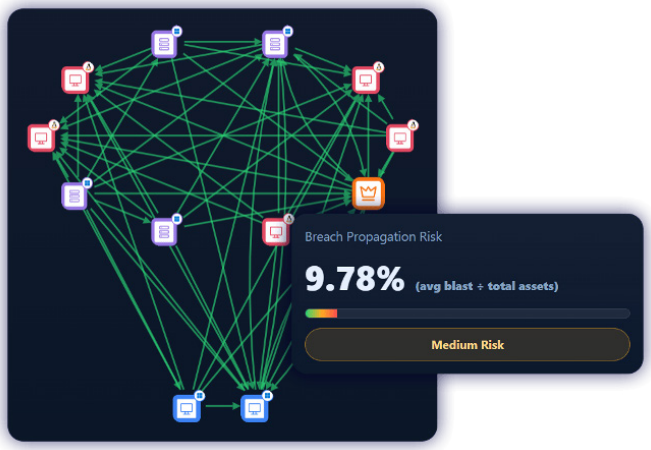
CISO RESOURCES

MYTHOS Resilience Readiness Pack



Know the Reach. Cut the Paths. Prove It.

AI-speed attacks are changing the job of the CISO and CIO and old approaches are not enough.

- **Detect and respond is too slow:** By the time an alert is investigated, an attacker or rogue AI agent may already have moved.
- **Fixing every vulnerability will not work:** There are too many assets, too many exposures, and too little time.

If something gets in, how far can it go and what have we already done to contain it?

The **MYTHOS Resilience Readiness Pack** gives security and IT leaders a clear answer. Zero Networks shows the internal pathways a vulnerability, compromised identity, exposed system, or AI-speed attacker could use to move across your environment.

Zero shows how those paths can be reduced with permanent, automated containment.

Built for Leaders Who Need Confidence

MYTHOS readiness helps CISOs and CIOs answer the hard questions before the next incident.

It gives you a board-ready story when leadership asks what you are doing about AI-speed attacks. It gives your team a way to focus on the paths that matter most. And it gives the business confidence that one exposed system, vulnerable asset, or stolen credential does not have to become a company-wide disruption.

From Exposure to Containment

CTAM and vulnerability programs help identify what is exposed. Zero shows whether that exposure can spread internally and how to stop it. With automated microsegmentation, privileged access controls, and just-in-time MFA, Zero creates a permanent containment layer across the environment. That means resilience no longer depends on catching every attack fast enough or fixing every issue in time.

What You Get

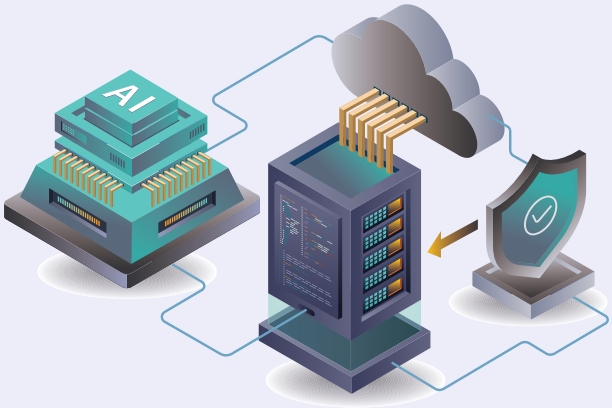
With the MYTHOS Resilience Readiness Pack, you can show:

- ✓ How far an issue could move today
- ✓ Which internal paths create the most business risk
- ✓ How much reach Zero can reduce
- ✓ What permanent containment looks like
- ✓ How you are turning MYTHOS concern into measurable action

Zero provides the breach-path analysis, executive-ready content and board-level narrative so you can walk in with a **credible answer**.

Why Zero Networks

Most tools tell you what is exposed. Zero shows whether it can spread — and then closes the paths. Zero Networks' lateral movement research found that one compromised host can often reach **up to 85%** of the environment. With Zero containment in place, that reach can be reduced to virtually zero for protected assets and privileged pathways.



Get the Mythos Resilience Readiness Pack

ZERO Networks