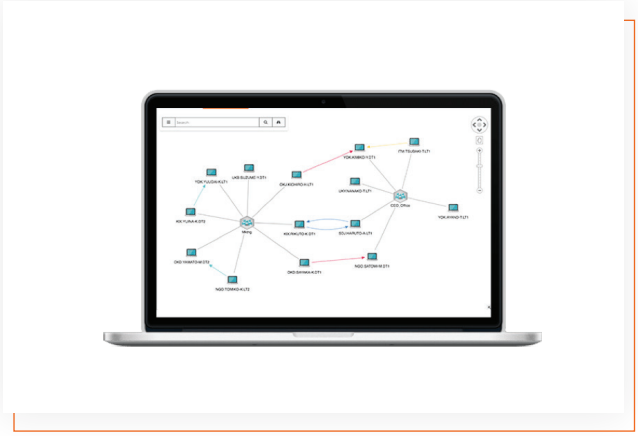
THREATPATH® ATTACK PATH VULNERABILITY ASSESSMENT

The Attivo ThreatPath® solution, part of the modular ThreatDefend Endpoint Detection Net family of products, provides continuous monitoring of attack surface vulnerabilities and risk reduction of lateral movement paths an attacker would take to compromise a network. The solution exposes and creates visual graphs of the avenues an attacker could traverse through the internal network based on misconfigured endpoints, active sessions, and risky cached or saved credentials. Organizations can activate native remediation options and integrations with workflow and incident management systems like Service Now and JIRA from inside the dashboard to automate remediation actions and processes. Collectively, these reduce an attacker's mobility and limits access to critical assets while giving organizations broad attack path situational awareness.

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. Click-throughs provide simple, detailed views of the weaknesses and system details needing isolation or remediation. Organizations can then use this information to decrease exposures based on severity and for insight into prime locations for planting decoy credentials.



ATTACK PATH VULNERABILITY REPORTING

The ThreatPath solution provides easy-to-understand views and reporting on attack path vulnerabilities that are within the network. The UI shows interactive maps and searchable, sortable, or filterable tables demonstrating the possible attacker lateral movement paths and provides actionable insights that organizations can use to strengthen policies and prevent attacker lateral movement. This feature provides continuous monitoring of the attack surface for "shadow" admins accounts, orphaned credentials, stored domain administrator accounts, and many more..

ATTACK PATH ALERTING

The ThreatPath solution provides continuous assessment of endpoints on the network and alerts when new attack paths open to critical assets. The solution instantly notifies security teams of credential policy violations or misconfigurations that arise.

ATTACK PATH VULNERABILITY REMEDIATION

The ThreatPath solution provides direct remediation of misconfigurations and exposed credentials by removing the corresponding saved credentials, shared folders, and vulnerabilities. The result is a reduction of the attack surface and elimination of attack avenues available to attackers. The solution dramatically simplifies Incident workflow management and trouble ticket creation with in-depth data of the compromised asset and double-click integrations to automate trouble ticket creation. Customers benefit from visibility into these workflows, closed-loop remediation, and reporting for handling compromised systems.

DECEPTION ASSET MANAGEMENT

Organizations can use the ThreatPath solution to view and download all ThreatStrike deception lures, simplifying deception asset management.

CONCLUSION

It is critical to understand and have visibility into attack path risks before they present an attacker with the opportunity to penetrate a network. The ThreatPath solution provides crucial continuous awareness into possible attack path vulnerabilities and offers simplified views of asset relationships and avenues that create the most significant risks. The ThreatPath solution adds pre-attack visibility, vulnerability assessment, and works seamlessly with the Attivo ThreatDefend® Platform to strengthen an organization's overall security defense. The ThreatDefend Platform provides comprehensive network, endpoint, data, and application deceptions that efficiently and accurately reveal in-network attacker presence, analyze the attack, and simplify incident response.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in cyber deception and lateral movement attack detection, delivers a superior defense for revealing and preventing unauthorized insider and external threat activity. The customer-proven Attivo ThreatDefend® Platform provides a scalable solution for derailing attackers and reducing the attack surface within user networks, data centers, clouds, remote worksites, and specialized attack surfaces. The portfolio defends at the endpoint, Active Directory and throughout the network with ground-breaking innovations for preventing and misdirecting lateral attack activity. Forensics, automated attack analysis, and third-party native integrations streamline incident response. The company has won over 130 awards for its technology innovation and leadership. For more information, visit www.attivonetworks.com.
Learn more: www.attivonetworks.com