Silverfort

Mythos and the collapse of identity attack timelines: Why runtime is the only answer

Attack timelines are collapsing and detection can't keep up.
Silverfort enforces Identity Security at runtime, where attacks can still be stopped.

What is Mythos & why it matters

Anthropic's Mythos is a model built for advanced cybersecurity tasks, capable of finding and exploiting vulnerabilities with minimal human involvement. It doesn't introduce new attack methods but instead executes existing ones faster and more efficiently than ever before. That speed shift is what changes the game.

At Silverfort, we already see customers and partners using Mythos and similar AI capabilities in penetration testing with consistent results. The takeaway is clear: when attacks operate at machine speed, traditional detection is too slow to stop them.

To keep up, access controls must operate at the same speed, inline, at runtime.
That means enforcing access controls directly in the authentication flow, as soon as access is requested. If you rely on detection alone, you're already too late.

Detection now lags behind the attack timeline

Increasing automation compresses every stage of the attack lifecycle. AI agents execute full attack chains in one continuous flow, so lateral movement now begins within minutes and full attacks can be completed in hours. No pauses, no delays, no human friction.

Attack timelines are collapsing:*

Breakout time (2025):
34 minutes
(29% faster YoY)

Fastest lateral movement:
4 minutes
(85% faster YoY)

Fastest exfiltration:
6 minutes
(down from 4.5 hours)

Even real-time detections are too slow for action. By the time detection happens and SOC teams can respond, the attack is already in motion.

*ReliaQuest 2026 Annual Cyber Threat Report

Why runtime is the only answer

Detection tells you what happened, but it can't stop the action from happening. Identity Security at runtime is the only way to face the speed of AI-based attacks.

Control happens 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 entire IAM infrastructure and secures it from within. It eliminates the complexity of protecting every identity and extends coverage to assets that were previously unprotectable, including non-human identities (NHIs), legacy systems, command-line tools, and IT/OT infrastructure.
To achieve this, Silverfort leverages its patented Runtime Access Protection™ (RAP) technology, which natively integrates with your entire IAM infrastructure to enforce security controls at runtime—stopping threats before they can cause damage.

What Silverfort delivers

Secure every identity across every environment
Protect all humans, service accounts, NHIs, and AI agents across AD, cloud, and hybrid environments.

Runtime protection at the moment of access
Evaluate behavior and risk to dynamically enforce controls during authentication, *before* access is granted.

Unified visibility with proactive risk reduction
Eliminate blind spots and reduce exposure before attackers or AI models can exploit it.

Real-time dynamic containment
Apply adaptive controls to instantly restrict, isolate, or block suspicious activity as threats emerge.

AI agents execute attacks in real time, faster than humans can react. If you're not protecting at runtime, you're already too late.

Learn more

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.