Frequently Asked Questions

1. **How much personal information will Entreda get when I enroll?**
   None. Entreda does not obtain any "actual" data. Only metadata is collected, which is data about data. In other words, there is no context and no personal information that Entreda has access to. What Entreda does obtain is information about your security settings. For example, Entreda knows if you have a password policy set, but obtains zero information about the actual password. As for the Cloud Drive and USB data leakage monitoring feature, if enabled, Entreda can see documents moving in and out of these applications and if they have been altered (for example the title of the document). However, Entreda is NOT able to view any context which actually resides in the document. Further, Entreda does not look at your browsing history or your email. Details of information gathered can be found in the Privacy Policy.

2. **Do I need the Entreda Applet on my home computer when accessing the office desktop? What if I am using Terminal services or VPN?**
   It is highly recommended that every device that accesses privileged information (either directly or indirectly) have the Entreda Applet installed. In fact, it is recommended that any device that is used for business usage should have the app installed. If the endpoint used is breached, then you are at risk. An example of this would be the endpoint you are using is not secure, and there is key-logging software installed on it.

3. **What about a device that only receives client info through my CRM app (for example: Redtail)?**
   Yes, any device which accesses, delivers or receives any privileged information should have the Entreda Applet installed.

4. **What constitutes as "business" use of a mobile device?**
   It is recommended to catalog any device that has access to privileged info (PII). If the device is used to access any client or business sensitive info (including email), then you should install the app. However, if you are only using your phone to make calls, then it is not needed.

5. **What is PII data?**
   Personal Identifiable Information – any data that could potentially identify a specific individual.

6. **Does my support staff also need the Entreda Applet installed?**
   It depends. Please see above.

7. **What if I have a device that I use temporarily, do I need the Entreda Applet installed?**
   Yes, any device that is used to access privileged information should have the app installed. Please see guidelines above.

8. **Are printers, scanners, fax machines devices that need to have the Entreda Applet installed?**
   Devices that are enrolled into the service include: Desktops/Laptops/Servers (Windows/Windows Server/ Mac OS) and Mobile devices (IOS/Android). Printers, scanners or fax machines are not enrolled into the service, but Entreda does monitor the network and looks for all devices that are on it.
9. **Where are Entreda's servers physically located? Is any data ever processed outside of the U.S.?**

No. All Entreda servers are based in the US, and run on Amazon Web Services (AWS). FINRA also uses AWS.

10. **Would Amazon cloud be considered secure then?**
    Yes, Amazon Web Services (AWS) is secure. In fact, FINRA also uses AWS.

11. **If you have an "entryway" into my computer, won't a hacker be able to piggyback on it?**
    No. Entreda doesn't have access to the device. All Entreda communication to/from your device is done through a secure connection.

12. **Is drive encryption required?**
    Mobile devices such as tablets, phones, notebooks and laptops must have their drives encrypted. For desktop devices (and servers), while not required, it is a good idea to have the drives encrypted.

13. **What disk encryption software do you recommend?**
    The Security Checklist FAQ provides a whitelist of approved applications for this purpose. The encryption will differ based on what type of OS the device is running (i.e. Windows uses BitLocker, and Mac OS uses FileVault).

14. **How does Disk Encryption remediation work?**
    Entreda Unify leverages the operating system's built-in support for disk encryption (Bitlocker in Windows and FileVault for MAC OS X). If a non-"business class" Windows operating system is used (home/basic version), user needs to upgrade their operating system to a business class operating system (the "business class" OS upgrade typically costs $99 per user).

    For users that are failing encryption, Entreda representatives will schedule calls with reps and remote into a handful of devices to configure disk encryption. As each environment is different, need to ensure sufficient data is gathered, before enabling automatic remote disk encryption.

15. **My business already has a managed service plan (IT provider) with a 3rd party. The 3rd party has their own agent installed on our PCs (Logmein, as well as an antivirus package). Is that all going to have to be removed and not used in order to comply with Entreda?**
    No. Entreda Unify is designed to work in conjunction with IT provider solutions. Entreda's solution should not conflict with other software agents used to monitor networks, end-points or applications. The primary purpose of the Entreda Unify app in such environments would be to provide a checks and balances (an independent 3rd party attestation) that your IT environment meets SEC/FINRA cybersecurity policies and provides real-time evidence reports to this effect. Additionally, as a side benefit, Unify provides a firm-level dashboard and cybersecurity risk score which can help you visualize your firm's cybersecurity posture in a single place.

16. **Are you forcing me into a sandbox where one of the potential "fails" is for not allowing Windows auto updates? I don't want to install all operating system updates.**
    No. The Entreda platform is built to make the customer aware of issues, it does *not* force the user to update, it just suggests they do so when the application detects there's an update, or a patch, that needs to be taken care of, with an option to update the patch in real-time. Further Entreda classifies the patches into two categories: "critical" and "optional." It is recommended that "critical" patches get applied immediately as these are typically security

related. “Optional” patches are not as critical and can be applied later at your discretion. Please note any device setting change (remediation) is an “opt-in” meaning that the user will need to accept the change from a prompt that appears on your device.

17. **If I have a bunch of "fails" due to things I view differently than Entreda (i.e., Window auto updates), won't this look bad on the report?**
    Entreda’s solution is designed to be customizable. You can create exceptions to Entreda’s “fail” methodology which would essentially prevent your worry of a “bad” looking report for this scenario. These exceptions are logged.

18. **How does the Auto-remediation feature work? Do apps get installed without permission? What about viruses & malware?**
    Every device setting change (remediation) is an “opt-in” meaning that the user will need to accept the change from a prompt that appears on your device. As part of the remediation process the application sends a prompt to the user with a “yes” or “no “option, allowing the user to decided. Whether or not the user accepts the remediation, this gets logged in the dashboard for compliance purposes. The auto-remediation feature only occurs if something is a “fail.” As part of the monitoring, Entreda makes sure you have anti-virus and anti-malware software installed to minimize exposure for viruses and malware.

19. **What auto-remediations are enabled by default?**
    All auto-remediations are disabled by default. Note: WIFI remediation (automatic VPN) is an optional feature.

20. **What are the default password policy requirements?**
    By default, the password policy settings are as follows for Windows & Mac OS :
    Password “complexity” (or “strength”) must contain at least 3 of the following elements:
    - Lowercase letter (a through z)
    - Uppercase letter (A through Z)
    - Numbers (0 through 9)
    -Symbols (#$%&, etc.).

    Password Length: Minimum of 8 characters
    Password Aging Policy: 90 days

21. **Are you able to see what my password is?**
    No. Entreda is unable to see the actual password, and instead checks what polices have been set on the device.

22. **If I don’t find any peer-to-peer (P2P) software in my applications, does this mean I don’t have any installed?**
    Not necessarily. Some applications get installed in different locations and may not necessarily be viewable from the applications section of your device. Entreda checks all locations and provides a comprehensives list of all applications installed. Further, if any P2P software is found, these will get flagged through a black-list that is constantly updated (details of which are in the Security Standards Checklist FAQ document).

23. **Does FINRA require penetration testing? I read that penetration testing is an extra service.**

It really depends on the size of your IT environment and configuration. It is a good idea to do penetration testing as a cybersecurity practice as it is an effective way to determine where your network vulnerabilities exist. The analogy to this is a firm conducting internal audits, periodically, to ensure the highest possible state of a firm's cybersecurity posture. Vulnerability Assessment and Penetration Testing is an extra service that Entreda offers and if this is something you are interested in, please contact Entreda.

24. **Do I need to be concerned with the performance of my device as the Entreda app is always running in the background?**
    Entreda has specifically built the Applet to run as a very light weight tool in the background. There are some general guidelines on the system requirements in the guidelines documentation, which are similar to other apps. However, if your device is already on the border of having insufficient resources, installing one more app will further exacerbate this. This can commonly be addressed by disabling start-up programs that are not being used

25. **How often does the Entreda Applet update and when is my broker dealer told about audit failures? Will my broker dealer be notified of every standard failure, or will we get a chance to fix most or all issues?**
    The Entreda Applet runs continuously in the back ground, and syncs in real time with the Unify web console. Both yourself and your broker dealer has access to the Unify Web Console. Typically, after a third flag there will be an escalation.

26. **Does Entreda do anything to monitor the security of our own office network or is it solely for the purpose ensuring that we have the right tools to make our interactions secure (such as watching for virus' running on my system)?**
    Entreda Unify ensures that your cybersecurity posture is elevated for devices, users and networks. Specific examples include items such as Operating System update settings/patches, password policies, software programs (such as Antivirus) and ensuring all are configured and/or running correctly, as well as making use of alternate secure networks. Entreda is there to provide "peace of mind" from an IT compliance perspective.

27. **My iPhone has a four-digit numerical password (and also a fingerprint passcode), are either or both of these acceptable?**
    Yes. It is essential to have some sort of authentication system in place on your mobile device (password, or fingerprint scanner) fingerprint would be the safer way to go, but either one is acceptable.

28. **Does Entreda have a list of suggested tools for bettering our security tools?**
    Yes, Entreda has a white list of vendors. These are detailed in the Security Checklist FAQ as well as the Compliance Summary document.

29. **Does Entreda conflict with webinar/screen sharing apps such as join.me or gotowebinar ?**
    No. Entreda does not interfere with any of these applications.

30. **Is Anti-Virus included with the Entreda app? If so, can I cancel my subscription?**
    The decision as to whether to keep your existing package is yours. Some clients prefer to use their own package. If you don't have an anti-virus package already installed, then Entreda will install a package.

31. How does Entreda screen employees?

Entreda has a strict policy requiring employees to submit a background check. Please note that as part of the engagement Entreda has gone through a due-diligence process already. A customer due-diligence package along with SOC reports is available upon request.

Note that Entreda does not obtain any "actual" data. Only metadata is collected, which is data about data. In other words, there is no context and no personal information that Entreda has access to. What Entreda does obtain is information about your security settings. For example, Entreda knows if you have a password policy set, but obtains zero information about the actual password. Details of information gathered can be found in the Privacy Policy.

32. Can I change the screen lock settings to be longer than 15 minutes on my computer?

A "passing" screen-lock setting, per SEC/FINRA guidelines, is defined as having the screen lock function enabled with a screen-lock timeout of 15 minutes (or less). If the screen lock is not enabled and/or the timeout is set to greater than 15 minutes, this is categorized as a "fail."

33. **Do I still need a router/firewall on premise at my office if my client device has its firewall enabled?**

Yes. The client firewall and on premise firewall/router serve different roles - both are required. Each provides a different layer of protection.

34. How can I separate my home office network between business and family/guest usage?

This can be answered in two ways:

- It is a good idea to segregate the networks if you have a home office as it can allow for increased privacy and security. The ability to do this will depend on the router. Essentially you'll want to have 2 different subnets. One for business and one for family/guests. However, as many home routers don't support different subnets or the ability to isolate networks, an alternate solution can be to setup a "double NAT" network (refer to: http://security.stackexchange.com/questions/76547/is-double-nat-a-secure-way-to-create-a-public-wifi-network). Your local IT person is best equipped to provide assistance on this.
- Alternatively, you can take advantage of the (optional) built-in cloud VPN/alternative network feature, which provides a secure session for your network access.

35. **What companies do recommend for file share? Is dropbox secure?**

Dropbox has poor security efforts as it is built as a consumer-based product so security is not one of their biggest concerns. We recommend cloud applications which are specifically built for businesses as they have more layers of security (examples include: Box, Citrix ShareFile NetDocuments). FINRA has list of companies that are approved. It is required that your file share should encrypt data at rest and in motion. Solutions like Dropbox, Google Drive and Symantec File Share are not compliant out of the box. If you use Google Drive or Dropbox and prefer to continue using these programs, you can sign up for a separate program called Boxcryptor to secure these.