FCW

SAFE AT HOME

Securing federal IT in the remote-work era

SPONSORED BY: SONICWALL®

As the COVID-19 crisis has unfolded, remote work has become increasingly the norm across the private sector and in federal government as well. By late fall, federal employees working remotely topped 70 percent in many agencies and as high as 90 percent in others, according to testimony to Congress in November.

Yet remote work brings with it new perils, especially in the area of cybersecurity. Federal technology leaders are concerned about the growing potential for cyber compromise at a time when workers are logging in via their personal devices, from their home networks.

Government already was experiencing a rise in cybercrime, even before the pandemic sent everyone home from the office. In 2018, U.S. government agencies reported 31,107 cyber incidents, Statista reports, and that figure has only continued to rise. Government leaders acknowledge the risk and have proposed $18 billion in cyber funding in the 2021 federal budget.

COVID -19 only served to escalate the situation. When the pandemic struck, the FBI's Cyber Division reported 4,000 complaints of cyberattacks per day, a 400 percent increase versus pre-coronavirus times. Experts say at least a part of this rise is the result of the rapid shift to a work-from-home footing.

After federal employees packed up and went home last spring, agencies—including the FBI and the Cybersecurity and Infrastructure Security Agency (CISA)—put out warnings about the possibility of bad actors specifically looking to exploit the new remote-work environment. Lawmakers echoed the call, noting that government systems could be at risk in the volatile and fast-changing IT situation. "Our federal information systems are subjected to persistent cyber-attacks that pose a significant national security threat, and our government is not currently prepared to effectivity respond to them," warned Senator Gary Peters.

While the coming of a vaccine should help return things to "normal," work won't be like it was before.

More than a third of firms that have switched to remote work say work-from-home will persist even after the pandemic, Harvard Business School reports. In government as elsewhere, there is an expectation that remote work will remain in place for many employees, even after the pandemic.

With that being the case, it is imperative that government take a fresh look at the vulnerabilities that may have arisen with the rush to work from home. Federal IT leaders need to evaluate not just their specific point-fixes around security, but their overall approach to safeguarding both end users and federal networks.

Going forward, government needs a holistic approach to security. Federal agencies need an effective and coherent means to safeguard networks in real time, while also protecting the vast and growing landscape of user endpoints from possible cyber incursion.

> "The rate at which agencies adopted a strategy of maximum telework…left little time for administrators to check their networks, improve policies and apply updates."
>
> *—Congressional Research Service*

THE REMOTE-WORK CHALLENGE

In order to re-envision federal cybersecurity, it's helpful to first take a step back and consider the changed threat landscape, to look at some of the ways in which remote work has increased vulnerabilities across federal systems.

It's important, first, to recognize the high bar that government sets for itself in regard to data security. In addition to high-value information in support of

national security, federal systems are chock full of citizens' personal data, including financial information, demographic details, and various other forms of personally identifiable information. From both a regulatory standpoint and an ethical perspective, government must shield this information from prying eyes, even as it seeks to safeguard critical security data from attacks by state and non-state actors.

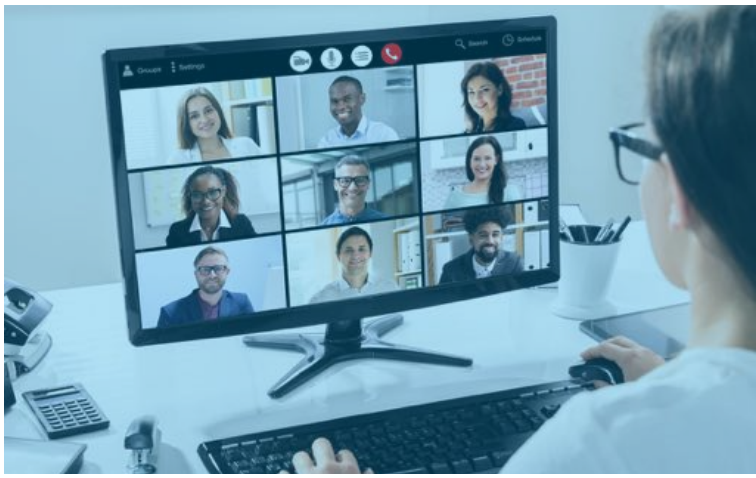
In short: The cyber stakes are high in government.

The rush to remote work in many cases has made a difficult situation worse. Employees logging in from home are no longer operating within the previously-defined digital perimeter: They may be on commercial networks, and may be using personal devices for federal work. At the same time, the sheer scale of the digital footprint has been magnified exponentially: Each of those end user devices, each external connection that wasn't there before, represents a potential point of compromise.

With the quick pivot to telework, federal IT teams may have not had the opportunity to sufficiently safeguard this changed landscape, according to government overseers. "The rate at which agencies adopted a strategy of maximum telework in response to COVID-19 left little time for administrators to check their networks, improve policies, and apply updates," the Congressional Research Service (CRS) reports.

CRS highlights a range of potential hazards that arise in this scenario. "Employees are no longer accessing agency computing resources from inside agency facilities, with the physical security that comes with those facilities," they note. "They may be using unsecured home networks or devices (e.g., unpatched equipment) to access agency information. Agencies may have had to increase network access rapidly to allow for maximum telework, without establishing, testing, and refining security measures to protect data."

Adversaries looking to exploit the situation won't just poke at federal networks. They will also focus



their energies on the at-home employees, who may represent the weak link in the security chain. "With so many users teleworking, an adversary may only need to compromise one or a few user devices, and then use their VPN connection to access agency information, appearing as legitimate traffic and network use to an agency's internal defenses and logs," CRS warns.

It's long been understood that the end user is the greatest risk in cyber security, as bad actors deploy a range of behavioral-based attacks to compromise systems. With the workforce now operating remotely, that risk is multiplied.

Users may lack the sophistication to safeguard their home connections. They don't know about the need for a secure Wi-Fi SSID; they may not be aware of the importance of certificates, or the significance of a VPN connection.

In addition, their use of a single device for both personal and work tasks may create a new potential for disruption. Employees who have internalized the mantra of countless IT security seminars—don't open a suspicious link—may ignore that advice when checking their personal email. If that (now compromised) device is then used for federal work, entire systems could potentially be exposed to risk.

"Employees who telework from home need to keep Government property and information safe and secure and separated from their personal property and information." *—OPM*

The Office of Personnel Management has issued guidance around this. "Employees who telework from home need to keep Government property and information safe, secure, and separated from their personal property and information," OPM notes. In practice, though, most federal IT leaders recognize that they cannot rely on end users alone to act in ways that safeguard agency systems.

Adversaries and bad actors likewise are fully aware of the situation, and are looking for ways to leverage their current advantage. Why is phishing on the rise? Experts say the trend tracks directly to the jump to telework, and the likelihood that cyber best practices are no longer fully in force.

After the initial rush to telework, many agencies looped back to put in place stronger security protocols. With work-from-home likely to persist, however, the point fixes and temporary safeguard they have implemented likely will prove insufficient. What's needed is something bigger and new—a holistic approach to cybersecurity that gives equal weight to network defenses and end-user device controls.

A NEW APPROACH

Federal agencies need a new approach to security, one that enables them to take command of a borderless reality where the proliferation of use end points—along with new apps, devices, and sensors—is continuously reshaping the security landscape.

They need a holistic approach, one that leverages a layered security platform in order to mitigate risk and protect a widely dispersed workforce. With security that encompasses not just the network but also the plurality of user connections, IT needs an approach that will support employees working from home without inheriting the potential security vulnerabilities inherent in personal networks.

This all-encompassing approach would offer real-time intelligence, with automated insights into threat performance throughput. A layered security platform should detect and block the most evasive cyberattacks across expanding points of exposure. It should defend the organization from ever-increasing vulnerabilities associated with remote work, while also securing on-premises, SaaS and cloud applications.

One may envision this overarching approach to security as standing on three legs: Policies and protocols; next-generation firewalls and end user devices.

- **Policy and governance** – In order to effectively ensure security in a work-from-home environment, federal IT leaders need to put forth sound policy regarding the uses of technology. They need coherent governance to ensure that devices are kept current, that passwords are used in a secure way, and that suspect events are addressed in a timely and effective manner.

  Moreover, IT leaders need tools that can enforce these policies without adding to the already weighty burden of technology management. Under telework, technology teams are fielding ever-greater volumes of help desk calls. They are engaged in many manual tasks around not just security, but mere functionality, as they labor to keep remote workers productive. In this environment, they need a security platform that automates much of the manual work, enforcing policy by default and thus, freeing skilled IT workers to focus on higher-level tasks.

- **Next-gen firewalls** – While remote work has dissolved some of the conventional boundaries that used to differentiate the "inside and outside" of the network, firewalls remain a key protection.

  Federal agencies typically will architect IT information and processes in siloes. In the midst of telework, firewalls function as a key safeguard, serving as protective barrier not just against outside incursion but also in the event that malicious content or processes should find their way inside.

  Leveraged in support of intrusion prevention and intrusion detection, firewalls can scan for threats, identify potential malware, and raise the alarm when there are indications of an intrusion.

- **End user devices** – Recognizing that employees at home remain the weak link in the security chain, a complete approach to federal IT security will put special emphasis on the hardening of end user devices.

IT needs the ability to secure devices, and to ensure that these end points remain secure as long as they are interacting with federal networks. They need the means to scan devices, to ensure security protocols are current and applications are up to date. Likewise, IT needs control over the factors that could potentially influence end-device behavior, such as the ability to attach peripherals via USB.

In the big picture, the ability to harden the end point is key to managing the overall security of the federal network and its associated assets.

An across the board approach to security will address all these key areas, layering on a variety of protections in support of a true defense-in-depth deployment. A platform approach can support secure remote access, cloud app security, and secure email, while also delivering endpoint protection, advanced threat protection, and the next-generation firewalls needed to safeguard systems against the multiplicity of threats that emerge each day at the boundaries of telework.

The SonicWall solution

A longtime leader in the security arena, and a trusted partner in federal government, SonicWall offers a cyber platform ideally suited to support the emerging needs around telework. Taken together, its combination of resources—with trusted firewalls, in-depth security expertise, and capabilities around end-point security—can help to safeguard federal data and processes in the current landscape.

SonicWall provides U.S. government-certified cybersecurity solutions for administrative, intelligence, and military organizations and agencies. To ensure U.S. federal agencies and organizations can deploy SonicWall products and solutions with full confidence, all SonicWall products are compliant with the National Defense Authorization Act (NDAA), specifically Section 889. This key safeguard prohibits federal agencies and their contractors from procuring critical IT from specific Chinese companies.

SonicWall products, services and technology are also compliant with a number of key U.S. federal laws and regulations, including TAA, FIPS-140-2, Common Criteria, DoDIN APL, CSfC, USGv6, IPv6 Phase 2 and more.

What exactly do these solutions entail? Let's take a deeper look:

SECURE MOBILE ACCESS

SonicWall Secure Mobile Access (SMA) is a unified secure access gateway that enables organizations to provide anytime, anywhere and any-device access, to any application.

SMA's granular access control policy engine, context-aware device authorization, application-level VPN and advanced authentication with single sign-on enable organizations to move to the cloud with ease, and to embrace work-from-home protocols in a hybrid IT environment.

With SMA, agencies can enforce granular access control policies and get high-performance layer-3 SSL VPN. SMA gives them visibility into every connecting device and delivers browser-based clientless secure access.

At a time when IT talent is stretched thin, SMA enables agencies to consolidate access management. The IT team can provide users with secure access to data center, cloud and SaaS resources, all from a single portal. They can enable federated single sign-on (SSO) using SAML 2.0 authentication. All this, in turn, helps to reduce complexity in access management for hybrid IT environments.

For the mobile workforce, SMA delivers a seamless, secure access experience, with an always-on connection. The system automatically and continually checks the integrity and health profile of the connecting device while delivering an intuitive, pain-free experience for the end user.

At the same time, SMA enhances security across a number of fronts. It can integrate with multi-engine sandboxing to automatically identify and quarantine potential threats. It will prevent malicious files from being uploaded into your network, protect against DDoS and zombie attacks from compromised endpoints, and enforce stacked multi-factor authentication for added security.

Specially, SMA provides a secure file share mechanism that utilizes multiple security components to block malicious files, while allowing only trusted users and endpoints, and clean files into the network. Significant features include:

- **Clientless Access:** Rather than have IT install clients on every endpoint device, users simply open their choice of web browser and login to a secure access portal, which encrypts the session with strong SSL/TLS.
- **Strong Authentication:** SonicWall SMA supports industry standard authentication methods that use RADIUS and Kerberos for campus-hosted applications, and SAML 2.0 for cloud-hosted SaaS applications.
- **Endpoint Profiling:** The endpoint control feature for SMA allows the administrator to enforce granular access-control rules based on the health status of the connecting device. Prior to granting access, mobile devices are interrogated for essential security information such as jailbreak or root status, device ID, certificate status and OS versions. Laptops and PCs are also interrogated for the presence or absence of security software, client certificates, and device ID. Devices that do not meet policy requirements are not allowed network access, and the user is notified of non-compliance.

With SMA, IT can enforce granular access control policies based on the type of user—employee, contractor, partner or vendor—as well as the device being used, application being accessed and location of access. It also offers scanning of downloaded files for malware and zero-day threats.

A central management server (CMS) for SMA provides reporting and monitoring capabilities including Capture ATP test results and session information such as user ID and IP address. It gets end-to-end network visibility and an audit trail for reporting and compliance.

CAPTURE CLIENT

With end-user devices now the front line of security, SonicWall Capture Client offers federal agencies a unified client platform that delivers multiple endpoint protection capabilities, including next-generation malware protection and application vulnerability intelligence.

Capture Client leverages cloud sandbox file testing, comprehensive reporting, and enforcement for endpoint protection. It provides consistent assurance of client security, with easy-to-use and actionable intelligence and reporting.

A device control feature allows administrators to control what USB devices can be connected to or are blocked from connecting to an endpoint, as a means to prevent malware threats spreading via USB devices, and also to prevent data exfiltration. Administrators have flexibility: They can ban USB connections altogether, for example, or can permit them based on trusted vendors.

Capture Client also brings to bear next-generation antivirus capabilities to mitigate attacks before, during, and after they execute. It continuously monitors system behavior, strengthening organizational confidence in the face of ransomware and advanced threats.

With IT skills stretched thin, agencies can leverage Capture Client to ease the burden on the IT workforce.

Administrators can secure endpoints, no matter where they are. A global dashboard delivers high-level metrics, along with the ability to manage multiple tenants within a single pane of glass. Admins can quickly find and diagnose critical vulnerabilities, supported by active sandboxing capabilities as well as dynamic white/blacklisting and cloud intelligence.

NEXT-GEN FIREWALLS

Even as remote work expands the organizational perimeter, firewalls remain the bedrock of any network security deployment. Firewalls are key to delivering advanced threat protection in an increasingly boundless IT ecosystem.

SonicWall Network Security Manager (NSM) gives administrators everything they need for centralized and comprehensive firewall management. It enables IT to onboard and manage dozens or hundreds of firewalls centrally from one interface, and to deploy and administer firewalls remotely with Zero-Touch Deployment.

NSM simplifies set-up with configuration wizards, and empowers IT to identify and remedy security risks through detailed analytics and intuitive dashboards. Administrators can quickly and easily deploy new firewalls using custom configuration templates, and can impose federate security policies.

Combined with the Capture Advanced Threat Protection (ATP) sandbox service, SonicWall firewalls have been awarded ICSA Labs' highest level of firewall, anti-malware and advanced threat defense certifications. Some key features include:

- **Advanced Threat Protection** – IT teams can prevent Zero-Day and unknown malware in its tracks with Real-Time Deep Memory Inspection (RTDMI) and Reassembly-Free Deep Packet Inspection (RFDPI). Robust on-box technology paired with cloud-based updates help agencies to stay ahead of the threats.

- **Multi-Instance Firewall** -- A modernized approach to legacy multi-tenancy, Multi-Instance uses containerized architecture to run multiple independent firewall instances, software versions, and configurations on the same hardware without the need to manage multiple appliances.
- **Unified Policy** – A unified policy approach enables administrators to combine Layer 3 to Layer 7 access and security rules into a single policy, thus reducing rule management overhead. Intuitive policy creation and visual workflow reduce configuration errors and deployment time for a better overall security posture.

Even as the perimeter expands to encompass the realities of work-from-home, advanced firewalls continue to deliver critical security safeguards. As part of a holistic approach to security, firewalls remain a vital component of the overall cybersecurity infrastructure.

CONCLUSION

Moving forward

As agencies rethink their cyber priorities in response to the work-from-home paradigm, they will likely look for partners who bring unique strengths and capabilities, along with a proven track record of success.

The SonicWall approach has a demonstrated efficacy rate of greater than 98 percent. In testing, it will identify and effectively address nearly all threats. Driving that success rate is the SonicWall Capture Labs Threat Research Team, which works behind the scenes to gather, analyze, and vet cross-vector threat information.

Drawing on more than 1 million security sensors in nearly 200 countries and territories, the team has access to cross-vector, threat-related information shared among SonicWall security systems, including firewalls, email security, endpoint security, honeypots, content-filtering systems and the SonicWall Capture Advanced Threat Protection multi-engine sandbox. The team also leverages shared threat intelligence and exploits from more than 50 industry collaboration groups and research organizations.

In addition, SonicWall differentiates its offering by providing its users with risk meters, a key tool in the effort to stay current against fast-changing cyber threats.

Risk meters detect immediate threat risks and take defensive action. As the perimeter expands, risk meters support IT with customizable threat data and risk scoring for the entire network infrastructure. Metering is customizable to specific network requirements and to the current condition of the network ecology. This customizable threat data provides a very specific defense layer: A real-time, graphics-assisted analysis. Security teams can see potential security gaps, recognize incoming attacks, and monitor all possible threat vectors.

All this underscores the holistic nature of the SonicWall solution. Far more than just a bullwork against incursions, SonicWall delivers a full suite of mutually supportive security solutions. Back-end research supports real-time detection and remediation, with management tools designed to ease the IT workload, while effectively and efficiently securing end users and their vulnerable endpoint devices.

To learn more about SonicWall solutions contact SonicWall's U.S. Federal Team: FederalTeam@SonicWall.com

SONICWALL®