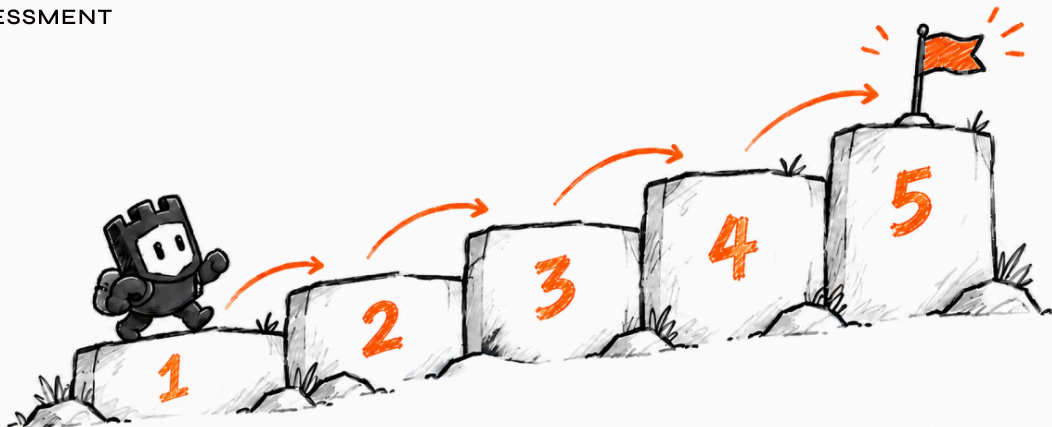




Active Directory security maturity self-assessment

Evaluate where your organization stands across five maturity levels, then work through the processes, KPIs and management decisions that move you up.

A. Maturity methodology

This methodology is based on CMMI, with each step adapted to the specifics of Active Directory. CMMI is a brand of Carnegie Mellon University and is used in this document as a reference for the five maturity steps.



1. Initial

KNOW YOUR BACKYARD

This step is the scope. Defining scope is easy for most projects, but it is a challenge from a security perspective: an Active Directory security project starts without knowing all the ADs in the enterprise scope, and some may have relationships with ADs outside the company's scope.

2. Repeatable

PERFORM SECURITY CONTROLS PERIODICALLY

This step ensures that a consistent set of actions is performed. There is no written documentation yet, but basic vulnerabilities are checked.

3. Defined

PROVE TO MANAGEMENT AND AUDITORS YOU ARE DOING SOMETHING

This step documents the processes already in place. For Active Directory, this means that a process to detect attackers (monitoring) exists and that vulnerabilities are limited by a hardening project. Detection and hardening rules are written in an auditable document.

4. Managed

FOLLOW THE EFFECTIVENESS OF YOUR CONTROLS

KPIs are produced and checked in this step, which confirms the effectiveness of the processes in place.

5. Optimizing

BE AT THE TAIL OF HACKERS

Continuous improvement is in place. New attacks are mitigated quickly and threat hunting is established.

B. Self-evaluation

The goal of this self-assessment is to evaluate your security maturity relative to your peers. Answer each question with yes or no, based on your current capabilities and practices.

1. Initial

- Are all Active Directories known and assigned to an owner accountable for their security?
- Have all trusts with third parties and external companies been removed, or has the associated risk been mitigated through formal risk acceptance?

2. Repeatable

- Do processes exist to regularly check that the basics are in place (provisioning and deletion, privileged account management, AD interconnection, known vulnerabilities)?
- Has the risk of cross-domain contamination been evaluated (SID Filtering enforced everywhere except when a migration is in progress)?

3. Defined

BASIC MONITORING

- Does the addition of a new administrator raise an alert?
- Is there a log of all actions related to AD configuration changes (GPO, group membership)?

BASIC HARDENING

- Does each administrator have a specific account, separate from their day-to-day account, for admin activities?
- Is a limit on the number of administrators enforced on a forest basis, and have administrators signed a charter defining their responsibilities?

4. Managed

EFFECTIVE MONITORING AND FORENSICS

- Does a process exist to handle monitoring alerts in an acceptable time frame?
- Are login logs collected so you can find which computer a user logged on to, and vice versa?

PREVENTING SOME ATTACKS

- Is there enforcement prohibiting a domain administrator account from logging on to workstations?
- Do you have a bastion, or require domain administrators to use two-factor authentication (for example PIV or GIDS smart cards)?
- Are old protocols (NTLMv1, LM, null session, SMBv1, ...) disabled, including on domain controllers?

5. Optimizing

- Do you have a watch process for new attacks?

HUNTING

- Is a process in place to check for Active Directory compromise (backdoors)?
- Can persistence or cross-domain moves (Golden Ticket, DCSync) be detected?

C. Improve your maturity level

1. Initial

Processes to follow on this step: 1.1 Domain coverage, 1.2 Ownership, 1.3 External trusts.

1.1 Domain coverage

DO YOU ACTUALLY KNOW HOW MANY DOMAINS YOU HAVE IN YOUR ACTIVE DIRECTORY?

Domain coverage is the first and foremost step in securing your Active Directory. It ensures that the whole perimeter of the company is covered and that there are no hidden domains. This section gives insight into the current status of the tool's deployment across your perimeter through relevant objectives and KPIs.

If you identify a domain monitored by PingCastle that is out of your scope (an external company, for instance), we recommend that you:

- Remove all the trusts
- Scan the domain where the trust was detected
- Classify the domain as out of scope

You can also remove a domain completely. Scan the domain again after removal and set it as "removed".

KPI to follow	Objective
Percentage of domains audited	80% or more
Number of domains not audited	0
Number of PingCastle versions	3 or fewer
PingCastle reports over 1 month old	0

INDICATORS TO COLLECT

- Status of the domains (not audited, in exception, audited > 6 months, audited > 1 month and < 6 months, audited > 1 week and < 1 month, audited < 1 week)
- PingCastle versions deployed

1.2 Ownership

ARE YOU SURE THAT ALL YOUR DOMAINS ARE ACTUALLY MONITORED BY SOMEONE?

Once you have a clear view of your whole perimeter, define clearly the ownership of every domain. Each domain must be assigned to an owner entity accountable for its security. Security only improves when people feel included in the process.

A few points about ownership:

- When a domain is added in PingCastle, it is often Ownerless, Auto-Created, or both. This must be temporary.
- A domain can be put in exception, meaning its score does not impact the global score. This feature is exceptional.
- Ensure that the functional levels in use are still supported, both by PingCastle and by Microsoft.

KPI to follow	Objective
Number of ownerless domains	0
Number of auto-created domains	0
Percentage of domains in exception	Less than 20%
Number of domains with an unsupported functional level	0

INDICATORS TO COLLECT

- Status of the domains (auto-created, in exception, active, out of scope, removed)
- Functional level of the Active Directory domains

1.3 External trusts

ARE YOU AWARE THAT YOUR DOMAINS ARE EXPOSED ON THE INTERNET WITHOUT PROTECTION?

Trust types

To out-of-scope domains	Between one of your domains and a domain not managed by you. This trust should be removed.
To removed domains	Between one of your domains and a removed domain. This trust should be removed.
To unsafe domains	Between one of your domains and a domain not monitored by PingCastle. Remove the trust or add the unmanaged domain to PingCastle.

To auto-created domains	Between one of your domains and an auto-created domain. The auto-created domain should be reviewed.
Other	Between domains without particular attention points.

With the perimeter under control, the goal is to reduce its exposure on the Internet. Trusts toward uncontrolled domains can create major security risks, and external trusts are often overlooked even though they are one of the main entry points for elaborate, targeted attacks.

This section aims to reduce as much as possible the number of external trusts that are neither controlled nor secured:

- Trusts to domains without clearly identified ownership
- Trusts to domains that are out of your scope
- Trusts to domains that have been removed
- Trusts to domains neither protected nor monitored

If you remove a trust, scan all domains again so that PingCastle registers the removal.

KPI to follow	Objective
Number of trusts to auto-created domains	o
Number of trusts to out-of-scope domains	o
Number of trusts to removed domains	o
Number of trusts to unsafe domains	o

INDICATORS TO COLLECT

- Trusts
- Status of trusted domains

MANAGEMENT DECISIONS

- Run PingCastle and build the domain cartography.
- Configure PingCastle reporting by assigning each domain to its owner.
- Prepare the removal of trusts with unknown third parties.

2. Repeatable

Processes to follow on this step: 2.1 Internal trusts, 2.2 Lower the risk score.

2.1 Internal trusts

DO YOU REALIZE THAT BADLY IMPLEMENTED TRUSTS CREATE A MAJOR RISK OF CROSS-CONTAMINATION?

Now that the perimeter is under control and all trusts are identified, secure them properly. Once a domain is compromised it can be used to compromise others, so internal protections must be well enforced. Every unprotected interconnection between domains is a risk of cross-contamination in case of a breach.

This section covers two main points:

- Internal trusts that do not follow basic security rules
- Migrations between domains that are ongoing or unfinished

If you remove a trust, scan all domains again so that PingCastle registers the removal.

KPI to follow	Objective
Number of trusts in critical status (trust score = 100)	0
Number of trusts without protection (no SID Filtering)	0
Number of trusts in migration (declared in the risk register)	10% or less
Number of unfinished migrations (presence of SID History)	0

INDICATORS TO COLLECT

- Activation status of SID Filtering
- Register of migrations in progress
- Absence of SIDHistory, proving completion of a migration

2.2 Lower the risk score

ARE YOU AWARE OF ALL THE POSSIBLE SECURITY ISSUES IN YOUR ACTIVE DIRECTORY?

This step focuses on the global risk of an AD. The global score represents the level of risk, and the long-term objective is to lower it, step by step, starting with the highest scores. It goes further in the security assessment of your Active Directory.

The score is the maximum of four sub-processes, each calculated automatically by PingCastle from many technical rules:

- Stale objects
- Privileged accounts
- Trusts
- Anomalies

The maximum is computed per report, not as the maximum of the sub-process averages.

KPI to follow	Objective
Number of domains with critical risk (score = 100)	o
Number of domains with high risk (score ≥ 75 and < 100)	o
Number of domains with medium risk (score ≥ 50 and < 75)	o
Number of domains with low risk (score ≥ 25 and < 50)	o

INDICATORS TO COLLECT

- Risk score of all Active Directory domains

MANAGEMENT DECISIONS

- Run PingCastle on each domain weekly to detect new trusts quickly, and report deployment and score evolution to management.
- Involve all owners in putting SID Filtering in place, except for time-limited migrations. Configure these migrations in the PingCastle reporting configuration to follow them.

Next steps turn visibility into action and move from periodic assessment to a living control system: assess, audit, manage, safeguard, protect, recover, then repeat.

This is where PingCastle hands off to the rest of the [Netwrix Directory Security portfolio](#)⁷. When you're ready to move from periodic assessment to continuous protection, Netwrix extends the same maturity model into continuous monitoring, automated directory management, least-privilege access, detection, and recovery, on-premises and in Entra ID.

3. Defined

MONITORING

- Collect critical changes in AD and Entra ID, such as configuration, GPOs, changes and membership events, so you can investigate promptly.
- Configure alerts for important changes such as administrators group membership changes.

Indicators: number of critical change types collected, number of alerts configured, percentage of sensitive assets covered by alerting.

4. Managed

AUTOMATING DIRECTORY MANAGEMENT

- Automate joiner, mover, and leaver processes, a common source of drift. Accounts are created late or with the wrong rights, group memberships pile up as people change roles, and leavers keep access longer than they should. Netwrix Directory Manager provisions, updates, and deprovisions accounts from HR or other authoritative sources across AD and Entra ID.
- Keep group memberships current with rule-based Smart Groups, and expire and attest groups so stale access does not build up between audits. This lowers PingCastle's stale objects findings over time.
- Use workflow-based delegation so managers, group owners, and the helpdesk can handle routine changes without native directory rights. This shrinks the admin population PingCastle flags under privileged accounts, and frees IT operations to work through the issues PingCastle reports.

ENFORCING LEAST PRIVILEGE

- Remove standing admin rights and give elevated access only for the task at hand. Standing admin accounts are valuable to attackers because they stay usable whether or not anyone needs them.
- Record privileged sessions so you can show who did what. This shrinks the pool of accounts an attacker can abuse and gives auditors evidence of how privileged access was used.

Indicators: number of stale objects, percentage of joiner/mover/leaver changes handled automatically, number of standing privileged accounts, percentage of privileged sessions recorded.

5. Optimizing

REAL TIME THREAT DETECTION AND RESPONSE

- Detect and respond to AD and Entra ID attacks, such as DCSync, Golden Ticket, and other techniques attackers use to compromise your Active Directory and Entra ID.

RECOVERY

- Be able to recover AD, Entra ID and Okta objects and attributes, or entire AD forests quickly, minimizing downtime and business impact, and test that recovery before you need it.

Indicators: time between a new attack and its mitigation; time to restore AD objects, a domain, or a full forest, measured in regular recovery tests.