



# Introducing PreVeil SIEM Connector

PreVeil's secure Email and File Sharing platform logs all User, Administrator and System activities for review and analysis. Logs are cryptographically secured which ensures they cannot be altered or deleted and offer an immutable history of PreVeil system activities. Logs are available to Administrators via the PreVeil Administrative Console and can be decrypted and exported when needed for more detailed analysis.

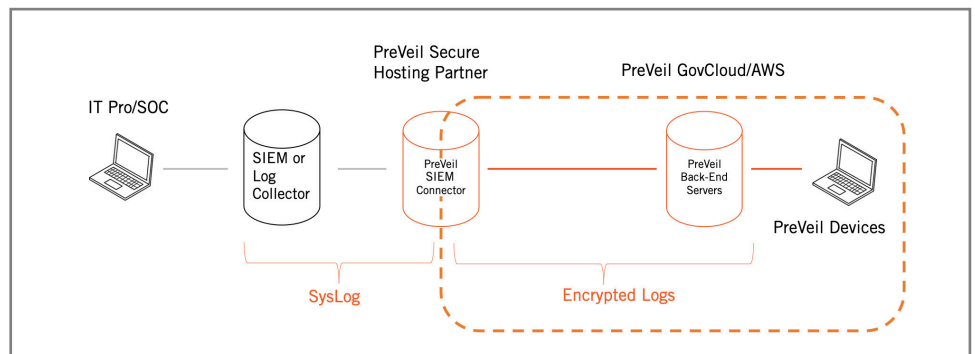
With PreVeil's SIEM Connector tool, customers can access PreVeil logs using their existing SIEM and add real time, automated alerts and monitoring of PreVeil logs via their SIEM. With this capability, account holders can bring rapid visibility to suspicious activities and behaviors.

## Value

Defense contractors addressing NIST 800-171 and CMMC Level 2 compliance requirements must periodically analyze logs of systems that touch CUI. The new PreVeil SIEM Connector enables system managers to easily decrypt and ingest logs generated by the PreVeil platform into a SIEM. This allows for rapid review of PreVeil events and correlation of PreVeil system events with irregularities or potentially malicious activities detected in logs from other systems.

## Architecture

PreVeil's SIEM Connector automates the conversion of PreVeil system logs into a standard (Syslog) format that is then transmitted to the SIEM. PreVeil provides full support for the SIEM Connector environment.



### Sample logs

PreVeil System	PreVeil User	PreVeil Admin
Account creation	Share data	Org create
Invitations to join	Move data	Approval group actions
Lock/unlock device	Delete data	Approval group changes
Re-key actions	Access data	Invite user
Delete device	Device info	Delete user
Respond to approval request	Accept share	Update/promote user
	Delete email	Trusted community changes

To learn more about how PreVeil can help, contact us at [preveil.com/contact](https://preveil.com/contact) or +1 (857) 353-6480.