Information Security Whitepaper

This document outlines the information security program at Terminus Software, Inc. It is owned and managed by Terminus. This document shall not be duplicated, used, or disclosed for any purpose other than the originally intended purpose.

terminus

TABLE OF CONTENTS

1. ORGANIZATION & COMPLIANCE

1.1 Purpose

This document outlines Terminus' strategy to protect Terminus and its customer data. Defined controls are required in order to ensure the confidentiality, integrity, and availability of the data environment at Terminus. It serves as a standard in which Terminus customers and potential customers can utilize to assess the security controls in place. The intent of this document is to emphasize and reinforce Terminus' commitment to information security. The confidentiality, integrity, and availability of customer data are our highest priority.

1.2 Information Security Office

Terminus has established an information security office managed by the Director of Information Security. This position is responsible for the overall administrative, technical, and physical security of the organization. Other responsibilities include but are not limited to, evaluating risks and threats to the organization's information assets, governance, compliance, evaluation and recommendation of technical controls, incident response, disaster recovery & business continuity, and development & implementation of security policies. Members of the Terminus information security office hold the following certifications:

Certified Information Systems Security Professional (CISSP)

Certified Information Security Manager (CISM)

Certified in Risk and Information Systems Control (CRISC)

Certified Information Systems Auditor (CISA)

Security+

1.3 Compliance & Security Certification

Terminus has completed the examination for Service Organization Controls (SOC) 2 with independent audit firm, Schellman & Company LLC. Our SOC 2 report can be provided upon request. This important step has been taken to ensure our customers understand that we are committed to the protection of their data and complying with industry standard security controls and best practices.

2. DATA CENTER SECURITY

2.1 Security Controls

Terminus products run on Amazon Web Services (AWS) infrastructure. Amazon's data centers are compliant with various standards such as: PCI DSS, SOC 1/2/3, ISO 27002 & 9001, FISMA, HIPAA, FedRAMP, The Cloud Security Alliance, and are regularly tested for security controls and compliance by independent third parties. Data center compliance reports can be provided upon request. Terminus reviews the results of these assessments to ensure appropriate security controls exist and customer and Terminus data remain secure. AWS operates the cloud infrastructure to provision a variety of basic computing resources such as processing and storage. The AWS infrastructure includes the facilities, network, hardware, and operational software (e.g., host OS, virtualization software, etc.) that support the provisioning and use of these resources. The AWS infrastructure is designed and managed according to security best practices and a variety of security compliance standards. Terminus leverages this to build a secure architecture on top of secure computing infrastructure. AWS manages the security configuration of its managed services products. These services provide the scalability and flexibility of resources with the additional benefit of being managed. For these services, AWS will handle basic security tasks like guest operating system and database patching, firewall configuration, and disaster recovery. In addition, Terminus is responsible for and manages advanced, detailed, and specific security tasks and configuration such as encryption, data management, and access control.

3. SYSTEM SECURITY

3.1 Identity & Access Management

Terminus grants access to users based on business need & justification and access requires a written request by the individual's manager and is setup with least privilege. Unique security credentials are created and assigned to users to ensure individual accountability and for audit and logging purposes. By default, users have no access to resources until permissions are explicitly granted. Terminus IT administrators setup granular access to specify which services, APIs, and resources users can access and users are granted access based on roles. In addition, users who access customer data in our AWS environment must use multi-factor authentication. A user's username, unique password, and a six-digit single-use code is required to access our AWS environment. Authentication logs are retained and show login/logoff dates and times, changes made, service/resource accessed etc. and the logs are reviewed as needed. Access management reviews are conducted quarterly or when there are significant changes to our environment such as an employee departure. Our password policy aligns to the latest version of NIST 800-63-3. The AWS root account is known to a small set of individuals and the user's username, unique password, and a six-digit single-use code is required when using root access. The device which produces the six-digit single-use code is stored in a fire, water, and tamper proof safe in a secure office which requires key access that's limited to a small number of individuals. The root account is used for emergencies or whenever root access is required to complete certain functions within our AWS account. When employees depart Terminus, access to our environment is promptly removed. Standard user access is centrally managed using single-sign on technology which manages access to various applications in our environment. This allows us reliable integration to all our web and mobile apps, use of a full-featured federation engine, granular access policies, real-time security reporting, and adaptive authentication.

3.2 Vulnerability Management

Terminus checks for vulnerabilities regularly and applies patches and updates based on criticality and impact to the business. Terminus performs patch and configuration management and uses resources from external repositories, vulnerability reporting bulletin websites, and global threat intelligence to reduce risks and protect data. Terminus uses an automated service which performs security assessments against our infrastructure. Security assessments check for unintended network accessibility of our Amazon EC2 instances and for vulnerabilities on those EC2 instances. Assessment use pre-defined rules packages mapped to common security best practices and vulnerability definitions. Some of the assessments include checking for access to our EC2 instances from the internet, remote root login being enabled, or vulnerable software versions installed. The findings are reviewed regularly. All critical, high, and medium risks are tracked until remediation is complete. Critical vulnerabilities are remediated no later than 3 days and high vulnerabilities are remediated no later than 5 days depending on environmental changes that may be impacted.

3.3 Endpoint Management

Terminus centrally manages endpoints to ensure our standard configuration is in place. Some of the areas we focus on include but aren't limited to: operating system updates & patches, third-party application updates & patches, disk encryption, device lockouts, password policies, application management, asset inventory, etc.

3.4 Endpoint Protection

Endpoint protection provides real-time protection against viruses, spyware, trojans, worms, advanced persistent threats, and ransomware. Terminus endpoints are protected with real-time scanning and detection. Virus, spyware, trojans, worms, advanced persistent threats, and ransomware detection and removal is also performed immediately to prevent infections and outbreaks. Updates are performed in real-time and full system scans are performed weekly in addition to daily scans of critical areas where malware is commonly installed such as system memory, startup objects, and disk boot sectors. Also, end users have the ability to perform a full system scan on demand at any time. In addition, Terminus provides protection against web-based threats by blocking access to websites that are known to have malware.

3.5 Endpoint Firewall

Endpoint firewalls seek and stop suspicious behaviors typical of malicious attacks before they can execute and wreak havoc on a host system. Terminus endpoints use firewalls to protect against malicious traffic and prevent the download of malicious applications. It provides an extra layer of protection against advanced persistent threats and zero-day attacks. Endpoint firewalls also provide security features such as application, programs, services, and network connection blocking.

3.6 Server Security

Servers use securely hardened images that run the necessary services to support business operations. Servers are checked regularly for unnecessary services and ports that are in use. In addition, servers are managed using a standard base configuration that aligns to industry standards and best practices such as the National Institute of Standards & Technology (NIST) and Information Standards Organization (ISO) 27002. We physically and logically separate the database instances from application servers. Administrative access to servers is based on business need. Requests and changes to access servers are managed via a tracking process that involves a ticket with written justification from a manager or above. Access to the server environment is audited quarterly or more frequently when a significant change to the environment occurs. In addition, logging is enabled across the environment that captures information such as: login/logoff times, changes made, files/data accessed, individuals who accessed the server, etc.

4. NETWORK SECURITY

4.1 Penetration Testing

Terminus hires an independent security vendor to perform annual penetration testing. Penetration testing provides an objective real-world view of the state of security of an organization and its environment. Terminus engages penetration testers on an annual multiple week engagement to test the production environment. To ensure vendor neutrality and independence, penetration testing vendors are rotated annually. The areas covered each year include but are not limited to the following:

- External network penetration test: internet-based penetration test against Terminus public IP addresses
- Internal network penetration test: white and/or grey box testing against production systems
- Application security testing

4.2 Network Firewalls

Terminus uses dedicated firewalls for its network and VPN. The firewalls are cutting edge stateful inspection-based devices. Multiple zones are employed to ensure the highest level of security is achieved and each zone has its own set of rulesets allowing only traffic that is necessary to perform business.

Firewalls protect Terminus against malicious users and incidents that originate outside or inside the network. These firewalls are in place to monitor and control communications at the external boundary and at key internal boundaries within the network enabling filtering on both ingress and egress traffic. These boundary devices employ rulesets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services. ACLs or traffic flow policies are established on each managed interface which manage and enforce the flow of traffic. Every firewall on the Terminus network uses an inbound implicit deny all rule and allows only the traffic that is necessary for business purposes.

4.3 Threat Detection & Intrusion Prevention

Terminus uses tools for intelligent threat detection by collecting, analyzing, and correlating events from CloudTrail, VPC flow logs, and DNS logs across all of our associated AWS accounts. Detections are made more accurate by incorporating threat intelligence (such as lists of known malicious IP addresses provided by AWS Security and third-party threat intelligence partners). Our threat detection also uses machine learning to detect anomalous account and network activities such as detection of remote API calls from a known malicious IP address indicating potentially compromised credentials. Terminus can also detect direct threats to our environment indicating a compromised instance sending encoded data within DNS queries.

4.4 Network Monitoring

Terminus uses various tools to monitor our environment to detect anomalies and incidents to ensure 365x24x7 coverage. All inbound and outbound traffic is monitored. In addition, alerting is in place to notify us of attempted and active intrusions to our network. This monitoring and alerting provides us with visibility and extended coverage by having a team of professionals dedicated to monitoring and securing our environment. When an alert is detected that presents a risk to our business, our incident response plan is initiated to identify, respond, analyze, contain, remediate, and recover from an incident. Our network monitoring provides us with visibility and extended coverage by having a team of professionals dedicated to monitoring and securing our infrastructure and network.

4.5 Log & Event Management & Security Incident Management

Terminus uses log & event management and reporting tools to monitor the following but not limited to: services, programs, applications, API activity, system activity, authentication activity, processes, services, firewalls, servers, and VPN traffic. Our log management solution provides us with visibility into our environment and subsequently, reporting and troubleshooting capabilities. Based on the alerts received, our team responds and activates our incident response plan. Log messages are encrypted in transit via TLS over TCP and UDP. Logs are streamed in real-time via TLS and stored in encrypted format using server-side Advanced Encryption Standard (AES) 256-bit encryption in AWS data centers in the United States. Log data is retained for one year and securely purged after that point.

4.6 Two-Factor Authentication

All authorized personnel permitted to remotely connect into Terminus’ environment are required to use two-factor authentication. Terminus uses software tokens that implement two-step verification services using the time-based one-time password algorithm and HMAC-based one-time password algorithm for authenticating users. The software token provides a random six-digit one-time password derived from the current time and a shared secret key that rotates every 30 seconds which users must provide in addition to their username and password to authenticate.

4.7 Spam Filtering & Phishing Prevention

Email filtering protects the Terminus environment in three broad categories. The first is a reputation blacklist based on where the message originated. This list is updated daily and mitigates a majority of malicious or inbound spam email. The second is what software sent the message. Message headers and unique message identifiers are evaluated to determine the likelihood of spam. Lastly, the message content is analyzed and blocks messages based on keywords including sophisticated tactics such as common misspellings.

To prevent phishing, Terminus uses tools that participate in the Domain-based Message Authentication, Reporting & Conformance (DMARC) program which allows domain owners to tell email providers how to handle unauthenticated messages from their domain. Terminus has created a DMARC record within our administrative configuration and implemented a send policy framework (SPF) record and DomainKeys identified mail (DKIM) keys on all outbound mail streams. Terminus also uses advanced anti-phishing tools to protect users from malicious links in shortened web addresses and malicious content from linked images. We automatically flag emails from untrusted senders that have encrypted attachments or embedded scripts, warn against email that tries to spoof employee names or that comes from a domain that looks similar to our own domain, we use enhanced protections against spear phishing attacks by flagging unauthenticated emails, and we scan images for phishing indicators and expand shortened URLs to uncover malicious links.

5. APPLICATION SECURITY

5.1 Encryption

All login pages pass data via TLS and only support certificates signed by trusted Certificate Authorities.
All data is encrypted while in transit using TLS over HTTPS and at rest using AES 256-bit encryption.

5.2 Testing & Assessments

Terminus performs application security testing on its web applications. Two separate forms of security assessments are performed on applications. Static analysis looks at applications in a non-runtime environment to detect flaws in the software's inputs and outputs that cannot be seen through dynamic web scanning alone. Static analysis scanning is built into our development process. Dynamic analysis identifies security issues in running web applications before they can be exploited. Our web application testing tools perform OWASP, SANS/CVE, and industry standard web application testing. We conduct code reviews and scanning at different levels of the life cycle and software acquisition process. We use tools which check for security flaws and vulnerabilities in code at every code commit during the development process. In addition, our web applications are penetration tested by an independent security vendor annually. Terminus also uses an automated security assessment service that helps improve the security and compliance of our applications deployed on AWS. The service automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, a detailed list of security findings is produced and prioritized by level of severity. When issues are identified, they are tracked until remediation is complete.

5.3 Code Review

Terminus code undergoes a careful internal review process. All changes are reviewed by at least one reviewer prior to release to production and communicated during the change management process. Our software development life cycle manages all code quality delivery through a stringent process of code reviews, unit testing, integration tests, and static code testing. The internal code review process is designed to identify coding vulnerabilities, functional flaws, and ensure coding best practices are in place.

6. DATA PROTECTION & MANAGEMENT

6.1 Data Encryption

One of the most important aspects of data protection is encryption of data. All customer data that enters Terminus systems is transmitted over secure and encrypted channels from end-to-end using TLS over HTTPS. Furthermore, all customer information is encrypted at rest using AES 256-bit encryption including log and backup data. Terminus uses AWS Key Management Service (KMS) to provide us with centralized control of our encryption keys. We use KMS to create, import, rotate, and revoke keys. The keys are symmetric and are a combination of 256-bit Elliptic Curve Diffie-Hellman and AES-GCM (Galois Counter Mode) keys derived from a hardware secure module backing key in counter mode using Hashed Message Authentication Code (HMAC) with Secure Hash Algorithm (SHA) 256. The master keys in KMS are stored in highly durable storage in encrypted format to ensure they can be retrieved when needed. KMS automatically rotates master keys created in KMS annually without the need to re-encrypt data that has already been encrypted with our master key. We can create new master keys and control who has access to those keys and which services they can be used with. The master keys created on our behalf by KMS cannot be exported from the service. KMS stores multiple copies of encrypted versions of our keys in systems that are designed for 99.999999999% durability to help assure that our keys will be available when we need to access them. Terminus uses US – Virginia & Oregon regions for key storage. KMS is designed so that no one, including AWS employees, can retrieve our plaintext keys from the service. The service uses FIPS 140-2 validated hardware security modules (HSMs). Our plaintext keys are never written to disk and are only used in volatile memory of the HSMs for the time needed to perform our requested cryptographic operation. Also, KMS keys are never transmitted outside of the AWS regions in which they are created.

6.2 Data Retention & Backups

Data is retained as long as a customer continues to do business with Terminus and for 90 days after contract termination. At that point, Terminus will purge customer data. Customer data can also be deleted upon request by a customer. Backup data is retained for 14 days and purged after that point.

7. DISASTER RECOVERY & BUSINESS CONTINUITY

7.1 Data Center Availability

Terminus uses redundant data centers to ensure high availability of our data and infrastructure. Data centers are built in clusters in various global regions. Our data centers are online and no data center is "cold." In case of failure, automated processes move Terminus data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a failure, there is sufficient capacity to enable traffic to be load balanced to the remaining sites. We place instances and store data within multiple geographic regions and across multiple availability zones within each region. Each availability zone is designed as an independent failure zone. This means that availability zones are physically separated within a typical metropolitan region. In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, they are each fed from different grids from independent utilities to further reduce single points of failure. Availability zones are all redundantly connected to multiple tier-1 transit providers. In addition, data center electrical power systems are designed to be fully redundant and maintainable without impact to operations 24 hours a day, 7 days a week. UPS units provide backup power in the event of an electrical failure for critical and essential loads. Data centers use generators to provide backup power for the entire facility. Distributing applications and infrastructure in this manner provides Terminus with the ability to remain resilient in the face of most failure modes, including natural disasters or system failures.

8. PHYSICAL SECURITY

8.1 Data Center Physical Security

The Terminus primary and failover co-location facilities are SOC 1 compliant. A SOC 1 report can be provided upon request. Each facility is equipped with several layers of physical security that includes but is not limited to:

- Gated entry with manned gate
- Entry to only authorized personnel
- Restricted floor and cage access to authorized personnel
- Security cameras and 24x7 roaming security guards
- Visitor sign-in/sign-out logs
- Badge access

8.2 Corporate Office Physical Security

Terminus corporate offices include the following controls:

- Badge access to entry/exit points
- Restricted levels of access for employees (dependent upon job responsibilities)
- Security cameras at ingress and egress points
- Security guards in main building entrance and in garage
- Visitor sign-in/sign-out logs

9. ADMINISTRATIVE SECURITY

9.1 Security Policies

Terminus maintains a comprehensive set of security policies that align to ISO 27002 and map to common industry standards such as NIST, PCI, and HIPAA. Policies are developed, reviewed, and approved by our executive leadership team and published to all employees. Review and signature of the policies is required during the new hire process and by all employees annually.

9.2 Background Checks

All Terminus employees submit to a rigorous background check process. Terminus conducts background checks on all employees prior to hire that include national, state, and county criminal history, social security number trace, checks against the sex offender registry, driving records, education history, and work history for the previous ten years.

9.3 Security Awareness

All employees complete security awareness training on several topics such as information security, social engineering, internet & email safety, access control & passwords, protection of customer data, and physical security. Security awareness training helps employees recognize and respond appropriately to real and potential security concerns. It also educates employees on risks, how to respond to risks, and how to avoid them to better protect themselves, our environment, and customer & company data.