Tenable Technical and Organizational Measures for Tenable Products

Introduction

The following sets forth the technical and organizational measures implemented by Tenable to protect the privacy and security of customer data, including personal data. Tenable may change these measures at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting customer data.

Information security governance

Tenable operates an Information Security Management System (ISMS) which is aligned to the NIST Cybersecurity Framework and other security accepted frameworks and standards.

Tenable is independently certified to the ISO 27001:2013 standard.

Tenable has dedicated, internal full-time teams in the areas of IT, Information Security, Legal, and Human Resources to ensure best practices are enforced with respect to management of customer data. Tenable also has a dedicated cross-functional team to drive the Secure Software Development Lifecycle (SSDLC). This team is responsible for the coordination, communication, refinement, development of, and adherence to security controls in our processes.

Tenable maintains documented, internal information security and privacy policies that have been approved by management, and communicated to all relevant personnel and external parties utilizing appropriate document management processes. These policies are reviewed at least annually or when significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

Measures of encryption and anonymization of customer data

For Tenable cloud products, Tenable encrypts customer data in all states (at rest and in transit) using the industry accepted best practices and state of the art technologies to protect data from being accessed by unauthorized parties. Currently, the technology deployed is TLS 1.2 and AES-256. Encryption is applied to various application infrastructure layers, and can include disk, application, and database encryption. Encryption keys are stored securely and access is limited. Sharing of keys is prohibited and key management procedures are reviewed on a yearly basis. At the organizational level, data that could potentially identify a customer is anonymized before being ingested into our analytics platform, the Tenable Data Science Platform, via a one-way salted hash using SHA-256.

Availability controls

In order to protect customer data from accidental or unauthorized destruction or loss, Tenable employs backup and restore processes to provide restoration of business-critical systems which are regularly tested.

	For its cloud-based products, Tenable makes extensive use of AWS and Microsoft Azure cloud infrastructures which ensure the ongoing confidentiality, integrity, resilience and high availability of the products. More information on AWS's security controls for its data centers is available at https://aws.amazon.com/compliance/data-center/controls/. More information on Microsoft Azure's security controls for its data centers is available at https://docs.microsoft.com/en-us/azure/security/.
	For its cloud-based products, Tenable identifies and implements recovery requirements as part of its annual business impact and disaster recovery assessments. Tenable's Service Level Agreement is available at https://static.tenable.com/prod_docs/tenable_slas.html.
Security audits and assessments	
	Tenable performs regular internal risk assessments and audits on its systems and products. Tenable engages reputable third parties to conduct external audits to ensure that measures taken are appropriate and operating as required to ensure the security of customer data and supporting operations.
	Tenable leverages automated security testing to identify any potential vulnerabilities within product source code, dependencies, and underlying infrastructure before releasing new product features to customers. Tenable maintains assurance programs for its products including NIAP, CSA and regional certification and assurance standards.
	Tenable runs automated web application scans against its products on a frequent basis. This allows for bugs, common exploits, and security vulnerabilities/issues to be discovered early in the development process.
System and data access controls	
	For its corporate infrastructure, Tenable maintains a logging and monitoring policy aligned to industry best practices and in scope of the ISMS. Logs are reviewed on a regular basis. Tenable utilizes multiple authorization levels when granting personnel access to corporate systems, including those storing and processing customer data. Authorizations are managed via defined processes aligned with Tenable's security-related policies. Tenable reviews and audits this authorization process on a periodic basis.
	Tenable maintains an asset management policy as part of its ISMS. For its corporate infrastructure, pursuant to this policy, Tenable utilizes the following endpoint protections: ● Data loss prevention ● Antivirus & anti-malware protection ● Mobile device management (MDM) ● Local agents ● Encryption technologies ● Asset tagging
	Within Tenable products, customers have full control of user management via a user management interface. Tenable products provide logging capabilities, and user audit logs are available to customers through an audit-log API endpoint.

Tenable protects against brute force attacks against its cloud products by locking accounts out after five (5) failed login attempts. Customers can configure two-factor authentication and Tenable encourages all customers to enable integration into their Federated Identity Provider through SAML.

Customers licensing Tenable products can use Tenable's documented APIs or SDKs to build custom connections and control access via API keys.

Physical access controls

Tenable operates a management-approved physical security policy at all of its corporate locations. Controls in place include:

- CCTV
- Access badges
- Escorting of visitors in Tenable offices
- Visitor registration and logging
- Physical and logical access controls on systems

For Tenable cloud products:

- All AWS and Microsoft Azure data centers adhere to strict security controls including guards, CCTV, motion detectors, access control mechanisms and other measures to prevent equipment and data center facilities from being compromised.
- Only authorized representatives have access to systems and infrastructure within the data center facilities. Physical security equipment undergoes maintenance on a regular basis.
- Tenable regularly audits our critical data center providers as part of our Third Party Risk Management (TPRM) program.

Human resources security

Aligned to the requirements of ISO 27001:2013, Tenable undertakes the following human resource-related measures:

- Personnel background checks in accordance with local legal & regulatory requirements
- Training - Personnel is required to complete annual security and data protection training, as well as team-specific security and data protection training if their function involves the processing of customer data and/or personal data.
- Personnel are subject to confidentiality provisions in employment agreements that prohibit the misappropriation and misuse of customer data and company proprietary information.
- When Tenable's relationship with personnel is terminated, Tenable immediately removes their access rights to information, systems, and company facilities.

Third party control and management

Under its TPRM program, Tenable reviews every vendor (including sub-processors) through a rigorous risk assessment. This includes a review of the vendor's scope and an assessment of their criticality as well as a legal review, security and privacy questionnaire, architecture assessment, and certification review. The list of vendors is periodically reviewed based on

	the risk landscape and dependency for services and vendor criticality.
	Tenable imposes data protection contractual terms that protect customer personal data to at least the same standard Tenable is obligated to provide its customers (include valid data transfer mechanisms and compliance programs).
Technical support controls	
	When providing technical support to our customers, Tenable prohibits personnel from uploading/transferring customer data to: ● Public websites (e.g., PCAP analyzers, HAR analyzers) ● File sharing websites (e.g., Dropbox, OneDrive) ● A non-Tenable issued device (e.g., personal mobile phones, computers) ● A non-Tenable issues account (e.g., personal email) During the provision of technical support, Tenable personnel may only access customer data when connected to the secure Tenable network.
	Once a technical support engineer (TSE) resolves a customer's issue and closes the support case, the TSE ensures that: ● Any customer scan results and/or debugging data are promptly deleted from the TSE's laptop. ● If a Tenable.io customer uploads scan results to Tenable's Tenable.io lab instance for troubleshooting, such data is promptly deleted from the lab instance. Any customer data that has been provided to the Technical Support team via Tenable's secure upload site, Tenable Uploads, is retained for 90 days after it is uploaded by a customer to ensure that the data is accessible while a TSE troubleshoots the issue. After 90 days, such data is automatically deleted.