Tenable Documentation Glossary

Last Updated: May 19, 2026

Glossary

The following glossary describes terms and concepts that you may encounter in Tenable documentation and products. To view industry standard cybersecurity terms and concepts, Tenable recommends using the National Institute of Standards and Technology (NIST) glossary.

To view or print this information offline, download the [Tenable Glossary PDF].

A

accountability

Property that ensures that the actions of an entity may be traced uniquely to the entity.

activation

The process of inputting an activation factor into a multi-factor authenticator to enable its use for authentication.

Active Directory

A Microsoft directory service that manages identities, authentication, and access control in Windows domain networks. Tenable Identity Exposure continuously monitors Active Directory for misconfigurations, weak permissions, and attack paths that could allow attackers to escalate privileges or move laterally. Tenable products also use Active Directory credentials to perform credentialed scans, enabling deeper vulnerability assessment of domain-joined systems.

active scanning

The traditional Tenable vulnerability assessment method in which Tenable Nessus scanners actively probe target systems by sending packets and analyzing responses to identify vulnerabilities, misconfigurations, and missing patches. Active scans in Tenable can be credentialed or uncredentialed and are configured through scan policies that specify which plugins to run, scan timing, and performance settings. Active scanning provides

comprehensive, deep assessment of systems and is the primary method for vulnerability discovery in Tenable Vulnerability Management and Tenable Security Center.

advanced persistent threat

A sophisticated, well-resourced adversary that conducts prolonged, targeted campaigns to compromise organizations and maintain long-term access to their networks. Tenable helps organizations defend against APTs by providing continuous visibility into vulnerabilities, misconfigurations, and identity weaknesses that APT groups commonly exploit. Tenable's threat intelligence, integrated into VPR scoring, tracks when vulnerabilities are being actively exploited by APT groups and other advanced adversaries. Tenable OT Security specifically addresses APT threats targeting industrial control systems and critical infrastructure, which are high-value targets for nation-state and advanced criminal actors.

adversary

A malicious entity whose goal is to determine, to guess, or to influence the output of an RBG.

agent

A lightweight software program installed on a host that performs vulnerability assessments and reports findings back to Tenable. Tenable Agent are installed on laptops, remote endpoints, and systems behind firewalls that are difficult or impossible to reach via network-based scanning. Unlike network scanners, agents operate locally and do not require open network paths or scan credentials, making them ideal for distributed or mobile workforces. Agents communicate scan results to Tenable Security Center or Tenable Vulnerability Management.

alert

A notification generated when Tenable detects a security event, vulnerability threshold breach, or policy violation. Alerts in Tenable products can be configured to trigger on new vulnerability discoveries, changes in asset state, compliance failures, or risk score changes. Tenable Vulnerability Management and Tenable Security Center support alert rules that deliver notifications via email, syslog, or integrations with ticketing and SIEM platforms, enabling security teams to respond quickly to emerging risks.

anomaly

Condition that deviates from expectations based on requirements specifications, design documents, user documents, or standards, or from someone's perceptions or experiences.

antivirus software

A program specifically designed to detect many forms of malware and prevent them from infecting computers, as well as cleaning computers that have already been infected.

application firewall

A firewall that uses stateful protocol analysis to analyze network traffic for one or more applications.

application programming interface (API)

A set of defined endpoints and protocols that allow external systems and scripts to interact programmatically with Tenable products. Tenable provides REST APIs for Tenable Vulnerability Management, Tenable Security Center, and other platforms, enabling customers to automate scan management, retrieve vulnerability data, manage assets, and integrate Tenable findings into SIEMs, ticketing systems, and custom dashboards. API documentation and SDKs are available at developer.tenable.com.

artificial intelligence

(1) Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets. (2) An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action. (3) An artificial system designed to think or act like a human, including cognitive architectures and neural networks. (4) A set of techniques, including machine learning, that is designed to approximate a cognitive task. (5) An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.

asset

Any device, system, cloud resource, or identity that Tenable discovers and tracks within an organization's environment. In Tenable products, assets include physical hosts, virtual machines, containers, cloud instances, network devices, web applications, and OT/IoT devices. Each asset is assigned a unique identifier and associated with vulnerability findings, compliance results, and risk scores. Asset inventory is the foundation of exposure management — you can only secure what you can see.

Asset Criticality Rating (ACR)

A Tenable-proprietary score from 1 to 10 that reflects the business importance and sensitivity of an asset within an organization's environment. ACR is automatically calculated based on factors including the asset's function, the type of data it handles, its connectivity to other critical systems, and any custom criticality tags applied by the security team. Assets with higher ACR scores represent greater potential business impact if compromised. When combined with Vulnerability Priority Rating (VPR), ACR enables security teams to focus remediation efforts on the highest-risk vulnerabilities on the most critical assets first. ACR is a core feature of Tenable Lumin.

asset inventory

A continuously maintained, comprehensive record of all assets discovered across an organization's environment in Tenable. Asset inventory in Tenable includes physical hosts, virtual machines, cloud instances, containers, network devices, OT/ICS devices, IoT sensors, and web applications. Each asset record includes attributes such as IP address, hostname, operating system, installed software, open ports, vulnerability findings, and compliance status. Tenable builds and maintains asset inventory through a combination of network scanning, agent-based reporting, cloud connector integrations, and passive network monitoring, ensuring continuous coverage even as the environment changes.

attack surface

The totality of an organization's digital assets, systems, and entry points that are potentially exposed to attackers. Tenable's Exposure Management Platform helps organizations continuously discover, assess, and reduce their attack surface by providing unified visibility

across on-premises infrastructure, cloud environments, operational technology, and identity systems. Understanding attack surface is the first step in Tenable's exposure management approach: see everything, prioritize what matters, and act to reduce risk.

attacker

A malicious actor who attempts to exploit vulnerabilities to compromise systems, steal data, or disrupt operations. Tenable helps organizations understand their environment from an attacker's perspective by identifying exploitable vulnerabilities, excessive permissions, weak credentials, and attack paths that adversaries could use to achieve their objectives. Tenable Identity Exposure specifically models attack paths through Active Directory that attackers commonly exploit for privilege escalation and lateral movement. Tenable's Vulnerability Priority Rating (VPR) incorporates threat intelligence about active attacker exploitation to help security teams prioritize the vulnerabilities most likely to be targeted.

audit

In Tenable products, an audit refers to a compliance assessment that compares system configurations against a defined security standard or regulatory framework. Tenable performs compliance audits using audit files - configuration policy definitions aligned to standards including CIS Benchmarks, DISA STIGs, PCI DSS, HIPAA, SOC 2, and NIST 800-53. Audit results show which systems pass or fail individual controls, providing evidence for regulatory reporting and identifying configuration drift from secure baselines. Compliance audits in Tenable are distinct from vulnerability scans: audits check configuration correctness while scans detect software flaws.

audit file

A configuration file used by Tenable to define the compliance checks performed during a compliance audit scan. Audit files contain the specific configuration settings, registry keys, file permissions, and policy requirements that Tenable evaluates against target systems. Tenable provides pre-built audit files aligned to standards including CIS Benchmarks, DISA STIGs, PCI DSS, and HIPAA. Organizations can also create custom audit files to assess against internal security policies or specialized compliance frameworks.

B

backdoor

An undocumented way of gaining access to computer system. A backdoor is a potential security risk.

baseline

A known-good configuration state used as a reference point for compliance auditing and change detection. In Tenable, baselines are defined through audit policies that specify the expected configuration settings for operating systems, applications, and network devices. Tenable compliance scans compare current system configurations against established baselines — such as CIS Benchmarks or DISA STIGs — and report deviations as compliance findings requiring remediation.

benchmark

A documented set of secure configuration standards used as a reference for compliance auditing in Tenable. The most common benchmarks in Tenable compliance scanning are CIS Benchmarks, published by the Center for Internet Security, which provide consensus-based secure configuration guidelines for operating systems, databases, cloud platforms, and applications. Tenable provides pre-built audit policies mapped to CIS Benchmarks, DISA STIGs, and other industry benchmarks, enabling organizations to assess whether their systems meet these security standards.

breach

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses personally identifiable information for an other than authorized purpose.

C

CIEM (Cloud Infrastructure Entitlement Management)

A cloud security capability that discovers, analyzes, and governs the identities and permissions across cloud environments to enforce least-privilege access. Tenable Cloud Security includes CIEM capabilities that identify overprivileged users, roles, and service accounts across AWS, Azure, and GCP, revealing excessive permissions that could be exploited if an identity is compromised. CIEM is part of Tenable's CNAPP approach to cloud security, addressing the identity risk layer that CSPM alone does not cover.

cloud computing

A model for delivering computing resources — including servers, storage, databases, networking, and applications — over the internet on demand. Tenable Cloud Security provides visibility and risk assessment across major cloud platforms including AWS, Azure, and Google Cloud Platform, identifying misconfigurations, compliance violations, excessive permissions, and vulnerabilities across cloud infrastructure. Tenable's cloud security capabilities span Cloud Security Posture Management (CSPM), Cloud Infrastructure Entitlement Management (CIEM), and cloud workload protection.

cloud infrastructure

The computing resources-including virtual machines, storage, networking, and managed services-provided by cloud platforms such as AWS, Azure, and Google Cloud Platform. Tenable Cloud Security provides comprehensive security assessment of cloud infrastructure, identifying misconfigurations, compliance violations, and vulnerabilities across multi-cloud environments. Tenable discovers cloud infrastructure through direct integration with cloud provider APIs, assessing resources including EC2 instances, S3 buckets, Azure VMs, GCP Compute Engine, container registries, databases, and serverless functions. Cloud infrastructure findings are unified with on-premises and OT assessments in Tenable One to provide complete attack surface visibility.

cloud provider

A company that delivers cloud computing services over the internet, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). Tenable Cloud Security integrates directly with major cloud providers through their native APIs to continuously assess cloud security posture, identify misconfigurations, and detect excessive permissions. Tenable supports security assessment across multiple cloud providers in a single deployment, enabling organizations with multi-cloud strategies to maintain consistent security standards and unified visibility across all cloud platforms.

CNAPP (Cloud-Native Application Protection Platform)

A unified security platform that combines cloud security posture management (CSPM), cloud infrastructure entitlement management (CIEM), and cloud workload protection into a single solution for securing cloud-native applications. Tenable Cloud Security is a CNAPP that provides comprehensive cloud security coverage across AWS, Azure, and Google Cloud Platform, giving security teams a single view of cloud misconfigurations, excessive permissions, and workload vulnerabilities from development through production.

command and control

Command and Control' is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.

common vulnerability scoring system (CVSS)

An industry-standard framework for rating the technical severity of software vulnerabilities on a scale of 0.0 to 10.0. Tenable displays CVSS scores (both v2 and v3) for all identified vulnerabilities, giving security teams a standardized severity reference. However, Tenable recommends using Vulnerability Priority Rating (VPR) alongside CVSS, as VPR incorporates real-world threat intelligence and exploit availability to more accurately reflect which vulnerabilities pose the greatest actual risk in the current threat landscape.

compliance audit

An automated assessment that compares system configurations against a defined security standard or regulatory framework. Tenable performs compliance audits using pre-built audit policies aligned to standards including CIS Benchmarks, DISA STIGs, PCI DSS, HIPAA, SOC 2, NIST 800-53, and ISO 27001. Compliance audit results in Tenable products show which systems pass or fail individual controls, providing the evidence needed for regulatory reporting and remediation prioritization.

container

A lightweight, portable unit of software that packages an application and its dependencies into a standardized environment for consistent deployment. Tenable Cloud Security scans container images stored in registries such as Docker Hub, Amazon ECR, and Azure Container Registry for known vulnerabilities and misconfigurations before they are deployed to production. Tenable also assesses running containers in Kubernetes environments, providing continuous visibility into container security posture.

container image scanning

The assessment of container images for known vulnerabilities, outdated dependencies, and misconfigurations before or after deployment. Tenable Cloud Security scans container images stored in registries including Amazon ECR, Docker Hub, Azure Container Registry, and Google Container Registry, identifying vulnerable software packages and base images before they reach production. Integrating container image scanning into CI/CD pipelines allows development teams to catch and remediate vulnerabilities during the build process rather than after deployment.

container runtime

The software responsible for executing and managing containers on a host system, such as Docker Engine, containerd, or CRI-O. Tenable Cloud Security assesses container runtime security by scanning container images before deployment and monitoring running containers for vulnerabilities and misconfigurations. Tenable identifies vulnerable packages within container images, detects containers running with excessive privileges, and flags containers using outdated or compromised base images. Runtime security findings are integrated with

infrastructure and application vulnerabilities in Tenable's unified platform to provide comprehensive cloud-native security visibility.

credentialed scan

A vulnerability scan in which Tenable authenticates to target systems using valid credentials — such as SSH keys, Windows domain accounts, or database credentials — before performing the assessment. Credentialed scans provide significantly deeper and more accurate vulnerability findings than uncredentialed scans because they can enumerate installed software, check patch levels, assess local configurations, and detect vulnerabilities that are only visible from within the system. Tenable recommends credentialed scanning as the default approach for comprehensive vulnerability assessment of servers, workstations, and network devices. See also: uncredentialed scan.

critical infrastructure

The essential services that support a society and serve as the backbone for the society's economy, security and health.

CSPM (Cloud Security Posture Management)

Continuous monitoring and assessment of cloud infrastructure configurations against security best practices, compliance frameworks, and organizational policies. Tenable Cloud Security provides CSPM capabilities across AWS, Azure, and Google Cloud Platform, automatically detecting misconfigurations such as publicly exposed storage buckets, unencrypted databases, overly permissive security groups, and disabled logging. CSPM findings are mapped to compliance frameworks including CIS Benchmarks, PCI DSS, SOC 2, and HIPAA, enabling organizations to maintain continuous cloud compliance posture.

CVE ID

Common Vulnerabilities and Exposures identifier-a unique reference number assigned to publicly disclosed security vulnerabilities. Tenable maps detected vulnerabilities to CVE IDs throughout its products, enabling security teams to cross-reference findings with the National Vulnerability Database (NVD), vendor advisories, and threat intelligence feeds. When viewing vulnerability findings in Tenable Vulnerability Management or Tenable Security

Center, each CVE ID is displayed with its associated CVSS score, VPR score, affected software versions, and links to detailed CVE information. Tenable plugins are continuously updated to detect newly published CVEs within hours of disclosure.

Cyber Exposure Score (CES)

A Tenable-proprietary metric that provides a single, aggregate measure of an organization's overall cybersecurity exposure. CES is calculated by Tenable Lumin based on the vulnerability data, asset criticality, and remediation maturity across all assets in an organization's environment. CES scores range from 0 to 1000, with lower scores indicating better security posture. Lumin displays CES alongside industry peer benchmarks, allowing organizations to understand their exposure relative to comparable organizations. CES enables security leaders to communicate risk in business terms and track improvement over time.

cyber security

The ability to protect or defend the use of cyberspace from cyber attacks.

cyber threat intelligence

Analyzed information about current and emerging threats, adversary tactics, and active exploits that provides context for security decision-making. Tenable incorporates threat intelligence from multiple sources — including Tenable Research, the National Vulnerability Database, and commercial feeds — to power Vulnerability Priority Rating (VPR). When new exploits are observed in the wild or a vulnerability is actively targeted, Tenable automatically updates VPR scores to reflect the increased risk, helping security teams focus on the vulnerabilities that matter most right now.

D

data integrity

The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.

device

Any physical or virtual hardware component discovered and tracked by Tenable in an organization's environment, including servers, workstations, laptops, network equipment, mobile devices, IoT sensors, OT controllers, and cloud instances. Tenable continuously discovers devices across all network segments and cloud environments, associating each with vulnerability findings, software inventory, and risk scores. Understanding the full device inventory is the foundation of exposure management.

discovery

The process by which Tenable identifies and inventories all assets within an organization's environment. Tenable performs discovery through network-based scanning, agent-based reporting, cloud connector integrations, and passive network monitoring. Discovery scans are often the first step in a Tenable deployment, establishing a comprehensive asset inventory before vulnerability assessment begins. Tenable can discover hosts, cloud resources, OT devices, and web applications across distributed and hybrid environments.

domain name

A label that identifies a network domain using the Domain Naming System.

E

event

An observable occurrence recorded by Tenable or a connected system that may indicate a security-relevant change in the environment. In Tenable OT Security, events include detected network communications, protocol anomalies, device configuration changes, and policy violations within operational technology environments. Tenable also ingests and correlates events from integrated SIEM platforms and generates its own events when vulnerability states, asset configurations, or risk scores change.

exposure

The degree to which an organization's assets are susceptible to attack, considering the combination of vulnerabilities present, the criticality of affected assets, and the likelihood of

exploitation based on current threat intelligence. In Tenable's exposure management framework, exposure is a more complete measure of risk than vulnerability count alone — it incorporates asset context, business impact, and real-world threat data. Reducing exposure is the core objective of Tenable One, Tenable's Exposure Management Platform.

F

file sharing services

Services that include but are not limited to information sharing and access to information via web-based file sharing or storage.

findings

The vulnerabilities, misconfigurations, compliance failures, and security weaknesses identified by Tenable during a scan or assessment. Each finding in Tenable includes details such as the affected asset, CVE identifier (if applicable), CVSS and VPR scores, plugin ID, severity rating, and remediation guidance. Findings are the primary output of Tenable scans and form the basis for prioritization, reporting, and remediation workflows in Tenable Vulnerability Management and Tenable Security Center.

firewall

An inter-network connection device that restricts data communication traffic between two connected networks. A firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance), which forwards or rejects/drops packets on a network. Typically firewalls are used to define zone borders. Firewalls generally have rules restricting which ports are open.

firmware

Embedded software stored in non-volatile memory that controls the basic operations of a hardware device. Tenable OT Security identifies firmware versions running on operational technology devices including PLCs, RTUs, HMIs, and network equipment, comparing them against known vulnerability data to detect outdated or vulnerable firmware. Tenable Nessus

also detects firmware versions on network devices and flags firmware with known CVEs as part of standard vulnerability assessments.

forgery

A (ciphertext, tag) pair produced by an adversary who is not knowledgeable of the secret key and yet is accepted as valid by the verified decryption procedure.

G

gateway

An intermediate system (interface, relay) that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables either one-way or two-way communication between the networks.

H

hacker

Unauthorized user who attempts to or gains access to an information system.

hardening

The process of reducing a system's attack surface by applying secure configurations, disabling unnecessary services, and enforcing security controls. Tenable supports hardening workflows through compliance audits that measure systems against hardening benchmarks such as CIS Benchmarks and DISA STIGs. Tenable identifies configuration weaknesses — open ports, default credentials, unnecessary services, weak permissions — and provides remediation guidance to bring systems into a hardened state.

harm

Any adverse effects that would be experienced by an individual (i.e., that may be socially, physically, or financially damaging) or an organization if the confidentiality of PII were breached.

hashing

The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data.

HIPAA

The Health Insurance Portability and Accountability Act, a U.S. federal law requiring healthcare organizations to protect the privacy and security of patient health information. Tenable provides pre-built HIPAA compliance audit policies that assess whether systems handling protected health information (PHI) meet required security controls. Tenable Security Center and Tenable Vulnerability Management can continuously monitor healthcare environments for HIPAA compliance violations and generate audit-ready reports.

host

A networked system that Tenable discovers and assesses during a scan, including physical servers, workstations, virtual machines, and cloud instances. In Tenable products, hosts are identified by IP address, hostname, or cloud resource identifier and appear in scan results with associated vulnerability findings, software inventory, and compliance status. Tenable tracks host state over time, alerting teams when new hosts appear on the network or when a host's vulnerability profile changes.

hostname

The human-readable name assigned to a host on a network, used by Tenable to identify and correlate assets across scans. When performing DNS resolution, Tenable associates IP addresses with hostnames to provide richer asset identification in scan results. Hostnames can be used as scan targets in Tenable products and are displayed alongside IP addresses in asset inventory and vulnerability findings.

HTTP

A standard method for communication between clients and Web servers.

HTTPS

A standard method for communication between clients and Web servers.

hypervisor

The virtualization component that manages the guest OSs on a host and controls the flow of instructions between the guest OSs and the physical hardware.

I

identity

Unique group element \(0\) for which \(x+0=x\) for each group element \(x\), relative to the binary group operator \(+\).

identity provider (IdP)

A system that authenticates users and provides identity assertions to service providers. Tenable products support integration with enterprise identity providers using SAML 2.0, enabling single sign-on (SSO) for Tenable Vulnerability Management and Tenable Security Center. Supported identity providers include Okta, Microsoft Entra ID (Azure AD), and other SAML-compliant IdPs, allowing organizations to enforce centralized authentication policies and manage Tenable access through their existing identity infrastructure.

image

An exact bit-stream copy of all electronic data on a device, performed in a manner that ensures the information is not altered.

incident

An occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

incident response

The remediation or mitigation of violations of security policies and recommended practices.

individuals

An assessment object that includes people applying specifications, mechanisms, or activities.

industrial control system (ICS)

Networked systems used to monitor and control industrial processes including manufacturing, energy production, water treatment, and critical infrastructure. Tenable OT Security is purpose-built to provide visibility and vulnerability management for ICS environments, safely assessing programmable logic controllers (PLCs), remote terminal units (RTUs), human-machine interfaces (HMIs), and other OT devices without disrupting operational processes. Tenable identifies vulnerabilities, misconfigurations, and unauthorized communications in ICS networks.

industrial security

The portion of internal security that refers to the protection of industrial installations, resources, utilities, materials, and classified information essential to protect from loss or damage.

infrastructure as code

The process of managing and provisioning an organization's IT infrastructure using machine-readable configuration files, rather than employing physical hardware configuration or interactive configuration tools.

intelligence

In intelligence collection, a phrase that indicates that in the satisfaction of intelligence requirements, all collection, processing, exploitation, and reporting systems and resources are identified for possible use and those most capable are tasked.

interchangeable

The ability to combine signals from multiple PNT data sources into a single PNT solution, as well as the ability to provide a solution from an alternative source when a primary source is not available.

interface

A boundary between the IoT device and entities where interactions take place. There are two types of interfaces: network and local.

internet of things

Networked physical devices equipped with sensors and connectivity that collect and exchange data with other systems. Tenable OT Security provides discovery and vulnerability assessment for IoT devices in enterprise and industrial environments, identifying device types, firmware versions, and known vulnerabilities. Tenable helps organizations understand their IoT attack surface and prioritize remediation for IoT devices that are difficult to patch or protect through traditional means.

intrusion

A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so.

intrusion detection

The process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents.

intrusion prevention

The process of monitoring the events occurring in a computer system or network, analyzing them for signs of possible incidents, and attempting to stop detected possible incidents.

inventory

A listing of each item of material charged to a COMSEC account.

IoT device

A physical device with network connectivity and sensing or actuation capabilities, deployed in enterprise, industrial, or operational technology environments. Tenable OT Security discovers and assesses IoT devices alongside OT and IT assets, providing a unified view of the connected environment. Tenable identifies IoT devices by type, vendor, firmware

version, and known vulnerabilities, helping security teams manage a category of assets that is often invisible to traditional vulnerability management tools.

IPsec

An OSI Network layer security protocol that provides authentication and encryption over IP networks.

issuer

The organization that is issuing the PIV Card to an applicant. Typically, this is an organization for which the applicant is working.

K

kerberos

A network authentication protocol that uses tickets to verify the identity of users and services in Windows domain environments. Kerberos is used by Tenable when performing credentialed scans of Windows systems in Active Directory domains — Tenable can authenticate using Kerberos to gain the access needed for deep vulnerability assessment. Tenable Identity Exposure also monitors Kerberos configurations and ticket-granting policies for weaknesses such as Kerberoasting vulnerabilities and delegation misconfigurations.

key

A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm.

L

LDAP

The Lightweight Directory Access Protocol, or LDAP, is a directory access protocol. In this document, LDAP refers to the protocol defined by RFC 1777, which is also known as LDAP V2. LDAP V2 describes unauthenticated retrieval mechanisms.

lightweight directory access protocol (LDAP)

A protocol for accessing and maintaining directory services, commonly used to manage user accounts and authentication in enterprise networks. Tenable products can be configured to use LDAP or LDAPS (LDAP over SSL/TLS) for user authentication, enabling organizations to manage Tenable platform access using their existing directory infrastructure. Tenable Identity Exposure also assesses LDAP configurations in Active Directory environments for security weaknesses.

likelihood

A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability.

login

The establishment of an authenticated session between a person and a system. Also known as “sign in,” “log on,” or “sign on.”.

Lumin

Tenable Lumin is a risk quantification and exposure management capability within Tenable Vulnerability Management that transforms raw vulnerability data into business-relevant risk metrics. Lumin calculates Asset Criticality Rating (ACR) for each asset, aggregates findings into a Cyber Exposure Score (CES), and benchmarks an organization's security posture against industry peers. Lumin enables security leaders to communicate cyber risk in business terms, prioritize remediation efforts by business impact, and measure improvement over time.

M

machine learning

The development and use of computer systems that adapt and learn from data with the goal of improving accuracy.

malware

Malicious software designed to infiltrate, damage, or gain unauthorized access to systems. Tenable detects malware-related indicators during vulnerability scans, including known malware artifacts, backdoors, rootkits, and suspicious software installations. Tenable plugins identify systems with active malware infections or known malware-associated software present, enabling security teams to prioritize investigation and response. Tenable OT Security also monitors OT network traffic for malware communication patterns.

mandate

A mandatory order or requirement under statute.

misconfiguration

An incorrect or insecure system configuration that creates a security vulnerability or compliance violation. Misconfigurations are one of the leading causes of data breaches and are a primary detection target for Tenable products. Tenable identifies misconfigurations through compliance audits that compare system settings against security benchmarks, and through cloud security posture management (CSPM) that continuously monitors cloud infrastructure for insecure configurations. Misconfiguration findings include open ports, default credentials, excessive permissions, unencrypted data, and improperly configured services.

MITRE ATT&CK

A globally recognized knowledge base of adversary tactics, techniques, and procedures (TTPs) based on real-world cyberattack observations. Tenable maps vulnerability findings and threat detections to MITRE ATT&CK techniques, helping security teams understand how identified vulnerabilities could be used by attackers in the context of known attack patterns. Tenable OT Security specifically maps ICS threats to the MITRE ATT&CK for ICS matrix, providing operational technology teams with threat context aligned to industrial adversary behavior.

mobile device

A portable computing device such as a smartphone, tablet, or laptop that connects to enterprise networks and may access sensitive data. Tenable discovers and assesses mobile devices as part of comprehensive asset inventory, with Tenable Agent providing vulnerability assessment for laptops and endpoints that roam outside the corporate network. Tenable Vulnerability Management tracks mobile device vulnerability status and integrates with mobile device management (MDM) platforms to enrich asset data.

multi-factor authentication

An authentication method that requires users to verify their identity using two or more independent factors before gaining access. Tenable Vulnerability Management and Tenable Security Center support multi-factor authentication to protect platform access, and Tenable can be configured to require MFA through SAML SSO integration with enterprise identity providers. Tenable Identity Exposure also assesses Active Directory and Entra ID environments for accounts that lack MFA enforcement, identifying a high-risk exposure that is frequently exploited by attackers.

N

National Vulnerability Database

The U.S. government's repository of standardized vulnerability data, maintained by NIST and used as a primary source for CVE information, CVSS scores, and vulnerability metadata. Tenable integrates NVD data into its vulnerability intelligence, using CVE identifiers and CVSS scores from the NVD as foundational data that is then enriched with Tenable Research threat intelligence to produce Vulnerability Priority Rating (VPR) scores. Tenable plugin coverage maps directly to NVD CVEs, enabling customers to query scan results by CVE identifier.

P

passive scanning

A network monitoring method in which Tenable passively observes network traffic to discover assets, identify running services, and detect vulnerabilities without sending packets to target systems. Tenable's passive scanning capability, available through Tenable Network Monitor and integrated into Tenable Vulnerability Management, continuously analyzes network communications to build asset inventory and identify security issues. Passive scanning complements active scanning by providing continuous visibility without the overhead of scheduled scans and without risking disruption to sensitive systems.

patch

A software update that fixes a specific vulnerability, bug, or security weakness in an application or operating system. Tenable identifies missing patches during vulnerability scans by comparing installed software versions against known patch levels, and flags systems that are running unpatched software with known CVEs. Tenable provides detailed patch information in scan results including the relevant CVE identifiers, CVSS and VPR scores, and remediation steps needed to apply the fix.

patch management

The process of identifying, testing, and applying software patches to fix vulnerabilities across an organization's systems. Tenable supports patch management workflows by continuously identifying unpatched systems, prioritizing patches by Vulnerability Priority Rating (VPR), and integrating with patch management platforms such as Microsoft SCCM, Ivanti, and others. Tenable Vulnerability Management provides patch management dashboards that track remediation progress and measure patch velocity over time.

pci dss

The Payment Card Industry Data Security Standard, a set of security requirements for organizations that store, process, or transmit credit card data. Tenable provides pre-built PCI DSS compliance audit policies that assess cardholder data environments against all required controls, including vulnerability scanning requirements mandated by PCI DSS.

Tenable Security Center and Tenable Vulnerability Management generate PCI DSS compliance reports suitable for submission to Qualified Security Assessors (QSAs) and for internal audit purposes.

penetration testing

A simulated cyberattack conducted to identify and demonstrate exploitable vulnerabilities in systems before real attackers can. Tenable Nessus is widely used in penetration testing workflows to enumerate vulnerabilities, identify attack surface, and inform manual exploitation efforts. Tenable products support penetration testing through discovery scanning, credentialed assessment, and detailed plugin output that gives testers the information needed to understand and demonstrate exploitable conditions.

plugin family

A category that groups related Tenable Nessus plugins by the type of vulnerability, compliance check, or system they assess. Plugin families in Tenable products include categories such as Windows, Linux, Web Servers, Databases, and SCADA Systems. When configuring scan policies in Tenable Vulnerability Management or Tenable Security Center, security teams can enable or disable entire plugin families to focus scans on specific technology areas or compliance requirements.

policy

In Tenable products, a policy is a configurable set of rules that defines how a vulnerability scan or compliance audit is performed. Scan policies specify which plugins to run, what scan settings to apply, which credentials to use, and how to handle scan performance parameters. Compliance audit policies define which configuration checks to evaluate and against which security benchmark. Policies allow security teams to standardize assessment approaches across their organization and ensure consistent coverage.

port scan

A network reconnaissance technique in which Tenable discovers which network ports are open on target systems and which services are listening on those ports. Port scanning is typically the first phase of a Tenable vulnerability scan, performed during the discovery

process before detailed vulnerability checks begin. Tenable's Tenable Nessus scanners use various port scanning methods including TCP connect scans, SYN scans, and UDP scans to map the attack surface of target systems. Port scan results inform which subsequent vulnerability checks (plugins) are relevant for each discovered service.

private cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

proxy

An application that “breaks” the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. Note: This effectively closes the straight path between the internal and external networks making it more difficult for an attacker to obtain internal addresses and other details of the organization’s internal network. Proxy servers are available for common Internet services; for example, a hyper text transfer protocol (HTTP) proxy used for Web access, and a simple mail transfer protocol (SMTP) proxy used for e-mail.

proxy server

A server that services the requests of its clients by forwarding those requests to other servers.

public cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Q

query

A search or filter expression used to retrieve specific vulnerability, asset, or compliance data from a Tenable platform. Tenable Vulnerability Management and Tenable Security Center

support querying across asset inventory and vulnerability findings using filter conditions such as CVE ID, CVSS score, plugin family, asset tag, and operating system. Saved queries and filters allow security teams to create persistent views of their environment and power custom dashboards and reports.

R

remediation

The process of addressing and resolving vulnerabilities, misconfigurations, and compliance failures identified by Tenable. Tenable provides prioritized remediation guidance for each finding, including specific patch versions, configuration changes, and compensating controls. Tenable Vulnerability Management and Tenable Security Center integrate with IT ticketing systems such as ServiceNow and Jira to create and track remediation tickets directly from vulnerability findings. Tenable tracks remediation progress over time, allowing security teams to measure velocity and demonstrate risk reduction to stakeholders.

repository

A Tenable Security Center component that stores vulnerability scan data, compliance audit results, and asset information for a specific group of scanners and networks. Repositories enable multi-tenant deployments by segmenting data based on organizational boundaries, security classifications, or geographic regions. Each repository maintains its own database of findings and can be configured with different retention policies, access controls, and integration settings.

risk management framework (RMF)

A structured process defined by NIST Special Publication 800-37 for managing security and privacy risks across federal information systems. Tenable supports RMF workflows by providing continuous monitoring capabilities that satisfy the Assess and Monitor steps of the RMF lifecycle, generating the vulnerability assessment data and compliance evidence required for system authorization packages. Tenable Security Center is widely used in government environments for RMF compliance.

role-based access control (RBAC)

A security model that grants users access to system features and data based on their assigned role within an organization. Tenable products implement RBAC to control what different users can see and do within the platform. Tenable Vulnerability Management and Tenable Security Center define roles such as Administrator, Scan Manager, and Analyst, each with specific permissions for managing scans, viewing results, configuring policies, and generating reports. Organizations can customize roles to match their security team structure.

S

sandbox

A system that allows an untrusted application to run in a highly controlled environment where the application's permissions are restricted to an essential set of computer permissions. In particular, an application in a sandbox is usually restricted from accessing the file system or the network. A widely used example of applications running inside a sandbox is a Java applet.

satellite

Bus and payload combined into one operational asset.

SCADA

Supervisory Control and Data Acquisition — industrial control systems used to monitor and control geographically distributed infrastructure such as power grids, pipelines, water treatment facilities, and transportation networks. Tenable OT Security provides passive and active assessment capabilities for SCADA systems, safely identifying vulnerabilities, misconfigurations, and unauthorized network communications without risking disruption to critical operational processes. Tenable maps SCADA-specific vulnerabilities to known CVEs and ICS-CERT advisories.

scan template

A predefined scan configuration in Tenable that specifies the target scope, plugin selection, credential settings, and scan performance parameters for a particular type of assessment.

Tenable provides built-in scan templates for common use cases including Basic Network Scan, Advanced Dynamic Scan, Web Application Tests, PCI Quarterly External Scan, and more. Security teams can use built-in templates or create custom templates to standardize scanning across their organization and ensure consistent coverage.

scan zone

A network segment or group of assets in Tenable Vulnerability Management that shares common scanning infrastructure, typically defined by geographic location, network topology, or security boundaries. Scan zones allow organizations to deploy Tenable Nessus scanners close to target systems to optimize scan performance and ensure that scans can reach assets behind firewalls or in remote locations. Each scan zone has dedicated scanners assigned to it, enabling distributed scanning across global or segmented networks.

scanner

A Tenable component that performs vulnerability scans and compliance audits by executing Tenable Nessus plugins against target systems. In Tenable Vulnerability Management, cloud-hosted scanners are managed by Tenable, while customers can also deploy Tenable Nessus scanners as virtual appliances or on-premises instances. In Tenable Security Center, administrators deploy and manage their own Tenable Nessus scanners across the environment. Scanners connect to the Tenable platform to receive scan instructions, download plugin updates, and report findings.

scanning

The process by which Tenable systematically examines systems, networks, and applications to discover assets, identify vulnerabilities, and assess compliance with security policies. Scanning in Tenable includes multiple methods: active scanning with Tenable Nessus scanners, agent-based scanning with Tenable Agent, passive network monitoring, cloud connector integrations, and web application scanning. Scans are configured through scan policies that define which plugins to run, credentials to use, scan timing, and performance parameters. Tenable Vulnerability Management and Tenable Security Center provide centralized scan management, scheduling, and results aggregation across distributed environments.

secure communications

Telecommunications deriving security through use of National Security Agency (NSA)-approved products and/or protected distribution systems (PDSs).

security assertion markup language (SAML)

An XML-based protocol that enables single sign-on (SSO) by securely exchanging authentication and authorization data between an identity provider and a service provider. Tenable Vulnerability Management and Tenable Security Center support SAML 2.0 for SSO integration with enterprise identity providers including Okta, Microsoft Entra ID, and other SAML-compliant systems. SAML integration allows organizations to manage Tenable access through their existing identity infrastructure and enforce centralized authentication policies.

security assessment

A systematic evaluation of an organization's systems to identify vulnerabilities, misconfigurations, and compliance gaps. Tenable performs security assessments through multiple methods: network-based scanning using Tenable Nessus, agent-based assessment using Tenable Agent, cloud posture assessment using Tenable Cloud Security, and OT environment assessment using Tenable OT Security. Each assessment type produces findings that are aggregated in Tenable platforms for prioritization, reporting, and remediation tracking.

security information and event management

A platform that aggregates, correlates, and analyzes security event data from across an organization's IT environment to detect threats and support incident response. Tenable integrates with leading SIEM platforms including Splunk, Microsoft Sentinel, IBM QRadar, and others, forwarding vulnerability findings, asset data, and scan results to enrich SIEM-based threat detection. Tenable's vulnerability context helps SIEM platforms prioritize alerts by identifying which affected assets have exploitable vulnerabilities.

security posture

An organization's overall cybersecurity health, reflecting its ability to identify, protect against, and respond to threats. Tenable Lumin quantifies security posture through the Cyber Exposure Score (CES), which aggregates vulnerability data, asset criticality, and threat intelligence into a single metric that can be tracked over time and benchmarked against industry peers. Improving security posture is the outcome of Tenable's exposure management approach: continuous assessment, risk-based prioritization, and measured remediation.

security risk

The effect of uncertainty on objectives pertaining to asset loss and the associated consequences.

segment

In the CFB mode, a sequence of bits whose length is a parameter that does not exceed the block size.

sensitive information

Information where the loss, misuse, or unauthorized access or modification could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act); that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

sensitivity

A form of bias that results from failures in the heuristics humans use to make decisions.

sensor

A Tenable component that collects data from monitored systems and reports findings to a central platform. In Tenable OT Security, sensors passively monitor operational technology network traffic to discover OT devices, identify communications patterns, and detect security threats without disrupting industrial processes. In Tenable's broader architecture, the term

may also refer to data collection components including Tenable Nessus scanners and Tenable Agent that act as distributed sensors feeding vulnerability data to Tenable Vulnerability Management or Tenable Security Center.

service

A software component participating in a service-oriented architecture that provides functionality or participates in realizing one or more capabilities.

signature

In Tenable products, a signature refers to the detection logic within a plugin that identifies a specific vulnerability, misconfiguration, or security condition. Each Tenable plugin contains signature-based detection code that checks for the presence of known vulnerabilities by examining software versions, configuration settings, or system behaviors. Tenable Research continuously updates plugin signatures to cover newly discovered vulnerabilities, ensuring detection coverage remains current.

single sign-on

An authentication method that allows users to access multiple applications with a single set of credentials and one login event. Tenable Vulnerability Management and Tenable Security Center support SSO through SAML 2.0 integration with enterprise identity providers, enabling security teams to access Tenable platforms using the same credentials they use for other corporate applications. SSO simplifies user management, enforces centralized authentication policies, and supports MFA requirements across the organization.

smart card

A credit card-sized card with embedded integrated circuits that can store, process, and communicate information.

software bill of materials

A structured inventory of all software components, libraries, and dependencies used in a software product or system. Tenable identifies software components present on scanned systems, providing visibility into the software inventory that forms the basis of SBOM analysis. When a vulnerability is discovered in a widely used component such as Log4j or

OpenSSL, Tenable's software inventory data allows organizations to quickly identify all affected systems across their environment, accelerating response to supply chain vulnerabilities.

spam

Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

special character

Any non-alphanumeric character that can be rendered on a standard, American-English keyboard. Use of a specific special character may be application dependent. The list of 7-bit ASCII special characters follows: ` ~! @ # $ % ^ & * ( ) _ + | } { “ : ? > < [ ] \ ; ’ , . / - =.

spyware

Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

SQL injection

A web application vulnerability in which an attacker inserts malicious SQL code into an input field to manipulate a database query, potentially enabling unauthorized data access, modification, or deletion. Tenable detects SQL injection vulnerabilities in web applications during web application scans, identifying input fields and parameters that are susceptible to injection attacks. Tenable plugins test for SQL injection conditions using safe detection methods that confirm vulnerability without causing damage to the target application.

stability

An inherent characteristic of an oscillator that determines how well it can produce the same frequency over a given time interval. Stability does not indicate whether the frequency is right or wrong, but only whether it stays the same. The stability of an oscillator does not necessarily change when the frequency offset changes. An oscillator can be adjusted, and its frequency moved either further away from or closer to its nominal frequency without changing its stability at all. The stability of an oscillator is usually specified by a statistic, such as the Allan deviation, that estimates the frequency fluctuations of the device over a given

time interval. Some devices, such as an OCXO [Oven Controlled Crystal (Xtal) Oscillator] have good short-term stability and poor long-term stability. Other devices, such as a GPS disciplined oscillator (GPSDO), typically have poor short-term stability and good long-term stability.

static code analyzer

A tool that analyzes source code without executing the code. Static code analyzers are designed to review bodies of source code (at the programming language level) or compiled code (at the machine language level) to identify poor coding practices. Static code analyzers provide feedback to developers during the code development phase on security flaws that might be introduced into code.

superuser

A user who is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

symmetric key

A cryptographic key that is used to perform both the cryptographic operation and its inverse (e.g., to encrypt, decrypt, create a message authentication code, or verify a message authentication code).

T

tampering

An intentional but unauthorized act resulting in the modification of a system, components of systems, its intended behavior, or data.

target

A system, network range, or group of assets specified for assessment during a Tenable vulnerability scan or compliance audit. Targets in Tenable can be defined using IP addresses, IP ranges, CIDR notation, hostnames, or asset tags. When configuring scans in Tenable Vulnerability Management or Tenable Security Center, administrators specify

targets to control which systems are assessed, ensuring scan coverage aligns with security requirements and network topology.

task

An activity that is directed toward the achievement of organizational objectives.

telemetry

Data collected and transmitted from remote systems to a central platform for monitoring, analysis, and reporting. Tenable agents and sensors continuously collect vulnerability, configuration, and software inventory data from endpoints and network segments and transmit this telemetry to Tenable Vulnerability Management or Tenable Security Center. This continuous telemetry flow enables near-real-time visibility into changes in the security state of the environment without requiring manual or scheduled scan initiation.

Tenable Agent

A lightweight software component that installs on endpoints, servers, and other systems to perform local vulnerability assessments without requiring network-based scanning. Tenable Agent continuously monitors the host system, running vulnerability checks, software inventory collection, and compliance audits locally. Unlike network-based Tenable Nessus scans that require network connectivity and may be blocked by firewalls, Tenable Agent operates from within the system itself, providing comprehensive assessment of laptops, remote workers, cloud instances, and systems in isolated network segments. Agents report findings to Tenable Vulnerability Management or Tenable Security Center, enabling continuous visibility even when systems are offline or roaming outside the corporate network.

Tenable AI Exposure

Tenable's solution for identifying and managing security risks in artificial intelligence and machine learning systems, including generative AI applications, AI models, and AI infrastructure. Tenable AI Exposure discovers AI assets across an organization's environment, assesses them for vulnerabilities and misconfigurations specific to AI/ML systems, evaluates data exposure risks, and identifies shadow AI usage. As organizations

rapidly adopt AI technologies, Tenable AI Exposure helps security teams understand and secure their AI attack surface alongside traditional IT, cloud, and OT assets within the Tenable One platform.

Tenable Attack Surface Management

Tenable's solution for continuously discovering and assessing internet-facing assets, shadow IT, and unknown external exposures that attackers can see and exploit. Tenable Attack Surface Management provides an attacker's-eye view of an organization's external attack surface, automatically discovering domains, subdomains, IP addresses, cloud assets, and web applications without requiring agents or credentials. The platform identifies vulnerabilities, misconfigurations, and security weaknesses in external assets, prioritizes findings using Vulnerability Priority Rating (VPR), and integrates with Tenable Vulnerability Management and Tenable One to provide unified visibility across internal and external attack surfaces.

Tenable Cloud Security

Tenable's cloud-native application protection platform (CNAPP) that provides comprehensive security coverage across multi-cloud environments including AWS, Azure, and Google Cloud Platform. Tenable Cloud Security combines cloud security posture management (CSPM), cloud infrastructure entitlement management (CIEM), container and workload security, and infrastructure-as-code scanning to give security teams complete visibility into cloud risk from development through production. Findings are unified in a single console with prioritization, compliance reporting, and remediation guidance.

Tenable Enclave Security

Tenable's solution designed for vulnerability management in air-gapped, classified, and disconnected network environments where systems cannot connect directly to the internet or cloud services. Tenable Enclave Security enables organizations operating in high-security or classified networks - such as government agencies, defense contractors, and critical infrastructure operators - to perform comprehensive vulnerability assessments using Tenable Nessus and Tenable Security Center without requiring internet connectivity. The solution provides mechanisms for securely transferring plugin updates and vulnerability data

into isolated enclaves while maintaining compliance with security classifications and network segmentation requirements.

Tenable Exposure Management

Tenable's comprehensive approach to cybersecurity that unifies vulnerability management, cloud security, identity security, OT security, and attack surface management into a continuous, risk-based program. Tenable Exposure Management sits above individual Tenable products within the Tenable One platform, providing the framework and methodology for discovering assets, assessing vulnerabilities, prioritizing risks based on business impact and threat intelligence, and measuring security posture improvement over time. This exposure-first approach moves beyond traditional vulnerability management to address the full spectrum of cyber exposure across an organization's modern attack surface.

Tenable Identity Exposure

A Tenable product that continuously monitors Active Directory and Microsoft Entra ID (Azure AD) for identity-based vulnerabilities, misconfigurations, and attack paths. Tenable Identity Exposure identifies weaknesses such as accounts without MFA, Kerberoastable service accounts, dangerous delegation configurations, and Active Directory misconfigurations that could allow privilege escalation or lateral movement. By exposing identity risk alongside infrastructure vulnerabilities, Tenable Identity Exposure gives organizations a complete picture of their attack surface.

Tenable Nessus

Tenable's flagship vulnerability scanner and the most widely deployed vulnerability assessment tool in the world. Tenable Nessus performs comprehensive vulnerability scanning of network hosts, identifying known vulnerabilities, misconfigurations, and compliance issues across operating systems, applications, network devices, and cloud infrastructure. Tenable Nessus is available as Tenable Nessus Professional for individual security practitioners and Tenable Nessus Expert for advanced use cases including infrastructure-as-code scanning and cloud asset discovery. Tenable Nessus is also the underlying scan engine for Tenable Vulnerability Management and Tenable Security Center.

Tenable One

Tenable's Exposure Management Platform that unifies vulnerability management, cloud security, OT security, identity security, and web application security into a single platform providing comprehensive visibility across the modern attack surface. Tenable One combines the capabilities of Tenable Vulnerability Management, Tenable Cloud Security, Tenable OT Security, Tenable Identity Exposure, and Tenable Web App Scanning, with Tenable Lumin providing risk quantification and ExposureAI providing AI-powered analysis across all data. Tenable One enables organizations to see every asset, find every vulnerability, prioritize by business risk, and measure their security posture over time.

Tenable OT Security

Tenable's purpose-built security solution for operational technology (OT) environments including industrial control systems, SCADA systems, and critical infrastructure. Tenable OT Security discovers and assesses OT devices including PLCs, RTUs, HMIs, historians, and engineering workstations, identifying vulnerabilities, firmware weaknesses, and network communications anomalies without disrupting operational processes. Tenable OT Security provides a unified view of IT and OT assets, enabling organizations to manage converged IT/OT risk from a single platform.

Tenable Patch Management

Tenable's integrated solution for identifying, prioritizing, and tracking the remediation of missing patches across an organization's infrastructure. Tenable Patch Management complements Tenable Vulnerability Management by not only identifying unpatched systems but also helping security and IT teams prioritize which patches to deploy first using Vulnerability Priority Rating (VPR) and Asset Criticality Rating (ACR). The solution integrates with existing patch deployment tools such as Microsoft SCCM, Ivanti, and others, enabling teams to push patches directly from Tenable or track remediation progress when patches are deployed through other systems.

Tenable Security Center

Tenable's on-premises vulnerability management platform, designed for organizations that require local data residency, air-gapped deployments, or high-volume enterprise scanning at

scale. Tenable Security Center provides comprehensive vulnerability assessment, compliance auditing, and security reporting for on-premises, hybrid, and OT environments. It is the preferred platform for government agencies, regulated industries, and enterprises with strict data sovereignty requirements. Tenable Security Center uses Tenable Nessus scanners and Tenable Agent as its underlying assessment engines.

Tenable Vulnerability Management

Tenable's cloud-based vulnerability management platform that provides comprehensive asset discovery, vulnerability assessment, and risk-based prioritization as a SaaS solution. Tenable Vulnerability Management is the foundation of Tenable One, Tenable's Exposure Management Platform, and integrates with Tenable Lumin for risk quantification, Tenable Web App Scanning for application security, and hundreds of third-party platforms for ticketing, SIEM, and IT operations. Tenable Vulnerability Management delivers continuous visibility across cloud, on-premises, and hybrid environments without requiring on-premises infrastructure.

threat intelligence

Analyzed data about active threats, adversary behavior, and exploitation activity that informs security decision-making. Tenable Research produces and curates threat intelligence that is integrated directly into Tenable products, powering Vulnerability Priority Rating (VPR) scores that reflect the current likelihood of exploitation for each vulnerability. When Tenable Research observes a new exploit being used in the wild, VPR scores are automatically updated, ensuring that customers are always prioritizing based on the most current threat landscape.

time scale

An agreed upon system for keeping time. All time scales use a frequency source to define the length of the second, which is the standard unit of time interval. Seconds are then counted to measure longer units of time interval, such as minutes, hours, or days. Modern time scales, such as UTC, define the second based on an atomic property of the cesium atom, and thus standard seconds are produced by cesium oscillators. Earlier time scales

(including earlier versions of Universal Time) were based on astronomical observations that measured the frequency of the Earth’s rotation.

TLS

Transport Layer Security — a cryptographic protocol that secures communications between systems over a network. Tenable scans identify TLS misconfigurations including expired or self-signed certificates, use of deprecated protocol versions (TLS 1.0, TLS 1.1, SSL 3.0), weak cipher suites, and improper certificate validation. Tenable provides detailed plugin output for TLS findings including remediation steps, enabling organizations to enforce strong encryption standards across their environment. Consolidate with 'transport layer security (TLS)' entry.

transparency

Amount of information that can be gathered about a supplier, product, or service and how far through the supply chain this information can be obtained.

transport layer security (TLS)

See TLS. Consolidate this entry with the TLS entry above to eliminate duplication.

trojan

In the machine learning context, a malicious modification to a model that is difficult to detect, may appear harmless, but that can alter the intended function of the system upon a signal from an attacker to cause a malicious behavior desired by the attacker. For Trojan attacks to be effective, the trigger must be rare in the normal operating environment so that it does not affect the normal effectiveness of the AI and raise the suspicions of users. In the machine learning context, trojan may be used interchangeably with backdoor pattern.

truncation

A process that shortens an input bitstring, preserving only a sub-string of a specified length.

trust

A belief that an entity meets certain expectations and therefore, can be relied upon.

tunneling

Technology enabling one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network.

two-factor authentication

Proof of the possession of a physical or software token in combination with some memorized secret knowledge.

U

uncredentialed scan

A vulnerability scan performed without authentication credentials, assessing only what is visible from the network — such as open ports, network services, and externally detectable software versions. Uncredentialed scans are faster and simpler to configure than credentialed scans but produce less comprehensive results, often missing vulnerabilities that require authenticated access to detect. Tenable recommends using uncredentialed scanning for external attack surface assessment and initial asset discovery, while using credentialed scanning for thorough internal vulnerability assessment. See also: credentialed scan.

V

virtual machine (VM)

A software-based emulation of a physical computer that runs an operating system and applications in an isolated environment. Tenable scans virtual machines as standard assets, assessing them for vulnerabilities and compliance issues using the same methods as physical hosts. Tenable integrates with VMware vSphere and cloud hypervisors to discover VMs across virtual infrastructure and ensure they are included in vulnerability management programs regardless of their power state or network visibility.

virtualization

The simulation of the software and/or hardware upon which other software runs.

VPN

A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network.

vulnerability assessment

A systematic evaluation of systems to identify and prioritize security vulnerabilities before attackers can exploit them. Tenable performs vulnerability assessment through multiple methods including network-based scanning with Tenable Nessus, agent-based assessment with Tenable Agent, cloud posture assessment with Tenable Cloud Security, and OT environment assessment with Tenable OT Security. Vulnerability assessment in Tenable produces detailed findings including CVE identifiers, CVSS and VPR severity scores, proof-of-concept details, and step-by-step remediation guidance. Results are aggregated in Tenable Vulnerability Management or Tenable Security Center for risk-based prioritization and remediation tracking.

vulnerability management

The continuous process of discovering assets, identifying vulnerabilities, prioritizing remediation, and measuring risk reduction across an organization's environment. Tenable provides vulnerability management through its Exposure Management Platform, with Tenable Vulnerability Management serving as the cloud-based VM solution and Tenable Security Center as the on-premises platform. Tenable's approach to vulnerability management is distinguished by Vulnerability Priority Rating (VPR), which incorporates real-world threat intelligence to prioritize the vulnerabilities that matter most, and Asset Criticality Rating (ACR), which factors in business impact. Tenable vulnerability management spans on-premises infrastructure, cloud environments, OT/ICS systems, containers, and web applications.

Vulnerability Priority Rating (VPR)

Tenable's proprietary risk scoring system that combines CVSS severity with real-world threat intelligence to help organizations prioritize which vulnerabilities to remediate first. Unlike CVSS, which measures the technical severity of a vulnerability, VPR incorporates dynamic threat data including active exploitation in the wild, availability of exploit code, malware campaigns, and threat actor activity. VPR scores range from 0.0 to 10.0 and are recalculated continuously as the threat landscape evolves. When Tenable Research observes a vulnerability being actively exploited, VPR scores increase automatically to reflect the heightened risk. Tenable Vulnerability Management and Tenable Security Center display VPR scores alongside CVSS scores, enabling security teams to focus remediation efforts on vulnerabilities that pose the greatest real-world risk to their organization.

vulnerability scanner

A tool that performs automated security assessments to identify vulnerabilities in systems. Tenable Nessus is the most widely deployed vulnerability scanner in the world, serving as the underlying scan engine for Tenable Vulnerability Management and Tenable Security Center. Tenable Nessus is available as Tenable Nessus Professional for individual security practitioners and Tenable Nessus Expert for advanced use cases including cloud discovery and infrastructure-as-code scanning. Tenable Nessus scanners execute plugins - detection scripts that check for specific vulnerabilities, misconfigurations, or compliance violations - and report findings to the Tenable platform for prioritization and remediation tracking.

vulnerability scanning

The automated process by which Tenable identifies security weaknesses in systems by executing Tenable Nessus plugins against target hosts. Vulnerability scanning in Tenable can be performed through network-based Tenable Nessus scanners, locally-installed Tenable Agent, or cloud connector integrations. Tenable scans detect missing patches, misconfigurations, weak credentials, and known CVEs across operating systems, applications, network devices, and cloud infrastructure. Scan results include severity ratings (Critical, High, Medium, Low, Info), CVSS scores, VPR scores, and detailed remediation guidance.

W

web browser

Client software used to view Web content.

web portal

Provides a single point of entry into the SOA for requester entities, enabling them to access Web services transparently from any device at virtually any location.

web server

A computer that provides World Wide Web (WWW) services on the Internet. It includes the hardware, operating system, Web server software, and Web site content (Web pages). If the Web server is used internally and not by the public, it may be known as an “intranet server.”.

web service

A software component or system designed to support interoperable machine- or application-oriented interaction over a network. A Web service has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards.

website

A set of related web pages that are prepared and maintained as a collection in support of a single purpose.

Z

zero trust

A security model based on the principle of 'never trust, always verify,' requiring continuous validation of every user, device, and connection before granting access to resources. Tenable enables zero trust architectures by providing the continuous asset visibility and vulnerability assessment that zero trust frameworks depend on — you cannot enforce least-privilege access to assets you cannot see or assess. Tenable Lumin and Tenable Identity

Exposure provide the asset risk context and identity security data needed to make informed, dynamic access decisions.

zero trust architecture

A security design approach that implements zero trust principles across an organization's systems, networks, and identity infrastructure. Tenable supports zero trust architecture by providing continuous visibility into asset inventory, vulnerability status, and identity exposure — the foundational data that zero trust policy engines require to make access decisions. Tenable Security Center and Tenable Vulnerability Management integrate with zero trust platforms to share risk context that informs dynamic access policies.