Brought to you by:

thycotic

Privileged Access Cloud Security

for dummies®
A Wiley Brand

Know your cloud access security challenges

Define and secure cloud privileged access

Get best practices for privileged cloud access

Joseph Carson, CISSP

Thycotic Special Edition

About Thycotic

Thycotic is the leading provider of cloud-ready privilege management solutions. Thycotic's security tools empower over 10,000 organizations, from small businesses to the Fortune 500, to limit privileged account risk, implement least privilege policies, control applications, and demonstrate compliance. Thycotic makes enterprise-level privilege management accessible for everyone by eliminating dependency on overly complex security tools and prioritizing productivity, flexibility, and control. Headquartered in Washington DC, Thycotic operates worldwide with offices in the United Kingdom and Australia. For more information, visit **www.thycotic.com**

Privileged Access Cloud Security

Thycotic Special Edition

by Joseph Carson, CISSP

for dummies®
A Wiley Brand

Privileged Access Cloud Security For Dummies®, Thycotic Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-119-74993-6 (pbk); ISBN: 978-1-119-74996-7 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Carrie Burchfield-Leighton

Sr. Managing Editor: Rev Mengle

Acquisitions Editor: Ashley Coffey

Business Development Representative: Molly Daugherty

Production Editor: Tamilmani Varadharaj

Introduction

Both human and non-human privileged accounts exist everywhere in IT environments. They're used by IT administrators, as well as business users, to automate and manage critical data, applications, and IT services that power successful businesses. These accounts used to be safeguarded inside a defined perimeter with firewalls, VPNs, and so on. But in the always-on, Internet-connected global marketplace, those traditional perimeters have disappeared as most organizations rely to some degree on cloud-based applications to conduct business.

Remote workers, third-party contractors, and business users with personal devices are now accessing privileged accounts every day across the globe. Making sure these users get easy and secure access to the cloud poses ever-growing cybersecurity threats from misuse or abuse by cybercriminals and malicious insiders.

According to the 2020 Verizon Data Breach Investigations Report, for example, cloud data breaches increased to 24 percent of *all* breaches. Among these cloud breaches, 77 percent involved compromised user credentials. And, according to global security firm McAfee, more than one out of four or 27 percent of organizations using platform-as-a-service (PaaS) has experienced data theft from its cloud infrastructure.

About This Book

While privileged access management (PAM) covers all privileged access security, this book focuses on the challenges and best practices involved in privileged access security for the cloud. Its goal is to give IT managers, administrators, systems administrators, and security professionals a better understanding of the specific risks associated with privileged access cloud security — and how to minimize and mitigate threats. The stakes are high. One compromised local admin account on a remote user laptop can have a cascading effect, putting your entire organization at risk.

In writing this book, I assumed you had a basic level of IT expertise and experience, including familiarity with IT networks and the use of privileged accounts (human and non-human) across

the organization. This book may also be useful in educating business unit managers and non-IT executives about the importance of privileged credential security — and the risks involved if resources aren't allocated to help automate their proper management.

Icons Used in This Book

This book uses the following icons to indicate special content.

REMEMBER

You don't want to forget this information. It's essential to gain a basic understanding of privileged access cloud security.

WARNING

Watch out! Pay close attention to these details. They focus on serious issues that have a major impact on you and your organization's cloud security.

TIP

The Tip icon points out practical advice that saves you time and effort in putting together your own privileged access cloud security strategy.

Beyond the Book

Managing and controlling access to privileged accounts is a continuous process as more applications utilize the advantages of cloud-first strategies. Cloud-ready, automated access control tools are essential to protecting the critical data associated with privileged accounts. To help you plan and execute your own cloud access control strategy, visit `www.thycotic.com` for free resources, including software tools, white papers, videos, and product information.

IN THIS CHAPTER

- Recognizing cloud services
- Seeing how cloud security is different
- Facing access challenges

Chapter 1
Understanding Privileged Access Cloud Security

The forces of digital transformation require a new perspective on how to enforce effective control of privileged access and security, especially as organizations expand cloud adoption. As your organization moves to the cloud, you need to understand the new risks and how traditional security practices must evolve to minimize threats.

Looking at Typical Cloud Services

The cloud is basically someone else's servers in another location that allows you to use those resources when required. The cloud is an on-demand, shared network of connected computer resources. Cloud services are organized into several categories:

- **Infrastructure as a Service (IaaS):** Typically computing, networking, and storage that allows you to run your own platforms, such as operating systems, applications, and databases for your data
- **Platform as a Service (PaaS):** Platform dependencies such as operating systems, programming languages, databases, and web servers that run your applications

- **Software as a Service (SaaS):** Typically an application or on-demand software that you subscribe to and use without worrying about the underlying dependencies
- **Security Software as a Service (SECSaaS) and Managed Security as a Service Providers (MSSP):** Cloud solutions that help organizations with migrating to the cloud, finding skilled security resources, and reducing the dwell time to detect data breach security incidents, (which reduce the impact or cost of a data breach)

Spotting Key Cloud Security Differences

On-premises security and cloud security *are* different. I like to use the analogy of a car when explaining the differences. *On-premises security* is like parking your car in your garage. You protect the car with a garage door, which is the primary security control. You don't need to worry about whether the car door is locked, the window is closed, or anyone can see what's inside the car.

Anyone inside the garage is an authorized privileged user who can gain access through the garage door. As long as that person has satisfied the security control — such as having the authorized key or a garage door opener, she gets access. After she's inside the garage, she can move around as required.

When *securing a cloud environment*, the garage door method doesn't work. If you drive your car out of the garage and park it in a shared parking lot, which is similar to what the cloud is in terms of being a shared resource, you need to reconsider the security controls:

- Access control to the car (privileged access management)
- The ability to see inside the car (encryption)
- Identity verification of the person accessing the car (multi-factor authentication)

REMEMBER

Controlling access to the cloud is one of the most critical security controls a company can undertake. You need to not only protect the authentication to the cloud applications but also provide continuous validation and verifications of privileged user actions after they've been authenticated.

Seeing the Benefits of Cloud Security

Cloud solutions come with many benefits:

- **High availability and geo-redundancy:** You can't underestimate the confidence that access will always be there despite service disruptions or outages.
- **Pay as you go, minimizing upfront investments:** Avoid the demands and hassles of getting permission for a capital expense in limited IT budgets.
- **Reduced time spent on maintenance:** Many IT teams are short-staffed these days. Avoid server maintenance and software upgrades that waste resources and time.
- **Hitting the ground running:** Your cloud solution is easy to set up, and the latest version is always at your fingertips without procuring expensive hardware.
- **Highly secure:** Cloud solutions provide more security tools, integrations, and options for security pros to utilize.

Dealing with Cloud Security Access Challenges

With the benefits of cloud solutions (see the preceding section), you also must recognize the hurdles. The security for the cloud is different and introduces many new challenges. According to the Open Web Application Security Project (OWASP), the biggest risks and challenges most organizations face are

- Accountability and risk
- Identity federation
- Regulation and compliance
- Business continuity and resilience
- Privacy and third-party usage of data
- Service and data integration
- Multi-tenancy and physical security

- Incident analysis and security
- Infrastructure security

All these challenges have to have causes, right? The following list gives you the top causes for security incidents and breaches related to the cloud:

- **Poor access management:** Default passwords, credential stuffing, phishing, and abusing stolen credentials are all too common causes of security breaches.
- **Insecure applications and APIs:** Automation without authentication, hardcoded passwords and tokens, and even clear text authentication often lead to security incidents. DevOps has increased these security risks as well.
- **Misconfigured cloud storage:** Public-facing database breaches can result from misconfigured security policies' use of default settings, which sometimes means giving public access to everyone. Default settings don't always mean security is enabled.
- **Distributed Denial of Service (DDoS) attacks:** When a cloud service becomes the target of a DDoS attack, you become a secondary victim. If you're totally dependent on the cloud service, your service will also be impacted.
- **Overprivileged users:** This practice means that after an attacker has compromised an overprivileged account, he can carry out the attack in fewer steps.
- **Shared credentials:** Lost visibility, poor audit trails, and no control with shared credentials result in easy-to-guess passwords or poor practices.
- **Password only security controls:** For many companies, a single password is the only security control keeping unauthorized cybercriminals from abusing their cloud solutions.
- **Securing third-party access and remote employees:** Opening access means you lose control and visibility. Identity access management (IAM), which is the process that combines policies and technology to enable authorized access, becomes the new perimeter.
- **Shadow IT:** The practice of employees obtaining their own IT solutions and cloud services without approval from IT is called Shadow IT.

IN THIS CHAPTER

- Asking the right questions to assess risk
- Assessing considerations in your approach to privileged cloud access

Chapter 2
Securing Privileged Cloud Access

Securing privileged cloud access begins by understanding what it means for your specific organization and how the causes for incidents outlined in Chapter 1 affect you. That means you need to ask the right questions. Some organizations assume access relates only to certain roles or employees. In fact, most privileged access also involves non-human accounts that manage infrastructure, remote access, automation, service accounts, third-party access, and DevOps privileged accounts.

Mapping Cloud Apps and Data

In order to secure cloud access, begin by understanding where data and applications are and how they're used so you can map both to your privileged access security controls. Get started by answering these key questions:

- **Why are privileged accounts needed?** What tasks do your privileged accounts perform in your organization?
- **What types of privileged accounts do you need?** What accounts are typically related to the level of access that these accounts have throughout the organization?

- **Who uses privileged accounts and how often?** Are privileged accounts used by the cybersecurity team to deploy patches, the support team to fix issues, third parties to deploy software, or developers to execute code?
- **Where are privileged accounts found?** Have you mapped locations, such as public cloud, cloud storage, SaaS application login, or web services?
- **How do privileged accounts get used?** Are privileged accounts automated, interactively entered by a person, copied/pasted, or auto-filled?
- **How are privileged accounts secured?** Are privileged accounts protected with multiple security controls or just a simple human created password?
- **What is the risk impact?** If privileged accounts get compromised, what's the possible malicious activity an attacker can do with the account?

REMEMBER

Business users may not have elevated privileges for a specific account, but they may have access to sensitive privileged data, such as a doctor with access to all patients' records.

Approaching Privileged Cloud Access

When you start your journey to privileged cloud access, take into account these considerations:

- **Define access:** Your business functions rely on data, systems, and access, and dependencies on these entities vary from one organization to another, so make sure to define your privileged cloud access. If you aren't sure how to get started, refer to your disaster recovery plan — it typically classifies your critical business systems, applications, and data. Then, map your privileged accounts to your business risk and business operations.
- **Develop IT cloud access policies:** Your organization should have a policy that details acceptable use and responsibilities for privileged cloud accounts. Your working understanding of who has privileged access, and when it's used, is vital. Treat privileged accounts separately by clearly defining a

privileged account and spelling out acceptable use policies. Identify and track ownership of privileged accounts throughout their life cycle.

- **Use a risk register:** Use a risk register as part of your IT cloud access policy that requires any new cloud application to register the data impact risk along with the privileged access management (PAM) matrix questions. You can automate this with a risk classification that determines what additional security controls must be included to reduce any risks identified.
- **Discover your privileged accounts:** Automated PAM software identifies your privileged accounts, implements continuous discovery to curb privileged account sprawl, identifies potential insider abuse, and reveals external threats. Ongoing visibility of your privileged account landscape is central to combating and reducing cybersecurity threats.
- **Understand business users' privileged access:** All access is becoming privileged whether it's due to the level of access of the account or the access users have to sensitive company data. Business users fall into this category, so consider them as having privileged access.
- **Protect your passwords:** Verify that your solution can automatically discover and store privileged accounts; schedule password rotation; audit, analyze, and manage individual privileged session activity; and monitor accounts to quickly detect and respond to malicious activity. Protecting your privileged account cloud passwords goes beyond having a password manager. Establish Single Sign-on sessions to target systems for better operational efficiency of administrators that combine multi-factor authentication and privileged access security.


TIP

Minimize the ability for humans to create and choose passwords. This oversight reduces cyberattacks that use techniques, such as credential stuffing, while minimizing exploits of bad cyber hygiene behavior, such as password reuse.

- **Limit IT admin access:** Develop a least-privilege policy to enforce least privilege on endpoints and to limit IT admin access to cloud applications without disrupting business operations. Privileges should only be granted on demand

when required and approved. Least-privilege and application-control solutions enable seamless elevation of approved, trusted, and whitelisted applications while minimizing the risk of running unauthorized applications.

- **Monitor and record sessions:** Your PAM solution should monitor and record privileged account activity, which helps enforce proper behavior and avoid mistakes by users. Audit, record, and monitor privileged activities to assist with regulatory compliance.
- **Detect abnormal usage:** Visibility into the access and activity of your privileged accounts in real time helps catch suspected account compromise and potential user abuse. Track and alert user behavior. Early detection of security incidents significantly reduces the cost of a data breach.


WARNING

You must manage, monitor, and restrict the administrative access of IT outsourcing vendors and managed service providers (MSPs) to cloud and internal IT systems because many incidents result from compromised third parties.

- **Respond to incidents:** Include privileged access in your incident response plan in case an account is compromised. Simply changing privileged account passwords or disabling the privileged account isn't adequate when a privileged account is breached. If you need help with your incidence response plan, check out `thycotic.com/solutions/free-it-tools/free-privileged-account-incident-response-policy-template`.
- **Audit and analyze:** Continuously monitoring privileged account usage via audits and analysis reports helps identify unusual behaviors that may indicate a breach or misuse. These automated reports track the cause of security incidents and demonstrate compliance with policies and regulations.

IN THIS CHAPTER

- Starting with a least-privilege everywhere strategy
- Automating and integrating access controls
- Making trust adaptive and dynamic

Chapter 3
Five Best Practices for Securing Privileged Cloud Access

This chapter explains five best practices for enabling privileged cloud access security without perimeters. It outlines how you can secure access by your IT administrators and privileged business users to the systems, applications, and data they need to perform their jobs from any location while satisfying strong access security controls and continuous verifications of identities.

Enable Widespread Least-Privilege Access Security

Least-privilege cybersecurity enables enforcement of a zero-trust, risk-based security model. After a user is verified, the user's access is limited to only what's necessary to accomplish a specific task or job. In the past, least privilege was seen by employees as a negative experience that prevented them from performing their jobs when privileges were restricted and that increased IT support calls to gain access. As a result, organizations often enabled

local privileged access for almost every employee — a highly risky practice that can be abused by cybercriminals to elevate privileged access.


TIP

Fortunately, some solutions facilitate just-in-time (JIT) privileged access to the cloud with detailed security controls. With this in mind, IT and business users can

- Get the access they need when they need it
- Increase productivity
- Reduce support costs
- Minimize risks from cyber threats

For example, if a user needs access to a database or cloud storage that contains sensitive data after she has already authenticated, she should be required to get further authorization. That authorization could include on-demand security controls, such as multifactor authentication, access workflow, and the recording of session activity to assure the risk of abuse is reduced.

With many organizations operating in hybrid on-premises and cloud environments, implementing least privilege on servers or endpoints isn't enough. Least-privilege security controls must encompass all privileged access, including cloud-based systems, applications, databases, and infrastructure.

Automate Access to Make Security Work for You

Security controls must be scalable, efficient, and require the least amount of resources possible — and that requires automation. For example, organizations that experience a breach can reduce the cost of a cyber incident by half if they have automated controls. With a shortage of skilled IT security professionals, automated tools are essential to managing consistent and secure cloud privileged access.


REMEMBER

Automation also mitigates the risk of human error by reducing the amount of manual effort required to complete tedious and repetitive low-level tasks. Leverage solutions with application programing interface (API) capabilities that can be integrated into

automated workflows and ticketing systems to streamline access approvals and provide access automatically after proper identity verifications have been completed.

Integrate Solutions to Create a Security Society

Siloed cloud security solutions are no longer acceptable. Your cloud security controls should offer automated API integration of other security tools. Integrated solutions help create a "security society" where all tools and components can enhance and complement each other to improve security posture and reduce overall cyber risks.

For example, consider a vulnerability scanner that needs to scan a cloud infrastructure and requires privileged access to conduct the scan successfully. Instead of duplicating credentials for the scan, you can integrate the vulnerability scanner to a privileged access cloud security solution.

REMEMBER

Security solutions that integrate are solutions that work in the background, bringing more value to an organization.

Minimize User Friction by Implementing Usable Security Solutions

Users have too often viewed security controls as a barrier to productivity. Time and again, productivity and ease of use are the very benefits that drive users to move to the cloud. Your privileged access cloud security solution must build in ease of use, operating in the background as much possible. Security tools that are too complex aren't just difficult to use; they're downright dangerous.

REMEMBER

Security solutions must add value to the business on multiple levels:

- Having an intuitive interface
- Being quick to learn
- Providing immediate value
- Contributing to making each user's job easier

Implement transparent and highly extensible tools, so you can match your own workflow and systems.

Move Beyond Zero Trust to Adaptive Risk-Based Trust

A least-privilege security model assumes that for any user or system to gain authorized access, the prospective user must earn trust through verification controls. Implementing this model poses challenges because going from trusting everything in the network to trusting nothing typically frustrates employees and impacts productivity. Most organizations now recognize security controls that reduce productivity will ultimately be rejected and become ineffective.

As more critical resources and data continue to move to the cloud, your security controls must be dynamic and able to adapt to evolving threats. Create policies or rules across the enterprise for identities, services, applications, data, and systems. For example, you can have an "always-verify" and "always-monitor" policy for third-party vendors or contractor identities. Internal employee classifications would be adaptive based on the sensitivity of the data being accessed. An always-verify policy requires credentials and multifactor authentication, while an always-monitor policy audits and records all activity.

Zero-trust grants only necessary access to critical assets. Organizations typically start with a zero-trust approach beginning with high-risk areas such as supply chain, contractors, temporary employees, sensitive networks, and privileged accounts. Companies are extending their zero-trust security approach to remote employees, third-party vendors, and contractors who need access to corporate resources.

Adaptive risk-based trust enables the business to reduce risk by using zero trust as the baseline for how organizations build trust scores that will be used to determine how much security must be satisfied to gain access to the cloud, applications, networks, and systems.

FREE RESOURCES FOR
PRIVILEGED ACCESS CLOUD SECURITY

WHITEPAPERS AND REPORTS

Critical Controls for Modern Cloud Security

Learn how your security team can have a consistent Privileged Access Management (PAM) strategy to mitigate vulnerabilities across your cloud attack surface including multiple business and technical functions utilizing different types of cloud resources.

https://thycotic.com/resources/pam-for-the-cloud/

KuppingerCole Report: "Thycotic Access Controller"

Digital transformation, Cloud, and Hybrid IT environments are putting new demands on PAM. To manage privileged access cloud security, Thycotic has integrated three new Access Controller products into its portfolio of PAM solutions to meet these challenges.

https://thycotic.com/resources/access-controller-products-kuppingercole-report/

CLOUD ACCESS SECURITY TOOLS AND TRIALS FOR IT PROFESSIONALS

Free Trial of Thycotic's Cloud Access Controller

Thycotic Cloud Access Controller ensures that IaaS and SaaS users have the necessary privileges required for their roles. Role Based Access Controls can be precisely defined to control what each user can click, read, or modify within any web application. Separation of roles and duties is easily enforceable on standard accounts and shared accounts for web applications. Administrators have a dashboard of activity that clearly displays activity, for tighter cloud app security, uninterrupted productivity, and streamlined compliance.

https://thycotic.com/products/cloud-access-controller/

Free Trial of Thycotic's Secret Server

Protect your privileged accounts with our enterprise-grade PAM solution available both on-premises, or in the cloud.

https://thycotic.com/products/secret-server/

Secure privileged access to cloud applications

With the increasing adoption of cloud applications and services, organizations across the globe must understand and manage the challenges posed by privileged access from remote employees, third-parties and contractors. Making sure these users get easy and secure access to the cloud poses ever-growing cybersecurity threats from cybercriminals and malicious insiders. This book gives you the foundational knowledge you need to define and implement privileged access cloud security and protect your organization.

Inside...

- Pros of privileged access cloud security
- Cloud access security challenges
- Mapping privileged access to cloud services
- Privileged cloud access requirements
- Approaches to securing cloud access
- Cloud privileged access best practices
- Finding success with automated solutions

thycotic

Joseph Carson, multiple infosec award winner, has 25+ years of experience in enterprise security. He's the author of *PAM For Dummies* and *Least Privilege Cybersecurity For Dummies*. Joseph, an active member of the cyber community, speaks at global conferences, advising governments and critical infrastructure, financial, and maritime industries.

ISBN: 978-1-119-74993-6
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.