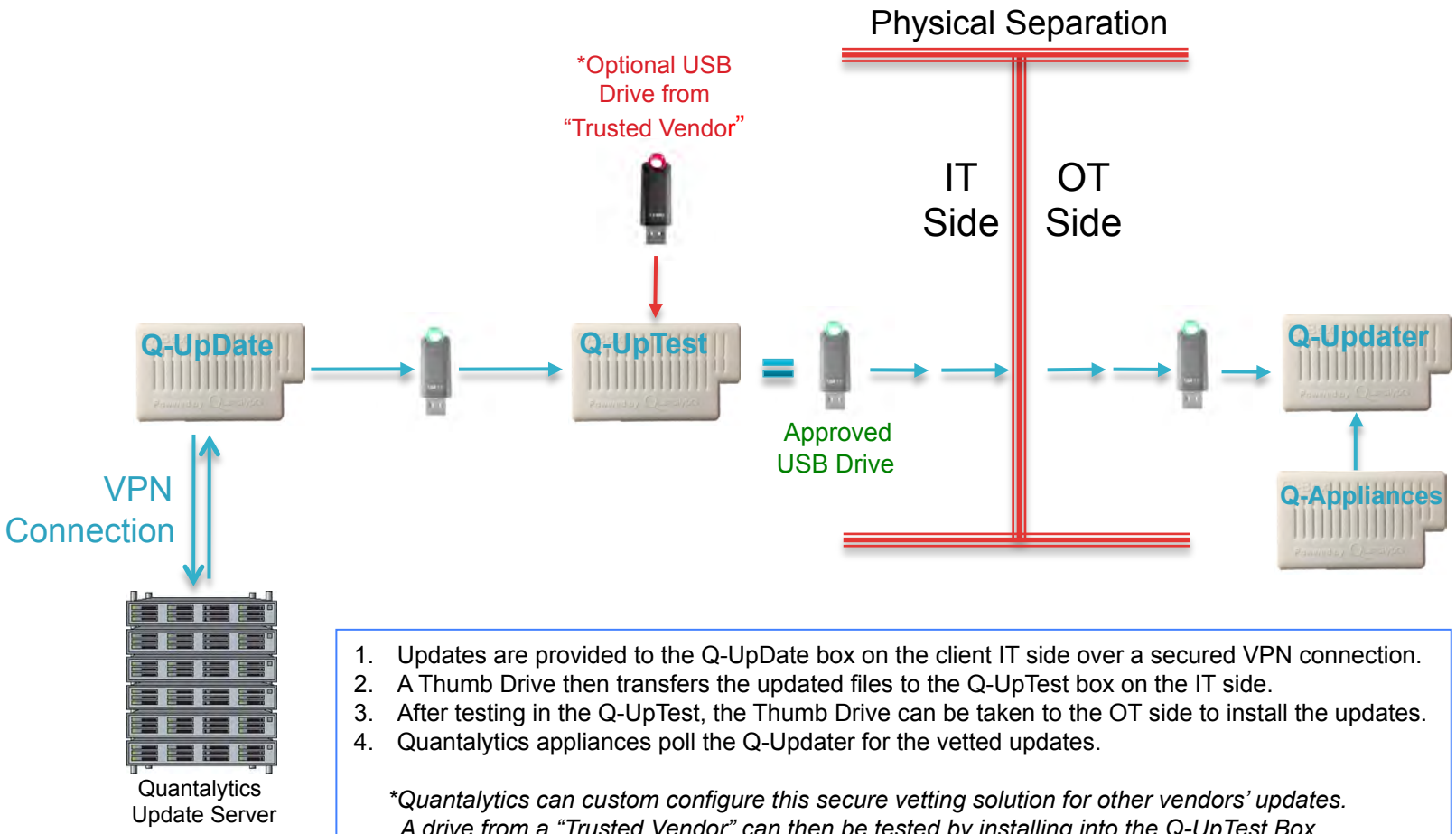
Overview for:
Q-Updating Solution
OT (Operation Technology Network)



1. Updates are provided to the Q-UpDate box on the client IT side over a secured VPN connection.
2. A Thumb Drive then transfers the updated files to the Q-UpTest box on the IT side.
3. After testing in the Q-UpTest, the Thumb Drive can be taken to the OT side to install the updates.
4. Quantalytics appliances poll the Q-Updater for the vetted updates.

**Quantalytics can custom configure this secure vetting solution for other vendors' updates. A drive from a "Trusted Vendor" can then be tested by installing into the Q-UpTest Box.*

Q-Updating Solution for Air-Gapped OT Networks

It is not enough to have appliances in place to defend the OT Network. For defenses to work over the intermediate and long term, the appliances need updating. Quantalytics has developed a secure, auditable and transparent solution to this otherwise intractable problem for air-gapped OT Networks - safely providing updates.

The **Q-Update** is an appliance that sits on a VLAN in the IT Network that communicates via VPN to Quantalyics's servers, and receives update packages. Alerts are given when a new update is available. A staff member inserts a thumb drive, which the Q-Update completely reformats before using, and copies the update package(s) to the thumb drive. The copying process is controlled via a web interface, and alerts are sent both when a copy process is begun, and finished. Every step is logged and auditable so as to determine which operator downloaded what package(s), and when.

The thumb drive is taken to the **Q-UpTest**, which is also on the IT Network. The update packages are validated. This means not only checking their hashes, but actually running the packages. By running the packages, the operator can confirm that they install correctly, or not. Again, notifications are sent, and fully auditable logs are created. The Q-UpTest provides quality control and assurance for updates, and guards against a physical man-in-the-middle attack, where a thumb drive may be altered after receiving update packages, but before being deployed.

Finally, the thumb drive is taken to the **Q-Updater**, which is on the OT Network. The operator uploads the packages through a web interface. The Q-Updater also performs validation testing on the thumb drive and the packages, again, to prevent a physical man-in-the-middle attack. The Quantalytics appliances on the OT Network query the Q-Updater, and when they find the appropriate update packages, download and install them. Every step in this update process is logged and auditable, and on the IT side, the Q-UpDate and Q-UpTest e-mail reports and warnings.

All Quantalytics appliances are internally hardened against hackers as an additional precaution. Among the steps taken: deploying ModSecurty, a Web Application Firewall, TinyHoneyPot for internal obfuscation, Fail2ban to block brute force login attempts, IPTables, and ClamAV for anti-virus protection. Two-factor authentication is available as an option.

The Q-Updater can also be customized to verify updates from approved vendors.

646-449-7810
info@quantalytics.com