Overview of Tamarac Security Controls

October 29, 2014

ENVESTNET®
Tamarac®

Contents

Introduction

Tamarac invests heavily in its data hosting, redundancy, security, and performance systems so you can focus on serving your clients and growing your business. All Tamarac applications are stored in world class SSAE-16 Type II compliant datacenters to ensure our systems are available and your data is backed up. This document describes the security controls in place, including physical, application, system, and operational security.

Certifications

Tamarac is SOC1 Type I/SSAE-16 certified.

Tamarac hosts its test and production systems at Rackspace Hosting datacenters. Rackspace Hosting is SSAE16/SOC1 Type II certified and undergoes annual audits.

Physical Security

Tamarac's datacenters are hosted in Elk Grove, IL (primary) and Reston, VA (failover).

Physical security controls in place include:

- Access is limited to Rackspace data center technicians (U.S. employees only).
- Biometric scanning is used for controlled access.
- Security camera monitoring and recordings are retained for one month.
- 24x7 onsite staff, providing additional protection against unauthorized entry.
- Tertiary fire suppression systems (extinguishers, FM200, dry pipe sprinklers).
- N+1 redundant UPS and backup generators to prevent brownouts, power outages, etc.
- Primary/backup HVAC to provide consistent temperature control.
- Picture IDs are used for all employees.
- Unmarked facilities to maintain a low profile.
- Audit logs to sensitive areas are reviewed regularly.
- Physical security is audited by an independent firm

Operational Security

Employee Security

Tamarac employees and key vendors sign non-disclosure agreements at hiring, which requires them to protect the confidentiality of Tamarac's and its customers' confidential information. Any offer of employment is contingent upon a background check and the applicant's consent and submission to a pre-employment drug test.

- **Background and Reference Checks.** Tamarac is committed to providing a safe environment for its employees and customers. It is also important that the company protect its funds, property, and other assets. Accordingly, the company has established hiring guidelines to ensure that we select employees who support our mission.

  Before an employment offer can be issued, each applicant must authorize Tamarac to check his/her background, including criminal history, Social Security Number, employment, education, references, and credit history, if applicable. All background checks are conducted in compliance with the federal Fair Credit Reporting Act and all other federal and state laws, and may include:

- **Social Security Number Verification**. An outside firm will confirm that the Social Security Number given by the applicant does belong to that person, and that it is not in use by any other person.

- **Employment Verification.** Tamarac or an outside firm may verify previous employment listed by the applicant, including dates employed, position(s) held, reasons for departure, eligibility for rehire, and performance information.

- **Education Verification**. Tamarac or an outside firm may verify education listed by the applicant, including dates attended, major(s), and degree(s) earned.

- **Criminal Record Check.** An outside firm will conduct a search of criminal records databases for each state and/or county in which the applicant has lived during the previous seven years.

  If a criminal record check shows evidence that the applicant has been convicted of a violent crime, or a felony financial crime for positions that include fiduciary responsibility and/or access to company funds or cash, within the previous seven years, the applicant will be denied employment.

  If an applicant has been convicted of another crime and has disclosed the conviction during the application and interview process, the company might still consider hiring the applicant. In such situations, the hiring decision will be made based on all of the information gathered about the applicant, including other background and reference checks and further information provided by the applicant. The hiring manager and Human Resources may also consider the nature and number of convictions, the dates, and the relationship that a conviction has to the duties and responsibilities of the position.

  If an applicant has been convicted of crimes that he/she did not disclose during the application and interview process, the applicant will be denied employment. Any decision to accept or reject an applicant with a conviction is solely at the discretion of Tamarac.

- **Credit Check.** An outside firm may obtain a credit report for applicants who are being considered for positions that include fiduciary responsibility and/or access to company funds or cash. Credit checks will be run only when there is a legitimate, job-related business need.

  If the results of the background check influence a decision to deny employment or withdraw a conditional offer to an applicant, Human Resources will provide the applicant with a statement of his/her consumer rights, a copy of the background report, and a letter explaining the "adverse action" process.

The applicant will have five business days to provide additional information and/or dispute inaccurate information before the offer is formally withdrawn.

All background and reference check information will be treated and protected as confidential. Hiring managers should contact Human Resources with any questions regarding background and reference checks and results.

Employee Training

All Tamarac employees attend training classes to familiarize them with the culture of compliance. This training is required for all employees and covers some bit not all of the following areas:

- Username & Passwords
- Appropriate Usage
- Malicious Content
- Physical Security
- Workstation Security
- Security Updates
- Data Confidentiality
- Clean Desk Policy
- Compliance

Password Policy

There is a formal procedure to add, change, and delete user accounts and access, assign roles, and perform the necessary audits.

Our password policy is as follows:

Enforce initial password change	Enabled
Enforce password history	9 passwords remembered
Maximum password age	45 days
Minimum password length	8 characters
Password complexity requirements	Must contain characters from three of the following four categories: • English uppercase characters (A-Z) • English lowercase characters (a-z) • Base 10 digits (0 -9) • Non-alphanumeric characters ($#@!)

Access Privileges

Employee access to network printers and network resources is based upon the employee role and location, Tamarac employs a least privilege data access process, meaning permissions are restricted to only those authorized to perform work on the server.

Human Resources immediately notifies Tamarac IT when an employee is terminated or leaves the company. Once notified, Tamarac IT will disable network access, email access, etc. for the employee; depending on the severity, this could happen immediately or by the end of the business day. User accounts are reviewed quarterly by management.

Remote Access

Remote access via the internet is granted to the corporate/back-office network. The remote access is secured by using an encrypted VPN tunnel for all remote access communication.

Workstation & Back-office Network Security

Workstations are a standard build of Windows 7 and 8. They include virus protection. Microsoft Office is the standard productivity suite. Additional applications are installed based on department function and employee role.

All workstations are set to a locking screen-saver through Group Policy settings that cannot be disabled by the end-user. All workstations are actively monitored by a network-based asset management tracking system. This feature provides a complete hardware and software component update daily.

All laptops are encrypted by BitLocker to protect against data theft.

Data Destruction

When computer workstations are removed from active inventory, the hard drive is removed and commercially destroyed by RetireIT according to DOD standards.

Antivirus & Spyware

All workstations and servers are protected by Kasaya anti-virus and spyware protection products.

- **Workstations, laptop computers, and servers.** Kasaya anti-virus is installed on every server, workstation and notebook computer. The pattern files available from the vendor are pre-configured to check for updates hourly. The end user is prohibited from disabling or uninstalling the virus protection product. Kaseya an email notification to Systems when it detects a pre-determined event.
- **Email Servers.** The mail servers are protected by TrendMicro ScanMail™ for Exchange. It scans all emails and attachments automatically. The pattern files available from the vendor are pre-configured to check for updates hourly. Additionally, certain at-risk attachment types are automatically blocked.
- **Virus Outbreak Prevention.** Tamarac Systems and networking groups will activate the Outbreak Prevention Procedures supported under the Trend Micro product suite that includes (a) blocking network shares, (b) blocking port access, and (c) denying write access to files and directories, depending on the form of the virus outbreak.
- **Virus & Spyware Perimeter Filtering.** In addition to the virus and spyware protection provided by the Trend Micro suite of products, Tamarac uses the M86 Web Filter appliance. The M86 Web Filter examines content for spyware, Trojans, and viruses at the network perimeter before Internet traffic reaches workstations or servers using Kaspersky. Email, before it is scanned by Trend Micro's ScanMail™

is pre-scanned through an Ironport™ gateway appliance using Sophos anti-virus. The perimeter is protected via multiple layers using the three different commercial products: Trend Micro, Sophos, Kaspersky.

Back-Office Network Security

Back-office or corporate servers are built with Microsoft Windows Servers. These servers use a hardened build of the Windows operating system based on the following Microsoft documents: Windows Server Security Guide, Version 2.1 and Threats and Countermeasures Guide.

Directories are locked down based upon these guidelines and all non-essential Windows services are disabled. All servers have virus protection installed as described in an earlier section.

Email Protection

Tamarac uses implicit TLS connections for all email transmissions.

All Tamarac email (external and internal) is archived by a 3rd party archival service and retained in read-only mode.

All internal and external email is scanned for sensitive information (PII) and notifications are sent to Envestnet's Compliance Group and to the Systems & Networking Group. Additionally, the Compliance Group runs periodic scans against mailboxes using different dictionary and phrase criteria.

Physical Media Data Security & Disposal

Locked shred bins or shredders have been placed in the Tamarac offices for disposal of confidential documents.

Tamarac maintains a clean desk policy, which requires all employees to secure confidential information (including investor personally identifiable information) from visibility when not being used.

Application Security

Advisor Xi is designed with security measures that ensure the protection and privacy of client data. Our system maintains all model information, account settings, and restrictions so you can keep a single and secure database of record. Account holdings information is uploaded daily into Tamarac and purged nightly to ensure that you are basing your trades on the most current information.

- Access via SSL - minimum 128-bit encryption
- The software utilizes .NET session management for authenticating individual users and allowing permissions through the applications
- Only stored procedure access to the database - each stored procedure and page request authenticates the users
- No dynamic SQL or access to data tables
- Software is SQL injection protected which prevents unauthorized access to the application and its data
- Application supports only a single login per user
- Role-based access to program areas
- User accounts can be restricted to view data based on the financial account – for example, advisors can be restricted access to only their assigned financial accounts
- To prevent password guessing, accounts are locked after 5 unsuccessful sign in attempts
- IP restrictions (whitelisting and blacklisting)
- Trade approval workflows to deter accidental trades – for example, a trader will have to confirm that a trade is valid before it's submitted

Application Development Process

This section provides details of Tamarac coding practices that ensure scalable and security code used in all Tamarac applications.

The software development process starts with defined requirements in Rally. These requirements are reviewed by product development, product management and our executive team. Testing includes a code review, integration, and regression testing before the code is deployed to a production environment. In addition, all code goes through internal and external testing to check for any possible security vulnerabilities. Any vulnerabilities must be corrected before the code can be deployed to a production environment. Our authorized Development Team Managers confirm that the testing is satisfactory and the release package can be released to production.

All product changes are thoroughly documented in our online Support & Training Center two weeks before release to production. Our Customer Support team is trained on all product changes prior to deployment to production.

All code is securely checked via Microsoft Team Foundation Server (TFS). Microsoft TFS software is used to securely store and maintain source code. The level of access is provided based on job duties.

AlertLogic vulnerability scans are performed quarterly on the production environment to ensure that the software remains secure. Application penetration is conducted every 12 – 18 months by Trustwave.

All software is current and patched on a regular basis. Tamarac tests the patches in a test environment prior to deployment to a production environment.

Software Architecture

Access to Tamarac's applications requires only the use of Internet browsers. Supported versions include, Firefox, Internet Explorer, and Google Chrome.

Tamarac uses a 3-tier application architecture for our Web applications. The Presentation Tier uses a combination of industry standard technologies like JavaScript, CSS and HTML to create a rich user interface that is cross-browser compatible. We use Microsoft tools and technology for the Business and Data Tiers, including C# and Microsoft SQL Server for our databases.

Application Logging

Tamarac has adopted a centralized approach to logging any errors that occur during the operation of our applications, this allows us to quickly identify and resolve issues when they arise.

All successful and unsuccessful access activities are recorded in the system and in application logs, including username, action, and date / time of access. Every data change is logged in the system and in application logs.

Application Authentication

Tamarac applications are accessible via a Web browser, and supports IP range restriction including whitelists and blacklists. User sign in and data actions are tracked in audit logs. Users are automatically signed out of the applications after a period of inactivity. Tamarac has a strong password policy in place and administrators can set password parameters around length, special characters, mixed case, and expiration periods.

System Security

Tamarac has designed its Advisor Suite infrastructure using leading hardware to provide the most secure, scalable and reliable platform. Rackspace manages Tamarac system security including the network and operating system.

Controls in place include:

- Dedicated HA Firewalls with stateful inspection
- Dedicated intrusion detection to provide an additional layer of protection against unauthorized access
- Dedicated redundant load balanced switches
- System installation using a hardened, patched operating system
- System patching to provide ongoing protection
- Data protection with onsite/offsite backups
- Alerts are monitored by our security team 24x7
- Penetration testing

Our network archtecture diagram is available by request.

Business Continuity & Disaster Recovery

Facilities

Tamarac uses two separate data centers: one in Elk Grove, IL (primary) and one in a remote location (secondary). Both N+1 redundant data centers are managed by Rackspace and have multiple high-speed data communication trunks provided by various network service providers to minimize the effects of bandwidth constraint or outages affecting one provider.

Computer Systems

Tamarac uses hardware managed by Rackspace and software in redundant configurations. Web and application servers use RAID 0+1 disk subsystems. Database servers use a combination of RAID 0+1 and RAID 5. These configurations protect individual systems against the effects of hardware failures, especially to active data systems. In addition, these systems are designed to provide high availability wherever possible. They are monitored by multiple levels of utility software that automatically generate alerts sent to Rackspace and Tamarac personnel if an abnormal condition arises or a predetermined threshold has been reached. Other components, such as firewall devices and load balancers are implemented in redundant high-availability configurations so a failure of one device will not impact production processing.

Data Protection and Reliability

Tamarac will provide a fault-tolerant processing environment with multiple levels of backup. A full and complete alternate processing center is available. Finally, archive data is available off-site for protection of customer data. To this end, the current infrastructure design and procedures are valuated to sustain and improve reliability.

Primary Data Center

The safeguards described above are designed to deal with an event or failure of a system, subsystem or hardware component in the primary data center.

Secondary Data Center

The secondary data center is a hardened Rackspace facility. This data center is linked to the primary data center via a dedicated point-to-point circuit and/or a VPN tunnel. Web/Application Data is replicated from the primary data center to the secondary data center continuously. Database backups are replicated from the primary to the secondary data center multiple times per day. In addition, encrypted copies of the data center backups are sent to a secure offsite electronic vault. In the event of a failure at the primary data center database backups would be restored on secondary equipment and DNS records would be modified to point to new data center.

Primary Data Center Restoration

The intent is to restore processing at the primary data center as soon as possible. When systems and networking are available again at the primary site, the backup data flow is reversed, and the initial primary data center comes back online as a "mirror" to the secondary data center where processing is occurring. After a period of testing and evaluation, Tamarac will schedule a transition back to the primary data center. The final data center restoration step is to restore all database backups on primary equipment and point DNS records to primary facility.

Off-Site Data Backup

Tamarac partners with Rackspace and Iron Mountain to deliver data backup and offsite storage. The vendors back up the media disk and securely transport it to secure offsite storage facilities.

Incident Response

If there is any abnormal or otherwise suspicious activity, or if Envestnet Tamarac employees or clients report unusual activity, the security incident response team is mobilized. The incident first responders are:

- SVP, Technology
- VP, Information Technology
- VP, Development

Subsequent members are engaged to complete the team and include:

- Group President, Envestnet Tamarac
- VP, Client Services
- VP, Account Management
- VP, Services
- SVP, Client Relations
- Human Resources

If unexplained or suspicious activity is detected, a determination is made as whether this is a valid or invalid activity.

- Valid activity: activity will continue to be monitored
- Invalid activity: security barriers to suppress the activity will be enacted and monitoring continued.

If penetration or breech of data or information is suspected, the following actions will be initiated:

- Notification of Executive Management Committee.
- Immediate isolation of the potentially targeted system(s).
- If penetration confirmed, client notification initiated by VP, Client Services.
- Determination of the degree and manor of intrusion.
- Determination of data integrity and data security on the systems in question.
- Determination of remediation path by Information Technology and Development team.
- Remediate.
- Invoke post mortem
- Engage Envestnet external auditors
- Report back to clients on findings

Problem Incident Management

Tamarac provides live technical support services on weekdays from 5:30 A.M. to 4:30 P.M. Pacific Time, Friday, excluding holidays observed by Tamarac. We also have a case management system in our online Support & Training Center where you can submit support requests. To verify the identity of the person submitting the support request, the email address is validated against the address we have on file and the phone number and contact information is validated against the information we have on file.

DISCLAIMER

The services and materials described herein are provided on an “as is” and “as available” basis, with all faults. Envestnet disclaims all warranties, express or implied, including, without limitation, warranties of merchantability or fitness for a particular purpose, title, non-infringement or compatibility. Envestnet reserves the right to add to, change, or eliminate any of the services and/or service levels listed herein without prior notice.