Reinventing Identity Security:

Mitigating Admin and Service Account Risk with Automated, Agentless, MFA-Enhanced Identity Segmentation

ZERO. Networks

1 Introduction

In current IT environments, the risk tied to privileged and service account logins presents a significant threat. Admin accounts, possessing high-level access to sensitive servers, can use the same credentials to log in from less secure machines, inadvertently exposing their credentials to potential attackers.

Service account credentials, if stolen, can be utilized by attackers on any machine within the network; this vulnerability allows unauthorized users to move laterally within the network, intensifying the potential for extensive access and damage.

These very real scenarios emphasize the importance of restricting logon capabilities for each account based on its necessity and designated privilege. This paper will challenge today's status quo when it comes to privileged account security and outline a better, more effective solution that reinvents identity security.

2 Challenges

Admin or service accounts with privileged rights pose a significant security threat to organizations. Attackers specifically target these accounts, as compromising them provides them opportunities to move laterally and access other sensitive servers containing confidential data.

To reduce the risk of unauthorized or malicious activities, the principle of least privilege dictates that users and systems should be granted only the minimal access rights and permissions necessary to perform their assigned tasks.

The challenge, however, lies in the extensive effort required to specify logon rights and permissions for each user. This process requires resources, a thorough understanding of each role, and the potential security implications of granting access. Additionally, as organizations grow and employee roles evolve, maintaining and updating these permissions becomes complex, demanding a strict governance model to ensure security without impeding operational efficiency.

In practice, most organizations today struggle to maintain strict admin and service account logons and permissions. Often, this means that any user account can authenticate and log in to every machine – either physically or across the network. This excessive login permission broadens the possibility of unauthorized access, data loss, and unauthorized control over various machine levels.

A myriad of critical risks stem from this governance reality, including identity theft, data exfiltration, spread of malware, and ransomware.

3 Existing Solutions and Their Shortcomings

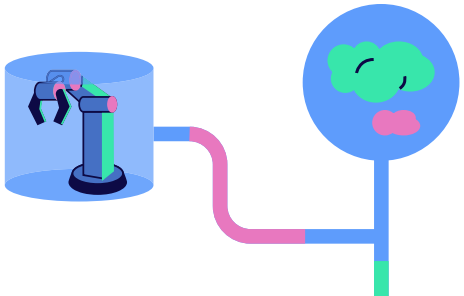
Current solutions offer only partial remedies to the abovementioned security challenges. They are either cumbersome, expensive, and negatively impact IT performance, or not comprehensive enough:

Microsoft Tiered Forest Model

Microsoft's tiered forest model, often referred to in the context of Privileged Access Management (PAM) and the Enhanced Security Administrative Environment (ESAE), is designed to mitigate risks associated with admin tasks in Active Directory environments.

To limit exposure to attackers, Microsoft's tiered model partitions admin privileges across three tiers (typically): Tier 0 for domain admins, Tier 1 for server admins, and Tier 2 for user workstation admins. The goal is to ensure that admin credentials from a higher tier (e.g., Tier 0) are never exposed to a lower tier (e.g., Tier 1 or Tier 2), thereby limiting the potential for attackers to elevate their privileges.

Example:
Domain admins (Tier 0) cannot log on to enterprise servers (Tier 1) and user workstations (Tier 2). Server admins (Tier 1) cannot log on to domain controllers (Tier 0) and user workstations (Tier 2).



In high-security environments, organizations use dedicated Active Directory forests for each tier, providing an added layer of security by isolating highly privileged accounts from potential threats in the main forest.
While the tiered model is effective in creating a least privileged approach to admin logins, it has a few shortcomings:

- **Complex implementation and deployment:** Reading through hundreds of pages of documentation, breaking Active Directory into three forests, and manually managing user identities require a substantial effort that many IT teams are incapable of handling.
- **Relying on professional services:** Most organizations hire professional services for this purpose, a process that takes many months, or even years, to deploy and incurs significant costs.
- **Introducing IT inefficiencies:** For enhanced security, the tiered model mandates that IT admins keep a separate physical workstation for each tier they operate in. Managing separate credentials on multiple workstations adds management complexity and negatively impacts IT efficiency and productivity.

Privileged Access Management (PAM)

Privileged Access Management (PAM) controls privileged user access to critical IT resources.

It operates by centralizing the management of privileged credentials, such as sensitive admin passwords. It stores these credentials in a secure vault. When users need privileged access, they request it through the PAM system, which then retrieves the necessary credentials, grants time-limited access, and logs the activity. This ensures that privileged accounts are not directly exposed, passwords are regularly rotated (changed) without user intervention.

Example:
When an IT admin needs access to a sensitive database, they request access via the PAM rather than logging in with a known password. The PAM verifies the admin identity, retrieves the necessary privileged credentials from a secure vault, and grants the admin a time-limited password. Once the task is completed or the access duration expires, the PAM rotates the password so it cannot be reused (however, PAM cannot control the duration for which credentials remain valid, see below).

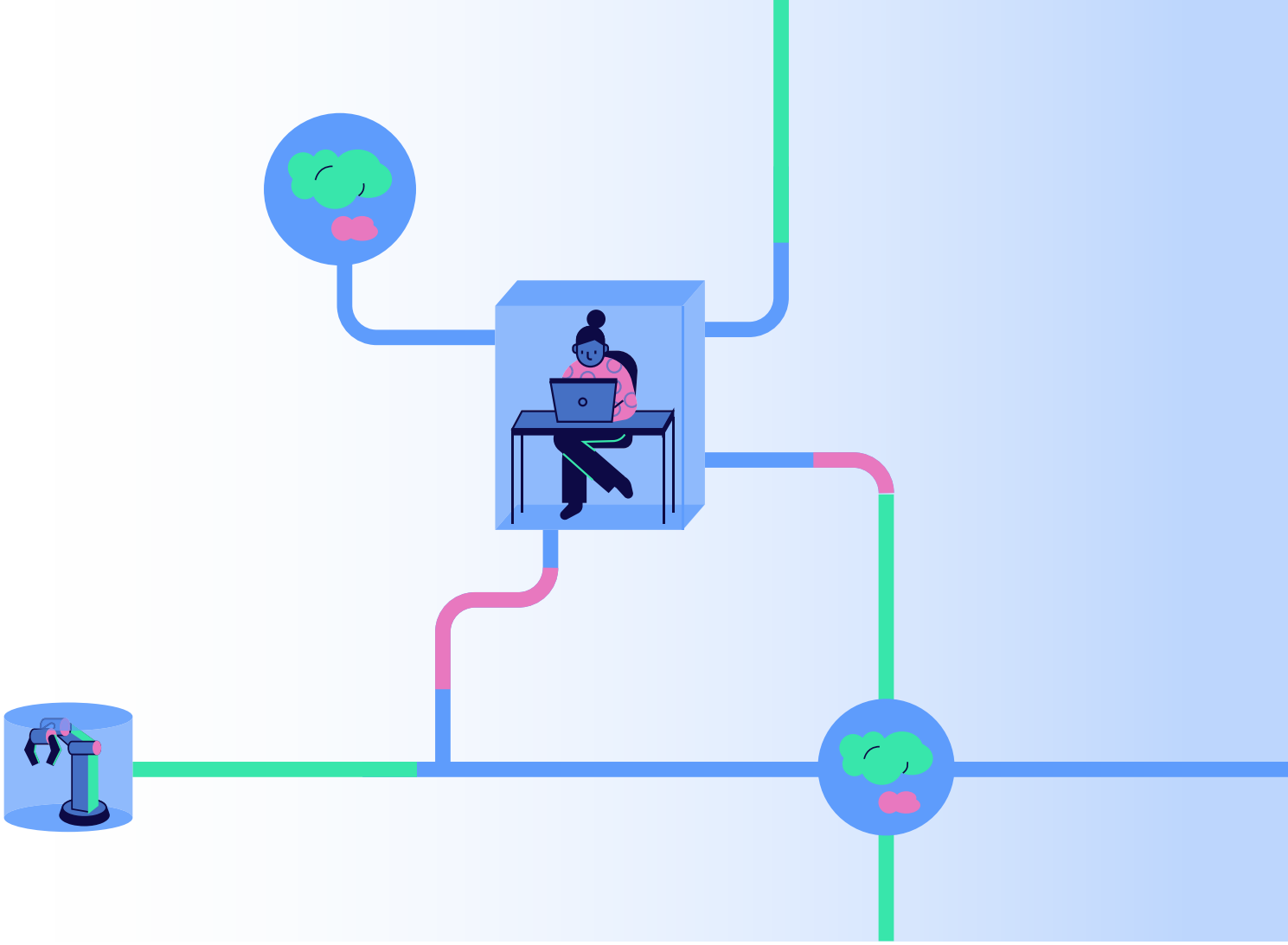
While PAM is widely adopted by large organizations, it has several significant shortcomings:

- **Complex to deploy:** Setting up a PAM solution is often complicated, especially in large and heterogeneous IT environments. It involves integrating diverse systems, managing multiple access levels, and ensuring strict security protocols without disrupting existing workflows.

- **User resistance:** Due to the additional steps required in retrieving privileged credentials, PAM is notoriously perceived unfavorably by admins, as it requires more steps, taking additional time and generally hurting user experience.

- **No control over where credentials are used:** User resistance to PAM frequently results in admins finding ways around the system, inadvertently increasing the attack surface. Often, admins may use PAM credentials on machines for which they weren't intended, as PAM cannot control where the credentials are used.

- **No control over how long credentials remain valid:** When a user authenticates, their username and password are converted into a Kerberos ticket and NTLM hash. This ticket facilitates single sign-on, enhancing the user experience by eliminating the need for repeated logins. However, this convenience also poses a security risk as the ticket can be easily exploited by malicious actors. By default, the ticket remains valid for a week, even if the associated password changes within that period. Thus, a stolen ticket **allows the attacker to move laterally in the network for a week, even if PAM has already rotated the password (!)**



4 Zero Networks Identity Segmentation

Zero Networks Identity Segmentation is a patent-pending, simple, fully automated, and agentless identity segmentation solution, marking an evolutionary leap in identity security. It is the latest addition to the Zero Networks platform which includes network segmentation and zero trust network access.

Zero Networks Identity Segmentation revokes logon rights for all human and service accounts on every asset in the environment and then provisions them using a zero trust, least-privilege approach, enhanced by multi-factor authentication (MFA).

Unlike legacy solutions, its deployment and ongoing maintenance require nearly no IT involvement.
Its two core pillars include:

1. **Human Account MFA-Based Segmentation:** Monitoring and controlling user logons to temporarily allow logon and privileged access after authenticating with MFA;

2. **Service Account Automated Segmentation:** Identifying service accounts and limiting their logon and access to only where necessary, blocking logons on all other assets in the environment.

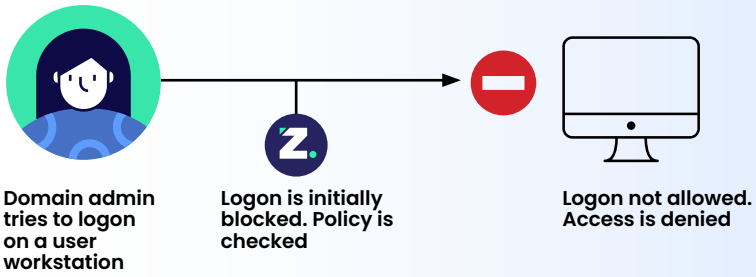
Human Account MFA-Based Segmentation

As previously outlined, admin accounts that have ongoing and outstanding logon rights pose major security risks, as attackers can exploit them for broad unauthorized access within the environment.

Zero Networks Identity Segmentation tackles this problem by revoking logon rights from all privileged admin accounts to all assets in the environment, effectively "sanitizing" the environment from excessive logon rights. This helps stop lateral movement if credentials are stolen.

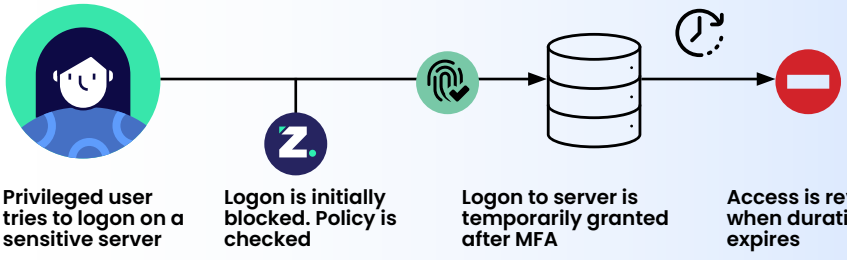
Unlike PAM solutions that cannot control where user credentials are used, Zero Networks only allows user logons to where they are intended, blocking logon attempts on all other assets. Let's look at a couple of common use cases.

With Zero Networks, IT teams can impose a certain user or user groups to only logon on specific machines or machine groups. This could be restricting domain admins to logon only on the domain controller, and not on less secure machines such as user workstations (effectively emulating the Microsoft tier model without its associated cost and complexities)



Example:
A domain admin is using their credentials to connect to a user workstation. By default, Zero Networks has no outstanding logon rights, and if no prior permission has been explicitly granted, the logon attempt fails, and access is denied.

Where privileged access is required, Zero Networks allows an admin user or group to logon on a specific machine or machine groups (and these machines alone) only after successful MFA.



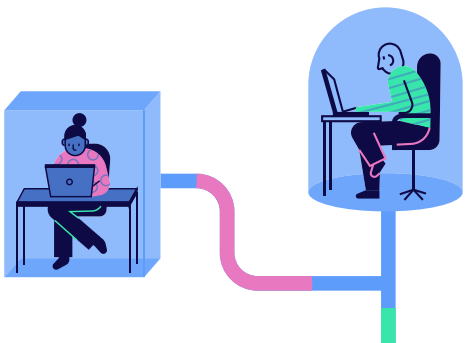
Example:
When an IT admin needs access to a sensitive server, an MFA prompt is invoked. If authentication is successful, the admin receives time-limited access to the server by granting temporary logon rights only on that server. Once the access duration expires, the logon right is removed and access is revoked.

With Zero Networks Identity Segmentation, even if an attacker gains unauthorized access to admin credentials, these credentials do not have logon rights anywhere else in the environment, and the MFA prevents the attacker from accessing the asset for which the credentials are intended.

Service Account Automated Segmentation

Service accounts often possess elevated privileges on various assets in the environment, use static credentials that rarely change, and typically lack regular monitoring. They might be used across multiple clients and servers, increasing exposure, and are sometimes misused or poorly documented.

Zero Networks Identity Segmentation addresses these weaknesses using a fully automated, three-step process:

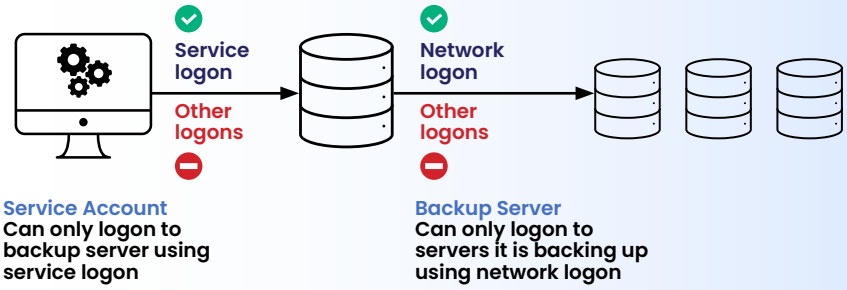


1. **Discovery:** Initially, Zero Networks auto-discovers every service account within the environment and makes them visible to the IT team. This streamlines the removal of inactive accounts that could potentially be exploited.

2. **Monitoring and Learning:** After the discovery phase, Zero Networks continuously monitors all service account login attempts. It also logs details related to the logon types used, such as interactive, network, service, batch, and others.

3. **Restriction:** Zero Networks revokes logon rights for all service accounts on every asset in the environment and then provisions them using a zero trust, least-privilege approach based on its learning. It ensures that service accounts can only log on to the specific assets where they are intended to operate, using only the logon types that are required to operate. Access to all other assets and logon types is blocked.

By segmenting service accounts access to the specific assets and logon types where they are required to operate, the potential harm from compromised service account credentials is substantially minimized.



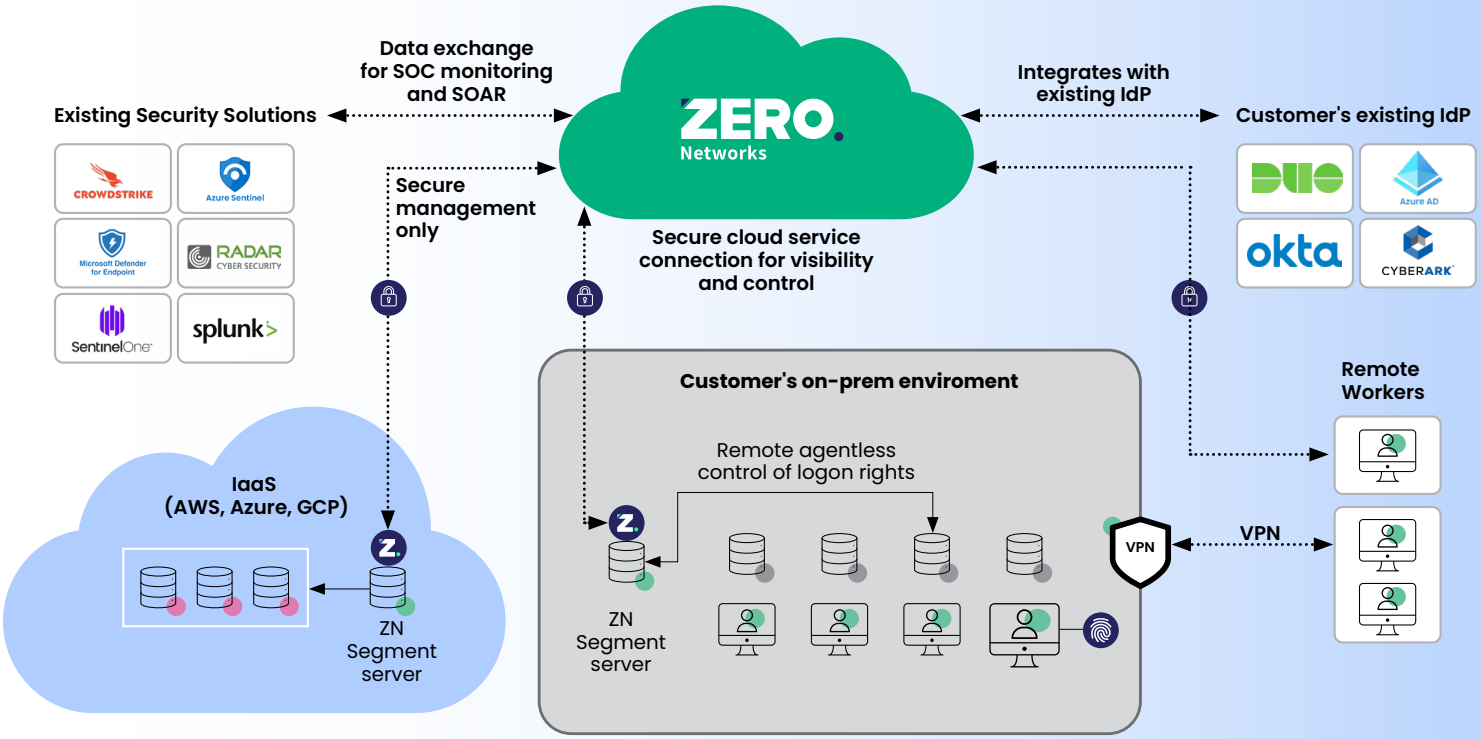
Example: Restricting backup service account logons

Backup service account logons are restricted by two automated rules: The first permits a service logon type solely on the backup server, while the second allows network logon only from the backup server to the servers it is backing up. Any other logons, such as interactive, remote desktop, or network logons to client machines, are blocked as they are unnecessary.

Insights and Reports

Zero Networks provides comprehensive insights and reports, detailing aspects like the type of accounts (whether human or service), the specific destination assets they access, the privileges they utilize, and the outcomes (success / failure) of their login attempts. These reports can seamlessly integrate with various SIEMs.

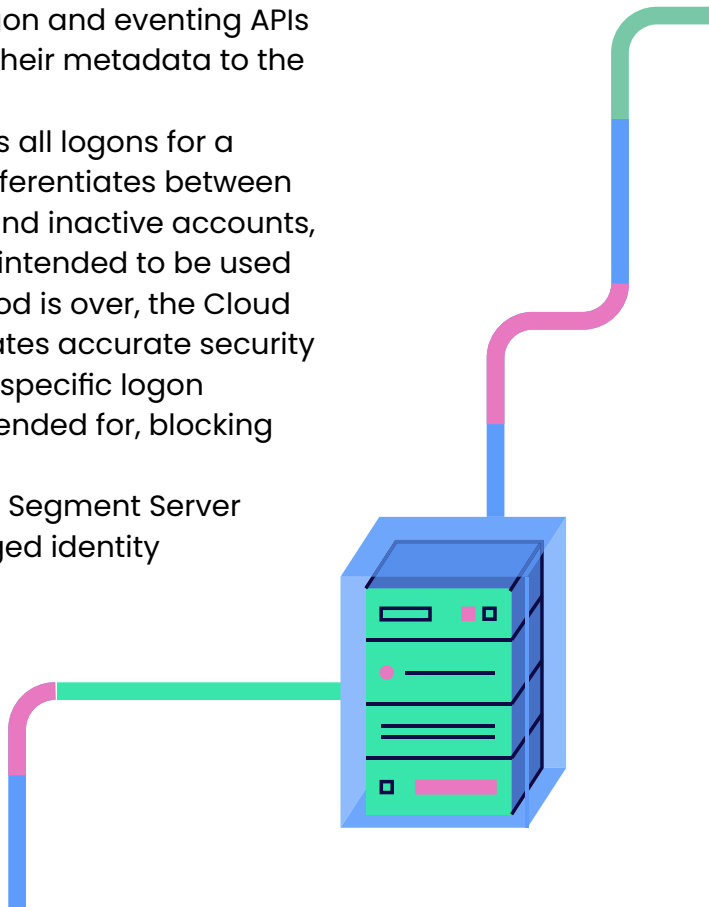
How does it work?



The process begins with installing a Zero Networks Segment Server on the network. A Segment Server is a simple, stateless virtual appliance that doesn't require any backups or maintenance and is not inline with logon or network traffic. It leverages various logon and eventing APIs to monitor all logon types, and sends their metadata to the Zero Networks Cloud.

The Cloud Automation Engine learns all logons for a recommended period of 30 days. It differentiates between human and service accounts, active and inactive accounts, and understands which accounts are intended to be used on each asset. When the learning period is over, the Cloud Automation Engine automatically creates accurate security policies that restrict logons (including specific logon types) solely to the assets they are intended for, blocking everything else.

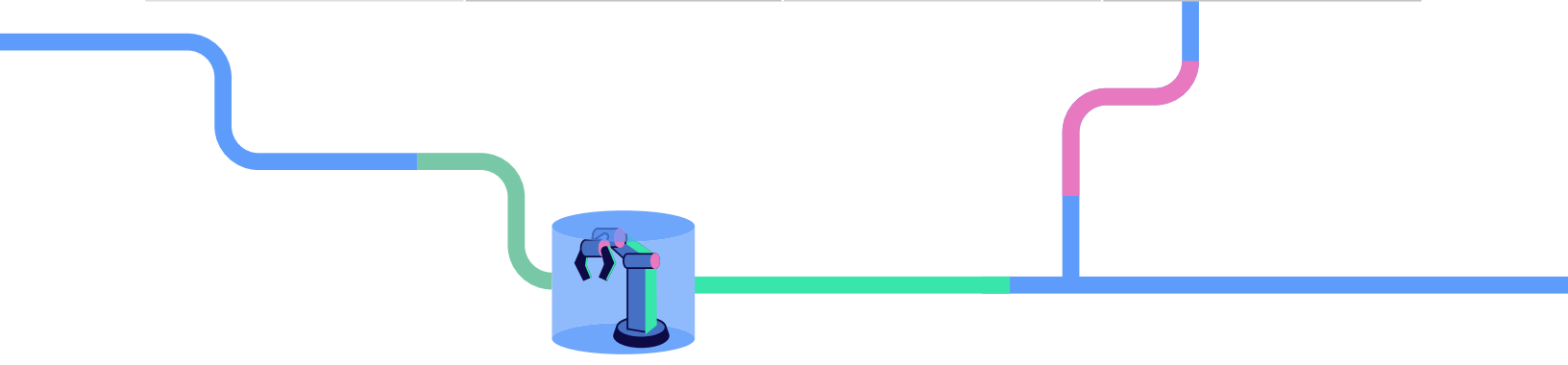
The policies are then applied by the Segment Server on all assets to achieve a least privileged identity segmentation of the environment.



5 Combining Identity Segmentation with Microsegmentation and ZTNA

Identity Segmentation, Microsegmentation, and Zero Trust Network Access (ZTNA) – all part of the Zero Networks platform – are individual security concepts that, when integrated, create a cohesive and fortified zero trust strategy. Let's explore how they operate together to safeguard IT environments.

	Identity Segmentation	Microsegmentation	ZTNA
	WHO can access	**WHAT they can access**	**HOW they can access**
Purpose	Governs access based on user identities, ensuring access only to resources pertinent to their roles or functions.	Divides the network into small, isolated segments, up to a segment per machine.	Securely connects remote users to the organization based on a "never trust, always verify" philosophy.
Functionality	Evaluates various parameters like user roles, service account purpose, and device attributes to make access decisions.	Implements fine-grained firewall rules and policies for each segment based on the specific needs and risk profiles of the resources within that segment.	Access to network resources is provided on a need-to-know basis, and every request is authenticated, authorized, and encrypted before access is granted.
Benefit	If user credentials are stolen, the attacker cannot move laterally, as they're restricted by the identity attributes and permissions of the compromised user or service account.	If one segment is compromised, the attack is confined to that segment, preventing lateral movement across the network.	Reduces the attack surface by ensuring only validated and authorized entities can access network resources, thus mitigating threats from both external attackers and insider threats.



When Combined:

- **Holistic Zero Trust Posture:** The triad of Identity Segmentation, Microsegmentation, and ZTNA ensures that zero trust security is addressed at every layer. Identity ensures "who" can access, Microsegmentation defines "what" they can access, and ZTNA stipulates "how" they can access.

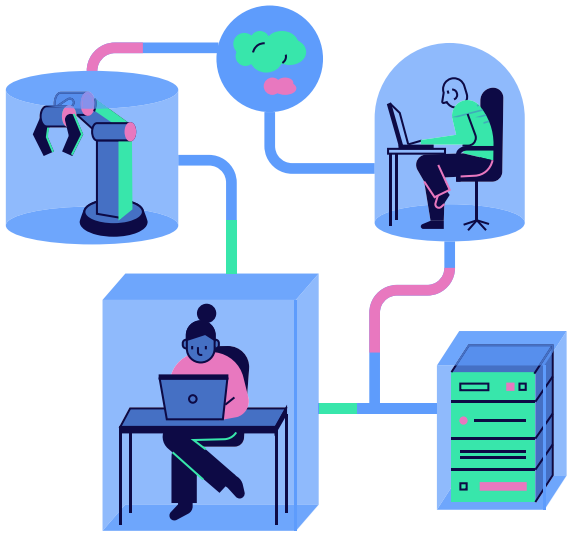
- **Reduce Security Toolset:** Apply a single pane of glass for all zero trust needs, reduce various identity security solutions, network security appliances, segmentation, internal firewalls, remote access solutions for both employees, third-party vendors, and proxy solutions.

- **Dynamic Access Control:** By utilizing Identity Segmentation with ZTNA, access controls are dynamically adjusted based on user behavior, role changes, or device context, ensuring real-time adaptability.

- **Granular Visibility:** With all three components in play, there's an in-depth view of network activity and account activity, allowing anomalies or malicious activities to be detected swiftly.

- **Enhanced Threat Containment:** The combination ensures that if an entity gains unauthorized access, it's confined to a very specific part of the network and under very specific permissions, severely limiting potential damage.

- **Streamlined Compliance:** The integrative approach makes it easier for organizations to meet stringent data access and protection requirements of various compliance standards.



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