Zero Trust Security for Agentic AI

Zero Trust principles are fundamental to enterprise security. So why don't they apply to AI agents?

If agents are the knowledge workers of the future... why do they all have admin access?

Many enterprises look to Zero Trust to provide least-privilege access across their environments. Yet these same organizations grant AI agents broad backend access – essentially giving them the broad privileges that Zero Trust was designed to eliminate.

This exposes a critical gap: How do you apply least-privilege access to AI agents without compromising functionality?

Zentera solves this by enabling AI agents to *inherit access privileges from their human users*, extending Zero Trust principles to the AI layer.

The challenge: excessive AI privileges

Enterprise AI agents require backend access to storage, databases, and tools, creating a security dilemma:

- **Over-privileged agents**: Broad agent access creates massive security risks and potentially exposes sensitive data across the enterprise
- **Under-privileged agents**: Restricted agent access limits their usefulness, defeating the purpose of automation
- **Static permissions**: Fixed permissions can't adapt to when different users interact with the same agent
- **Audit complexity**: Without carrying user context through agent actions, the visibility needed for compliance and forensic analysis is lost

The solution: Zero Trust role inheritance

How it Works

1. Identity Propagation
Users authenticate to the corporate directory (Active Directory, LDAP, or modern identity providers). That identity binds to their enterprise Ai sessions.

2. Dynamic Role Assignment
Agents inherit user roles. A junior analyst's prompt is restricted to the financial docs, while the CEO's prompt can reference operations data.

3. Network-Level Enforcement
CoIP® Platform enforces agent roles at the Virtual Chamber microsegmentation boundary – at the network level, and before any data access occurs.

zentera™

Key Capabilities

Granular Network-Level Access Controls

- Access permissions change dynamically based on who is prompting the agent
- Unified corporate-level control solution for all assets, including next-gen AI systems

Complete Audit Trail

- Every agent action is traceable to the originating user
- Full visibility into what assets were accessed, by which agent, on behalf of which user
- Simplified compliance with regulatory requirements

Seamless Integration

- Works with existing identity management systems
- No changes required to AI agent code or prompts
- Compatible with all major LLM platforms and agent frameworks

Zero Standing Privileges

- Agents have no inherent access rights
- Privileges are granted only for the duration of user interaction
- Automatic privilege revocation when sessions end

Business Benefits

Reduced Risk: Eliminates the attack surface created by over-privileged AI agents

Maintained Productivity: Agents remain fully functional within appropriate access boundaries

Regulatory Compliance: Clear audit trails and role-based access satisfy regulatory requirements

Simplified Management: No need to maintain separate permission models for AI systems

Faster AI Adoption: Security concerns no longer block agentic AI deployment

Architecture Overview

The solution operates through three integrated layers:

Identity: Zentera authenticates users against corporate directories and associates users with roles

AI Agents: Zentera traces user sessions through the AI application

Enforcement: Zentera's Virtual Chambers create dynamic, microsegmented zones that enforce the inherited access rights at the network level, ensuring agents cannot exceed their inherited privileges

Getting Started with Zentera Zero Trust for AI Agents

✓ Deploy Zentera's CoIP Platform

✓ Integrate Zentera with your existing identity provider (SAML2, Oauth 2.0, OpenID Connect)

✓ Protect assets in Virtual Chambers, aligned with your data classification

✓ Deploy Zentera zLink agents to protect your enterprise AI VMs or Kubernetes systems

About Zentera Systems: Zentera provides Zero Trust security solutions for powerful microsegmentation and access control, without infrastructure disruption or application downtime. Contact us at sales@zentera.net.