Jonas Bülow Knudsen June 22, 2023

Posts from SpecterOps team members on various topics relating information security

Tier Zero is a crucial group of assets in Active Directory (AD) and Azure. Its purpose is to protect the most critical components by creating a security boundary and preventing a complete compromise.

Defining Tier Zero for your environment is not a straightforward task. It involves examining various assets and their relationships. You need to consider if principals are meant to have the level of control they have and if they are essential for the enterprise identity infrastructure's operability.

We want to make this process of determining Tier Zero easier for organizations. In this blog post series, we will explain how we define Tier Zero and explain what common assets we recommend to be part of Tier Zero.

This blog post was written together with Elad Shamir and Justin Kohler. It is the first in a series released after each episode of our webinar series called *What is Tier Zero*. You can watch the first episode here: Defining the Undefined: What is Tier Zero.

Check out Part 2 here: What is Tier Zero — Part 2

History of Tier Zero

This timeline shows the launch of Azure and AD, governance/best practice models for managing secure access, and some particularly notable toolsets for manipulating Azure and AD:

It was 13 years after AD was in place that we got more concrete guidance on how to manage and segment access. It is no wonder most organizations are in the place they are today when they had limited vendor guidance early on besides "Least Privilege".

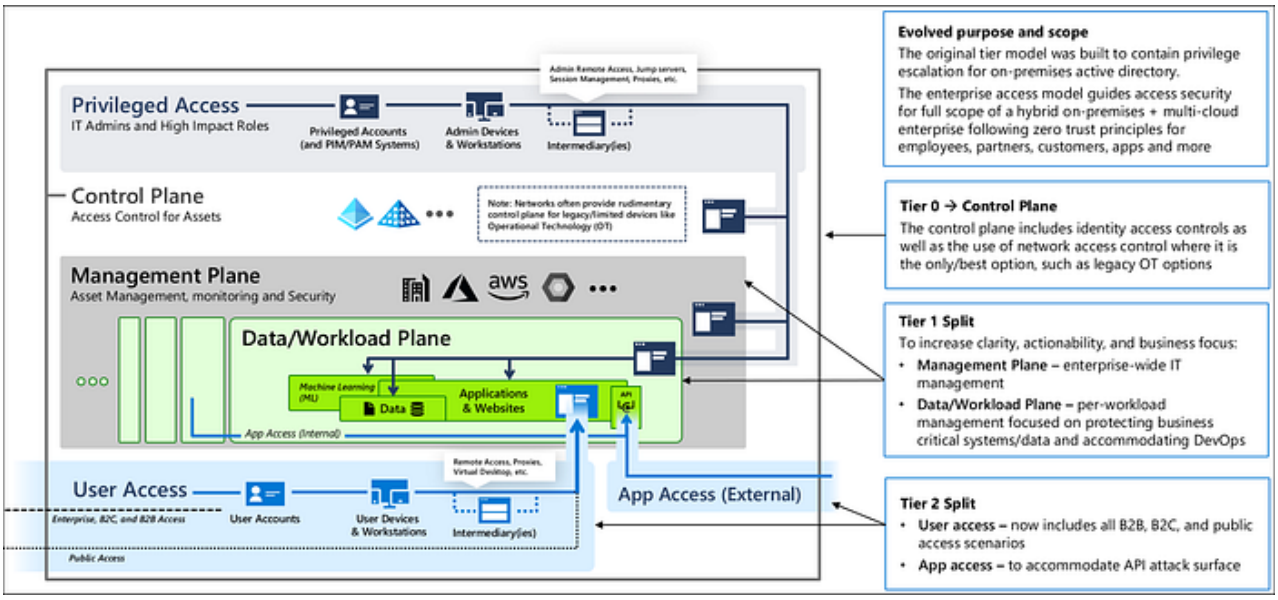
We had a model for managing secure access starting in 2012 but we had no way of verifying implementation. Said a different way, how could we ensure we were doing it correctly to protect our environment? Annual pentests most likely highlighted that we were not doing it correctly.

Andy, Rohan, and Will released BloodHound which started visualizing Attack Paths in 2016 and it became immediately apparent how big of a problem this was. BloodHound helps penetration testers find the shortest attack path to a given target, but it does not reveal the full extent of the problem with all the attack paths to Tier Zero and the exposure of the attack paths. We started getting that visibility with BloodHound Enterprise in 2021. We wrote about a common question after deploying BloodHound Enterprise when we provided visibility: Active Directory Attack Paths — "Is it always this bad?".

This timeline of secure access governance models leaves us with a few takeaways:

1. Take it easy on our partners in IT operations and AD / AZ administrators, they have been forced to build with late guidance and bad visibility.
2. Governance models only work if you can validate implementation with technical control.
3. Ambiguous guidance needs to be defined before it can be implemented.

The third takeaway leads us to the question that forms the title of this series: *What is Tier Zero?* It is impossible to isolate and protect the critical assets of the environment without determining what assets that is. In Microsoft's latest model for secure access, theEnterprise Access Model, Tier Zero is renamed to the *Control Plane*:



Most are more familiar with "Tier Zero" and we will use Tier Zero for this series.

The current explanation around the scope of Tier Zero is too high level and generates questions. These questions inhibit the adoption or generate gaps in the implementation. This is why we have decided to create this series — to provide our definition of Tier Zero and explain which common assets belong to Tier Zero and why that is.

Defining Tier Zero

Microsoft's Tier Zero Definition

When Microsoft initially introduced the concept of Tier Zero, they defined it as follows:

of enterprise identities in the environment. Tier 0 includes accounts, groups, and other assets that have of the Active Directory forest, domains, or domain controllers, the assets in it."

This definition leaves a lot to be desired. It starts with "Direct Control" and then shifts to "direct or indirect administrative control". What does that mean? Is it a contradiction?

It then introduces an additional qualifier: “and all the assets in it”. What if a principal controls all assets but one? Where do we draw the line? Some would say that all Tier Zero principals can control each other and, indeed, **all** assets in AD. Still, we will challenge that argument later in this post.

Direct vs. Indirect Control

What is “control”? And what is the difference between direct and indirect control?

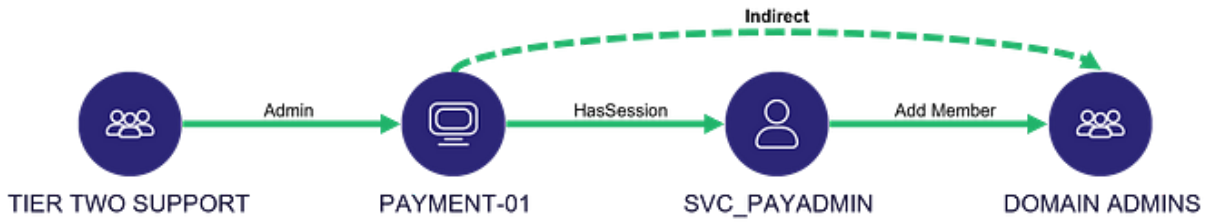
The simplest way to define “control” or “administrative control” in this context is a relationship that can contribute to compromising the controlled asset or impact its operability.

“Direct” control could mean a couple of things:

- A direct relationship between the controlling and the controlled objects, i.e., one “hop” away
- Having explicit rights on the controlled asset (e.g., having the Add Member rights on a group)

On the other hand, “indirect” control could also mean a couple of things:

- Control has the transitivity property, meaning that if A controls B and B controls C, then A also controls C
- The control relationship is implicit



What is Implicit Control?

Understanding the concept of “implicit control” requires returning to the fundamental principle behind the tiering model, the “Clean Source Principle”.

The Clean Source Principle dictates that all security dependencies must be as trustworthy (secure) as the object being secured.

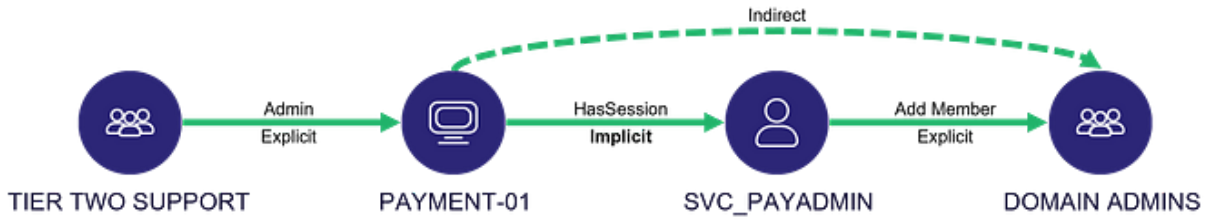
Microsoft made the connection clear by stating that “any subject in control of an object is a security dependency of that object”. That statement does not necessarily mean that the opposite statement is also true. But we argue that, indeed, any security dependency of an object has control of the object, which is one way of defining “implicit control”.

One example is the infamous “HasSession” edge. Suppose a user is logged onto a host. In that case, the host is in control of the user because the host is in possession of the user’s Kerberos tickets, NT hash, and maybe even cleartext password in some cases.

There are exceptions, such as a Restricted Admin Mode RDP session established with Kerberos authentication, but we won't elaborate on that here.

A more straightforward example is hardware. If an attacker can compromise the hardware on which a domain controller runs, the attacker can compromise the domain controller. It also applies to virtualization, i.e., if an attacker compromises a hypervisor on which a domain controller runs, the attacker can compromise the domain controller.

One last very common example is EDR agents. Most EDR agents nowadays grant analysts and operators the ability to interrogate the host remotely by executing commands and manipulating the operating system. In fact, some EDR agents could make great C2 implants. If such an EDR is installed on a domain controller, then all the users and systems that can control that EDR can also control the domain controller through transitivity or "indirect" control.



What Makes a Security Dependency?

The simplest way to define a security dependency is that a component's security relies on another component's security.

In that case, compromising a security dependency **may** allow compromising components that depend on it. Keep in mind that some attacks have multiple prerequisites; therefore, compromising a security dependency may be insufficient for compromising the component that depends on it. Nevertheless, it is still a security dependency and must be protected accordingly, as per the Clean Source Principle.

For example, suppose an account may be protected by MFA, e.g., the user must enter a password and present a FIDO device to authenticate. Even though the password is insufficient for compromising the account by itself, it must remain protected regardless of the second authentication factor.

Better Tier Zero Definition

Putting all these considerations and definitions together, we propose the following Tier Zero definition:

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

You might notice that with this definition, a principal might belong to Tier Zero because it is in control of enterprise identities, even though it is not in control of the enterprise identity infrastructure. Also, this definition does not necessarily dictate that all Tier Zero principals and assets are in control of each other.

What assets belong to Tier Zero — Part 1

To get started with the list of assets we think belong to Tier Zero, we will look at what Microsoft consider Tier Zero.

Microsoft used to have a list of the assets they recommended to include in Tier Zero in their online documentation for the AD tier model. This list can still be found on the Wayback Machine here. Today, it is less obvious, but Microsoft still provide a similar list in their documentation. In the section Privileged access security levels, Microsoft goes into the details of what they consider *privileged security*:

is the highest level of security designed for roles that could easily cause a major incident and potential material damage to the organization in the hands of an attacker or malicious insider.

…

Privileged access security roles typically include:

> *related roles*

We will in this blog post series go through this list and determine whether we would recommend considering the items as Tier Zero. Additionally, we will discuss assets that are not on this list but may belong to Tier Zero as well.

The bold items in the list were what Microsoft had in their list for the AD tier model documentation. In the next sections, we will dive into those items and whether we think these AD groups should be part of Tier Zero.

Administrators, Domain Admins, Enterprise Admins

These three groups have full control over most of AD's essential objects and are inarguably part of Tier Zero.

Backup Operators

The Backup Operators group has the SeBackupPrivilege and SeRestorePrivilege rights on the domain controllers by default. These privileges allow members to access all files on the domain controllers, regardless of their permission, through backup and restore operations. Additionally, Backup Operators have full remote access to the registry of domain controllers. To compromise the domain, members of Backup Operators can dump the registry hives of a domain controller remotely, extract the domain controller account

credentials, and perform a DCSync attack. Alternative ways to compromise the domain exist as well. The group is considered Tier Zero because of these known abuse techniques.

Account Operators

The Account Operators group has GenericAll in the default security descriptor on the AD object classes: User, Group, and Computer. That means all objects of these types will be under full control of Account Operators unless they are protected with AdminSDHolder. Not all Tier Zero objects will be protected with AdminSDHolder typically, as not all Tier Zero objects will be included in Protected Accounts and Groups. This means Account Operators members have a path to compromise Tier Zero most often.

It is possible to delete all GenericAll ACEs for Account Operators on Tier Zero objects. To protect future Tier Zero objects, one would have to either remove the Account Operators ACE from the default security descriptors or implement a process of removing the ACEs as Tier Zero objects are being created. However, we recommend not using the group and classifying it as Tier Zero instead.

Domain Controllers

The Domain Controllers group has the GetChangesAll privilege on the domain. This is not enough to perform DCSync, where the GetChanges privilege is also required.

There are no known ways to abuse membership in this group to compromise Tier Zero. However, the GetChangesAll privilege is considered a security dependency that should only be held by Tier Zero principals. Additionally, control over the group allows one to impact the operability of Tier Zero by removing domain controllers from the group, which breaks AD replication. The group is therefore considered Tier Zero.

Group Policy Creator Owners

The Group Policy Creator Owners group has the privilege to create new GPOs. However, members of the group can only edit or delete GPOs that they have created themselves. The group has no privileges to link GPOs to an OU, a site, or the domain.

There are no known ways to abuse membership of the Group Policy Creator Owners group to compromise Tier Zero. The group is not a security dependency for Tier Zero and is therefore not considered Tier Zero.

Print Operators and Server Operators

The Print Operators group and the Server Operators group have local privileges on the domain controllers and can log on locally on domain controllers by default. Print Operators can load device drivers and Server Operators can read and backup all files among other privileges.

It is feasible to remove the logon privilege from the groups on the domain controllers, such that the groups have no known abusable path to Tier Zero. However, the local privileges are considered security dependencies for the domain controllers, and the groups are therefore considered Tier Zero.

Cryptographic Operators and Distributed COM Users

The Cryptographic Operators group and Distributed COM Users group have local privileges on domain controllers but no privilege to log in. Cryptographic Operators can perform cryptographic operations and Distributed COM Users can launch, activate, and use Distributed COM objects.

There are no known ways to abuse the membership of the groups to compromise Tier Zero. The local privileges they have on the domain controllers are considered security dependencies, and the groups are therefore considered Tier Zero.

Read-only Domain Controllers

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.

Whether the group is a security dependency for read-only domain controller servers is not clear, but read-only domain controller servers are not considered Tier Zero (only the read-only domain controller AD objects are). The Read-only Domain Controllers group is therefore not considered Tier Zero. We will dive deeper into how read-only domain controllers should be handled in one of the following blog posts.

Schema Admins

The Schema Admins group has full control over the AD schema. This allows the group members 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. This attack could be remediated by removing any unwanted ACEs on objects before they are promoted to Tier Zero, but we recommend considering the group as Tier Zero instead.

The Tier Zero Table

To make it easier for organizations and security principals to define Tier Zero in a given environment, we have created a table for common assets that we recommend considering Tier Zero. The table currently only contains the AD and domain controller groups we have covered in this blog post, but we will add more assets throughout the *What is Tier Zero* webinar and blog post series.

We hope the community will help build the table, such that everyone can benefit from the knowledge. Any feedback and contributions are much appreciated.

You can view and contribute to the table here:
https://github.com/SpecterOps/TierZeroTable/