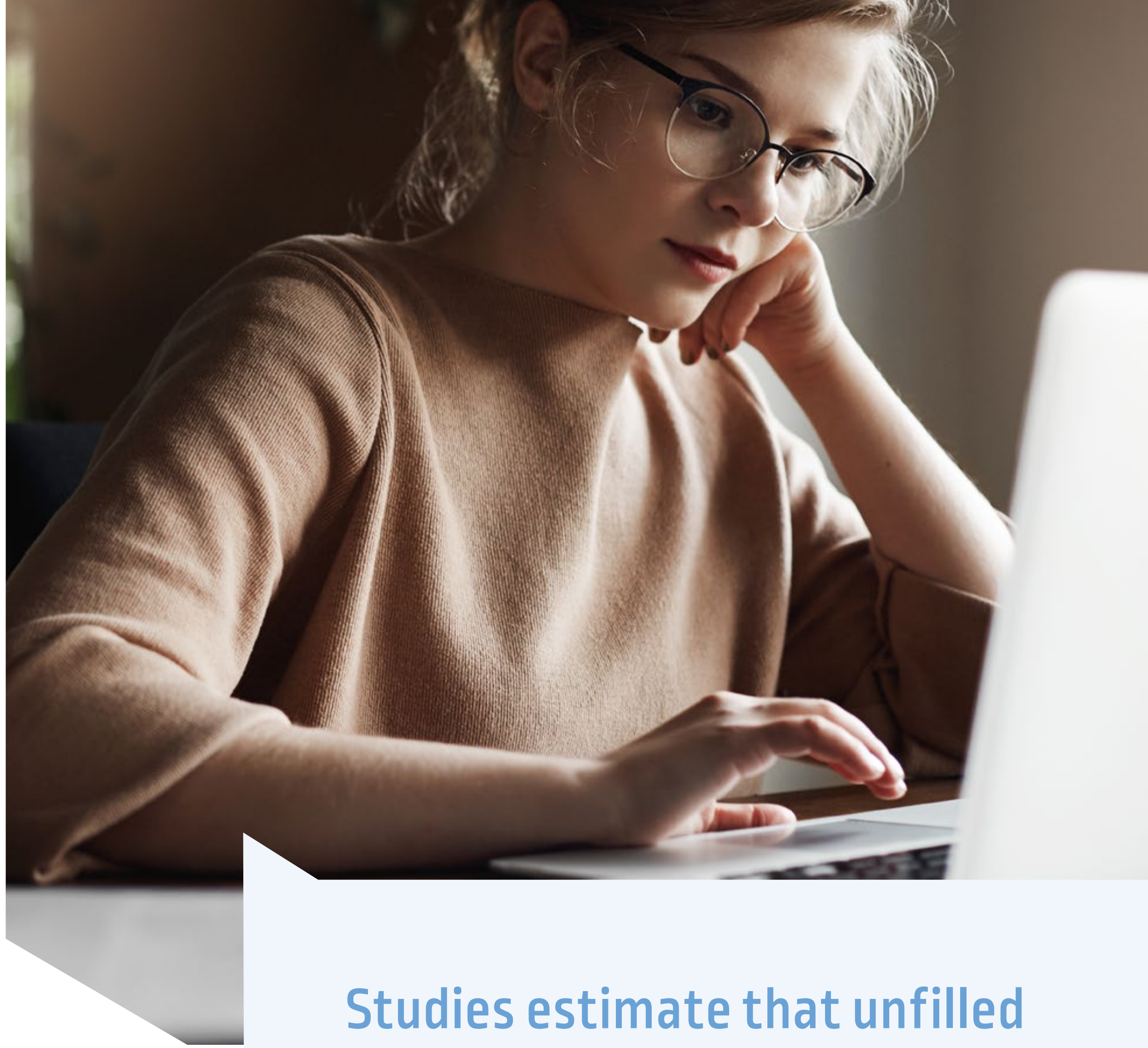
That is likely why PAM as a Service is quickly gaining momentum as the approach of choice for companies embarking on new PAM initiatives. In a 2019 CyberArk survey, 55.8% of all respondents indicated that they were already, using or planning to deploy PAM as a Service. By adopting PAM as a Service, organizations can be in production much quicker than they would otherwise.

[3] Gartner, Top 10 Security Projects for 2019, Brian Reed, Neil MacDonald, Peter Firstbrook, Sam Olyaei, Prattek Bhajanka, 11 February 2019

5. FOCUS ON SECURING PRIVILEGED ACCESS, NOT MANAGING INFRASTRUCTURE

Studies estimate that unfilled cybersecurity jobs will reach 1.8 million by 2022.[4] Having a surplus of trained security professionals at your disposal just simply isn't a reality for the vast majority of organizations. Privileged Access Management is a critical step for protecting assets across a corporate infrastructure, whether hybrid or cloud environments.

Because PAM as a Service is hosted in the cloud, it frees up your staff to focus on the core competencies of your business. Adopting a SaaS model for privileged access reduces the number of subject matter experts, full time employees or 3rd party vendors needed to manage additional infrastructure. Instead, your organization can allocate these resources towards tackling proactive security measures like securing credentials, isolating sessions, and enforcing least privilege.



Studies estimate that unfilled cybersecurity jobs will reach 1.8 million by 2022.[4]

[4] Marten Mickos, "The Cybersecurity Skills Gap Won't Be Solved in a Classroom", Forbes

About CyberArk

CyberArk (NASDAQ: CYBR) is the #1 leader in SaaS deployments for privileged access management, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. The company is trusted by the world's leading organizations, including more than 50 percent of the Fortune 500, 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. To learn more about CyberArk, visit www.cyberark.com, read the CyberArk blogs or follow on Twitter via @CyberArk, LinkedIn or Facebook.

THIS PUBLICATION IS FOR INFORMATIONAL PURPOSES ONLY AND IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER WHETHER EXPRESSED OR IMPLIED, INCLUDING WARRANTY OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, NON-INFRINGEMENT OR OTHERWISE. IN NO EVENT SHALL CYBERARK BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND IN PARTICULAR CYBERARK SHALL NOT BE LIABLE FOR DIRECT, SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE OR LOSS OF USE, COST OF REPLACEMENT GOODS, LOSS OR DAMAGE TO DATA ARISING FROM USE OF OR IN RELIANCE ON THIS PUBLICATION, EVEN IF CYBERARK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

06.20. Doc. 398924759