CHECKLIST FOR PREPARING YOUR

IDENTITY FABRIC FOR THE AGENTIC ERA

Your identity fabric is ground zero for AI

100:1 Ratio of non-human identities to human identities in 2026

99% Of non-human identities (NHIs) are over-permissioned

80% Of workload identities are unused but still retain access

The stakes are high: 74% of organizations believe AI will increase attacks on identity infrastructure, yet only 32% are confident they could fully regain control after an AI-related breach.

Report:
The State of Identity Security in the AI Era

AI is the stuff of productivity dreams—and security nightmares. Your business leaders are racing to adopt generative and agentic AI to move faster and unlock new efficiencies, as they should: The benefits are real today and will only grow.

But to do its work, AI still needs to log on. Identity is the last perimeter standing, even (or especially) in the agentic age.

Agents will discover credentials, exploit excess permissions, and propagate attacks at machine speed. As your business bets more on agents, it bets more on your identity fabric—because if identity fails, so do the agents and every process they support.

How can you unlock the productivity benefits of agentic AI while preventing rogue agents from instigating a cyber disaster? Use this checklist to get your identity fabric ready for the agentic era—before, during, and after an attack.

Before the attack: Harden and reduce your attack surface

Attacks are ongoing, so hardening is continuous—and it's more urgent now that weaponized AI can find and exploit your security debt faster than ever.

- **Assess your entire hybrid identity posture.** Look across every IdP, including AD, Entra ID, Okta, and Ping for AI agents that use credentials. Nearly every organization runs a mix of IdPs, and attackers exploit the seams between them.
- **Kill standing access: Move to just-in-time, just-enough.** Permissions only accumulate—Bob keeps his accounting rights, then adds finance, then IT—until standing access sprawls across the org. Rigorously apply least-privilege, just-enough, just-in-time access, with approvals and reviews, to agents, users, and the resources they consume.
- **Lock down Tier 0.** The dangerous attack paths often aren't obvious, such as an admin group nested inside a group Bob belongs to, or an HR attribute that silently grants access. Understand which permissions can reach Tier 0 directly or through indirect attack paths or shadow access.
- **Clean up non-human accounts (NHIs) and service accounts.** Discover, classify, and right-size the machine identities that agents increasingly run on.
- **Make credentials phishing-resistant.** The single easiest, highest-impact step is passkeys—cryptographic verification tied to a physical device—your best defense against spear phishing and deepfakes.

During the attack: Detect and disrupt at machine speed

Identity-based attacks rose 32% in just the first half of 2025. They're background noise now, not exceptional events. Attackers move at AI speed, so your defense has to accelerate, too.

- **Track every critical change continuously.** The first change an attacker (or rogue agent) makes is the one you want to see, and undo.
- **Automate rollback, then page a human.** Don't just fire an alert: Auto-revert the suspicious change and then ask the human whether they meant to do it. Your security doesn't have to be perfect. It just has to be fast enough that attackers move on.
- **Set hard boundaries for agents.** Enforce no standing privilege, no shared secrets, and no agents acting as humans. Insist on scoped, just-in-time, ticket-bound access that expires.
- **Use human "dual-key" approval for Tier 0.** Agents can be socially engineered too, so pair AI assistance with human sign-off on your most sensitive systems.

After the attack: Recover cleanly—and plan to fail

An identity outage is a business outage. When attackers control the identity ecosystem and you don't, they can compromise anything and you can't even log in to fix it. That's an extinction-level event.

- **Keep dedicated, immutable, identity-specific backups.** Identity systems aren't just another workload you back up with the VM. They need special tooling so you can bring identity up first in a cleanroom.
- **Recover only the identity layer to a trusted state.** Restore the forest cleanly with forensic insight into what the attacker touched, then rebuild the rest.
- **Don't let recovery depend on the fabric that's down.** The tools you rely on to recover, and the out-of-band communications your team needs, can't run on the same compromised identity infrastructure.
- **Rehearse realistic identity-failure scenarios.** Teams tend to drill only for what they prepared for. Conduct tabletop exercises for the attacks you didn't expect.

> If identity goes down, all your agents do too, along with the business processes they support."
>
> **Alex Weinert**
> Semperis Chief Product Officer

Put AI to work on defense, with eyes open

Agents can be allies. Use them to assess your environment against known risks, simulate attack impact to prioritize fixes, triage anomalies, and accelerate threat hunting. They can even help you build, practice, and improve your crisis response plan. Just remember that agentic AI won't solve resilience for you. Core recovery still relies on deterministic, heavily vetted components. An agent can invoke the cleanroom, but it can't be the cleanroom.

Agentic AI is here, and you need to set strong boundaries. Your identity fabric is what creates and enforces those boundaries. Use these guidelines to strengthen your identity resilience so you can embrace the productivity gains of AI tools while preventing an AI-generated cyber disaster.