thycotic

# Critical Controls

## for Modern Cloud Security

# Executive Summary

**The cloud makes new levels of speed and scale possible, while freeing people from the time and expense of on-premise infrastructure so they can spend time on critical projects.** With virtual resources supporting you behind the scenes, you can stop installing and patching servers, maintaining uptime, and responding to problems at 3 AM. Instead, moving to the cloud demands that IT operations and security teams update their skills and practices to support a new, more efficient way of working.

In a cloud model, managing privileged access to workloads, services and applications remains your responsibility, not the cloud providers'. It's also your responsibility to make sure data going to and from the cloud (via Web browsers, Email, File exchanges such as SFTP, APIs, SaaS products, and streaming protocols) is properly secured.

Unfortunately, many organizations aren't adequately implementing and enforcing these policies around this privileged access. According to Gartner, through 2023, at least:

**99%**
**of cloud security failures will be the customer's fault.**

**50%**
**of issues attributed to inadequate management of identities, access and privileges.**[1]

This paper will show you how Privileged Access Management (PAM) is a critical control for modern cloud security. We will break down the most common cloud use cases, across Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), and DevOps, that are vulnerable to privileged account attacks. You'll learn how to use PAM to mitigate some of the biggest vulnerabilities across the cloud attack surface so you can realize the promise of the cloud and secure your most sensitive assets.

> **The challenge exists not in the security of the cloud itself, but in the policies and technologies for security and control of the technology. In nearly all cases, it is the user — not the cloud provider — who fails to manage the controls.**
>
> **— Gartner**[2]

[1] *Gartner 2019 Innovation Insights for Cloud Security Posture Management*
[2] *https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/*

# More Moving Parts = More Risk

**15%**

**annual growth of cloud computing, including cloud-based SaaS, IaaS, PaaS.**

**It's a safe bet that you're either already established in the cloud or you've got plans to get there.**

Cloud technology has become core to many business and IT functions. The number of users accessing cloud services, the volume of activities occurring in the cloud and the amount of data cloud services hold is escalating. Eighty-three percent of organizations use the cloud to store sensitive information, including personal and financial data, privileged credentials, and product or corporate-related IP.

All that activity is increasing the number and type of vulnerabilities across your attack surface, as many organizations are finding out the hard way. Organizations are now averaging 4.3 threats each month[3], stemming from external actors, malicious insiders, or unintentional mistakes, resulting in 80% of organizations experiencing at least one compromised account.

For the most common cloud use cases, let's look at the areas of increased risk and identify how PAM controls can help.

[3] *https://cloudsecurity.mcafee.com/enterprise/en-us/assets/skyhigh/white-papers/cloud-adoption-risk-report-2019.pdf*

# PAM Controls To Secure Your Cloud Environment

## 1. Infrastructure-as-a-Service (IaaS)

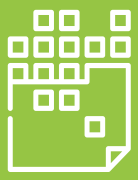
**65%**

**of organizations around the world use some form of IaaS.**

Through IaaS, you can rapidly add compute and storages resources and manage them with elasticity. Additionally, large scale "blob stores" for data storage (like AWS S3) are globally distributed systems that enable even the smallest teams to store petabytes of information.

Analyzing billions of anonymized cloud events, McAfee found that IaaS misconfiguration is rampant. Organizations typically have at least 14 misconfigured IaaS instances running at any given time, resulting in an average of 2,269 misconfiguration incidents per month. These can be as simple as forgetting to check a box during set up. The most common misconfigurations include:

**Unrestricted access**



**Lack of inbound and outbound data encryption**

**Failure to turn on Multi-Factor Authentication (MFA)**

On top of these issues, 5.5% of all AWS S3 buckets are misconfigured. Most organizations have at least one AWS S3 bucket set with "open write" permissions, giving anyone and everyone access to inject data into cloud environments, including malicious code that could modify records.[4]

[4] *https://cloudsecurity.mcafee.com/enterprise/en-us/assets/skyhigh/white-papers/cloud-adoption-risk-report-2019.pdf*

## How PAM Can Help

**40%** **of medium-to-large enterprises by 2020 will have deployed PAM tools to address IaaS privileged security concerns.**[5] To mitigate IaaS vulnerabilities and protect your critical resources, we have found the most effective ways to use PAM solutions include:

### Protect root accounts for servers you set up in the cloud.

When you set up compute resources with your cloud provider, there are several actions you can take to reduce risk. Secure these privileged credentials in a PAM vault, confirm MFA is required for root access, and set up session monitoring and recording for root account activity.

### Limit access to the cloud control panel.

The control panel or console is where you have access to everything in the cloud environment, including servers, databases, messaging, and more. It's also where users and roles are created and assigned access. It's an attractive target for cyber criminals and must be closely governed. PAM solutions help you limit the people with control panel access. Only those most trusted admins should be able to grant access and control resources such as provisioning virtual machines. Even the activities of this trusted team should be fortified with MFA.

### Govern ongoing access to resources.

PAM solutions allow people and resources to use systems, while limiting the actions they can take. With PAM, teams can automatically establish new compute instances, connecting securely to a vault with SSH or Remote Desktop Protocol (RDP) to automatically retrieve credentials. In DevOps organizations, where a broad range of cloud resources are continuously created, used, and retired at large scale, PAM automates high-speed secret creation, archiving, retrieval and rotation.

[5] *Gartner Predicts 2018: Identity and Access Management*

## 2. DevOps CI/CD Environments

Instead of releasing a few application updates per year, more and more development teams are pushing frequent micro-releases to react more rapidly to market demand. Corporate pressure to remain competitive can create a culture of productivity over security. They're using the cloud to make it happen.

**52%**
**of organizations use some form of Platform-as-a-Service (PaaS) to develop applications.**

**94%**
**of IaaS/PaaS use is in Amazon Web Services (AWS).**

**78%**
**use both AWS and Azure, which means many developers have multiple accounts which need to be managed and protected.**

**27%**
**have experienced data theft.[6]**

DevOps teams need on-demand access to cloud-based applications and databases to administer systems and debug issues. It's common for developers to share private keys and credentials for immediate access, which increases the risk of insider threats, either malicious or accidental. Within applications they build, developers may hardcode passwords or store them externally in GitHub or locally in a spreadsheet to save valuable time. These passwords may provide access to data or other critical corporate resources that live in the cloud. Rapid development practices require rapid PAM practices and solutions built for the cloud.

## How PAM Can Help

### Manage access to admin consoles.

The control panel, or dashboard, for PaaS resources gates usage of containers, microservices, databases, and orchestration tools used for application development and deployment. PAM tools can govern, monitor, and record access to this central management console.

### Secure how tools talk to each other.

Tools within an integrated DevOps toolchain need to seamlessly and automatically work together, according to policies and thresholds, to maintain the necessary velocity in the development cycle. PAM solutions allow for cross-talk among development applications via API injections, instead of inserting a human which introduces potential for error into the mix and slows things down.

### Eliminate the need for hardcoded or externalized credential in code.

With PAM, instead of housing secrets in unsecure repositories where they can be hijacked and exploited, credentials can be pulled from a secure vault. There, they can be hidden and rotated automatically to mitigate risk. Usage can also be tracked to monitor for unexpected activity.

[6] *https://cloudsecurity.mcafee.com/enterprise/en-us/assets/skyhigh/white-papers/cloud-adoption-risk-report-2019.pdf*

## 3. SaaS Applications

**1,935** **cloud services used by the average enterprise, an increase of 15% over last year, primarily due to SaaS growth.**


**of business applications (e.g. Office 365, Salesforce.com, project management tools, etc.) account for that figure. Unfortunately, most IT teams think their organizations only use 30 cloud services.[7]**

### How can they be this far off?

Business teams often license cloud services directly, under the radar of IT oversight. When people have trouble remembering multiple passwords, they may store credentials locally on their computer, within their Google accounts or in their browsers. Worse, they may use the same password for multiple tools and rarely, if ever, change them. In addition to using SaaS tools internally, they're collaborating with others and potentially providing open links to unknown third parties outside the organization.

## How PAM Can Help

PAM removes the human element from securing SaaS credentials. Instead of multiple, insecure passwords, PAM tools allow a single secret to be kept under tight control in a central, secure vault. SaaS systems automatically fetch credentials from the vault, which can also be connected to identity management tools or Active Directory, providing role-based access controls to govern SaaS functionality for different levels of users. As a result, users can continue to use the SaaS tools they need, while security and IT teams have visibility and control to enforce consistent security policies.

### Plug-ins for single-sign-on.

For a basic level of control, PAM tools simply inject stored credentials into browser-based SaaS tools so users can simply login to get their work done.

### SAML integration.

For a deeper level of control, PAM with SAML integration allows you to enforce consistent policies for password complexity and rotation.

[7] *https://cloudsecurity.mcafee.com/enterprise/en-us/assets/skyhigh/white-papers/cloud-adoption-risk-report-2019.pdf*

## Which Solutions Are Right For Cloud Security?

You can't wait to properly secure your cloud resources. As your business becomes more reliant on the cloud for infrastructure, application development, and business process automation, your security focus needs to adapt. Take steps to get ahead of misconfigurations and inconsistent controls before they allow attackers to take advantage and infiltrate sensitive data.

### Take a close look at your cloud systems.

Audit your AWS, Azure, Google Cloud Platform or other IaaS/PaaS configurations to make sure you are configuring resources as you intended. Confirm this through testing and validation.

Understand if the DevOps tools you use have privilege security functions built in and if they meet your expectations. Many DevOps tools have nascent, inconsistent or non-existent security controls.

Thoroughly vet your SaaS vendors to see what type of privilege security controls they have in place, including MFA and encryption.

### Develop PAM strategies for efficient, consistent management.

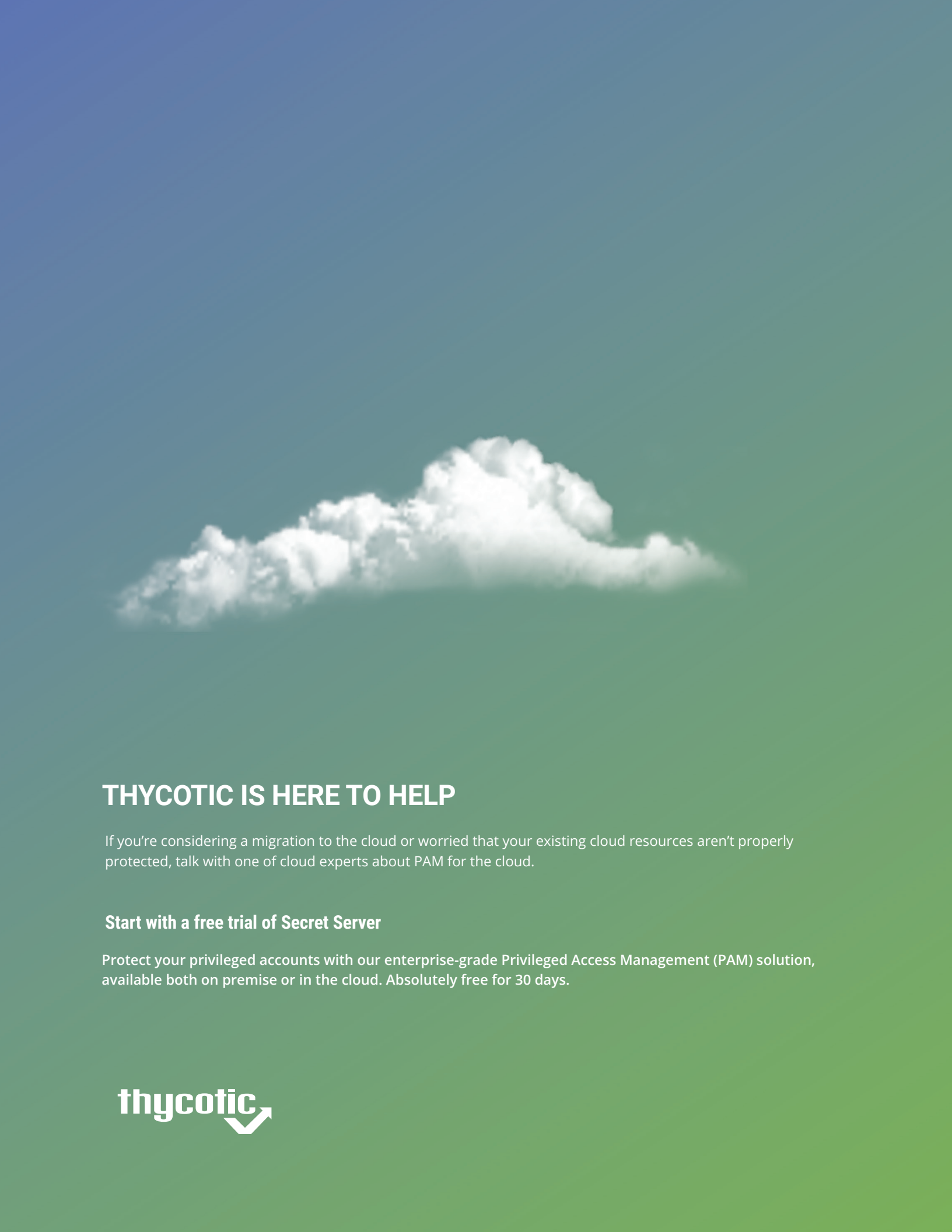
Even with multiple business and technical functions utilizing different types of cloud resources, it's possible for your security team to have a consolidated view of privileged access across your organization and to manage those privileges according to consistent policies. Look for PAM tools that fit seamlessly into different cloud scenarios. Prioritize automation and simple, policy-based control over human intervention and complexity.

### Look for cloud-native solutions.

Managing growing capacity and maintaining top performance for PAM solutions can be tricky with an on-premise approach. If on-premise solutions take up valuable systems resources or require hours or days to learn, not only will your team lose productive time, they may avoid using the tools entirely. In comparison, a cloud-based PAM solution can scale easily. It can match the growth of your privileged accounts, applications, and users without slowing down other resources or losing control. That's one reason Gartner expects 30% of all new PAM deployments to be cloud-based within the next year.[8]

There is a difference between software that is simply "lifted and shifted" from an on-premise data center to the cloud and a solution that is purpose-built with the cloud in mind from the start. PAM designed for the cloud enables tighter integration between secrets, cloud-based infrastructure, and cloud-based applications. It can scale more rapidly to keep up, even with the velocity demands of DevOps teams. To help you fully capitalize on the promise of the cloud, choose cloud-native PAM solutions.

[8] *Gartner Market Report*



# THYCOTIC IS HERE TO HELP

If you're considering a migration to the cloud or worried that your existing cloud resources aren't properly protected, talk with one of cloud experts about PAM for the cloud.

### Start with a free trial of Secret Server

**Protect your privileged accounts with our enterprise-grade Privileged Access Management (PAM) solution, available both on premise or in the cloud. Absolutely free for 30 days.**

thycotic