PREVEIL

Trusted Communities:

Restoring trust and security to business email

Trusted Communities: Bringing trust and security back to email.

Email is the most widely used tool for business communications. It is also the most frequent target of cyberattacks. For CIOs and CISOs, protecting their organization's email is particularly challenging because hackers have exploited the open nature of email and made it their favorite tool of attack. Phishing and spoofing emails are routinely used to compromise not only individual user accounts and passwords but also IT administrators and servers.

The open nature of email also makes it virtually impossible to restrict attackers' access to targets. Faced with this paradox, organizations have deployed a variety of stopgap security tools. They have even resorted to training employees to not trust email. Yet the breaches continue unabated.

What is one to do? This e-book describes a new capability called **Trusted Communities** which uses encryption and a walled garden of trusted users to provide extensive and fundamental email security. Trusted Communities protects organizations against phishing, spoofing, admin compromise and server attacks, thus restoring trust to email.

Trusted Communities

noun

Def: A platform which augments the security of existing email and file sharing by providing employees with a secure channel that is insulated from phishing, spoofing and Business Email Compromise (BEC) attacks. Sensitive data sent through this channel stays secure even if individual user passwords are stolen, IT admins are compromised and servers are breached.

The challenge of email security

Email attacks can be understood by focusing on three main areas:

Attacks on users enable criminals to compromise and access users' content. These type of attacks also compromise individual passwords and enable account impersonation.

Attacks on IT admins, who have broad access privileges, can compromise the emails and security of the entire organization.

Attacks on servers result in the loss of large amounts of stored emails. Potentially, multiple organizations can be compromised with such an attack.

We will look at each of these challenges separately and discuss how Trusted Communities can work to resolve the challenges.

91% of cyber attacks begin with an attack on individuals' emails.
-Digital Guardian

Malicious or careless insiders can easily use administrator privileges to gain unlimited access to the network. Cybercriminals, who know all about administrator credentials, can crack weak or standardized administrator passwords to break into your system.
-Security Intelligence

In 2017, the Equifax data breach enabled hackers to steal 145 million records by exploiting vulnerabilities in the server software. As of 2018 – a year after the patches were released - 7 tech giants still haven't updated their servers.
-ZDNet

Go Phish – Attacks on the user

Organizations deploy a variety of solutions to protect their emails yet their emails remain vulnerable. This vulnerability remains because attackers have numerous tools in their arsenal to breach email accounts:

- **Password compromise:** Most email systems use passwords as their first line of defense, which also means they are the first point of attack. Passwords are a weak technique for authenticating a user's identity because they can be easily guessed or stolen. Worse still, once compromised, passwords can be used to access user emails from anywhere in the world. Attackers are able to guess user passwords through dictionary-based attacks. They are also able to purchase passwords on the dark web or trick users into revealing them using phishing schemes. Some enterprises believe that the use of two-factor authentication (2FA) can stop an attacker from compromising an account. However, sophisticated attackers routinely bypass 2FA.[1]
- **Phishing:** One of the most common techniques used by attackers is phishing. When criminals phish a user, they typically send an email to trick the recipient into doing something such as giving up their password or downloading malware. Despite the best efforts of an IT organization, phishing attacks almost always succeed.
- **Spoofing and Business Email Compromise (BEC):** Since email systems do not have effective means of establishing a sender's identity, attackers can easily spoof legitimate users. This is achieved by using an email address that is very similar to the one used by the real user. The goal is to trick the recipient into revealing sensitive information. Once attackers have spoofed someone in the company like a financial officer or CEO, this identity can then be used in a BEC attack to request other employees' personal identifying information, payment for fake invoices or money transfers.

1 – The highly respected security writer Bruce Schneier recommends Stuart Schecther's blog on *Before you Turn on Two Factor* to understand the pitfalls of using 2FA.

Attackers at bay- Protecting the user

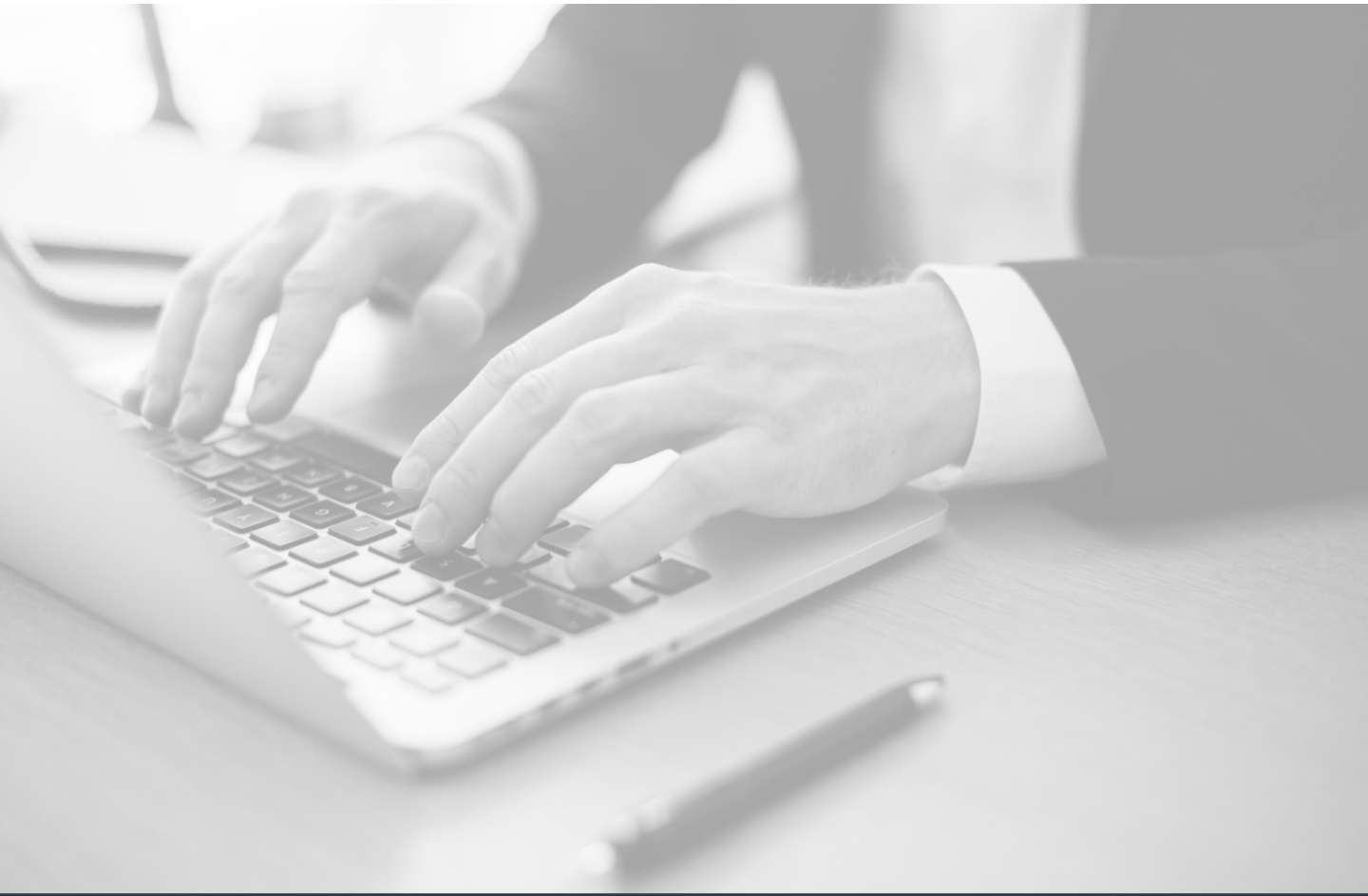
Protecting a user's email account is a virtually insurmountable challenge because a legitimate contact and an attacker can both deliver their email to the same inbox. The user is also unable to easily determine the integrity of the email's content. Compounding these vexing issues is that the user doesn't know if their account has been compromised and is being accessed remotely. Plugging these fundamental holes in email security demands a fresh perspective.

- The **first step** in improving email security is **eliminating passwords**. Instead of passwords, the email account should use an encryption key, called a 'User Key' to establish the identity of the user. The User Key should only be stored on the user's devices that they will use to access their account. Such a system has numerous benefits:
    - Unlike passwords, the User Key cannot be guessed. Based on 256-bit encryption, the User Key has more possible combinations then there are atoms in the universe.
    - The user does not need to know nor remember their User Key since it is stored on their device.
    - Attackers cannot access a user account remotely because it's only accessible via the User Key.
    - User Keys act as an incontrovertible means of establishing the sender's identity.
- The **next step** in improving email security is blocking attackers from communicating with the user. If the attacker cannot communicate with the user, they cannot deliver their malicious phishing or spoofing email. This can be accomplished by starting from scratch with a second inbox and selectively **whitelisting** trusted individuals or third parties for communication. This restriction enables the formation of a **trusted community** of people within the user's own organization as well as partners, suppliers and other trusted individuals outside of the organization.
- **Finally,** the secure email system should use **end-to-end encryption**, the gold standard for encryption which ensures that only the sender and recipient can read the email. Attackers will be unable to log into a user account remotely and with end-to-end encryption, the email will be tamperproof and secure throughout its journey from sender to the recipient. Even if the email server is breached, the attacker will only get encrypted gibberish.

Attackers at bay- Protecting the user (continued)

An elegant way of implementing all the elements described above in an easy-to-use manner is by creating a trusted email inbox with the user's existing email address. This inbox would only be used to send and receive end-to-end encrypted emails from other trusted users. This Trusted Inbox could be implemented and seamlessly integrated with popular email clients such as Microsoft Outlook or MacMail so that the user continues to use email just the way they are used to.

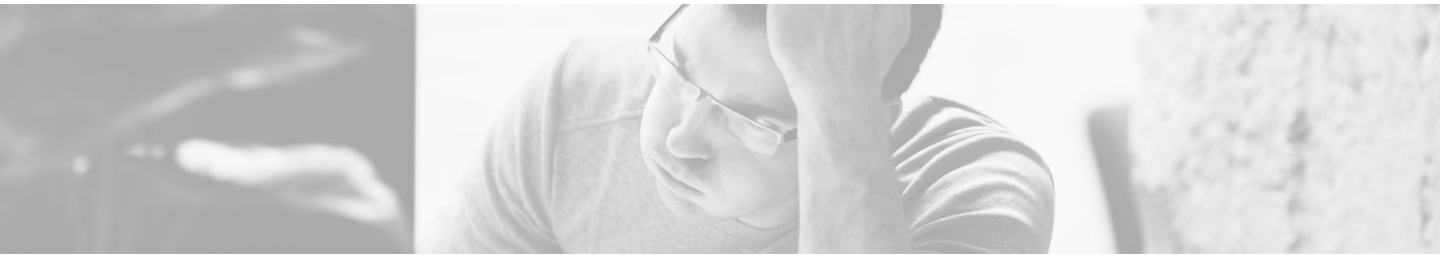
The Trusted Inbox would also sit alongside the user's unsecure email account and have the same email address. This works much like the popular messaging service iMessage which exists alongside non-secure SMS Text messages, but uses the same phone number and messaging application.



Keys to the kingdom = Administrator compromise

Administrators are also targeted by techniques similar to those used on individuals such as phishing, spoofing, BEC attacks and password guessing. Admins are a central point of attack because they have the proverbial keys to the kingdom and this super-user status gives them access to everyone's files.

Additionally, by enabling admins to have total access, the organization also makes itself vulnerable to unintended as well as rogue attacks. Organizations such as the Democratic National Committee[2] (DNC) and Deloitte[3] were compromised by attackers who gained control of the organization by compromising a single employee. In the case of the National Security Agency[4] (NSA), the organization was compromised by Edward Snowden who went rogue.



EXAMPLES OF ADMIN COMPROMISE

2 - Russian hackers, affiliated with the GRU, infiltrated DNC network servers as early as April 2016 and gained access to the email accounts and computers of party officials. The GRU initially used various online fake personas to craft "spear phishing" emails to trick high profile campaign leaders into clicking on links that enabled the hackers to obtain login and password credentials. The attackers then were able to put X-Agent malware to track keystrokes of at least one individual with admin-level access to gain privileges to DNC servers.

3- In September 2017, Deloitte was hit by a major cyber attack that compromised its email system and certain client records. Hackers compromised the confidential emails and plans of some of its blue-chip clients and transferred or copied a significant amount of confidential data. According to security expert Brian Krebs, the hack involved "the compromise of all administrator accounts at the company as well as Deloitte's entire internal email system"

4- In 2013, Edward Snowden compromised the National Security Agency (NSA). Snowden was one of about 1,000 system administrators who helped to run the agency's networks. He leaked classified details about NSA surveillance programs to the press .

Restoring trust

Reestablishing trust in the security of the administrator requires CIOs and CISOs to reconsider the paradigm of how administrators are privileged. In most organizations, admins are given superuser privileges to perform privileged activities such as accessing user emails and initiating eDiscovery. However, this also makes the admin vulnerable to serious cyberattacks because an attacker can compromise the entire organization by breaching a single admin. These opposing requirements can be elegantly addressed in a trusted email system by cryptographically distributing trust between multiple admins.

Distributed trust is a concept similar to the distribution of nuclear launch keys which prohibit any one individual from initiating a nuclear attack. Trust from a centralized authority is eliminated and instead given to a trusted group so that no single person can initiate a launch.

Similarly, by distributing trust among admins of an organization, multiple individuals are required to provide their **cryptographic approval** before an Admin can perform a privileged activity. If a single admin is compromised, a privileged activity cannot take place.

In a typical organization, if an attacker compromises a single admin, the attacker compromises the entire organization. However, by distributing the trust or authority among a set of individuals, the admin is no longer a central point of attack which provides a strong security guarantee for the organization.

Can't patch them all - How servers are compromised

Conventional email and file sharing systems store emails and files on servers. IT and security teams deploy all kinds of protections to prevent hackers from getting to the servers but these measures are inevitably thwarted.

The reason for attackers' success is that there are thousands of vulnerabilities that can be exploited to compromise servers, ranging from software bugs in server code to administrator compromise to vulnerabilities in firewalls. These weaknesses plague the server's integrity and even if patches are produced, the updates to servers often lag. Through these weaknesses, access to the servers is enabled.

There is no way to keep attackers from your servers 100% of the time. Eventually attackers will find a chink in the armor and get through. And, once an attacker compromises a server they get full access to all the stored emails and files on the server. Whether companies are using on-premise servers or farm out storage to the cloud, servers are equally vulnerable.

Attacks on the server provide the mother-lode in terms of valuable information. Yahoo[5] and Siemens[6] are well known examples of incidents where email servers have been successfully breached. As was seen in these attacks, server compromise had catastrophic consequences for the organization.

EXAMPLES OF SERVER COMPROMISE

5 – In August 2014, approx. 500 million Yahoo accounts were compromised. Names, email addresses and passwords were breached. The hack began with a spear-phishing email sent in early 2014 to a Yahoo company employee. The successful attack enabled the hacker to start poking around the network, where he looked for two prizes: Yahoo's user database and the Account Management Tool, which is used to edit the database. He soon found them.

6- In June 2014, Chinese hackers compromised a Siemens server containing all user password hashes. The hackers then used that information to log into Siemens servers using a network admin's user credentials (along with other users) and stole 407GB of IP spanning Siemens Energy, Technology, and Transportation business.

No more whack-a-mole

Securing the server might seem like a game of whack-a-mole as new vulnerabilities are constantly popping up and challenging the security of the server. It is almost impossible to protect against every known weakness and new weaknesses are constantly uncovered. Additionally, admins can potentially be compromised at any point. Bringing trust back to servers is perhaps the most challenging proposition for reestablishing trust for the email community.

However, with end-to-end encryption, email and file data on the server always remain encrypted and unreadable by attackers. If the data on hacked servers represent no value to criminals due to encryption then the whole act of hacking servers becomes pointless. Even if hackers breach the server and access all the stored emails, all they get is gibberish.

End-to-end encryption defines the gold standard for data security. Only the user's device and the device of message recipients can authenticate identity and decrypt messages. The server never has access to decrypted data. Data remains secure even when breached.

A new day for trust

If we combine the capabilities defined in this e-book for protecting the user, protecting the admin and securing the data on the server, we have established the basis for a **Trusted Community**. Together, these techniques allow the users to securely communicate and collaborate with others without concern that their information will be hacked.

- Trusted Communities require starting from scratch with a secondary inbox. From this point, admins can then enable **whitelisting** of trusted individuals. Whitelisting restricts email to only allow messages from fellow employees, contractors or third parties the enterprise trusts. As a result, email exists in a walled garden, cut off from potential attackers. Users cannot be victims of phishing and spoofing attacks.
- True Trusted Communities also result from the use of public-key cryptography. Since a private key is used to authenticate user identities, **passwords can be eliminated**. Consequently, criminals cannot steal identities and instigate BEC attacks.
- **End-to-end encryption** is a vital component of Trusted Communities. Through end-to-end encryption, emails and files are protected and remain private even when user passwords are stolen, admin accounts are compromised and servers are breached. If criminals hack your account, all they get is gibberish.
- **Distributed trust** represents a key component for Trusted Communities because it ensures that admins cannot become a point of compromise. Trust is divided among the admins of an organization and can only be established if users provide their cryptographic consent. Privileged activities remain secure.
- Finally, by creating a **trusted email account** with the user's regular email address and making it accessible from their existing email application such as Outlook or G Suite, the user has the last necessary element to enable a Trusted Community. A Trusted Community augments existing business solutions by making encryption easy for employees to use and ensuring the secure email account becomes a fluid part of email's workflow.

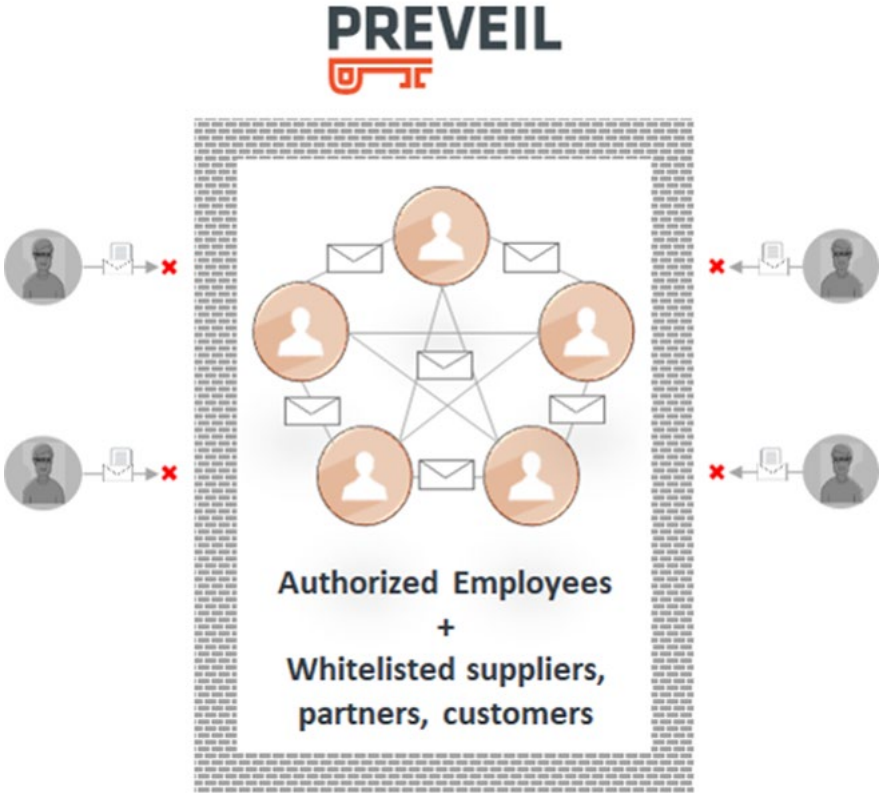
No single element from the above taken in isolation suffices to provide a Trusted Community. Instead, all of the above are required for a Trusted Community to exist. Only in conjunction can these elements provide a secure method for communication and file sharing that eliminates phishing, spoofing and BEC.

PreVeil = Trusted Community for the Enterprise

PreVeil understands the challenge email and file sharing pose to today's enterprises. PreVeil's answer to these challenges is providing users with a Trusted Community for email and file sharing, which brings security to these enterprise functions.

PreVeil allows users to implement its software solution on top of existing Outlook and G Suite user interfaces and doesn't require companies to switch to a new platform. Companies can choose to use PreVeil in specified pockets of the organization that might be responsible for sensitive IP or financial data. Alternatively, the whole enterprise can adopt the PreVeil solution.

When users adopt PreVeil, they are assured of having the gold standard of end-to-end encryption, and the ability to create a locked-down Trusted Community for their enterprise.



Ready to start trusting email again?

Bring confidence and trust back to your email and file sharing solutions. PreVeil over the elements. Contact PreVeil today.

CONTACT US

About PreVeil

PreVeil makes encryption usable for everyday business. PreVeil's encrypted email and file sharing services enable the creation of "Trusted Communities" for an organization's most security sensitive partners, suppliers, and customers.

PreVeil replaces insecure passwords with transparent cryptographic authentication, insulating users from phishing, spoofing and business email compromise attacks. Our patented Approval Group features minimize the threat of a single compromised admin putting an entire organization at risk. All messages and documents are encrypted end-to-end, which means that nobody other than intended recipients – not even PreVeil – can read the data.

The RESULT: Trusted Communities comprised of white-listed organizations and individuals who communicate via their favorite email platforms (like Outlook), using their regular email addresses.

Learn more about how PreVeil is transforming data protection at www.preveil.com