Hackers & Security Professionals at Black Hat:

Where they agree & where they differ

Executive Summary

During the Black Hat annual conference in Las Vegas August 3-8, 2019, Thycotic conducted research with nearly 300 attendees identifying either as "hackers" (49%) or "security professionals" (51%). Surveying participants every year at Black Hat, Thycotic aimed to gauge the opinions of both the security professional defenders tasked with keeping systems secure, and hackers tasked with breaking into systems to identify weaknesses. Only 4% of hacker respondents to our survey identify themselves as criminals using their skills for malicious activity. Thus, most hackers we surveyed consider themselves as helping improve security and a valuable resource for reducing risks from cyberattacks.

This year survey questions focused on cyber security issues associated with privileged account access and credential governance, particularly for service accounts, which Gartner has designated a top priority two years in a row.

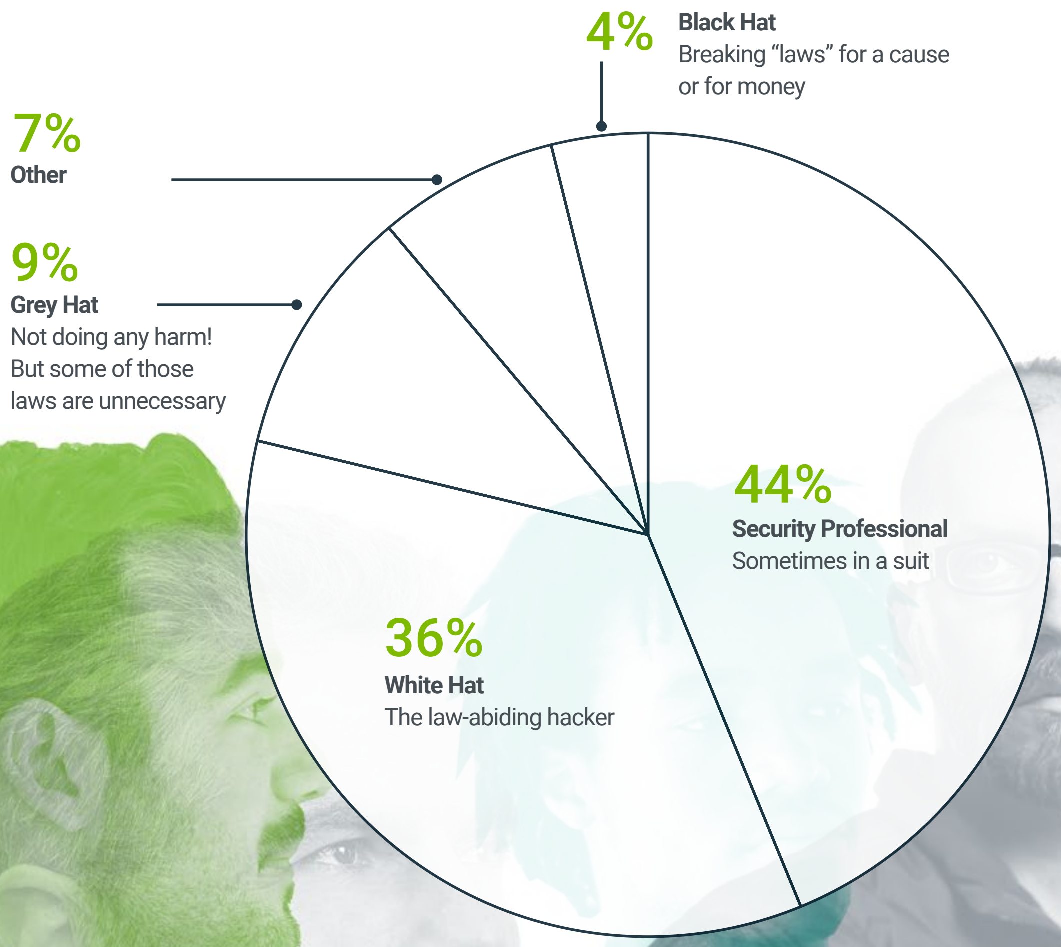
49%

IDENTIFIED AS HACKERS

51%

IDENTIFIED AS SECURITY PROFESSIONALS

What kind of hacker do you identify as?



Where they agree

Both hackers and security pros strongly agree that service accounts are an attractive target because hackers can easily elevate privileges and gain access to sensitive information.

Service accounts are typically used in operating systems to execute applications or run programs, either in the context of system accounts (high privileged accounts without any password) or a specific user account, usually created manually or during software installation. On Unix and Linux systems, they are often known as init or inetd, and are also capable of launching programs.

Service accounts can pose a significant risk to organizations because they are so difficult to manage and secure properly, especially across multiple accounts for different services, tasks, and other applications. These accounts are time consuming to control and prone to human error when managed manually. Service account passwords are also a challenge: administrators can't safely change a service account password if they don't know where it's used without risk of bringing down other applications.

Frequently, in software installations, the password for the service accounts either remains the default vendor password (easily found on the internet) or is in the memory of the consultant who installed the software.

Both hackers and security professionals are in near identical agreement on the best ways to protect a service account from compromise:

#1 **Remove unnecessary service accounts**

#2 **Rotate credentials frequently**

#3 **Monitor all privileged account activity to detect suspicious behavior**

1/3

SECURITY PROS SAY SERVICE ACCOUNT PASSWORDS ARE CHANGED ONLY AFTER AN INCIDENT OR NEVER ROTATED!

Where they differ

Service accounts (24%) and domain admin accounts (26%) were considered most vulnerable targets by security pros while hackers preferred domain admin accounts (33%), root accounts (30%) and then service accounts (20%).

Nearly 50% of security pros believe hackers would sell stolen sensitive data for profit and only 10% would disclose it responsibility. Hackers say the opposite. 50% of hacker respondents say they would disclose hacked information responsibly while less than 5% would sell the info or hold it for ransom.

Shockingly security professionals appear to not trust hackers; however, research shows that most hackers are good citizens using their skills to help organizations improve security. It is critical that both sides find common ground. Therefore, not only is communication important between hackers and security professionals/executive boards, it is also necessary they join forces with a goal of exposing threats and minimizing risks.

This differentiation is important, and why many in the industry are moving away from the term "hacker" as a bad guy, and instead using the more appropriate "cybercriminal" for those hacking with malicious intent.

KEY TAKEAWAYS

#1 Get control of your service accounts now! Remove unnecessary accounts, rotate passwords frequently, and monitor activity.

#2 Hackers target privileged accounts in the cloud, on-premises, and hybrid environments without a clear preference.

#3 Security professionals and hackers still have a “trust gap” that needs to be addressed.

Which cloud providers have the best security?

A significant number of security pros (36%) and hackers (22%) did not feel any of the major providers, such as AWS, Microsoft or Google, were especially good at protecting their IT environments from threats. Hackers seemed to have a better opinion of AWS (32%), followed by Google (22%) and Microsoft Azure (20%). Security pros rated AWS (30%) ahead of both Microsoft (18%) and Google (15%).

#1

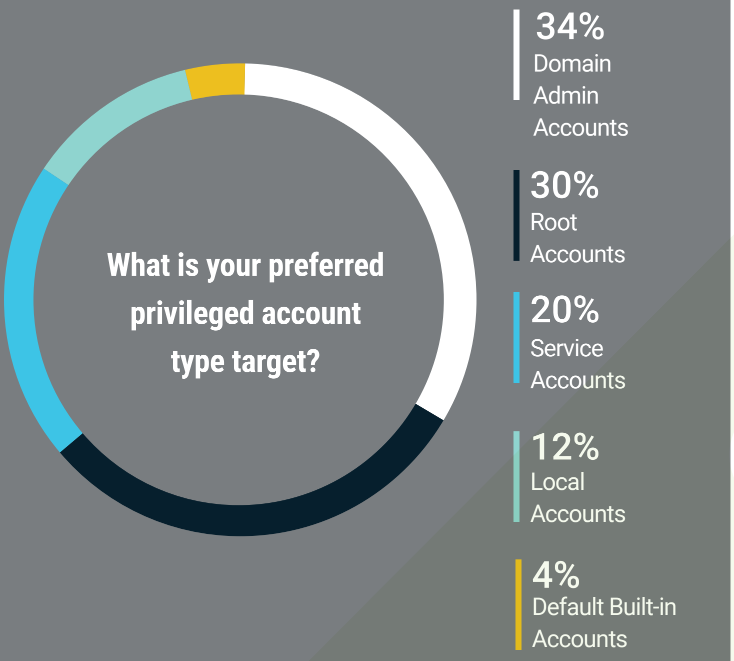
Get control of your service accounts now! Remove unnecessary accounts, rotate passwords frequently, and monitor activity.

Service accounts can be privileged local or domain accounts that are used by an application or service to interact with the operating system. Service accounts may have domain administrative privileges depending on how they are used by applications. Local service accounts can interact with a variety of Windows components, which makes coordinating password changes difficult.

Survey Results

What type of privileged accounts are the best targets (most vulnerable)?

Hacker preferences when targeting privileged credentials

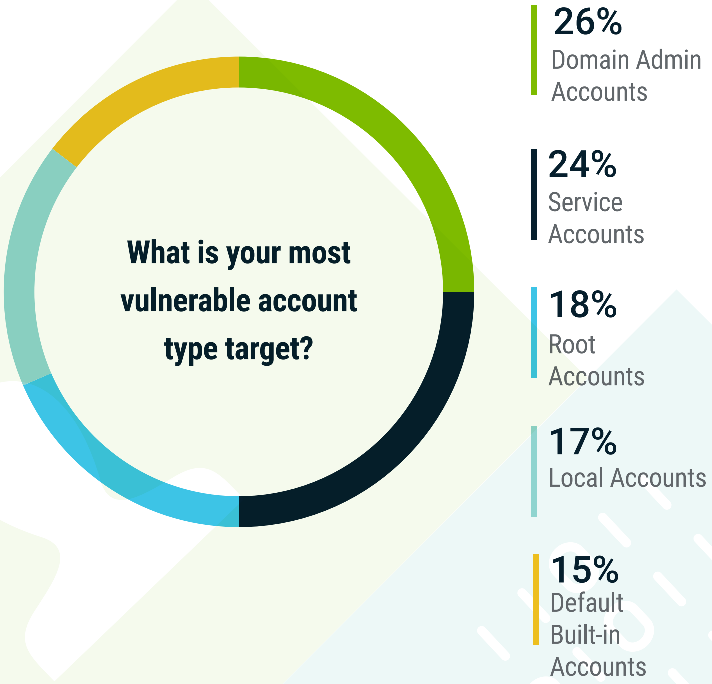


34% of hackers prefer Domain Admin Account targets

30% prefer to target Root Accounts

20% prefer to target Service Accounts

Security pros worry about these privileged accounts as most vulnerable



26% say Domain Admin Accounts are most vulnerable to hackers

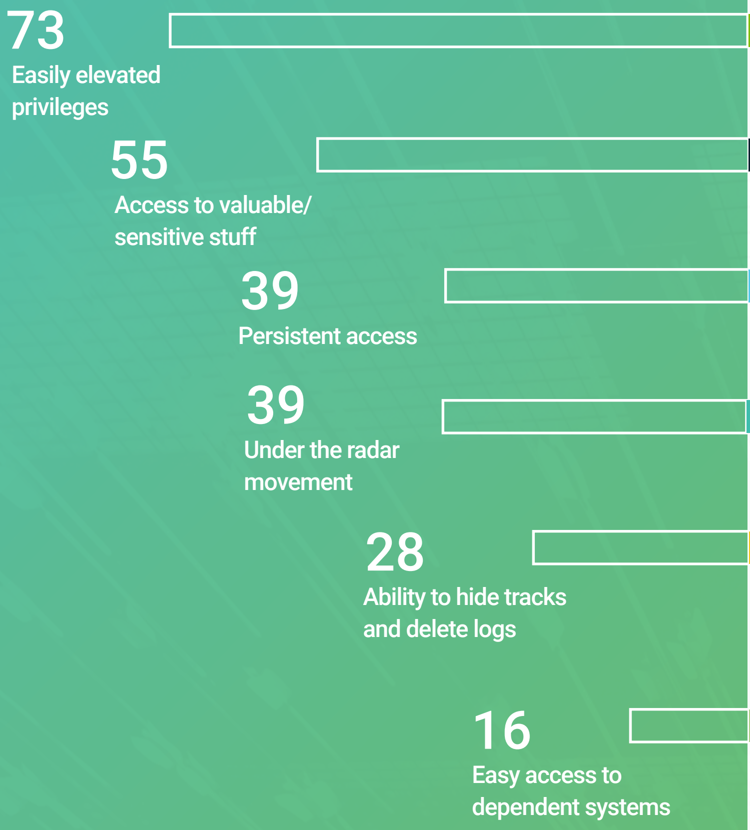
24% say Service Accounts are most vulnerable

18% say Root Accounts are more vulnerable

17% say Local Admin accounts are the most vulnerable

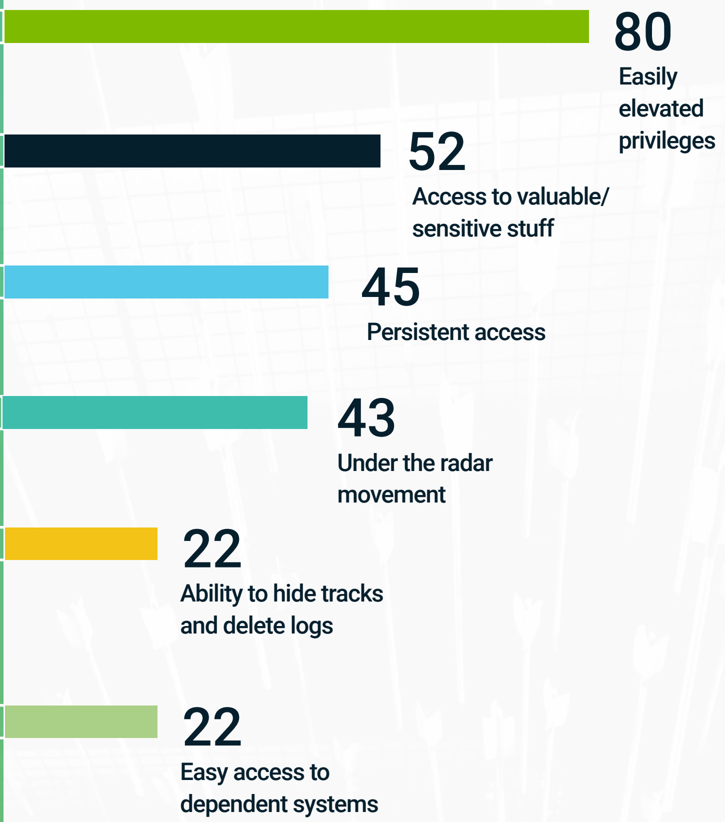
Why are service accounts a favored target of hackers?

Number of responses to this question based on top two choices



Security pros agree with hackers on why service accounts are such an attractive target.

Number of responses to this question based on top two choices



Top reasons hackers like to compromise service accounts

#1 **Easily elevated privileges**

#2 **Access to valuable/sensitive data**

#3 **Persistent access**

#4 **Under the radar movement**

Top reasons security pros think service accounts are such a popular hacker target

#1 **Easily elevated privileges**

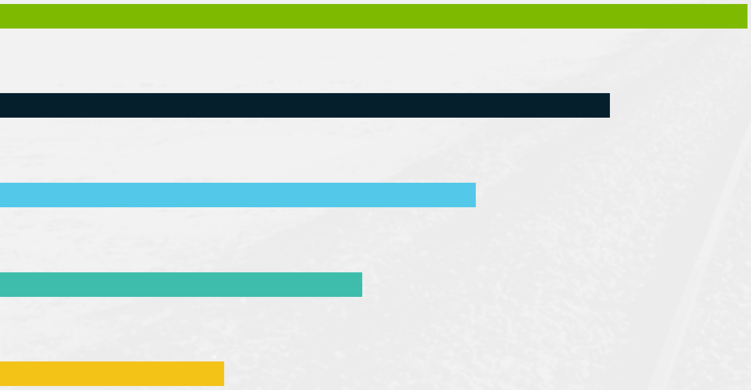
#2 **Access to valuable/sensitive data**

#3 **Persistent access**

#4 **Under the radar movement**

How do hackers cover their tracks when hacking a service account?

Number of responses to this question based on top two choices



Top ways hackers cover their tracks after compromise

#1 **Delete audit logs**

#2 **Move laterally through the network in case exploited account is discovered**

#3 **Hide within existing service usage**

75
Delete audit logs

62
Move laterally on the network in case exploited account is discovered

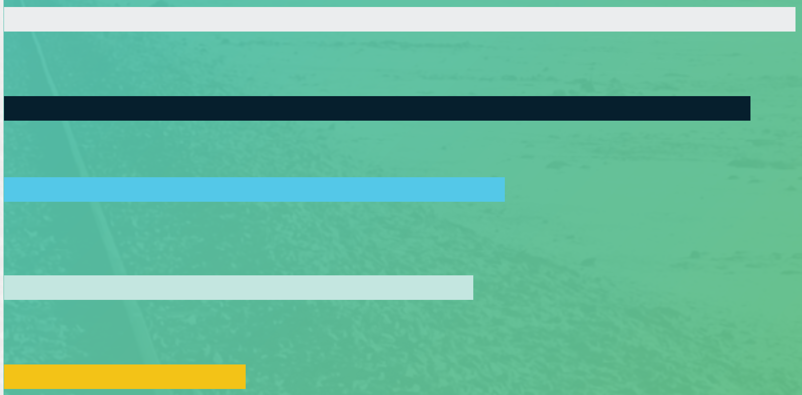
50
Hide within existing service usage

38
Create more privileged accounts as a diversionary tactic

25
Change security configuration

Here's how security pros think hackers cover their tracks.

Number of responses to this question based on top two choices



Security pros agree with hackers about top ways to cover their tracks after compromise

#1 **Move laterally through the network in case exploited account is discovered**

#2 **Delete audit logs**

#3 **Hide within existing service usage**

76
Move laterally on the network in case exploited account is discovered

72
Delete audit logs

48
Hide within existing service usage

45
Create more privileged accounts as a diversionary tactic

23
Change security configuration

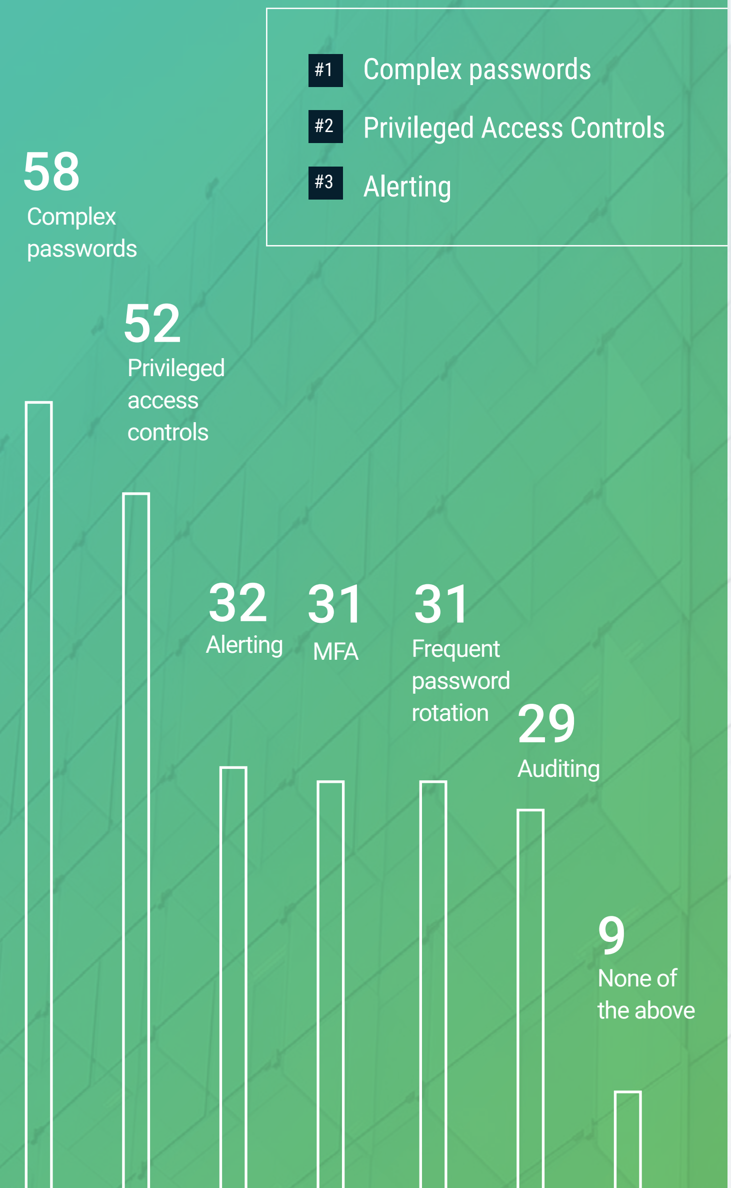
What kinds of protections for service accounts exist?

Alerting was an area where security professionals and hackers differed on what security controls protect service accounts. Hackers find alerting was a top 3 protection they encounter; however, security professionals had this much lower on their priority list. It appears that alerting makes a hacker's job more difficult; however, security professionals might not be doing enough to enable alerting to protect service accounts.

Here are the top three protections hackers run into when targeting service accounts.

What security controls do you come across on service accounts?

Number of responses to this question based on top two choices



#1 Complex passwords

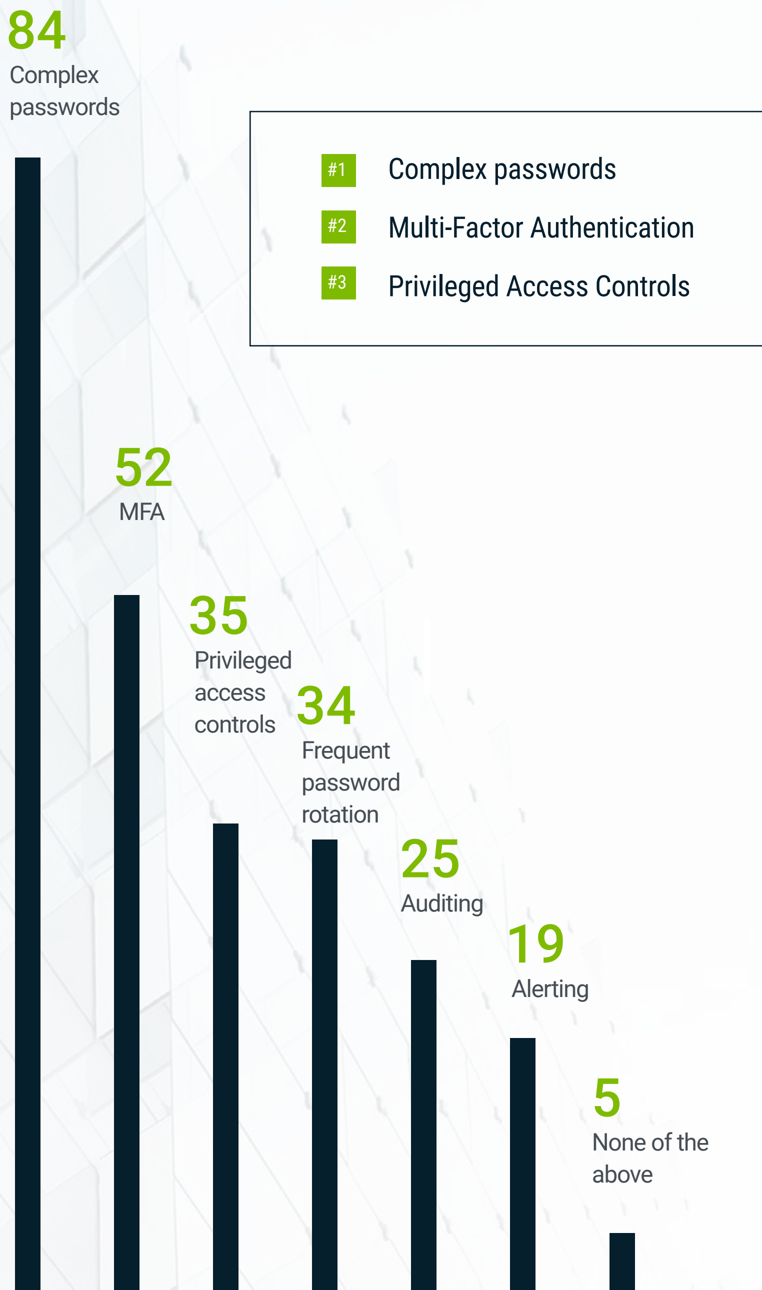
#2 Privileged Access Controls

#3 Alerting

Top security tools that security pros use to protect their service accounts

What security controls do you to protect your service accounts?

Number of responses to this question based on top two choices



#1 Complex passwords

#2 Multi-Factor Authentication

#3 Privileged Access Controls

How often to you change or rotate passwords on service accounts?

Service account and application passwords are often set to never expire and subsequently remain unchanged. Failing to change service account passwords represents a significant security risk because service accounts often have access to sensitive data and systems.

Here's what hackers encounter in the field when targeting service accounts.

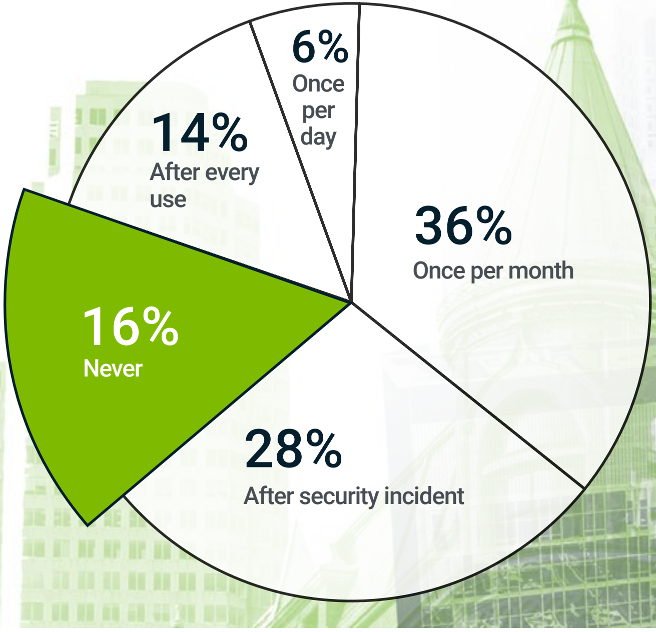
For the service accounts you target how often are passwords generally rotated?

16% of organizations never rotate passwords on service accounts!

28% only rotate passwords after a security incident!

36% rotate passwords once a month

Hackers discover organizations tend to rotate service account passwords once per month meaning they have up to one month to elevate privileges, laterally move around the network to remain hidden and avoid detection. Majority of companies use only complex passwords to protect service accounts; however, privileged access security controls are on the rise.



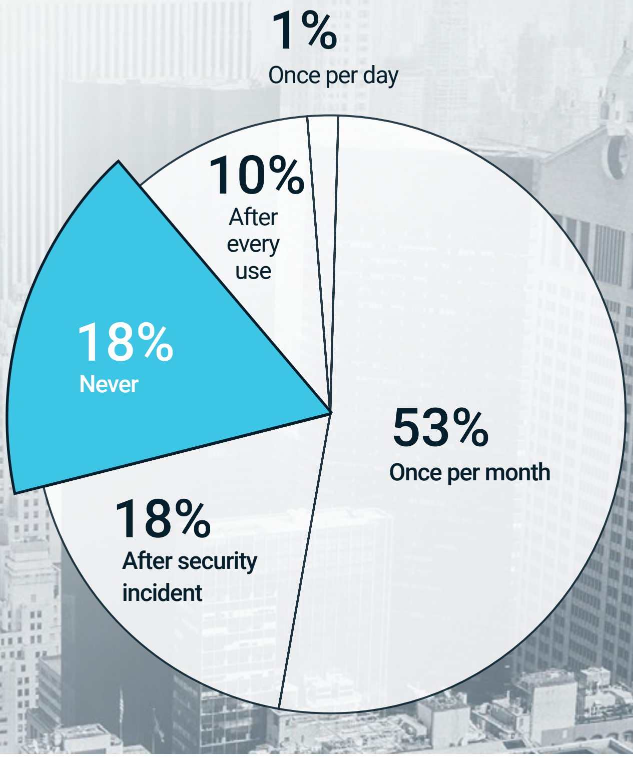
Here's what security pros say they do in practice.

How often are passwords generally rotated on your service accounts?

18% of security pros admit they never rotate passwords on service accounts!

18% rotate passwords only after an incident!

53% say they rotate passwords once a month



What's the best way to protect service accounts from compromise?

Both hackers and security pros strongly agree: the best way to protect service accounts is to discover and remove unnecessary ones, followed by frequent rotation of passwords. Yet 18% of security pros say service account passwords are changed only after a security incident, and 18% never rotate service account passwords!

Here's what hacker respondents said works best to protect service accounts.

Number of responses to this question based on top two choices

What is the best thing companies can do to prevent a service account compromise?

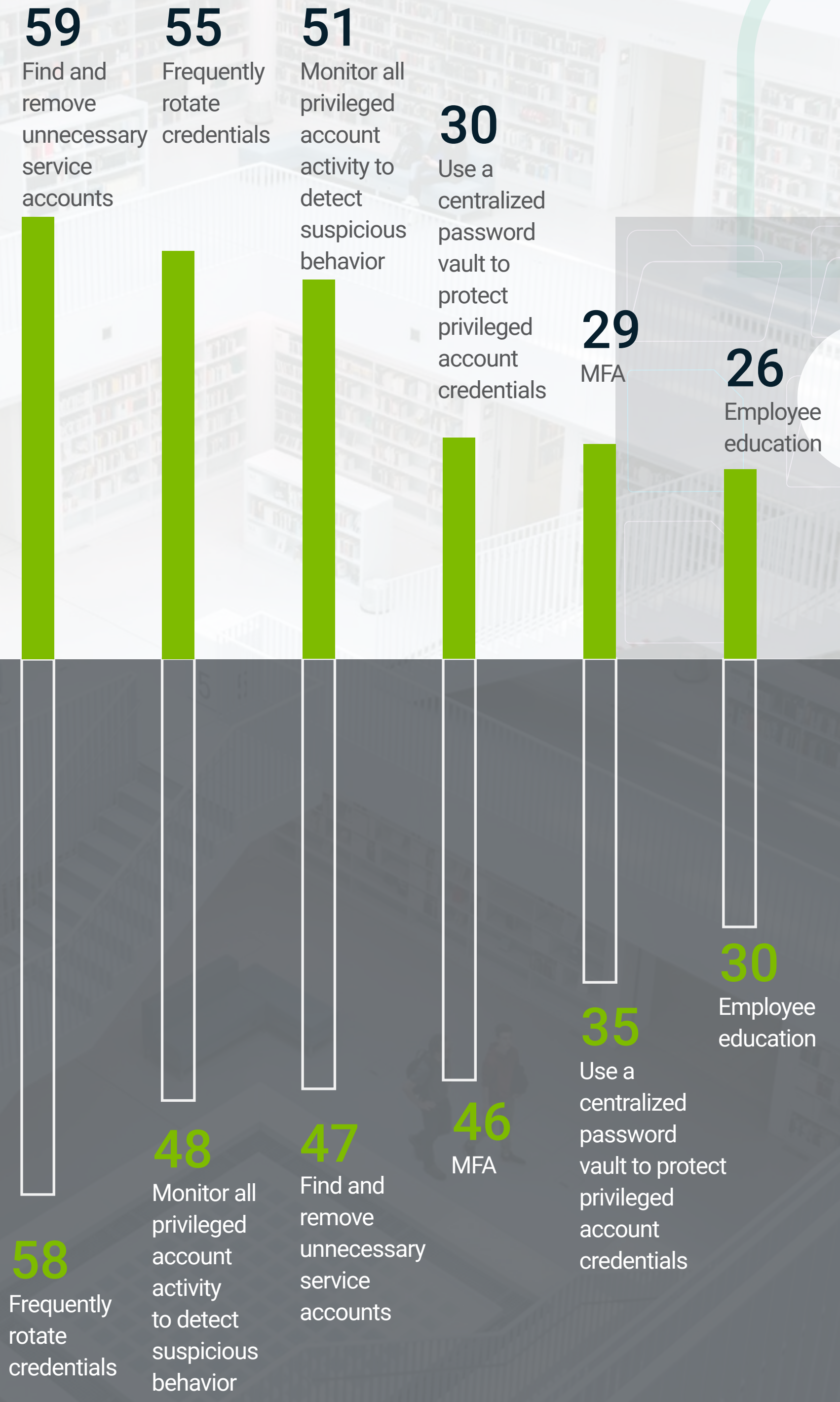
- #1 Find and remove unnecessary service accounts
- #2 Frequently rotate credentials
- #3 Monitor all privileged account activity to detect suspicious behavior

Security pros agree with hackers; these are the best ways to protect service accounts.

Number of responses to this question based on top two choices

What is the best thing you can do to prevent this type of compromise?

- #1 Frequently rotate credentials
- #2 Monitor all privileged account activity to detect suspicious behavior
- #3 Find and remove unnecessary service accounts



thycotic.com | sales@thycotic.com

thycotic

Recommendations

Removing unnecessary service accounts is one of the most effective steps to reduce the risks associated with service accounts. However, it appears to be one of the most neglected in the lifecycle of service accounts management. Most organizations focus on business continuity, setting default or static passwords that never get changed for fear it might break something. However, when a service account is no longer required, there needs to be an automated process that decommissions those accounts to eliminate vulnerabilities.

Rotating credentials makes it more costly and difficult for attackers to have persistent access, and both security professionals and hackers agree that rotating passwords frequently increases the security of service accounts.

Free Resources

KuppingerCole White Paper: "Privileged Access Governance"
https://thycotic.com/kuppingercole-pag

Webinar: "Top 10 Service Account Management Best Practices"
https://thycotic.com/top10-serviceaccount-practices

Free Tool: Service Account Risk Snapshot for Windows
https://thycotic.com/risk-snapshot

Define and classify service accounts

Every organization is different, so you need to map out what important applications and programs rely on data, systems, and access. One approach is to reuse a disaster recovery plan that typically classifies important applications and specifies which need to be recovered first. Make sure to align your service accounts to your business risk and operations.

Provision and decommission service accounts

Because service accounts run critical processes, these accounts multiply quickly creating service account sprawl with more dependencies than you can count. Bring your service accounts to a one-to-one state, where one service account runs one service, and review and decommission accounts on a regular basis.

Discover your service accounts continuously

Use automated privileged access management (PAM) software to identify your service accounts and implement continuous discovery to make sure all accounts are protected. This helps ensure full, on-going visibility of your service account landscape crucial to combatting cybersecurity threats.

Monitor service account activity

Your PAM solution should be able to monitor, record, and alert on service account activity. This will help enforce proper behavior and avoid mistakes by employees and other IT users because they know their activities are being monitored.

THE CENTRAL THEME OF BLACK HAT 2019: **communication!**

In his opening remarks, Jeff Moss, also known as Dark Tangent, described the challenges security professionals are experiencing today. He emphasized that communication can be the difference between getting fired or achieving security goals and budget. He also covered the rule of law along with major trends, such as decentralization.

Delivering the main keynote, "Every security team is now a software team," Dino Dai Zovi head of security at Square, recognized the value of fear in managing cyber security. First you must fear the impact of the threat, he argued, then understand and assess the risks and ultimately reduce those risks by mitigating them where possible. The best way to overcome fear is to understand the nature of risks and find automated solutions to help manage cyber security risks so that your security teams can scale and become more efficient in dealing with threats.

Privileged accounts are everywhere

Privileged accounts, such as service accounts, are everywhere in the IT environment. They give information technology the building blocks for managing vast networks of hardware and software that power our information-driven world. Yet for most people they are invisible.

Because privileged accounts are used by systems administrators to deploy and maintain IT systems, they exist in nearly every connected device, server, database, and application. In addition, privileged accounts extend well beyond an organization's traditional IT infrastructure to cloud environments and employee-managed corporate social media accounts.

That means organizations can typically have two to three times more privileged accounts than employees. And, in many cases, some privileged accounts, such as service accounts, within an organization may be unknown, unmanaged, and therefore unprotected.

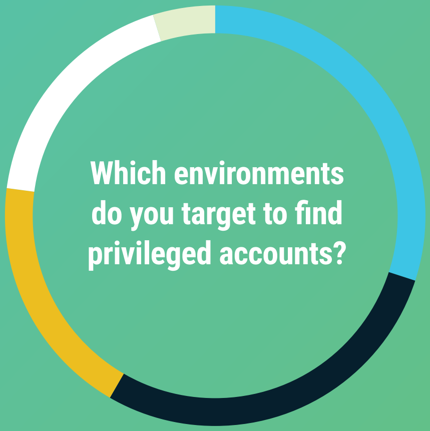
#2

Hackers target privileged accounts in the cloud, on-premises, and hybrid environments without a clear preference.

While some security professionals might consider cloud environments a broader or more vulnerable attack surface that's less well defended than on-premises operations, hackers were rather agnostic when targeting privileged accounts.

Survey Results

Here's how hackers responded



Which environments do you target to find privileged accounts?

30%
On-premises

29%
Cloud

19%
Doesn't matter where it is, resistance is futile!

17%
Hybrid cloud/on-prem

5%
Supply Chain Contractors

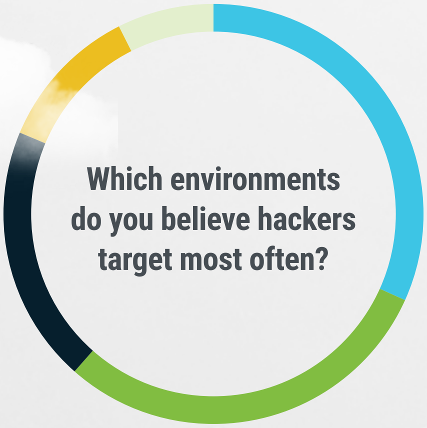
30% of hackers target credentials on-premises

29% target credentials in the cloud

17% target credentials in hybrid cloud-on-premises environments

19% say the type of environment doesn't matter

Here's what Security Pros thought



Which environments do you believe hackers target most often?

32%
Doesn't matter where it is, resistance is futile!

29%
Cloud

20%
On-premises

11%
Supply Chain Contractors

8%
Hybrid cloud/on-prem

29% say hackers target cloud environments more often

20% say hackers target on-premises

32% feel it doesn't matter

11% say supply chain/ contractors are most frequent targets

Recommendations

Protect your service account passwords

Proactively manage, monitor, and control service account access with password protection software. Your PAM solution should automatically discover and store service accounts.

Schedule password rotation

Use an automated function in your PAM solution to schedule password rotation on all service accounts.

Audit and analyze service account activity

Use a PAM solution to audit, analyze, and manage service account activity. Monitor password accounts to quickly detect and respond to malicious activity. Continuously observing how service accounts are being used through audits and reports will help identify unusual behaviors that may indicate a breach or misuse. These automated reports also help track the cause of security incidents, as well as demonstrate compliance with policies and regulations. Determine if service accounts are still required, review security controls and update expiration dates.

Free Resources

2019 Global Research Report: "Security as a Service on the Rise"
https://thycotic.com/sas-research

Webinar: "How Cloud Adoption Makes PAM in the Cloud a Top Priority
https://thycotic.com/pam-cloud-adoption

Free Tool: Weak Password Finder for Active Directory
https://thycotic.com/weak-password-finder

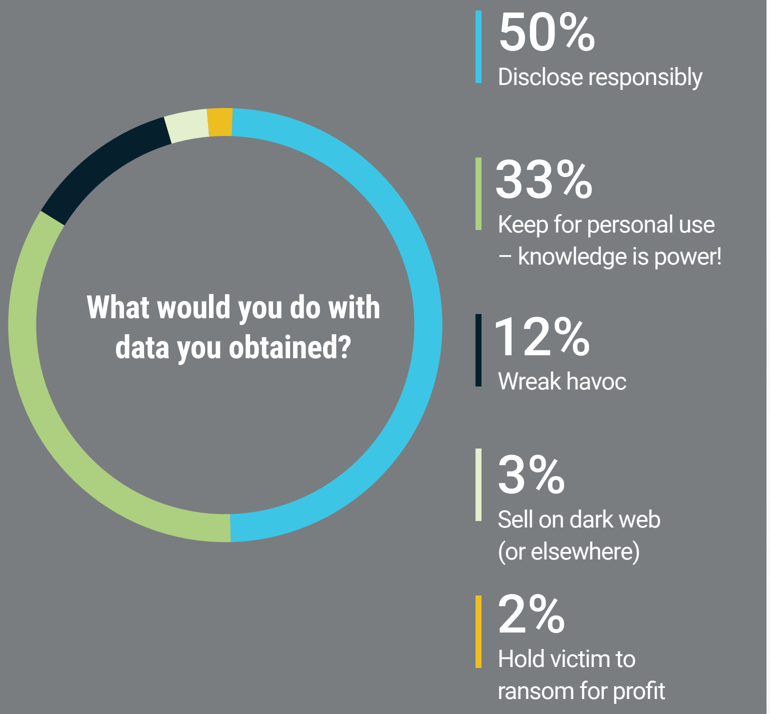
#3

Security professionals and hackers still have a “trust gap” that needs to be addressed

While the Black Hat conference attracts more than 19,000 hackers and security professionals from all industries, there appears to be “trust gap” between hackers and security pros. Nearly 50% of security pros believe hackers would sell stolen sensitive data for profit and only 10% would disclose it responsibility. Hackers say the opposite.

Survey Results

Here’s what hackers said they would do with compromised data



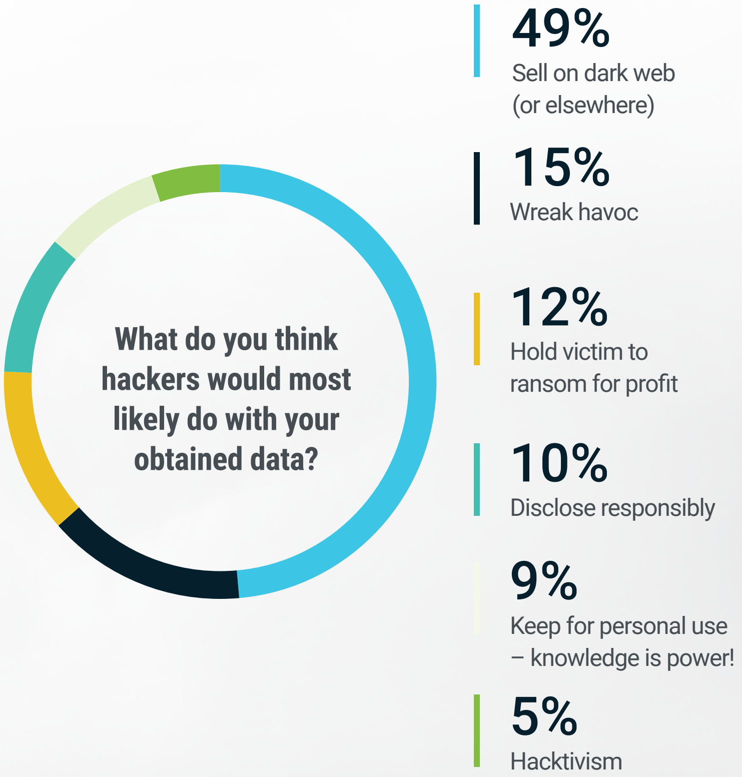
50% would disclose data responsibly

33% would keep data for personal use

12% would wreak havoc with stolen data

5% would sell data on the dark web or ransom

Here’s what security pros think hackers would do with their data



49% of hackers would sell stolen data on the dark web

15% would wreak havoc with stolen data

12% would hold data for ransom

10% would disclose data responsibly

Recommendations

Echoing Jeff Moss's comments in his keynote address to Black Hat attendees, cyber security is all about communication—and that means going beyond successfully communicating to the executive board. Security pros need to become better communicators but also engaged listeners. While security professionals and hackers use different techniques, they are ultimately trying to solve the same problem albeit from different perspectives.

Just as security professionals must balance security with productivity among employees, they must also find common ground and open communication channels with hackers. In the past, the media has often portrayed hackers negatively, however, their actions and insights may ultimately prove to contribute significantly to reducing risks from cyberattacks.

Free Resources

Research Report: "The CISO Challenge-Aligning Business Enablement with Enforcement"
https://thycotic.com/cyber-exec-report

Webinar: "2019 Black Hat Conference Debrief: Key Takeaways and Insights"
https://thycotic.com/blackhat-2019-debrief

White Paper:
"The Anatomy of a Privileged Account Hack"
https://thycotic.com/anatomy-of-a-hack

Basic rules of thumb for cyber security pros going forward:

#1 Think business value first

#2 Drive a positive security experience

#3 Make security an integral part of your corporate culture

#4 Be a sincere listener

#5 Work together with hackers to understand threats and risks

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 UK and Australia.

www.thycotic.com

thycotic