SECURITY OVERVIEW

NETWORK SECURITY

All access to the web server through TLS HTTPS protocol passes through a PALO ALTO Firewall (Firewall Appliance) at the segmented DMZ network. This firewall also utilizes Wildfire IDS/IPS mechanisms for incoming and outgoing traffic to all networks.

SERVER SECURITY

The web server for production sits in the DMZ network. It is firewalled to allow only HTTPS traffic to the web server via the HTTPS protocol. Access to this server, other than HTTPS, is only given to authorized personnel in charge of managing the server.

The Database server sits in the internal network and does not have outbound or inbound internet access. The only access from the WA web server is through the firewall over a non-standard SQL port.

The servers are patched on an ongoing basis from a centrally managed patch management system. The patches and updates are scheduled and applied through the patch management process and procedures from the IT Server Management Team.

DATA IN TRANSIT

All data transmitted via the web browser to the WA Connect portal is encrypted via TLS AES-256 bit encryption. The servers are configured to connect over the highest level of the secure encryption ciphers via the TLS protocols.

DATA AT REST

All WA Connect data is stored in a database on the database server and is not stored on the web server. The database itself is housed on a NetApp SSD SAN Array. The NetApp SSD SAN Array utilizes the Full Disk Encryption protocol with self-encrypting drives and AES-256 bit encryption. The backup profiles and procedures are SAN Snapshots and password protected backup files stored on the NetApp SAN. An audit trail of all transactions and transactional data is stored in the system by username and IP address for accountability.

A/V SOLUTIONS

All servers, either in DMZ or internal networks including all workstations in the enterprise, have a centrally managed a/v solution installed and managed. All servers have an additional layer of protection with visibility of all processes being run in real time, which includes processes that are run in memory. This extra layer of protection helps uncover and protect from advanced threats and malicious internet connections. This layer also sends notifications of any suspicious activities or processes that might be running on this web server.

All files uploaded into WA Connect and scanned in real time from an updated A/V engine that detects malicious file uploads and cancels the upload if a malicious or infected file is detected.