SOLUTION BRIEF

IDENTITY THREAT DETECTION AND RESPONSE

Attivo NETWORKS
A SentinelOne Company

The threat landscape has changed with the rapid migration to remote working and cloud migration. This change has effectively removed the network edge and driven companies to shift their security posture based on identities versus devices.

Identity Threat Detection and Response (ITDR) is a new security category explicitly designed to protect identities and the systems that manage them. IDR is not a replacement but instead, a complement to Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), Network Detection and Response (NDR), formerly known as Network Traffic Analysis, and other detection solutions. IDR is unlike these other solutions in that it looks for credential theft, misuse, privilege escalation, and identity exposures that create attack opportunities. IDR fills a significant gap in the identity security landscape, differentiating itself from identity protection systems such as Identity and Access Management (IAM), Privilege Access Management (PAM), or Identity Governance and Administration (IGA) that secure authentication and authorization. It represents a significant step forward, marking the introduction of a new category of security solutions.

THE NEED FOR ITDR

Identity-based attacks are on the rise, and today's organizations must detect when attackers exploit, misuse, or steal enterprise identities. Attackers increasingly use credentials and leverage Active Directory (AD) to progress their attacks. As organizations move to the public cloud and human/non-human identities increase exponentially, the need to protect identities and detect identity-based attack activity grows in priority.

Adopting solutions that protect identities is vital, given the damages occurring from identity misuse. Analyst research has found that credential data now factors into the majority of all breaches, highlighting that attackers consistently attempt to access valid credentials and exploit them to move throughout networks undetected. Credential misuse has also enabled the growth of attack tactics like Ransomware 2.0, with ransomware now making up a growing number of breaches[1].

WHAT IS ITDR AND WHY IS IT IMPORTANT?

At its core, ITDR detects credential theft and privilege misuse, attacks on Active Directory, and risky entitlements that create attack paths. In contrast to existing identity protection tools like IAM, PAM, or IGA that focus on authorization and authentication, ITDR solutions protect identities, entitlements, and the systems that manage them, ensuring the right people have access to the resources they need. ITDR provides visibility to credential misuse, entitlement exposures, and privilege escalation activities, extending from endpoint to AD and multi-cloud environments.

[1] Verizon Data Breach Investigations Report

In comparison to EDR, ITDR solutions operate similarly but focus on different things. EDR solutions look for attacks on endpoints and collect data for analysis, whereas ITDR solutions look for attacks targeting identities. When EDR detects an attack, it requires a response action to stop the process, isolate the system, or assist in the investigation. In contrast, an ITDR solution adds a layer of defense upon detecting an attack by providing fake data that redirects the attacker to a non-production asset like a decoy. It can also automatically isolate the compromised system conducting the identity-based attack from the rest of the network, limiting interaction only with the decoy environment. EDR tools and ITDR solutions can assist in the incident response by collecting forensic data and gathering telemetry on the processes used during the attack.

Some ITDR solutions can also manage the identity attack surface by providing visibility to exposures that leave enterprise identities open to attack. These exposures include credentials stored on endpoints, AD misconfigurations that allow attackers to extract data or conduct attacks, or excessive entitlements in cloud environments that give attackers access to sensitive or critical workloads and data. Reducing these exposures protects enterprise identities by limiting what attackers can target or exploit.

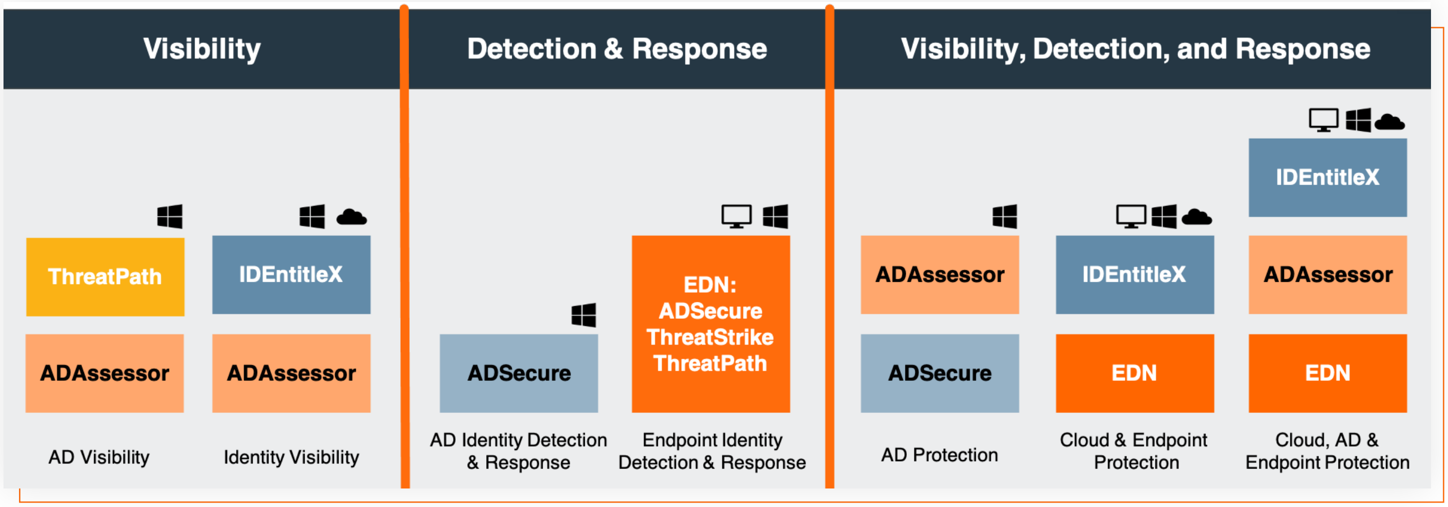
An increasing number of attacks leverage on-premises exploits to target the cloud. Organizations are dealing with the issues of permission sprawl with the volume of human and non-human identities they must manage, especially with the widespread shift to remote working, cloud migration, and increasing adoption of DevOps practices. This issue has emphasized the need to prevent attackers from obtaining excessive rights or the privileges to move across domains and cloud environments. ITDR solutions can seamlessly extend to the cloud and deliver detailed entitlement visibility for identities - including users, applications, containers, serverless functions, and other assets.

CONCLUSION

Today, identity security is central to the cybersecurity threat landscape, and the ability to detect and respond to identity-based threats is essential. While many tools intend to keep networks secure, ITDR gives organizations a critical new weapon in their arsenal to find and fix credential and entitlement weaknesses and detect live attacks on a real-time basis. As modern cybercriminals attempt to exploit vulnerable credentials and entitlements to move through networks undetected, ITDR solutions play a meaningful role in stopping them, whereas other tools simply cannot.

ATTIVO IDENTITY THREAT DETECTION AND RESPONSE SOLUTIONS

Attivo Networks has leveraged its deep experience in privilege escalation and lateral movement detection to become a significant player in the ITDR space. In the last year, the company has secured its leadership position based on its broad portfolio of ITDR solutions.



Visibility

ThreatPath
ADAssessor
AD Visibility

IDEntitleX
ADAssessor
Identity Visibility

Detection & Response

ADSecure
AD Identity Detection & Response

EDN:
ADSecure
ThreatStrike
ThreatPath
Endpoint Identity Detection & Response

Visibility, Detection, and Response

ADAssessor
ADSecure
AD Protection

IDEntitleX
EDN
Cloud & Endpoint Protection

IDEntitleX
ADAssessor
EDN
Cloud, AD & Endpoint Protection

ATTIVO IDENTITY SECURITY PRODUCTS:

- ADSecure for detection of unauthorized activity and attacks on Active Directory
- ADAssessor for continuous visibility to exposures with Active Directory& activities that would indicate an attack
- IDEntitleX for end-to-end visibility to cloud entitlement (CIEM) exposures
- Endpoint Detection Net (EDN) for protection against credential theft and misuse, prevention of Active Directory exploitation, attack path visibility, attack surface reduction, and lateral movement detection

ATTIVO IDENTITY BUNDLES:

- Identity Detection Bundle: Includes ADSecure as part of the EDN® suite, which provides a full Identity Threat Detection and Response (IDR) solution to detect AD attack, protect against credential theft and misuse, visualize attack paths, as well as detection for lateral movement.

- Endpoint Identity Visibility Bundle: Includes ADAssessor and EDN Suite's ThreatPath®, which gives a comprehensive view of threats and vulnerabilities that can provide access to AD. The solutions analyze endpoints to identify stored credentials and misconfigurations that attackers can compromise, continuously monitor exposed credentials and critical paths, and identify lateral attack paths. ThreatPath® finds, analyzes, and ranks by urgency any attack paths attackers may use.

- Identity Visibility Bundle: Includes ADAssessor with IDEntitleX, which adds visibility for overprovisioning and excess entitlement management across multi-cloud environments.

Learn more about Attivo's identity solutions here.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, a SentinelOne company, provides Identity Threat Detection and Response (ITDR) and cyber deception solutions for protecting against identity compromise, privilege escalation, and lateral movement attacks. Through data cloaking, misdirection, and cyber deception, the platform efficiently prevents attacks across Active Directory, cloud environments, and devices.

Follow us on Twitter @attivonetworks
Facebook | LinkedIn: AttivoNetworks