Research Brief

Putting Security Front and Center in the New World of Hybrid Work

Introduction

When the pandemic erupted in the spring of 2020, it didn't take long for government agencies to send people home to work remotely. Soon enough, it became business as usual.

A survey by the National Association of State CIOs (NASCIO) found that the shift to remote work had a largely positive impact. Despite some initial concerns about the ability of employees to be focused and productive while working at home, most employees thrived.

"Our IT staff can effectively work remotely, still deliver projects on time or ahead of schedule and be accountable for their work," one CIO told NASCIO.

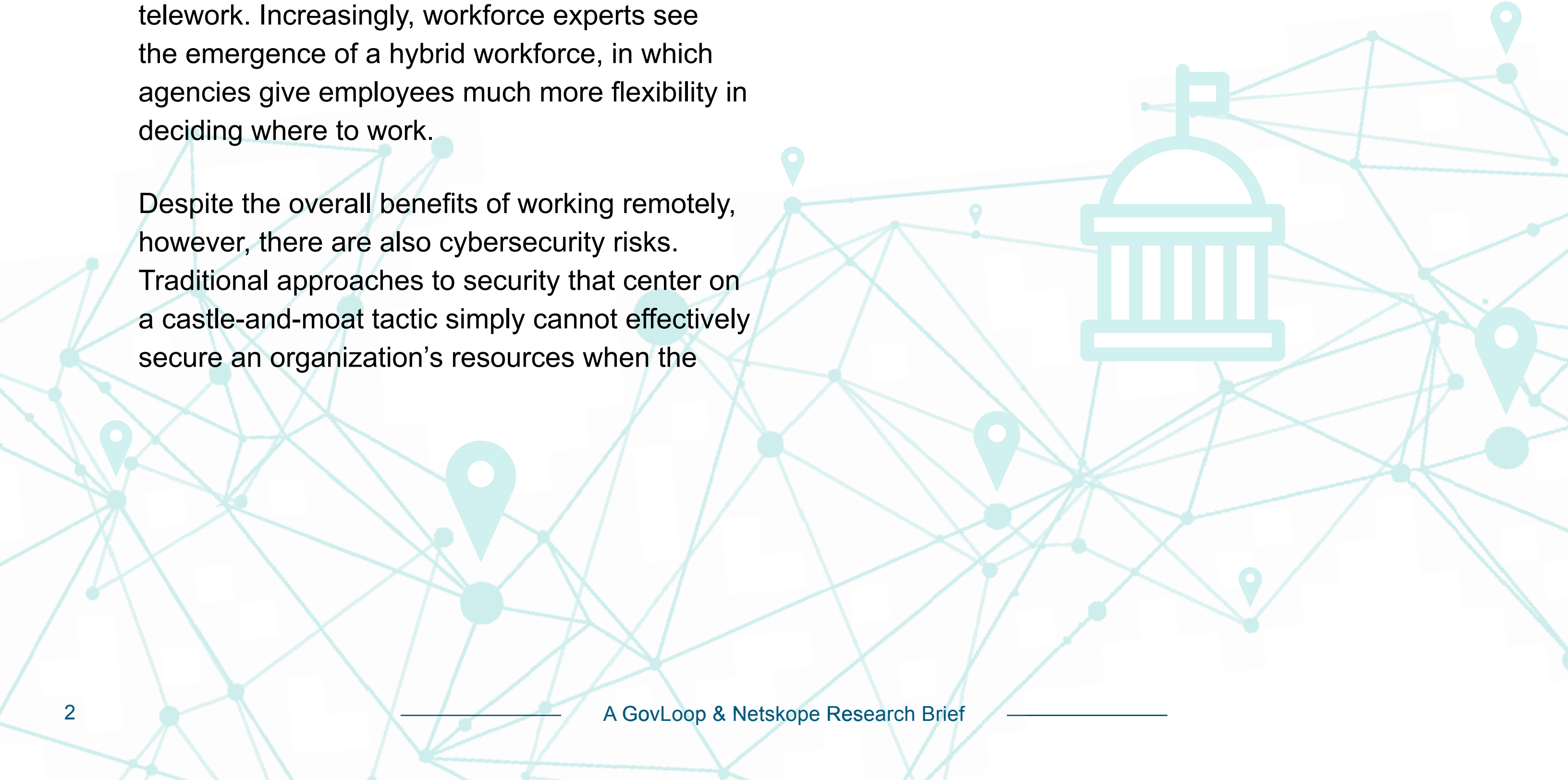
While many state and local agencies once resisted telework, that began to change even before the pandemic. In a 2021 survey, the Center for State and Local Government Excellence found that 53% of agencies now offer regular telework as a job perk for many positions.

That number is likely to climb now that more agencies have seen the intangible benefits of telework. Increasingly, workforce experts see the emergence of a hybrid workforce, in which agencies give employees much more flexibility in deciding where to work.

Despite the overall benefits of working remotely, however, there are also cybersecurity risks. Traditional approaches to security that center on a castle-and-moat tactic simply cannot effectively secure an organization's resources when the majority of the workforce is spread across disparate locations outside of the organization's moat, or traditional perimeter. Preparing for a future that includes more permanent telework means rethinking the way employees connect, shoring up security throughout the distributed environment, clamping down on unapproved applications, adopting a Zero Trust approach throughout the organization and generally employing a more data-centric and cloud-first approach to cybersecurity.

In spring 2021, GovLoop teamed with Netskope, the SASE leader that allows users to safely and quickly connect directly to the internet, any application and their infrastructure from any device, on or off the network.

We surveyed 230 federal, state and local government employees to better understand the security challenges facing their organizations in a work-from-anywhere world, and the initiatives these organizations are leading to secure their networks, systems and data.



Rethinking the Approach to Remote Work

Figure 1: How much of your organization's workforce is likely to work remotely some or all of the time after offices reopen?

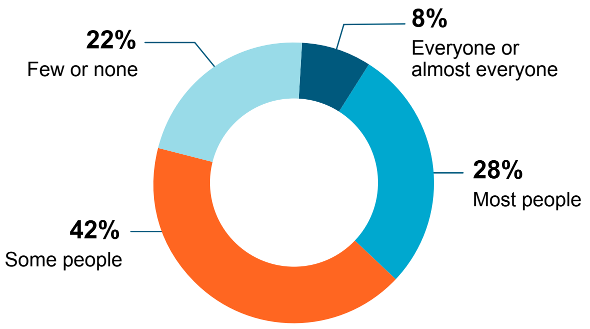
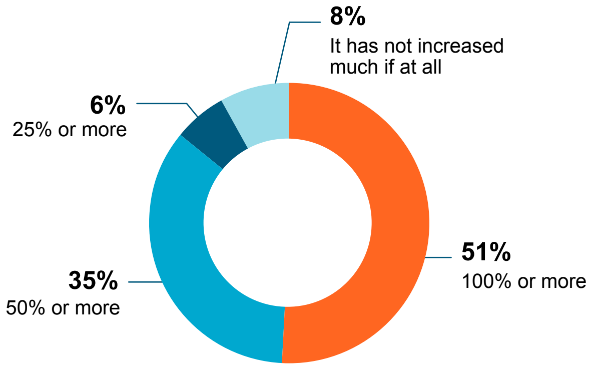


Figure 2: To what extent has your organization's use of virtual private networks (VPNs) increased during remote work?



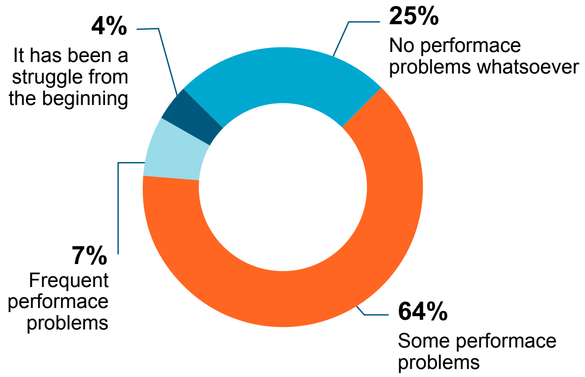
It shouldn't come as much of a surprise that so many employees like working from home. The time savings from eliminating commuting alone is invaluable, not to mention greater flexibility, and in many cases, higher productivity. It's so popular, in fact, that most survey respondents expect some or most people to continue working remotely, at least part of the time, for the foreseeable future (see Figure 1).

During the pandemic, agencies used what they had—typically, a virtual private network (VPN)—to provide secure connectivity to remote workers (see Figure 2). While a VPN can be used for remote access, by design a VPN is not intended to handle the volume of traffic generated by today's remote workforce. In fact, according to survey respondents, more than half experienced performance problems with their VPNs due to an increase in demand and usage by remote users (see Figure 3).

While a VPN can enable enough connectivity to complete a variety of tasks, it's not always the best means of ensuring work is done in a secure manner. Massive increases in traffic and usage can actually result in more security vulnerabilities, as users typically have unfettered access to the infrastructure.

Instead of struggling to retrofit a VPN to handle the uptick in usage and remote security issues, mature agencies are choosing to adopt a cloud-based connectivity approach. This allows agencies to provide secure resources to employees while enabling the same type of user and traffic control that was possible when traffic flowed through a VPN and firewall.

Figure 3: How has your organization's VPN handled the increase in remote workers?



An ideal solution starts with a cloud access security broker (CASB), a cloud-based solution that fully protects data and files shared between users from any location. Jason Ohs, a federal systems engineer at Netskope, recommends pairing the CASB with a cloud-based Zero Trust network access (ZTNA) solution and a cloud-enabled secure web gateway. Zero Trust assumes that no entity or access is trusted inside the network until it has been validated. The most effective Zero Trust architecture models follow the Department of Defense's Zero Trust Reference Architecture (NIST pub. 800-207) and the National Security Agency's Cybersecurity Information Sheet.

The ZTNA directly connects remote workers to agency applications running in public cloud environments or private data centers, while the secure web gateway protects cloud services, applications, websites and data regardless of the device, location or user by preventing malware, detecting advanced threats and filtering websites.

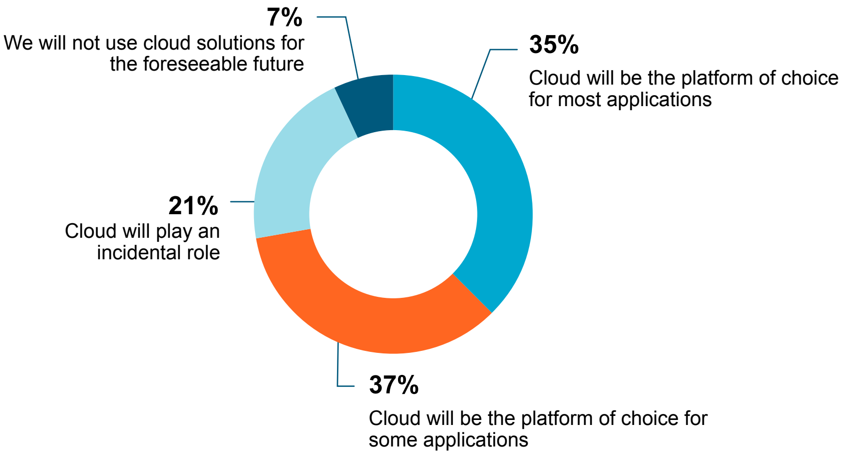
If giving up the VPN is just too painful, Ohs says it's fine to keep it around during the transition to Zero Trust.

"Move SaaS applications and web traffic off of the VPN, be selective of the application and web traffic at first to meet the risk posture of the organization—and look at policy around application instance and activity control," he said. "Don't move your Microsoft 365 agency instance off the VPN, instead move over the contractors' instance while limiting the ability for them to complete upload actions to limit risk while you are setting up data loss prevention (DLP) scanning and policy. Leverage remote browser isolation for web traffic on untrusted categories or new domains to minimize VPN usability issues while also making it easier to transition to TIC 3.0 and begin setup of Zero Trust for SaaS and web. The move will increase the performance, pushing less traffic over the saturated link as you make the transition to ZTNA."

Agencies can still allow users to go through the VPN as they're setting up the ZTNA, Ohs said. "The move to a Zero Trust model is a fundamental change and to do it correctly you need to look at things on a resource, application and data level. This takes time, so the best way to make the transition successful is to have a solution that allows flexibility and a path to positioning the agency for its cloud-based future securely," he said.

Cloud Security in the Remote Work Era

Figure 4: Which statement best describes the role of cloud in your organization's long-term digital transformation strategy?



Public sector organizations have made real progress in adopting cloud resources over the past several years, but nothing has sped up adoption as quickly as the events of the past 18 months. According to the survey, the vast majority of agencies rely more heavily on cloud solutions today, especially for remote work, than at any time in the past. And it's sticking; about three-quarters of respondents expect cloud to be the platform of choice for more applications going forward (see Figures 4 and 5). Other research backs this up, including a recent survey that found that 67% of government's hybrid cloud adoption has accelerated by a year or more due to the pandemic.

Figure 5: To what extent has your organization's use of cloud solutions increased during remote work?

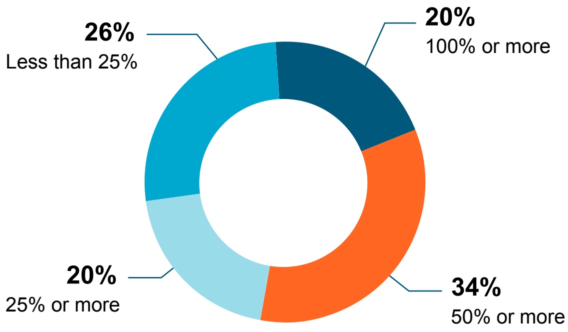
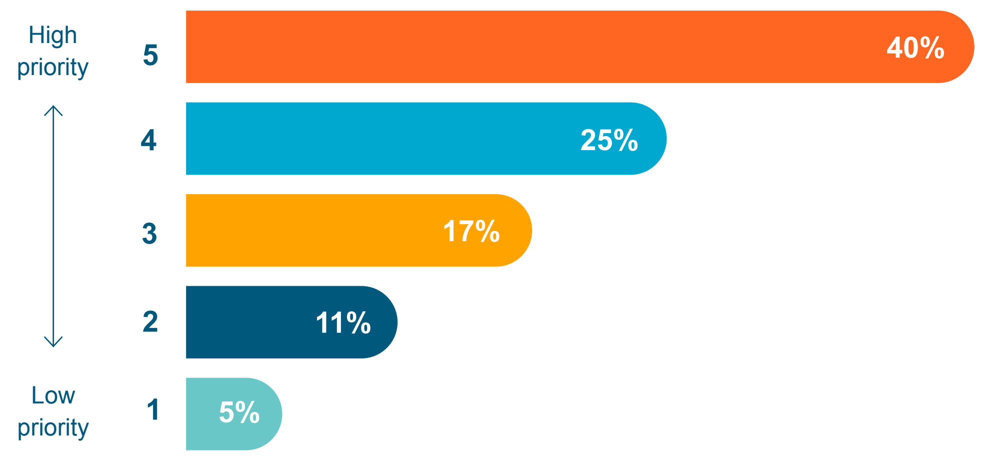


Figure 6: On a scale of 1 to 5, to what extent does your organization make cloud security a priority? 1 = Not a priority at all, 5 = A top priority



At the same time, less than half of survey respondents said their agencies have made cloud security a top priority—a surprising result, given the reality of the hybrid work scenario most agencies expect to adopt (see Figure 6). There are plenty of reasons why cloud security should be a top priority, including the possibility of data leakage, loss of visibility of user activity and maintaining compliance with regulatory requirements. Yet it *is* important, according to industry experts. Forrester Research, for example, notes a major shift in spending priorities from the public sector around both securing the cloud and delivering security in the cloud.

In some cases, cloud security may not be seen as a major concern because respondents expect cloud providers to take care of all security-related issues. Others may not realize that the resources they are accessing actually reside in the cloud. For example, Microsoft 365 is delivered as a cloud service, but many employees may not realize it.

Despite these misconceptions, cloud security is critical, especially in the era of hybrid remote work. That means finding ways to make the cloud a secure foundation for hybrid work environments.

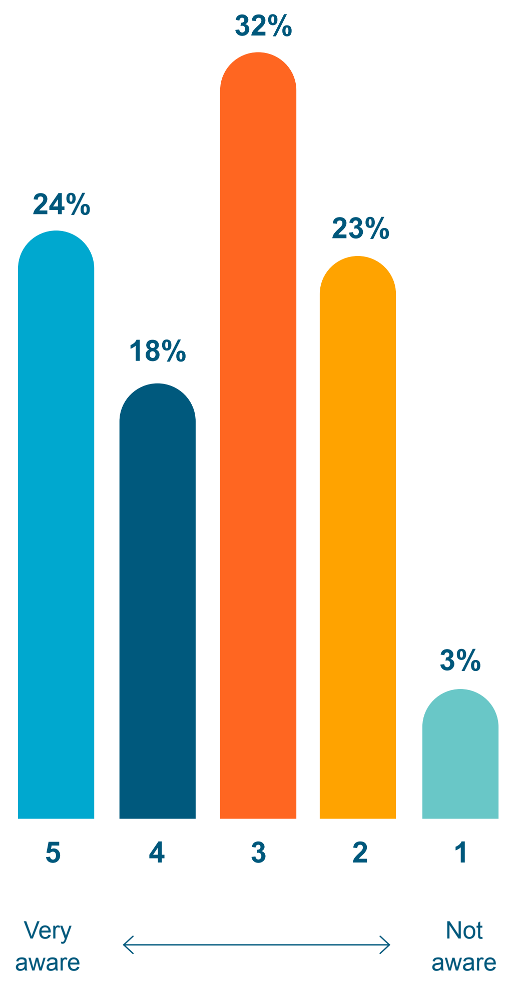
Identity is a major pillar of cloud security, and should be a first-line defense. “In many ways, identity is the new perimeter,” said Matt Clark, Netskope senior cloud security engineer. “When it comes to working from anywhere, agencies need to be able to identify users quickly and effectively.”

Visibility is another nonnegotiable. “If you can’t inspect the data, then you don’t know if it’s a weaponized document or if you have sensitive information leaving the agency,” Clark said. The ability to decrypt traffic for apps, cloud services and web at scale to gain the proper visibility into payloads, along with the visibility into what type of data is being used and shared, is critical.

Understanding the Risks

According to the survey, public sector managers and employees are all over the map when it comes to understanding the security risks associated with the cloud (see Figure 7), like shadow IT (see sidebar below). While about 42% of respondents said their co-workers and managers were aware or aware of the risks, about 26% were generally not aware and more than 32% fell in the middle. While that's understandable—it's complicated and ever-changing—understanding the risks is crucial. Here are three reasons why it's so complicated.

Figure 7: On a scale of 1 to 5, to what extent do you think your co-workers and managers understand the security risks associated with the cloud? 1 = Not aware at all, 5 = Very aware



1. Always-changing threats and techniques

There are more state-sponsored attacks than ever, and they are going after bigger and bigger targets. More advanced and targeted blackmail and extortion techniques continue to emerge, often using cloud enablement for delivery, along with more insidious social engineering techniques.

2. Human error

That includes misconfigurations and misdelivery, the use of nonsecure application programming interfaces and compliance violations.

3. Over-reliance on vendors

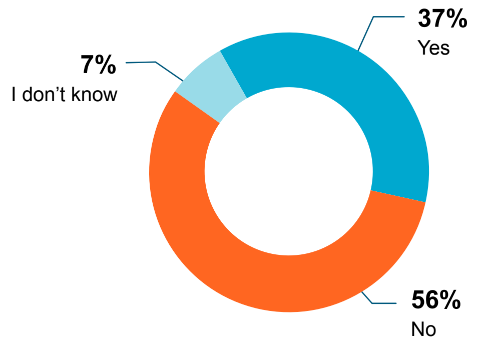
Many organizations make the mistake of relying on cloud vendors for everything related to security. Typically, vendors provide such capabilities as data classification, encryption and policy and access control. While these are the responsibility of the vendor, there are other important cybersecurity practices that are not. They include knowing where your data is, discovering and classifying content stored in cloud apps against sensitive data profiles, preventing sensitive data leakage, finding and controlling risky user behavior, controlling access by all user groups, implementing identity management and securing all users, whether on-premises, mobile or remote. This division of labor is commonly called the shared responsibility model.

The Dangers of Shadow IT

There may not be a large organization in existence that hasn't experienced the repercussions of shadow IT. Shadow IT—that is, hardware, software and services being used by employees without the approval of the IT department—can be a serious problem. Despite the dangers, more than half of respondents to the survey said their organizations don't have complete visibility into the use of shadow IT (see Figure 8).

One recent report found that 97% of cloud apps used by enterprises aren't managed by a centralized IT or security function. Instead, they were brought on and used by individuals within the organization, without approval. The same report also found 83% of users routinely used personal apps on managed devices.

Figure 8: Does your organization have complete visibility into the use of shadow IT —that is, commercial services (e.g., DropBox) that are being used without permission from the IT department?



> *"Whatever tools you use, make sure you can achieve very granular visibility into the use of shadow IT. It's also important to have comprehensive data loss prevention (DLP) coverage—and the more advanced the DLP capabilities, the better."*

– Matt Clark, Netskope senior cloud security engineer

Since it's difficult to determine when a shadow IT service may be involved, agencies should always encrypt sensitive data, which protects the data if it falls into the wrong hands, and decrypt the traffic to understand the types of data flows that are occurring.

Other critical capabilities include:

- Supporting real-time malware inspection on traffic entering and exiting cloud services
- Applying and enforcing adaptive policies based on content and context
- Layering policies with "allow" and "block" actions
- Discerning the difference between sanctioned versus unsanctioned (i.e., shadow IT) instances of the same application

Left unchecked, shadow IT can result in:

Loss of visibility and control, resulting in security vulnerabilities

The IT department can't monitor and control what it can't see. That means that software, hardware and other shadow IT may contain vulnerabilities that can't be addressed because they aren't known or identified. For example, if an employee emails data from a shadow IT application to someone outside the agency, that data immediately becomes public. Similarly, if an employee uses his or her own private instance of Microsoft 365 instead of the sanctioned version, data may inadvertently be shared between the two, introducing security vulnerabilities.

Noncompliance

Public sector organizations must comply with a host of standards and regulations, and go to great lengths to ensure that systems, software and other technologies meet those standards. It's relatively easy for shadow IT to evade detection and cause the entire agency to become noncompliant if the IT department lacks visibility and granular policy controls.

Additional cost

There are many potential expenses associated with shadow IT, including noncompliance fines, security remediation costs and operational costs due to underutilization of sanctioned applications.

Data loss

Data accessed or processed by unapproved software is more likely to be compromised or lost. Because shadow IT isn't connected to an agency's backup or storage systems, any outage is likely to result in permanently lost data. Data can also be permanently lost when an employee leaves the agency, but has been using personal accounts to store agency data.

Visibility is the key to preventing and managing shadow IT. That means implementing the right tools like CASB to discover cloud services and other shadow IT technologies.

The Data-centric Approach to Cybersecurity

Securing the networks, servers and applications that surround data is critical to overall security, but it's just as important to apply security to data itself. It's especially important in remote work environments, where there are so many ways it could be misused or exfiltrated, resulting in the disruption of IT services, network downtime, poor user experience, phishing attacks and much more (see Figures 9 and 10).

Figure 9: How concerned are agency leaders about the security of data and applications in the remote work environment?

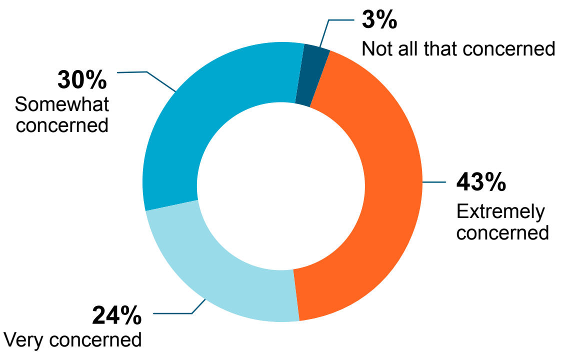


Figure 10: What do you see as the biggest network concern in a remote or hybrid environment? Check all that apply.

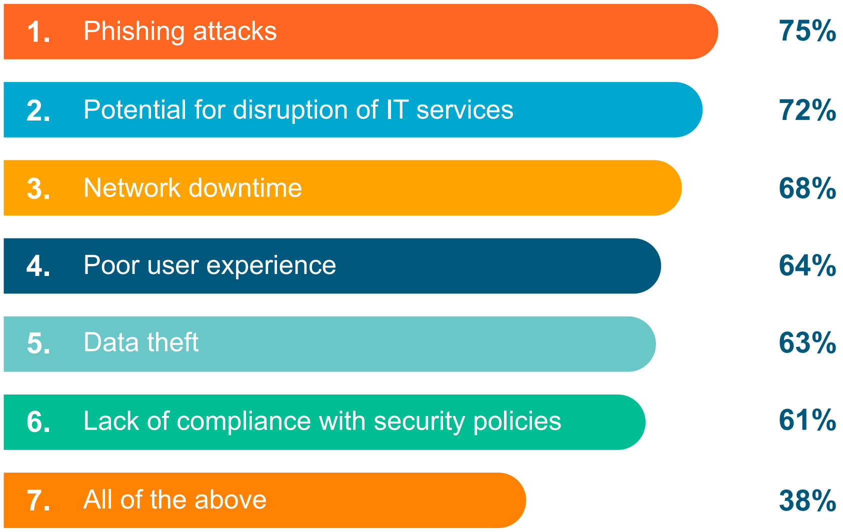
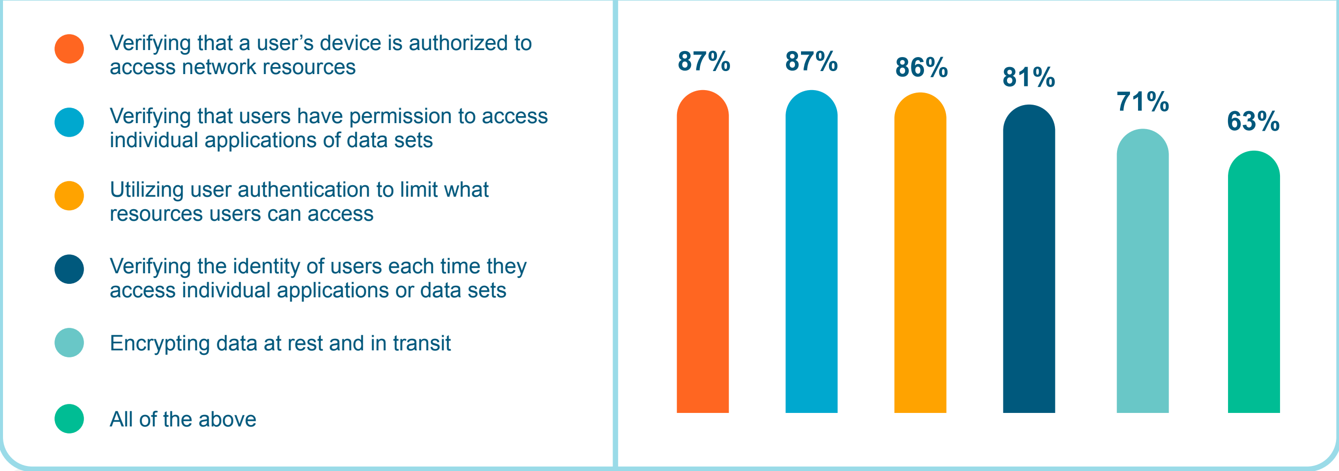


Figure 11: What security controls does your organization require? Check all that apply.



Creating a true data-centric approach to cybersecurity means improving agency visibility and control. That means securing data at the moment of creation, ensuring that all activity related to that data is logged and monitored, and protecting that data by thoughtfully creating policies around who can access it. Agencies have made good strides in achieving these goals, but truly keeping data safe at all times is an ongoing task (see Figure 11).

The tasks include:

☑ **Verify that a user's device is authorized to access network resources.** "What's to prevent me from using my device in a way that could compromise the data, or uploading a document that may be weaponized or downloading sensitive information?" said Clark. To avoid these situations, use technology to verify that the device has a certificate from a trusted certificate authority, verify full disk encryption at the endpoint and that policies are up to date and being enforced. If existing policies aren't doing the job, it's time to change them. For example, if it's an untrusted device, it makes sense to change the policy to allow users to access applications, but not download or upload data.

☑ **Implement user authentication to limit the resources users can access.**
Without authentication, users should be prohibited from accessing any agency resources. Agencies should strongly consider implementing multi-factor authentication (MFA) beyond user ID and password, to include more advanced methods of authentication, such as biometric identification, answering specific questions or using ID cards.

☑ **Verify that users have permission to access individual applications or data sets.**
By using access permissions and credentials to secure data, agencies can specify which users or groups are authorized to access specific data, and which actions they can perform on the data. Ideally, access control would integrate with some type of identity solution to truly understand who is accessing the data.

☑ **Verify the identity of users each time they access individual applications or data sets (i.e., Zero Trust).** It's not enough to authenticate users once; they must be verified each time they attempt to access or use data. For example, invoke step-up authentication with adaptive policies based on activity and data sensitivity. This is the Zero Trust approach to security.

The Netskope Advantage

Netskope's data-centric, cloud trust approach to Zero Trust safely enables direct-to-net communications while securing remote workers accessing managed and unmanaged apps, cloud services, websites and private applications in public clouds and data centers.

Netskope's FedRAMP-approved solutions include:

Netskope Private Access

Provides Zero Trust network access to private applications and data running in public cloud environments or private data centers. NPA allows organizations to retire legacy VPN hardware and move toward a more secure cloud-first remote access architecture.

Next Generation Secure Web Gateway

Prevents malware, detects advanced threats, filters websites by category, protects data and controls applications and cloud services for any user, location or device.

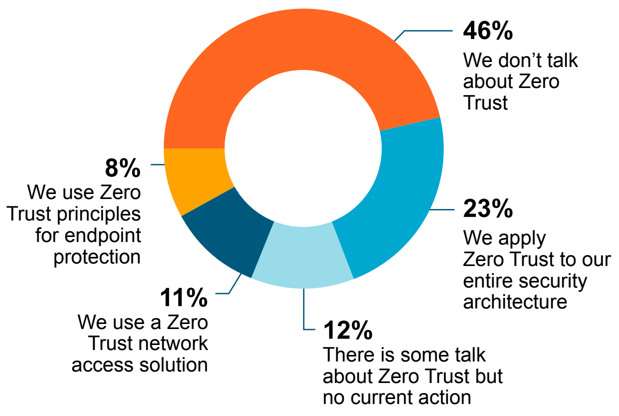
CASB

Allows organizations to quickly identify and manage cloud application usage and prevent sensitive data from being exfiltrated. Its patented Netskope Cloud XD technology eliminates blind spots to quickly target and control activities across thousands of apps and cloud services.

For more information, visit netskope.com/solutions/government.

The Future Is Zero Trust

Figure 12: Which statement best describes the role of Zero Trust security in your organization?



Implementing a Zero Trust approach is the best way to protect data, applications and other sensitive resources. With this approach, organizations do not trust users or devices attempting to access resources without verifying them, every time. Done right, it provides full visibility and control over both users and devices, preventing them from accessing untrusted applications, services and data. This can significantly reduce risks from both hackers and malicious insiders.

Despite the importance of Zero Trust, more than half of survey respondents say their agencies don't prioritize it, and less than 23% apply Zero Trust to their entire security architecture (see Figure 12).

"I don't think it's that public sector agencies don't want to implement Zero Trust. I think this is a state of transition for many agencies, and they are trying to figure out how to proceed," said Ohs. "It's not an easy transition; if you're looking at the perimeter as a fortress and a firewall as your gate, you have to change your processes to do Zero Trust by looking at identity as the perimeter. It's about rewriting the architecture along with the mindset."

Conclusion

Public sector employees like remote work and expect to continue it in some fashion, and cloud solutions are more popular than ever. But agencies don't have complete visibility into the use of shadow IT, VPNs are at their breaking point and agencies also lack the visibility and control they need to truly protect data, especially in remote work environments.

Agency adoption of cloud security best practices and solutions is critical to ensure business continuity and agency mission sustainment—and that the applications and services required for that sustainment are accessed and utilized in a secure manner. Also critical, as the Biden administration has made clear with the recent Executive Order, is the implementation of a Zero Trust architecture to provide security in today's largely distributed environment.

The survey shows that public sector agencies are on the right track. With the right knowledge and tools, agencies can make the necessary leap to a secure, remote future.

About Netskope

Netskope, the SASE leader, safely and quickly connects users directly to the internet, any application, and their infrastructure from any device, on or off the network. With CASB, SWG, and ZTNA built natively in a single platform, the Netskope Security Cloud provides the most granular context, via patented technology, to enable conditional access and user awareness while enforcing Zero Trust principles across data protection and threat prevention everywhere. Unlike others who force tradeoffs between security and networking, Netskope's global security private cloud provides full compute capabilities at the edge.

Netskope is fast everywhere, data-centric, and cloud-smart, all while enabling good digital citizenship and providing a lower total-cost-of-ownership.

To learn more, visit netskope.com/solutions/government.

About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

govloop.com | @govloop

1152 15th St. NW Suite 800
Washington, DC 20005
P (202) 407-7421 | F (202) 407-7501
www.govloop.com
@GovLoop