Tenable One Scoring Explained Quick Reference Guide

Last Revised: August 25, 2025

Table of Contents

Tenable One Scoring Explained: Overview

The building blocks for the Cyber Exposure Score (CES) in the Tenable One Exposure Management Platform are similar to those used for years in Tenable products (e.g., Tenable Vulnerability Management, Tenable Lumin). These mechanisms have to date only been used for vulnerability management data. Tenable One expands these concepts into new realms of the attack surface.

The following concepts are foundational to the scoring utilized in Tenable One:

- Vulnerability Priority Rating (VPR): The severity and exploitability of a given vulnerability. A vulnerability's VPR is expressed as a number from 0.1 to 10, with higher values corresponding to higher likelihood of the vulnerability leading to a compromise and a higher impact on the asset. This score is found in Tenable Vulnerability Management.
- Asset Criticality Rating (ACR): Rates the criticality of an asset to the organization. An asset's ACR is expressed as an integer from 1 to 10, with higher values corresponding to the asset being more critical to the business. This score is utilized in Tenable Lumin.
- Asset Exposure Score (AES): A combination of the VPR and ACR of a given asset.

Scoring (Beta) / Legacy Scoring

Tenable is currently updating the way scores are calculated by switching data models. This guide includes information about how scores are calculated using both the "new" and "legacy" Tenable data models.

For more information, see:

- Scoring (Beta)
- Legacy Scoring

Data Timing

Data within Tenable One refreshes on the following cadence:

- Asset Data: Asset information is updated every time the asset is seen as part of a scan.
- Tag Application: When a tag is first created, it can take several hours to assign the tag to the appropriate asset, depending on the number of asset and the tag's rules.
- Tag Reevaluation: Every 12 hours, Tenable One automatically reevaluates tags to ensure they apply to any new assets, and are removed from any inactive assets.

Scoring Caveats within Tenable One

The weakness counts and severities within the tab and other areas within the Tenable Inventory user interface may not match because each segment counts instances differently:

For Tenable Vulnerability Management assets:

- Weakness counts: Are distinct CVE counts
- Exposure score counts: Distinct (plugin ID, CVE ID) counts to allow for recasted plugins to affect exposure scores

For Tenable Web App Scanning assets:

- Weakness counts: Number of distinct CVEs + distinct plugins where the plugin has no CVEs but has a VPR
- Exposure score counts: Distinct plugin ID counts with VPR > 0. This is to account for plugin ID vulnerabilities with no CVE and to allow for recasted plugins to affect exposure scores

For Tenable Identity Exposure assets:

- Weakness counts: Distinct IoEs observed directly on the asset
- Exposure score counts: Includes IoEs observed directly on the asset plus those inherited from related assets to account for inherited IoEs in exposure scores

For Tenable Cloud Security assets:

- Weakness counts: Cloud Security misconfigurations plus any CVEs found on the asset
- Exposure score counts: Only Cloud Security misconfigurations are counted for exposure scores.

Scoring (Beta)

As a result of migrating the Tenable One data model, there have been several updates to the way scores are calculated across Tenable One.

Exposure Classes

The new scoring model includes the introduction of **Exposure Classes**. The exposure class of an asset or finding is determined by the sensor that assessed the asset or detected the finding. For example, an asset assessed by Tenable Nessus belongs to the Vulnerability Management (VM) exposure class. Likewise, a finding detected by Tenable Nessus is considered a VM finding.

The **Exposure Classes** are:

- Vulnerability Management (VM)
- Web Application Scanning (WAS)
- Identity (ID)
- Operational Technology (OT)
- Cloud Security (CS)
- Third Party

> **Note:** It is possible for an asset to belong to multiple exposure classes. Additionally, while the sensor determines the exposure class, not every sensor belongs to its own exposure class.

The key change to scoring is that an asset can now have multiple Asset Exposure Scores (AES) depending on what Exposure Classes it belongs to. Each asset also has a Global AES that aggregates the exposure information from all of the Exposure Classes to which it belongs. For example, an asset may have a VM AES, an Identity AES, and a Global AES.

While an asset can have multiple AES, it can only have one Asset Criticality Rating (ACR). If more than one ACR can be determined for an asset that belongs to multiple exposure classes, Tenable One uses a hierarchy of authority to determine the appropriate ACR for the asset.

To consistently compute the AES for an exposure class:

1. Calculate the **Vulnerability Density** for an asset based on whatever weaknesses are present and the associated severity of those weaknesses. Vulnerability Density is a function of the number of weaknesses on the asset and their severity as reflected by the VPR scores.
2. Combine the Vulnerability Density with the ACR (which can be model-generated or user-defined in the case of VM assets) and then scale the result to produce the AES for the given exposure class.

The Global AES for an asset follows the steps above, but instead pools weaknesses from all exposure classes to use in the Vulnerability Density calculation.

Tenable One calculates a Cyber Exposure Score (CES) for each exposure class by taking the average of the AES in each case. Additionally, Tenable One calculates the Global CES by averaging the Global AES. Each CES provides a different view of your Cyber Exposure.

Vulnerability Management (VM)

Vulnerability Priority Rating

The prioritization of vulnerabilities in Tenable Vulnerability Management is derived from the Vulnerability Priority Rating (VPR) which takes a risk-based approach to prioritization based on the characteristics of the vulnerability and threat intelligence.

Asset Criticality Rating

The Asset Criticality Rating (ACR) rates the criticality of an asset to the organization. An asset's ACR is expressed as an integer from 1 to 10, with higher values corresponding to the asset being more critical to the business.

Asset Exposure Score Computation

Each licensed asset belonging to the VM exposure class is given a score from 0 to 1000. Tenable One computes these values by weighing the VPR values of active weaknesses and the ACR.

Enhancements

Enhancements to Tenable Vulnerability Management scoring include:

- While CVSS classifies 60% of CVEs as High or Critical, our original VPR reduced this to 3%. VPR (Beta) now pushes this even further, focusing teams on just 1.6% of critical vulnerabilities. This means significantly reduced workloads and higher efficiency without compromising on risk.

- In addition to existing inputs like NVD and CVSS, VPR now incorporates data from the Tenable Security Response Team, Tenable Vulnerability Intelligence, cybersecurity web articles, and CISA. These provide greater visibility into actively exploited vulnerabilities.

- **(Not supported in FedRAMP environments)** Generative AI is now used to read curated web articles at scale and tag CVEs (e.g., targeted by ransomware, exploited in the wild, zero-day), helping predict near-term exploit likelihood. It also provides contextual metadata, including AI-driven threat summaries describing the vulnerability and past threat actor targeting, and remediation summaries detailing steps to take. This AI augments our human research experts, scaling our ability to monitor public data and news while providing clear, human-readable insights.

- VPR (Beta) provides more detailed information on why each score was assigned, facilitating greater explainability for the end-user. This includes lists of targeted regions and industries based on curated web articles, helping customers prioritize risks most relevant to them.

- VPR (Beta) places equal weighting on the "threat score" (derived from the likelihood of exploitation) and the "impact score" (from CVSS). This is a minor adjustment to the original VPR which places greater weight on the impact score.

- The ACR for VM assets is now based on the Global Asset Profile classification and subclassification of the assets.

- The Vulnerability Density computation is based on counts of CVE instances rather than plugin instances. CVE IDs provide a standardized enumeration of vulnerabilities.

- Since the Vulnerability Density computation is based on counts of CVE instances, it no longer makes sense to distinguish between local and remote detections. Instead, it is planned to incorporate whether a CVE can be remotely exploited or not in the VPR algorithm in the near future.

- Informational plugins are excluded from the Vulnerability Density calculation even if they have an associated CVE.

- Based on customer and internal feedback, we have adjusted the weakness severity weights used in the Vulnerability Density calculation. The weights for low and medium severity weaknesses have been reduced meaning these weaknesses individually increase the Vulnerability Density to a lesser degree than before. Conversely, the weights for high and critical vulnerabilities have been increased slightly. The result of these changes is that Tenable One highlights assets that have high or critical vulnerabilities to a greater degree than before.
- Previously, VM benchmarks were the average CES for the relevant group of containers (population or industry). VM benchmarks now consider the percentage of assets that a customer has scanned with authentication. For example, this means that the benchmark each customer sees is relative to their industry (or population) peers who scan a similar percentage of their assets with authentication. As a best practice, Tenable recommends using authenticated and agent-based scans wherever possible to gain a comprehensive insight into exposures.

  > **Tip:** For more information about Cyber Exposure Score (CES), see Cyber Exposure Score in the *Tenable Vulnerability Management User Guide*.

Web Application Scanning (WAS)

Vulnerability Priority Rating

In Tenable One, the concept of Vulnerability Priority Rating (VPR) extends to web application scanning. Where a web application detection is associated with a CVE, VPR scores already exist at the CVE level. For detections not associated with CVEs, such as OWASP Top 10 vulnerabilities, Tenable uses the Common Weakness Enumeration (CWE) as a surrogate to measure the threat for a given detection, and uses the CVSS vector for the detection to determine the potential impact.

Asset Criticality Rating

As with VPR, the concept of Asset Criticality Rating (ACR) extends to web applications. The algorithm is a function of three primary components:

- **Exposure**: Represents the extent to which the web application is exposed to external internet factors (e.g., "Crawler hidden, public internet facing web application")
- **Type**: Represents the character of the web application (e.g., "Moderately complex web application supporting legacy HTTP protocol access, using paid digital certificates with valid SSL certs")
- **Capabilities**: Represents the web application’s abilities, hinting at purpose (e.g., "Web application supports user logins, significant API usage, and handles PCI data")

These features and components are combined in a rules engine to produce the ACR for the web application being measured.

Asset Exposure Score Computation

Each licensed asset belonging to the WAS Exposure class is given a score from 0 to 1000. Tenable One computes these values by weighing the VPR values of active weaknesses and the ACR.

Enhancements

The weakness severity weights have been adjusted for the WAS exposure class vulnerability density calculation. The weights for low and medium plugins have been reduced. As in the VM exposure class, the result of these changes is that Tenable One highlights assets that have high or critical vulnerabilities to a greater degree than before.

Identity (ID)

Vulnerability Priority Rating

Tenable One assigns the Vulnerability Priority Rating (VPR) for ID weaknesses at the deviance (vulnerability/IOE) level based on the existing severity levels created in Tenable Identity Exposure:

- **Critical:** Weaknesses that can be used by an attacker with unprivileged access to compromise the Active Directory.
- **High:** Post-exploitation techniques or techniques that require chaining to be dangerous.
- **Medium:** Indicates a limited risk for the Active Directory infrastructures.

- **Low:** Weaknesses with low impact on the Active Directory. Certain business contexts may allow low-impact weaknesses that do not necessarily affect AD security.

> **Note:** Weaknesses cannot be observed directly on the identity asset type. Instead, the weaknesses on these assets are propagated from related assets (for example, accounts related to the identity, groups which the accounts are members of, tenants/domains which contain the accounts).

Asset Criticality Rating

Tenable Identity Exposure calculates the Asset Criticality Rating (ACR) for ID assets using two components:

- The **Hierarchy Component** looks at an individual's position within their company hierarchy.
    - This logic relies on the intuition that the higher the position of an individual within the hierarchy, the more access to business critical information they have.
    - This component considers the business title of the user and the scores of the user’s manager and subordinate.
- The **Entitlement Component** rates the user based on the level of access they have.
    - This component captures the level of access that an account has over other assets.
    - Accounts with high levels of privileges tend to have control over many resources in the environment, and can usually perform more “severe” actions such as update, delete, or change existing objects.

Tenable One weighs these two components and combines them to generate the ACR.

Asset Exposure Score Computation

Each licensed asset belonging to the ID exposure class that is either a user account or an identity is given a score from 0 to 1000. Tenable One computes these values by weighing the VPR values and the ACR.

The ID exposure class Cyber Exposure Score (CES) is the average of the AES across ONLY Identity assets. Because they already count towards the AES for Identity assets, Account assets are excluded from this calculation.

Likewise, the Global CES calculation for the ID exposure class only includes the Global AES from Identity assets.

Operational Technology (OT)

A major enhancement within Tenable One scoring is the addition of Operational Technology assets and their data, which are now visible throughout Tenable One.

OT asset exposure scores are imported directly from Tenable OT Security, but are scaled to range from 0-1000. When assigning risk scores for assets within the OT exposure class, Tenable One considers the following points:

- Real-time events that are relevant to a specific device and are detected over the network.
- Known vulnerabilities seen per asset.
- Asset Criticality based on the asset type.
- Mutual Backplane risk for controllers.

Cloud Security (CS)

Asset Exposure Score Computation

The cloud exposure score is based solely on the severity of findings detected on an asset. The severity of findings is dynamically determined in the Tenable Cloud Security product based on the asset, related assets features, and the features of misconfigurations found on an asset.

Severities are determined by several features, including:

- Ports open to the internet on an asset
- The severity of vulnerabilities detected
- The privileges and permissions to other assets

Scored Resource Types

Tenable One assigns Asset Exposure Scores to assets within the following categories:

- Virtual machines (e.g. EC2 instances, EC2 launch templates)
- Container repositories and clusters (e.g. ECR repository)
- Storage buckets (e.g. S3 buckets)

Asset Criticality Rating

ACR is not calculated for cloud assets. When an asset such as an EC2 instance is scanned with other sensors (for example, Nessus), then Tenable One takes the ACR from other exposure classes (mainly VM). ACR does not influence the AES.

Enhancements

Enhancements to Tenable Cloud Security scoring include:

- Dynamic severities take into account the context of an asset and related assets resulting in a more complete view of the exposure
- Tenable significantly reduced the number of cloud resource types that receive an Asset Exposure Score, resulting in a less diluted and more actionable Cyber Exposure Score.

Frequently Asked Questions

- *Q: Will the publicly accessible assets have a higher Asset Exposure Score score than assets that are not publicly available, even if they have the same vulnerabilities?*
  - A: Yes. The severity of findings on a publicly available asset is higher and the fact that an asset is publicly available is detected as an additional finding, which increases the AES.
- *Q: What impact does Asset Criticality Rating have on exposure scores?*
  - A: ACR has no impact on AES. The severity of findings used in the calculations already depend on asset details such as public/internet exposure or high level privileges.
- *Q: How many resource types receive an AES?*

- A: Currently, 15 resource types across three cloud providers (AWS, Azure, GCP) receive Asset Exposure Scores. The resources belong to three categories: virtual machines, docker containers, and storage.

Global

Tenable One assigns every licensed asset a Global Asset Exposure Score (AES) based on the aggregated weaknesses across all exposure classes to which the asset belongs.

Tenable One calculates the Global Vulnerability Density by combining the severity weights and weakness counts across all exposure classes for each asset. This Vulnerability Density is combined with the Asset Criticality Rating (ACR) to calculate the Global AES.

> **Note:** If an asset belongs to multiple exposure classes, the Global AES will be greater than or equal to the maximum AES across all applicable exposure classes.

Legacy Scoring

The first step in the scoring process is to calculate the AES of assets, which are then aggregated to the CES by taking an average of the AES values across a group of assets.

For Tenable One, a consistent approach for computing the AES across the categories involves the following:

1. Calculate the **Vulnerability Density** for an asset based on whatever weaknesses are present and the associated severity of those weaknesses. Vulnerability Density is defined as the number of vulnerabilities on that asset, their severity as reflected in the VPR scores and whether or not those vulnerabilities are remotely discoverable.
2. Combine this result with the ACR (which can be model-generated or user-defined in the case of VM assets) and then scale the result to produce the AES.

In addition to a CES for each of the categories, a Global CES is also generated by considering the AES across the entire attack surface assessed by Tenable One (i.e. assets from Tenable Vulnerability Management, Tenable Web App Scanning, Tenable Identity Exposure, and Legacy Tenable Cloud Security). Such scores are updated within hours of running a scan.

Computing Resources (Tenable Vulnerability Management and Tenable Lumin)

The following scores can be found within Computing Resources data sources.

Vulnerability Priority Rating

The prioritization of vulnerabilities in Tenable Vulnerability Management is derived from the Vulnerability Priority Rating (VPR) which takes a risk based approach to prioritization based on the characteristics of the vulnerability and threat intelligence.

Asset Criticality Rating

The Asset Criticality Rating (ACR) found in Tenable Lumin rates the criticality of an asset to the organization. An asset’s ACR is expressed as an integer from 1 to 10, with higher values corresponding to the asset being more critical to the business.

Asset Exposure Score Computation

In Tenable Lumin, each asset is given a score from 0 to 1000. These values are computed based on the weighting of the VPR values and the ACR.

Web Applications (Tenable Web App Scanning)

Vulnerability Priority Rating

In Tenable One, the concept of Vulnerability Priority Rating (VPR) extends to web application scanning. Where a web application detection is associated with a CVE, VPR scores already exist at the CVE level. For detections not associated with CVEs, such as OWASP Top 10 vulnerabilities, Tenable uses the Common Weakness Enumeration (CWE) as a surrogate to measure the threat for a given detection, and uses the CVSS vector for the detection to determine the potential impact.

Asset Criticality Rating

As with VPR, the concept of Asset Criticality Rating (ACR) extends to web applications. The algorithm is a function of three primary components:

- **Exposure**: Represents the extent to which the web application is exposed to external internet factors (e.g., "Crawler hidden, public internet facing web application")
- **Type**: Represents the character of the web application (e.g., "Moderately complex web application supporting legacy HTTP protocol access, using paid digital certificates with valid SSL certs")
- **Capabilities**: Represents the web application’s abilities, hinting at purpose (e.g., "Web application supports user logins, significant API usage, and handles PCI data")

Tenable combines these features and components in a rules engine to produce the ACR for the web application.

Cloud Resources (Tenable Cloud Security)

> **Note:** Currently, Tenable One only supports the ingestion of Tenable Cloud Security data. For more information, contact your Tenable Representative.

Vulnerability Priority Rating

When calculating the VPR for Cloud policy violations (detections), Tenable uses the NIST Common Configuration Scoring System (CCSS). This scoring system addresses software security configuration issues. CCSS is largely based on CVSS and CMSS, and it is intended to complement them. The CCSS metrics are organized into three groups: base, temporal, and environmental. Base metrics describe the characteristics of a configuration issue that are constant over time and across user environments. Temporal metrics describe the characteristics of configuration issues that can change over time but remain constant across user environments. Tenable uses environmental metrics to customize the base and temporal scores based on the characteristics of a specific user environment.

For each policy category, such as Encryption and Key Management, Tenable derives the confidentiality, integrity, and availability (CIA) impact and exploitability parameters based on the nature of the configuration issue. In CCSS, the Exploitation Method metric can be either Active (A) or Passive (P). Active misconfigurations can be actively exploited by an attacker (e.g., unencrypted S3 bucket) while passive misconfigurations make life tougher for defenders (e.g., logging is disabled). For Temporal & Environmental metrics, Tenable derives the exploit level using external threat sources while the remediation level is based on internal policy violation data.

Asset Criticality Rating

For ACR, Tenable maps cloud assets to higher level categories of exposure based on the resource type and features (properties) extracted from cloud resource configuration data:

- Access Exposure
- Key/Data Exposure
- Private/Internal Exposure
- Public Exposure
- VPC Misconfig
- Potential Vulnerabilities

Tenable assigns weights to these exposure categories based on publicly available incident data.

Identity (Tenable Identity Exposure)

Vulnerability Priority Rating

Tenable Identity Exposure assigns the VPR at the deviance (vulnerability) level based on the existing severity levels created in Tenable Identity Exposure:

- **Critical:** Deviances that can be used by an attacker with unprivileged access to compromise the Active Directory.
- **High:** Post exploitation techniques or techniques that require chaining to be dangerous.
- **Medium:** Indicates a limited risk for the Active Directory infrastructures.
- **Low:** Deviances with low impact on the Active Directory. Certain business contexts may allow low-impact deviances that do not necessarily affect AD security.

Asset Criticality Rating

Tenable Identity Exposure calculates ACR for user and computer accounts using a rule based system. Rules fall into three broad categories depending on the properties evaluated:

- **Capabilities**: Represents an objects capabilities within Tenable Identity Exposure. This is inferred from various properties of the asset. For example, a KRBTGT account or managed service account receives a high capability score.
- **Group Permissions**: Assets can have greater or lower levels of permissions depending on the groups they are members of. In particular, administrative groups and groups that have write access to other important objects. Examples of groups are DomainAdmins, DomainUsers, Administrators, and BackupOperators.
- **Object Type**: Looks at the user account control attribute of the object to score it. If the attribute contains one or more of the listed values (normal, disable, workstation, server, interdomain), then Tenable Identity Exposure assigns the asset a score.

Once Tenable Identity Exposure assigns each feature a score, it calculates the ACR by taking the maximum score observed and penalizing disabled accounts.