USE CASE

# ENDPOINT DETECTION NET (EDN) SUITE USE CASES

Attivo NETWORKS

Now more than ever, it is critical for organizations to protect their endpoints and prevent attackers from spreading throughout the network. Most will use various forms of Endpoint Protection Platforms and Endpoint Detection and Response solutions to defend endpoints from attacks. The Attivo Networks® Endpoint Detection Net (EDN) suite provides capabilities that complement these existing endpoint security solutions. It achieves this by ambushing attackers at the endpoint, detecting them early in the attack cycle, and denying their lateral movement. The EDN suite creates an environment where every endpoint becomes a decoy, designed to disrupt an attacker's ability to break out and further infiltrate the network. It does this without requiring agents on the endpoint or causing disruption to the regular endpoint or network operations. The solution's ability to collect forensic data on all attack activity gives organizations company-centric adversary intelligence to enhance their security posture and strengthen defenses.

The following use cases highlight the capabilities that the EDN suite provides.

## PROTECT ACTIVE DIRECTORY (AD) DATA FROM THEFT AND EXPLOITATION

Attackers query AD from an endpoint to extract information on privileged domain accounts, systems, and other high-value objects. They use this information to compromise accounts, elevate privileges, and move laterally to access critical organizational data. The EDN suite returns fake Active Directory results, making an attacker's tools and reconnaissance untrustworthy while redirecting the attacker's focus and efforts into a decoy environment. The organization gains early alerting on attempts to access AD data while obscuring the attack surface, misinforming the attacker, and misdirecting the attack.

## PROTECT ENDPOINT CREDENTIALS FROM THEFT

Attackers steal stored or in-memory credentials to reuse for access to production assets. The EDN suite creates deceptive credential lures that breadcrumb attacks into a decoy environment. The organization gains early alerting of credential theft attacks while misdirecting the attack into the decoy environment for forensic collection. The organization can then use this adversary intelligence to strengthen defenses.

## PREVENT ATTACKERS FROM TRAVERSING AND EXPLOITING MAPPED SHARES

Attackers access mapped shares on the endpoint to compromise the file server (such as with ransomware). The EDN suite creates hidden shares that lead to decoy file servers that alert on the activity while recording it. If the attack involves ransomware, the high-interaction deception occupies the malware, giving the organization time to respond while limiting the damage to decoy files with no production value.


© 2020 Attivo Networks. All rights reserved.

## REDUCE THE EFFECTIVENESS OF NETWORK RECONNAISSANCE

Attackers scan network segments and endpoints to find production assets and available services. The EDN suite disrupts attacker attempts to discover other systems to compromise through the network decoys projected throughout the network that obfuscate the attack surface with systems that appear identical to production assets.

## REDUCE THE ATTACK SURFACE AVAILABLE FOR ATTACKER EXPLOITATION

Attackers leverage stored or orphaned credentials, or endpoint policy misconfigurations to move from system to system. The EDN suite preemptively identifies and remediates these lateral attack paths before attackers can use them, reducing the available attack surface while improving existing defenses.

## DETECT AND PROTECT AGAINST MAN-IN-THE-MIDDLE ATTACKS

Attacks conduct Man-in-the-Middle attacks to steal credentials as they traverse the network. The EDN suite detects MitM activity with decoys on every network segment, giving the organization early alerting on the event while feeding attackers fake credentials that lead to decoys. Attempts to use these credentials generate alerts while the decoys collect forensic evidence for later analysis.

## SUMMARY

The use cases highlighted above showcase the capabilities that the EDN suite provides for organizations to bridge coverage gaps and improve security. The EDN suite portfolio includes the ThreatStrike® deceptive credentials and mapped shares, the ThreatPath® assessment tool to identify credential exposures and lateral paths, and the ADSecure module to protect against unauthorized Active Directory queries. These capabilities provide the means to strengthen existing defenses, detect and alert on attackers as they attempt to move from an endpoint, misinform them as they gather information, and misdirect them to decoys for engagement when deployed with a BOTink® deception server. The solution works in tandem with existing EPP, and EDR controls to defend the endpoint more effectively, acting as a force multiplier to detect and deny attackers the ability to move deeper into the network while remaining undetected.

## ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in deception technology, provides organizations of all sizes with an active defense for early and accurate threat detection. The Attivo ThreatDefend® Platform delivers comprehensive detection for on-premises, cloud, and specialized attack surfaces with a deception fabric designed to efficiently misdirect and reveal attacks from all threat vectors. High-fidelity alerts are backed with company-centric threat intelligence and automated attack analysis, forensics, native integrations streamline incident response. The company has won over 130+ awards for its technology innovation and leadership. Learn more: www.attivonetworks.com

© 2020 Attivo Networks. All rights reserved.