

DATASHEET

ATTACK PATH VALIDATION

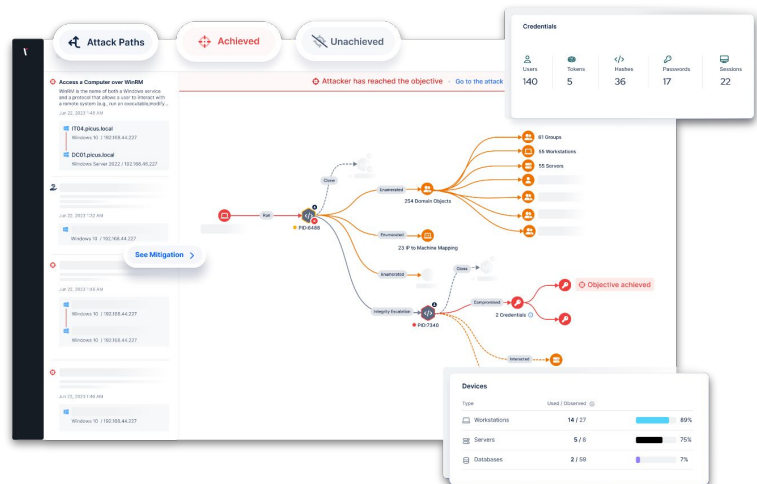
STOP ADVERSARIES IN THEIR TRACKS BY ELIMINATING THE ROUTES THEY COULD TAKE TO COMPROMISE YOUR USERS AND ASSETS

With cyber security breaches now an operational reality, it's essential to plan for the worst. Understanding how sophisticated adversaries with network access could accomplish their objectives is key to minimizing the potential impact of incidents.

Picus Attack Path Validation (APV) automatically discovers and visualizes the steps evasive attackers with initial access to an internal network could take to compromise critical servers, workstations and users.

Powered by Picus' **Intelligent Adversary Decision Engine**, this powerful tool simulates real-world attack techniques to identify high-risk attack paths and supplies actionable insights to remediate them.

 **Discover the shortest paths attackers could take to obtain domain admin privileges**



HOW ATTACK PATH VALIDATION STRENGTHENS YOUR INTERNAL NETWORK SECURITY

 **Reveals and validates paths to critical assets**

By simulating real-world adversary actions in your network, Picus APV identifies the shortest routes attackers could take to obtain domain admin privileges and verifies that they are actual paths that can be exploited, not ones that exist in theory.

 **Provides a broader view of high-risk attack paths**


Unlike manual red teaming exercises, which are conducted from a single initial access point, Picus APV provides a broader perspective by enabling you to run simulations from multiple areas of your network and obtain results in minutes, not weeks.

 **Helps prioritize vulnerabilities and misconfigurations**

Identify entities on your network where multiple attack paths converge and obtain mitigation recommendations to address vulnerabilities and misconfigurations at choke points to ensure you achieve the best security impact.

 **Hardens Active Directory security**

Mitigate weaknesses that could enable an attacker to compromise your Microsoft Active Directory and consequently gain control all users, systems and data in your environment.

 **Automates manual red teaming**

Automate offensive security testing to save time and money and to ensure that manual engagements deliver better outcomes, such as discovering unknown vulnerabilities.

 **Test security control effectiveness**

With Picus APV, gauge whether your organization's endpoint security is configured to detect and prevent lateral movement and other evasive techniques used by adversaries.

WHAT IS AN ATTACK PATH?

An attack path is a visualization of a route an attacker, that has breached an organization's network, could take to achieve an objective. Most organizations have thousands of potential attack paths that, if left unmanaged, continually grow and make it easy for cybercriminals to compromise critical assets.

Common exposures that attackers can exploit once inside a network include misconfigurations, poor identity and access management, inadequate network segmentation, and unpatched vulnerabilities.

HOW DOES PICUS HELP MANAGE ATTACK PATHS?

Picus Attack Path Validation strengthens internal network security by discovering and helping to disrupt the paths that, left unseen and unmanaged, could enable attackers to obtain Windows Domain Administrator credentials.

Unlike other solutions, Picus APV doesn't overwhelm security teams by revealing thousands of theoretical paths that are challenging to prioritize. Instead, it simulates the actions of a real-world attacker to discover the shortest path and verify that it poses a genuine risk.

Active Directory Security is a major issue for security teams since compromising the account of a domain admin could enable attackers to access critical systems and data, impersonate users, and achieve deep persistence.

AN INTELLIGENT APPROACH TO SIMULATION

Central to Picus APV is the product's **Intelligent Adversary Decision Engine**. Based on the results of network discovery and enumeration, it determines how to achieve the objective in the most efficient and evasive way possible.

Real-world actions simulated by Picus APV include:

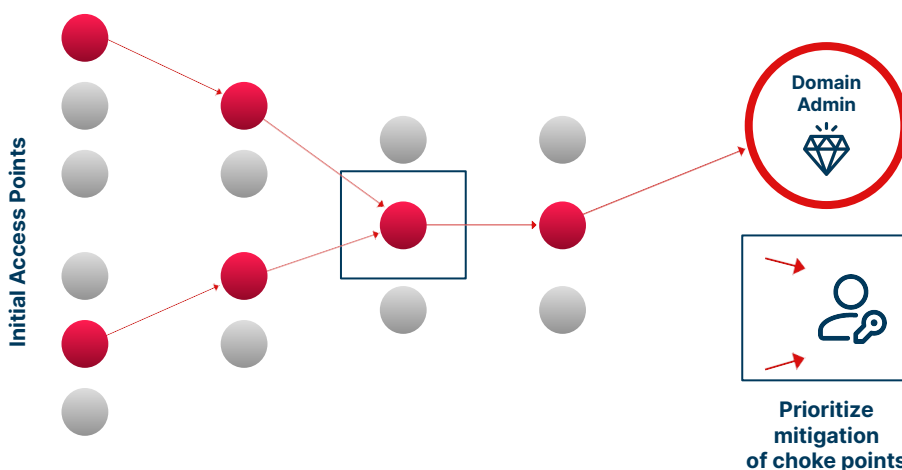
- ✓ Credential harvesting
- ✓ Password cracking
- ✓ Data Gathering
- ✓ Lateral movement
- ✓ Pivoting
- ✓ Privilege escalation
- ✓ Masquerading
- ✓ Relay
- ✓ Vulnerability exploitation
- ✓ Kerberoasting

PRIORITIZE REMEDIATION FOR MAXIMUM IMPACT

To provide a broader view than manual red team exercises, Picus APV makes it quick and easy to run simulations from multiple initial access points.

Identify the entities where multiple attack paths converge and prioritize mitigating vulnerabilities and misconfigurations at these choke points to maximize impact.

So you can harden your network security quickly, APV supplies mitigation recommendations for all actions successfully performed during an assessment.



KEY FEATURES

- ✓ **Automated attack path mapping**
Visualize high-risk attack paths and take swift action to remediate them.
- ✓ **Intelligent decision engine**
Get a realistic view by validating your security against evasive attacks simulations.
- ✓ **A library of real-life attack actions**
Discover attack paths by simulating the latest attack techniques, all mapped to the Unified Kill Chain.
- ✓ **Customizable assessment options**
Tailor simulations by defining the scope and actions that can be performed.
- ✓ **Mitigation suggestions**
Get insights to address vulnerabilities and misconfigurations.
- ✓ **Fully agentless deployment**
Execute a binary on an initial access point to trigger an assessment.

Identify and eliminate high risk attack paths



[LEARN MORE](#)



*average score at time of press in November 2023

www.picusecurity.com

  picusecurity

© 2023 Picus Security. All Rights Reserved.
All other product names, logos, and brands are property of their respective owners in the United States and/or other countries.