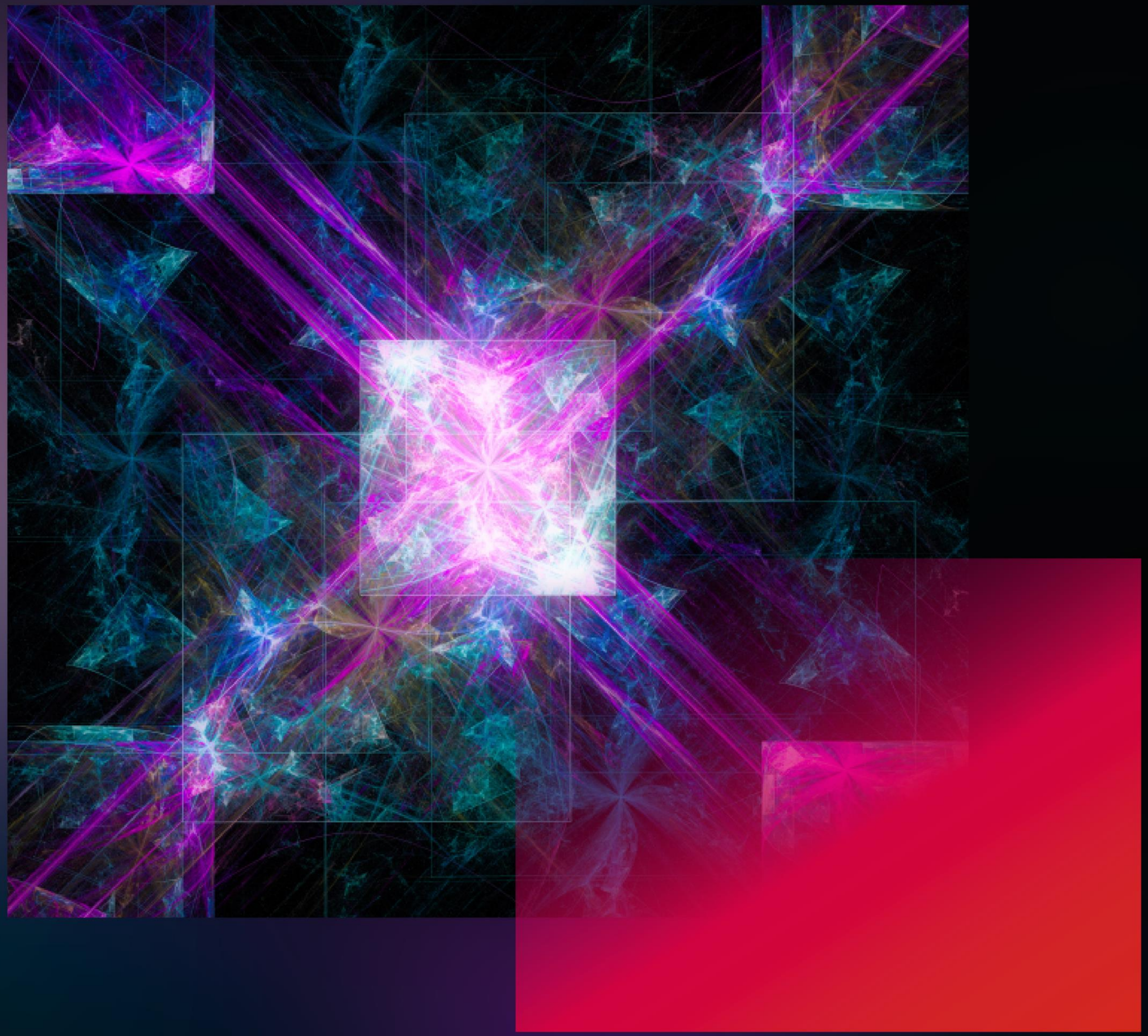
semperis

Webinar – Identity Days 2024

AD Migration : Why Security is not an option ?



Matthieu TRIVIER
Director of Pre-Sales, Semperis

KKR INSIGHT PARTNERS

Microsoft Partner
Enterprise Cloud Alliance
Microsoft Accelerator Alumni
Microsoft Co-Sell
Microsoft Intelligence Security Association (MISA)

semperis

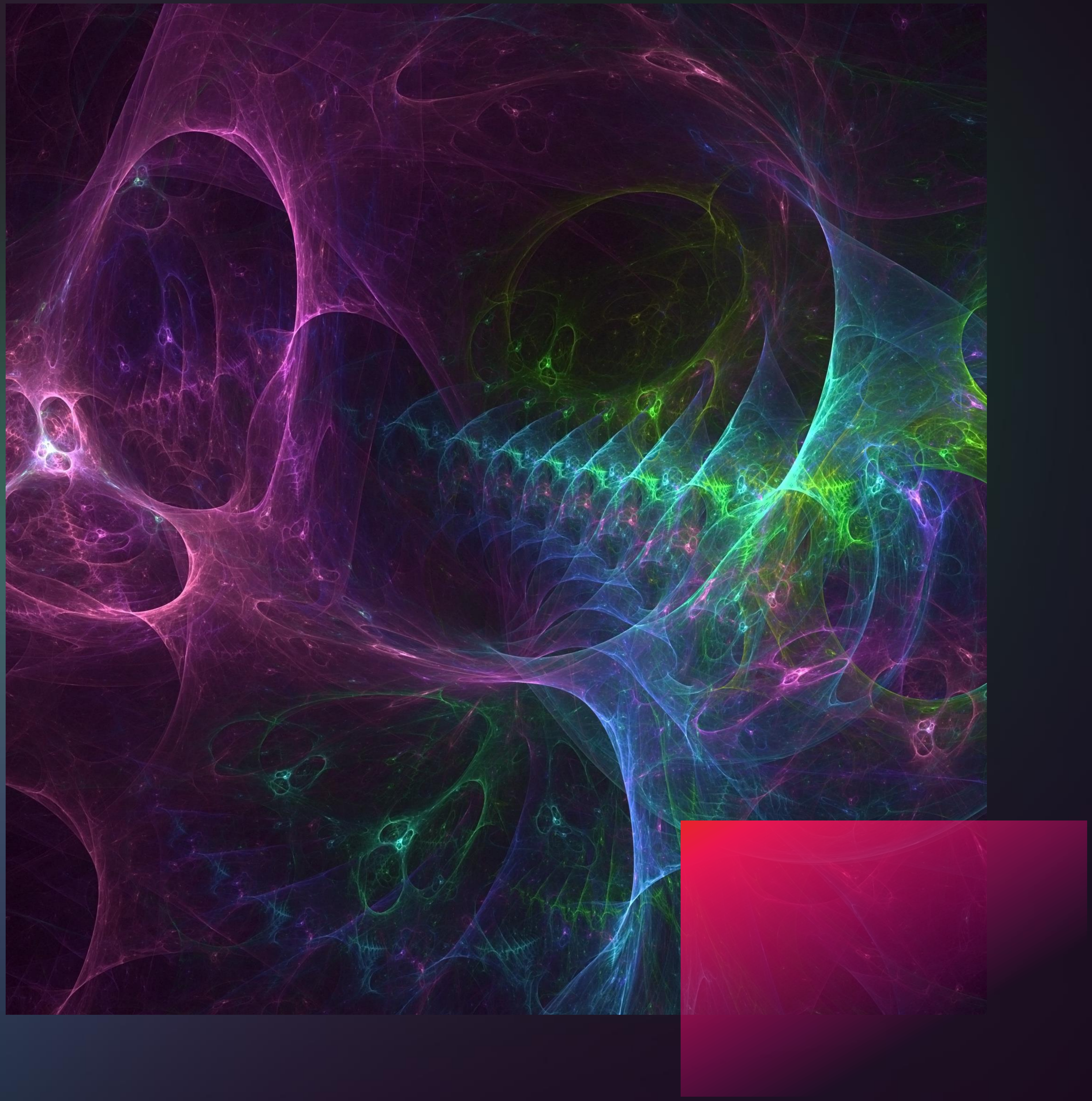
whoami

Matthieu TRIVIER

Director of Pre-Sales @ Semperis

For 15 years, I have been discussing Identity and Resilience with those who are willing to listen to me.

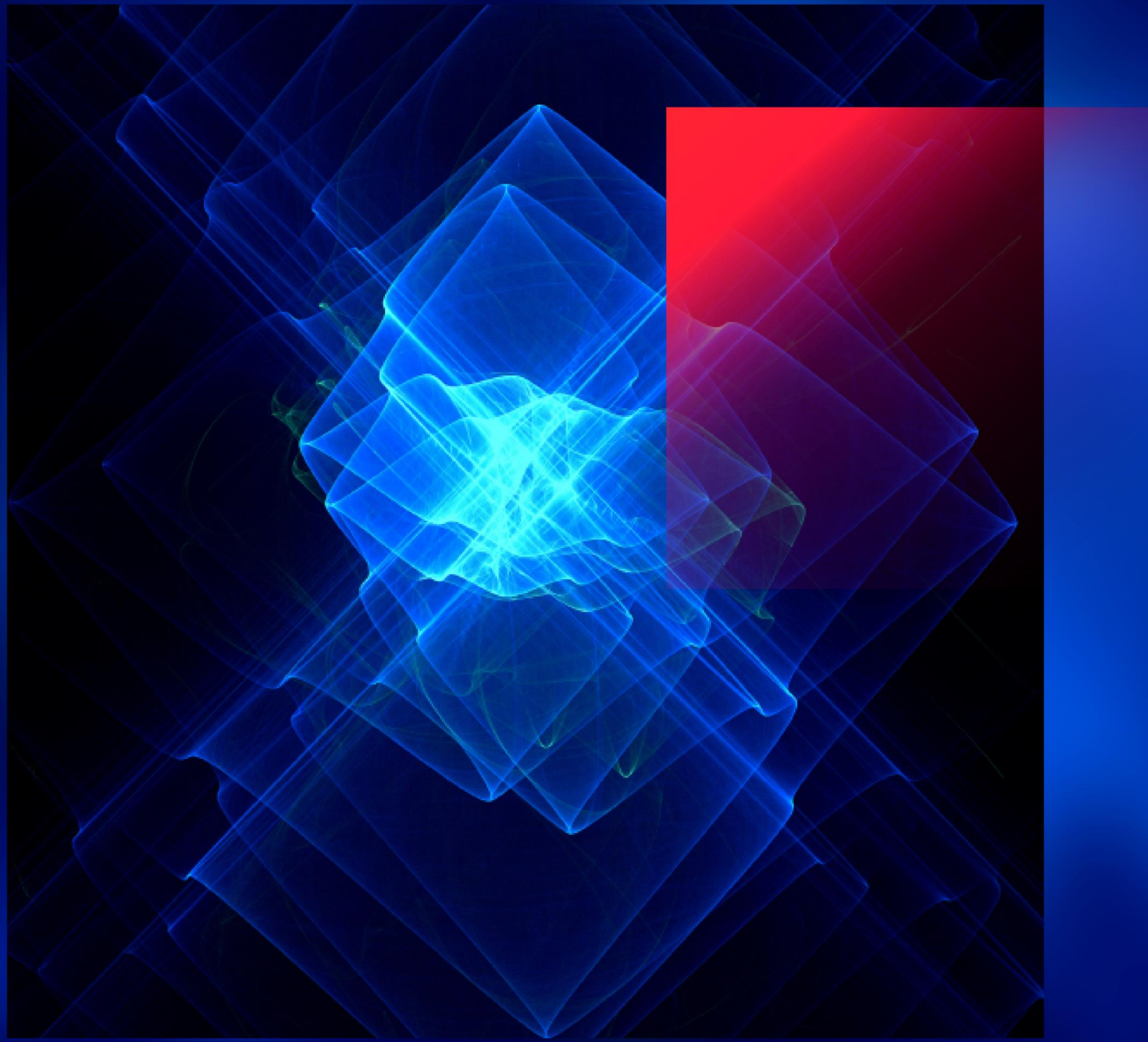
But also, sneakers and self-sustainable life, for those who prefer a lighter subject



semperis

Agenda

- AD Migration: Why ?
- AD Migration Risks
- How Semperis can help ?
- Introducing Semperis MAD
- Q&A !



semperis

AD Migration: Why ?

semperis

The Need

for Transforming Active Directory Environments

Mergers & Acquisitions

Consolidate or Segregate AD for a Merger, Acquisition or Divestiture

Prepare for the Cloud

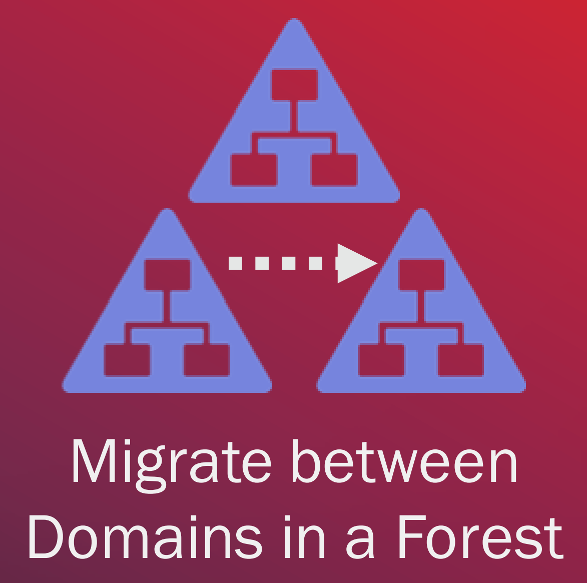
Consolidate AD to Avoid Issues when Migrating to Microsoft 365

Modernization Initiatives

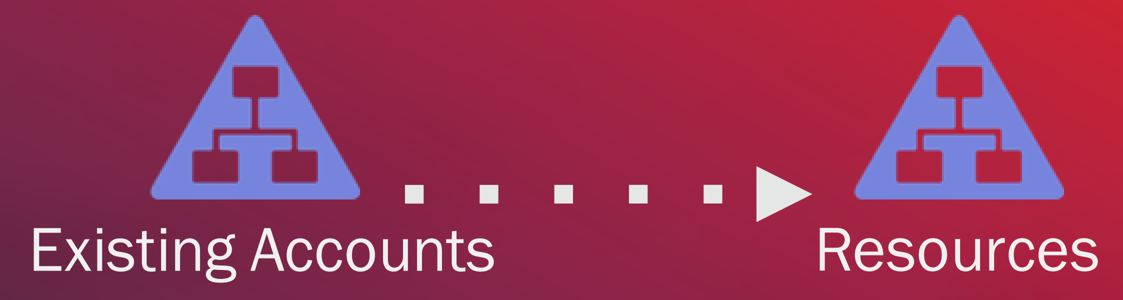
Restructure and Consolidate AD to Augment Efficiency, Manageability, and Security

semperis

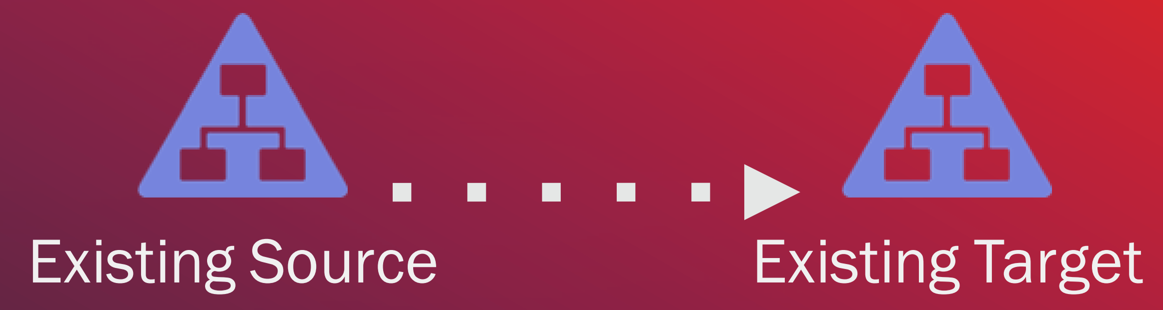
Types of Active Directory Migrations



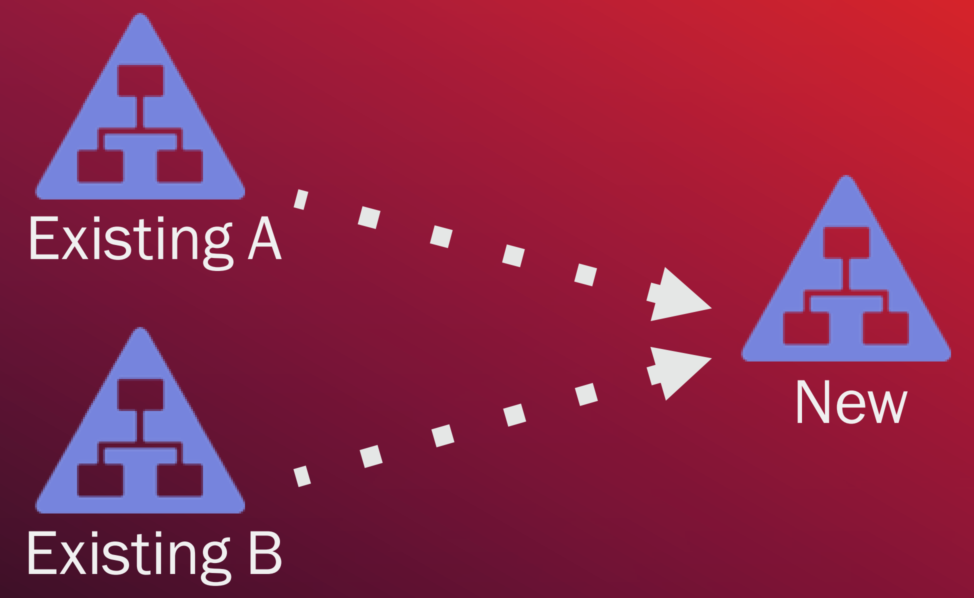
Intra-Forest Migration between Domains in the Same Forest



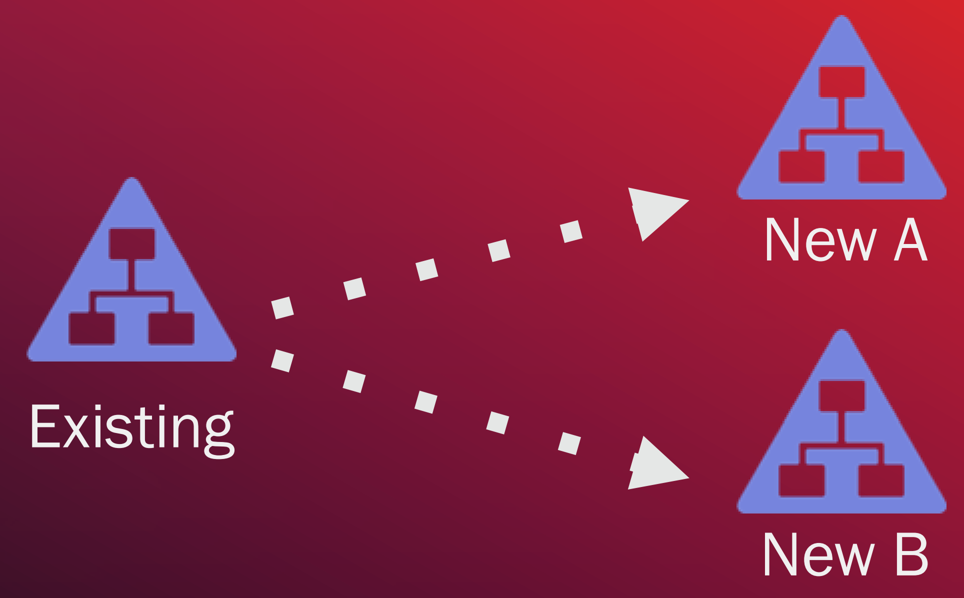
Separate a Forest into Accounts & Resources Forests



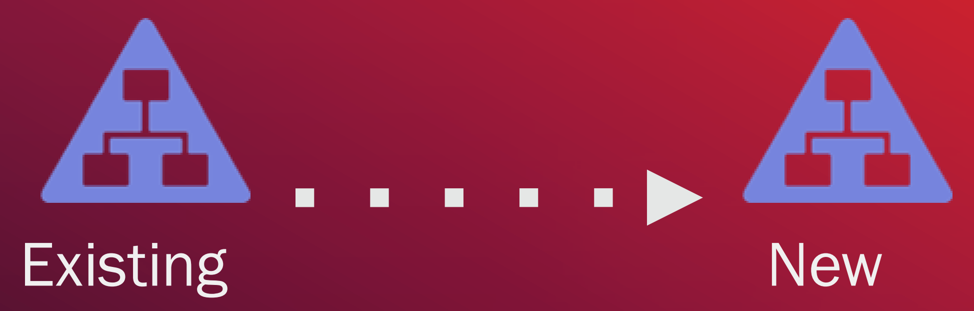
Merge a Forest into Another Existing Forest



Merge Two Forests into a New Forest

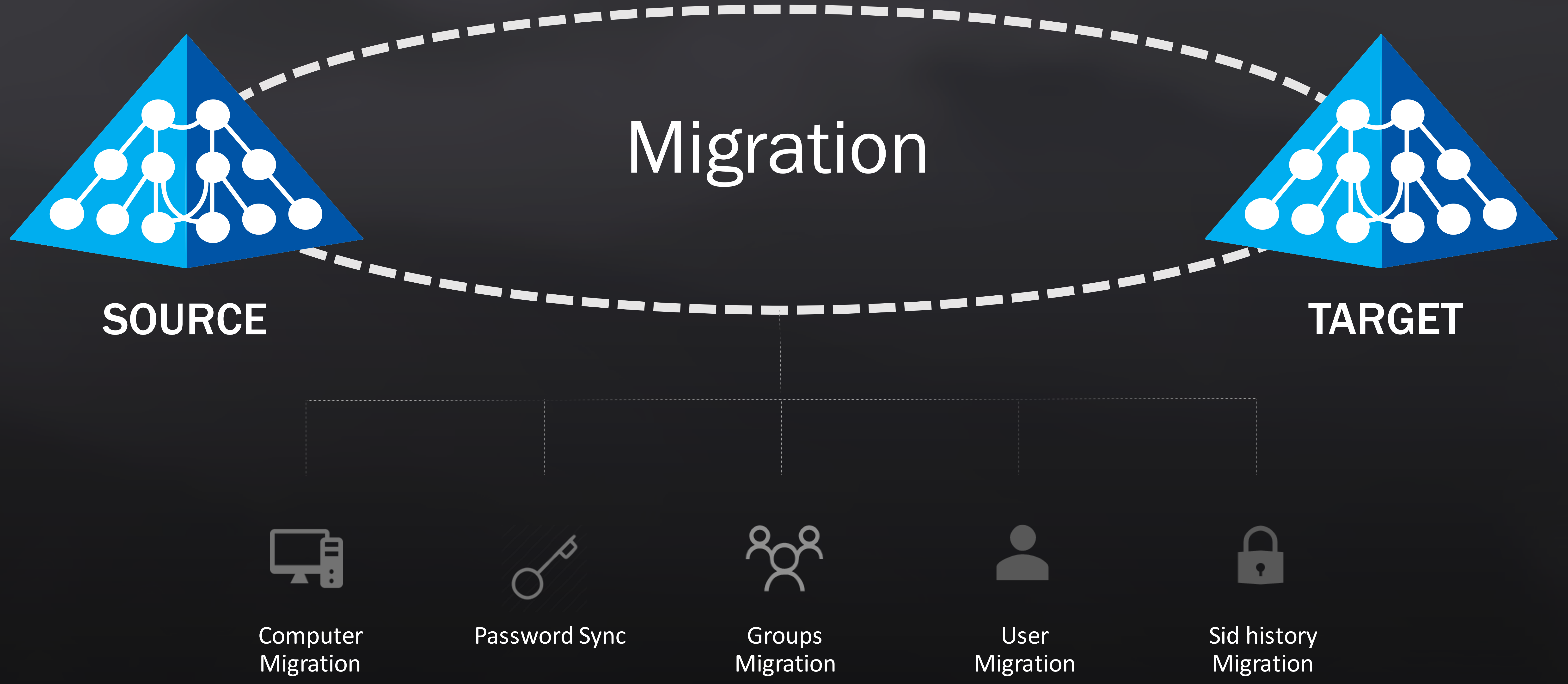


Split a Forest into Two Separate Forests



Move a Forest into a New Forest

Active Directory Migration – Objects to consider



Migration

SOURCE

TARGET

Computer Migration

Password Sync

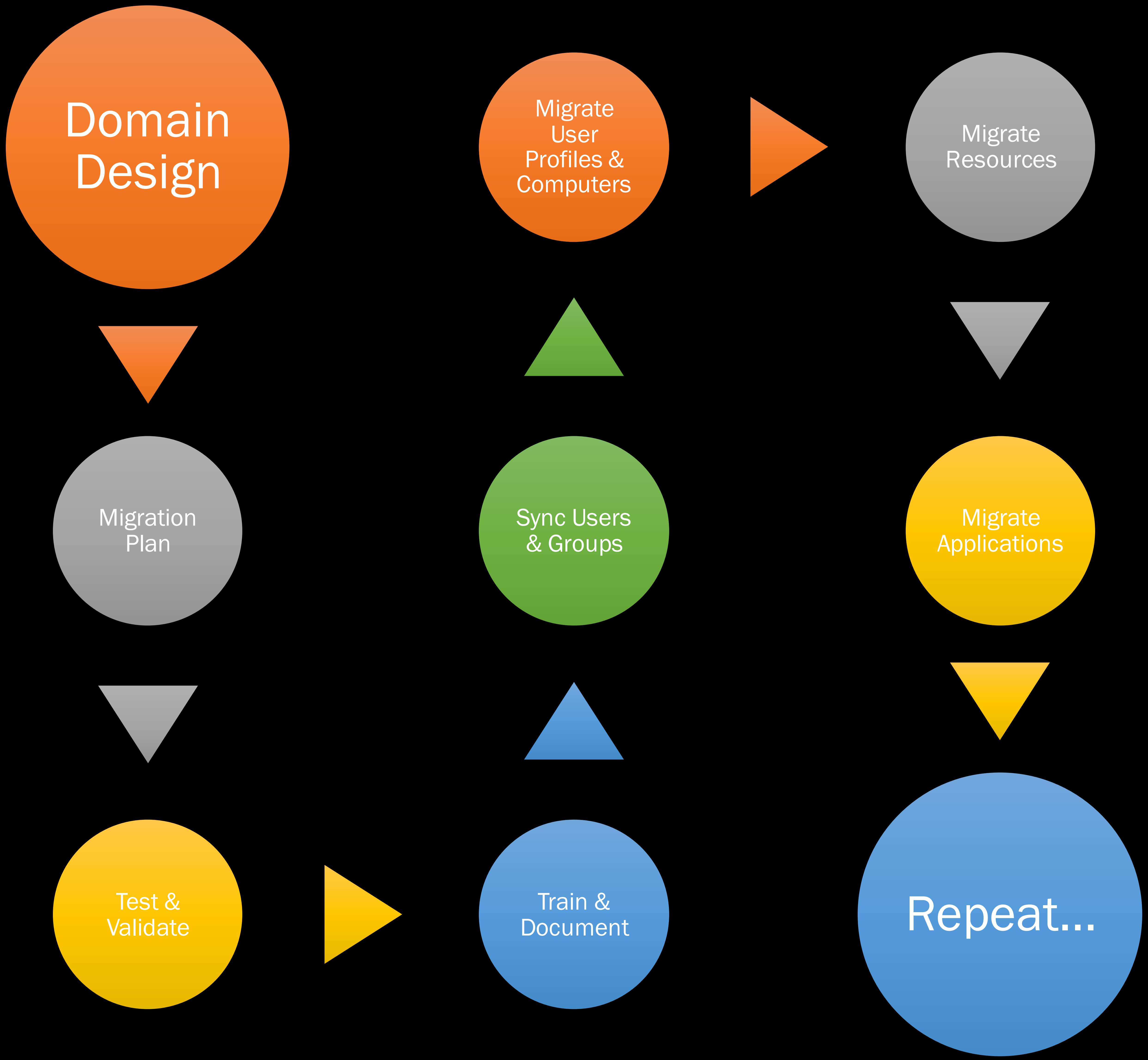
Groups Migration

User Migration

Sid history Migration

semperis

Migration Steps



semperis

Why is AD modernization such a security priority?

In a word, cyberattacks.

When organizations look at the cybersecurity risk matrix, Active Directory is right up there in red.

Security is the single most compelling reason to migrate to a pristine AD forest or perform an AD forest or domain consolidation.

- **AD-based attacks:** AD is exploited in 9 out of 10 attacks, so modernization is urgently needed
- **Technical debt:** Attackers bank on AD vulnerabilities caused by years of configuration drift
- **Unmanageable risk:** Multi-forest environments multiply risk, as one breached forest can lead to a complete compromise through trust abuse
- **Attack surface reduction:** AD modernization is the surest way to dramatically reduce your attack surface

semperis

AD Migration Risks

semperis

Legacy Migration Risks

All migrations are different, but they all share the same challenges.

One rule: “DON’T IMPACT THE BUSINESS !”

To minimize risk and streamline migration, security is usually overlooked. Security is also mostly considered in the target environment, not in the source.

- Planning
- Non-compliance
- Data loss
- Downtime
- Complexity

semperis

CASE STUDY

Migration Risks

➔ Enabling risky features

➔ Breaking production

➔ Migrating privileged accounts as is

➔ Dealing with duplicates

- **Problem:** How do I maintain permissions on legacy apps/shares during migration ?
- **Risk:** Enabling SIDHistory – Allowing attackers to abuse it (*because you will NEVER clean it after migration*)

- **Problem:** How do I safely test a migration between Forest A and Forest B ?
- **Risk:** Testing in production – Very bad habit, you might break something

- **Problem:** How do I manage privileged accounts during the migration ?
- **Risk:** Migrating as-is – Extending your attack surface

- **Problem:** How do I deal with duplicates and potential sync or migration errors ?
- **Risk:** Errors happen – You need a safety net !

« A Challenger Appears ! »

semperis

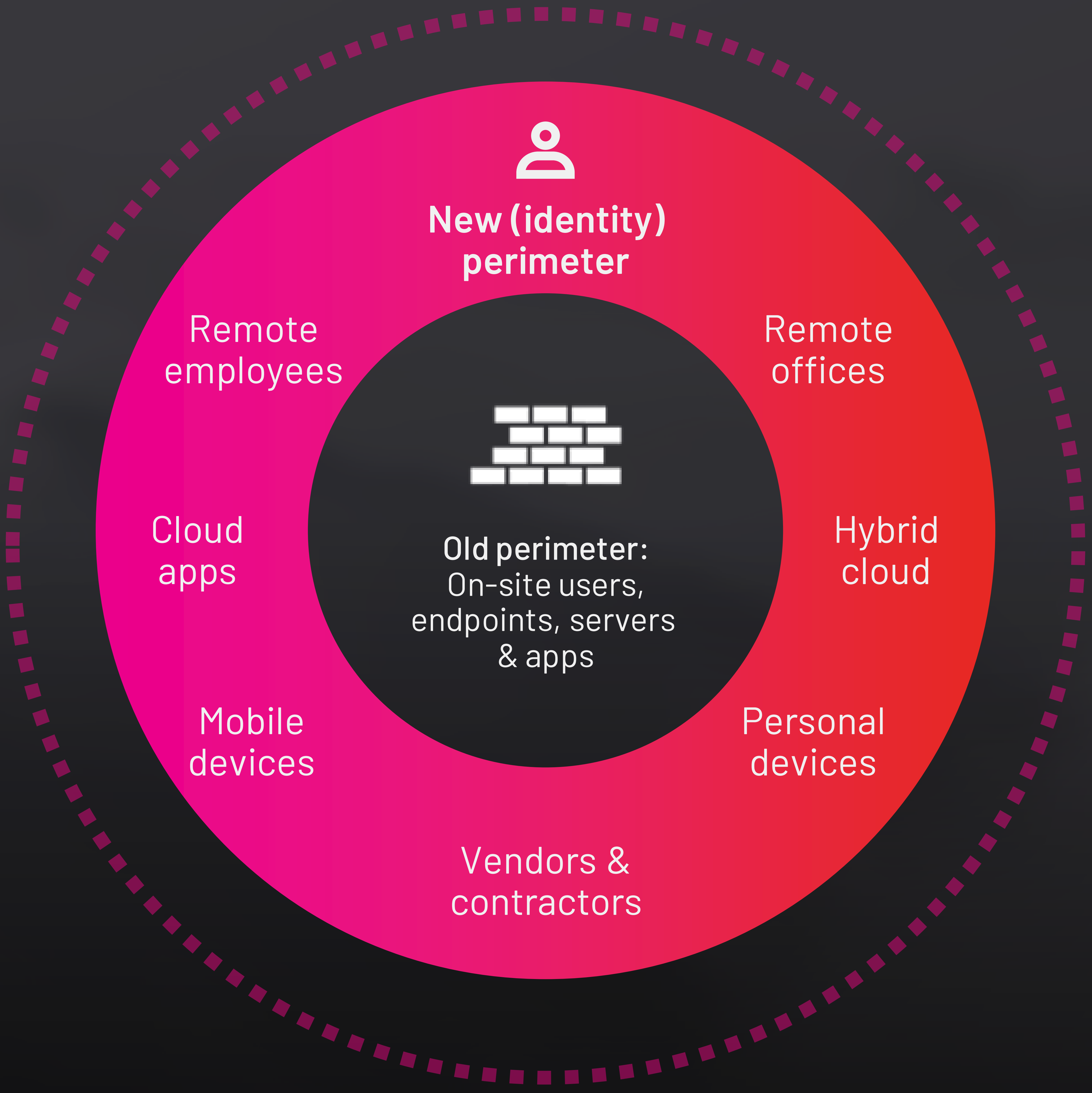
SECURITY CHALLENGES

Protect the shifting & expanding enterprise

1 Keep legacy environments secure

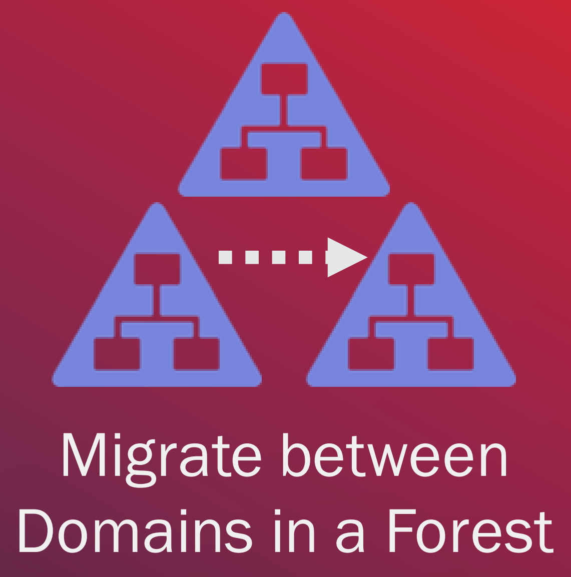
2 Enable digital transformation

3 Security consolidation & automation

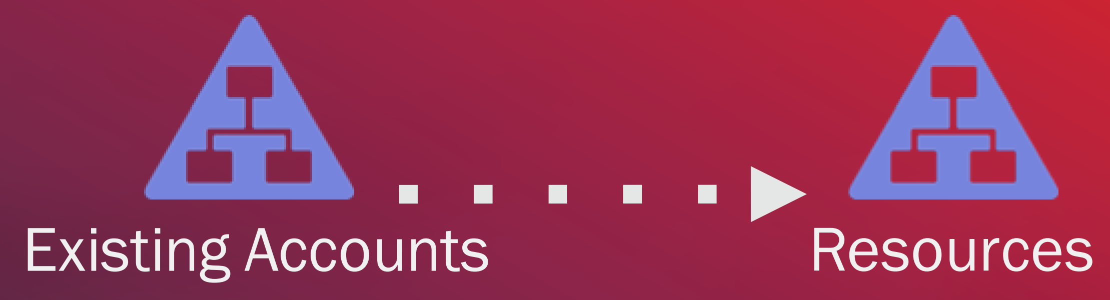


semperis

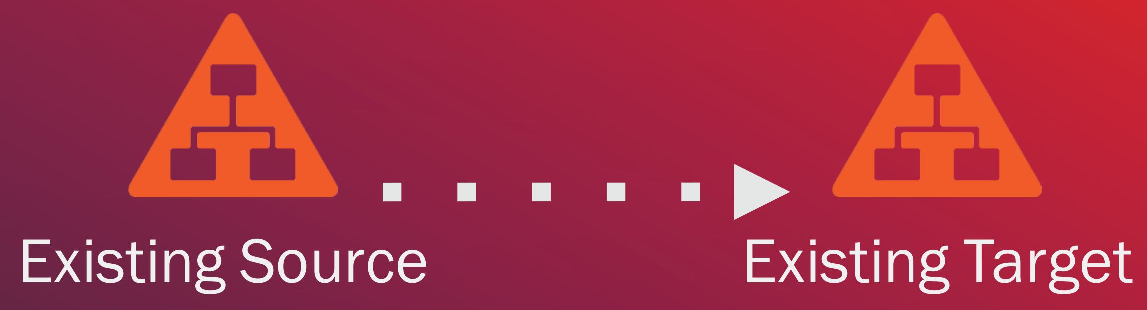
Types of Active Directory Migrations



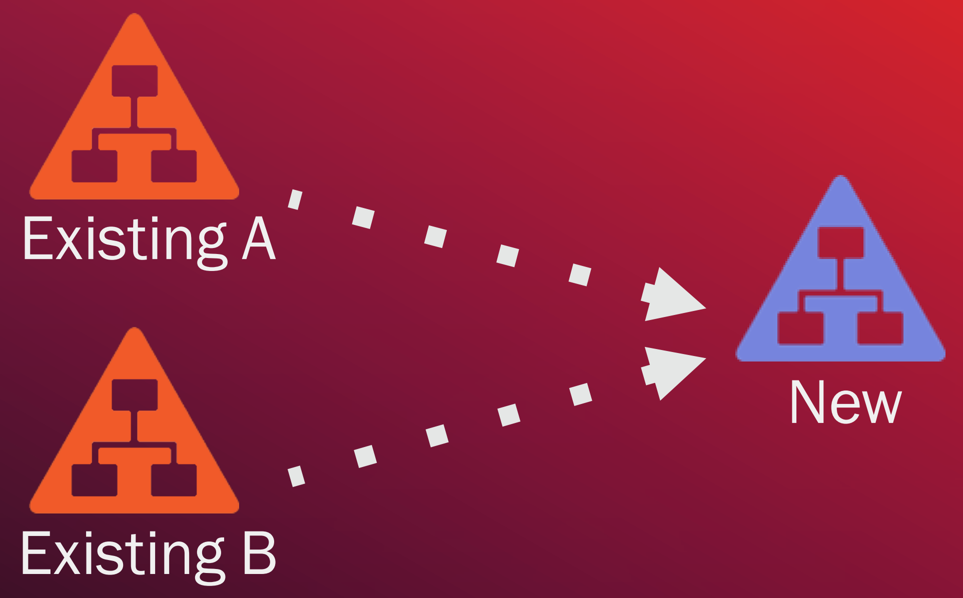
Intra-Forest Migration between Domains in the Same Forest



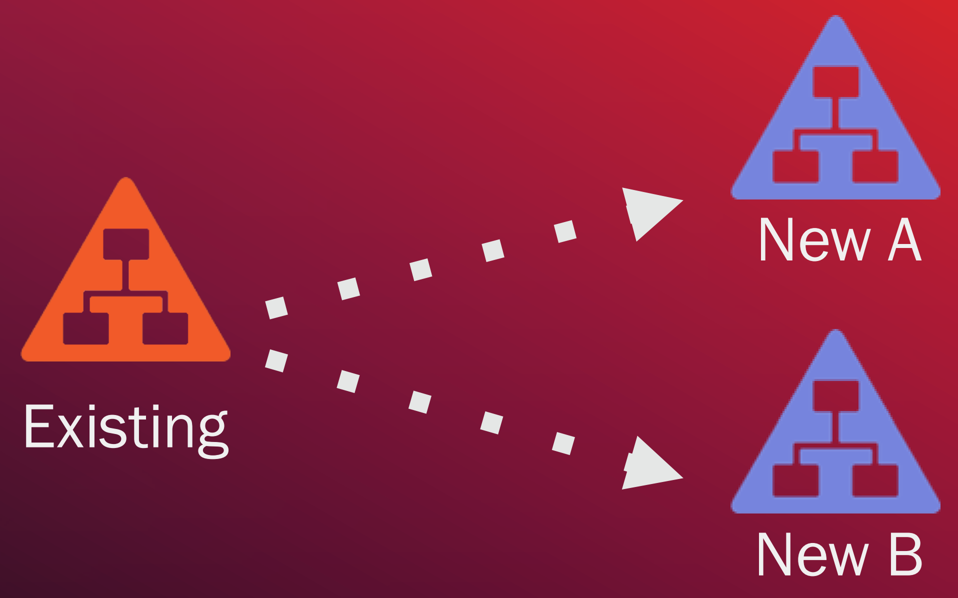
Separate a Forest into Accounts & Resources Forests



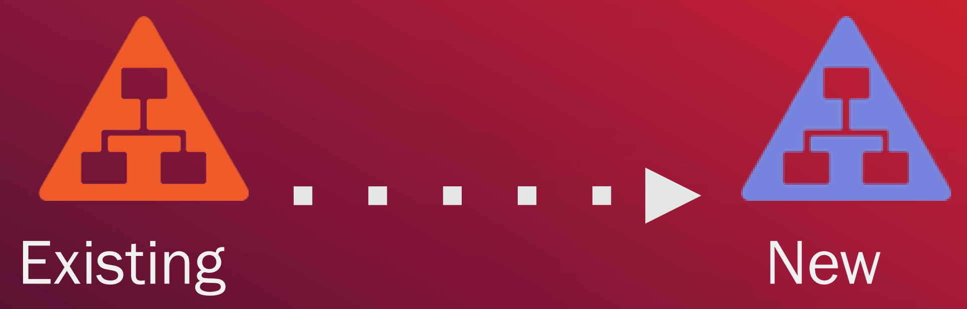
Merge a Forest into Another Existing Forest



Merge Two Forests into a New Forest



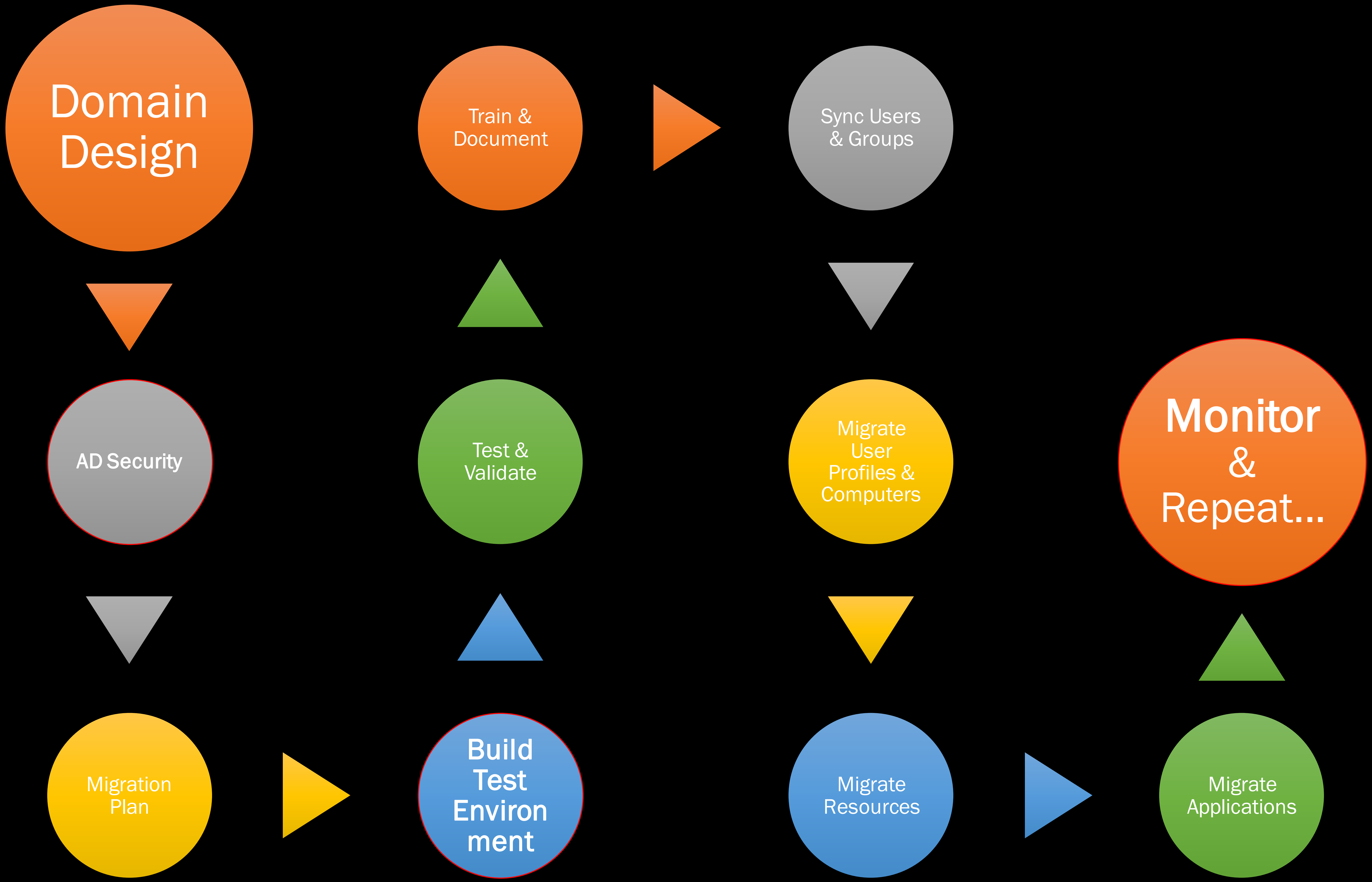
Split a Forest into Two Separate Forests



Move a Forest into a New Forest

semperis

Migration Steps



Domain Design

AD Security

Migration Plan

Build Test Environ ment

Test & Validate

Train & Document

Sync Users & Groups

Migrate User Profiles & Computers

Migrate Resources

Migrate Applications

Monitor & Repeat…

semperis

How Semperis can help ?

semperis

ABOUT SEMPERIS

Foundational identity security

Identity-driven cyber resilience and threat mitigation for hybrid and multi-cloud environments

Gartner peerinsights™

5.0 ★★★★★

TOP 5 FASTEST-GROWING CYBERSECURITY COMPANIES

Technology Fast 500 2023 NORTH AMERICA Deloitte.

3 YEARS IN A ROW OF DOUBLE-DIGIT GROWTH

NAMED TO FORTUNE'S CYBER 60 2024 LIST

Inc. Best Workplaces 2023

2 CONSECUTIVE YEARS ON THE LIST

#14 ON DUN'S 100 2022 RANKING OF BEST STARTUPS

150+ COMBINED YEARS OF MICROSOFT MVP EXPERIENCE

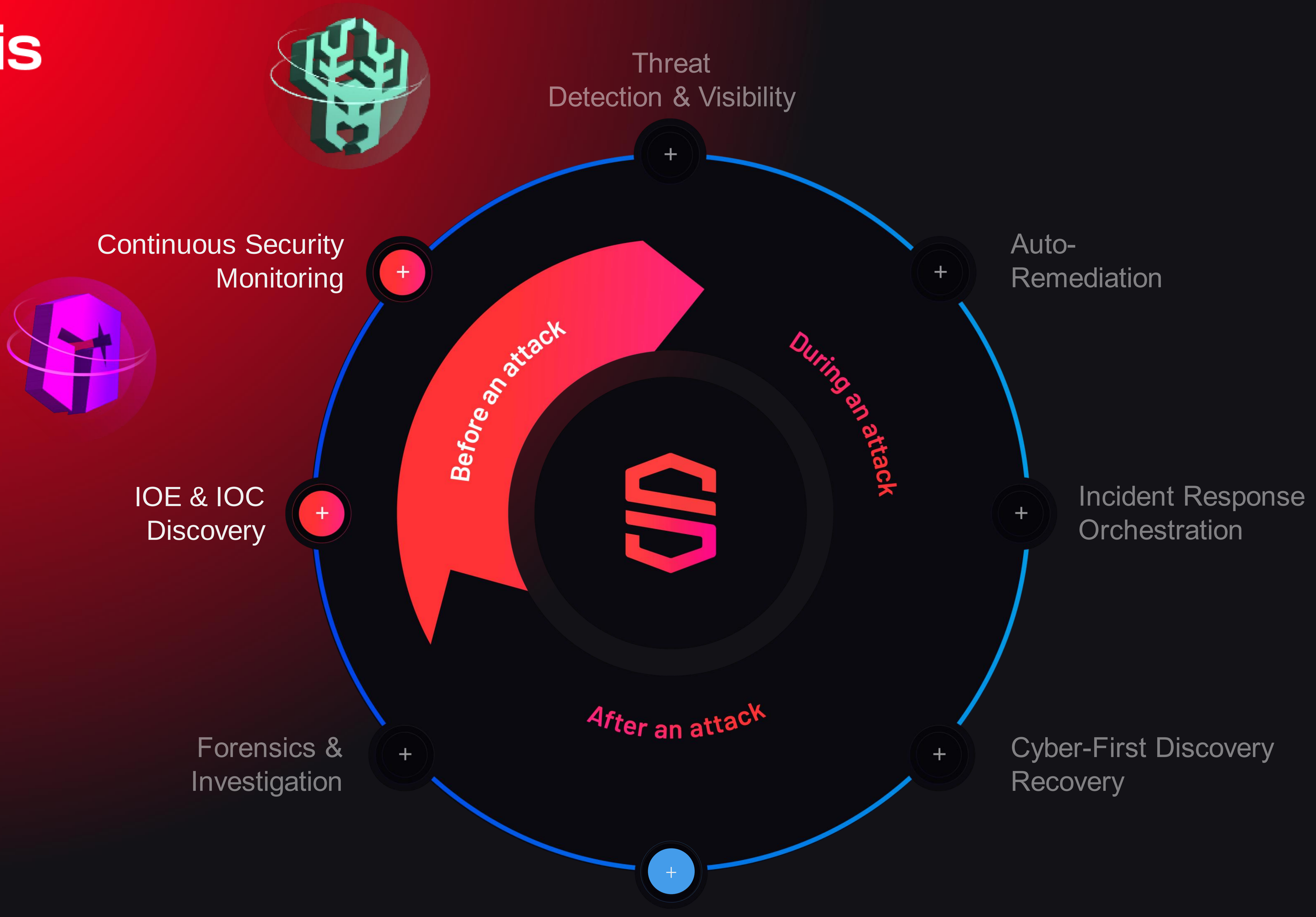
EY Entrepreneur Of The Year® 2023 Award Winner

EY HONORS SEMPERIS CEO MICKEY BRESMAN

TOP 10 OF US 100 FASTEST-GROWING VETERAN-OWNED BUSINESSES

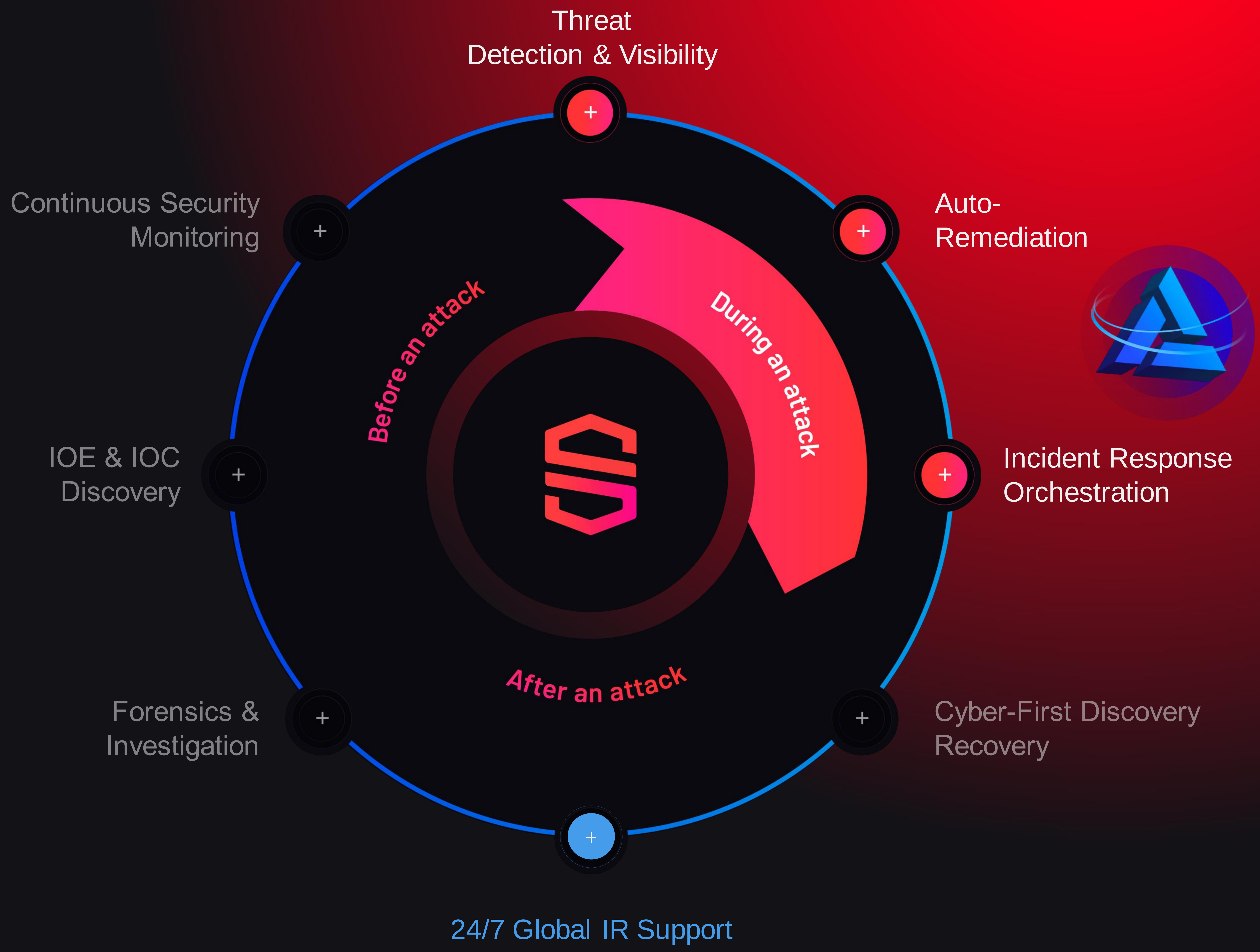
semperis

PRE
attack

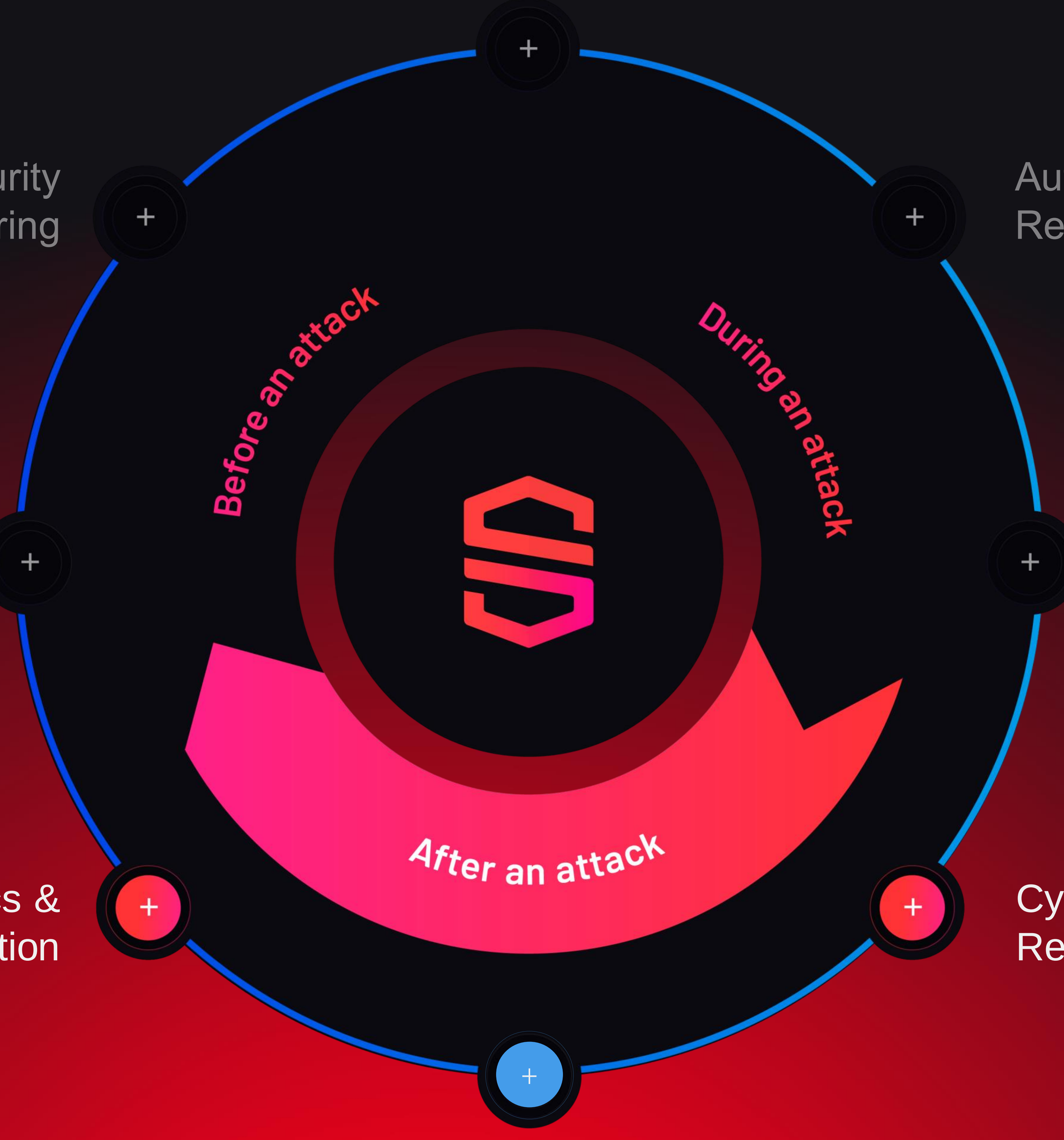


24/7 Global IR Support

DURING attack



POST attack



Threat Detection & Visibility

Auto-Remediation

Incident Response Orchestration

Cyber-First Discovery Recovery

24/7 Global IR Support

Forensics & Investigation

IOE & IOC Discovery

Continuous Security Monitoring

Introducting Semperis MAD

semperis

AD MIGRATION & CONSOLIDATION

Security-centric approach to AD migration and consolidation

Prioritize security pre, during, and post migration

Pre migration

- Find and fix existing security vulnerabilities with Purple Knight
- Map privileged accounts with Forest Druid and apply appropriate security policies
- Conduct cyber-first backup of AD forest with Active Directory Forest Recovery (ADFR) to ensure recovery in case of attack or migration mishaps

During migration

- Use ADFR to clone source and destination environments for lab testing
- Gain migration process visibility with Directory Services Protector (DSP)
- Synchronize directories and migrate objects with Semperis Migrator

Post migration

- Remove SID History, retire old domains and similar, while benefiting from a safety net with DSP and ADFR
- Continuously monitor new environment with DSP to track and roll back malicious changes
- Use ADFR to ensure the ability to automatically recover the entire AD

semperis

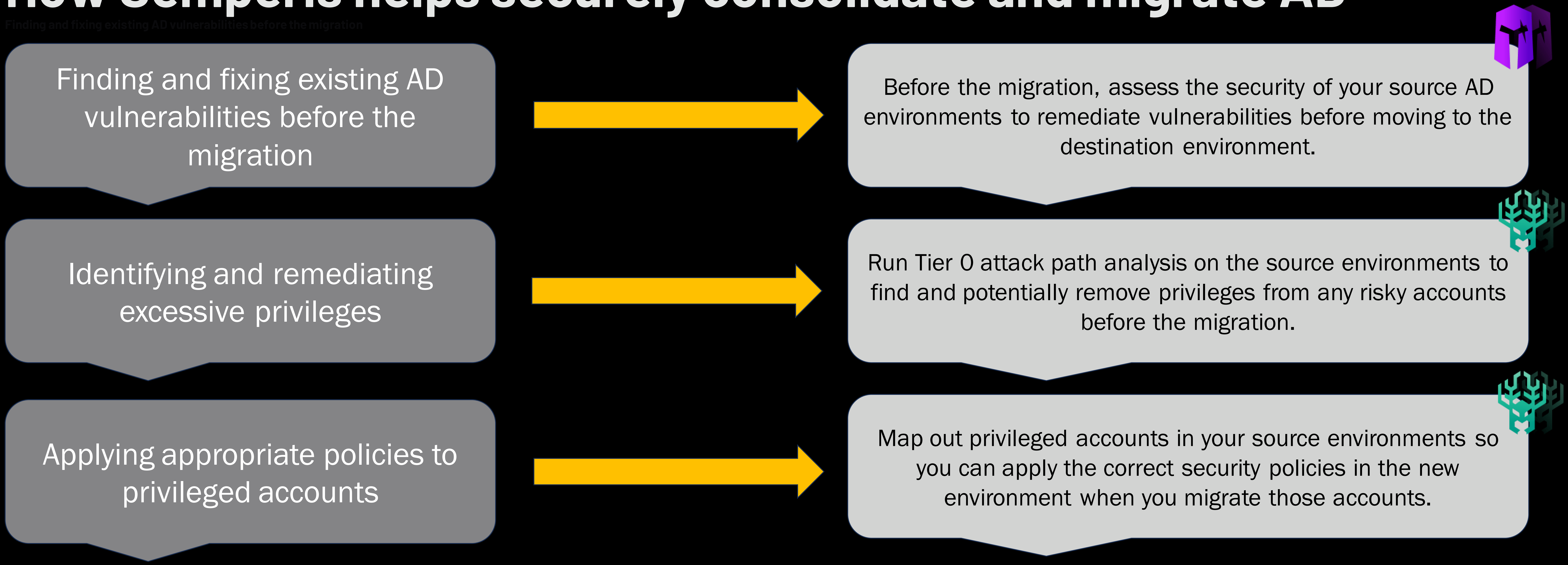
Semperis Migrator for Active Directory

- ✓ Security-Centric Solution & Methodology
- ✓ Powerful Synchronization Engine
- ✓ Secure automated agent deployment
- ✓ End-user Portal for ad hoc requests
- ✓ Centralized discovery and reporting
- ✓ Integration with other Semperis solutions

semperis

How Semperis helps securely consolidate and migrate AD

Finding and fixing existing AD vulnerabilities before the migration



Finding and fixing existing AD vulnerabilities before the migration

Before the migration, assess the security of your source AD environments to remediate vulnerabilities before moving to the destination environment.

Identifying and remediating excessive privileges

Run Tier 0 attack path analysis on the source environments to find and potentially remove privileges from any risky accounts before the migration.

Applying appropriate policies to privileged accounts

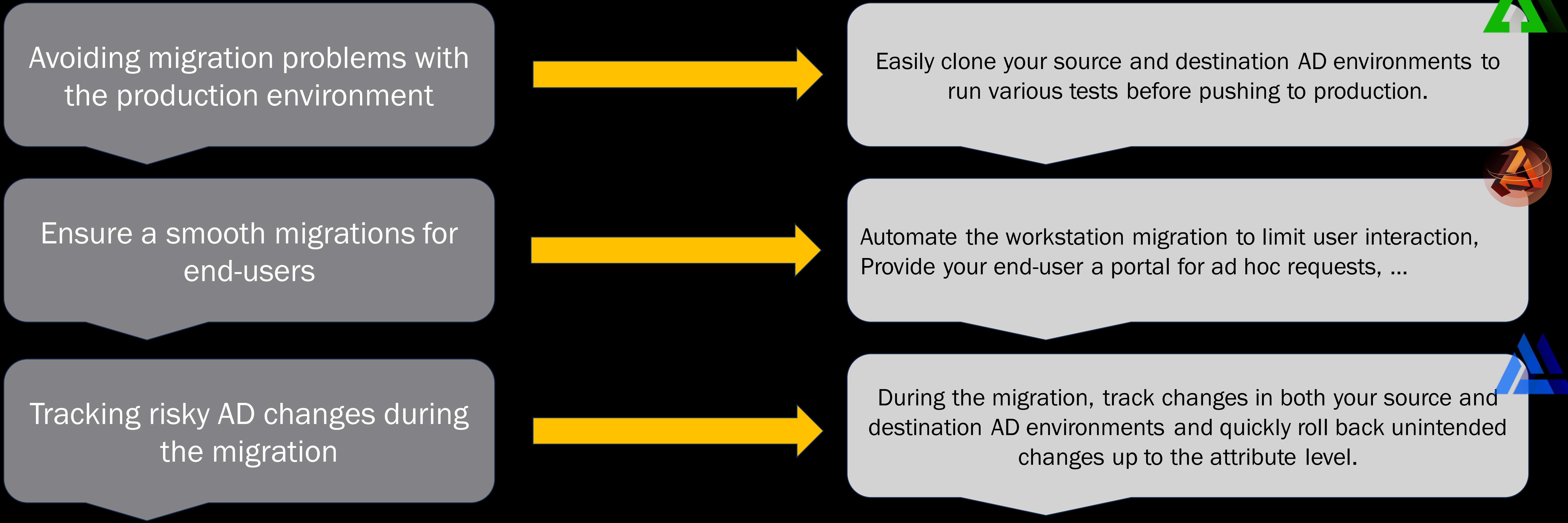
Map out privileged accounts in your source environments so you can apply the correct security policies in the new environment when you migrate those accounts.

https://www.semperis.com/solutions/active-directory-migration-consolidation/

semperis

How Semperis helps securely consolidate and migrate AD

Finding and fixing existing AD vulnerabilities before the migration



Avoiding migration problems with the production environment

Easily clone your source and destination AD environments to run various tests before pushing to production.

Ensure a smooth migrations for end-users

Automate the workstation migration to limit user interaction, Provide your end-user a portal for ad hoc requests, …

Tracking risky AD changes during the migration

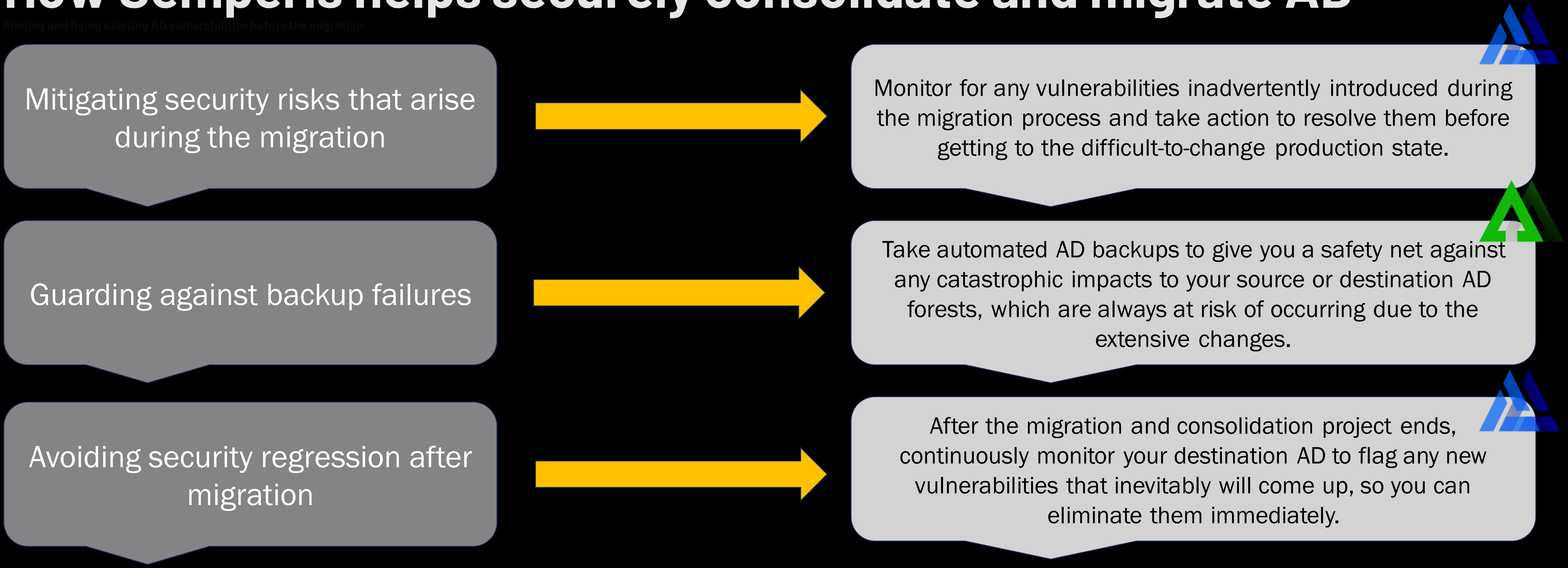
During the migration, track changes in both your source and destination AD environments and quickly roll back unintended changes up to the attribute level.

https://www.semperis.com/solutions/active-directory-migration-consolidation/

semperis

How Semperis helps securely consolidate and migrate AD

Finding and fixing existing AD vulnerabilities before the migration



Mitigating security risks that arise during the migration → Monitor for any vulnerabilities inadvertently introduced during the migration process and take action to resolve them before getting to the difficult-to-change production state.

Guarding against backup failures → Take automated AD backups to give you a safety net against any catastrophic impacts to your source or destination AD forests, which are always at risk of occurring due to the extensive changes.

Avoiding security regression after migration → After the migration and consolidation project ends, continuously monitor your destination AD to flag any new vulnerabilities that inevitably will come up, so you can eliminate them immediately.

https://www.semperis.com/solutions/active-directory-migration-consolidation/

semperis

Thanks for attending !

Questions ?