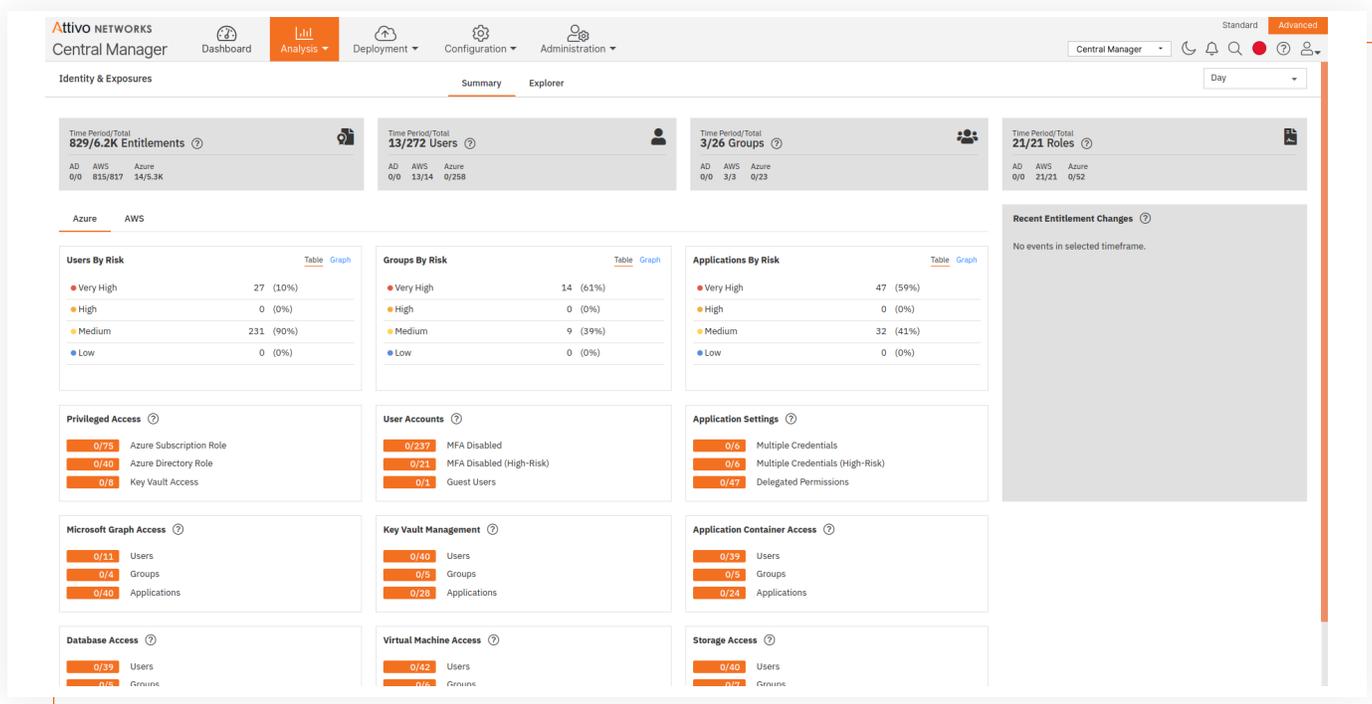


# IDENTITLEX FOR CLOUD IDENTITY AND ENTITLEMENTS VISIBILITY

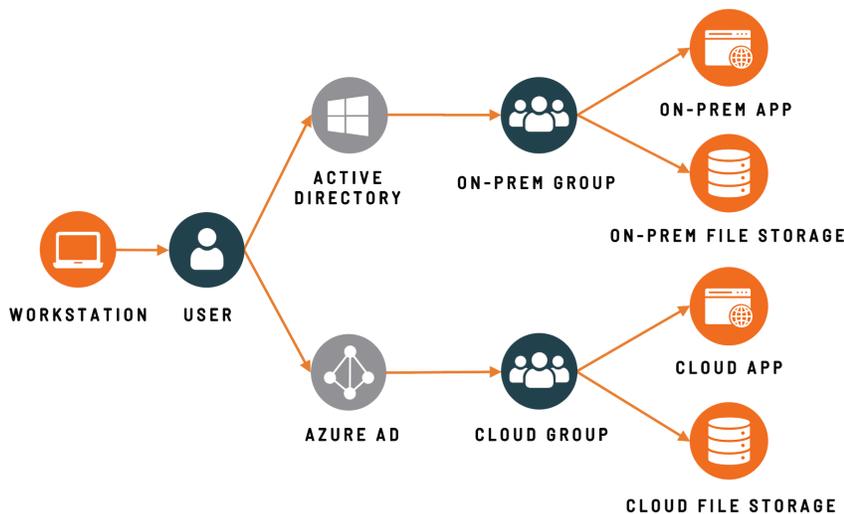
Active Directory user accounts are the principal identity and the primary security focus in a traditional enterprise network. As organizations expand to the cloud, they must provision identities and entitlements for users and “non-human” identities such as applications, virtual machines, containers, serverless functions, and other objects. These identities and entitlements increase the attack surface, and therefore the risks, to the organization. The Attivo Networks IDEntitleX solution efficiently addresses these challenges.

## IDENTITLEX CAPABILITIES

1. Global cloud visibility: Understand your exposure with identity and entitlement summaries across platforms.
2. Platform-specific cloud visibility: Monitor entitlements to key cloud services, such as AWS S3 and Azure Key Vault.
3. End-to-end Visibility: View endpoint, Active Directory, and cloud exposures from a single pane of glass.
4. Object-specific risk assessment: Isolate objects by risk and analyze the details of their entitlements.
5. Entitlement visualization: Graph the end-to-end relationships between objects to understand the extent of access and how it was granted.
6. Customizable risk assessment: Customize the risk assigned to an entitlement to optimize assessments.
7. Entitlement change tracking: Generate events when entitlement changes impact critical objects.



IDEntitleX Dashboard



Enterprise-wide Identity Visualization

## BENEFITS

The IDEntitleX solution provides the following features across all three environments (endpoint, Active Directory, and Cloud) from a simple to use, consolidated dashboard:

- Entitlement policy management
- Change monitoring and analysis
- Security posture analysis
- Identity, role/permission, and resource discovery
- Entitlement visualization
- Cross-cloud entitlement correlation

Collectively, these solutions will dramatically reduce the ability of an attacker to find their targets, move laterally, and escalate their privileges. This functionality in the Attivo ThreatDefend Platform is also available within the standalone Endpoint Detection Net Suite and ADSecure protection solution.

## HOW IT WORKS

Setup consists of the following high-level steps:

- IDEntitleX is a software license that works in conjunction with an Attivo Central Manager (ACM) or EDN Manager on premises or inside your cloud.
- For AWS clouds, create an access key for each account you want to analyze.
- For Azure clouds, register an app for each account you want to analyze.
- From within the ACM or EDN Manager console, define a cloud connection object for each created access key and registered app.

## 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. Attivo has 150+ awards for technology innovation and leadership. [www.attivonetworks.com](http://www.attivonetworks.com)