MENLO SECURITY

A winning remote work game plan

Keep remote employees productive and free from malware

Use Case

Modern enterprises need modern approaches to workforce security

Now that work is returning to a post-pandemic normal, it's time to sit up, look around, and ask yourself: where is everyone?

Many of your coworkers are at home, where they will continue to work permanently. Others will shuttle back and forth between home and office in a hybrid work pattern. When every agency's workforce was scattered in response to COVID-19, most acted quickly to stand up a remote work environment built on VPNs, firewalls, and CAC readers.

Moving forward, with President Biden's Zero Trust cybersecurity mandate[1] in mind, you need to come up with a comprehensive game plan to protect your agency's data while giving remote workers seamless access to the data they require to do their jobs.

Identifying the risks of remote and hybrid access

First, take stock of what you're up against:

1. **Remote dangers.** Personal devices and home networks are highly vulnerable. Some agencies allow BYOD, but who knows for sure what's on those personal smartphones? A trip to the neighborhood coffee shop and its unsecured Wi-Fi network could expose data, including user passwords, to the public. Common web browsing patterns could play into the hands of a host of threats: malware, phishing, ransomware, advanced persistent threats (APTs), zero-days, or drive-by downloads.

2. **Encrypted threats.** Although 90% of websites[2] use the HTTPS protocol to encrypt web traffic, what happens when the threats themselves are encrypted? Because many security tools cannot monitor SSL transmissions, encrypted threats pass right through, along with legitimate traffic. As a result, user devices can be compromised while agency security teams are left in the dark.

1. The White House. "Executive Order on Improving the Nation's Cybersecurity"

2. Google. "HTTPS encryption on the web – Google Transparency Report"

3. Kim Komando. "Half a million VPN passwords leaked - Is your info compromised?"

4. CISA. "Trusted Internet Connections 3.0Remote User Use Case"

3. **VPNs and TICs.** Although VPNs are widely relied on for secure connectivity, the fact is, some VPNs have been compromised.[3] Trusted Internet Connections (TICs), meanwhile, are mandated for many agency communications. While the Cybersecurity and Infrastructure Security Agency's (CISA) TIC 3.0 guidance[4] incorporates protocols for remote work, both VPNs and TICs create latency that slows network response for remote users. While a performance drop-off might not have been a top concern when sporadic, ad hoc remote work was the rule, in a permanently restructured remote or hybrid workforce, lost minutes due to latency will be multiplied many times over, eroding the productivity of your agency. That's unacceptable.

4. **Staff pressure.** When the pandemic caused offices to shut down in 2020, security teams scrambled to support the surge in the remote workforce, taking on a time commitment that is unsustainable over the long haul. The shift to remote work also resulted in a huge increase in phishing and ransomware attacks. Not only does this attack surge vastly increase the need for better security, it also overloads security teams, who face an escalating number of alerts. Since it's unlikely you'll be getting an influx of network and security staffers in the near term, you will need to do more with less.

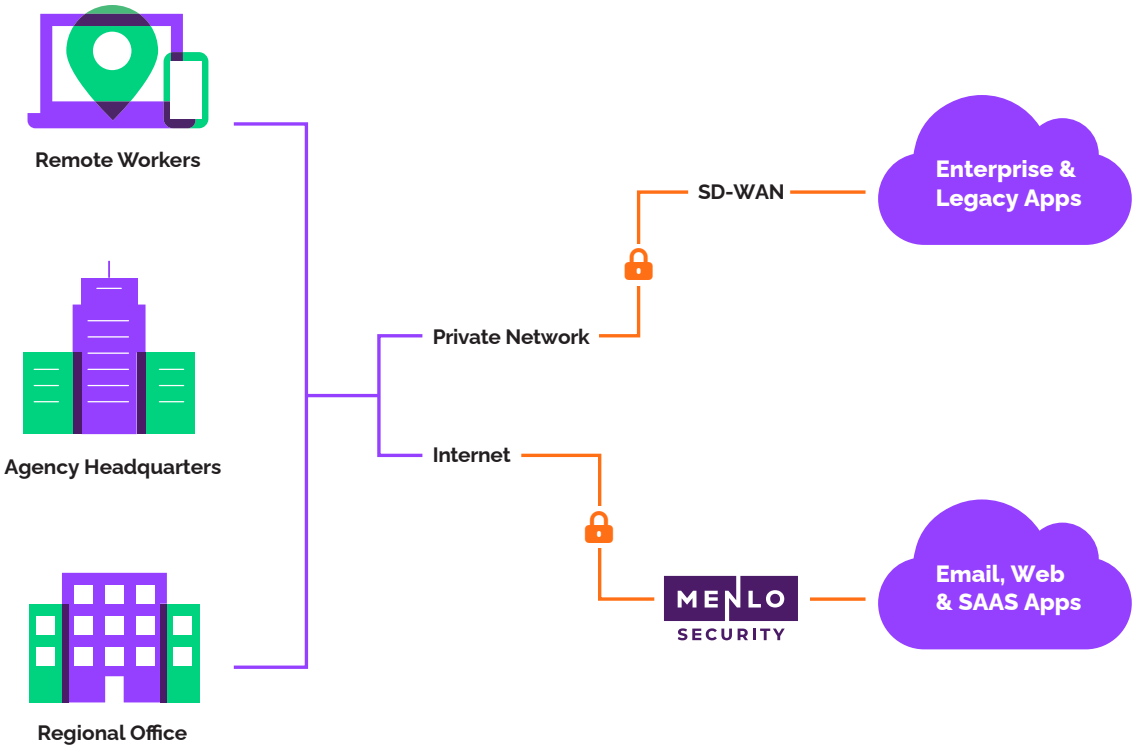
5. **Classified spillover.** When the same personal device is connected to a classified and an unclassified network, malware contracted from personal browsing can make its way to the classified network, creating a serious breach.

Security equals freedom to perform

Faced with those challenges, a sound, coherent strategy for remote, Zero Trust Network Access should focus on these goals:

Freedom from attacks. Your remote workforce needs to be productive and worry-free. They need to access agency servers as well as web-based applications while remaining free from malware, phishing, ransomware, and other attacks. Exposure of classified information can jeopardize your agency's mission. Malware resulting in downtime will degrade not just one worker's productivity, but that of the worker's entire team.

Freedom to roam. To enable workers to maintain a high level of productivity, they will need fast, reliable, and secure Internet access. However, performance will suffer if traffic must be backhauled across the agency VPN. The remedy: A split VPN that sends classified traffic across the encrypted VPN, separating it from email, web browsing and SaaS applications.



Remote Browser Isolation will enable you to achieve both these goals. A cloud-based isolation solution works with SD-WAN environments, separating web browsing and email traffic from classified agency VPN traffic and sending it to a cloud-based Secure Web Gateway (SWG) that isolates traffic by creating a virtual "air gap" that prevents malicious downloads from ever reaching users' devices. Documents from web sites or email attachments — in all popular formats, including Word, Excel, PowerPoint, and PDF — are displayed remotely using HTML 5, which prevents malware from spilling over into classified traffic.

Cloud isolation also works with mobile device management (MDM) tools to protect smartphones and tablets. That can help protect workers who are permanently remote, such as those who perform field data collection or equipment maintenance.

Empower Zero Trust with the power of isolation

The Menlo Security Cloud Security Platform powered by an Isolation Core™ keeps malware entirely separate from your users' devices, so there's no need for extensive endpoint security tools and the corresponding management overhead they create. Instead of chasing down false alarms and plugging breaches after they occur, your hard-pressed staff is freed up to focus on strategic goals that advance your agency's mission.

Menlo's Cloud Security Platform is a proven, patented, proactive solution that is used today by civilian and defense agencies to enable true Zero Trust security. It's a key element in a game plan to enable your agency to succeed in the new normal by making your remote and hybrid workforce both highly productive and secure.

Discover how you can boost the efficiency of remote workers while keeping malware off their systems. We're ready to answer your questions at: ask@menlosecurity.com.

MENLO SECURITY

To find out more, contact us:

menlosecurity.com

(650) 695-0695

ask@menlosecurity.com

About Menlo Security

Menlo Security enables organizations to eliminate threats and fully protect productivity with a one-of-a-kind, isolation-powered cloud security platform. It's the only solution to deliver on the promise of cloud security—by providing the most secure Zero Trust approach to preventing malicious attacks; by making security invisible to end users while they work online; and by removing the operational burden for security teams. Now organizations can offer a safe online experience, empowering users to work without worry while they keep the business moving forward.