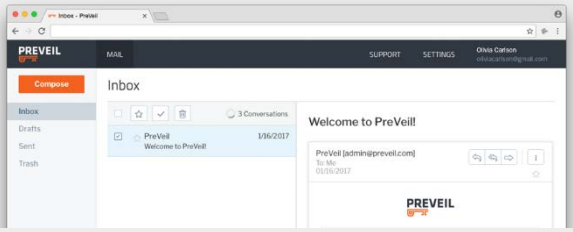
PreVeil. Finally, enterprise encryption end-users love

PreVeil protects your data even when user passwords are stolen, admin accounts are compromised or servers are breached. Fundamentally, PreVeil provides users with better data protection and privacy, combined with a seamless end-user experience and minimal IT overhead.

PreVeil is an easy-to-use encrypted email and file sharing app with powerful enterprise features

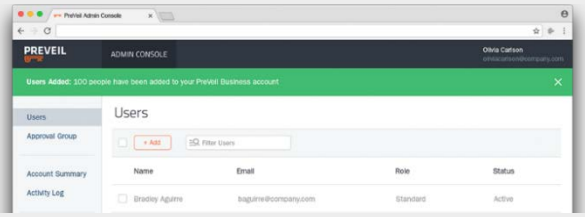
PreVeil Drive

Users can easily store, sync and share files – both internally and with 3rd parties – while maintaining security with end-to-end encryption.



PreVeil Email

Protect emails with end-to-end encryption, using seamless integration into Outlook, Mac Mail and mobile devices.



Admin Console

Provision and manage user accounts, access corporate data when required, and monitor logs. Optional integration with Active Directory.

PreVeil security principles and benefits

Unparalleled Ease of Use

PreVeil easily integrates with Outlook and Mac Mail. Ultimately, this makes it simple for IT to implement and easy for employees to use.

No Passwords = Reduced attack surface

Account access is protected by private keys stored on users' devices. Accounts remain secure, even when passwords are stolen.

Protecting Privileged Admin access

PreVeil cryptographically distributes privileged access across a pre-determined set of admins. Consequently, IT can gain access to corporate data, without creating a single point of failure.

End-to-End Encryption. Security's gold standard

Only desired endpoint devices can access user data. No server can ever access your keys. Neither PreVeil nor attackers ever see your data.

PreVeil for the Enterprise. Ensuring enterprise encryption without compromise.

The Privileged Access Paradox

Corporate IT and Security teams face a unique security challenge: Their job mandate requires superuser privileges in order to access employee files and emails. Yet this creates significant risk that a single compromised admin account could provide attackers with the keys to all corporate data.

PreVeil's patented Approval Groups™ technology solves this paradox. With Preveil, Privileged Access is cryptographically distributed across a pre-determined set of administrators. This ensures that a hijacked admin account cannot compromise the organization. And yet, IT has a mechanism to easily complete required Corporate Governance functions in addition to provisioning and managing the User Base. All this functionality is available to IT / Security teams, while maintaining ease of use.

Corporate Governance

E-discovery

PreVeil provides end-to-end encryption for employees' emails and files. Yet, at times, due to the demands of litigation or investigations, admins need to access this very data. PreVeil cuts through this challenge with its E-Discovery capabilities. In combination with PreVeil's patented Approval Groups™, PreVeil's e-Discovery module enables this level of investigation without creating a hole in a company's security. This solution requires a pre-defined number of individuals to cryptographically consent before e-Discovery can take place.

Encrypted Logs

Within PreVeil, every user and admin action is hashed and cryptographically logged. This provides organizations with full visibility into user activity, file modifications, key transfers and alike. Logs are fully auditable, encrypted and tamper proof.

Provisioning and Managing the User Base

Device Management

In a world of BYOD, admins need to have the ability to lock down email accounts and limit access to files on devices that have been lost or stolen. With device management, admins can cryptographically lock specific devices and/or accounts and make them inaccessible. At the same time, users' emails and files remain intact and are never deleted.

Bulk provisioning and deprovisioning

When it comes to onboarding dozens or hundreds of users with a new software solution, admins are frequently challenged by the need to create accounts for each individual in the company. Bulk provisioning enables admins to create PreVeil accounts for the entire organization by simply uploading a CSV file containing the employees' names and emails.

Rekey

In the event a user's device has been compromised or stolen, admins need to leverage device management to lock the account and to access rekey to create a new key pair. Rekey enables admins to create a new and unique public/ private key combination, allowing users to once again access their emails and files. The original public/ private key pair is decommissioned and is no longer associated with the employee's personal email and files.