FACT SHEET

Cybersecurity After Mythos: Contain or Collapse

Why breach containment is the only viable path forward

In early 2026, Anthropic's Claude Mythos Preview AI model autonomously found thousands of critical zero-day vulnerabilities across major operating systems, browsers, and widely used infrastructure — and created working exploits for many of them. In Firefox alone, it turned more than 72% of the flaws it found into working exploits.

This is not a research benchmark. It ran against production code that powers the world's servers, browsers, and firewalls. Many had been deployed for decades without anyone noticing the flaws.

Defenders working in weeks can't keep up with attackers working in seconds.

The consequences are here:

- Exploitation timelines shrink from months to hours or less.
- Patch backlogs, already large, become permanently unmanageable.
- The assumption that "we'll patch it before it's exploited" no longer holds.
- Established operating models can't scale, no matter how hard teams try.

Mythos collapses the time between vulnerability discovery and working exploit to near zero — machine speed, at scale.

What's new for defenders

Mythos may not break existing tooling. But it does break the timing assumptions every security program is built on. Here's what changes:

- Detection, triage, and response still move at human speed. Attackers now compress their timeline while defenders must sort, correlate, and wait for decisions.
- Identity-driven, malware-free attacks make lateral movement appear normal, bypassing signature-based detection.
- Defenders often detect attackers only after lateral movement begins.
- A 30–90 day patch cycle is now an operational risk defenders can no longer ignore. Flaws can be discovered and exploited far more quickly than before.

The questions have changed

Before Mythos, the defining security question was: "Can we find, fix, and block every exploit before attackers use them?" That race is over.

Old question	New question
What's vulnerable?	What is reachable right now?
Is it patched?	What paths exist from a foothold to critical assets?
Did an alert fire?	How big is the blast radius if one control fails?

Security effectiveness is no longer defined by detection speed or patching velocity. It is defined by blast radius - how far an attacker can move once inside.

Mythos changes what attackers can find and how fast they weaponize it. But it doesn't change the physics of an attack:

- A zero-day exploit opens the door.
- The internal environment sets the limits.
- Lateral movement turns a breach into a disaster.

Zero Trust is the way forward

Zero Trust has been discussed for years as best practice. Post-Mythos, it becomes the minimum viable architecture. Illumio makes it operational — not theoretical — across data center, cloud, endpoint, and hybrid environments:

- **Define the core.** Know which assets, identities, and control planes are truly mission-critical.
- **Assume breach.** Design as if an attacker will get a foothold somewhere outside the core.
- **Allow only explicit paths.** Least-privilege, resource-level policy governs who or what may talk to what.
- **Verify continuously**. No implicit trust based on network location, inherited access, or stale context.
- **Isolate fast.** When compromise is suspected, the design limits attackers' reach and accelerates containment.

How Illumio helps

The Illumio Breach Containment Platform is the core security layer for hybrid environments. With real-time visibility and microsegmentation at scale, you can enforce Zero Trust policies at the speed AI demands. With Illumio, you can stop lateral movement, limit access, and reduce exposure — so that an initial compromise never turns into an enterprise-wide disaster.

The platform

The Illumio Breach Containment Platform pairs proactive containment with AI-powered detection — two products that work as one.

Illumio Segmentation

Market-leading microsegmentation to:

- Proactively limit lateral movement
- Reduce exposure
- Shield vulnerable systems from attack
- Protect critical workloads
- Accelerate your Zero Trust strategy

Illumio Insights

Complete AI-powered observability and detection to:

- Identify and secure vulnerable workloads in real time
- Spot and contain threats instantly
- Accelerate microsegmentation
- Continuously strengthen security posture

Key benefits

Single platform, unified control

Deployed in minutes, managed through a centralized console. One platform for end-to-end breach containment.

Flexible and scalable

Adapts seamlessly across hybrid, multi-cloud, on-premises, and OT environments to meet evolving needs.

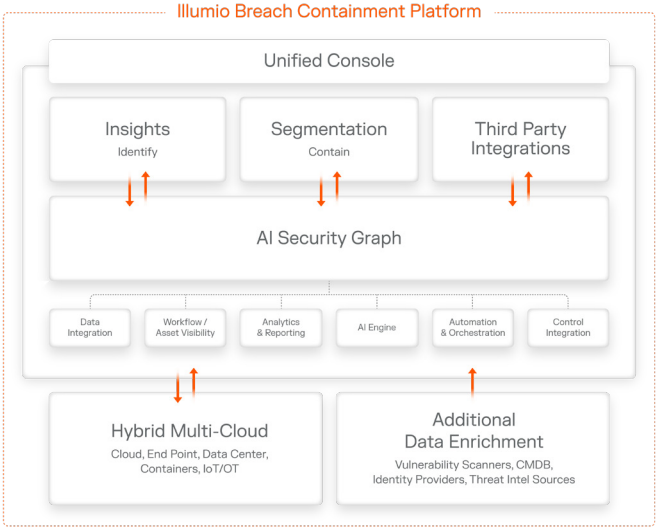
Speed and precision

Real-time observability with the agility to scale effortlessly. Network agnostic. Stable, predictable architecture.

How it works

The Illumio Breach Containment Platform follows a simple model: see your risk, set policy, and stop attackers before they move.

- **Assess risk.** Visualize communication and traffic across workloads, devices, and the internet with real-time observability — powered by your security graph and enhanced with our AI.
- **Define security controls**. Automatically set granular segmentation policies that adapt dynamically as your environment changes. Enforce least privilege access. Restrict unnecessary traffic. Control communications.
- **Contain the attack.** Proactively protect with a resilient architecture. Reactively isolate compromised systems during an active attack to stop the spread.



What Mythos Changes	The Control Gap It Exposes	How Illumio Answers It
Zero-day flaws found and weaponized at AI speed.	Patch cycles are too slow to matter.	Vulnerability-agnostic segmentation holds regardless of exploit.
Exploitation window collapses to near zero.	Prevention stack is overwhelmed before responding.	Pre-built segmentation policy contains damage even before incident response.
Lateral movement determines breach impact.	Implicit trust enables free movement inside.	Microsegmentation blocks lateral paths and shrinks the blast radius.
No vulnerability too obscure or buried to stay hidden.	Assume-breach posture is now mandatory, not optional.	Real-time observability + Zero Trust policy = survivable architecture.
Identity-driven attacks bypass signature detection.	Detection happens after lateral expansion begins.	Architecture-level policy limits reach before detection fires.

Illumio in a post-Mythos world

Illumio fills the very control gap that Mythos makes urgent: containing lateral movement, no matter what vulnerability attackers exploit.

- **Vulnerability-agnostic protection.** Illumio Segmentation limits lateral movement whether the exploit is known, unknown, or brand new. You don't need to know the CVE for the policy to hold.
- **Turns the compromise you can't prevent into incidents you easily contain.** Microsegmentation prevents one compromised workload from turning into an enterprise-wide problem.

Breach containment is non-negotiable in the age of AI. AI makes compromise cheaper, faster, and more scalable. Containment makes it survivable.

Proven leadership

Illumio is built for the agentic AI era. Recognized as a Leader in the Forrester Wave™ for Microsegmentation, we protect:

- 15+ of the Fortune 100
- 6 of the 10 largest global banks
- 3 of the 5 largest enterprise SaaS companies

You can't stop breaches. You *can* stop disasters.

Frontier AI models are making attacks faster and easier. Illumio makes sure breaches don't spread. Visit:

illumio.com/illumio-platform

About Illumio

Illumio is the leader in ransomware and breach containment, redefining how organizations contain cyberattacks and enable operational resilience. Powered by an AI security graph, our breach containment platform identifies and contains threats across hybrid multi-cloud environments — stopping the spread of attacks before they become disasters.

Recognized as a Leader in the Forrester Wave™ for Microsegmentation, Illumio enables Zero Trust, strengthening cyber resilience for the infrastructure, systems, and organizations that keep the world running.