ZERO.
Networks

Identity Segmentation

SILO CITY
INFORMATION TECHNOLOGY

Gain Control of Admin and Service Accounts

Zero Networks easily provisions all logon rights based on least privilege to prevent lateral movement

Admin and privileged service accounts are prime targets for attackers, as compromising them provides access to the organization's most sensitive servers. While the principle of least privilege aims to limit these risks, it is difficult to implement due to the manual, lengthy, and complex process of governing access rights. This results in broad logon permissions, leading to threats like data breaches, malware, and ransomware.

Identity Segmentation with Zero Networks

The Zero Networks platform features a simple, fully automated, and agentless identity segmentation solution. It revokes logon rights for all admin and service accounts and then provisions them based on least privilege, enhanced by multi-factor authentication (MFA).

Admin Accounts are restricted to pre-approved assets after MFA

Service Accounts are automatically restricted to necessary assets and logon types

Automated

Agentless

MFA-Enhanced

An Evolutionary Leap in Identity Security

Service account discovery and visibility
Get insights on account usage, eliminate inactive accounts

Auto-restrict service account logons
Prevent unauthorized access and lateral movement

MFA privileged logons
Enable admin logon where intended, blocking all other logon rights

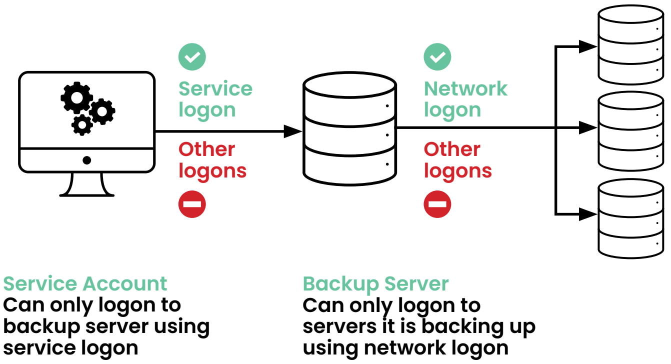
Eliminate risk from credential theft
Prevent Pass the Ticket, Golden Ticket, Kerberoasting, and other attacks

PAM augmentation & Tiered Model alternative
Extend granular security without the associated cost and complexity

Comply with regulations and cyber insurance
Adhere to visibility, MFA, and strict control of privileged and service accounts

How It Works

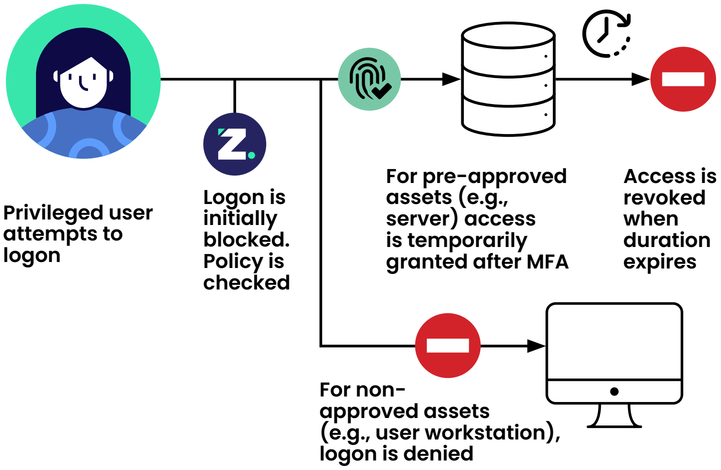
Service Accounts: Zero Networks' patent-pending technology learns all logons for a recommended 30-day period, understands which service accounts and logon types are intended to be used on each asset, and automatically restricts logon rights and types to these assets.



Service Account
Can only logon to backup server using service logon

Backup Server
Can only logon to servers it is backing up using network logon

Admin accounts: Zero Networks enables IT teams to restrict admin accounts, permitting temporary logon to pre-approved assets only after MFA, and blocking all other logon rights.



Privileged user attempts to logon

Logon is initially blocked. Policy is checked

For pre-approved assets (e.g., server) access is temporarily granted after MFA

Access is revoked when duration expires

For non-approved assets (e.g., user workstation), logon is denied

ZERO. Networks

Segment Everything
Connect Everyone

Zero Networks is a unified zero trust platform for network segmentation, identity segmentation, and remote access. To see us in action visit zeronetworks.com or contact us at contact@zeronetworks.com