illumio

FACT SHEET

Cybersecurity nach Mythos: Eindämmung ist die einzige Chance

Warum Breach Containment ab sofort unverzichtbar ist

Anfang 2026 fand die Anthropic-KI *Claude Mythos Preview* selbstständig Tausende kritische Zero-Day-Schwachstellen in allen gängigen Betriebssystemen und Browsern und in weit verbreiteter Infrastruktur – und lieferte für viele davon auch gleich Exploits mit. Allein bei Firefox entwickelte das Modell funktionierende Exploits für 72 % der gefundenen Sicherheitslücken.

Und das war kein Forschungsprojekt. Mythos prüfte den Produktivcode, mit dem die Server, Browser und Firewalls dieser Welt laufen. Viele davon waren seit Jahrzehnten im Einsatz, ohne dass jemand die Fehler bemerkt hätte.

Angreifer brauchen jetzt nur noch Sekunden. Ihnen gegenüber steht eine Abwehr, die eher in Wochen rechnet.

Was das bedeutet:

- Die aktive Ausnutzung beginnt nicht erst nach Monaten, sondern spätestens nach ein paar Stunden.
- Patch-Backlogs, vorher schon ellenlang, lassen sich nun endgültig nicht mehr abarbeiten.
- Das Prinzip „Patchen, bevor es ausgenutzt wird“ funktioniert nicht mehr.
- Bisherige Betriebsmodelle können nicht skalieren, egal wie sehr man sich bemüht.

Mythos verkürzt die Zeit zwischen Entdeckung und Ausnutzung auf nahezu null.

Was sich in der Abwehr ändert

Mythos macht die vorhandenen Tools nicht nutzlos, aber es verändert radikal das Timing, auf das sich jedes Security-Programm verlässt. So stellt sich die Lage jetzt dar:

- Erkennung, Triage und Reaktion laufen noch in menschlicher Geschwindigkeit ab. Vorfälle müssen sortiert und korreliert, Entscheidungen abgewartet werden. Angreifer dagegen werden immer schneller.
- Angreifer, die statt Malware auf Identitäten setzen, fallen im System nicht gleich auf, weil sie die signaturbasierte Erkennung umgehen.
- Angreifer werden oft erst dann bemerkt, wenn sie sich längst lateral bewegen.
- Ein 30- bis 90-tägiger Patch-Zyklus ist jetzt ein ernstes operatives Risiko, weil Schwachstellen wesentlich schneller entdeckt und ausgenutzt werden können.

Neue Fragen

Vor Mythos lautete die Frage: „Können wir jeden Exploit finden und blocken, bevor Angreifer ihn nutzen?“ Dieses Wettrennen ist jetzt Geschichte.

Alte Frage	Neue Frage
Was ist verwundbar?	Was ist aktuell erreichbar?
Ist es gepatcht?	Welche Pfade führen vom Zugangspunkt zu kritischen Assets?
Wurde ein Alert ausgelöst?	Wie groß ist der Angriffsradius, wenn eine Schutzmaßnahme fehlschlägt?

Entscheidend für die Wirksamkeit von Schutzmaßnahmen ist nicht mehr, wie schnell Schwachstellen erkannt und gepatcht werden, sondern wie groß der Angriffsradius ist – wie weit ein Angreifer kommt, wenn er einmal im System ist.

Mythos verändert, was Angreifer finden und wie schnell sie es ausnutzen können, aber der Ablauf ist immer noch derselbe:

- Ein Zero-Day-Exploit öffnet das Tor.
- Die interne Umgebung setzt die Grenzen.
- Durch laterale Bewegung wird der Angriff zur Katastrophe.

Zero Trust wird unverzichtbar

Seit Jahren schon ist es als Best Practice im Gespräch, aber spätestens nach Mythos ist Zero Trust jetzt die Grundvoraussetzung. Illumio setzt Zero Trust operativ – nicht nur theoretisch – im Rechenzentrum, in der Cloud, bei Endpoints und in hybriden Umgebungen um:

- **Kern definieren.** Welche Assets, Identitäten und Control Planes sind wirklich geschäftskritisch?
- **Von Angreifbarkeit ausgehen.** Das Design muss von der Annahme ausgehen, dass ein Angreifer sich irgendwo außerhalb des Kerns Zugang verschaffen wird.
- **Nur explizite Pfade zulassen.** Mit Least-Privilege-Richtlinien auf Ressourcenebene wird geregelt, wer oder was womit kommunizieren darf.
- **Immer überprüfen.** Kein implizites Vertrauen basierend auf Netzwerkstandort, vererbtem Zugriff oder veralteten Daten.
- **Schnell isolieren.** Wird eine Kompromittierung vermutet, hält das Design die Angreifer auf und der Angriff kann schneller eingedämmt werden.

Wie Illumio hilft

Die Illumio Breach Containment Platform ist die entscheidende Sicherheitsschicht für hybride Umgebungen. Mit Echtzeit-Einblick und Mikrosegmentierung können Sie Zero-Trust-Richtlinien mit dem Tempo durchsetzen, das die KI erzwingt. Illumio hilft Ihnen, laterale Bewegung zu stoppen, den Zugriff einzugrenzen und die Angriffsfläche zu reduzieren – damit aus dem Erstzugriff keine unternehmensweite Katastrophe wird.

Die Plattform

Die Illumio Breach Containment Platform kombiniert proaktives Containment mit KI-gestützter Erkennung – zwei Produkte in einem.

Illumio Segmentation

Marktführende Mikrosegmentierung:

- Grenzt laterale Bewegung proaktiv ein
- Reduziert die Angriffsfläche
- Schirmt verwundbare Systeme ab
- Schützt kritische Workloads
- Beschleunigt Ihre Zero-Trust-Strategie

Illumio Insights

Umfassende KI-gestützte Observability und Erkennung:

- Ermittelt und schützt verwundbare Workloads in Echtzeit
- Entdeckt und stoppt Bedrohungen sofort
- Beschleunigt die Mikrosegmentierung
- Stärkt kontinuierlich die Security Posture

Wichtigste Vorteile

Eine Plattform, einheitliche Kontrolle

Innerhalb von Minuten bereitgestellt, verwaltet über eine zentrale Konsole. Die Plattform für das komplette Breach Containment, von Anfang bis Ende.

Flexibel und skalierbar

Passt sich in Hybrid-, Multi-Cloud-, On-Premises- und OT-Umgebungen nahtlos an, wenn sich die Anforderungen ändern.

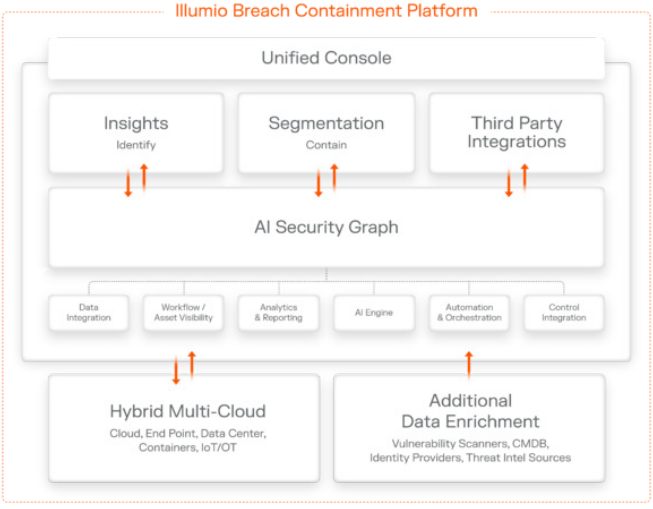
Schnell und präzise

Echtzeit-Observability mit der Agilität, einfach skalieren zu können. Netzwerkunabhängig, mit einer stabilen, planbaren Architektur.

So funktioniert es

Die Illumio Breach Containment Platform funktioniert nach einem ganz einfachen Modell: Risiko sehen, Richtlinie festlegen, Angreifer aufhalten.

- **Risiko bewerten.** Sie sehen die Kommunikation und den Datenverkehr zwischen Workloads, Geräten und dem Internet mit Echtzeit-Observability – in Ihrem Security Graph, unterstützt von unserer KI.
- **Sicherheitsmaßnahmen definieren.** Automatisch werden granulare Segmentierungsrichtlinien festgelegt, die sich dynamisch anpassen, wenn sich Ihre Umgebung verändert. Damit wird das Least-Privilege-Prinzip umgesetzt, unnötiger Datenverkehr eingeschränkt und die Kommunikation kontrolliert.
- **Angriff eindämmen.** Eine resiliente Architektur schützt Ihre Umgebung proaktiv. Und reaktiv werden bei einem Angriff die kompromittierten Systeme isoliert, um die Ausbreitung zu stoppen.



Was sich durch Mythos ändert	Problem in aktuellen Prozessen	Wie Illumio das Problem löst
Zero-Day-Schwachstellen werden durch KI extrem schnell gefunden und ausgenutzt.	Patch-Zyklen sind viel zu langsam, um mitzuhalten.	Schwachstellenunabhängige Segmentierung hält jedem Exploit stand.
Ausnutzungsfenster verkürzt sich auf nahezu null.	Prävention ist überlastet, keine rechtzeitige Reaktion möglich.	Vordefinierte Segmentierungsrichtlinien dämmen den Schaden ein, noch bevor die Incident Response angelaufen ist.
Laterale Bewegung bestimmt das Ausmaß des Schadens.	Implizites Vertrauen ermöglicht freie Bewegung im System.	Mikrosegmentierung blockiert laterale Pfade und verkleinert den Angriffsradius.
Jede Schwachstelle wird gefunden, egal wie klein oder versteckt.	„Assume Breach"-Ansatz ist jetzt Pflicht, nicht mehr optional.	Echtzeit-Observability + Zero-Trust-Richtlinien = widerstandsfähige Architektur.
Identitätsbasierte Angriffe umgehen die Signatur-Erkennung.	Angreifer werden erst erkannt, wenn sie sich bereits lateral bewegen.	Richtlinien auf Architekturebene halten Angreifer auf, noch bevor die Erkennung anschlägt.

Illumio in der Welt nach Mythos

Illumio schließt die Kontrolllücken, die durch Mythos hochriskant geworden sind: Laterale Bewegung muss zuverlässig aufgehalten werden, egal welche Schwachstelle die Angreifer ausnutzen.

- **Schwachstellenunabhängiger Schutz.** Illumio Segmentation begrenzt laterale Bewegung bei bekannten Exploits genauso wie bei unbekannten und ganz neuen. Die Richtlinie greift immer, auch wenn Sie den CVE nicht kennen.
- **Einfache Eindämmung.** Kompromittierungen sind unvermeidbar, aber Mikrosegmentierung verhindert, dass Angreifer sich ausgehend von einem Workload im ganzen Unternehmen ausbreiten können.

Anerkannte Führungsposition

Illumio ist für das Agentic-AI-Zeitalter gebaut. Wir werden im Forrester Wave™ für Mikrosegmentierung als Leader geführt, und zu unseren Kunden gehören:

- > 15 der Fortune 100
- 6 der 10 größten globalen Banken
- 3 der 5 größten SaaS-Unternehmen

Breach Containment ist im KI-Zeitalter unverzichtbar. Durch KI werden Angriffe schneller, billiger und besser skalierbar. Containment verhindert, dass das zur Katastrophe wird.

Angriffe sind unvermeidbar. Katastrophen nicht.

Frontier-KI beschleunigt und erleichtert Angriffe. Illumio sorgt dafür, dass sie sich nicht ausbreiten können.

illumio.com/de/illumio-platform

Über Illumio

Als führender Anbieter von Ransomware- und Breach-Containment bietet Illumio eine neue Art, Cyberangriffe einzudämmen und betriebliche Resilienz zu erreichen. Unsere Breach-Containment-Plattform mit dem KI-gestützten Security Graph erkennt und stoppt Bedrohungen über die gesamte Umgebung hinweg – in der Cloud, im Rechenzentrum und bei Endpoints. So werden Angreifer aufgehalten, bevor sie katastrophalen Schaden anrichten.

Illumio, im Forrester Wave™ Report als Leader im Bereich Mikrosegmentierung positioniert, ermöglicht Zero Trust und stärkt die Cyberresilienz der Infrastrukturen, Systeme und Organisationen, die die Welt am Laufen halten.

Copyright © 2025 Illumio, Inc. Alle Rechte vorbehalten. Illumio® ist eine Marke oder eingetragene Marke von Illumio, Inc. oder seinen Tochtergesellschaften in den USA und anderen Ländern. Marken Dritter, die in diesem Dokument genannt werden, sind Eigentum ihrer jeweiligen Inhaber.