Making It Safe for Federal Employees to Work Remotely

Security Tips for Enabling Teams to Work Outside the Office

Table of Contents

Security Risks to Watch for When People Work Remotely

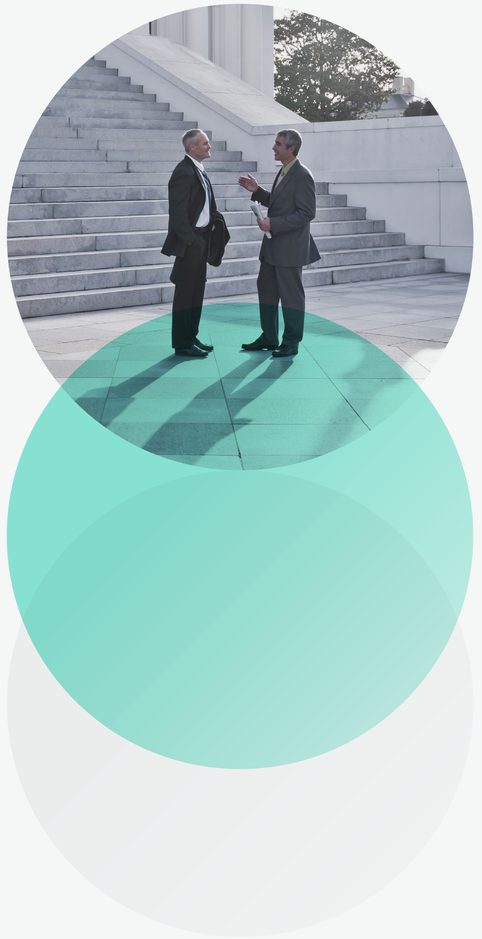
Given the current global climate, it's likely that your workforce has seen a huge increase in employees working from home. In 2018, only 22% of federal employees teleworked at some point, despite 42% of the workforce being eligible. But in 2020, the Office of Management and Budget released guidance recommending agencies implement "maximum" telework flexibility where possible, and OMB is urging agencies to extend telework.* While you may have some security in place to accommodate this sudden shift, it's tough to be fully prepared.

* Meritalk. "CDM The Next Chapter", 2020 https://www.telework.gov/reports-studies/reports-to-congress/2019-report-to-congress.pdf

Security Risks to Watch for When People Work Remotely

Having people work remotely changes many things. Assumptions about how your people get to apps in the cloud or on-site—and how you protect them—often can be turned inside out. You can use Forcepoint solutions to help your enterprise stay safe and your people remain productive as they:

- Work from any location without fear of data compromise or data loss
- Use work-related email, including clicking on links
- Access websites and content from home or public Wi-Fi networks
- Log in to and store data in your cloud-based apps
- Connect back into your enterprise network for internal apps and data



You've probably already begun adopting cloud-based applications and allowing some people to work from the road or at home. But processes that worked for a small number of people may not function well at scale. This ebook is designed to offer solutions for those looking to extend protections as increased numbers of employees work from home or other off-site locations.

Our mission at Forcepoint is to help foster safe and trusting environments to protect employees and critical data everywhere. Here are a few quick tips to enable your people to work efficiently and securely outside the office.

Extending Remote Access to Mission-critical Resources

Agencies today face the immediate challenge of enabling secure, remote access to mission-critical resources. Trusted Thin Client Remote (TTC-R) provides a simple solution to this challenge, allowing secure access to an agency's data center from laptops and hybrid devices.

Access to Mission-critical Resources from Ruggedized, Tactical Deployments to Agents in the Field and Teleworkers

Many agencies must now extend access to mission-critical resources to teleworkers. This is where a solution like Trusted Thin Client Remote (TTC-R) can help—by solving the challenge of connecting employees to work from any location without fear of data compromise or data loss . This requires a solution that saves all work products at an appropriately networked agency's data center, not on endpoint devices.

Forcepoint TTC-R is a secure multi-network access solution that solves the difficult problem of satisfying security needs while enhancing user productivity. It works regardless of the user's physical location—securing people in ruggedized, tactical deployments to agents in the field and teleworkers. TTC-R is the same client software that is designed to satisfy information assurance accreditation community requirements, eliminate potential leaks and risks, and provide users with a familiar Windows® desktop environment. Trusted Thin Client is a "Raise the Bar" (RTB) solution that is included on the United States National Cross Domain Strategy Management Office (NCDSMO) Baseline list.

Forcepoint secure information-sharing solutions have a proven track record of proactively preventing government and commercial organizations from being compromised, while fostering the secure access and transfer of information. TTC is designed to meet or exceed extensive and rigorous security Assessment & Authorization (A&A) testing for simultaneous connections to various networks at different security levels.

Enhancing Your Email Phishing Protection Outside the Office

Like many agencies, you likely already have email security in place that has been configured to provide remote access to email from mobile or managed devices.

Enhancing Your Email Phishing Protection Outside the Office

As the number of people who work remotely increases, you may want to double-check that you're protecting email going in both directions:

- → **Inbound** – Messages and attachments sent to your users should be inspected for phishing, ransomware, malware, spam, and other undesirable content.
- → **Outbound** – Messages and attachments that your users send should be scanned to make sure that sensitive data, intellectual property, and other business information is not being transmitted inappropriately (this is often referred to as Data Loss Prevention or DLP). You should also be inspecting outbound traffic for malware to ensure your employees aren't infecting your customers.

If you're using Forcepoint Email Security and already provide remote access to email, simply make sure that the mail transfer agent you've connected to email has enough network capacity between the agent and the internet to support an increase in remote traffic.

Phishing messages which entice users to click on seemingly benign links on the web continue to be the leading source of attacks. While most email security systems will flag or block links to websites that are known to be bad, previously unseen sites may not be blocked. Workers who are no longer in the office need web security that protects them no matter where they are.

Safeguarding People as They Browse and Use the Web Differently

Your employees are working differently, and these differences open more possibilities for security risk as the threat landscape evolves. Additionally, you must account for the merging of work and home life and how that impacts a person's day-to-day web activities.

Two things to consider:

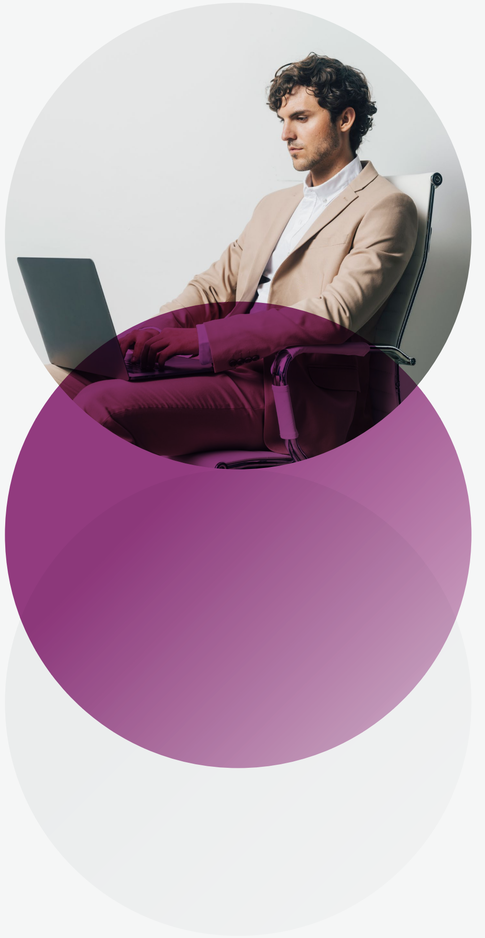
- → How protected are employees working off the agency network? How protected is your agency and its data?
- → How will you deal with increased web usage, including personal browsing?

Safeguarding People as They Browse and Use the Web Differently

Your agency likely went from working in the office to working from home. Unfortunately, traditional on-premises solutions, like an appliance-based secure web gateway, only protect users when they're on network. While going to the cloud has been a concern for some, particularly amidst rapid SaaS adoption (of both sanctioned and unsanctioned cloud apps), the reality is that the cloud is more friend than foe—now more than ever. This is especially true with securing web usage. Your network must provide users the same level of protection at home as they would have in the office.

Forcepoint's cloud-based Web Security enables your new or existing work-from-home workforce to safely access web content, adapting to how your people work beyond just the cloud applications they access. At a time when going to the office isn't an option, sending your children to school isn't an option, and attending in-person appointments, meetings, and gatherings—work-related and personal alike—isn't an option, what do you do? Increased web usage is guaranteed as your now-remote employees stay connected by reading the news, checking LinkedIn, and using the web to continue their everyday lives. So, between work-related web usage and personal browsing, protecting your agency from web-borne threats is key.

Forcepoint's cloud-based Web Security ensures that users are protected, no matter where they are working from. Access to the web will always be needed, and maintaining productivity while balancing safe access and powerful yet flexible protection is the key to securing your people and your data.



Ensuring Data Security in a Multi-cloud Environment

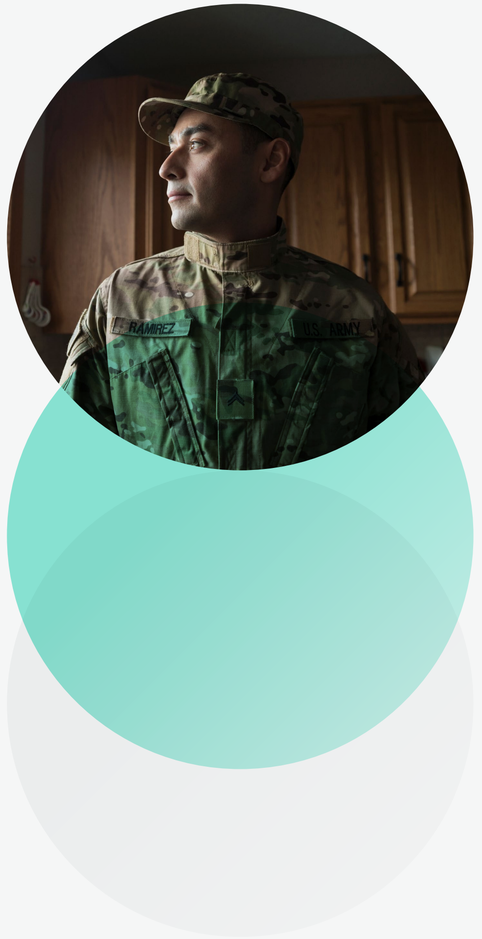
Cloud security is most often a shared responsibility: The cloud provider sees to its own infrastructure security, leaving agencies to secure their data and user activities on top of that infrastructure.

This means your agency is responsible for elements such as user behavior, access, data policies, usage policies, and compliance. This remains true for both managed and unmanaged devices in a remote working model.

Ensuring Data Security in a Multi-cloud Environment

Every agency has certain tools in place to protect critical data and intellectual property. If you've implemented Forcepoint DLP, your first step to optimize for remote work is to start examining policies. Start with critical back-office data that you may have had to move to the cloud rapidly—are you ensuring access is restricted to only critical users during this time? Leverage predefined policies for this type of data, and tune them. For highly sensitive information, you have the option to implement data fingerprinting and enable policies that can control this data wherever it goes, as well as implement restrictive policies based on movement.

Next, you may want to examine implementing data leakage policies, which can detect and prevent low and slow data movement and ensure security, especially for regulated or personal data. In parallel, ensure your policies enable reporting of data from endpoint to cloud, in order to maintain compliance during this time.



Ensuring Data Security in a Multi-cloud Environment

Many agencies will decide this is a time to start expanding more specific data controls for cloud applications that haven't traditionally been enabled. This is where a solution like Forcepoint CASB can help by providing visibility and control to sanctioned and unsanctioned cloud applications and managed and unmanaged devices. And, as any security team would agree, you need more than network perimeter defenses and endpoint protection.

Forcepoint focuses on the common denominator across every scenario: the human user. Forcepoint CASB provides insight into usage patterns and device profiles, enforces policies proactively, and exercises account protections across managed and unmanaged endpoints. This is key to identifying and responding to abnormal activity to protect both your users and data in the cloud. Forcepoint data protection makes it easy to then fortify your data security posture—unifing your data policies across all channels (Endpoint, Network, and Cloud) from a single console of control.

Lastly, you may need to examine an expansion of your overall picture of data protection, and where it's deployed in your agency. Whether you are pushing out endpoint control remotely to a larger pool of users, preventing data breaches with proactive risk-adaptive data policies, or expanding visibility and control into cloud application access or data movement, Forcepoint can help you create a plan and/or provide the services you need to keep data secure—no matter where your people and your data are located.

Connecting Remote Workers to Internal Apps and Data

While many of the applications and data your people need are likely in the cloud already, there might be some that are only available from inside your agency network. Your remote workers will typically use a virtual private network (VPN) to securely connect their devices, in through your firewalls.

Connecting Remote Workers to Internal Apps and Data

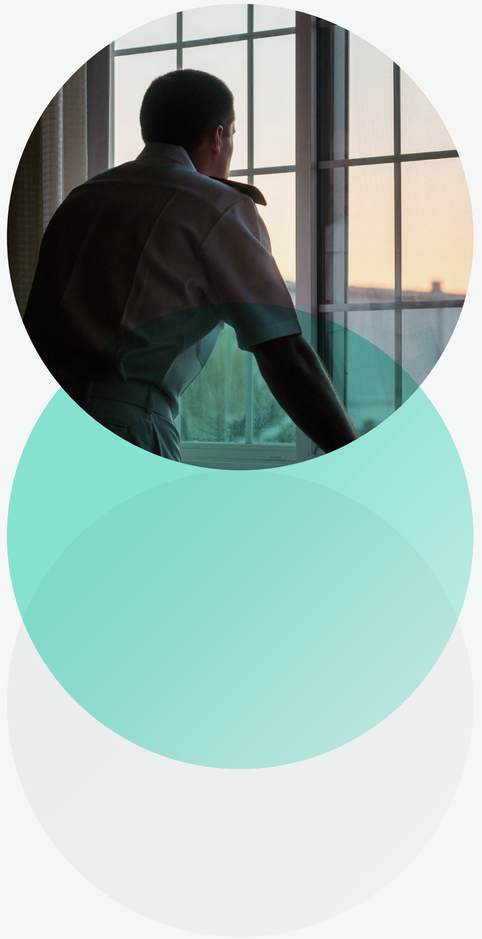
Full VPN capabilities come built into Forcepoint NGFW

If you need to provide VPN access to users who haven't previously worked remotely, or you're experiencing problems with your existing VPN solution, all Forcepoint NGFWs come with full VPN capabilities built in; there are no additional licenses to buy. You can give your users safe, easy connectivity to internal web apps through their browser with our SSL VPN portal—no special endpoint client software required.

Or, for admins who need full network access, our VPN client software for Windows and macOS can be downloaded from support.forcepoint.com. These VPN clients are easy to set up and connect to your Forcepoint NGFW.

Protecting app workloads you move into the cloud

If you're moving data from internal systems to workloads in public cloud environments like Microsoft Azure Government Cloud or Amazon Web Services (AWS GovCloud), virtual software versions of Forcepoint NGFW can prevent unauthorized access from other parts of the internet. These vNGFW virtual appliances, available in the Microsoft and Amazon public cloud marketplaces, are managed from your Forcepoint Security Management Center (SMC) the same way as your physical appliances—even using the same policies, reports, and dashboards.



Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

Learn more about Cloud Security at forcepoint.com/cloud-security

[Making-It-Safe-for-Federal-Employees-to-Work-Remotely-Ebook-EN] 14MAY2020]