Banking and Financial Services Mythos Fact Sheet

Banking was bulit for availability, but Mythos made that a liability. Breach containment is now the only viable security strategy.

Banking runs on availability. Core systems, payment rails, and settlement engines must stay up and running. Most banks run a mix of legacy, on-premises, and cloud infrastructure.

That complexity creates gaps. Vulnerabilities stay open longer than security teams want, and patches must wait on change control cycles.

Mythos changes what that backlog costs you. And the consequences for banking are immediate:

- Patch backlogs are already large. Mythos makes them permanently unmanageable at current speed.
- The assumption that "we'll patch it before it's exploited" no longer holds for any open exception.
- A 30–90 day patch cycle is now operational risk, not risk reduction.
- Established operating models can't scale, no matter the effort.

Warning flags for banks

Mythos creates major pressure points that banks can no longer manage around.

The patch backlog is no longer manageable

Mythos found thousands of zero-day vulnerabilities across major operating systems and browsers. Many had been sitting in production code for 10 to 27 years, unknown, untouched, and live in systems banks depend on every day.

According to Verizon's 2025 Data Breach Investigations Report, attackers reach mass exploitation within five days of disclosure. Full remediation in a regulated bank takes weeks. That gap is where breaches will happen.

> "Mythos could crack the whole cyber risk world open."
>
> **Andrew Bailey**
> Governor, Bank of England

Executive accountability is on the rise

Executives are now expected to own the volume of risk Mythos surfaces. The gap between what's discoverable and what remediation programs can realistically fix is exactly where personal liability sits.

- Under NYDFS Part 500, the CEO and CISO must co-sign an annual compliance certification.
- DORA Article 5 puts ICT risk against named individuals in the management body, on a register, with personal liability attached.
- The UK Senior Managers Regime works the same way, as do equivalent frameworks in Singapore, Australia, and Hong Kong.

These rules were written when risk was bounded by what humans could discover. Mythos changes that. Executives are now accountable for a risk volume their programs can no longer keep pace with.

Severe and plausible risk

"Severe but plausible" used to describe a sophisticated, multi-stage attack, the kind that cascades through critical systems and pushes an institution past its limits. That scenario now describes what any attacker with access to a capable AI model can attempt. They can map attack paths, chain vulnerabilities, and move before defenses respond. The plausible boundary has shifted to meet the severe one.

The blast radius is widening

Banks share cloud platforms, core banking vendors, payment processors, and API infrastructure with dozens of peer institutions. One compromised provider can hand an attacker trusted access across all of them.

Detection speed and patch velocity matter less than they used to. What matters now is blast radius: how far an attacker can move once they're in. Most security programs aren't built around that question yet.

Old question	New question
Is the vulnerability on the patch schedule	Can an attacker reach our critical applications before we patch them?
Did our last red team engagement pass?	Was it calibrated against an AI-accelerated adversary?
Have we attested to our controls under DORA, SM&CR, or NYDFS?	Can we show our maximum blast radius if those controls fail tonight?
Have we audited our shared cloud provider?	Can we show, in writing, what our maximum blast radius is if those controls are overwhelmed tonight?
Have we audited our shared cloud provider?	If that provider is compromised, how far into our environment does an attacker spread before any control stops them?

How Illumio helps

Most banks were built for availability. That design made lateral movement easy for anyone who gets inside the network.

In a post-Mythos world, breaches are more inevitable than ever. Breach containment is the only strategy that holds up under those conditions. Illumio is built to contain breaches. When a breach happens, it stays small, contained, and survivable with Illumio.

Illumio delivers:

- **Protection that doesn't depend on knowing the vulnerability.** Illumio Segmentation limits lateral movement whether the exploit is known, unknown, or brand new. The policy holds without needing to know the CVE.
- **Compromise that stays contained.** Microsegmentation stops one compromised workload from becoming an enterprise-wide problem.
- **Containment built in, not bolted on.** Illumio prepares your institution to be ready for breaches. When they happen, containment is already in place. A small security incident stays small instead of spreading into catstrophe.
- **Evidence executives can stand behind.** Named individuals under DORA, SM&CR, NYDFS, and APRA can show active containment controls before an incident, not in response to one.

Learn more about how to prepare for Mythos with Illumio.

illumio.com/resource-center/mythos-fact-sheet

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.