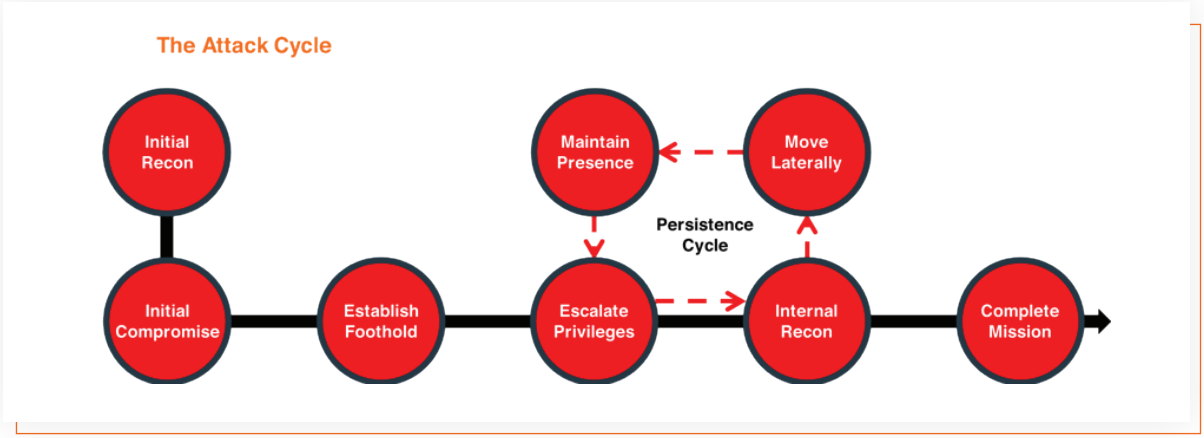
Attivo NETWORKS

LATERAL MOVEMENT DEFENSE

Prevent In-Network Attacker Lateral Movement

Attackers have proven they can evade the perimeter to establish a beachhead inside a network from which they can laterally move while remaining undetected, often for months to years. Traditional security controls are simply not designed to stop the in-network tactics that attackers use to elude detection while traversing the network. The Attivo Networks ThreatDefend® platform is uniquely equipped to prevent, detect, and reveal these tactics while denying attackers visibility and access to sensitive or critical data to exploit.

UNDERSTANDING ADVANCED ATTACKS



The above graphic is a representation of a typical attack cycle.

The first system an attacker compromises from outside is just a beachhead, usually accomplished using social engineering (such as phishing emails) or exploiting externally vulnerable services.

Once an attacker compromises a host inside the network and establishes a foothold, they must ensure that they can always return to continue their attacks. They install back doors and remote access tools to establish persistence mechanisms, using covert communications channels to remain hidden. They must then break out from this initially compromised system to move around.

In the next stage of the attack, they conduct discovery activities to identify subsequent targets. They search the local system for data and credentials they can steal to progress their attacks. They also query Active Directory (AD)

from a domain-joined system and extract sensitive information, such as domain administrator accounts, domain controller addresses, service principal names, or Kerberos tickets. They can use this data to find targets, compromise systems, and elevate privileges. Many recent attacks involved attackers compromising Active Directory for lateral movement.

Many recent attacks involved attackers compromising Active Directory for lateral movement.

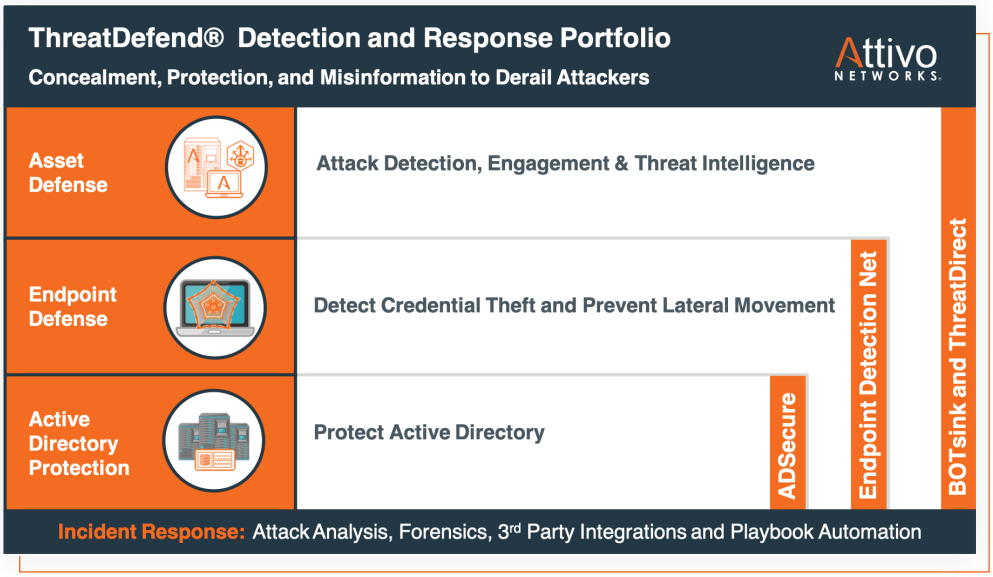
Once they identify their next targets, they fingerprint the systems for any open ports or services to exploit or use the data they gathered from AD to compromise them. They then move laterally to the target and install their persistence mechanisms.

Next, they look for sensitive or critical data to either use to further their attacks or exploit for gain. They repeat this cycle of discovery, credential theft, privilege escalation, lateral movement, and data collection until they complete their mission. These steps can occur in any order and often do.

PROVIDING IN-NETWORK DEFENSES WITH THE THREATDEFEND PLATFORM

Security solutions deployed inside the network, such as IDPS, segmentation firewalls, EDR, and EPP, are good at preventing known attacks from an initial compromise. However, these security controls can do little to detect in-network threat activity because attackers use native tools and advanced tactics to remain hidden. The Attivo Networks ThreatDefend platform takes a different approach, providing visibility and prevention against actions attackers must perform to conduct discovery, credential theft, privilege escalation, lateral movement, and data collection.

The ThreatDefend platform provides early and accurate detection of in-network threats, regardless of attack method or surface, using deception and concealment technologies. It provides a comprehensive protection fabric designed to confuse the attacker with disinformation on AD objects, credentials, shares, bait, and other decoys, and misdirections. Additionally, it hides sensitive or critical data to derail adversaries



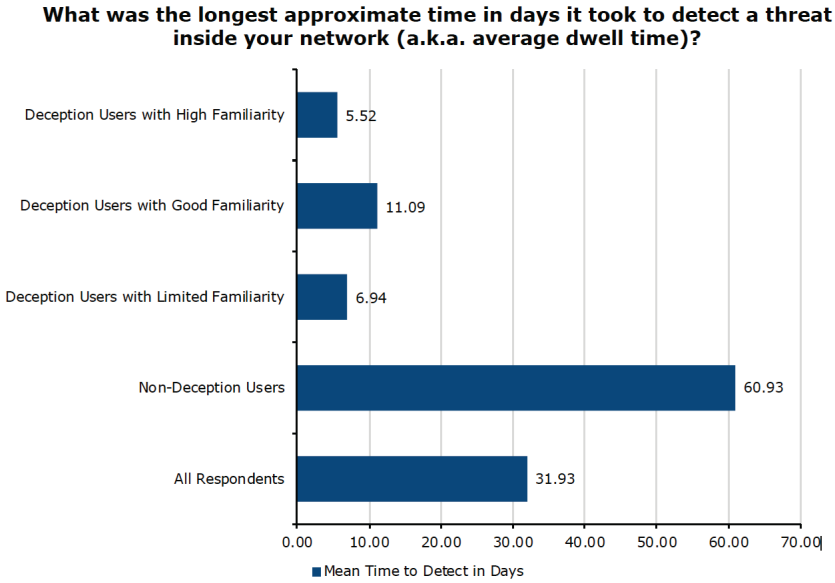
early in the attack lifecycle. Automated intelligence collection, attack analysis, and third-party integrations also aid security teams in accelerating incident response. Most AD security solutions focus on policies and infrastructure. The ThreatDefend platform uniquely focuses on detecting and protecting against attacks that target the data within AD, which is instrumental in derailing discovery, credential theft, privilege escalation, data collection, and lateral movement.

In alignment with MITRE Shield guidelines, the ThreatDefend Platform creates an active defense against attackers using its many modular components. In fact, DIY testing with the MITRE ATT&CK® evaluations shows a marked 42% improvement in detection performance over an EDR solution used alone. The Endpoint Detection Net (EDN) suite includes exposed credential and attack path visibility, deceptive credentials and lures to obfuscate the attack surface, concealment functions to hide and deny access to data, and the functionality to redirect malicious connection attempts to decoys for engagement. ADSecure for Active Directory defense comes either with the EDN suite or as a standalone solution. The Attivo BOTsink® deception servers provide decoys the native integrations for automated incident response, and the Informer dashboard displays gathered threat intelligence. The ThreatDirect deception forwarders support remote and segmented networks. The Attivo Central Manager (ACM) for BOTsink and the EDN Manager for standalone EDN deployments add enterprise-wide deception fabric management.

The ThreatDefend platform enhances existing security controls by efficiently adding internal network visibility, prevention, and detection for those tactics that attackers use to bypass traditional defenses, move laterally through the network, and escalate privileges.

Research shows that the ThreatDefend platform reduces dwell times by a factor of 12.

https://go.attivonetworks.com/rs/949-ZIG-021/images/A%20Definitve%20 market%20Guide%20to%20Deception%20Technology%20Research%20Paper2019.pdf



DENYING, DETECTING, AND DERAILING LATERAL MOVEMENT

The ThreatDefend platform provides visibility into and protection against attacker lateral movement across the network, as highlighted below:

DETECTING CREDENTIAL EXPOSURES

- Find exposed lateral movement paths using the ThreatPath solution and remediate them
- Analyze the presence of new user accounts, privilege accounts, or service accounts on endpoints, Active Directory using the ThreatPath solution

DENYING CREDENTIAL STEALING

- Deploy lures across all endpoints, raising alerts on theft and leading attackers to decoys

DENYING ACTIVE DIRECTORY DATA HARVESTING AND PRIVILEGE ESCALATION

- Prevent and detect kerberoasting attacks with the ADSecure solution by hiding the service accounts, thereby mitigating the risk of kerberoasting and silver ticket attacks while alerting in real-time
- Analyze the presence of attackers on domain-connected endpoints discovering privileges in Active Directory while getting real-time visibility into domain enumeration
- Detect and prevent attacker lateral movement from a domain-connected system

DENYING ACCESS TO DATA

- Deploy SMB mapped shares to decoys
- Apply concealment policies to restrict access to production network file shares, OneDrive mapped drives, or other sensitive storage from attacker tools
- Apply concealment policies to restrict access to data documents on endpoints from attacker tools

DERAILING INTERNAL DISCOVERY

- Deploy decoys mimicking critical servers, code repositories, databases, file servers, and other deceptive assets
- Deploy ThreatDirect (TD) forwarders, either TD-VM or TD-EP, across all subnets and expand deception coverage
- Deploy the ThreatDefend® Deflect function to detect port and service discovery activities – the Deflect function turns every endpoint into a decoy and engages attackers as they fingerprint and discover network services

CONCLUSION

The Attivo Networks ThreatDefend platform is customer-proven to reduce dwell times with early lateral movement detection. No other platform provides a cohesive detection fabric covering the enterprise on-premises, in the cloud, and at remote sites across the network, on endpoints, and in Active Directory. Security teams can benefit from the integration, visibility, information, and early detections that the platform provides to existing security controls.

Organizations gain the means to protect themselves against lateral movement and privilege escalation tactics of adversaries. The platform's unique functionality significantly enhances existing security controls. It serves as a critical defense layer to detect attackers conducting credential access, discovery, lateral movement, and collection activities. Investigators attribute the success of many recent high-profile security breaches to gaps in in-network lateral movement detection and protection. Organizations deploying the ThreatDefend platform will gain an efficient and powerful internal security control for closing these detection gaps and the time an attacker can remain undetected within their networks.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in lateral movement attack detection and privilege escalation prevention, delivers a superior defense for countering threat activity. Through cyber deception and other tactics, the Attivo ThreatDefend® Platform offers a customer-proven, scalable solution for denying, detecting, and derailing attackers and reducing attack surfaces without relying on signatures. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, in the cloud, and across the entire network by preventing and misdirecting attack activity. Forensics, automated attack analysis, and third-party integrations streamline incident response. Deception as a defense strategy continues to grow and is an integral part of NIST Special Publications and MITRE® Shield, and its capabilities tightly align to the MITRE ATT&CK® Framework. Attivo has won over 130 awards for its technology innovation and leadership.
www.attivonetworks.com

ANSB011321
www.attivonetworks.com