ATTIVO NETWORKS THREATPATH CYBER HYGIENE & ATTACK SURFACE REDUCTION

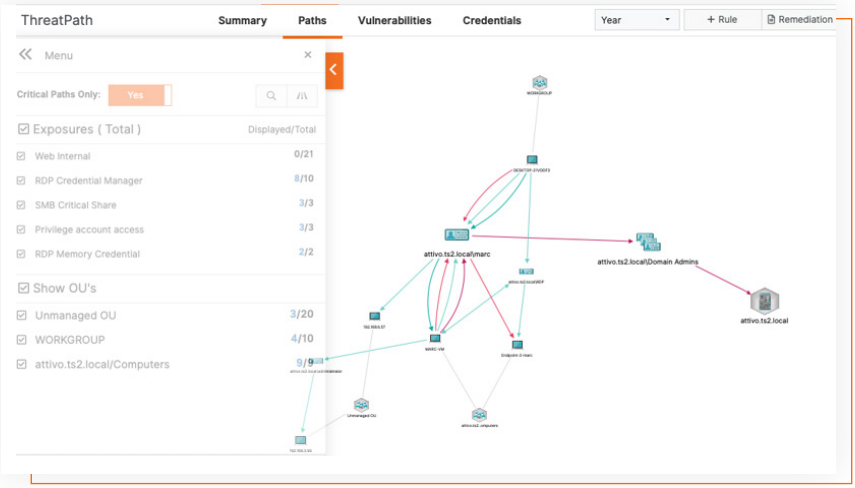
The Attivo ThreatPath® solution, part of the modular ThreatDefend Endpoint Detection Net family of products, provides continuous attack surface monitoring, reduce attack paths, and improves organizations cyber hygiene.

ATTIVO THREATPATH – CONTINUOUS ATTACK SURFACE REDUCTION

- ThreatPath provides visibility for organizations to defend against advanced attackers who move laterally across the network using stolen exposed credentials.
- Visualize how attackers can reach critical assets with exposed credentials that they can leverage. Uncover and remediate cached credentials in real time before attackers exploit them.
- Provides historical visibility into critical exposed paths, local admins accounts, Misconfigured SMB Shares, Browser credentials, etc.
- Get visibility into AD privileged accounts, Shadow admin accounts (Accounts with special ACL privileges that are left over on the endpoints) and AD Service Accounts.
- Check for risky ACLs and groups who have permission to them. Find groups with access to “Replicate Directory Changes’ ACL, groups with access to “Change Password”, etc.
- Monitor and get alerted on changes to AD Privileged Groups and risky ACLs using ThreatPath.

Enhances an organization’s cyber-hygiene by continuously monitoring and providing visibility into:

- Exposure of Enterprise Application Credentials
- AD Privileged Accounts
- AD Shadow Admin/ Delegated Accounts
- AD Service Accounts
- Local Admin Accounts
- Exposed Cloud Credentials
- Misconfigured SMB Network Shares
- Passwords Re-used Across Systems
- Exposed Web App Credentials



KEY PRODUCT FEATURES

Attack Surface Visibility

An interactive topographical map provides an intuitive view of how an attacker can move laterally from the initially-compromised system to other susceptible endpoints based on exploitable system configurations and stolen credentials. Visualize how attackers can reach critical assets and which credentials they can leverage.

Policy Rule Engine

Allows security practitioners to define rules to monitor exposed credentials for high value targets.

Remediation

Enforce policy violations and remediate credential exposures.

Good Cyber Hygiene Reduces the Organization's Attack Surface

- Remediate risky exposed credentials in real-time before attackers exploit them
- Identify paths that attackers can exploit to high value assets
- Discover which systems are at risk due to exposed credentials
- Find systems not adhering to the organization's best practices

Vulnerabilities & Misconfigurations

Apply policies that check for vulnerabilities and misconfigurations that attackers exploit to move laterally across the network.

DEPLOYMENT

- The Attivo ThreatPath solution can deploy across an organization's endpoints (Windows, Linux, & Mac OS) to provide immediate visibility into where its attack surface originates from.
- ThreatPath service consumes minimal CPU cycles, deploys as a service on endpoints to run periodically or on-demand to perform attack surface analysis.
- A management platform provides the means to search and assess risk across endpoints, view exposed credentials, etc.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in preventing identity privilege escalation and detecting lateral movement attacks, delivers a superior defense for countering threat activity. ThreatDefend® Platform customers gain unprecedented visibility to risks, attack surface reduction, and speed up attack detection. Patented innovative defenses cover critical points of attack, including at endpoints, in Active Directory (AD), in the cloud, and across the entire network. Concealment technology hides critical AD objects, data, and credentials. Bait and misdirection efficiently steer attackers away from production assets, and deception decoys derail lateral movement activities. Attivo has won over 150 awards for its technology innovation and leadership. www.attivonetworks.com.