TRUESEC

Active Directory Tiering Implementation

What Is AD Tiering Implementation?

The concept of putting our most valuable things in the most protected place isn't new. It's been around pretty much since we've had....well, things. Using a tiering model in Active Directory (AD) hasn't been around as long, but the concept of AD tiering and recommending its implementation has been around for more than a decade.

Given that approximately 90% of Global Fortune 1000 companies use AD as a primary method to authenticate, it's surprising that tiering isn't implemented more often.

The lack of deployment has historically been because the implementation of AD tiering is perceived as a large, complex project often associated with significant risks to the availability of a company's systems and resources.

That's what's different about Truesec's AD Tiering Implementation. We've implemented tiering in countless ADs without impacting businesses. With Truesec, AD Tiering is typically accomplished in a few days, not weeks or months, as some would have you believe.

What We've Learned

We're one of the most trusted organizations in cyber incident response, and we collaborate with global leaders in the community to learn and educate. One of the more common techniques of cybercriminals we've observed is that they tend to move laterally through networks (e.g., from computer to computer) until they locate credentials they can use to elevate their privileges. They do this until they obtain domain admin access. By implementing a tiered model for the AD, the attacker is unable to locate anything outside of the tier in which they are located. Tiering creates multiple zones (or "tiers") that separate frequently compromised devices such as regular workstations from valuable ones (e.g., domain controllers, backup systems, PKI, and other business-critical applications or systems).

AD Tiering Implementation will provide you with:

- A team using a battle-proven, efficient methodology to implement and document tiering without impacting your business.
- An efficient, secure use of your existing infrastructure investments.
- A means to make it more difficult for attackers to attempt to compromise sensitive systems.
- The ability to protect the most valuable assets and systems without adding complexity for the business.
- Advice from Truesec on how to continue to increase your cyber resilience.

About Us

As a global cybersecurity company, we're proud to be at the forefront of protecting organizations and our society against cyber threats. Our purpose has been clear since day one: Creating safety and sustainability in a digital world by preventing cyber breach and minimizing impact. We never cease to challenge and reinvent ourselves to help defend your most valuable data assets every day.

TRUESEC

A Safe Digital Future

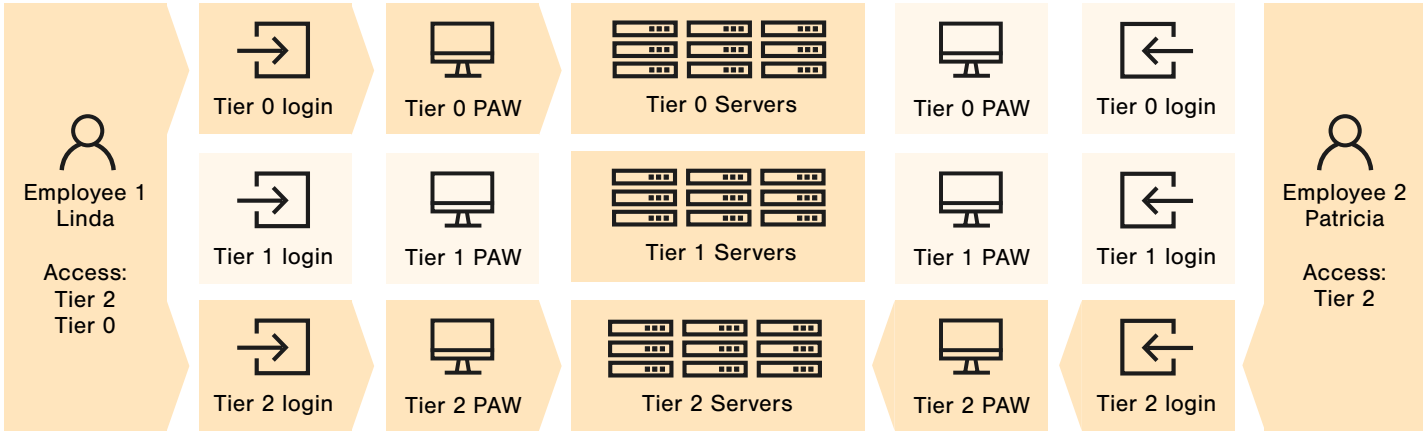
Sweden	Denmark	US
truesec.com	truesec.com	truesec.com
+46 8 10 00 10	+46 8 10 00 10	(904) 900-4532
hello@truesec.com	hello@truesec.com	hello@truesec.com

The Truesec Promise

We always strive for the best results for our customers.
That is a Truesec promise.

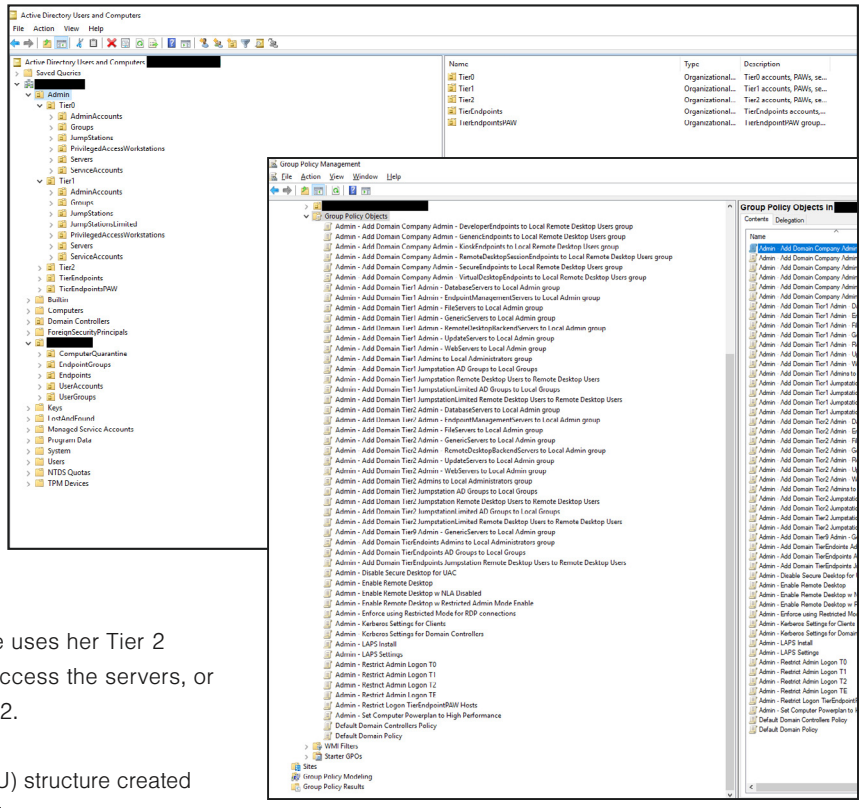
A Brief Look Into a Tiered Active Directory

As previously noted, when the AD is tiered, you limit the exposure of sensitive credentials. The result will look something like this:



This image illustrates that Employee1 (let's call her Linda) can perform administrative tasks in Tier 0 and Tier 2. Employee 2 (who we'll call Patricia) can only perform administrative tasks in Tier 2.

When Linda works in Tier 0, she logs in with her Tier 0 admin account, using the Tier 0 privileged access workstation (PAW), and can only move horizontally within Tier 0. Neither the admin account nor the PAW can be used to access any other tier. This is due to the logon and control restrictions put in place by the group policy objects (GPOs) created in AD when implementing the Truesec tiering model.



Similarly, when Linda performs administrative tasks on any server in Tier 2, she logs in with her Tier 2 admin account on the Tier 2 PAW.

Patricia can only do administrative tasks in Tier 2. She uses her Tier 2 admin account on her Tier 2 PAW and then she can access the servers, or systems, she should be able to administer within Tier 2.

An example of the GPOs and the organizational unit (OU) structure created by the Truesec tiering model is shown here as an overview.

TRUESEC
A Safe Digital Future

Sweden
truesec.com
+46 8 10 00 10
hello@truesec.com

Denmark
truesec.com
+46 8 10 00 10
hello@truesec.com

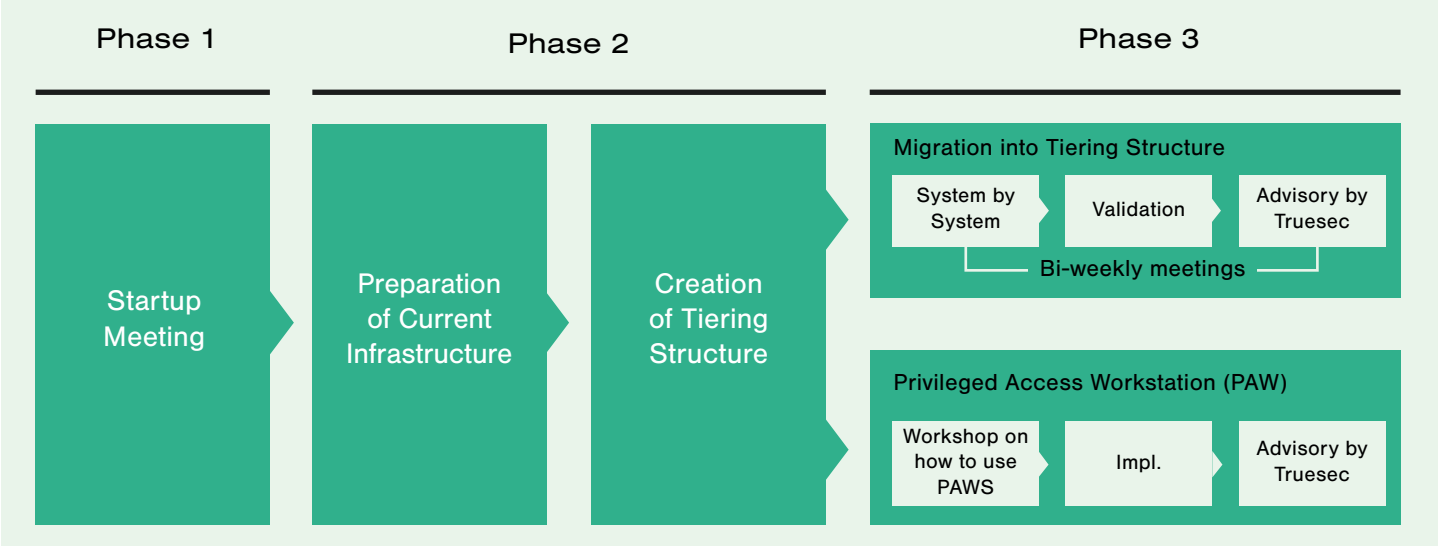
US
truesec.com
(904) 900-4532
hello@truesec.com

The Partnership

We see our work with our customers as a partnership.
We work together to get the best results and prevent incidents.

Methodology

This is best done together by the experts from Truesec and the team that manages the operation of the IT resources. This ensures that information and knowledge are transferred quickly and efficiently.



The 3 Phases

Phase 1 - Knowledge

We conduct a startup meeting that includes the concepts and benefits of working with a tiering model. Examples of areas covered:

- Why to use a tiering model
- The tiering model
- Why and when to use a privilege access workstation (PAW)
- Ways of working for admins

Phase 2 - Implementation

In Phase 2, the environment is prepared, and information regarding current and future privileged users is collected. Then the new tiering structure is created with all the policies and settings required. “Break the glass” accounts are also created.

Phase 3 - Guidance

In Phase 3, the systems are protected one by one in the new tiering model by your team. Also, the implementation of privileged access workstations (PAW) is completed. As this establishes a new way of accessing the environment for some administrators, experts from Truesec are there to guide and assist during this phase. This is supported by a bi-weekly meeting with Truesec experts to answer questions and provide further guidance.

TRUESEC
A Safe Digital Future

Sweden
truesec.com
+46 8 10 00 10
hello@truesec.com

Denmark
truesec.com
+46 8 10 00 10
hello@truesec.com

US
truesec.com
(904) 900-4532
hello@truesec.com

If You Are Under Attack, Call Truesec

+46 (0) 8 10 72 00
incident@truesec.com

What Is Included	AD Tiering Implementation
Scoping	✓
Startup Meeting	✓
Preparation of Current Infrastructure	Often Prepared by IT Operations With Aid From Truesec
Creation of Tiering Structure in Active Directory	✓
Creation of Group Policy Objects to Govern Access in AD	✓
Creation of Security Groups for Group Policy Object Filtering	✓
Creation of New Admin Accounts Per Tier	✓
PAW Workshop	✓
Technical Configuration for Joining the PAWs to the Correct OUs	✓
Implementation of Authentication Policy Silos for PAWs	✓
Migration of Critical Infrastructure to Tier 0 (AD, PKI, AAD Connect)	✓
Identification of Other Critical Infrastructure That Should Be in Tier 0	✓
Migration of Other Critical Infrastructure That Should Be in Tier 0	Optional
System by System Migration to Ensure Resilience of Operations	Optional
Technical Validation of Permissions Required for Each System	Optional
Advisory Services Provided by Truesec	Optional

How To Get Started With AD Tiering Implementation

You start by talking to your Truesec customer contact or any of our experts. Together you'll begin the journey to protect your organization's sensitive information and safeguard your corporate brand by scoping the assignment and determining what actions would benefit you most.

By implementing AD Tiering, you'll acquire the assistance of experts using a battle-proven, efficient methodology to implement and document tiering without impacting your business. This will increase your capability to protect your most valuable assets and systems.