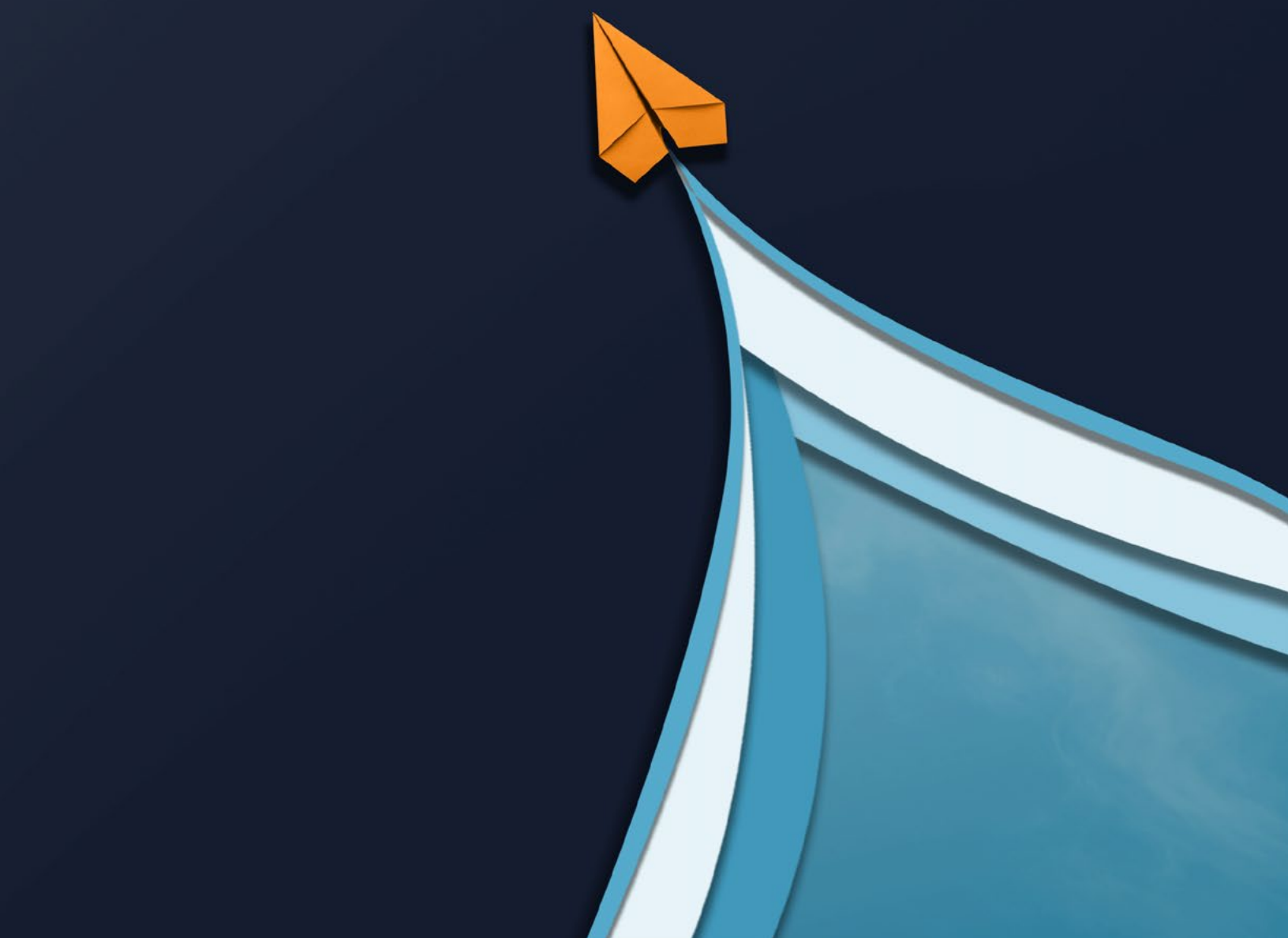
merlin

JUNE 2020

Secure remote access

WITH ZERO TRUST



How federal agencies can modernize, scale and support mass telework

EMBRACING A REMOTE WORKFORCE

We live in the digital age, where technology is entrenched into every aspect of life. This is perhaps most obvious in the world of work. Where, when, and how we perform our jobs is changing. The days when work resources were located behind a firewall, only accessible from an office computer, are long gone. A 2018 study found that 70 percent of professionals work from home one day a week and up to 53 percent work remotely at least half of the time.[1] That same year, 45 percent of federal government employees engaged in some form of situational telework.[2]

45 percent of federal government employees engaged in some form of situational telework in 2018

The COVID-19 pandemic has made the number of teleworkers skyrocket. According to a recent survey of federal employees and contractors, 98 percent are teleworking during the public health emergency.[3] Agencies throughout the federal government have moved quickly to ensure their systems can support this momentous surge in telework. For example, the Department of Defense—where just 15 percent of employees teleworked in 2018[4] —conducted a massive rollout of 900,000 user accounts in April for its new remote work environment.[5] But one of the long-lasting roadblocks to organizations permanently embracing telework is the belief that working away from the office lowers overall productivity.

This notion of lowered productivity, however, is incorrect. A two-year study performed on a control group of 500 employees by Stanford professor Nicholas Bloom found that telecommuters' productivity is boosted by the equivalent of a full workday.[6] Not surprisingly, the tech-savvy younger generation of American workers prefers the flexibility to work remotely and factor it into their evaluation of potential employers.[7] Assessments on productivity among federal workers during COVID-19 tell a similar story. Nine out of 10 workers say they are either

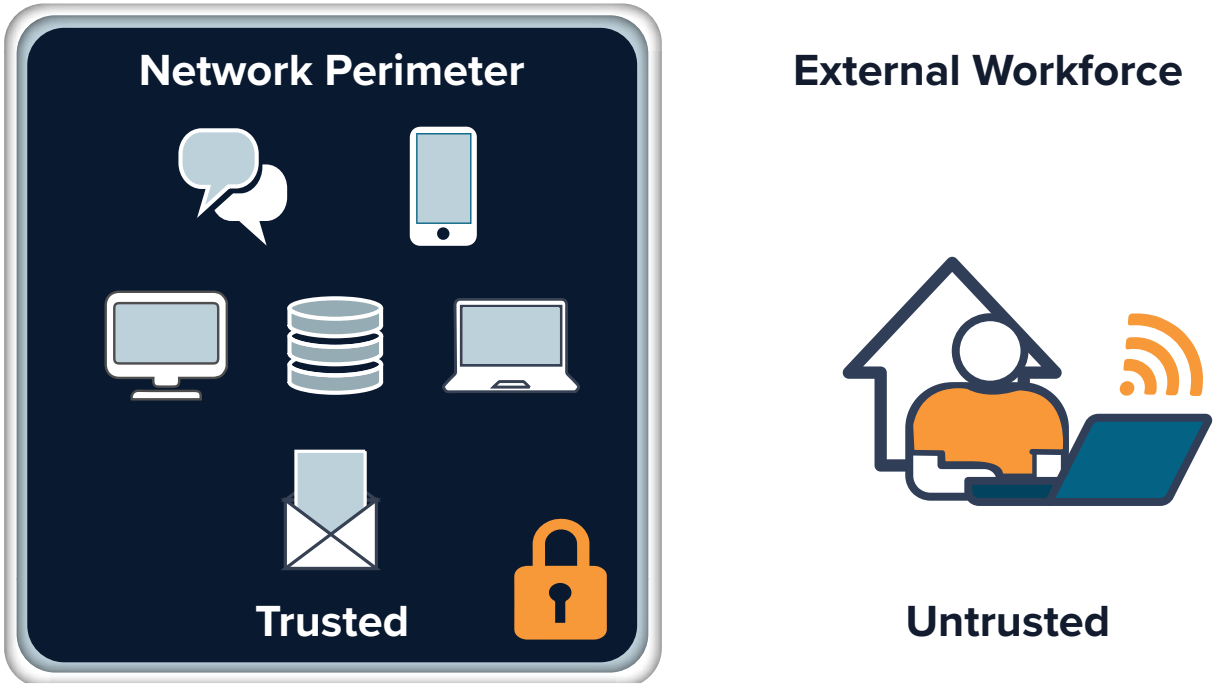
1 https://www.cnbc.com/2018/05/30/70-percent-of-people-globally-work-remotely-at-least-once-a-week-iwg-study.html
2 https://www.telework.gov/reports-studies/reports-to-congress/2019-report-to-congress.pdf
3 https://federalnewsnetwork.com/wp-content/uploads/2020/05/050120_FNNtelework_survey_results_FINAL.pdf
4 https://federalnewsnetwork.com/mike-causey-federal-report/2020/04/will-telework-ever-be-the-new-normal/
5 https://www.c4isrnet.com/it-networks/2020/04/16/how-dod-expanded-its-networks-to-beat-the-telework-spike/
6 https://www.inc.com/scott-mautz/a-2-year-stanford-study-shows-astonishing-productivity-boost-of-working-from-home.html
7 https://www.comptia.org/content/research/managing-the-multigenerational-workforce-2018

as productive or more productive working from home, with 52 percent of them saying they are more productive.[8] Also, the Office of Personnel Management (OPM) maintains telework.gov, a website dedicated to telework for the federal workforce. According to OPM's most recent annual report to Congress, 83 percent said telework improved their morale, 77 percent said telework helped them manage stress, and 68 percent said telework improved their health.[9]

Already expanding during the last decade, the adoption of telework has increased exponentially during COVID-19. This spike is challenging conventional remote access infrastructures and attracting more attacks on legacy remote access solutions like the Virtual Private Network (VPN).[10] The challenge is aligning and adapting to a heavily remote workforce while supporting current infrastructures, and of course, making it more secure.

FEDERAL TELEWORKER CHALLENGES

Federal agencies face unique challenges in delivering telework capabilities. Agencies are required to align with the Trusted Internet Connections (TIC) 2.0 architecture, released in 2012 and built upon the "trusted vs. untrusted" approach to security. To enable remote access, the approach brings teleworkers into the trusted perimeter, leveraging the TIC security stack to perform the required security checks. While this approach is sound for users within the trusted network, it does not scale well for teleworkers and cloud workloads.



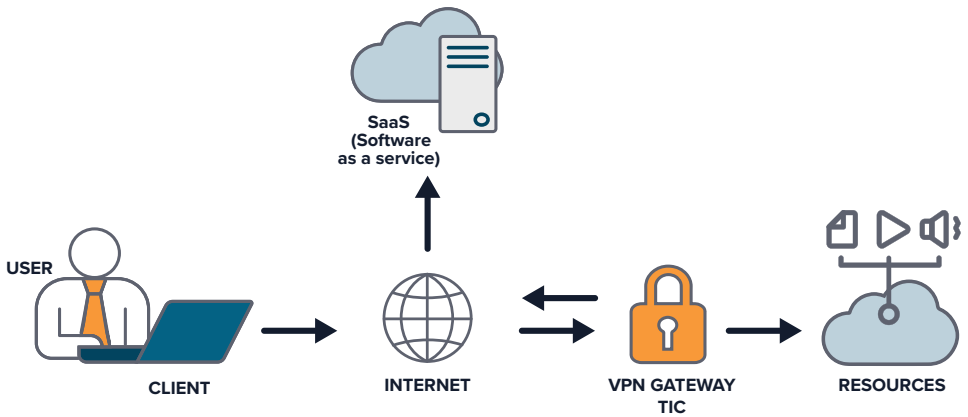
8 https://federalnewsnetwork.com/mike-causey-federal-report/2020/05/feds-are-enjoying-full-time-telework-but-doubt-agencies-will-embrace-it-later/
9 https://www.telework.gov/reports-studies/reports-to-congress/2018-report-to-congress.pdf
10 https://www.us-cert.gov/ncas/alerts/aa20-073a

Some of these remote access technologies, such as VPNs, bring usability and security issues. Support for tablets and cellphones can be limited or nonexistent for VPN access. From a security perspective, VPNs can struggle with:

- Ensuring the connecting client is safe from infections, lack of patching, etc. Especially if the user's device is not GFE (government furnished equipment).
- Verifying the user is who they claim to be.
- Establishing that the client's home or shared network is safe from potential threats that could leverage the client's computer for an attack.
- Protecting agency resources from a potential threat from the client, since VPNs provide network access instead of granular application access.

COVID-19 has highlighted the capacity and scalability issues of remote access as agencies deal with an unprecedented flood of remote users. The DoD asked workers to refrain from non-essential network usage (e.g., music streaming apps) while actively working to block media intensive websites like YouTube.[11] Other agencies worked to limit users accessing networks at the same time and limit the number of simultaneous connections to specific remote access solutions, like Citrix.[12] Exacerbating the issue, there was an inevitable surge in teleworkers accessing specific bandwidth-heavy resources for online meetings (Zoom, GoToMeeting, etc.).

Things become more complicated when accounting for cloud-based resources like software as a service (SaaS) offerings, which many agencies use. Due to TIC 2.0 requirements, all agency traffic must travel through the TIC. Thus, any remote users connecting to a SaaS application incur twice the bandwidth cost due to the hairpinning nature of traveling down an internet connection and then back out. Further, the user experiences unnecessary latency by traversing the TIC as opposed to going directly to the SaaS resource. Lastly, the security stack at the TIC is taxed watching traffic that, in the end, does not end up on the agency network.



11 https://federalnewsnetwork.com/defense-main/2020/03/as-pentagon-gears-up-for-more-teleworkers-its-networks-already-feeling-the-strain/
12 https://www.nextgov.com/cio-briefing/2020/03/mass-telework-causes-operational-strains-agencies/163851/

For example, an employee working remotely in Illinois may need to access a SaaS application hosted in Chicago, in their "backyard." That employee needs to connect to their VPN to the TIC in a data center in Ashburn, Va. Once that employee is connected, they will need to travel back to the SaaS application in Chicago, experiencing latency and at the mercy of any network issues affecting a large portion of the East Coast.

Last fall, the OMB released a memorandum regarding the impending TIC 3.0 that provides agencies a path forward to leverage cloud resources to avoid the hairpinning of TIC 2.0 when accessing cloud resources. One of the new use cases directly references remote users and access to all resources, both in the cloud and on-premises.[13] CISA released updated guidance, referencing the original memorandum, to address the surges occurring during COVID-19. This guidance highlights the need for a greater focus on authentication methods, as well as providing alternative paths to cloud resources, like leveraging a security as a service provider (SECaaS) to avoid hairpinning caused by TIC 2.0 requirements.[14]

SECURING A DISTRIBUTED WORKFORCE

As more workloads move to the cloud and teleworking is further embraced, or necessitated by external events, we need to reevaluate approaches that worked in the perimeter-secured environment. The idea of trusted vs. untrusted environments is gone, replaced by a focus on using zero trust architecture (ZTA), where everything is untrusted until proven otherwise. Government agencies need to account for workloads that are in data centers and distributed in multiple cloud locations. This means platform as a service (PaaS), infrastructure as a service (IaaS), software as a service (SaaS), or any of the other myriad of "as a service" offerings in this cloud-first age. Further, flexibility must be incorporated in the design to account for all the cloud vendors. The multi-cloud approach is becoming widely accepted, with a recent survey indicating that 87 percent of enterprises now use more than one provider.[15]

87% of enterprises use more than one cloud provider

As emphasized by the COVID-19 pandemic, the ability to provide surge capacity is critical during crises. For some solutions, this can require the need to purchase new licenses, procure new hardware, or increase bandwidth to the on-premises remote access solutions. Thus, leveraging cloud-based solutions that provide highly scalable, elastic architecture is a logical step in providing secure remote access.

13 https://www.govloop.com/pdf-viewer/?file=https://www.govloop.com/wp-content/uploads/2019/09/M-19-26.pdf
14 https://www.cisa.gov/sites/default/files/publications/CISA-TIC-TIC%203.0%20Interim%20Telework%20Guidance-2020.04.08.pdf
15 https://www.zdnet.com/article/multicloud-everything-you-need-to-know-about-the-biggest-trend-in-cloud-computing/

ZERO TRUST ARCHITECTURE (ZTA)

Zero trust is not an industry agreed-upon framework like those of the Center for Internet Security (CIS) or NIST, but that will soon change. NIST released the second draft of Special Publication 800-207 "Zero Trust Architecture"[16] in February and the final version is almost ready.[17] When the publication comes out, it will be the latest government step toward security based on zero trust principles. Since 2002, federal agencies have adapted to the Federal Information Security Modernization Act (FISMA), TIC, Federal Identity, Credential, and Access Management (FICAM), the Risk Management Framework (RMF), and the Continuous Diagnostics and Mitigation (CDM) program.

The goal of all these government initiatives is to restrict access to data and resources to authorized users. Technical limitations that existed when these programs came out meant mostly static security policies that were enforced at choke points like firewalls. Today, we can continuously assess requests and provide granular access using zero trust principles. Zero trust can be understood as a framework that incorporates other principles, like least privilege, and concepts like micro-network segmentation into a new approach to address security needs. Thus, it is essential to provide clarity around the definition of zero trust before discussing the proposed solutions.

Gartner defines zero trust network access (ZTNA) as an architecture which "creates an identity- and context-based, logical-access boundary around an application or set of applications. The applications are hidden from discovery, and access is restricted via a trusted broker to a set of named entities. The broker verifies the identity, context, and policy adherence of the specified participants before allowing access. This removes the application assets from public visibility and significantly reduces the surface area for attack."[18]

> "Ensure the right people are connecting to only what they need, as quickly and securely as possible, with the sustained objective of providing end-users with a seamless experience."

While this definition fully encompasses the concept of zero trust, it can be refined for secure remote access. The goal of secure remote access leveraging zero trust is to: Ensure the right people are connecting to only what they need, as quickly and securely as possible, with the sustained objective of providing end-users with a seamless experience.

16 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf
17 https://www.meritalk.com/articles/final-zero-trust-special-publication-coming-soon-nist-official-says/
18 https://www.gartner.com/en/documents/3912802/market-guide-for-zero-trust-network-accesss

IDENTITY AS THE PERIMETER

Remote users could be on any number of devices and working from anywhere in the world. Therefore, moving the perimeter from the firewall to the endpoint is an essential step in providing secure remote access. The challenge of doing this for security teams is accounting for the distributed nature of the applications:

- **Are they in multiple internal data centers?**
- **Are they located in another agency's data center?**
- **Are they distributed across multiple cloud applications?**

Security leaders also need to account for the possibility that some, if not all, of the applications may be accessed from differing devices, which may or may not support agents and may fall outside of the agency's IT purview. Finally, as workloads become more distributed, there must be consideration around the viability of requiring users to maintain multiple credentials.

Securing identity across all the distributed workloads can be accomplished by leveraging an identity and access management (IAM) solution that integrates with those workloads. Leveraging a cloud-native IAM solution, known as identity-as-a-service (IDaaS), allows agencies to verify users' identities before they gain access to their data, whether it be in a private data center or a cloud-based solution. Selecting the right IDaaS solution provides agencies the "glue" that binds all these distributed applications together in a secure method leveraging adaptive multi-factor authentication (MFA) and single sign-on (SSO).

Adaptive MFA provides contextual-based access, allowing agencies to increase security based on the context of each user's access. This approach allows IT teams to overlay logical security policies that only impact users when security may be affected. For example:

Limited MFA prompts when logging in from the office

More stringent MFA prompts while connecting from home, especially when accessing sensitive systems

Mid-session MFA prompts for logins from unexpected geographic locations

Getting rid of multiple accounts and password resets, SSO removes the need for users to keep multiple credentials. As studies have shown, complexity and rotation time of passwords increase the risk of passwords either being written down or forgotten, which require support desk intervention.[19] Thus, SSO increases worker productivity while increasing security and limiting unnecessary IT support.

19 https://www.techrepublic.com/article/the-end-of-passwords-industry-experts-explore-the-possibilities-and-challenges/

SECURING PRIVILEGED ACCOUNTS

Where securing the standard user is essential in a remote scenario, securing those workers with administrative-level access and requirements are critical. Recent market research indicates that 74 percent of breaches involve access to a privileged account, while 40 percent of organizations don't have an accurate inventory of the privileged accounts in their environment.[20] As the workforce becomes more distributed, it is imperative to protect privileged accounts with a privileged access management (PAM) solution.

Gartner advises four key pillars for employing a PAM solution:[21]

1. Track and secure
2. Govern and control
3. Record and audit
4. Operationalize

Simply put, privileged accounts must be secured similarly to PII: track who is using it, control how they are using it, provide an audit trail, and in turn, make the process integral moving forward. Lastly, implementing a forward-thinking PAM solution helps agencies add a significant piece in their ZTA.

SECURING THE WORKLOAD

After user identity is verified and secured, the focus can turn to securing the workload that the user needs access to. As stated earlier, routing all traffic to an on-premises location, only to hairpin it back to the cloud, is inefficient when accessing cloud workloads. Leveraging a SECaaS provider allows the security functionality to be performed in the cloud, directly connecting the user to on-premises or cloud resources. This approach also addresses some of the challenges around securing cloud resources. For example, when client traffic is routed through a SECaaS provider, agencies can deploy data loss prevention (DLP) technologies on the client's traffic or provide security to unmanaged devices accessing cloud resources.

A SECaaS provider can be leveraged to overcome some areas where older remote access systems have gaps, allowing for alignment with ZTA. For example, VPNs connect users to the network, not particular applications, while SECaaS providers can exercise least privilege—a core tenet of ZTA—to provide granular application access instead of full network access.

Limiting the number of systems a user's traffic must pass through and getting them to the required resource as quickly as possible, avoids unnecessary latency and failures along the path. The results are better user experience and enhanced security.

20 https://www.xtontech.com/blog/7-numbers-about-privileged-access-management/
21 https://www.gartner.com/en/documents/3899567/best-practices-for-privileged-access-management-through-

SECURING LEGACY SYSTEMS

Securing legacy systems is a challenge many agencies face. As much as 70-80 percent of federal agency dollars go to supporting legacy systems.[22] Some of the systems are more than 50 years old,[23] making them difficult or impossible to secure. Whether the systems are written in COBOL or running on no longer OEM-supported systems, IT support may be unwilling or unable to configure them to work with the latest security software for fear of impacting the functionality of critical legacy systems.

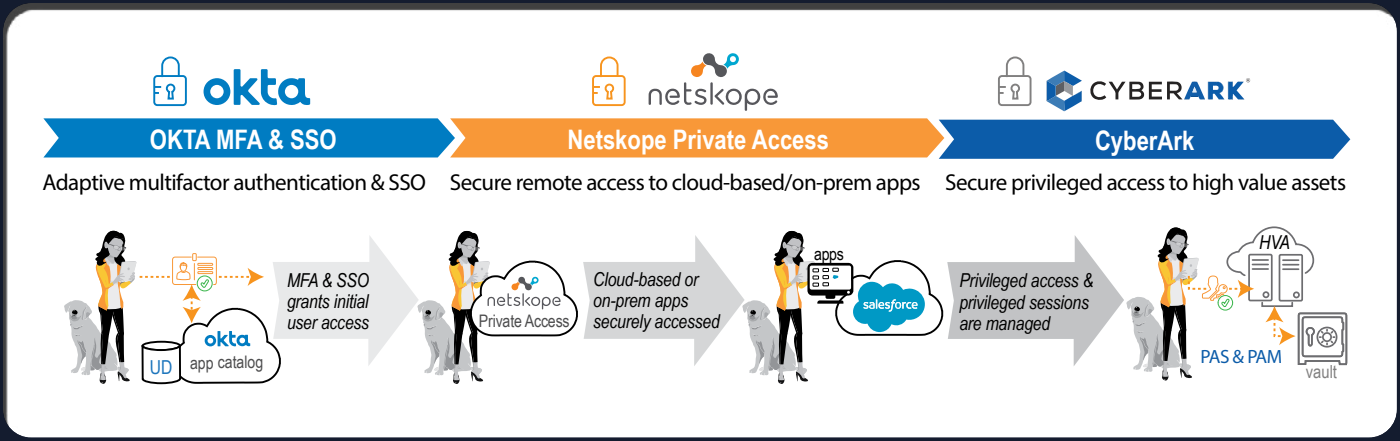
While there is a clear mandate[24] for agencies to modernize, waiting for modernization to occur before increasing security is not a reasonable approach. Agencies must address legacy systems as they move to a ZTA.

CLOUD-CENTRIC, SCALABLE SOLUTIONS

At Merlin, we work closely with customers every day to augment their remote access across both on-premises and cloud environments. Using our portfolio of technology partners, we deliver services that are compliant with industry regulations such as HIPAA, PCI DSS, and the government's Federal Risk and Authorization Management Program (FedRAMP).[25] We offer the following secure remote access solutions for federal agencies:

SECURE REMOTE ACCESS FOR PRIVILEGED ACCOUNTS

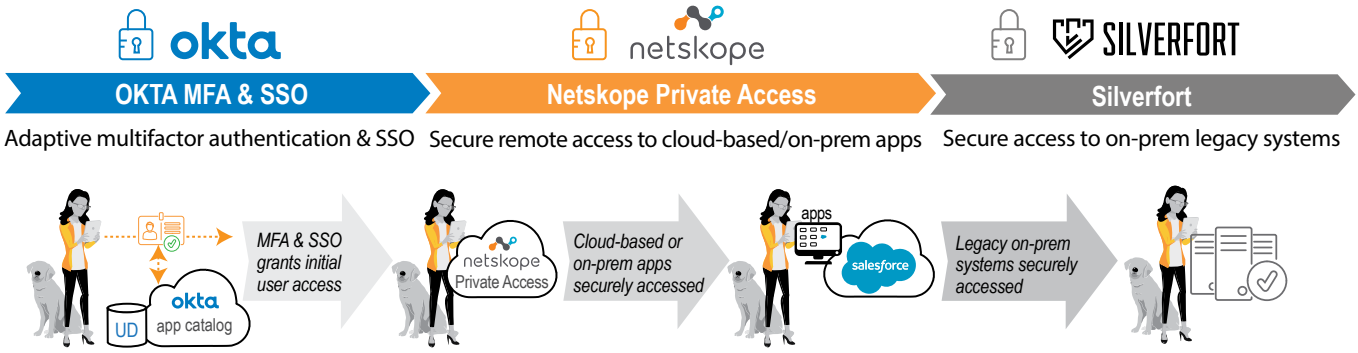
With Okta, Netksope Private Access (SECaaS), and CyberArk Privileged Access Security, agencies can provide secure remote access that leverages industry-leading IAM and SSO while providing increased security and the ability to audit users of privileged accounts.



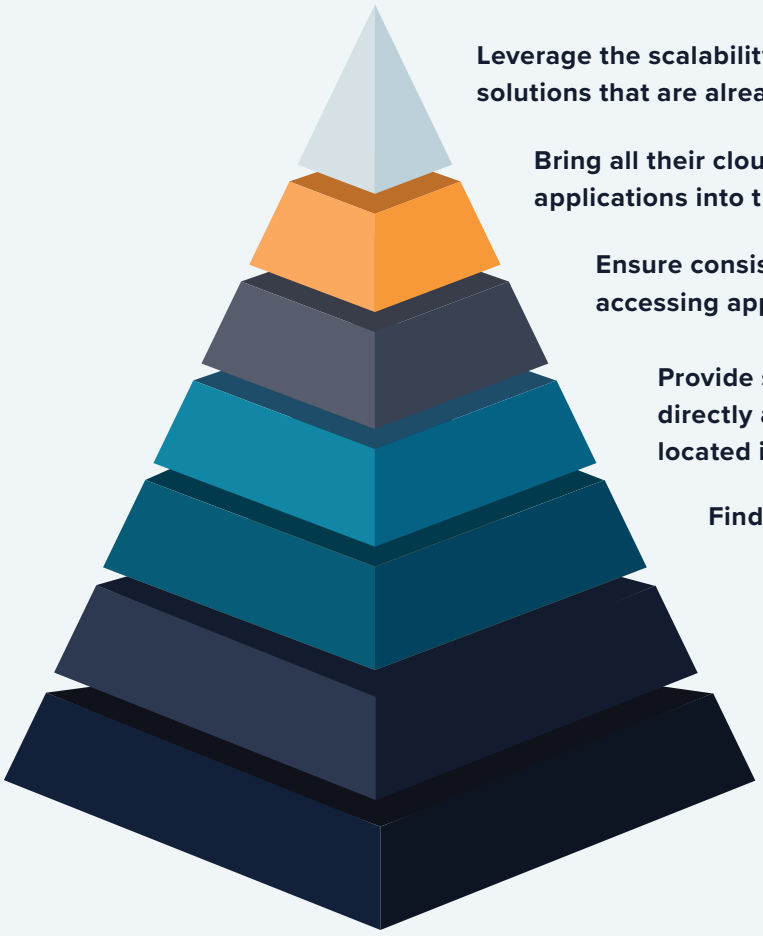
22 https://itmodernization.cio.gov/
23 https://www.fedramp.gov/about/
24 https://itmodernization.cio.gov/
25 https://www.fedramp.gov/about/

SECURE REMOTE ACCESS WITH ZERO TRUST

Agencies already on or starting the path to ZTA can leverage Okta, Netksope Private Access (SECaaS), and Silverfort to implement a secure remote workforce. Utilizing industry-leading IAM and SSO, these solutions enable zero trust by providing access to resources using least privilege and extending that security to legacy systems.



WITH THESE SOLUTIONS, FEDERAL AGENCIES CAN:



Leverage the scalability and elasticity of cloud solutions that are already FedRAMP approved

Bring all their cloud and on-premises applications into the IAM fold

Ensure consistent user experience whether accessing applications in the cloud or on-premises

Provide secure remote access to applications directly and with continuous monitoring, whether located in the cloud or on-premises

Find and secure access to privileged accounts

Provide audit capabilities for accounts that can cause the most harm

Extend zero trust to legacy systems

MERLIN SOLUTIONS

okta

Okta is an enterprise-grade identity management service, built from the ground up in the cloud and designed to address the challenges of a cloud, mobile, and interconnected business world. Okta integrates with existing directories and identity systems, as well as thousands of on-premises, cloud-based, and mobile applications, to enable IT to manage access anywhere, anytime, securely, and from any device.

netskope

Netskope Private Access provides zero trust network access to private applications and data in hybrid IT (public cloud and data center) environments. It is an integral capability of the Netskope Security Cloud and offers seamless connectivity for authenticated users, supports any application and protocol, reduces business risk, and simplifies IT infrastructure.

CYBERARK

CyberArk PAS can continuously scan the environment to detect privileged access and store privileged accounts in a secure vault. It can also automatically record and store privileged sessions within a centralized encrypted repository, allowing for auditing recorded and active sessions. CyberArk can proactively detect and alert SOC and IT teams of anomalous behavior that bypasses or circumvents privileged controls.

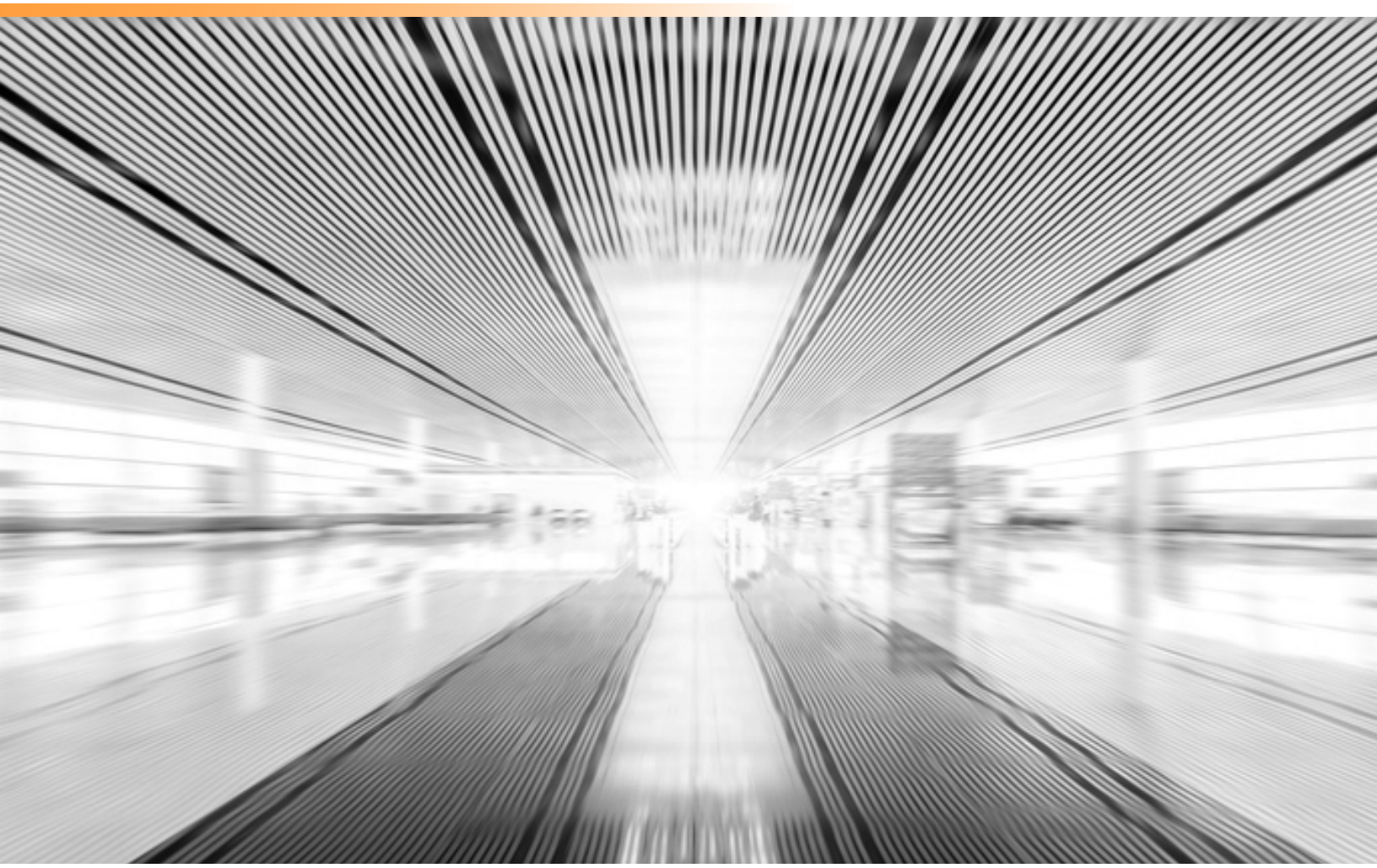
SILVERFORT

Silverfort enables adaptive multi-factor authentication (MFA), risk-based authentication (RBA), and zero trust policies across all sensitive corporate and cloud assets, including systems that could not be protected until today – without requiring any agents, proxies, or code changes.

CONCLUSION

During this era of digital transformation, workforces will continue to become more and more distributed. All the while, data, and applications are being spread across different cloud systems and on-premises locations. Federal agencies need secure remote access solutions that logically route end-users to the correct location while extending their security perimeter to wherever that user is. Using an integrated solution, leveraging IDaaS and SECaaS, agencies can take a significant step in securing their remote workers.

Moving the perimeter to the endpoint, using MFA, implementing least privilege for resource access, securing privileged accounts, and extending security to legacy systems provides federal agencies with increased security that is aligned with zero trust. By incorporating industry-leading solutions, agencies will position their best protection where the need is greatest: on the user and the data they require. Whether it is today or a few years from now, federal agencies can implement these technologies to more effectively provide secure remote access that ensures continuity of operations and a frictionless user experience.



ABOUT MERLIN

Merlin is the premier cybersecurity platform with a one-of-a-kind business model that leverages security technologies, trusted relationships, and capital to develop and deliver groundbreaking security solutions that help the federal government minimize security risk and simplify IT operations. In addition to selectively representing reputable cybersecurity brands, Merlin invests in visionary, emerging technologies and brings everything together into its lab where cybersecurity engineers integrate, test, and deliver innovative security solutions. With these integrated solutions, Merlin helps federal civilian and defense customers save time, money, and other resources while empowering them to more simply and effectively secure their systems, data, and users no matter how the network, security threats, and regulatory compliance requirements evolve.

Learn more at merlincyber.com.

AUTHORS

R. Casey Turner
is a Cybersecurity Solutions Architect at Merlin. He provides technical leadership in security solutions development and helps formulate scalable and adaptable solutions that meet business and compliance requirements.

Arin Karimian
is Merlin's Director of Content.