tenable one
Exposure Management Platform

ATTACK PATH ANALYSIS

DATA SHEET

Navigating Complexity Across the Modern Attack Surface

The dependency on vulnerability management alone is insufficient for organizations to meet the demands of today's complex environments. These environments stray beyond traditional IT assets and encompass cloud platforms, microservices, web applications, identity services and others. This complexity creates what we know as the modern attack surface and it now requires a diverse range of specialized tools to effectively and accurately assess for vulnerabilities and misconfigurations. This is crucial in determining the organization's highest areas of risk, but even then, you still have siloed stacks of security data.

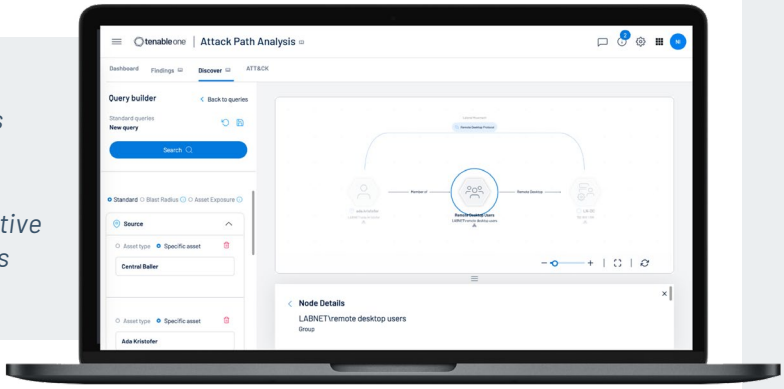
In the past, to do any form of aggregated, relationship-focused analysis, it had to be done manually. Security teams had to collaborate extensively to establish their own risk relationships and rely on their personal understanding of the infrastructure. This approach often resulted in incomplete perspectives of the environment, especially as new threats emerge on a daily basis, and environments along with the personnel who manages them are constantly shifting.

Proactive Security with Attack Path Analysis

Tenable One's Attack Path Analysis (APA) available in Tenable One Enterprise combines this rich context from siloed areas of your attack surface to take the guesswork out of security. The aggregated findings, assets, identities, privileges, and permissions are all correlated to help security leaders anticipate, prioritize and provide actionable insights. Up to this point, attack path analysis has primarily been used as a reactive tool in the event of an intrusion, enabling incident responders and forensic analysts to see where an attacker has been. It's now time to change this approach to prevent successful attacks.

Tenable APA puts such insights to use in a proactive way, enabling security professionals to prioritize remediations to apply choke points based on the exposures that are at the greatest risk of being leveraged in an attack path. This allows security teams to focus on what they've been hired to do: preventive security. As the organization's attack surface changes and the threat landscape evolves, so does the data reflected within Tenable One, so security teams always have the latest information they need to protect their organization.

Tenable Attack Path Analysis gives security teams the ability to take the attacker's perspective with context across their security data.



KEY BENEFITS

- **Use Prioritization to Inform Decisions**

  Take out your daily guesswork and know where to start first by viewing a list of your top exposures and threats that create attack paths.

- **Context from your Environment**

  Identify and prioritize attack paths based on your organization's unique context across the modern attack surface.

- **Take the Attacker's Perspective**

  See combinations of exposures that attackers can see that lead to lateral movement into unwanted access of your business critical assets.

- **Leverage MITRE ATT&CK**

  Stay up to date with how your environment compares against common adversary Tactics, Techniques and Procedures (TTPs) from MITRE ATT&CK.

- **Understand Relationships with Graph Modeling**

  Easily browse your environment to understand relationships and exposures in a graphical interface with additional details to focus mitigation efforts.

- **See Trend Lines and Heatmaps**

  Use various widgets and heatmaps to understand the latest trends from your environment.

Key Capabilities

Anticipate Critical Attack Paths

Anticipate and prioritize the most critical attack paths within your environment, just as attackers would see them, too. By leveraging advanced threat intelligence and analytics, Tenable's Attack Path Analysis empowers you to proactively identify and focus on the attack paths that pose the highest risk to your organization. This ensures that you can allocate your resources effectively and efficiently to mitigate potential threats.

Combine All Data Sources

Tenable's Attack Path Analysis solution incorporates your contextual data, offering unparalleled insights into your modern attack surface. By integrating seamlessly with your environment, our solution takes into account the unique characteristics of your infrastructure, applications, and users pulled from Tenable Vulnerability Management, Identity Exposure, Cloud Security and Web App Security. This understanding allows you to tailor your security strategies and responses to address the specific challenges and threats relevant to your organization.

Leverage the MITRE ATT&CK Framework

With Tenable's Attack Path Analysis, you can assess your organization's susceptibility to various attack techniques using the industry-standard MITRE ATT&CK framework. By mapping potential attack paths to the framework, you gain visibility into the techniques that pose the greatest risk. This knowledge empowers you to prioritize your security efforts and implement targeted countermeasures.

Map Relationships & Apply Choke Points

Explore your environment and its intricate relationships through intuitive visualizations and relationship mappings. These visual representations offer a clear and concise view, helping you identify hidden connections and potential attack paths. By visually mapping out the relationships between assets and vulnerabilities, you can easily comprehend the complexity of your environment and make well-informed decisions to strengthen your security posture and apply choke points.

AI-Powered Mitigation Guidance

Tenable leverages the power of artificial intelligence to deliver personalized and context-aware mitigation guidance for the most complex attack paths based on your unique environment. Analyze your specific context, combining threat intelligence and best practices, to receive step-by-step recommendations for mitigating the identified weaknesses. This ensures that you can effectively address complex attack paths no matter what your experience in security is.

Real-World View of Attack Paths

Tenable's Attack Path Analysis automatically draws and maintains the relationships among assets, vulnerabilities, and potential attack paths within your environment. By continuously updating this mapping, you have an up-to-date view of your attack surface as attackers perceive it. This real-time visibility ensures that you can stay ahead of emerging threats, respond swiftly to changes, and prioritize your security efforts effectively.

The Power of the Tenable One Platform

All within Tenable's Exposure Management Platform, combine data sources from Vulnerability Management, Identity Exposures, Cloud Security and Web Applications for effective Attack Path Analysis.

About Tenable

Tenable® is the Exposure Management company. Approximately 43,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies.