Attack Path FAQ

Quick Reference Guide

Last Revised: July 27, 2026

Table of Contents

Attack Path FAQ

The following are common questions and answers about Attack Path.

What data sources does Attack Path currently support?

Attack Path currently supports these Tenable products:

- Tenable One Vulnerability Management
- Tenable Security Center
- Tenable One Web App Scanning
- Tenable One Cloud Exposure
- Tenable One Identity Exposure
- Tenable One Attack Surface Management
- Tenable One OT Exposure

What is an Attack Path?

An attack path defines a source, a target, and one or more attack techniques leading an attack from the source to the target.

What is an attack technique?

Attack techniques represent 'how' an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access.

What attack techniques does Attack Path currently support?

For the complete list of attack techniques, see Attack Path Techniques.

How does Attack Path calculate attack paths?

Attack Path receives data and pairs it with advanced graph analytics, MITRE ATT&CK™, and Open Web Application Security Project® (OWASP) to map the possible attack techniques.

What triggers a specific Attack Path technique?

See the prerequisite section of each attack technique in Attack Path Attack Techniques to find the conditions that must exist for an attack query to run.

What is a finding shown on the **Findings** page?

A finding is an attack technique that exists in one or more attack paths leading to one or more critical assets.

What is a Choke Point?

A choke point is a place where potential attack paths merge together before reaching a critical asset. Attack Path uses a Choke Point Priority metric to determine the criticality of choke points.

How do you measure the severity of a finding?

The calculation includes mathematical algorithms, to assess the following:

- Likelihood: The number of attack paths using the technique associated with the finding.
- Impact: The number of critical assets that the technique allows an adversary to compromise.
- Method: The tactic associated with the technique such as lateral movement, privilege escalation, etc.
- Path: The starting point and ending point of the technique.

How does Attack Path determine if the asset is a Computer, Server, Workstation, or Domain Controller?

Attack Path determines the asset type as follows:

- Computer, Server, or Workstation – By parsing the operating system type and mapping it to the relevant type to determine if the asset is a Workstation, Server, or Computer.
- Domain Controller – By determining the domain controller through User Account Control.
- Other computer assets– By considering Computer as the base type for unknown assets.

When I delete an asset from **Findings** > **Asset**, how long does it take for Attack Path to remove that asset?

Attack Path triggers a data processing job every 30 minutes. Depending on the size of your data, it can take up to 5 hours for updates to reflect in Attack Path.

What are the different asset types inside the **Discover Query Builder**?

The **Discover** > **Query Builder** includes the following asset types:

Asset Types	Definition
CriticalAsset	• An asset with an Asset Criticality Rating (ACR) equal or greater than 7. • Other Tenable-defined static identifiers, such as domain administrators.
PrivilegedUser	A user account with administrator access on more than 10 devices.
DomainAdmin	A user account that is part of a group with full control of the domain including domain administrators, enterprise administrators, and

	administrators.
GlobalAdministrator	The global administrator is a user account with access to all administrative features in Microsoft Entra ID
ServiceAccount	A special type of non-human privileged account that can execute applications and run automated services, virtual machine instances, and other processes.
Executive	A human associated user account at the top of the organizational hierarchy, based on manager attribute in Windows-based systems.