DATA SHEET

YOUR DATA SECURITY AND PRIVACY REQUIREMENTS DEFINE HOW WE OPERATE

Your data security and privacy needs matter to Tenable, and we value the trust that you place in our products and services. Thousands of customers, including financial services organizations, healthcare providers, retailers, educational institutions and government agencies trust Tenable with their vulnerability data in our cloud platform.

Security is core to our corporate ethos, and Tenable allocates significant investment to protect the confidentiality, integrity and availability of all customer data. Tenable continuously assesses and implements additional measures to help improve our security program and address the ever-changing threat landscape.

One of our top priorities is not allowing customers to access any data other than their own and preventing any non-customer, bad actor or unauthorized Tenable representative to access, disclose, copy or otherwise violate the privacy and protection of the customers' data stored in the Tenable cloud platform. Tenable uses state-of-the-art container technology to create and segregate customer environments. Data contained within one container cannot leak or otherwise be intermingled with another container.

Tenable also focuses on the availability and reliability of the cloud platform because poor security controls can create problems that, while not a risk to customers' data, can affect the service availability. Tenable implements and enforces measures to ensure that Tenable services are highly available, guarded against attacks or simple faults and outages and always usable for our customers.

KEY BENEFITS

Safeguard Your Data
Take advantage of Tenable's state-of-the-art data encryption, network controls and container isolation to protect your vulnerability data.

Focus on Innovating
Leverage the comprehensive data security and privacy controls built-in the Tenable cloud platform so that you can focus on growing your business.

Boost Productivity
Rely on the industry's first uptime guarantee with leading service quality and enhanced disaster recovery procedures to ensure your service is always on.

Meet Compliance Requirements
Support CSA STAR and the Privacy Shield Framework for powerful security assurance in the cloud to comply with your compliance needs.

Gain Peace of Mind
Trust a security pioneer and leader to protect the confidentiality, integrity and availability of your most sensitive and proprietary data.

DATA SECURITY

Encryption

Tenable.io data is encrypted in transit and storage using modern ciphers and methods recommended by security industry and standards organizations worldwide. This includes the use of AES-256 and TLS Encryption ciphers. Encryption keys are stored securely and access is limited. Encryption is applied to various application infrastructure layers, and can include disk, application, and database encryption. Sharing of keys is prohibited and key management procedures are reviewed on a yearly basis.

Access Controls

Tenable provides a number of mechanisms to help customers keep their data secure and control access. We protect against brute force attacks by locking accounts out after five (5) failed login attempts. Customers can configure two-factor authentication and we encourage all customers to enable integration into their Federated Identity Provider through SAML. Additionally, customers can use our documented APIs or SDKs to build custom connections and control access via API keys.

Network Controls

The Tenable cloud platform is built on isolated, private networks using security groups and firewalls within virtual private clouds (VPC). All inbound and internal traffic is restricted to specific ports across a limited group of machines. All traffic rates, sources and types are actively monitored at various points in the network beyond ingress and firewalls. Tenable isolates customer data using application container technology and unique identifiers, which assures that access to customer data is limited to only that customer.

Regular Security Assessments

The Tenable information security program aligns to NIST Cybersecurity Framework, and other security accepted frameworks and standards. Tenable leverages our products to perform daily vulnerability, Docker container, and web application scans. Additionally, Tenable leverages our industry-leading security researchers and third-parties to conduct additional periodic security assessments of protective measures in place. Any identified issues are prioritized based upon risk and addressed accordingly. Corporate assets are regularly assessed and

logged for forensic purposes.

DATA PRIVACY

Data Anonymization

The data collected in our cloud does not include any scan data which contains PII or personal data. At the organizational level, data that could potentially identify a customer is anonymized before being ingested into the Tenable Data Science Platform, our analytics platform, via a one-way salted hash using SHA-256.

Data Access

Tenable provides a number of mechanisms to help customers keep their data secure and control access. We protect against brute force attacks by locking accounts out after five (5) failed login attempts. Customers can configure two-factor authentication and we encourage all customers to enable integration into their Federated Identity Provider through SAML. Additionally, customers can use our documented APIs or SDKs to build custom connections and control access via API keys. Access to the anonymized data is restricted to the Tenable Data Science and Research team only. Access is controlled through a central directory system. Security event and audit logs are collected and continuously monitored to detect and respond to anomalous behavior.

Data Localization

Collection and processing of customer scan data occurs inside the Tenable cloud platform within the geographic region where the customer's account is hosted, unless the customers explicitly selects a different geographic region for their data to reside. Those results are anonymized and then further aggregated with similar data from customers across the world in our analytics platform. Customer data is not moved from the region where the customer's Tenable.io is hosted until after it is permanently anonymized.

SECURE SOFTWARE DEVELOPMENT

Governance

Tenable has a dedicated cross-functional team across to drive the Secure Software Development Lifecycle (SSDLC). This group is responsible for the coordination, communication, refinement, development of and adherence to security controls in our processes. In order to ship secure, high quality products at pace, Tenable leverages automated Security Testing to identify any potential vulnerabilities within source code, dependencies, and underlying infrastructure before releasing to our customers.

Static Application Security Testing (SAST)

Tenable analyzes the application source code to determine bugs, tech-debt, and security vulnerabilities. A strict scoring criteria is adhered to by the Engineering teams to ensure not only security of code in our products, but quality as well. Any code not meeting this criteria is not shipped until resolved.

Dependency and 3rd Party Library Scanning

Tenable analyzes project dependencies to determine vulnerabilities and licensing issues. Strict scoring criteria prevents shipment of vulnerable dependencies in a Product until it is resolved by Engineering teams.

Dynamic Application Security Testing (DAST)

Tenable runs automated web application scans against the product suite on a frequent basis. This allows for bugs, common exploits, security vulnerabilities and issues to be discovered early on in the development process. By automating this approach, Tenable is able to improve the quality and security of our products for our customers.

Container Security

Tenable performs a vulnerability assessment on all container images to detect any vulnerable software running on a given container. Strict scoring criteria prevents the shipment of a vulnerable container until it is resolved by Engineering teams. A passing score is required for deployment.

Code Standards and Role Based Access Control

In line with the requirements of Certifications and industry best practices, Tenable has developed a baseline of source code control standards to provide proper hygiene around code repositories supporting our Products. These standards are developed across the company and automation has been deployed to enforce them. Standards automatically being enforced include but are not limited to: peer code reviews, role based access control, least privilege, code & repository ownership, segregation of duties, naming conventions, branch protections, and secrets management.

THIRD-PARTY RISK MANAGEMENT

Third-Party Management

Tenable reviews every vendor through a rigorous 3rd party risk management program. This includes a review of the vendor's scope and an assessment of their criticality as well as a legal review, security questionnaire, architecture assessment, and certification review. The list of 3rd parties is periodically reviewed based on the risk landscape and dependency for services and vendor criticality.

For More Information: Please visit ***tenable.com***
Contact Us: Please email us at ***sales@tenable.com*** or visit ***tenable.com/contact***

DATA SHEET

CERTIFICATIONS AND ASSURANCE

Cloud Security Alliance (CSA) STAR

CSA STAR is the industry's most powerful program for security assurance in the cloud. Tenable is a member of the CSA STAR program, and a public listing of the security controls in place for the Tenable.io platform is available for download from the CSA. Tenable responses to the Consensus Assessment Initiative Questionnaire (CAIQ) answer a set of over 140 questions encompassing key principles of transparency, rigorous auditing, and harmonization of standards, including indications of best practices and validation of security posture of cloud offerings.

Privacy Shield Framework

Tenable complies with the EU-U.S. Privacy Shield Framework and the Swiss – U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union, Switzerland, and the United Kingdom to the United States, respectively.

ISO 27001

The scope of the ISO/IEC 27001:2013 certification covers the ISMS supporting Tenable's legal areas, human resources, information technology, software development, executive leadership, and customer support functions. Following an extensive audit process, the certification was issued by Schellman & Company LLC. Details are publicly available in the Schellman Certificate Directory.

National Information Assurance Program (NIAP)

Tenable achieved NIAP certification across the Tenable.sc, Nessus Manager, Log Correlation Engine (LCE), Nessus Network Monitor and Nessus Agent products. Products undergo strict testing activities and security requirements before being added to the publicly available in the NIAP Product Compliant List.

SERVICE AVAILABILITY

Guaranteed Uptime

Tenable provides the vulnerability management industry's first uptime guarantee of 99.95% through a robust service level agreement. Service credits are offered if the SLA is not met, just like leading cloud vendors such as Amazon Web Services.

High Availability

Tenable makes extensive use of the AWS platform and other leading technologies to ensure that customers experience the best possible service and overall quality. Examples of redundancy and fault tolerance include: data storage clusters can recover from the loss of nodes without impacting service availability; Amazon Elastic Block Stores are used to take daily snapshots and store eight copies of data; data is replicated across clusters to provide fault tolerance in the event of a catastrophic failure of any node; and database instances manage the back end microservice framework to keep 30 days of snapshot data.

VULNERABILITY MANAGEMENT

Vulnerability Management

Tenable is a leading provider of vulnerability management. Tenable leverages its own solutions to conduct daily, weekly, or monthly scans of all corporate laptops, infrastructure and cloud environments. All findings are analyzed, ticketed and tracked in accordance with the Tenable Vulnerability Management Policy. Tenable's VM Program encompasses authenticated, agent, web application, and database scanning.

Third-Party Penetration Tests

Tenable leverages third parties for penetration tests of our applications, services and businesses as a whole. These have resulted in continuous updates to our products and processes for improving security and reliability. These assessments are part of ongoing compliance and security requirements to keep Tenable as a trusted provider of services.

Vulnerability Reporting Board

Tenable leverages a vulnerability report board (https://www.tenable.com/security) to receive and respond to any weaknesses or vulnerabilities identified from the broad security researcher community. As identified reports are triaged and responded to, Tenable releases security advisories for the benefit of customers, prospects and wider community.