Security Features

Baseline VCL security for the end-user environments:

- The VCL environments are not generally shared. One user to one machine.
- After an environment is used - the machine is reloaded(sanitized) with the same or another golden environment. All residual data is destroyed or overwritten during the reload process.
- Images can be setup to allow the user to have either administrative access or unprivileged access by using the image profile meta-data. This is on a per image basis.
- When users hit the 'Connect' button on the vcl web portal. Their incoming IP address is captured and used as the scope for the windows OS firewall. The linux OS makes use ssh configuration settings.
- Default access methods: Windows is Remote Desktop Connection, Linux is ssh (secure shell).
- Unless VCL environments are tied into enterprise identity management service. The VCL environments are configured with a one-time use password for the session and only for that active session. For each additional reservation a new session password is generated. NOTE: This only applies to the VCL environments and not with the VCL web portal.

Additional security measures depend on how the images are created, such as windows group policies, SELinux settings for Linux based environments, VPN, and network level firewalls within the infrastructure where the VCL machines resides.