# GAIN ENTERPRISE-WIDE IDENTITY RISK VISIBILITY

Advanced attackers find many ways to evade security controls and infiltrate an organization's network. Once inside, they target identities within the enterprise to advance their attacks. Using the information they gather from endpoints, Active Directory, and the cloud, they compromise identities such as user, service, application, and administrator accounts to gain privileged access to the on-premises and cloud networks.

Organizations currently lack awareness of identity and entitlement risks that span across their network. They need solutions that provide visibility to these exposures that attackers take advantage of to progress their attacks, which the Attivo Networks Identity Solutions provide.

## THE IMPORTANCE OF VISIBILITY FOR THE IDENTITY ATTACK SURFACE

Attackers view these identities as the primary mechanism to laterally move once they've established a beachhead inside the network. Organizations generally consider enterprise identities as a means to authenticate and authorize a user to access the network and its resources and do not always have the necessary visibility into identity and entitlement security hygiene issues or have reliable visibility to exposures at the endpoints, in Active Directory, or the cloud. This lack of visibility makes it difficult to know when identity risks through exposures, misconfigurations, or overly permissive provisioning become vulnerabilities for attackers to target.

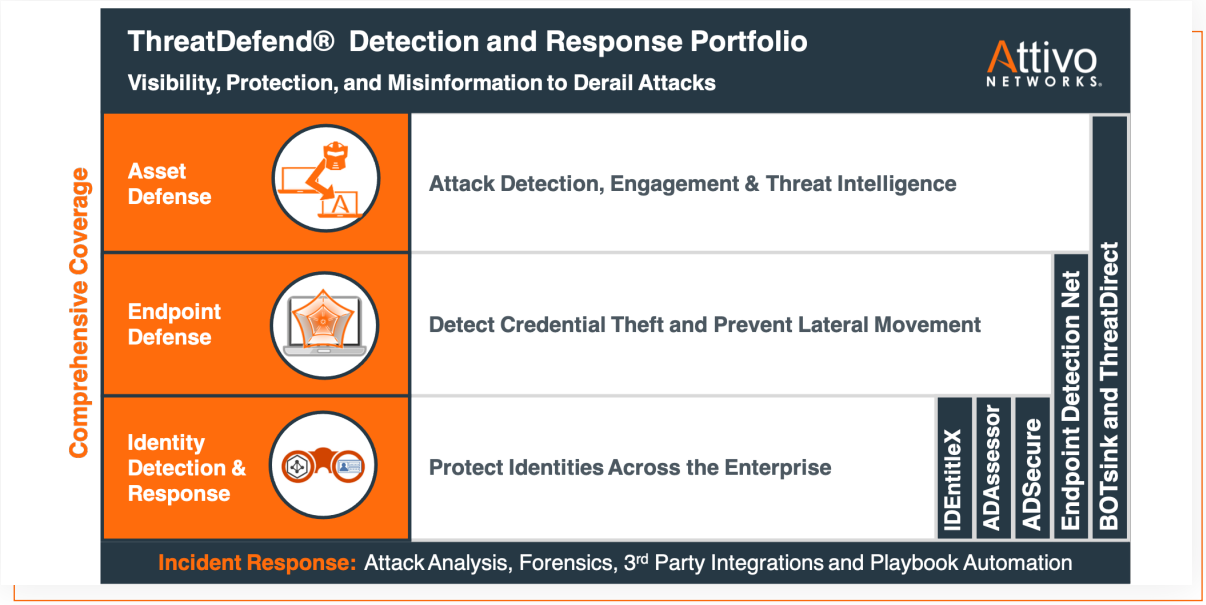
Security teams need adequate visibility to effectively manage identity risks and entitlement exposures across both on-premises and cloud environments, especially when network environments are more distributed than ever.

## THE ATTIVO NETWORKS IDENTITY SECURITY SOLUTIONS

The Attivo ThreatDefend® platform offers several solutions that collectively provide enterprise-wide visibility to identity risks and entitlement exposures, reducing the organization's identity attack surface at endpoints, in Active Directory, and the cloud. Attivo products that include visibility protection are the Endpoint Detection Net (EDN) suite (ThreatStrike®, ThreatPath®, ADSecure(also standalone), ADAssessor, and the IDEntitleX solutions. There are also identity bundles, which are available to simplify ordering.

The Attivo Networks EDN suite anticipates attacker methods to move laterally from infected endpoints and ambushes their moves with lures, bait, and misdirection to speed threat detection. The EDN suite boosts existing endpoint security detection performance by showing exposed credential attack paths, credential misuse, and

attempts to enumerate Active Directory (AD). Concealment technology hides and denies access to critical files, data, AD objects, and credentials. The suite delivers a comprehensive Identity Detection and Response (IDR) solution for preventing discovery, credential theft, privilege escalation, data collection, and lateral movement.



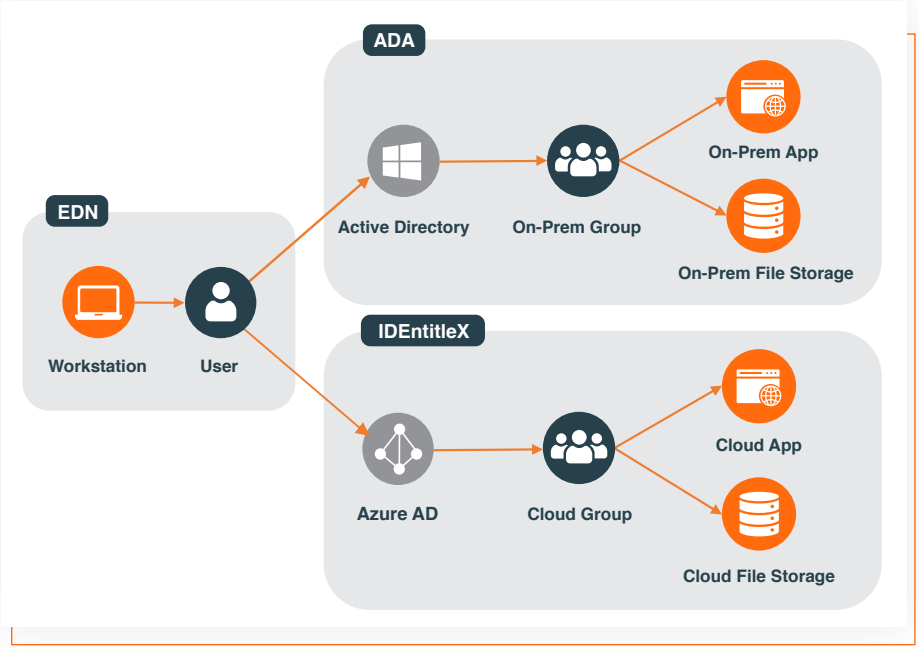

The EDN suite's ThreatStrike® endpoint module provides visibility to credential theft attempts by hiding and denying access to real credentials, and by creating decoy credential lures to detect and misdirect credential theft. The ThreatPath® module provides visibility to credential exposures at the endpoints to manage the endpoint attack surface, displaying these exposures in a graphical map and providing search and filter tools to aid in analysis.

The ADSecure solution provides visibility to Active Directory attacks by detecting and misdirecting unauthorized queries targeting AD objects and data. It modifies the query results, providing fake AD objects leading attackers to decoys for engagement, and displays the queries and commands the attackers ran.

The Attivo Networks ADAssessor solution provides customers with unprecedented visibility to Active Directory (AD) risk with continuous insight into exposures, overprovisioning, and misconfiguration for domains, users, and devices. It also detects mass changes to AD objects in real-time, indicating an attack is underway and providing an early warning for risky activities that typically go undetected. The solution deploys to a single standard workstation that belongs to the AD forest and comes with a management console for analysis and management.

The Attivo Networks IDEntitleX solution provides visibility and reduces the attack surface for identities and entitlements in the cloud. The solution includes multi-cloud support for AWS and Azure and provides detailed entitlement visibility for users, applications, virtual machines, containers, serverless functions, and other objects attackers target.

The Attivo identity security solutions give customers a unified dashboard view of identities and exposures across the organization, addressing provisioning management challenges while maintaining operational effectiveness.




## CONCLUSION

Attackers consider identities a high-priority target to advance their attacks, so organizations must prioritize their protection. Enterprise-wide visibility is a necessary component when reducing identity risks and entitlement exposures. Without adequate visibility to these exposures and risks across endpoints, Active Directory, and the cloud, attackers can inflict a great deal of damage to the organization.

The Attivo Network identity security portfolio gives organizations visibility to their identity risks and entitlement exposures to remediate or mitigate them before attackers exploit them.

## ABOUT ATTIVO NETWORKS

Attivo Networks®, the leader in identity detection and response, delivers a superior defense for preventing privilege escalation and lateral movement threat activity. Customers worldwide rely on the ThreatDefend® Platform for unprecedented visibility to risks, attack surface reduction, and attack detection. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, and cloud environments. Data concealment technology hides critical AD objects, data, and credentials, eliminating attacker theft and misuse, particularly useful in a Zero Trust architecture. Bait and misdirection efficiently steer attackers away from production assets, and deception decoys obfuscate the attack surface to derail attacks. Forensic data, automated attack analysis, and automation with third-party integrations serve to speed threat detection and streamline incident response. ThreatDefend capabilities tightly align to the MITRE ATT&CK Framework, and deception and denial are now integral parts of NIST Special Publications and MITRE Shield active defense strategies. Attivo has 150+ awards for technology innovation and leadership. www.attivonetworks.com