DATASHEET

Attivo NETWORKS®

DEFLECT ATTACKS WITH THE ENDPOINT DETECTION NET SUITE

Attackers have a myriad of ways to evade defenses to gain an initial beachhead on an internal system, but they must then move laterally to expand their foothold. They conduct discovery activities to find live systems that they then scan for open ports and services to exploit. The Attivo Networks® Endpoint Detection Net (EDN) solution includes the Deflect function, which detects malicious East/West threat activity and disrupts reconnaissance, preventing accurate fingerprinting of internal systems and redirecting attackers to decoys for engagement.

LATERAL MOVEMENT THREAT DETECTION

Organizations have perimeter defenses to prevent threats outside the network from getting in. These perimeter controls, such as firewalls, proxies, and Intrusion Detection/Prevention Systems (IDPS), look at what is commonly known as North/South traffic, communications to and from the internal network to the Internet. They look for signatures or behaviors that indicate malicious traffic and block it. Fewer organizations monitor East/West traffic, communications between one internal host (for example, a server in a datacenter) and another internal host. This lack of East/West traffic monitoring is what attackers leverage to move around laterally inside the network while remaining undiscovered.

Monitoring East/West traffic and identifying lateral movement can be problematic because the volume of traffic generated between systems can be overwhelming. There are many choices available to monitor internal traffic with current security controls, but they have downsides:

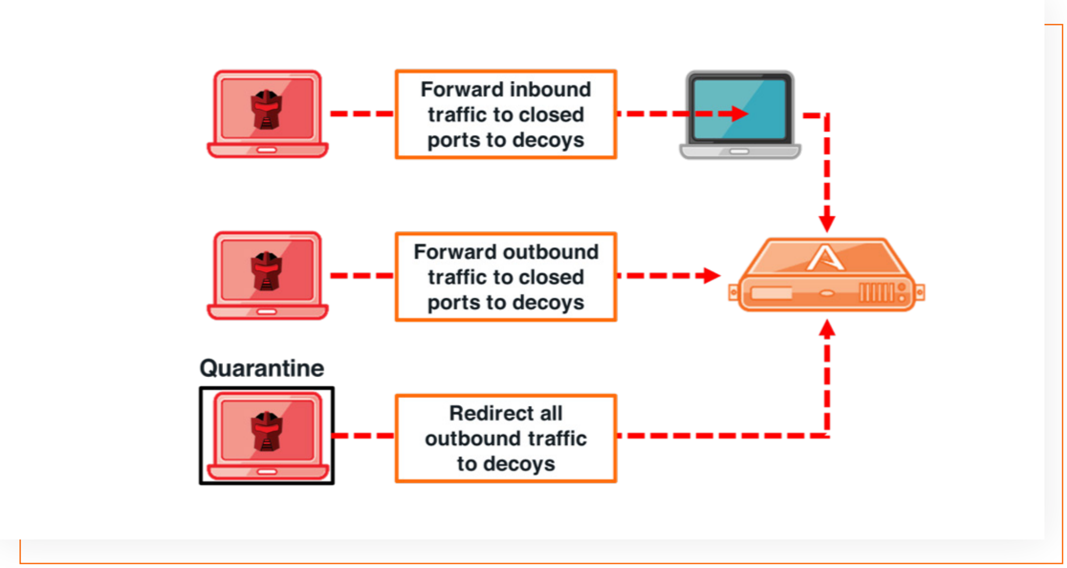
METHOD	PROS	CONS
Endpoint Logging	Native capability with modern OSes	Problems with storage and analysis at scale, must configure enterprise-wide
EDR Agent	Native capability with most EDR solutions	Problems with storage and analysis at scale, often a manual process
Netflow	Native capability with most core routers and switches	Negative impact on network performance, problems with storage at scale
Internal Firewalls	Repurpose older equipment for internal segmentation	Extra infrastructure and rules sets, scaling issues with logs and analysis
Internal IDPS	Repurpose older equipment for internal segmentation	Signature-based detection can miss threats, deployment challenges
Network Traffic Analysis	Accurate capability for in-network detection	Inefficiencies with storage and analysis at scale, challenging to tune, visibility issues

Once an attacker enters the network, they look around for other systems to compromise by conducting reconnaissance and discovery activities. When they find a live host, they fingerprint the system by scanning for open ports to identify available services and corresponding software versions. They use this information to target vulnerabilities or use exploits that give them access to the system, which was the case with the Heartbleed bug for OpenSSL and EternalBlue for SMBv1. Once they break into the system, they repeat the process, expanding their footprint, and maintaining persistence. These tactics and techniques often get overlooked as servers expect to communicate with other systems over ports where they offer services.

The method introduced by the Attivo Networks ThreatDefend® platform's EDN suite is a function called Deflect, which disrupts the attacker's ability to move laterally undetected.

EDN DEFLECT FOR EAST/WEST THREAT DETECTION AND ISOLATION

The EDN Deflect function is a module that deploys to endpoints to make them part of the deception fabric. The Deflect function identifies inbound or outbound discovery and lateral movement activity and disrupts the attacker's ability to fingerprint a system accurately. The function detects and alerts on traffic that touches a protected endpoint and forwards any communications that hit closed ports to decoys with a corresponding open port and service. It does not interfere with existing open ports and services. Since the attackers receive responses from any connection attempt, they can't get a clear picture of what services a given host offers. Any system with the Deflect function would appear to respond to the attacker with what they expect from the port and service. The Deflect function catches attackers early in the reconnaissance phase of their attack cycle, giving organizations a fighting chance to defend themselves before attackers can move laterally to find critical data.


Forward inbound traffic to closed ports to decoys
Forward outbound traffic to closed ports to decoys
Quarantine
Redirect all outbound traffic to decoys

For example, if attackers check port 80 on a protected Windows computer, the system would forward the traffic to a decoy web server, which would respond, making it seem like the Windows computer was a web server instead of a regular desktop. Meanwhile, the attackers would communicate with the decoy, which would generate alerts and record their interactions.

Because the Deflect function also handles outbound traffic from a host, organizations can use it to isolate an attacking system so it can only talk to the ThreatDefend platform's decoys and not to production assets. The Deflect function can forward all outbound traffic to the deception environment, so no matter where the attackers attempt to go, they only talk to the decoys.

CONCLUSION

The EDN Deflect function brings a needed capability to make every endpoint a part of the deception fabric. By denying attackers the ability to collect accurate information on their targets and disrupt their ability to move laterally undetected, the Deflect function gives organizations an early warning and an active defense against malicious East/West traffic to increase their security posture and catch attackers early in the attack cycle.

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