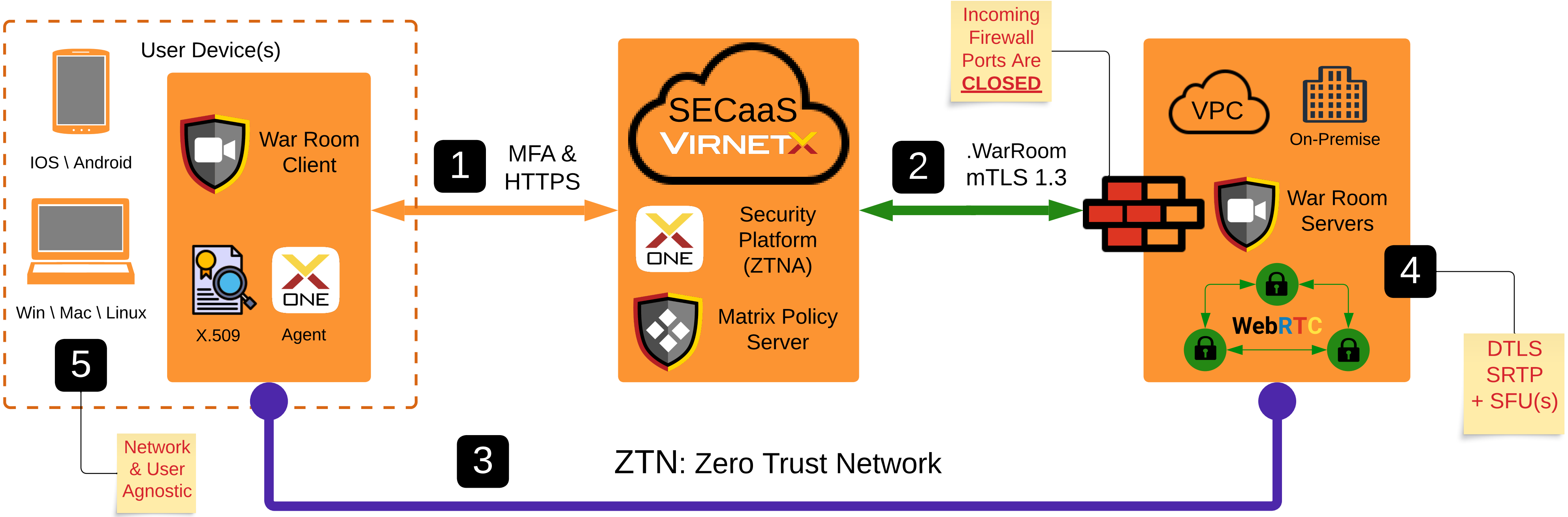
VIRNETX

HOW DOES WAR ROOM WORK?



1 War Room client opens and makes a secure HTTPS connection to the **VirnetX SECaaS Cloud**. VirnetX checks for software updates and does a compliance check to make sure the device has everything it needs to connect to War Room.

2 War Room uses the built-in VirnetX One Agent and VirnetX Matrix Server combining ZTNA, mTLS, SDNS and Admin Policies in order to secure connections from the War Room Client to the War Room Server environment **across organizational boundaries and from any network**. War Room provides a complete **hardened security platform** that you never have to see or manage!

3 The servers authenticate the user, their computing devices are validated by digital certificates (PKI), all network connections are ZTNA based and encrypted and these components adhere to **Zero Trust policies** that isolate them from unauthorized use. This secure construct is a **Dynamic ZTN (Zero Trust Network)**.

4 War Room Servers support WebRTC so application bit streams are encrypted. However **the bitstream is inside** the ZTN network that is also encrypted and thus **invisible to unauthorized users**. War Room **requires a ZTNA connection** and uses mTLS to connect to media servers where SFU's are implemented so the video \ audio quality is excellent even on low bandwidth networks.

5 All War Room meeting participants **must be** connected to the ZTN **prior to** joining a meeting. VirnetX **automates the process** of certificate installation, management, encryption, discovery and routing of data for all meeting participants **regardless of location**.

ZELERATION