SSH.COM

WHITEPAPER

Re-Thinking Privileged Access Management in the Age of Hybrid Cloud

As hybrid cloud grows, bad habits and risky behaviors put corporate data at risk

Executive Summary

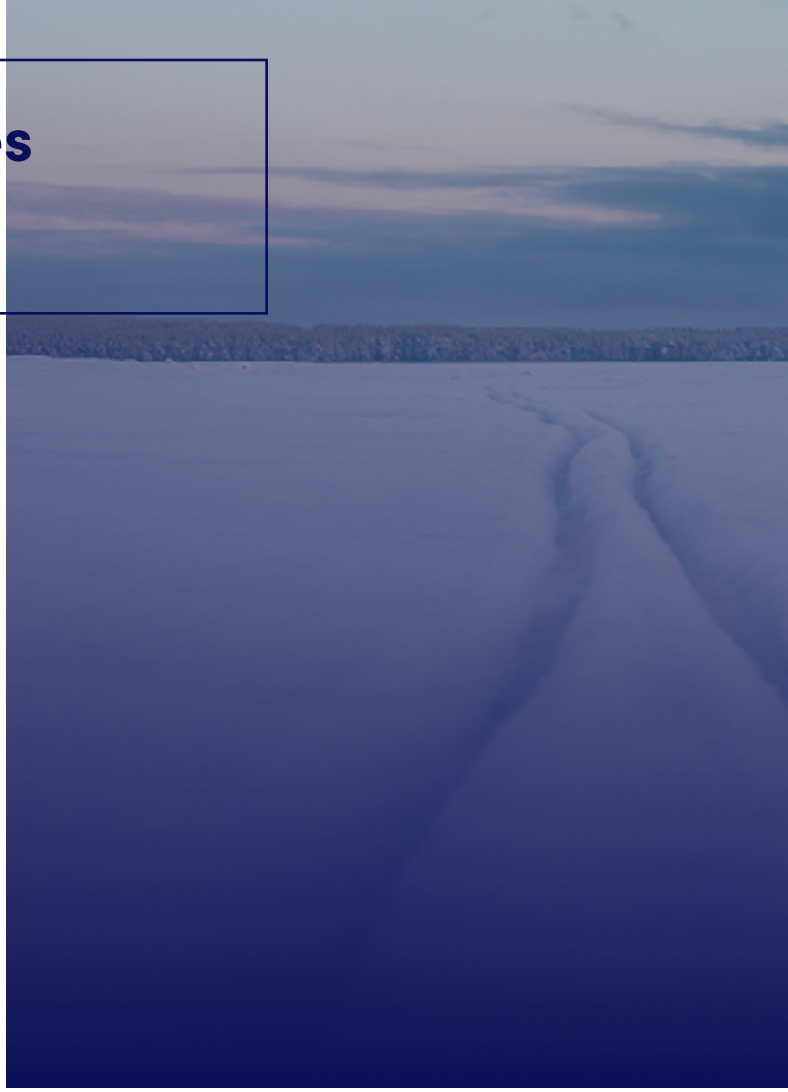
As more organizations race to the cloud, one IT paradigm is emerging as the preferred option: hybrid cloud. Companies are bringing public and private clouds into the picture alongside their legacy on-premises infrastructure to get the best mix of speed, agility, performance, and productivity for their workforces.

But, as IT environments become more complex, how strong are the security policies, controls, and processes that are meant to protect corporate data? Are gaps emerging that could potentially put businesses at risk?

We wanted to find out. In spring 2020, SSH.COM commissioned a study, conducted by Vanson Bourne, of 625 IT and application development professionals from different levels of seniority across the United States, United Kingdom, France, and Germany. We asked these individuals how they feel about cloud migration, and how their organization's privileged access procedures, policies and tools are holding up as their IT estate grows more complex.
We learned that high-risk behaviors in many organizations, including password sharing, excessive access, and the bypassing of software security controls, threaten to undermine the security of corporate IT. And we found that more than half of IT and application development professionals would be willing to sacrifice security for speed, bypassing software security controls if they were under pressure to meet a deadline.

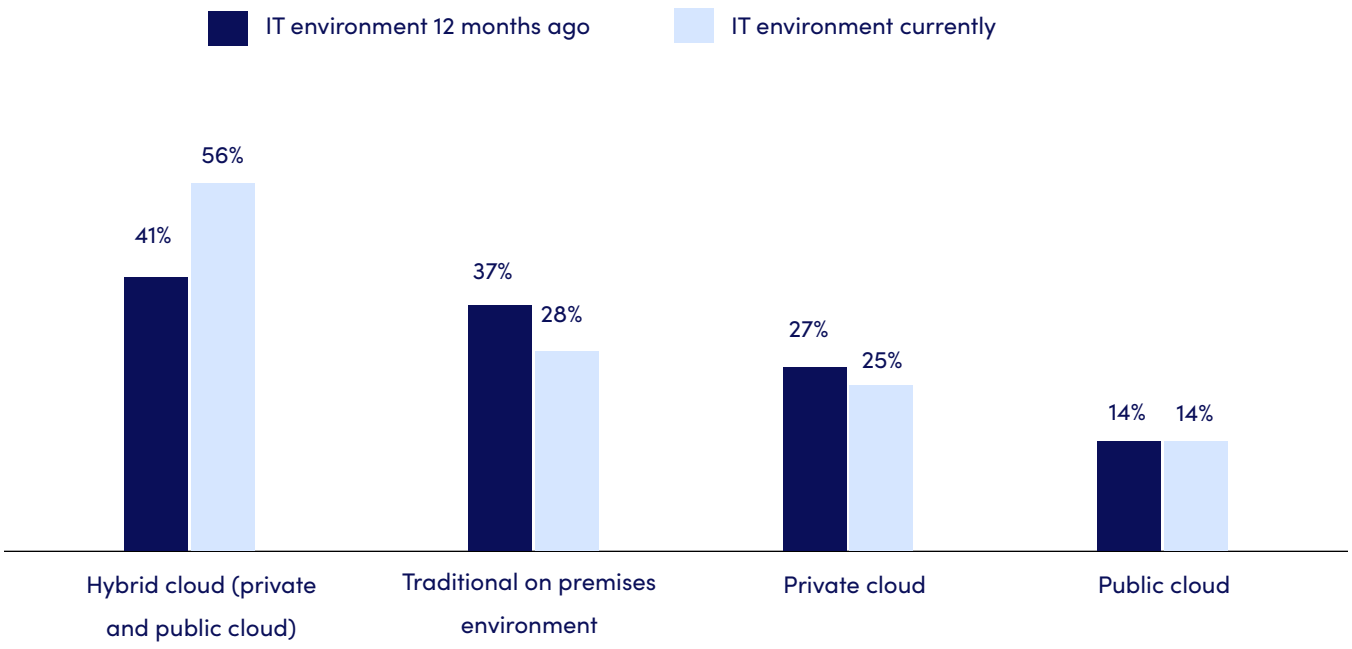
The results provide a view of the habits that threaten corporate IT, and a blueprint for how to re-think privileged access management in the age of the hybrid cloud.

Hybrid Cloud: Opportunities & Challenges



Make no mistake: IT and application development professionals are bullish on the cloud. In total, 87% of respondents said they feel very or fairly confident that their organization could run all its operations from the cloud.

Despite this, the most popular choice for companies is hybrid cloud, where some of the services are still run in an on-premise or in private cloud environments while other services are run in public cloud all orchestrated in unison. And that number is on the rise – 56% of respondents described their current IT environment as "hybrid cloud," an increase from 41% one year ago. Comparatively, the number of respondents who said their IT was hosted exclusively on-premises or in a public cloud or private cloud dropped year-over-year.



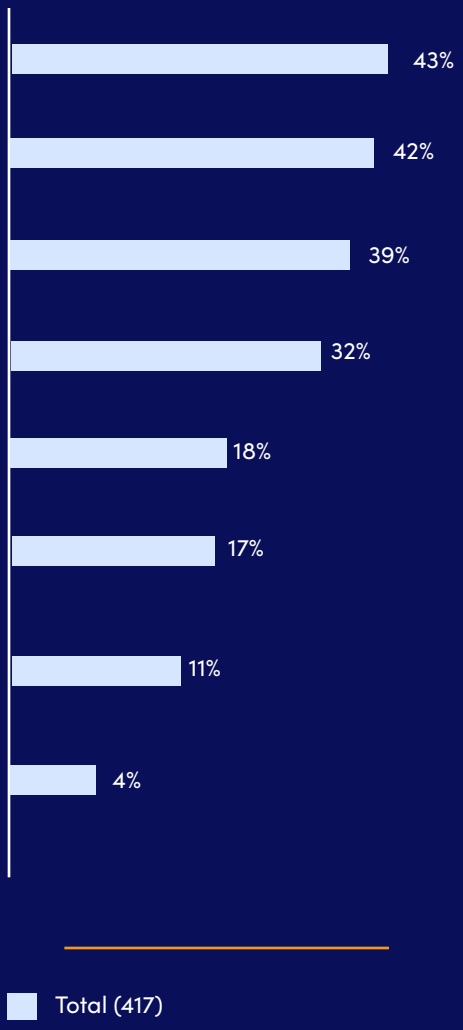
Hybrid Cloud: Opportunities & Challenges (cont.)

There are no signs that this shift is slowing down, and in fact, IT and application development professionals at all levels mostly believe that more cloud would be better. The majority – 82% – said that adopting more cloud services would make work somewhat or much faster when it comes to the speed of their go to market. Additionally, 42% said they expect that agility and productivity in the cloud would increase slightly if their organization didn't need to use legacy infrastructure as much – an additional 21% expect a significant increase.

Hybrid cloud also offers strategic benefits, including the flexibility to pick where to host certain IT resources based on evaluations of cost, performance, security or productivity. Our study found that most organizations (45%) are opting for centralized, in-house management of cloud IT services rather than outsourcing to a third-party MSP (36%) or allowing different in-house teams to manage their services independently (32%).

As for which cloud vendors to bring in, the "big three" service providers – Microsoft Azure, Google Cloud, and Amazon Web Services – are the most likely to be used, in that order. There is some variation when accounting for the size of the organization, and the choice isn't exclusive – on average, companies are actively using two vendors at a time.

Cloud vendor use



All the ways secure access to the cloud slows down work

Still, not every new cloud deployment goes as smoothly as intended. We found that companies experience several challenges with the tools they use to securely access cloud IT, including their privileged access management (PAM) software.

For respondents whose organizations use cloud solutions, we asked which common issues resulting from cloud access solutions, such as PAM, tend to slow down daily work. The biggest speed bump cited was configuring access (34%) – which could involve configuring SSH keys, switching between access protocols, or revoking access. Repeatedly logging in and out was the second-biggest hurdle (30%).

As one might expect, answers varied slightly depending on the nature of the job.

Application development professionals, who typically like to work fast and must often shift between environments to get work done, were most likely to say that they were slowed by frequent logging in and out (35%). Senior IT security leaders were most likely to say they were inhibited by things like configuring access (39%) or granting access to other users (34%). IT admins also expressed troubles with configuration (30%).

Speed Bumps

IT pros share the top secure accessaccess tasks that slow down work

34%
Configuring access

30%
Repeatedly logging in and out

29%
Granting access to other users

25%
Waiting for access

23%
Hopping between consoies

Cutting Corners: How IT and Application Development Pros Bypass Security Controls

Why is it important to understand common PAM challenges? PAM is the gateway to protected IT resources and data. If employees are struggling with the tools they use to access sensitive parts of the hybrid cloud infrastructure, they might feel emboldened to try workarounds or avoid PAM tools altogether. This bears out in our data, which revealed several risky secure access behaviors.

Before we examine those risky behaviors, let's first look at how organizations are currently managing the boundaries around their IT.

Modern boundaries for modern IT

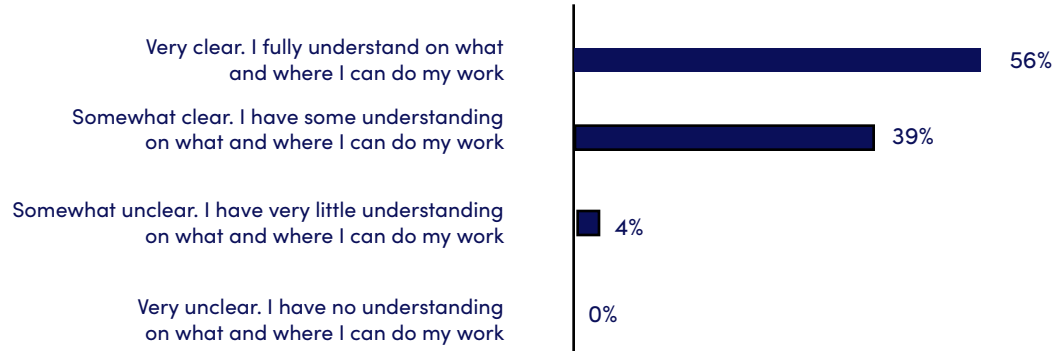
Privileged access management is much more complex in a hybrid IT infrastructure than in an on-premises infrastructure, if for no other reason than the fact that there are many more environments to worry about. IT users might need to log into several different clouds – recall that organizations are using, on average, two public cloud vendors.

And depending on their role and responsibilities, some IT users might require a deeper level of access to more sensitive information than their colleagues.At the same time, the nature of work has changed. More IT professionals are working outside of the office, from home and on- the-go. That means accessing sensitive corporate data from potentially unsecure networks.

So, it's clear that there is much work to be done to define the new boundaries of modern IT. Businesses essentially need to identify the user and his or her role, as well as the resources those users must access within the IT environment. Companies could also define where and when that access can be granted.

In our study, we wanted to understand how well-equipped organizations currently are to support these new paradigms. We asked respondents if they believe they have the right level of permissions and access rights to the services they use to get through their daily tasks. Most (73%) said yes, claiming that they rarely need to ask for any additional access for non-standard tasks. A smaller group (17%) said they have enough access to get through daily tasks but still need to ask for access most of the time, suggesting a potential speed bump.

Which of the following best describes how clear you believe your organization's IT perimeters and boundaries are?



Most IT and application development professionals (56%) said they have a full and clear understanding of the boundaries and perimeters that have been set by their organization around where they can work and what devices they can do work on. However, boundaries were a bit hazier for the rest of respondents, and results suggest some organizational policies may unwittingly create security gaps.

Public networks

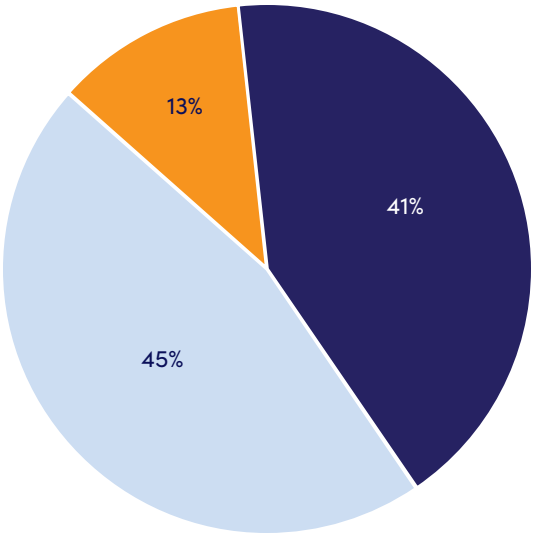
For example, we asked respondents if their company allows users to access internal IT resources from a public network – a clear possibility introduced by increasing remote work.

While 45% of respondents can currently access some internal resources via public internet, 41% said they can access their full set of internal resources. Access tends to become more restrictive as company size increases – 19% of respondents working at companies with 5,000 or more employees said they could not access any internal resources via a public network. Respondents from companies of between 3,000 and 4,999 employees were most likely (48%) to say they can access the full network from anywhere.

Public networks are inherently less secure than private ones, so in an ideal world, no organization would allow corporate IT to have full access to devices using the public internet. At the same time, it's not feasible to completely restrict this kind of access, because it would make employees unable to work remotely and therefore less productive.

Some sort of balance needs to be achieved, with employees able to access only the parts of the network they need to get the job done, and for limited periods of time, from specific locations. Some parts of the network may need to be totally restricted.

Does your company allow users to access internal IT resources from a public network?



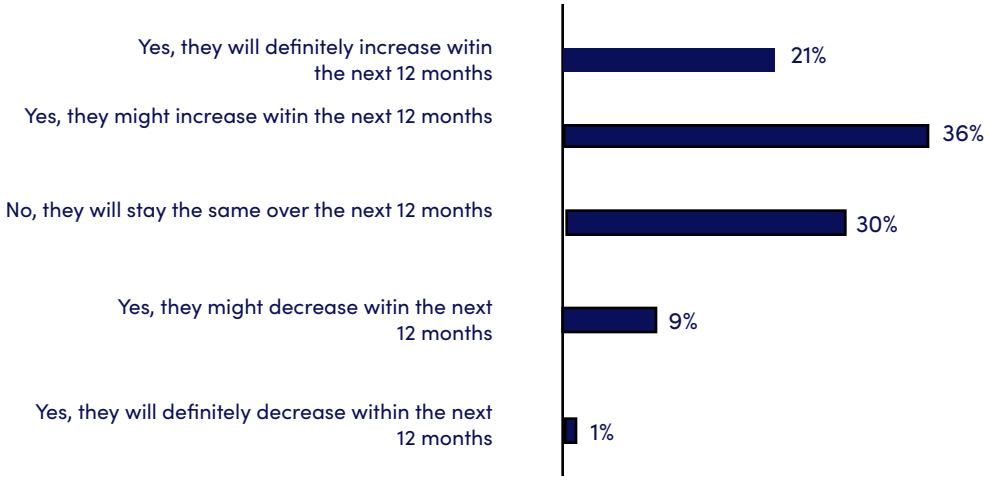
Third-party IT suppliers

Third-party access is another risk point. Businesses sometimes need to grant IT access to outside contractors who are working on special projects. We found that nearly a third – 29% - of respondents said that these contractors are given permanent access credentials for this kind of work.

Permanent credentials are inherently risky. They provide widespread access beyond the task at hand, and can be forgotten, stolen, mismanaged, misconfigured, or lost. If these credentials are obtained by cybercriminals, they can also be used to help attackers move laterally within a network. Given that contractor projects are often time-bound, and that outside access should always be revoked upon completion of the project, it would be safer instead to grant contractors temporary IT access for the duration of the contract.

Our survey found that organizations plan to increase their use of third- party IT suppliers in the next 12 months. It will be important for these companies to get a handle on their secure access policies sooner rather than later.

Does your organization plan to increase or decrease the use of third-party IT suppliers in the next 12 months?



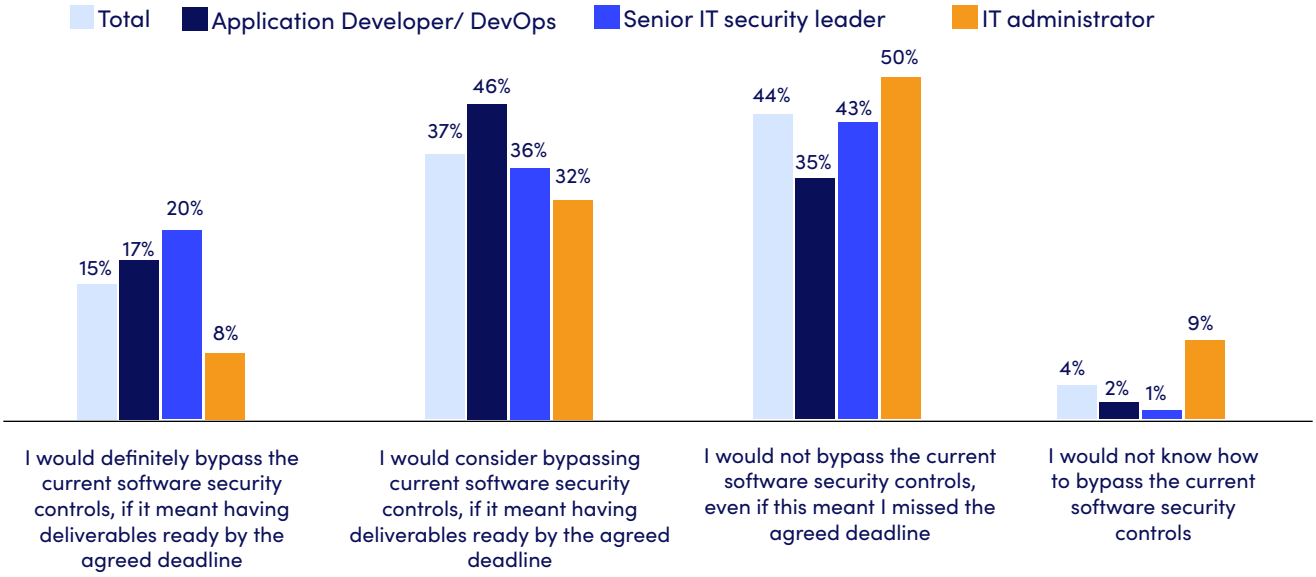
Finding loopholes

Besides security policies that create vulnerabilities, there is also the issue of users whose bad habits or risky behaviors drive them to bypass security controls. After all, just because users claim to understand their company's IT boundaries, doesn't mean they will always obey them, especially if there is a clear motivation for not doing so and if they are tempted by workarounds.

We presented respondents a scenario: if you were under pressure to meet a deadline, but software security controls were in the way, how would you act? More than half said they would "definitely" or at least consider bypassing those security controls to get the job done. Application development professionals (63%) were most likely to at least consider a workaround, while IT security leaders (56%) and IT admins (40%) were more likely to play it safe.

Only a small number of respondents said they would not know how to bypass security controls, meaning the vast majority of employees appear to have some expertise finding loopholes.

If you were under pressure to meet a deadline, but software security controls were in the way, how would you act?



The obvious question for businesses is: how often does the temptation to use a loophole arise? Realistically, it probably happens more often that most would care to admit. Every business is in a rush to deliver new products or meet a deadline. Developers are under special pressure and new ways of working, such as the DevOps model, have even been introduced to increase developer speed, agility, and productivity. The hope has always been that faster would not necessarily mean less secure, but clearly, workers will do what they need to do to get the job done.

Credential storing and sharing

We also wanted to explore habits around the storage and sharing of passwords or credentials. IT and application development professionals frequently use secure credentials, like SSH keys, to access IT environments. We found that while many say they're keeping those credentials locked away in encrypted folders or files on their computer, or in dedicated password management software like LastPass, RoboForm, or DashLane, others are much less careful with their credentials. A fifth of respondents admitted to keeping passwords in emails, and a slightly smaller proportion saying on paper, or in non- encrypted files and folders.

Additionally, 86% of respondents said that some or all privileges or credentials are saved to the target servers of applications in their organization. This is risky because if an attacker were to gain access to a server where a public key is stored, it could use that key to bypass password authentication in the future. Even if the password is reset, the attacker will retain access via the rogue key.

Shared accounts is another risky behavior – 70% of respondents said this can sometimes be an issue for their organization. There are plenty of reasons why organizations share credentials, and they ultimately boil down to convenience. Senior IT security leaders were most likely to say that sharing makes it easier for multiple users to access a team account (52%) or to improve employee productivity (52%).

Where IT and development professionals store passwords or credentials

54%
Encrypted files/folders on my computer

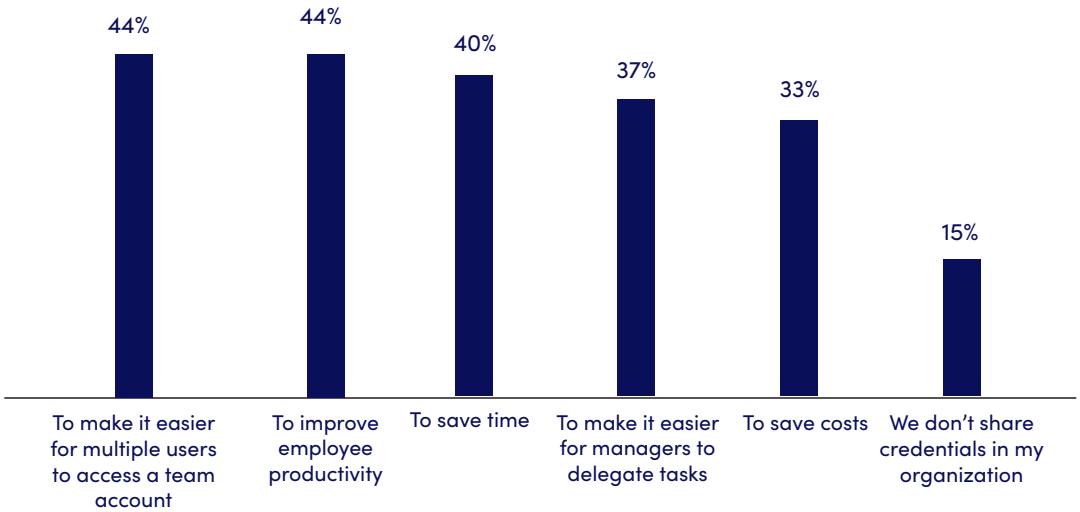
53%
Password manager software

20%
Emails

16%
On paper, locked away

15%
Non-encrypted files/folders on my computer

Top reasons why organizations share credentials



Can anyone be trusted?

Most organizations are already in the habit of protecting their perimeter from external threats, but the Zero Trust framework proposes that it's a mistake to inherently trust any users or devices who operate within a corporate network, even employees. The idea is that any device can be a hacker's entry point to the network, so no one inside or outside of the organization should be trusted with unrestricted access to privileged information.

At first glance, our findings would seem to support this notion – clearly, employees are falling into bad security habits that put the organization at risk. But does Zero Trust actually make for good security policy in practice? If the IT department is imposing strict Zero Trust security solutions on their workforce, does that restrict the fast-paced workstyle that modern developers need to do their best work? Could it even encourage workers to take more shortcuts?

After all, some level of trust and cooperation is required between each part of the business to ensure that value-driving products and services are delivered, especially at a time when developers are pushed to deliver better products, faster. Employees who cut corners on security are often well-meaning: they're just trying to find a faster way to meet deadlines. Rather than trying to restrict, control or penalize risky employee behaviors, what if businesses made it easier for employees to adhere to corporate security without slowing down work?

Simpler is Safer: The Case for User-Friendly Privileged Access

Generally, there seems to be appetite within organizations for newer, better tools to help manage work. In all, 40% of respondents said they were not completely confident that their company's existing solutions would easily adapt and scale for their needs within the next 12 months. And the wide majority (90%) believe that new tools and technology in their organization would make work easier.

When it comes to privileged access management, what should those new tools look like?

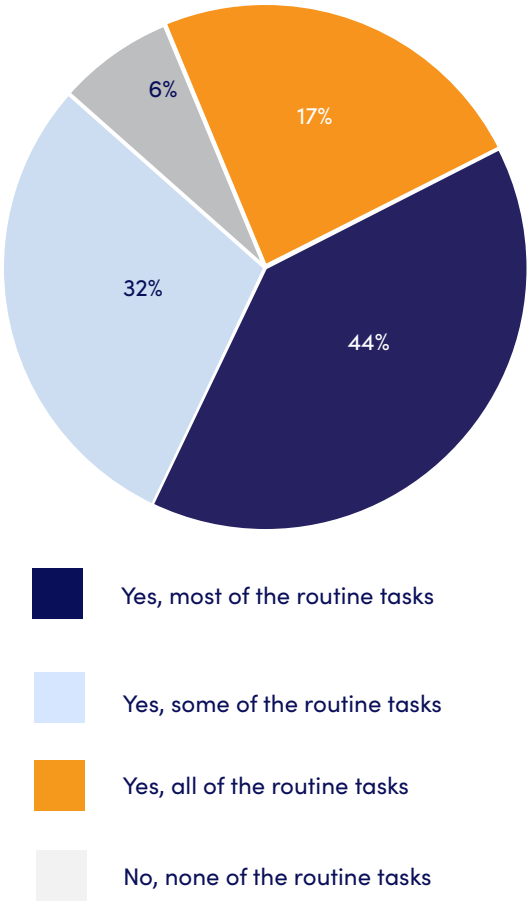
Automation

Automation could help by granting the right access levels to the right people at the right times, essentially taking the responsibility of secure access out of the hands of users. The majority of respondents (61%) said they believed automation could be a viable way to eliminate most of or all routine access and configuration tasks. Application development professionals are particularly optimistic: 72% said the same

What kind of tasks? For example, consider how long it takes for IT admins to manually configure account roles and responsibilities for every tool in the company.

Some centralized management tools include technical capabilities like auto-discovery to speed account set-up. Auto-discovery instantly pulls all current user identities, roles, and access rights from existing corporate directories, like Active Directory or an Identity Access Management (IAM) system, making upfront deployment faster. In the long run, these tools can automatically identify changes in user roles (including termination), the addition of new hosts to the IT estate, and even sunset inactive accounts based on time restrictions. The result is that IT admins would spend far less time on the minutiae of access configuration and routine management.

Do you believe that automation could remove the routine access or access configuration tasks from your day-to-day role in your organization?



Just-in-time access

Automation can also reduce the risk of human error – and therefore, the risk of data breaches – by eliminating situations where IT users must juggle needlessly complex routines that only open the door to mistakes.

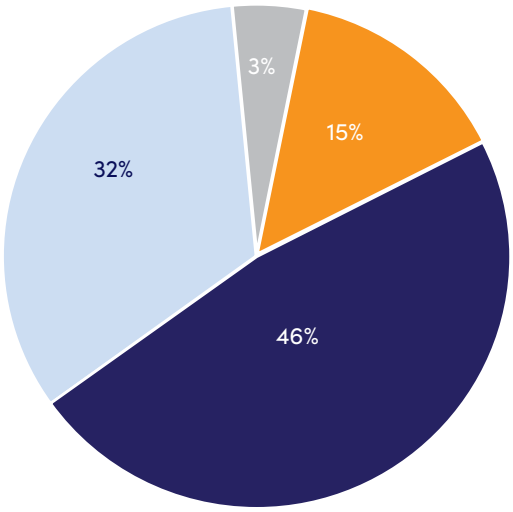
That's part of the reason why single sign-on (SSO) solutions have become more popular in recent years. According to our respondents, approximately 64% of their organization's access solutions support SSO, on average. These tools simplify the user experience by enabling them to automatically log in to all their required IT services with one click. In some cases, SSO can be enabled on any service that can be accessed via SSH, RDP or HTTPS connections. Fewer logins and fewer entry points means less chance for bad habits to take root.

Along the same lines, Gartner warns against the risk of standing privileges – or permanent access credentials that essentially have "always-on" access to an IT environment. These types of accounts often have unnecessarily high access privileges and therefore present a significant risk surface. Organizations would be well-served to investigate just-in-time access approaches and technologies, where access is granted only for the period in which it is needed.

Is artificial intelligence the future?

Looking ahead to the future, we also asked respondents for their perspective on the role of emerging technologies, such as artificial intelligence, in secure access management. For instance, AI could be programmed to replicate an organization's existing identity management group to produce role- specific access management rules. That would free up time for IT or security administrators who normally handle these tasks manually. Most respondents expressed a degree of trust in AI's ability to manage these tasks, so there is clear opportunity for companies to explore AI solutions that further reduce the manual burden of access management.

How trustworthy would you rate artificial intelligence (AI) in managing your access to critical resources and servers in your organization's network?



Conclusion

Organizations are clearly going to keep moving toward hybrid IT as they look to tap into its cost, agility and performance, and productivity benefits. That transition will stretch the boundaries of their IT infrastructure in more ways than one, and it could reveal policy shortcomings and risky user behaviors that are already making IT networks unsafe.

Decision makers are faced with an important choice: do they double-down on heavy-handed and restrictive IT security policies that impose strict limits on where, when and how their employees can work? Or, do they "go with the flow," instead crafting a security approach that reflects the inevitable realities of our changing workforce, and bring in solutions that allow employees to do their best work while staying safe?

The data shows that the first option just doesn't work – in fact, it introduces more security issues when restrictive access drives employees to seek workarounds. We believe the latter option is clearly the better approach, because it fits security into the day-to-day routines of workers – not the other way around.

Interestingly, the cloud just to happens to offer the best blueprint for the future of IT. Through the cloud, corporates can eliminate the need for users to install certain types of software, like document processing, file storage and sometimes even financial tools. Instead, users can trust the management and security of those tools to the experts.

Businesses need to embrace this way of thinking in security. Rather than forcing privileged IT users to manage credentials in accordance with a strict IT policy, why not just provide solutions that do all the heavy lifting for them, so they can focus on value-driving work?
These solutions should:

1. Provide consistent and coherent privileged access to on-prem and cloud environments, using roles to guarantee the right level of privilege for each session
2. Reduce errors and save time by connecting with existing AD/LDAP infrastructure.
3. Automatically link identities and their authorizations to roles for minimized
4. access configuration.
5. Provide SSO access for users to only their available servers.
6. Replace permanent credentials with just-in-time, temporary access to target hosts to reduce the threat surface.

Ultimately, we can reduce the capacity for human error by designing security solutions that put the user first, automate routines and reduce unnecessary complexity.

Finland

SSH Communication Security Oyj
Karvaamokuja 2 B 00380 Helsinki
www.ssh.com
+358 20 500 7000
info.fi@ssh.com

USA

SSH Communication Security, INC.
434 W 33rd Street, Suite 842
New York, NY, 10001, USA
www.ssh.com
+1 781 247 2100
info.fi@ssh.com

Hong Kong

SSH Communication Security LTD.
35/F Central Plaza, 18 Harbour Road
Wan Chai
Hong Kong
www.ssh.com
+852 2593 1182
info.fi@ssh.com