solarwinds

Passportal Data Protection in Transit and at Rest

APPLICATION

Your new password records are input to the internet browser on your computer. From there they are protected in transit by 2048-bit RSA keys, and at rest using over 300 different rounds of 256-bit symmetric encryption, with six different randomly generated keys. Your unique encryption key (organization key) is the final step in unencrypting your data for view within the browser.

1. 

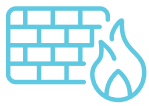
ORGANIZATION KEY

Two of the encryption keys used are unique to each password record, and one of the encryption keys called the Organization key is created and stored only on the MSP side. This encryption key is never stored or maintained anywhere within the Passportal infrastructure.

2. * * * *

PASSWORD AND PASSPHRASE TRANSMISSION

All inbound and outbound data communication traffic with the Passportal Cloud happens over TLS 1.2 using 2048-bit RSA keys to ensure the protection of your data in transit.

3. 

WEB APPLICATION FIREWALL PROXY

Unique encryption keys are retrieved from numerous sources for each password.

KEY SERVICE CLUSTER

- 256-bit symmetric encryption
- Password specific key

DATABASE CLUSTER

- Partner/MSP key
- Client key
- System key
- All internal transmissions happen over TLS 1.2

APPLICATION SERVICE CLUSTER

All encryption keys are generated randomly and used throughout the hundreds of rounds of encryption, while each password stored has its own unique key in addition to the other keys.

FULLY ENCRYPTED PASSWORD STORAGE