V2 Technical Questions

If your tech support could answer these questions for me, that'd be great. I have already answered the first part of 2, 7, and 10.

1. Is this a hosted or online subscription or is there a locally installed client application?
   Answer: It is hosted on a Datacenter's, it can be accessed from the browser or V2 application.
2. Is data stored in the cloud? If so, what type of data (HIPAA, CJIS, Personally Identifiable Information such as DL DOB or SSN)?
   Answer: Yes. The Data centers are periodically audited to comply with HIPAA, PCI, and SOC security standards. Also, these are some of the certifications held by the data centers: ISO/IEC 27001, PCI DSS, HIPAA, SOC 1 Type II and SOC 2 Type II, and STAR self-assessment.
3. If hosted, is the system TX-RAMP or FedRamp certified?
   Answer: No, at the moment.
4. If HIPAA, CJIS or PII, is the data encrypted in transit and at rest? If so, what type/level of encryption?
   Answer: Yes, in transit it is SSL/SSH with a minimum of 128-bits. On rest you can use BitLocker.
5. If HIPAA, CJIS or PII, can vendor provide a SOC report?
   Answer: Yes.
6. If HIPAA, CJIS, who all would have access to the encryption keys or unencrypted data?
   Answer: Only the owner/administrator and their users who are registered under V2 Cloud
7. *If hosted, do we or the vendor own the data if we no longer pay for their service?*
   Answer: CLIENT (YOU) DOES
8. If hosted, where are the data centers located?
   Answer: Yes, please check the following link.
9. If hosted, is the vendor externally audited?
   Answer: Yes, Data centers are periodically audited to comply with HIPAA, PCI and SOC security standards. Also we can provide you with the Business Associate Agreement (BAA).
10. *If hosted, who manages user accounts and account security settings?*
    Answer: END USER (BUILT INTO THE SOFTWARE AND CONTROLLED BY YOU.
11. If hosted, is Single Sign On available (Azure or OneLogin)?
    Answer: Yes, both.
12. Is there a cost for setting up Single Sign On?
    Answer: No.
13. Does this system include Multi Factor Authentication? If so, what methods?
    Answer: Yes, via email or with mobile authentication application.

Thanks,

Jon Denney

SAFE Software
(940) 367-2246

V2 Response:

Hello Jon,

I hope everything is well on your end. My name is Dan and I'm from the Customer Success Team.

You can tell to your client that all of our Cloud computers are hosted in OVH data centers. that are equipped with a fully redundant fiber network and power supply to provide maximum reliability and 99.95% SLA. The facilities are gated with restricted and logged staff access as well as 24/7 video surveillance. Data centers are periodically audited to comply with HIPAA, PCI, and SOC security standards. Also, these are some of the certifications held by the data centers: ISO/IEC 27001, PCI DSS, HIPAA, SOC 1 Type II and SOC 2 Type II, and STAR self-assessment.

Servers - All our servers run on the latest hypervisor updates with an all-inclusive UFW firewall for every virtual machine. To ensure data redundancy, we only use enterprise-grade NVMe drives with RAID-1 replication on all servers.

Networks - Every virtual machine comes with its isolated private network with no incoming port open. Firewalls and private networks between virtual machines can be configured from the management console. All public IPs have anti-DDoS protection included and connections to your office resources are made using site-to-site IPsec VPNs.

Connections - Connections to the Cloud desktops using the web and mobile app are encrypted using SSL HTTPS. Connections from the desktop application are made using RDP over SSH tunneling. All our apps support multi-factor authentication as well as SSO SAML integration. Furthermore, all connections are monitored with a lockout mechanism that is triggered after multiple failed login attempts. We do support and set up SSO in Azure AD, OKTA SSO, JumpCloud SSO, and Google SSO with V2 Cloud which is included in the Business Plans.

Backups - Our business plan includes daily snapshot backups with 7 days of retention. To ensure the data is immune to ransomware, we keep the snapshots offline in a secondary location. In case of a disaster, virtual machines can be recovered from a snapshot. Snapshots can also be used to recover individual files in case you or an end-user mistakenly delete them.

Antivirus - Our Business plan includes managed MalwareBytes Pro antimalware with real-time protection and nightly scans.

Kind Regards,