PREVEIL

Cybersecurity for Work from Home

Executive Summary

THE PURPOSE OF THIS BRIEF is to help enterprises of any size scale up their work-from-home capabilities quickly and securely by leveraging the latest technological advances in cybersecurity and applied cryptography.

The most obvious choices to enable work from home are virtual private networks (VPNs) and remote desktops. However, in addition to being cumbersome to deploy and manage, both also have significant vulnerabilities to cyberattacks. Indeed, the National Security Agency (NSA) is deeply concerned about the work that U.S. government employees and military personnel are doing from home, and thus recently issued **guidance** about the use of collaboration services for telework. In its list of criteria for safely using such services, the NSA's top recommendation is that the service use end-to-end encryption.

PreVeil's security paradigm, grounded in end-to-end encryption, satisfies this top NSA criterion and more. PreVeil assumes cyberattacks will occur and focuses instead on rendering them useless. Data is never decrypted on any server anywhere; if attackers successfully breach a server, all they will get is useless gibberish. PreVeil can be used in conjunction with VPNs or remote desktops to secure files, data and communications.

PreVeil deploys easily in minutes with no impact on your existing email and file servers, making configuration and deployment simple and inexpensive. It integrates seamlessly with the email and file sharing tools you and your employees already use, and clearly distinguishes between enterprise and personal messages, files and data.

PreVeil Drive allows your remote employees to share and store files with end-to-end encryption, overcoming security deficiencies in enterprise networks and workers' home equipment, mobile devices, and wifi connections. PreVeil Drive works like DropBox for file sharing, but with far better security.

PreVeil Email allows your remote employees to send and receive end-to-end encrypted emails using their existing email address. It integrates with mail clients such as Outlook, Gmail, and Apple Mail, and also works on browsers and mobile devices.

In short, PreVeil is easy to use and so it will be used by the remote workers your organization is depending upon now.

Finally, PreVeil's world-class end-to-end encryption provides the foundation for compliance not just with the NSA's cybersecurity guidance on work from home, but also with federal regulations for handling sensitive information such as that associated with the aerospace and defense industries, financial and legal services, and health care.

Our hope is that this brief helps you move your enterprise forward quickly and securely in these challenging times. We are here to support that effort.

Introduction

Working from home, or telecommuting, grew in the United States for full-time employees by 115% from 2007 to 2017, nearly 10 times faster than the workforce itself.[1] The increase has been driven by several factors, including technological advances that enable remote work; growing demands from employees for greater flexibility; and the cost savings associated with a remote workforce.

> ***Speed is of the essence as organizations make the transition to a remote workforce. So too is cybersecurity.***

The coronavirus has accelerated the exodus from workplaces, a trend that is expected to continue. Today, given the mass exodus from workplaces driven by efforts to mitigate the spread of the coronavirus, work at home is burgeoning. Some companies have already been working remotely and communicating securely, and so are ahead of the curve. But many, perhaps most, are not prepared for the cybersecurity challenges that remote work creates.

We understand that speed is of the essence as organizations make the transition to a remote workforce. So too is security. At PreVeil, we believe that speed and security need not be mutually exclusive.

This paper is intended for organizations with employees working remotely, perhaps for the first time, and who are handling sensitive information such as that associated with the aerospace and defense industries, financial and legal services, and health care. That said, any business with employees working on home computers, laptops, and mobile devices—all with questionable levels of security—and using wifi that may or may not be properly configured or being tapped into by a neighbor, stands to benefit from this brief.

Key considerations for securing work from home

To secure employees' work from home, a few straightforward considerations should be top of mind:

- Enterprise and home networks and systems need to be protected.
- Email and files that belong to the enterprise need to be secured. Doing so starts with delineating, or separating, work communications from regular day-to-day emails and files.
- Secure, work-related emails and files need to be accessible via mobile devices including phones and tablets, and on home computers including Macs and PCs (Windows).
- Employees working on their own home computers or laptops should not rely on passwords to authenticate cloud-based services.

[1] Global Workplace Analytics and flexjobs. *2017 State of Telecommuting in the U.S. Employee Workforce.* See: https://globalworkplaceanalytics.com/2017-state-of-telecommuting-in-the-us

- At the enterprise level, deployment and management of security solutions should be quick and simple.
- For remote employees, installation and removal of security solutions should be quick and simple.
- Security should be easy to use; if not, it won't be used.
- Any solution should be compliant with relevant regulations, such as federal guidelines for handling CUI (controlled unclassified information) or ITAR (International Traffic in Arms Regulations), or FINRA and HIPAA in the financial and healthcare realms.

Please know that these considerations need not be overwhelming. Solutions exist to help you address all of them and, likewise, minimize the cyber threats that increase with remote work. While cyber threats certainly are not new, cyber criminals see opportunity and haven't wasted any time trying to take advantage of the spike in work at home. The Department of Defense, for example, reported in early 2020 that cyberattacks on its networks had soared as remote work began to place unprecedented loads on its networks.

Vulnerabilities most likely to be exacerbated by remote work and expanded attack surfaces are all too familiar, including server and network attacks—both on home and enterprise systems—and password attacks such as phishing and spoofing. Administrators, too, are more vulnerable if they're working remotely.

Alternative approaches to work from home

The first order of business is to connect remote workers to their organizations' networks and servers. The emphasis now is on speed: scaling and getting workers at home back in action as quickly as possible. Technical alternatives for doing so are limited. The most obvious choices are to deploy virtual private networks (VPNs) or remote desktops.

> ***When both remote connections and security are taken into consideration, the best alternatives are end-to-end encryption applications, which can be used in conjunction with VPNs and remote desktops.***

But security can't be overlooked in the rush for connectivity, or the risk to your organization could grow exponentially. As described below, VPNs and remote desktops are particularly vulnerable given that they already are favored attack vectors for cyber criminals.

When both remote connections and security are taken into consideration, the best alternatives are end-to-end encryption applications, which can be used in conjunction with VPNs and remote desktops if your organization has already moved in those directions.

Virtual private networks (VPNs)

Virtual private networks allow remote workers to communicate and share files and data through secure "tunnels" to their enterprise network and servers and back. But VPNs are cumbersome to set up and manage, and are vulnerable to malware—both from the remote workers' home networks to the enterprise network, and vice-versa. And because VPNs present a larger attack surface than enterprise networks alone, they're more vulnerable to password and admin attacks as well. On the practical side, they can be difficult to work with.

The cybersecurity firm Radware recently reported that over the past year, enterprise VPNs have become the attack vector of choice for ongoing attacks from advanced persistent threat (APT) actors.[2] Radware's recommendations for securing VPNs are familiar but insufficient: keep up with the latest software patches, implement multi-factor authentication (MFA), use strong passwords, etc. As will be explained below, basic password-based protections still leave organizations vulnerable to many kinds of attacks.

Remote desktops

This approach to enabling remote work allows home computers to act as a "window" into a remote computer either at the workers' organization or in the cloud. Like VPNs, remote desktops are cumbersome to set up and manage. And they're expensive too. Remote desktops' particular vulnerabilities include password and admin attacks, keystroke loggers, and ransomware.

Remote desktop technology is based on Microsoft's Remote Desktop Protocol (RDP). Radware reports that RDP has been gaining traction as the attack vector for ransomware for several years; in Q1 2019, RDP accounted for nearly two-thirds of all ransomware attacks.[3] Similar to VPNs, Radware's recommendations for securing remote desktops focus on software patches, MFA, strong passwords, etc., and are insufficient.

End-to-end encryption applications

End-to-end encryption is the gold standard for protecting email and file sharing. That's why the NSA's recently released guidance on telework focuses on it. According to the NSA, the top two criteria for "selecting and safely using collaboration services for telework" should be: 1) Does the service implement end-to-end encryption? and 2) Are strong well-known, testable encryption standards used? PreVeil's end-to-end encryption is built on algorithms compliant with FIPS 140-2[4] and so meets these criteria and more, as outlined in the section that follows.

End-to-end encryption is based on the principle of zero trust, that is, any user—whether from inside or outside your organization's networks—needs to be authenticated. Too often, the default of traditional remote working solutions is to trust anyone who's communicating from within the network. That gives hackers who've made their way in, through any of a wide range of techniques, legitimacy and free rein within your network.

[2] Radware. *Coronavirus: Security Recommendations for Remote Access Threats,* March 18, 2020. See: https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/coronavirus-remote-access-threats/

[3] Geenens, Pascal. *Coronavirus: Its Four Most Prevalent Cyber Threats.* March 12, 2020. See: https://blog.radware.com/security/2020/03/coronavirus-its-four-most-prevalent-cyber-threats/

[4] FIPS 140-2 refers to the Federal Information Processing Standard Publication 140-2, entitled *Security Requirements for Cryptographic Models.* It defines the critical algorithms and security standards that the private sector must use for encryption in order to work with the U.S. government.

Authentication should be done not by passwords, which are too easy to compromise, but rather by cryptographic private keys stored only on users' devices.

End-to-end encryption ensures that data—emails and files—is encrypted on any device an at-home worker may use, and never decrypted anywhere other than on the recipient's device. This ensures that only the sender and the recipient can ever read the information being shared—and no one else. Data is never decrypted on any server anywhere; if attackers successfully breach a server, all they will get is useless gibberish.

A better alternative: PreVeil

PreVeil is based on MIT computer scientists' research on cybersecurity and applied cryptography. It leverages a fundamentally better security paradigm, grounded in world-class end-to-end encryption. PreVeil's approach to security presumes that cyberattacks will occur and focuses on rendering them useless. PreVeil doesn't depend on passwords, but instead authenticates users via strong cryptographic keys that are automatically created and stored on users' devices—and never in a central key server, eliminating central points of attack.

PreVeil deploys easily in minutes because it integrates with familiar Mac and PC applications. Further, it's easy to use and so it will be used by the remote workers your organization is depending upon.

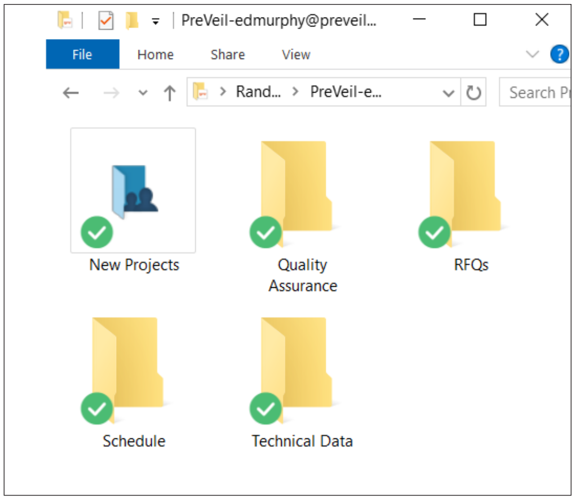
PreVeil Drive

PreVeil Drive ▶ VIDEO allows your remote employees to share and store files with end-to-end encryption, overcoming security deficiencies in enterprise networks and workers' home equipment, mobile devices, and wifi connections. PreVeil Drive works like DropBox for file sharing, but with far better security. And unlike Box, OneDrive, Google Drive, and DropBox, which always have access to your data, only you and the people with whom you've explicitly shared files can decrypt them.

PreVeil Drive users easily create folders for shared data. This approach separates your employees' work files and data from their personal, day-to-day online activity. In the current environment, where work and personal data and communications may well be residing on the same computers and devices, this delineation ramps up security for the work-related files.

PreVeil Drive is easy to use and automatically integrates with Windows File Explorer and Mac Finder. It's available for Windows, Mac and, with PreVeil's mobile app, for iPads and smartphones as well.

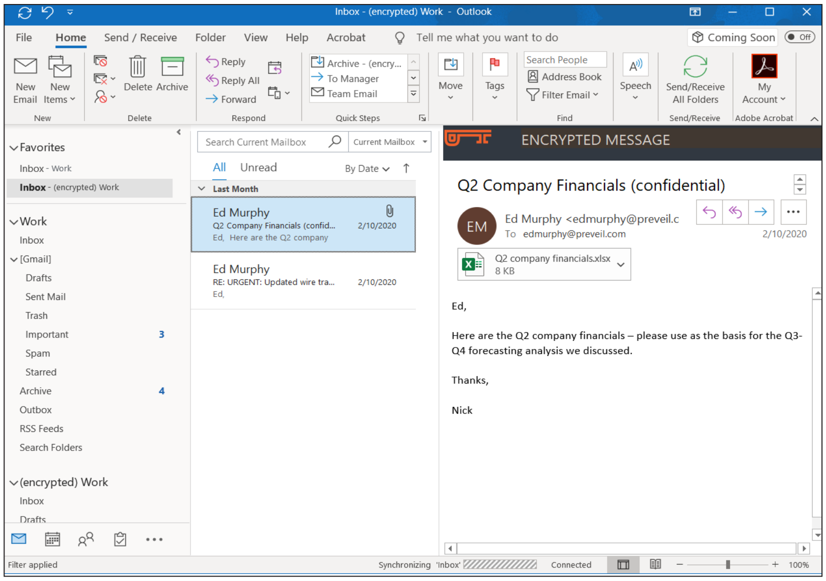
PreVeil Drive: Sharing and storing files



To facilitate remote work by teams, all shared files are synched automatically to authorized users' computers, smartphones or tablets, and any changes made to the files on one device are automatically synched to all devices sharing the data. Note, too, that folders and files can be as easily *unshared* as they are shared. Unsharing removes the data from its corresponding folder on all of the user's devices. This cryptographically-enforced unshare capability provides additional protection when employees are working on their own home computers or laptops.

PreVeil Email

PreVeil Email: Encrpypted inbox in Outlook



Ed Murphy
Q2 Company Financials (confid... 2/10/2020
Ed, Here are the Q2 company

Ed Murphy
RE: URGENT: Updated wire tra... 2/10/2020
Ed,

Q2 Company Financials (confidential)

EM Ed Murphy <edmurphy@preveil.c
To edmurphy@preveil.com
2/10/2020

Q2 company financials.xlsx
8 KB

Ed,

Here are the Q2 company financials – please use as the basis for the Q3-Q4 forecasting analysis we discussed.

Thanks,

Nick

PreVeil Email ▶ VIDEO lets you send and receive end-to-end encrypted emails using your existing email address. It integrates with mail clients such as Outlook, Gmail, and Apple Mail, and also works on browsers and mobile devices. When PreVeil Email is used with Outlook, Gmail, or Apple Mail, the installation process automatically creates a new set of mailboxes for your encrypted messages, helping remote employees separate their work and personal messages. Messages in these new mailboxes are encrypted and stored on PreVeil's servers. There are no changes to the mailboxes already in your mail program and no impact on the servers that store your regular, unsecure messages.

Cloud-based service

Many organizations have avoided the cloud, keeping their email and file servers on premise because they don't trust the security of cloud-based solutions. PreVeil's end-to-end encryption gives organizations the best of both worlds: end-to-end encryption that is even more secure than on-premise deployments, combined with the cost, scalability and agility of the cloud. Again, end-to-end encryption ensures that no one but intended recipients—not even PreVeil or its cloud service—can ever access user data.

For customers in regulated industries, PreVeil runs on Amazon Web Services' Gov Cloud, which provides the foundation for the regulations described in the section below on compliance.

Compliance with federal regulations

PreVeil provides the foundation for compliance not just with the NSA's cybersecurity guidance for work from home, but also with federal regulations for handling sensitive information such as that associated with the aerospace and defense industries, financial and legal services, and health care.

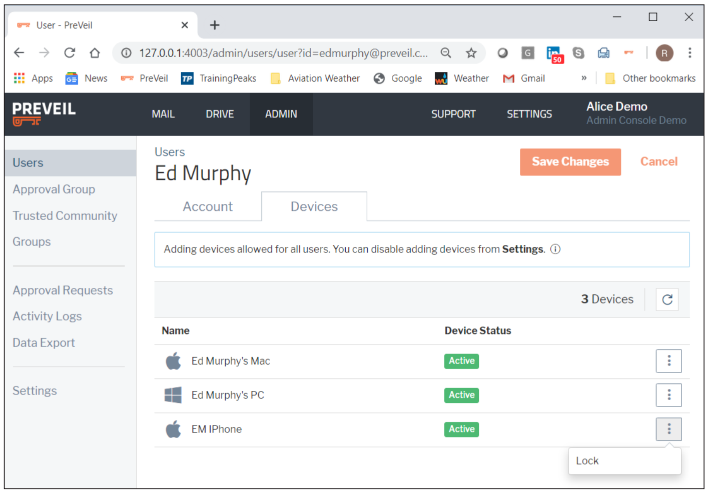
Specifically, PreVeil's Drive and Email solutions support compliance with:

- Virtually all of the controls required by the Department of Defense's new CMMC (Cybersecurity Maturity Model Certification) framework for processing and storing CUI. See PreVeil's CMMC white paper for detailed information on this subject.
- The State Department's most up-to-date regulations requiring end-to-end encryption for communications governed by ITAR (International Traffic in Arms Regulations). Federal regulations mandate that any company that manufactures, exports or brokers defense-related articles, defense services, or is involved with related technical data must be ITAR compliant.
- FINRA (Financial Industry Regulatory Authority) rules and guidance for securities firms and brokers designed to protect investors and ensure market integrity. FINRA regulations governing communications around financial transactions are addressed by PreVeil's tamper-proof logs and journaling, as well as its document versioning and reporting features.
- HIPAA (Health Insurance Portability and Accountability Act) regulations designed to protect the privacy and security of patients' health information. While in early 2020 the Department of Health and Human Services (HHS) temporarily issued waivers of HIPAA sanctions due to coronavirus,[5] HIPAA compliance is undoubtedly critical for healthcare providers in the long-term.

Administrative console

Using PreVeil's Admin Console, IT administrators can create, modify and delete users and groups, as well as set organization-wide data and recovery policies. Device management controls let admins disable lost or stolen devices quickly. Even though all files and emails are encrypted, admins have the tools they need to manage and access their organization's data. They can view activity logs and decrypt and export user data only with permission from a PreVeil Approval Group.

Administrative console: Device management controls



Users

Ed Murphy

Adding devices allowed for all users. You can disable adding devices from **Settings**.

3 Devices

Name	Device Status
Ed Murphy's Mac	Active
Ed Murphy's PC	Active
EM IPhone	Active

[5] Davis, Jessica. *HHS Issues Limited Waiver of HIPAA Sanctions Due to Coronavirus*, March 17, 2020. See: https://healthitsecurity.com/news/hhs-issues-limited-waiver-of-hipaa-sanctions-due-to-coronavirus

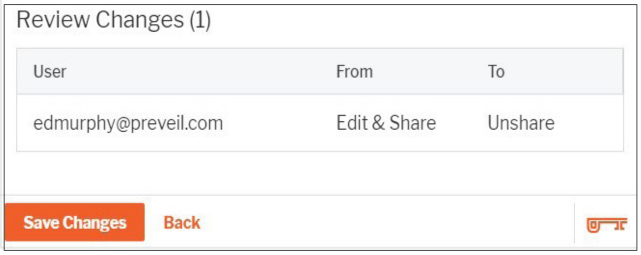
PreVeil's Approval Group feature also prevents admins from becoming central points of attack. By requiring several people to approve an administrator's sensitive activities (such as exporting corporate data), invasive actions are not possible. Much like the nuclear launch keys, requiring several people to authorize critical actions can help prevent malicious activity. In essence, trust is distributed amongst approvers instead of being centralized with one admin.

Further, for both Drive and Email, PreVeil's Trusted Communities allow administrators to restrict communications to whitelisted domains and email addresses. This ensures that only members of a trusted community can exchange emails and files - virtually eliminating phishing and spoofing attacks.

Easy to unshare and control access

PreVeil Drive makes it just as easy to unshare files and folders as it does to share them. For example, when an employee is no longer involved with a program, relevant files can be unshared, in which case the files will no longer be accessible by the employee and the copies located on their PreVeil Drive directories will be removed.

PreVeil Drive: Easy to unshare files and folders



Review Changes (1)

User	From	To
edmurphy@preveil.com	Edit & Share	Unshare

PreVeil also allows administrators to control access down to a device level. If a user's computer or phone has been lost or stolen, for example, the missing device can be locked to prevent further PreVeil access.

Easy to deploy and use

PreVeil deploys easily in minutes because it integrates with familiar Mac and PC applications. And PreVeil is easy for end users to adopt because it works with the tools they already use. Email can be integrated with Outlook, Gmail, or Apple Mail clients. File sharing works like DropBox and is integrated with the Windows File Explorer and Mac Finder.

Cost effective

PreVeil's email and file sharing service is a fraction of the cost of alternatives. Moreover, PreVeil need be deployed only to users handling your sensitive emails, files and data, whereas alternatives require deployment across an entire organization. And PreVeil does not impact existing mail and file servers, making configuration and deployment simple and inexpensive.

Conclusion

Working from home is a necessary alternative for many. Fortunately, it is possible to do so without compromising your organization's security. Technological advances can be deployed to protect sensitive and regulated information that your employees handle at remote worksites.

PreVeil leverages the latest technological advances in applied cryptography to offer unparalleled cybersecurity to protect your enterprise's communications and file and data sharing—regardless of where your employees are based. PreVeil deploys easily in minutes with no impact on your existing email and file servers. It integrates seamlessly with the email and file sharing tools you and your employees already use, and clearly distinguishes between enterprise and personal messages, files and data.

With PreVeil, your enterprise can quickly transition to remote work without sacrificing the security you need to minimize business risk and continue the important work you do.

To learn more about PreVeil, visit us at www.preveil.com/contact/.

PreVeil's principles: Grounded in the reality of today's security environment	
Uncompromising end-to-end encryption	Data is never decrypted in the cloud
Elimination of central points of attack	Trust is distributed amongst the admin team
No more passwords	Cryptographic keys automatically created instead
Secure activity logs	Attackers can neither glean information nor cover their tracks
Ease of use	Effective security must be as frictionless as possible

About PreVeil

PreVeil makes encryption usable for everyday business. PreVeil's encrypted email works with existing apps like Outlook or Gmail, letting users keep their regular email addresses. PreVeil Drive works like DropBox for file sharing, but with far better security. All messages and documents are encrypted end-to-end, which means that no one other than intended recipients can read or scan them—not even PreVeil. PreVeil is designed for both small teams and large enterprises. Visit www.preveil.com to learn more.

Additional copies of this paper can be downloaded at www. preveil.com/wfh-whitepaper.

PREVEIL

July 2020 v3