Defining the Undefined:
What is Tier Zero?

Elad Shamir, Jonas Knudsen, Justin Kohler

Agenda

- History of Secure Enterprise Access and Tier Zero
- Academic definition of Tier Zero
- Examining Microsoft’s original list of Tier Zero principals
- Introduce future sessions

Why this series?

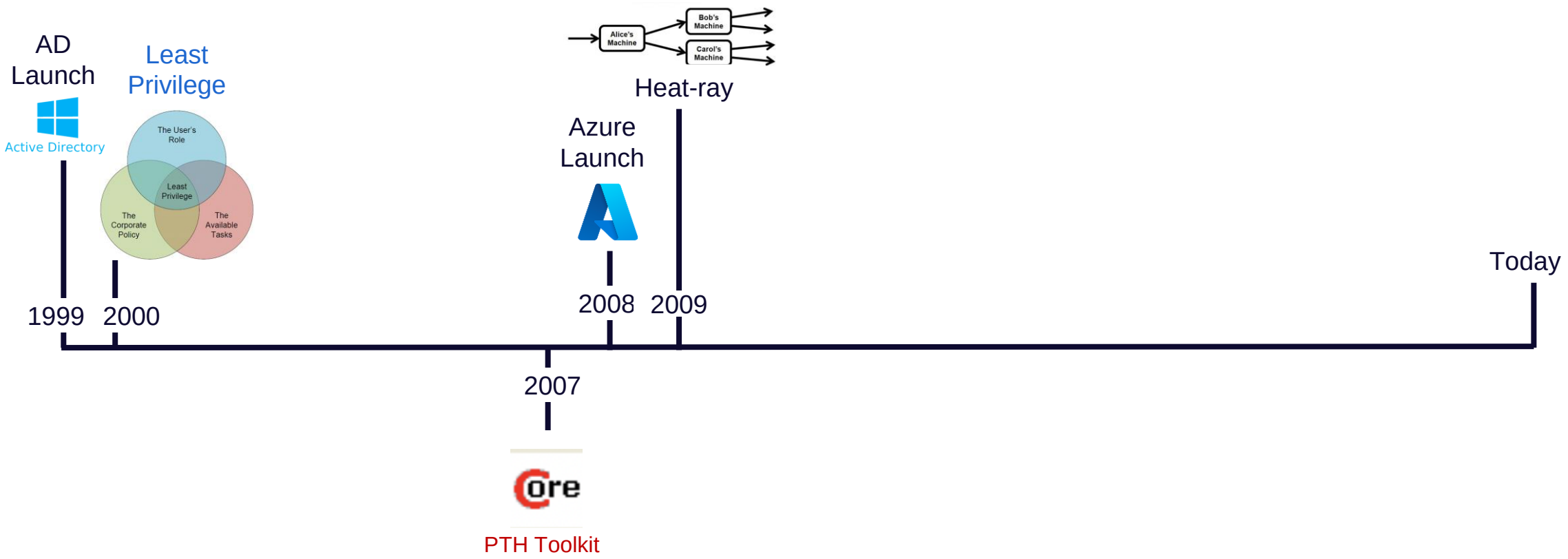
- Finally answer the question: What is Tier Zero / Control Plane?
- Existing resources are vague
- We can’t defend what we can’t define

Who is talking about this?

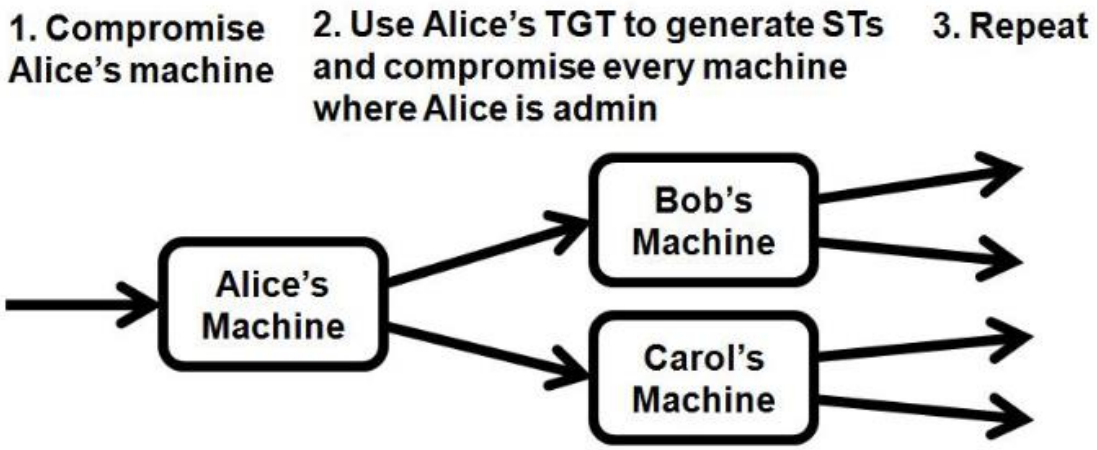
- SpecterOps Consulting resources with decades of experience abusing and defending access to Tier Zero
- BloodHound Enterprise resources with experience mapping Attack Paths across identities and resources in AD / Azure

History of Secure Enterprise Access

Evolution of Secure Enterprise Access



2009: Introducing the Identity Snowball Attack



Heat-ray: Combating Identity Snowball Attacks Using Machine Learning, Combinatorial Optimization and Attack Graphs

John Dunagan, Alice X. Zheng, Daniel R. Simon

https://www.microsoft.com/en-us/research/wp-content/uploads/2009/01/sosp2009-heatray-10pt.pdf

Attack Path

A user was phished.

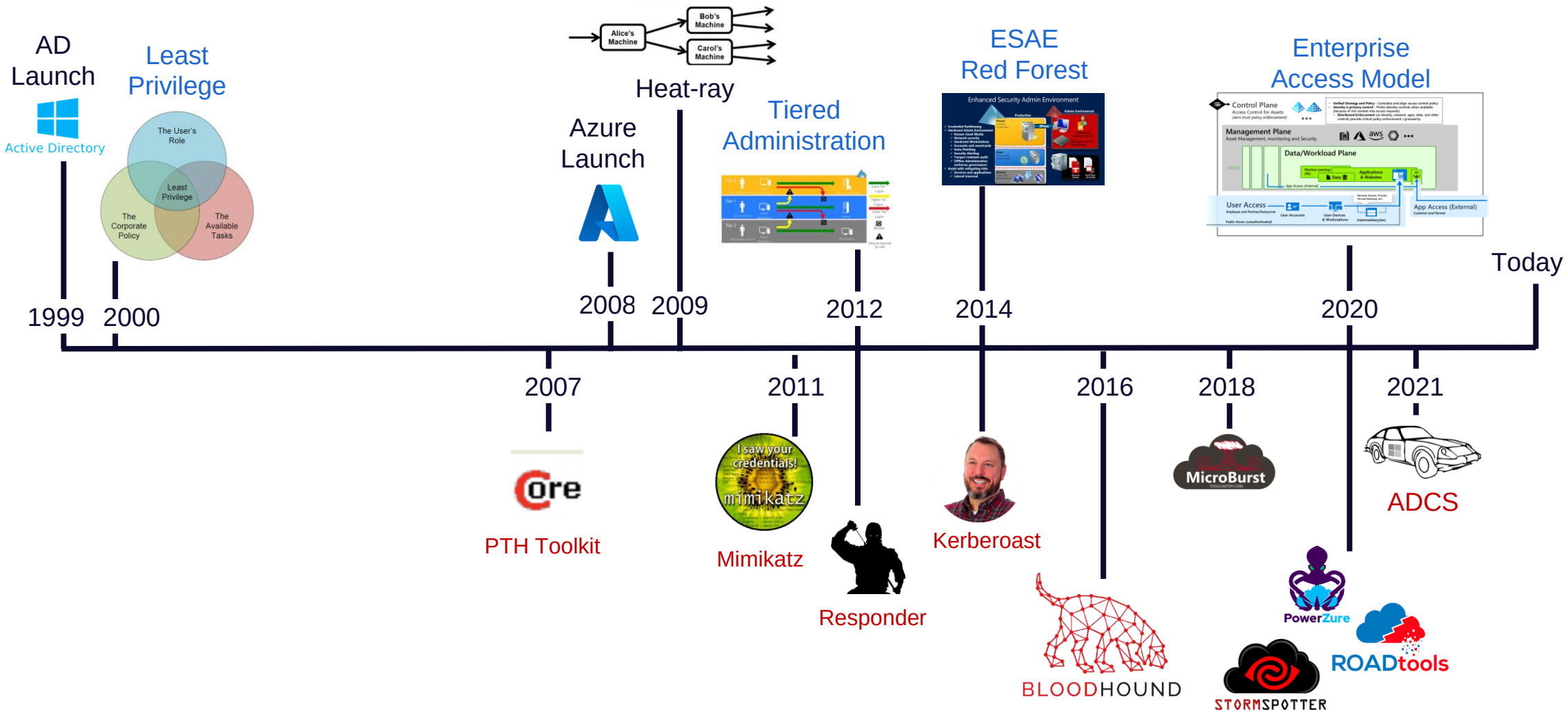
…which was a member of another group…

The user was a member of a group..

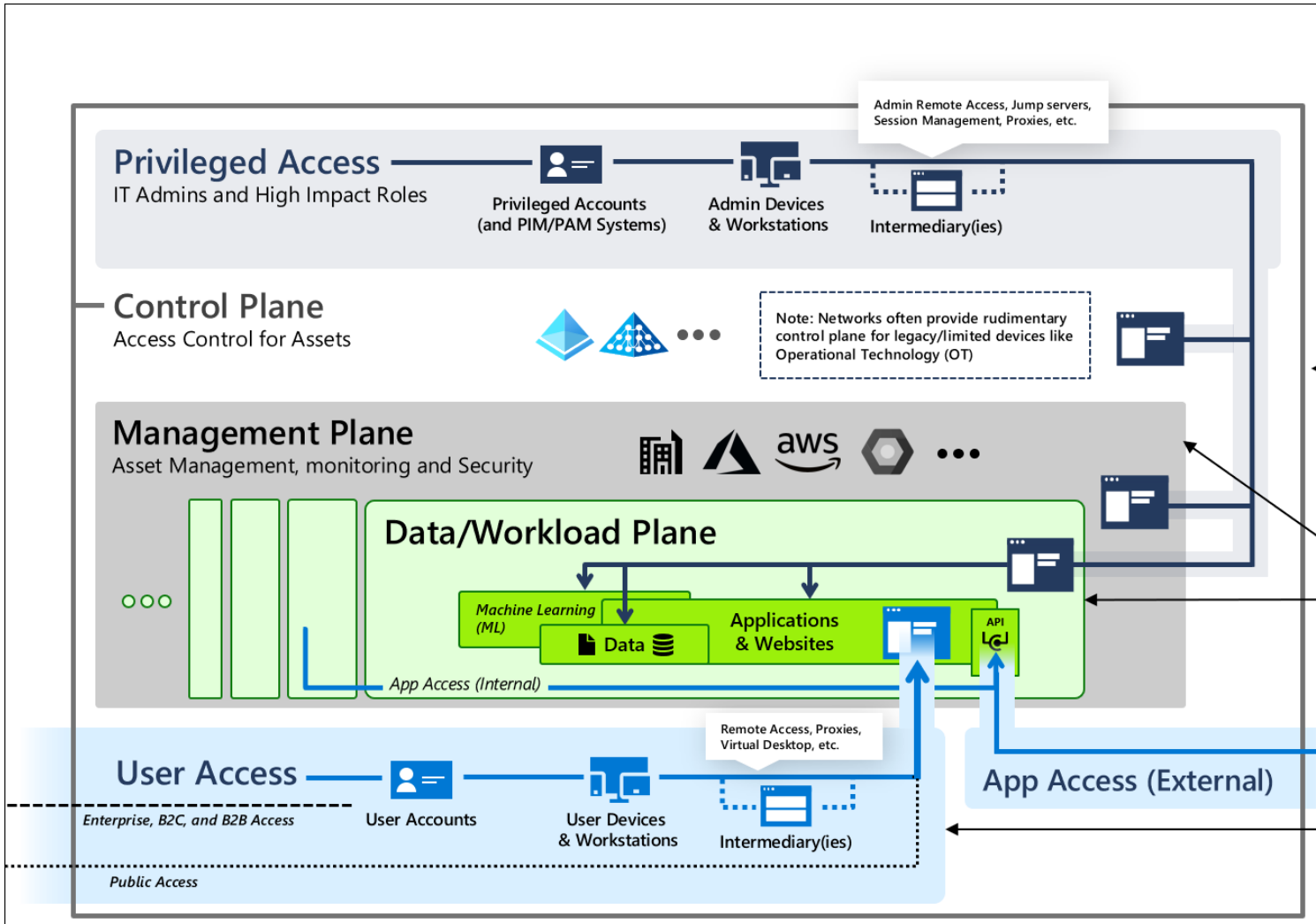
…which had local admin privileges over a system.

That service account had the “Add Members” privilege on the Domain Admins group.

Evolution of Secure Enterprise Access



Enterprise Access Model



Evolved purpose and scope

The original tier model was built to contain privilege escalation for on-premises active directory.

The enterprise access model guides access security for full scope of a hybrid on-premises + multi-cloud enterprise following zero trust principles for employees, partners, customers, apps and more

Tier 0 → Control Plane

The control plane includes identity access controls as well as the use of network access control where it is the only/best option, such as legacy OT options

Tier 1 Split

To increase clarity, actionability, and business focus:

- **Management Plane –** enterprise-wide IT management
- **Data/Workload Plane –** per-workload management focused on protecting business critical systems/data and accommodating DevOps

Tier 2 Split

- **User access –** now includes all B2B, B2C, and public access scenarios
- **App access –** to accommodate API attack surface

Tier Zero vs Privileged Access/Control Plane

- Tier Zero becomes Privileged Access / Control Plane
- The terms should be considered interchangeable
- Most are more familiar with “Tier Zero”
- We will use “Tier Zero” for this series

Tier 0 → Control Plane

The control plane includes identity access controls as well as the use of network access control where it is the only/best option, such as legacy OT options

Tier 1 Split

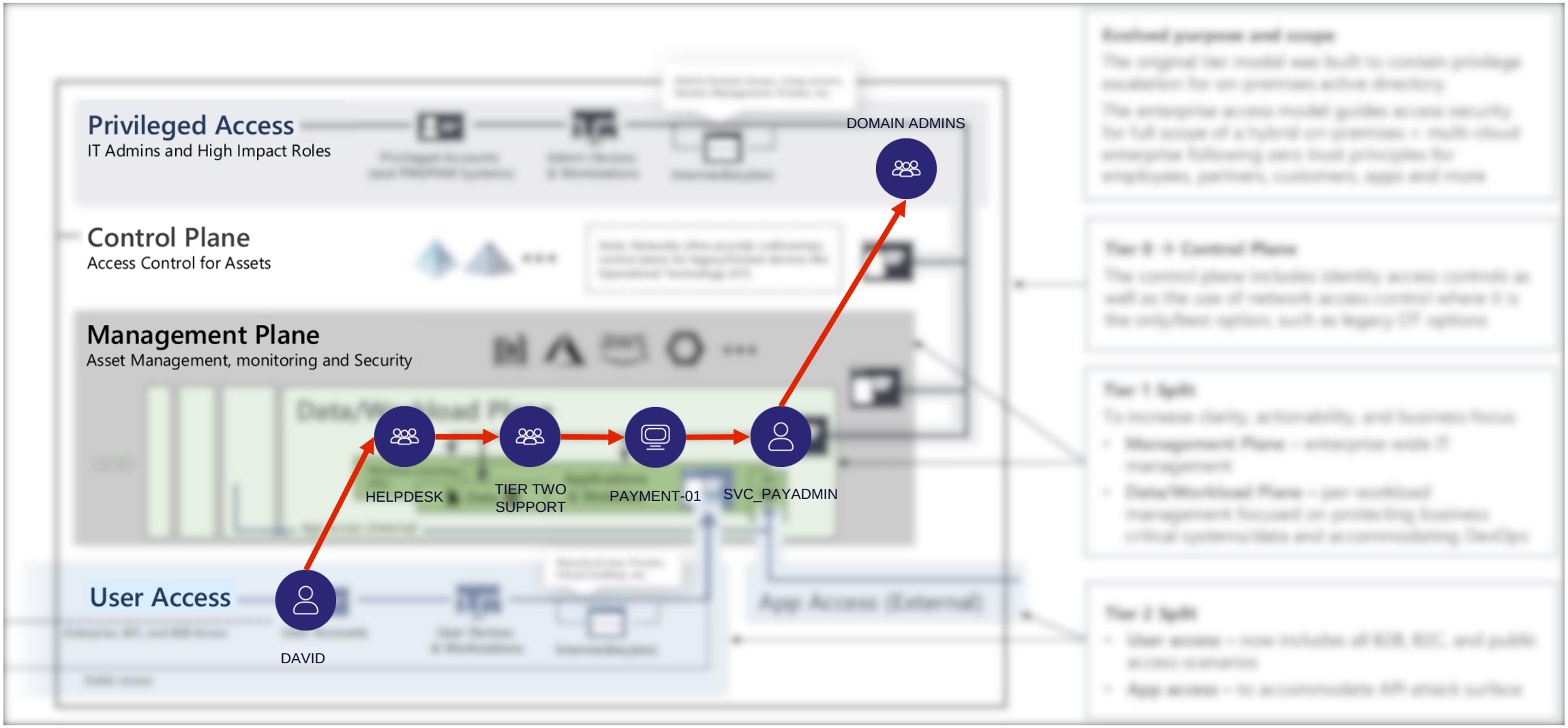
To increase clarity, actionability, and business focus:

- **Management Plane –** enterprise-wide IT management
- **Data/Workload Plane –** per-workload management focused on protecting business critical systems/data and accommodating DevOps

Tier 2 Split

- **User access –** now includes all B2B, B2C, and public access scenarios
- **App access –** to accommodate API attack surface

Enterprise Access Model



Academic Definition of Tier Zero

Microsoft’s Tier Zero Definition

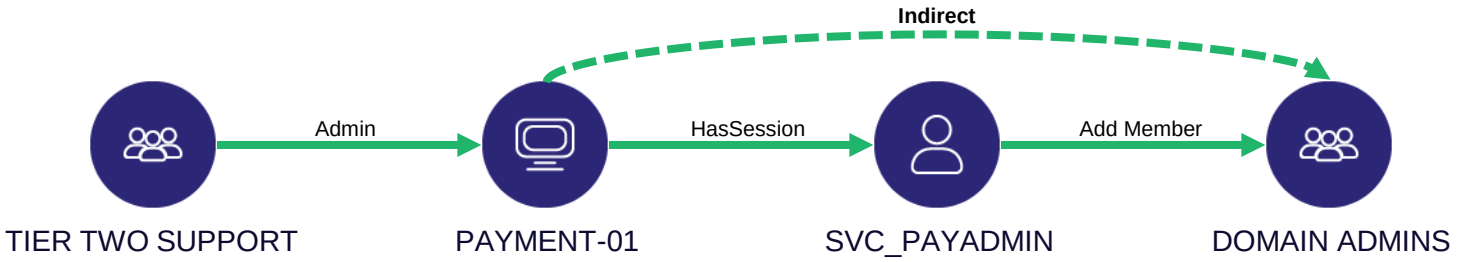
“**Direct Control** of enterprise identities in the environment.

Tier 0 includes accounts, groups, and other assets that have **direct or indirect administrative control** of the Active Directory forest, domains, or domain controllers, **and all** the assets in it.

The security sensitivity of all Tier 0 assets is equivalent as **they are all effectively in control of each other**.”

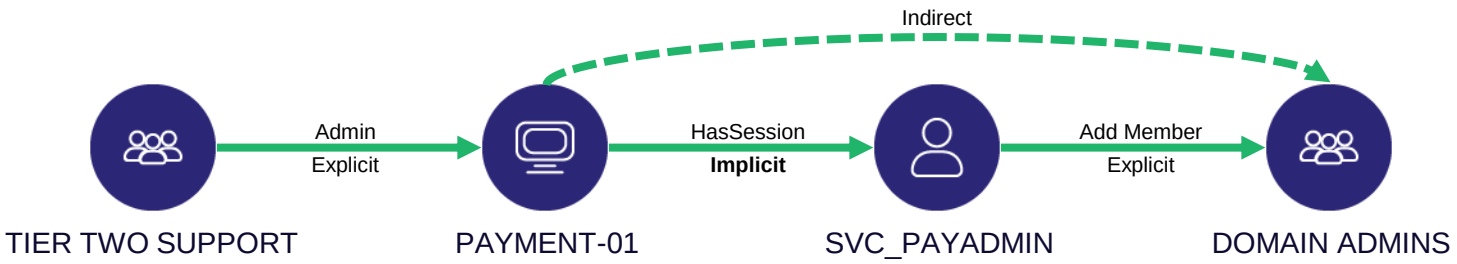
Direct vs Indirect Control

- Direct could mean:
  - One “hop” away from the controlled object
  - Explicit rights on the controlled object (e.g., Add Member)
- Indirect could mean:
  - Control is transitive: A controls B, B controls C, therefore A controls C
  - Implicit control



What is Implicit Control?

- The Clean Source Principle: All security dependencies must be as trustworthy as the object being secured
- “Any subject in control of an object is a security dependency of that object”
- Conversely, any security dependency of an object has *(implicit)* control of the object
  - Is it necessarily so?
- Examples:
  - Has Session
  - Agents (EDR)
  - Hardware / Hypervisors



What Makes a Security Dependency?

- If the security of one component relies on the security of another, then it is a security dependency
- Compromising a security dependency **may** allow compromising components that depend on it
- Some attacks have multiple prerequisites, therefore, compromising a single security dependency may be insufficient for compromising a component that depends on it
    - If the dependency doesn't contribute to **any** attack, then it is not a security dependency
- Examples:
    - The password is a security dependency of an account protected by MFA
    - A group with privileged access to a server is a security dependency even if it requires interactive logon

Better Tier Zero Definition

Tier Zero is a set of assets in control of enterprise identities and their security dependencies

Examining Microsoft’s Tier Zero principals

Microsoft’s Tier Zero List (Active Directory)

Enterprise Admins

Domain Admins

Schema Admins

BUILTIN\Administrators

Account Operators

Backup Operators

Print Operators

Server Operators

Domain Controllers

Read-Only
Domain Controllers

Group Policy Creator Owners

Cryptographic Operators

Distributed COM Users

Sensitive on-premises Exchange groups (including Exchange Windows Permissions and Exchange Trusted Subsystem)

Other Delegated Groups - Custom groups that may be created by your organization to manage directory operations.

Any local administrator for an underlying operating system or cloud service tenant that is hosting the above capabilities including

- Members of local administrators group
- Personnel who know the root or built in administrator password
- Administrators of any management or security tool with agents installed on those systems

https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-security-levels#privileged

Microsoft’s Tier Zero List (Active Directory)

Enterprise Admins

Domain Admins

Schema Admins

BUILTIN\Administrators

Account Operators

Backup Operators

Print Operators

Server Operators

Domain Controllers

Read-Only Domain Controllers

Group Policy Creator Owners

Cryptographic Operators

Distributed COM Users

Sensitive on-premises Exchange groups (including Exchange Windows Permissions and Exchange Trusted Subsystem)

Other Delegated Groups - Custom groups that may be created by your organization to manage directory operations.

Any local administrator for an underlying operating system or cloud service tenant that is hosting the above capabilities including

- Members of local administrators group
- Personnel who know the root or built in administrator password
- Administrators of any management or security tool with agents installed on those systems

Inarguably Tier Zero

Microsoft’s Tier Zero List (Active Directory)

Enterprise Admins

Domain Admins

Schema Admins

BUILTIN\Administrators

Account Operators

Backup Operators

Print Operators

Server Operators

Domain Controllers

Read-Only Domain Controllers

Group Policy Creator Owners

Cryptographic Operators

Distributed COM Users

Sensitive on-premises Exchange groups (including Exchange Windows Permissions and Exchange Trusted Subsystem)

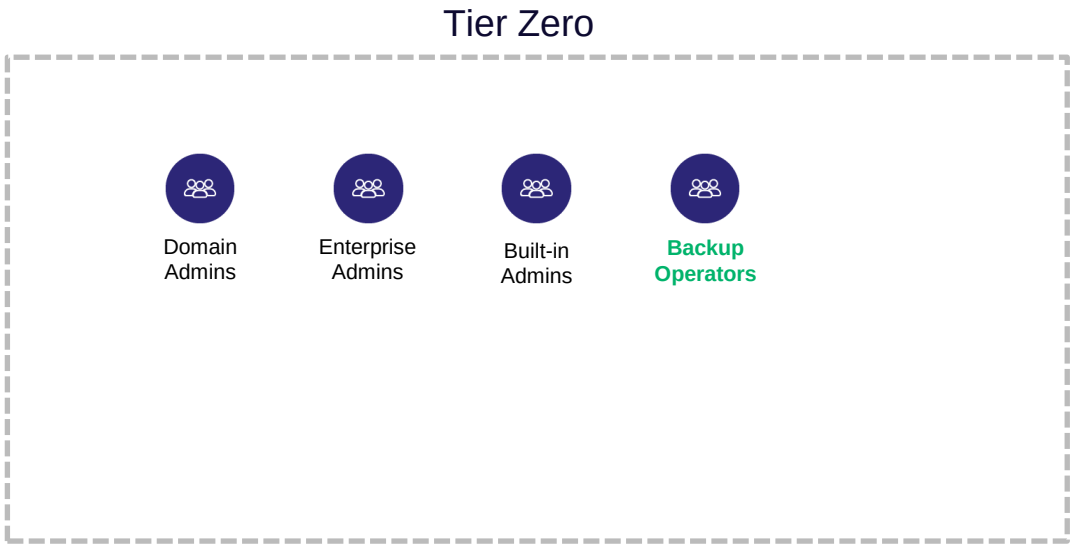
Other Delegated Groups - Custom groups that may be created by your organization to manage directory operations.

Any local administrator for an underlying operating system or cloud service tenant that is hosting the above capabilities including

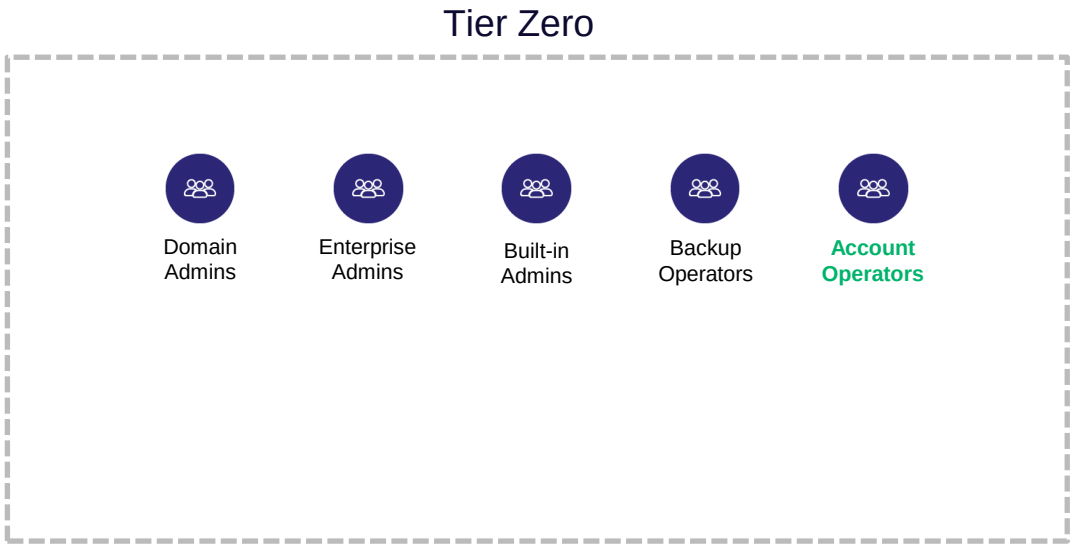
- Members of local administrators group
- Personnel who know the root or built in administrator password
- Administrators of any management or security tool with agents installed on those systems

Today’s Discussion

Name	**Backup Operators**
Identification	S-1-5-32-551
Rights	• Can read registry of DCs remotely incl. SAM database
Tier Zero Compromise?	Yes
Is it Tier Zero?	Yes

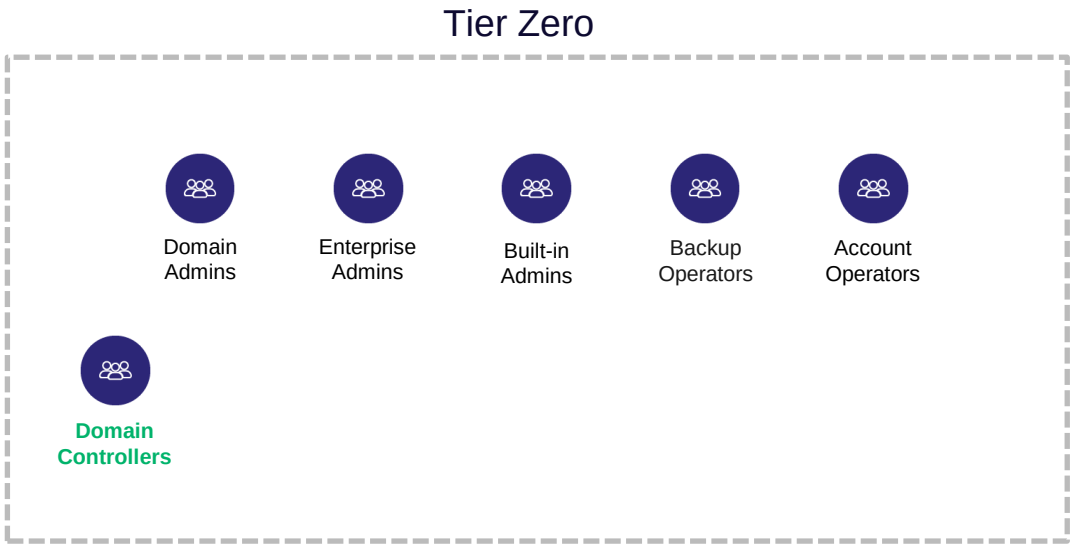


Name	**Account Operators**
Identification	S-1-5-32-548
Rights	• Full control in default security descriptor of User, Group, and Computer
Tier Zero Compromise?	Depends
Is it Tier Zero?	Yes

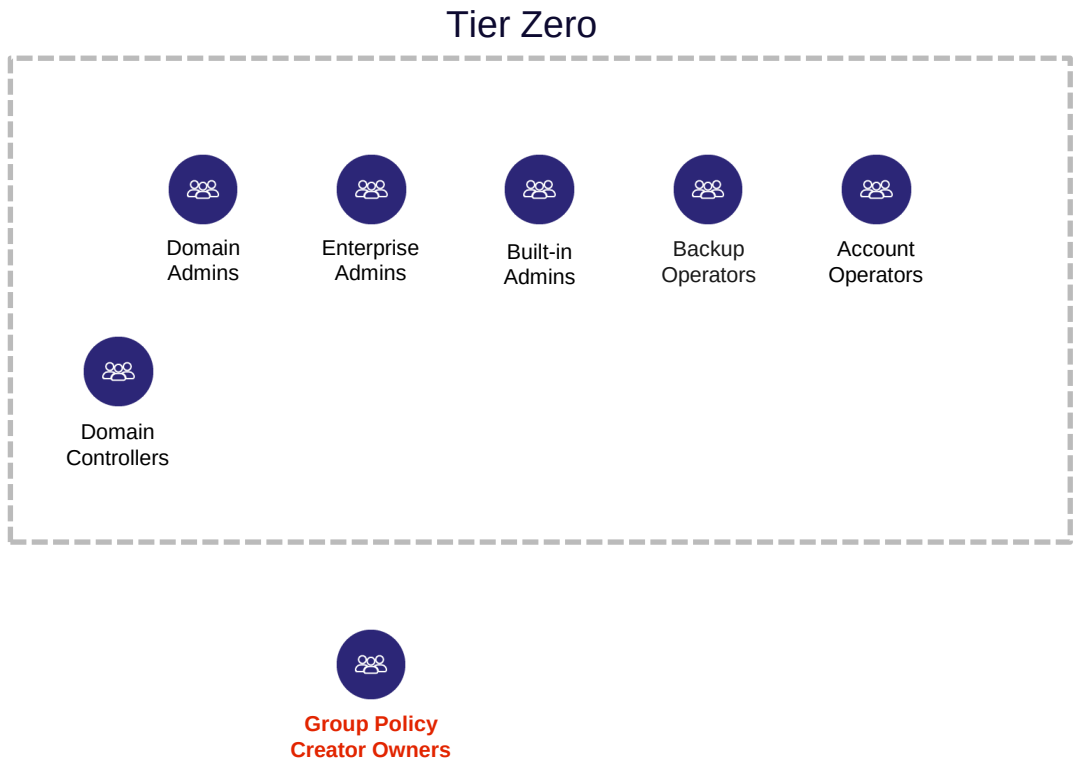


Observation: Per our definition, you may control enterprise identities without controlling the enterprise identity infrastructure

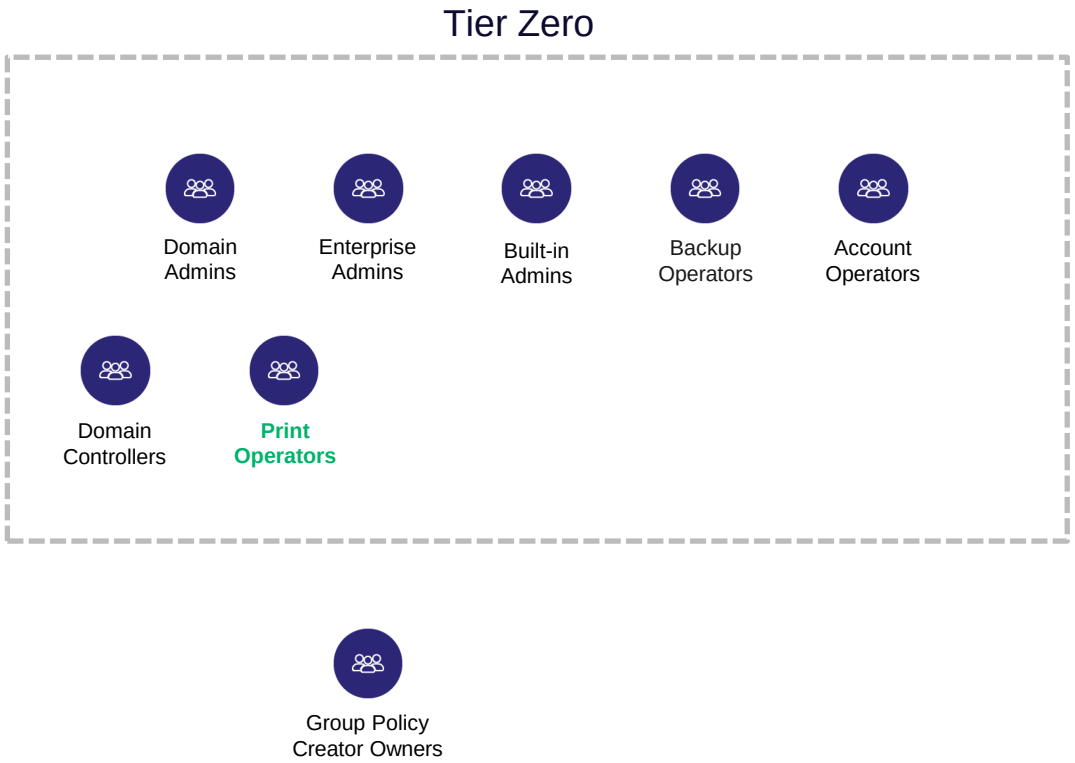
Name	**Domain Controllers**
Identification	S-1-5-21-<domain>-516
Rights	• Has GetChangesAll
Tier Zero Compromise?	No
Is it Tier Zero?	Yes



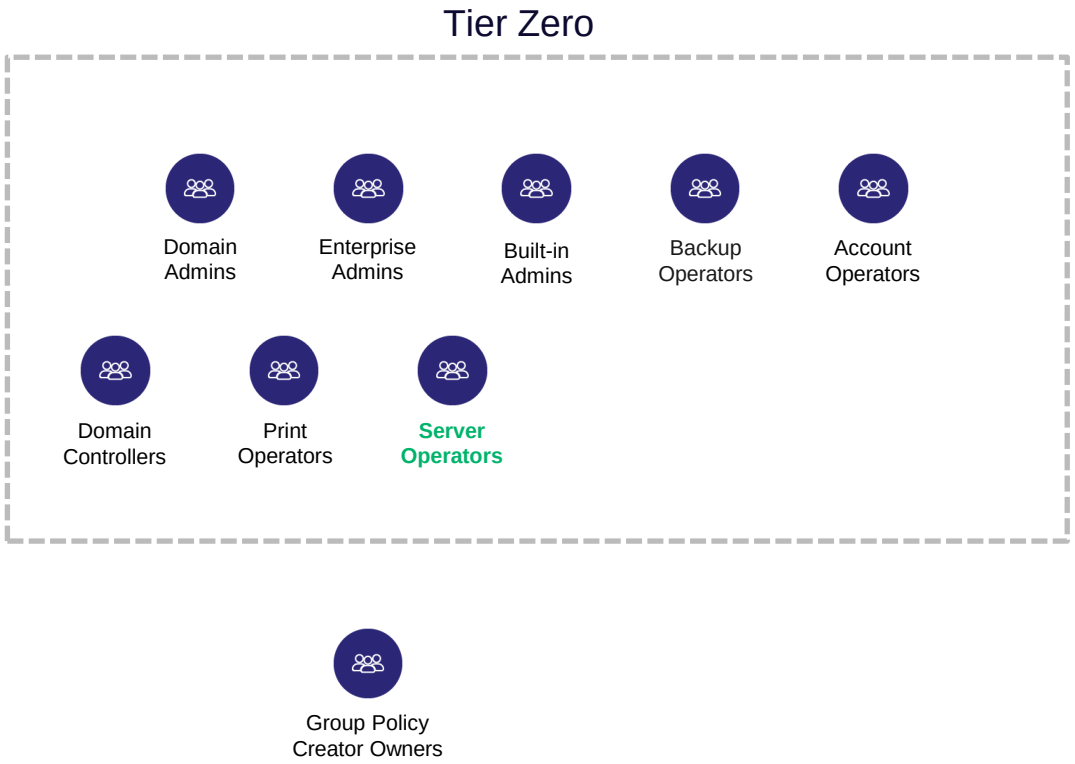
Name	**Group Policy Creator Owners**
Identification	S-1-5-21-<domain>-520
Rights	• Can create GPOs
Tier Zero Compromise?	No
Is it Tier Zero?	No



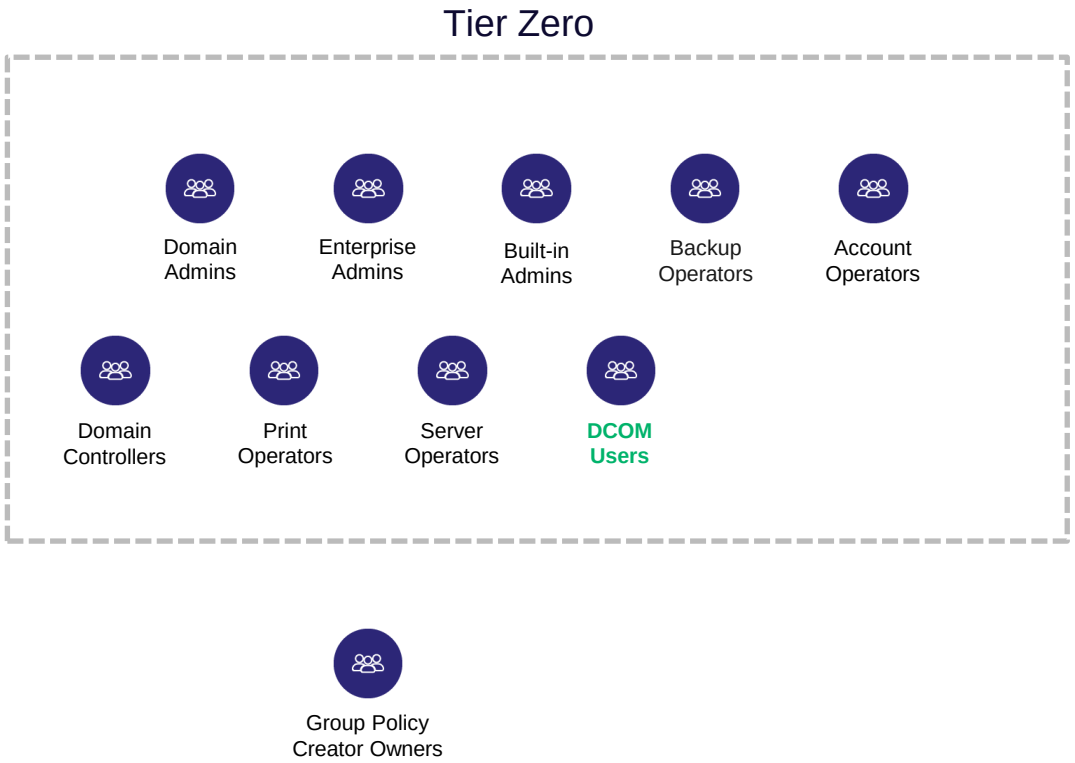
Name	**Print Operators**
Identification	S-1-5-32-550
Rights	• Can log in locally on DCs • Can load device drivers on DCs
Tier Zero Compromise?	Depends
Is it Tier Zero?	Yes



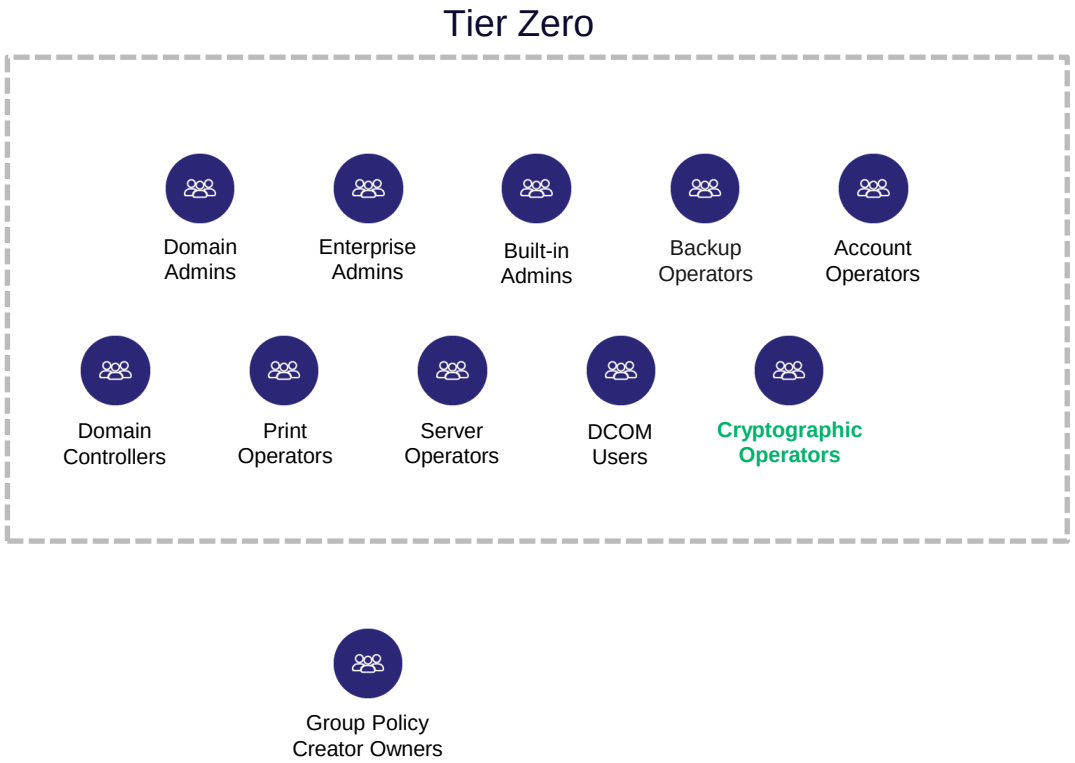
Name	**Server Operators**
Identification	S-1-5-32-549
Rights	• Can log in locally on DCs • Can read and backup all files on DCs
Tier Zero Compromise?	Depends
Is it Tier Zero?	Yes



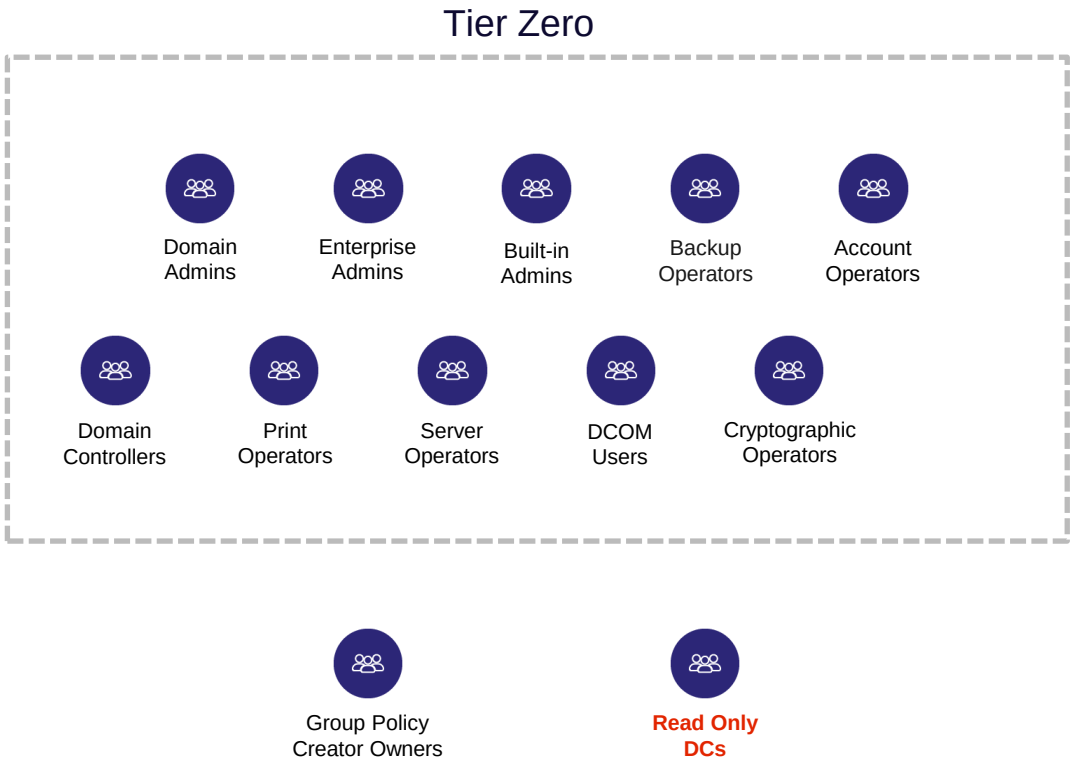
Name	**Distributed COM Users**
Identification	S-1-5-32-562
Rights	• Can launch, activate, and use Distributed COM objects on DCs
Tier Zero Compromise?	No
Is it Tier Zero?	Yes



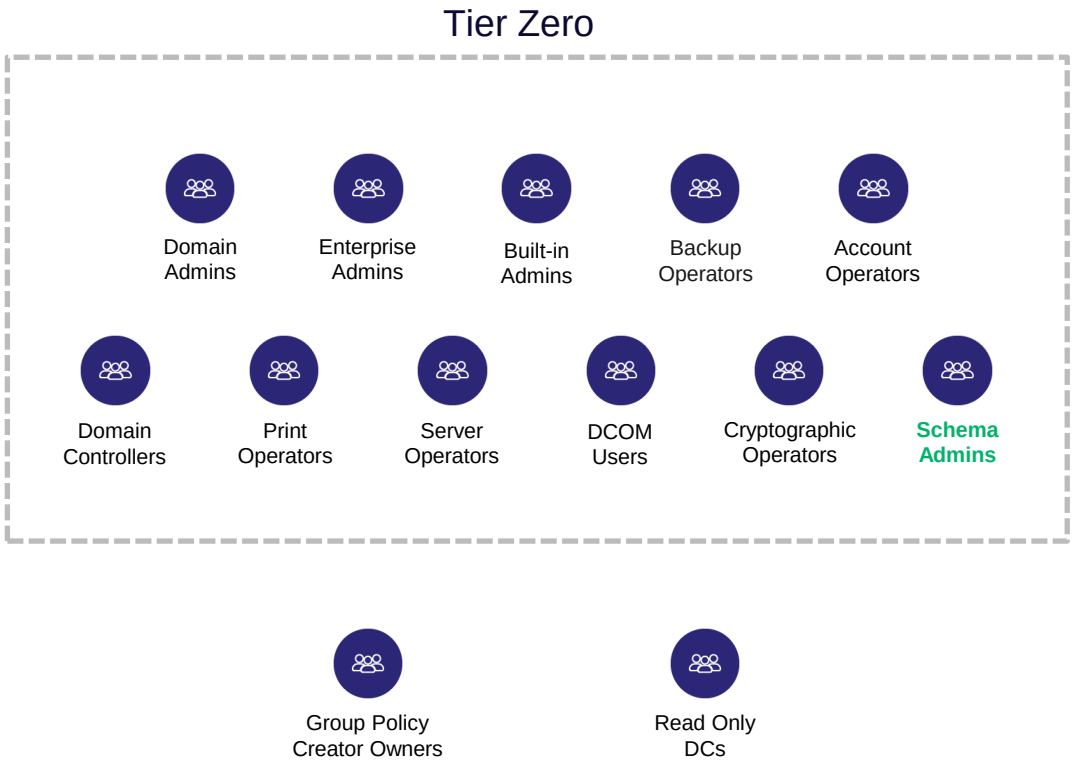
Name	**Cryptographic Operators**
Identification	S-1-5-32-569
Rights	• Has various privileges on DCs
Tier Zero Compromise?	No
Is it Tier Zero?	Yes



Name	**Read-only Domain Controllers**
Identification	S-1-5-21-<domain>-521
Rights	• No compromising privileges
Tier Zero Compromise?	No
Is it Tier Zero?	No



Name	**Schema Admins**
Identification	S-1-5-21-<root domain>-518
Rights	• Full control of AD schema
Tier Zero Compromise?	Depends
Is it Tier Zero?	Yes



Tier Zero Table

Name	Tier Zero	Tier Zero Compromise	Reasoning	Type	Identification	Protected by AdminSDHolder
Account Operators	YES	DEPENDS	The Account Operators group has full control of all Users, Groups, and Computers except for those protected by AdminSDHolder = Tier Zero without having control over Tier Zero.	DC group	SID: S-1-5-32-548	YES
Administrators	YES	YES	The Administrators group has full control over most of AD's essential objects.	DC group	SID: S-1-5-32-544	YES
Backup Operators	YES	YES	By Default, Members of Backup Operators can dump the registry hives of a DC remotely, extract the DC account credentials, and perform a DCSync attack.	DC group	SID: S-1-5-32-551	YES
Cryptographic Operators	YES	NO	The local privileges the group has on the DCs are considered security dependency, and the group is therefore considered Tier Zero.	DC group	SID: S-1-5-32-569	NO
Distributed COM Users	YES	NO	The local privileges the group has on the DCs are considered security dependency, and the group is therefore considered Tier Zero.	DC group	SID: S-1-5-32-562	NO
Domain Admins	YES	YES	The Domain Admins group has full control over most of AD's essential objects.	AD group	SID: S-1-5-21-<domain>-512	YES
Domain Controllers	YES	NO	This group is a security dependency for Tier Zero. Control over the group can impact the operability of DCs.	AD group	SID: S-1-5-21-<domain>-516	YES
Enterprise Admins	YES	YES	The Enterprise Admins group has full control over most of AD's essential objects.	AD group	SID: S-1-5-21-<root domain>-519	YES
Group Policy Creator Owners	NO	NO	This group has the privilege to create new GPOs but can't modify GPOs created by others and no privileges to link GPOs to an OU, a site, or the domain.	AD group	SID: S-1-5-21-<domain>-520	NO
Print Operators	YES	DEPENDS	This group's local privileges are considered security dependency for the DCs, and the group is therefore considered Tier Zero.	DC group	SID: S-1-5-32-550	YES
Read-only Domain Controllers	NO	NO	The Read-only Domain Controllers group has no compromising privileges, and there are no known ways to abuse membership in the group to compromise Tier Zero.	AD group	SID: S-1-5-21-<domain>-521	YES
Schema Admins	YES	DEPENDS	The Schema Admins group has full control over the AD schema which would allow an attacker to create or modify ACEs for future AD objects. An attacker could grant full control to a compromised principal on any object type and wait for the next Tier Zero asset to be created, to then have a path to Tier Zero.	AD group	SID: S-1-5-21-<root domain>-518	YES
Server Operators	YES	DEPENDS	This group's local privileges are considered security dependency for the DCs, and the group is therefore considered Tier Zero.	DC group	SID: S-1-5-32-549	YES

Access and contribute directly

- https://github.com/BloodHoundAD/TierZeroTable
- Submit contributions or refinements

Topics for next sessions

- Azure AD Roles
- More controversial on-prem principals (DNS Admins, Exchange, KRBTGT)
- Microsoft Identity additions (ADFS, ADCS, SCCM)
- Third-party solutions (PAM, EDR, Backup providers)

Questions