Attack Path Comparison Quick Reference Guide

Last Revised: July 27, 2026

Table of Contents

Welcome

This document provides a high-level overview of the main differences between the Attack Path modules in Attack Path and the following Tenable products:

- Tenable One Identity Exposure
- Tenable One OT Exposure

For more information, see:

- *Attack Path User Guide*
- *Tenable One Identity Exposure User Guide*
- *Tenable One OT Exposure User Guide*

Overview

Tenable One includes multiple products that have a product page called **Attack Path**. Each product has similar search functionalities, where you can visualize an attack path by providing a start point and an end point (asset).

This document describes some of the main use cases and differences between the **Attack Path** modules of each product so that you can maximize your experience within the platform.

To get started, see the following topics:

- Differences Between Attack Path Analysis and Tenable One Identity Exposure
- Differences Between Attack Path Analysis and Tenable One OT Exposure

Differences Between Attack Path Analysis and Tenable One Identity Exposure

Attack Path and Tenable One Identity Exposure overlap mainly on the Active Directory attack techniques. The **Attack Path** modules for Attack Path and Tenable One Identity Exposure were designed to achieve different objectives.

Attack Path highlights exploitable and realistic attack paths, which an attacker would likely choose, whereas Tenable One Identity Exposure enables thorough exploration and visualization of the underlying security relationships of Active Directory. Therefore, Attack Path is based on the MITRE ATT&CK™ framework and supports attack techniques across the endpoint, network, and cloud, whereas Tenable One Identity Exposure focuses on Active Directory security.

When to Use Attack Path and Tenable One Identity Exposure

Attack Path was developed from the attacker point of view and it best suits cybersecurity practitioners such as blue and red teams. For Tenable One users, you can use Attack Path when you want to search for all probable attack paths within the entire security stack across the Cyber Kill Chain.

Although most Tenable One Identity Exposure Indicators of Exposure (IoEs) are included in the MITRE ATT&CK™ Framework and also supported in Attack Path, IT administrators and Active Directory Security Engineers should use Tenable One Identity Exposure for full context and visibility to the bits and bytes of Active Directory.

Differences Between Attack Path Analysis and Tenable One OT Exposure

Attack Path and Tenable One OT Exposure overlap mainly with OT/ICS assets. The Attack Path modules for Attack Path and Tenable One OT Exposure were designed to achieve different objectives.

Attack Path highlights exploitable and realistic attack paths with converged IT and OT assets, to show security relationships, which an attacker would likely choose. Tenable One OT Exposure, on the other hand, enables thorough exploration and visualization of the underlying connections between Operational Technology attack vectors. Therefore, Attack Path is based on the MITRE ATT&CK™ framework and supports attack techniques for IT, ICS, network, and cloud, whereas Tenable One OT Exposure focuses strictly on OT/ICS environments.

Inconsistencies in Attack Path Results

There may be inconsistencies when comparing the **Attack Path** results in Attack Path, Tenable One Identity Exposure, and Tenable One OT Exposure with the same source and target inputs. The following are some of the probable causes for such behavior:

- **Lack of MITRE ATT&CK™ coverage** – Tenable One Identity Exposure and Tenable One OT Exposure might support attack primitives, security relationships, or configurations that are not covered in MITRE ATT&CK™ Framework and as a result their results do not match with the attack path results in Attack Path.
- **Lack of Attack Path coverage** – Attack Path parsing capabilities may not be on par with Tenable One Identity Exposure and Tenable One OT Exposure in some cases. Tenable is aware of the lack of support in several scenarios of special Access Control Entry (ACE) or Access Control List (ACLs) and group policy object (GPO) settings where there may be false positive or false negative.
- **Attack Path is not exploitable** – Attack Path only shows attack paths that are “believed” to be feasible to exploit. Some security relationships that create a vulnerability in Tenable One Identity Exposure and Tenable One OT Exposure may not be considered exploitable in Attack Path. Such scenarios include vulnerabilities that can be mitigated by other controls such as network segmentation or endpoint hardening. It is important to note that such behavior is intended and therefore it is a feature and not a bug.
- **Unsynced data** – Unsynced data can cause inconsistencies between the products. Tenable One Identity Exposure and Tenable One OT Exposure have their own data collection service and are considered to be real-time. However, Attack Path relies on a data lake and receives data from various Tenable products. A delay to sync the data between Tenable One Identity Exposure, Tenable One OT Exposure, and Attack Path is expected.