PREVEIL

Zero Trust

A better way to enhance cybersecurity and achieve compliance

Introduction

PRESIDENT BIDEN'S May 2021 *Executive Order on Improving the Nation's Cybersecurity* mandates rapid development of plans by every federal agency for modernizing their approach to cybersecurity by, among other actions, implementing Zero Trust Architecture. Clearly, the federal government recognizes the need to improve our nation's cybersecurity, with the Department of Defense (DoD) leading the way. According to Katie Arrington, DoD's CISO for Acquisition and Sustainment, DoD is moving forward with a "big push right now on Zero Trust," and CMMC is a part of that effort.[1]

This brief is written to help defense companies better understand Zero Trust principles. It describes how a Zero Trust mindset and architecture creates fundamentally better cybersecurity and, likewise, helps contractors comply with DoD regulations and win defense contracts. While at this point it is still possible to comply with NIST 800-171 and CMMC using legacy security systems, a better path to compliance is achieveable through modern Zero Trust systems, which offer both superior cybersecurity and compliance.

The National Security Agency's (NSA's) February 2021 memorandum, *Embracing a Zero Trust Security Model,* explains that "Traditional perimeter-based network defenses with multiple layers of disjointed security technologies have proven themselves to be unable to meet the cybersecurity needs due to the current threat environment." Instead, NSA recommends a Zero Trust model that "eliminates trust in any one element, node, or service" and "assumes that a breach is inevitable or likely has already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity."[2]

Zero Trust principles are not just a theoretical construct: this brief also describes PreVeil's email and file sharing platform, built from the ground up to implement Zero Trust principles. PreVeil's end-to-end encrypted communications system, in combination with modern end-point controls, protects data resources and Controlled Unclassified Information (CUI) at every point in an organization's communications and collaboration cycle, including, importantly, throughout its supply chain. Further, because PreVeil's platform embeds Zero Trust principles to protect CUI, it helps contractors comply with DFARS 252.204-7012, NIST 800-171, ITAR 120.54, and CMMC Level 3.

1 See: https://www.meritalk.com/articles/arrington-cmmc-should-help-with-zero-trust-memo-coming/
2 See: https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

A brief history of Zero Trust

In 1969, the Pentagon's Defense Advanced Research Projects Agency (DARPA) finalized development of a computer network, ARPANET, and late that year the first communications were sent via computer. Soon thereafter, in 1971, a DARPA developer wrote a program called "Creeper" that moved from one computer to another on its own. Creeper was harmless but portended the myriad worms, viruses, ransomware and cyberattacks—from teenage hackers to nation-states—that would present serious threats in the years to come.

Early efforts to secure networks and protect sensitive data focused on hardening the perimeter, essentially by creating the equivalent of bigger and bigger barriers around data and network boundaries. Early on, the Department of Defense (DoD) attempted to shift this mindset to what was called a "black core" strategy, that is, moving from a perimeter-based security model to one focused on the security of individual actions—including data access—generated from *inside* as well as from outside networks. This "de-perimeterization" approach gained traction through the work of the Jericho Forum, an influential international group of cybersecurity experts formed in 2004.

In 2010, John Kindervag, a senior analyst at Forrester, coined the term "Zero Trust" to describe the evaluation of trust on a per-transaction basis, as opposed to assessing it based on network location.

Despite this early recognition of the need to eliminate any vestiges of trust when it comes to protecting networks and core data, in 2021, the perimeter approach to cybersecurity continues to be practiced, leaving individuals, organizations and nations vulnerable to cyberattacks. That said, it is clear that momentum is building toward state-of-the-art Zero Trust approaches to cybersecurity.

NSA'S ZERO TRUST GUIDING PRINCIPLES

The NSA recommends that the Zero Trust security model be considered for all critical networks, including the Department of Defense network and Defense Industrial Base (DIB) systems. NSA guidance outlines three Zero Trust guiding principles:

1. ***Never trust, always verify.*** **Treat every user, device, application/workload, and data flow as untrusted. Authenticate and explicitly authorize each to the least privilege required using dynamic security policies.**
2. ***Assume breach.*** **Consciously operate and defend resources with the assumption that an adversary already has presence within the environment. Deny by default and heavily scrutinize all users, devices, data flows, and requests for access. Log, inspect, and continuously monitor all configuration changes, resource accesses, and network traffic for suspicious activity.**
3. ***Verify explicitly.*** **Access to all resources should be conducted in a consistent and secure manner using multiple attributes (dynamic and static) to derive confidence levels for contextual access decisions to resources.**

— NSA guidance:
Embracing a Zero Trust Security Model
February 2021

A Zero Trust Mindset Taking Hold: President Biden's Executive Order on Improving the Nation's Cybersecurity

The SolarWinds, Microsoft Exchange Server, and Colonial Pipeline cyberattacks brought cybersecurity issues to the fore at our nation's highest levels. The SolarWinds hack, orchestrated by Russia, gained access to computer networks at hundreds of large American companies and at least seven government agencies including the US Treasury and the Commerce, Energy, Homeland Security, and State departments. Nearly 300,000 Microsoft Exchange email servers were breached by a Chinese cyber espionage unit, affecting at least 30,000 US companies, and more worldwide. And the Colonial Pipeline hack by an Eastern European group exposed the remarkable vulnerability of US infrastructure, as a private pipeline that carries nearly half of all the transport fuels for the Atlantic seaboard states was crippled by ransomware.

These incidents helped spur release of President Biden's May 12, 2021 *Executive Order on Improving the Nation's Cybersecurity*, which reads in part:

> To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, the Federal Government must take decisive steps to modernize its approach to cybersecurity, including by increasing the Federal Government's visibility into threats, while protecting privacy and civil liberties. The Federal Government must adopt security best practices…[and] advance toward Zero Trust Architecture… (Section 3(a))

The Executive Order issues a mandate:

> Within 60 days of the date of this order, the head of each agency shall…develop a plan to implement Zero Trust Architecture, which shall incorporate, as appropriate, the migration steps that the National Institute of Standards and Technology (NIST) within the Department of Commerce has outlined in standards and guidance**…** (Section 3(b)(ii))[3]

3 See: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Zero Trust Architecture: Wide implementation expected

Biden's Executive Order makes clear that via mandated amendments to the Federal Acquisition Regulation (FAR), Zero Trust tenets will need to be built into any software the federal government acquires or that its contractors use. The aim is to improve not just federal cybersecurity, but also that of the private sector on which our nation is so dependent—as vividly revealed most recently by the Colonial Pipeline incident.

Changes to FAR and likewise, DFARS, the Federal Acquisition Regulations specific to Defense, mean that to continue to do business with the DoD, defense contractors will need to incorporate Zero Trust Architecture into their communication and collaboration platforms.

IMPLEMENTATION OF BIDEN'S MAY 2021 EXECUTIVE ORDER VIA GOVERNMENT CONTRACTS

"The benefit here is that typically executive orders really only apply to the federal government. And what we're going to see is through the power of the purse, through the purchasing apparatus of the United States government in the software from U.S. tech companies and others, we're going to see improved security standards and improved security performance."

— Christopher Krebs, former Director of CISA, DHS on Face the Nation, May 15, 2021

PreVeil: A Zero Trust Model for Communications and Collaboration

NSA's Zero Trust principles, as well as the National Institute of Standards and Technologies (NIST) Special Publication 800-207, *Zero Trust Architecture*, show how Zero Trust Architecture is designed to secure the entire breadth of computing services, data resources, and network locations across enterprises. This brief focuses on one of the most important aspects of that landscape, that is, communication and collaboration systems. These systems—particularly emails and sensitive documents—are by far the most targeted and vulnerable points of attack. As such, communication and collaboration systems are the logical first place to apply Zero Trust principles for enhanced cybersecurity.

Simply put, communication and collaboration systems have three key components, each of which presents security challenges:

- Servers, through which all emails and data pass;
- Users, up and down supply chains; and
- Administrators, whose data access often makes them a central point of attack.

A Zero Trust system assumes servers will be breached, user passwords will be compromised, and administrators will be prime targets of attackers.

PreVeil's email and file sharing platform, built from the ground up to implement Zero Trust principles, addresses the fundamental vulnerabilities presented by each of the three key components of a communications and collaboration system, as described below.

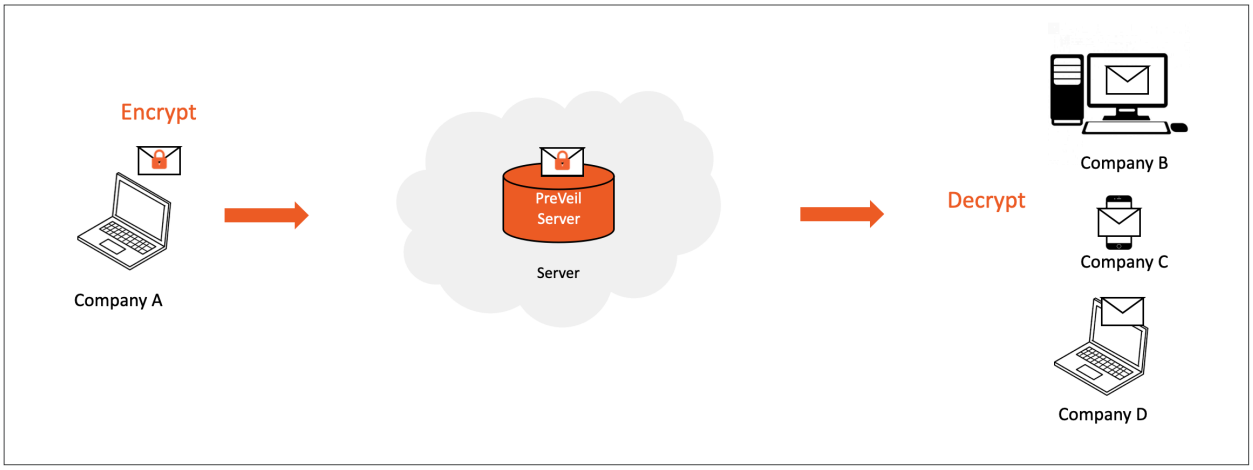
PreVeil's email and file sharing platform is built from the ground up to implement Zero Trust principles.

Fundamental vulnerability: Servers

Legacy systems that focus on securing the perimeter leave servers and their assets vulnerable when inevitable breaches occur. Even legacy systems that use encryption in transit and at rest—as called for in President Biden's Executive Order—don't go far enough. They're vulnerable to hackers because data is decrypted on the server when it's in use. If a server can see the data stored on it, hackers can too. Moreover, keys to decrypt data are accessible to servers; when attackers breach the server, they can access those keys and, likewise, all the data despite its encryption in transit or at rest. Decryption of the data on the server for scanning by service providers to gather information for their own commercial purposes also presents openings for hackers to exploit.

The Microsoft Exchange Server data breach gave attackers full access to decrypted user emails and passwords, administrative privileges on the server, and access to connected devices on the same network. By contrast, with PreVeil, all data is only ever encrypted and decrypted on a user's device—and never on a server in-between. Because PreVeil's end-to-end encryption protects data at all times, servers are eliminated as a point of failure. If hackers gain access to the server—which a Zero Trust mindset assumes is inevitable—they will find only gibberish. With PreVeil, no one but the intended recipient, not even PreVeil, can read users' messages and files. Figure 1 below shows how PreVeil helps organizations move from perimeter-focused security to a modern cybersecurity approach.

Figure 1: PreVeil's end-to-end encryption eliminates threat of server breaches



It is noteworthy that early in 2020 when the pandemic forced a rapid transition to remote work, the NSA—consistent with Zero Trust principles—recommended that the top two criteria to consider when assessing services enabling remote collaboration should be 1) whether that service implements end-to-end encryption, and 2) if the service uses well-known, testable encryption standards.[4] PreVeil meets each of these criteria by using FIPS 140-2 validated cryptographic modules for its end-to-end encryption. Moreover, the NSA guidance stipulates seven additional criteria for assessing collaboration services—all rooted in Zero Trust and all of which PreVeil meets.

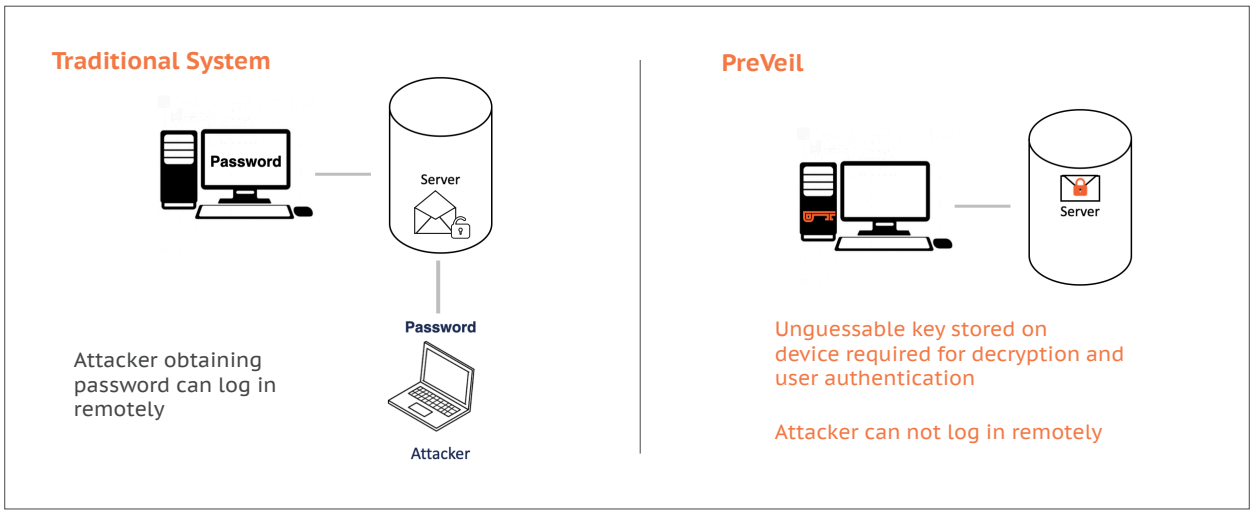
Fundamental vulnerability: Users

Users present a range of security threats that flow from access to their many devices and accounts. A primary security risk is built into most systems given that they use passwords to authenticate user identity, despite the fact that they are often weak and so are routinely guessed or stolen. Compromised passwords are used to impersonate a user's identity, gain unauthorized access to data, and/or escalate privileges to gain further network access.

PreVeil eliminates password vulnerabilities with keys

PreVeil's Zero Trust system assumes passwords will be breached and so protects data resources by eliminating the need for passwords. Instead, access to accounts is protected by automatically-generated cryptographic keys that are stored only on user devices and nowhere else, including servers. Unlike passwords, it is mathematically impossible for these 256-bit keys to be guessed by brute force techniques or by even the most sophisticated password cracking efforts. 256 bits means that the user's key is 10^{78} long. And even if all the passwords to a user's other accounts are stolen, their PreVeil account will remain secure. Figure 2 shows how cryptographic keys stored on devices—and not on servers—protect data.

Figure 2: PreVeil eliminates password vulnerabilities with keys



4 See: https://media.defense.gov/2020/Aug/14/2002477670/-1/-1/0/CSI_%20selecting_and_using_collaboration_services_securely_short_20200814.pdf

PreVeil takes security a step further than Biden's Executive Order, which calls for widespread adoption of multi-factor authentication, a tactic designed around passwords. Again, PreVeil addresses the core of the problem by eliminating passwords. Further, because PreVeil uses private cryptographic keys stored on devices to authenticate users, users can log in only directly from authorized devices, eliminating the common problem of hackers using stolen passwords or keys to log into networks from anywhere in the world. And if a device is stolen, administrators can quickly shut down all access to emails and files from that device.

PreVeil's Trusted Communities™ shut down phishing and spoofing attacks

Another security threat that targets users is phishing and spoofing. Traditional email systems give attackers unlimited access to users, as all they need is their target's email address to carry out their efforts. Attacker can flood users with a barrage of phishing or spoofing attempts over an unbounded period of time, and it takes just one user falling for one attempt to jump start a breach.

PreVeil's Trusted Communities™ feature virtually eliminates phishing and spoofing attacks by allowing administrators to restrict communications to white-listed domains and email addresses. Trusted Communities adhere to Zero Trust principles by restricting communications to only pre-approved and authenticated partners, as opposed to the free-for-all that dominates traditional email services today. A user can't fall for a phishing or spoofing attack if that communication is never able to reach them in the first place.

Ironically, this limitation of communications to pre-approved members of a group is already widely used by millions in applications such as WhatsApp and Signal—and yet isn't commonly practiced by CEOs of major corporations nor heads of US federal agencies.

Fundamental vulnerability: Administrators

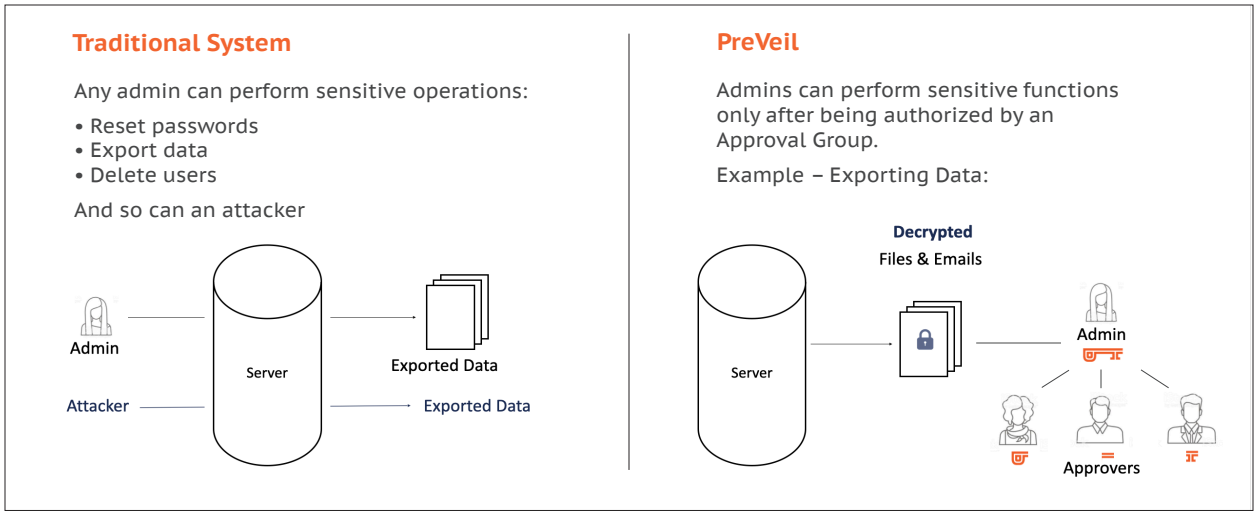
Given administrators broad privileges and access to organizations' data resources, the most serious data breaches occur when admins are compromised or go rogue. Indeed, it is not uncommon for hackers to compromise a single administrator and thereby gain access to the entirety of an organization's emails, files, and other data assets—which is what happened with the Microsoft Exchange Servers breach. The dilemma, though, is how to balance the real need for admins' access with security concerns.

PreVeil's Approval Group™ balances administrative privileges and security

PreVeil's Approval Group™ feature balances privileges and security by distributing trust across a predetermined set of administrators, once again adhering to Zero Trust principles by eliminating implicit trust in any single person who could compromise the entire enterprise. Administrators can still gain full access to data on an as-needed basis, but only after receiving authorization from a set of approvers.

Figure 3 shows how PreVeil distributes trust among a pre-approved group of administrators, each of whom holds a fragment of the cryptographic key needed to carry out administrative activities such as accessing accounts. Enterprises decide for themselves the size of their Approval Group, and how many members of that group's approval is needed for specified actions.

Figure 3: PreVeil reduces administrative vulnerabilities with Approval Groups



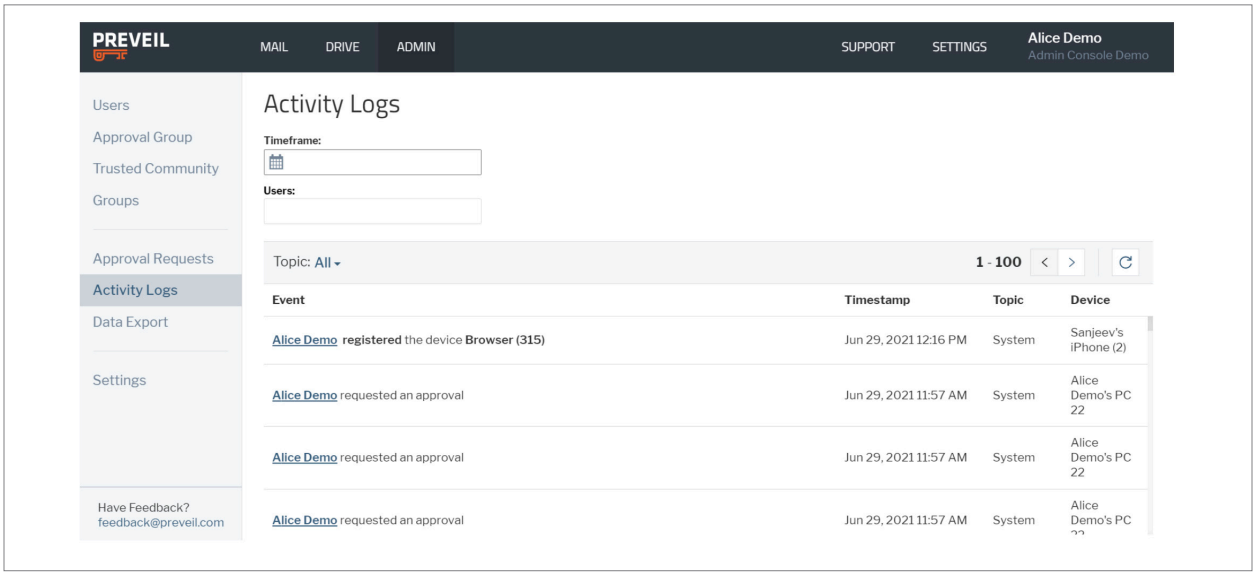
PreVeil protects logs and enables constant activity monitoring

Sophisticated hackers regularly thwart administrators' best efforts by covering their tracks. They tamper with activity logs and move undetected inside devices and networks, sometimes for months or even longer as in the SolarWinds attack. This unchecked access increases the potential for losses and damage.

Consistent with Biden's Executive Order, which calls for federal requirements for "robust and consistent logging practices," PreVeil automatically logs all actions using cryptographic techniques similar to those used in blockchains to ensure that log entries are tamper proof and cannot be deleted. The logs allow visibility throughout the network and its devices, enabling constant monitoring and assessment of the security status of organizations' data as specified in the NSA's *Zero Trust Guiding Principles*.

PreVeil's logging system also raises alerts in critical situations, such as when data is accessed from a new device, cryptographic keys are transferred, or a request for privileges is submitted. Figure 4 shows an example of such an alert.

Figure 4: PreVeil protects logs and raises alerts to enable constant monitoring



Finally, in keeping with the spirit of Zero Trust, PreVeil urges readers to not just trust us. Instead, we encourage you to verify for yourself that PreVeil's Zero Trust architecture and end-to-end encryption offers the cybersecurity your organization needs to protect its assets and do business with the DoD. To that end, PreVeil fully discloses how its platform works, which any reputable Zero Trust system does—including Signal, for example. PreVeil offers a detailed description of its architecture in its *PreVeil Security and Design: Architectural Whitepaper*, available to anyone for inspection.

PreVeil: Compliance with DFARS, ITAR, NIST and CMMC

PreVeil's modern Zero Trust security features and end-to-end encryption enable defense companies to achieve a high degree of compliance with DFARS 252.204-7012, NIST 800-171, ITAR 120.54, and CMMC Level 3. As enforcement of NIST 800-171 is ramped up, and the DoD's new security framework CMMC is rolled out, compliance is essential to completing ongoing defense contracts and winning new ones.

Key compliance attributes of PreVeil's platform include:

- FedRAMP Baseline Moderate equivalent
- Data encrypted and stored on FedRAMP High AWS Gov Cloud
- FIPS 140-2 validated cryptographic modules for encryption

PreVeil has several resources that provide detailed background and information on the fast-changing landscape of compliance and its ramifications for defense companies. For example, our paper on complying with CMMC, which offers a clear summary of CMMC and tips on how to get started on your organization's CMMC journey, has been downloaded more than 1,500 times by defense subcontractors and their primes, and is updated regularly.

Links to the CMMC paper and other relevant resources are provided at the end of this brief.

PreVeil: Simple and affordable

PreVeil leverages a fundamentally better security paradigm grounded in Zero Trust principles. But better security isn't enough: if security is difficult to use, it won't be used. PreVeil was created with this principle in mind so that your security objectives will be met.

PreVeil is affordable too—a particularly important factor for small- to medium-size defense contractors, who often don't have the resources and skills to build the secure systems they need. Hackers know this and frequently target such companies, but PreVeil helps to turn the tables on that tactic by offering world class security at low costs.

PreVeil is simple and affordable by design:

PreVeil Email and Drive deploy easily as an overlay system, with no impact on existing file and email servers, making *deployment and configuration simple and inexpensive*. Deployment can be completed in a matter of hours.

PreVeil is *easy for users to adopt* because it works with the tools they already use: PreVeil Drive's file sharing works like OneDrive and is integrated with Windows File Explorer and Mac Finder. PreVeil Email seamlessly integrates with Outlook, Gmail, or Apple Mail clients. Users can keep their regular email address.

Given its ease of deployment and use, PreVeil is *cost effective*. It need be deployed only to employees handling CUI, whereas alternatives require deployment across entire organizations. Savings add up—for CMMC Level 3 compliance, for example, PreVeil costs approximately *75% less than* GCC High and so is affordable even for small- to medium-size defense contractors.

Conclusion

The increasing cadence of high profile cyberattacks such as SolarWinds, Microsoft Exchange, and the Colonial Pipeline have led to more cybersecurity-related regulation across key sectors, including defense, healthcare, finance and education. Yet too often responses focus on achieving checkbox compliance with new regulations rather than addressing the fundamental weaknesses that led to the need for additional regulations in the first place. Our hope is that widespread adoption of a Zero Trust mindset will change that dynamic.

A Zero Trust mindset never trusts any user or device and assumes that network and data breaches have already occurred or will at some point. Zero Trust communications and collaboration systems are designed and managed from that vantage point, elevating cybersecurity to levels essential to protecting emails, files, and other data assets against sophisticated cyberattacks including, importantly, those supported by state actors.

To learn more about how PreVeil's state-of-the-art Zero Trust platform can help improve the security of your organization's communication and collaboration system, please access the compliance resources listed below and contact us at preveil.com/contact or +1 (857) 353-6480.

THE FUTURE IS HERE: SIMPLE AND SECURE MESSAGING SYSTEMS

Zero Trust principles aren't theoretical constructs. Millions of people worldwide use WhatsApp and Signal, which, like PreVeil, implement Zero Trust principles by using end-to-end encryption and limiting communications to approved individuals. These state-of-the-art platforms are simple to use, as evidenced by their seamless functioning and massive popularity. Moreover, WhatsApp and Signal are free, as is PreVeil for individuals. For enterprises, PreVeil is remarkably affordable—and because its platform secures data and file sharing as well messaging, PreVeil also tackles admin and activity log vulnerabilities.

PreVeil CMMC, DFARS, NIST and ITAR compliance resources

- *Complying with the Department of Defense's Cybersecurity Maturity Model Certification (CMMC 2.0),* which offers a clear summary of CMMC and tips on how to get started on your organization's CMMC journey. This paper has been downloaded more than 1,500 times by defense subcontractors and their primes, and is updated regularly.
- *Case Study: Defense contractor achieves 110/110 score on NIST SP 800-171 DoD audit.* A defense contractor using PreVeil as an overlay to its existing O365 Commercial system for all its users handling CUI achieved the highest possible score of 110 on a NIST SP 800-171 DIBCAC audit. This case study explains how the contractor got it done.
- *NIST SP 800-171 Self-Assessment: Improving Cybersecurity and Raising your SPRS Score.* The DFARS Interim Rule mandates that NIST 800-171 self-assessment scores be reported to the DoD, and it stands to reason that higher scores will win more contracts. This brief shows how PreVeil can help raise your self-assessment score by nearly 40 points.
- *Securing the defense supply chain: Helping your subcontractors comply with DFARS, NIST and CMMC.* The DFARS Interim Rule released in December 2020 has placed responsibility for subcontractors' compliance with DFARS, NIST and CMMC squarely on the shoulders of their contractors. This brief helps contractors accelerate their subcontractors' compliance efforts.
- *Getting Started with NIST SP 800-171 Compliance in Higher Education.* The US Department of Education, following the lead of DoD, is ramping up enforcement of NIST 800-171 requirements to protect federal student aid data. This brief outlines steps for universities to take now to achieve compliance.
- *PreVeil's End-to-End Encryption Enables ITAR Compliance.* New State Department guidelines exempt ITAR-restricted data from federal regulations when that data is secured using end-to-end encryption that meets standards specified in FIPS Publication 140-2. This brief explains the new guidelines and how PreVeil meets them.

To access additional briefs and resources, please visit PreVeil's resources page.

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.

PREVEIL

April 2022