Silverfort

# Stop AI-powered attacks: Why inline runtime identity controls are the only answer

## What are AI-powered attacks and why do they matter?

AI-powered attacks and Frontier AI models like Anthropic's Mythos are changing cybersecurity faster than most organizations realize.

These models dramatically lower the bar for sophisticated attacks, enabling attackers to execute complex campaigns with unprecedented speed and scale. They allow adversaries to discover Zero Day vulnerabilities, chain together misconfigurations, enumerate identities, move laterally, escalate privileges, and compromise environments—autonomously and at machine speed.

The real shift is not a new attack technique, but the ability to execute complete attack chains continuously and adaptively, without the delays, mistakes, or resource constraints that traditionally limit human operators.

Security teams have spent years building defenses around the assumption that there is meaningful time between attacker actions and defender response. Frontier AI collapses that response window. By the time detection fires, the attack may already be complete.

## Identity is the battlefield

What we saw consistently from customers and Glasswing CISOs is that AI-powered attacks go through identities. They exploit trust relationships, move laterally, and escalate privileges until they own the environment. That's why identity is both the primary attack surface and the last reliable control point.

**Yet most tools can't handle the scale and speed of AI-powered attacks**

**IGA is too static** and was built for governance, not machine-speed attack chains.

**Traditional PAM is too narrow** and secures only a limited set of accounts

**ITDR is too slow and reactive,** operating after suspicious behavior has already begun.

The organizations that stopped these models had one thing in common:

**Runtime Identity Security controls.**

## Why Runtime Identity Security is critical in the Frontier AI era

Identity is the last reliable enforcement point before an action is executed. Once access is granted, the attacker is already operating inside the environment. This is why Runtime Identity Security becomes critical in the age of AI-powered attacks. The only place attacks can reliably be stopped is inline, at the moment an authentication request occurs—*before* access is granted.

- Control happens inline - inside the authentication flow
- Decisions are made before access is granted
- Lateral movement and privilege escalation is stopped in real time

## Silverfort's Runtime Access Protection

Silverfort connects to your IAM infrastructure and agentic platforms, extending identity protection to assets that were previously unprotectable, with no changes to your infrastructure, systems, or apps.

Silverfort achieves this with its patented Runtime Access Protection™ (RAP) technology, which natively integrates with your IAM infrastructure to enforce security controls at runtime and stop threats before they can cause damage.

## What Silverfort delivers

**Inline protection for every identity**
Protect human users, service accounts and other non-human identities, and AI agents with controls enforced inline at authentication.

**Stop AI-speed attacks before they spread**
Block, challenge, restrict, or contain risky access before attackers can move laterally, escalate privileges, or expand blast radius.

**Contain and break the attack chain**
Don't let the model advance. Challenge access based on static credentials, temporarily breaking the trust imposed by other systems.

**Coverage where attackers actually move**
Extend controls to areas most identity tools cannot reach, including Active Directory, Kerberos, NTLM, legacy apps, OT and air-gapped environments.

> "Silverfort is phenomenal. It blocked Mythos' attempts to spread in the network. At some point we had to disable Silverfort's defenses to allow further testing."
>
> Security operations leader, Fortune 50 technology company

## About Silverfort

Silverfort secures every dimension of identity—human, machine, and AI—across cloud and on-prem environments. We are the first to deliver an end-to-end identity security platform that is easy to deploy and doesn't disrupt business operations, resulting in better security outcomes with less work. Discover every identity across every environment, analyze exposures to reduce your attack surface, and enforce security controls at runtime to stop lateral movement, ransomware, and other identity threats.