Tenable Cyber Exposure Study - Asset Inventory and Discovery

Last Revised: July 06, 2022

Table of Contents

Introduction 3

Asset Inventory & Discovery (SEE) Tenable.io Dashboard Widgets 5

Get Started - Establish the Foundation to Success 8

Asset Inventory Analysis and Review 9

Mapping, Classification, and Categorization of Assets 12

Key Asset Attributes 15

Introduction

The diverse location of assets makes it challenging to discover and identify assets. Understanding where critical assets are and accurately inventorying assets is the crucial first step in Risk-Based Vulnerability Management (RBVM). Through credentialed scanning, assets can be reliably identified and attributes collected, which enables organizations to establish and validate inventory management. Tenable.io helps validate and collect information needed to maintain a healthy asset inventory. As assets are discovered, an organization can begin to establish an inventory, which can be used to assess and mitigate associated risks to the organization.

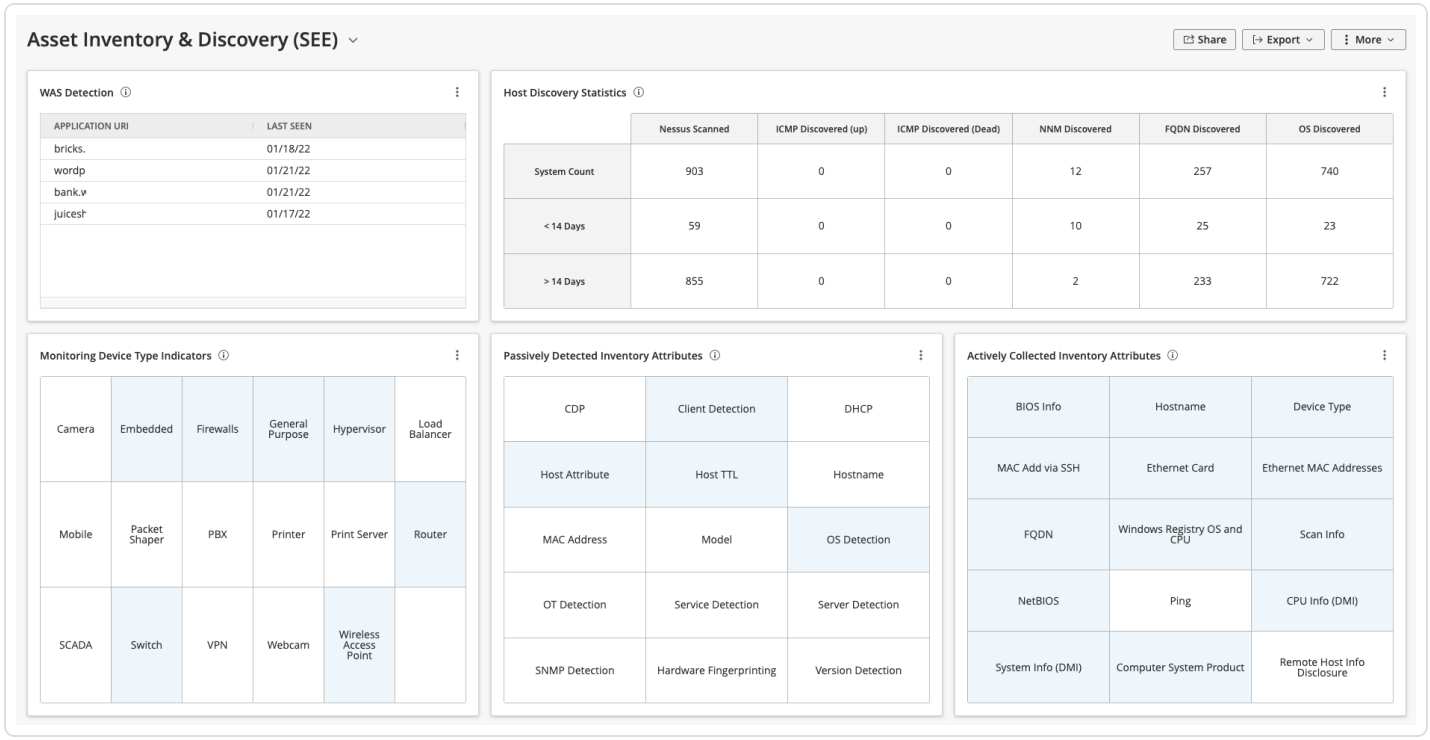
Attackers are not tied to a specific timezone and are continuously scanning the address space of target organizations, searching for new and possibly unprotected systems to be attached to the network. Transient devices, such as laptops or Bring-Your-Own-Device (BYOD) devices may be out of synchronization with security updates or already compromised providing a ripe attack vector. Often, hardware may be installed on the network one evening but not configured and patched with appropriate security updates until the following day, providing an easy target for exploitation. Devices that are not visible from the internet can be exploited by attackers who have already gained internal access and are hunting for internal pivot points.

Maintaining a comprehensive and up-to-date asset inventory is a fundamental and critical component of RBVM. Modern IT environments encompass on-premise, cloud infrastructure, mobile devices, ephemeral and transient assets, web applications, IoT devices, and more. Asset identification of all connected assets within an organization is a common baseline requirement in a number of security standards, such as NIST Special Publication 800-53 or General Data Protection Regulation (GDPR). Maintaining an asset inventory is also the critical first step in the *Discovery* phase of RBVM, allowing organizations to be more proactive. This document provides guidance to establish an asset inventory.

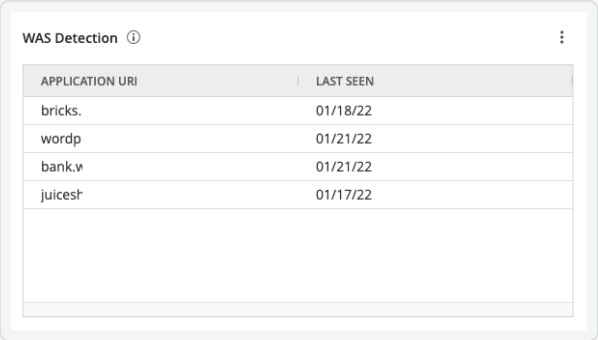
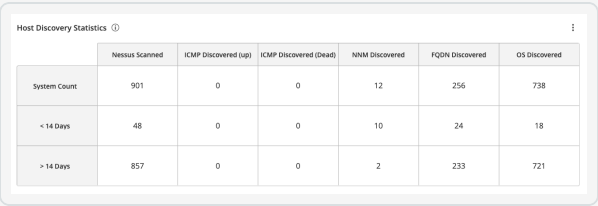
The first step of RBVM begins with asset discovery to identify and map every asset across the environment. Devices are detected through active scanning with Nessus and passive network analysis with Nessus Network Monitor to build a comprehensive list of assets and provide a clear picture of risk in the environment.

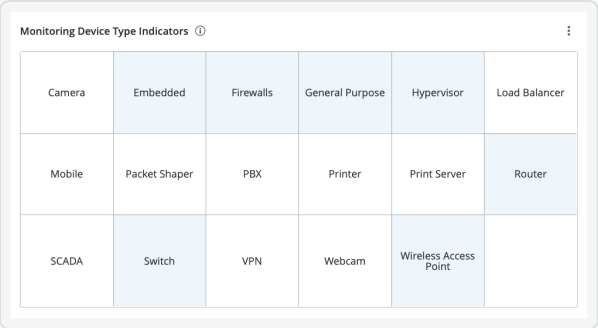
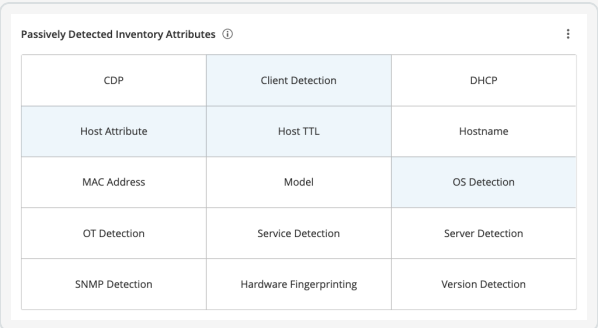
The Asset Inventory & Discovery (SEE) Tenable.io Dashboard displayed below provides guidance to establish an asset discovery, including:

- Actively and passively detected assets
- Asset discovery statistics
- Detected web applications
- Indications for device types (printers, cameras, routers, firewalls, WAPs)

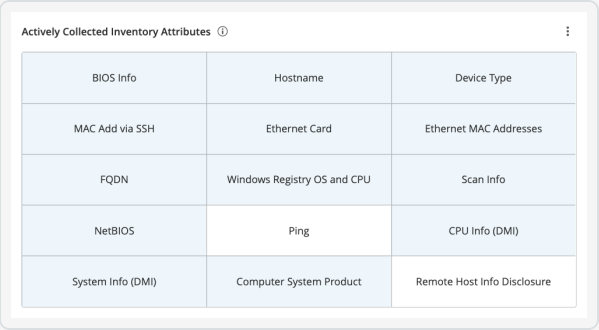


Asset Inventory & Discovery (SEE) Tenable.io Dashboard Widgets

Widget Description	Widget Image
The *WAS Detection* widget, which can be found in the Asset Inventory & Discovery (SEE) Tenable.io Dashboard and Tenable.io widget library, provides an updated list of Web Applications detected by Tenable.io WAS and displays the *Last Seen* date. When an application is selected, the vulnerability list and details for that web application are displayed. Developers and security teams can use this information to identify and categorize web applications.	
The *Host Discovery Statistics* widget, which can be found in the Asset Inventory & Discovery (SEE) Tenable.io Dashboard and Tenable.io widget library, provides a high-level view of host discovery. Each row depicts a different detection method, and each column uses the *Vulnerability First Seen* filter to identify when a plugin was first detected. The *Vulnerability First Seen* field is set when a plugin fires for the first time on an IP. Analysts can use this table to gain an understanding of how and when devices are first detected. The plugins used in this component are: • 12: Host TTL Discovered • 10180: Ping the Remote Host • 11936: OS Identification	

• 12053: Host Fully Qualified Domain Name (FQDN) Resolution • 19506: Nessus Scan Information	
The *Monitoring Device Type Indicators* widget, which can be found in the Asset Inventory & Discovery (SEE) Tenable.io Dashboard and Tenable.io widget library, uses the *Device Type* plugin and displays all existing device types. Plugin 54615 (Device Type) uses Nessus' OS fingerprinting ability to define the device type. There are 17 device types that are identified: camera, embedded, firewall, general purpose, hypervisor, load balancer, mobile, packet shaper, PBX, printer, print server, router, SCADA, switch, VPN, webcam, and wireless access point. When a device type is found, the indicator will change from white to blue. The data in this matrix does not count against the Tenable.io license.	
The *Passively Detected Inventory Attributes* widget, which can be found in the Asset Inventory & Discovery (SEE) Tenable.io Dashboard and Tenable.io widget library, displays passively collected asset attributes that can be used to build an asset inventory. When selected, each highlighted indicator provides a list of plugins with host counts. Analysts can then view the details of each discovered attribute.	

The *Actively Collected Inventory Attributes* widget, which can be found in the Asset Inventory & Discovery (SEE) Tenable.io Dashboard and Tenable.io widget library, displays actively collected asset attributes that can be used to build an asset inventory. When selected, each highlighted indicator provides a list of plugins with host counts. Analysts can then view the details of each discovered attribute.



Get Started - Establish the Foundation to Success

Assets, whether physical or virtual, connected to the network or not, can store or provide access to sensitive data. Organizations that begin with a strong asset discovery program can more easily establish an asset inventory that can be used to assess and mitigate risk.

All devices that connect to the network, regardless of connection duration, must be included in the asset inventory. Methods used to classify and categorize assets include:

- Identification via ARP, ICMP, TCP, SYN, and UDP
- OS fingerprinting
- Passively listening for talkers
- Frictionless Assessment (Scannerless/Agentless Cloud Asset Visibility)
- Data from switches and routers regarding connected devices
- NNM 6 (SIEM-collected DHCP Logging)

If network scanning is not yet fully deployed, switches and routers can be scanned with Nessus to find information about connected devices. This information can be used to build a scanning strategy, supplement discovery scans, or to confirm results from discovery scans.

Asset Inventory Analysis and Review

Use the following steps to analyze the business environment and lay a foundation for asset identification.

Identify and prioritize business-critical services and applications. This is a crucial step to ensure that assets are categorized by their significance to the organization. This includes items such as:

- Network diagrams
- Lists of known assets; If the organization does not have a current list of devices, a list of assets can be created by using SIEM-collected DHCP logs or other similar resources that track assets.
- Deployment roadmaps

Identify service and application owners and other stakeholders. This step is crucial if any questions arise during the discovery or classification phase, when new assets are discovered or assets are removed. For example, database teams know how many database servers are in operation, disaster recovery teams know how many failover devices are installed at each location, and web development and core infrastructure teams know where their devices are located.

Gather any required compliance requirements to ensure that identified assets are grouped together for compliance purposes. This may include devices that store or process financial information or health-related information, as there are specific regulatory requirements associated with this type of information. Finally, define a remediation workflow for how the organization will assess, analyze, and remove unauthorized devices.

Third-Party Integrations, Non-Traditional Assets, and Modern IT Assets

Organizations need a method to detect non-standard, sensitive, and ephemeral assets. Various methods can be used to detect non-standard assets, such as Operational Technology (OT) and ephemeral cloud assets.

Operational Technology

Operational Technology (OT) is commonly found across many industries including manufacturing, utilities (oil, gas, electric), maritime, rail, and aviation. Due to the convergence of IT and OT and the adoption of Industrial IoT (IIoT), IT environments can contain OT, and OT environments can contain IT. OT includes various types of devices, such as Industrial Control Systems (ICS), Human Machine Interfaces (HMIs), network devices, and IIoT. ICS, which includes Programmable Logic Controllers (PLCs), IO Modules, and Communication Adapters control processes that, if breached, could result in outages of critical components. An attack against OT systems could have significant impact or cause loss of life.

Tenable.ot has the ability to communicate with and passively monitor OT devices in each device's proprietary protocol to create an asset inventory. Tenable.ot can be configured and customized to the requirements of each unique environment. For more information about Tenable.ot, reference the Tenable.ot Product Page

Tenable.io Service Now Integration

The Tenable.io *Assets* View integrates with the ServiceNow Configuration Management Database (CMDB). The ServiceNow Identification Reconciliation Engine (IRE) reconciles the assets pulled in from Tenable.io and matches each asset to existing Configuration Items (CIs) to enrich the record with Tenable-discovered data and create a unified view of assets. This information can be used to create a more comprehensive asset inventory and vulnerability scanning strategy. For more information, reference: Tenable for ServiceNow Integration

Cloud Connector Integration

There are a number of Tenable.io Cloud Connectors available to assist with keeping an up-to-date, accurate asset count as cloud assets are deployed and decommissioned, such as: Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP). For more information, reference: Tenable Cloud Connectors Documentation

Frictionless Assessment

Frictionless Assessment (FA) leverages the AWS Systems Manager Inventory and AWS Systems Manager Agent (SSM Agent) to collect various data points from AWS EC2 instances and create an inventory of EC2 instances. FA is agent-less and scanner-less, because the Tenable Cloud Connector queries the API of specified Amazon accounts for assets and changes in asset state. Organ-

izations do not need to configure Nessus scanners, Nessus Agents, scans, or scan schedules to discover and assess assets with FA.

The most significant benefit of FA is the visibility of ephemeral cloud assets without the need to schedule scans or install scanners or agents. Every time an EC2 instance is provisioned in the AWS environment, the new asset is added to the Asset View in Tenable.io. The new asset can be automatically tagged as a new or rogue asset or tagged for more comprehensive scanning with a Nessus Scanner or Agent, if desired. If an AWS instance is decommissioned, Tenable.io will update the Asset View accordingly. FA Cloud Connector queries can be configured to poll for new assets as frequently as every 30 minutes to a maximum of seven days. FA requires the SSM Agent to be enabled and is limited to the vulnerabilities reported by the SSM Agent.

Data provided by FA includes:

- Changes in IP, FQDN, MAC, DNS, Instance ID Information
- AWS instance identification and configuration information
- Operating System
- System Type
- Shadow asset detection
- EC2 instance patch levels

More information on configuring FA can be found in: Frictionless Assessment for AWS.

Mapping, Classification, and Categorization of Assets

Once assets have been discovered across the attack surface, classifying and categorizing is the next crucial step. Ensure that collected data incorporates all assets, including OT, cloud assets, and container infrastructure, in addition to traditional on-premises IT assets. If a *Host Discovery Scan* still needs to be launched in Tenable.io, navigate to *Discover and Assess* under *Asset* View, select a *Discovery Method*, and choose the appropriate connectors. Classify assets to scope third party audits and ensure the appropriate assets are in scope for an audit. For example, the Payment Card Industry (PCI) mandates the PCI-DSS standard for assets that contain cardholder data. Organizations that are subject to third party PCI audits can reduce the cost of an audit by limiting in-scope IPs to only the assets that contain cardholder data. In addition to reducing the cost of the audit, limiting the scope to assets that contain cardholder data is more likely to result in passing an audit. Assets that do not contain cardholder data may not meet PCI control requirements and can introduce unnecessary risk of negative audit findings.

Identification is the process of matching a set of attributes collected by a sensor, such as Nessus, to an existing asset. If Tenable.io is unable to find an existing asset that matches the incoming asset, it is treated as a new asset and added to the Tenable.io *Asset* View.

Each identification request is based on a list of key-value pairs representing properties that have been collected to determine how assets are identified as unique. Tenable.io uses a subset of these properties, called *Identification Attributes* (IA), to determine if an asset has been previously seen.

The current list of IAs is:

- AWS EC2 Instance ID
- Azure VM ID
- GCP Instance ID
- BigFix Asset ID
- Tenable UUID
- BIOS UUID
- Network UUID
- MAC Address

- NetBIOS Name
- Fully Qualified Domain Name (FQDN)
- IPv4 address

IAs are ordered on a spectrum, from authoritative to speculative, based on their ability to accurately link a host to an existing asset. Internal IDs generated by cloud computing platforms, such as Amazon EC2, Microsoft Azure, and Google Cloud Platform (GCP), are 100% authoritative and unique. Every asset will have at most one value for an identifier in this class.

MAC Address, NetBIOS, FQDN, and IP are considered to be network-specific, depending on the network on which the asset resides. For an asset to be considered unique with the same MAC Address, NetBIOS, FQDN or IPv4, the asset needs to belong to the same defined *Network* in Tenable.io. For more information related to *Networks*, please refer to the Networks section of the documentation.

Query the Tenable.io API to identify additional asset attributes. Returned data can be filtered from various Tenable.io API endpoints based on asset attributes. Tenable.io also allows organizations to export asset details that include these attributes. The asset attributes are supported as filters or included in an export depending on the API endpoint that is in use. For a full list of asset attributes, consult the Common Asset Attributes document page. For more information on using the API to retrieve asset data from Tenable.io, please refer to Retrieving Asset Data From Tenable.io. For information on using the API to list assets, get individual asset information, import assets, and check the status of asset import jobs, reference the API Documentation for Assets. For more information about asset management, see *Assets* section of the Tenable.io Vulnerability Management User Guide.

As assets are identified, it is strongly recommended to categorize and group them using static and dynamic tags as well as Access Groups for permissions. Grouping assets together enables organizations to scan specific targets and control which users or groups can view and interact with specific assets. For additional information review: Access Groups

Identify and Categorize OT Devices

Tenable.ot customers have access to OT plugins in the 500000-599999 range. The *Device Type* value is collected from OT devices using these Tenable.ot plugins. The values returned in the plugin output are not controlled by Tenable.ot, but by the hardware vendor. For example, to identify all OT Controllers and modules, the following filter can be used:

- Plugin ID: 500000-599999
- Severity: INFO
- Plugin Output contains: superType: “Controllers”

OT assets can be tagged using the *Plugin Output* filter for the following categories:

- PLCs, Comm Adapters, IO Modules: category: "ControllersCategory"
- Everything else: category: "NetworkAssetsCategory"
- Cameras, Badge Access, UPS, Printers, non-ICS devices that are not IT-type: category: "IotCategory"

Addressing Unauthorized Assets

Unauthorized assets or shadow assets are unknown or not currently present in the asset inventory. These types of assets are typically left unpatched and unprotected and provide an open target to be exploited, providing a pivotal entry point to move through the network and reach critical assets and sensitive data.

Evaluate new assets that have recently been discovered or have not been assessed to determine whether they should be included in the organization’s asset inventory. Assess or remove these assets within 24 hours of detection.

For more information on identifying assets that have not been assessed, see: Identify Assets That Have Not Been Assessed.

Key Asset Attributes

There are a number of methods that can be used to collect key information to identify and categorize assets. Active scanning can perform high speed asset discovery, and Nessus can be installed on a variety of platforms, including Raspberry Pi. Nessus Agents can help organizations meet the challenges of obtaining vulnerability data from cloud environments, and Nessus Network Monitor (NNM) continuously monitors network traffic to detect new assets in on-premise environments. Most importantly, these sensors collect attributes that allow organizations to easily identify asset types for classification and categorization. The most important collected inventory attributes include:

- BIOS and Device Type
- Active and Passive OS Detection
- Active and Passive Asset Attributes:
- Ethernet (MAC/Vendor) Data
- FQDN
- Processor/System Information

Nessus is used to actively scan assets with a wide range of detection methods, such as banner grabbing, protocol detections, and advanced fingerprinting. Other items, such as hardware attributes that are collected passively, are also often part of hardware identification. Operating system detections are collected both passively and actively. Plugin outputs for the following plugins contain information that organizations may find useful in the classification and categorization process.

Useful plugins used for asset identification:

- 11936 - OS Identification
- 764487 - CDP Message Detection
- 50350 - OS Identification Failed
- 97993 - OS Identification and Installed Software Enumeration over SSH v2
- 34097 - BIOS Info (SMB)
- 34098 - BIOS Info (SSH)

- 34096 - BIOS Info (WMI)
- 55472 - Device Hostname
- 12053 - Host Fully Qualified Domain Name (FQDN) Resolution
- 54615 - Device Type
- 33276 - Enumerate MAC Addresses via SSH
- 35716 - Ethernet Card Manufacturer Detection
- 86420 - Ethernet MAC Addresses
- 12053 - Host Fully Qualified Domain Name (FQDN) Resolution
- 48942 - Microsoft Windows SMB Registry : OS Version and Processor Architecture
- 19506 - Nessus Scan Information
- 43815 - NetBIOS Multiple IP Address Enumeration
- 92372 - Microsoft Windows NetBIOS over TCP/IP Info
- 118730 - Windows NetBIOS / SMB Remote Host Report Tag
- 10180 - Ping the remote host
- 45432 - Processor Information (via DMI)
- 35351 - System Information Enumeration (via DMI)
- 48337 - Windows ComputerSystemProduct Enumeration (WMI)
- 42409 - Windows NetBIOS Remote Host Information Disclosure
- 1 - Passive OS Detection
- 7186 - DHCP Client Detection
- 7185 - DHCP Server / Client Detection
- 6640 - DHCPv6 client detection
- 6641 - DHCPv6 server detection

- 2313 - Host DHCP Address Release
- 7254 - Hostname Detection via DHCP

NNM Version 6 DHCP

NNM 6 provides security teams with the ability to poll events every five to ten minutes to identify assets from DHCP logs. NNM 6 queries DHCP logs from SIEM providers to record address assignment. In the DHCP exchange, many attributes of the asset are discovered and recorded to provide a choice of targets that may be added to a vulnerability scan. Organizations are often required to maintain an asset inventory to adhere to compliance standards, such as the CIS Critical Control 1. Security teams must have an accurate count of the assets on the network, including assets not owned by the organization to meet compliance requirements. Since many assets are not static, the likelihood of having full asset coverage in an active scan is slim. The data provided by NNM 6 can be leveraged to support compliance-based use cases, perform risk analysis, and establish new scan activities.