Project Glasswing & NodeZero®

Capabilities, Differences, and Complementary Value

Prepared For:

Security & IT Leadership

Purpose:

This document explains what Project Glasswing and NodeZero are, how they differ, and how they may work together to address different parts of the security problem.

What Is Project Glasswing?

Project Glasswing is a cybersecurity initiative launched by Anthropic in April 2026, built around Claude Mythos Preview — a frontier AI model designed to identify and work through software vulnerabilities.

The initiative's central mission is to harness AI's capabilities to improve defensive security outcomes in an era where AI-augmented cyberattacks are becoming increasingly realistic.

Key Characteristics

Code-level analysis: Glasswing operates at the source-code and binary level, reasoning across complex, interconnected systems to surface logic flaws that traditional scanners miss

Autonomous vulnerability discovery: Including both known (N-day) and previously unknown (zero-day) vulnerabilities across operating systems, web browsers, and open-source codebases

Controlled defensive context: Access is tightly managed and focused on defensive outcomes, while leveraging capabilities that include validating and developing exploits in controlled settings

Collaborative intelligence sharing: Participating organizations share learnings with the broader industry

What Mythos Demonstrates

Mythos doesn't just identify vulnerabilities — it can validate them, develop working exploits, and in some cases chain multiple weaknesses together.

The key shift is that the effort required to move from vulnerability discovery to real-world impact is collapsing.

This is not just acceleration. It changes how attacks are created.

In Plain Language

Project Glasswing is a research and remediation initiative. It uses advanced AI to analyze software at scale, identify weaknesses, and demonstrate how those weaknesses can be turned into real-world attacks.

What This Means for Security Teams

The initial reaction to Mythos has focused on vulnerability discovery. That's not the real shift.

The Real Shift

Historically, these were separate steps:

- Discovery
- Validation
- Exploitation
- Chaining
- Impact

Each required time, expertise, and effort.

Mythos compresses these steps into a much tighter loop — iterating between identifying weaknesses, testing them, and developing working exploitation paths.

Why This Matters

This changes three things:

Speed: Vulnerabilities can be turned into exploits faster

Scale: More paths can be explored in parallel

Accessibility: Less specialized expertise is required to produce meaningful results

This does not introduce entirely new classes of vulnerabilities.

But it significantly reduces the effort required to turn existing weaknesses into real-world impact.

What is NodeZero?

NodeZero is Horizon3.ai's AI-native Proactive Security Platform — a SaaS solution organizations deploy to continuously test and validate the security of their own environments.

Where Glasswing operates at the code and software layer, NodeZero operates inside your environment — validating how those risks actually manifest in practice.

Horizon3.ai built NodeZero around a simple principle:

The only way to truly understand your security posture is to test your environment the way a real adversary would.

NodeZero emulates real-world attacker behavior — not just identifying vulnerabilities, but chaining together misconfigurations, weak credentials, and software flaws to demonstrate real attack paths.

Exploitability is what matters. It allows teams to focus on what a real attacker could use, rather than what appears severe in isolation.

Core Capabilities of NodeZero

Continuous autonomous pentesting

Internal and external tests run on demand or on a recurring schedule

External asset discovery

Identifies internet-facing assets using DNS enumeration, OSINT, and crawling techniques

Attack path chaining

Connects vulnerabilities, identities, and misconfigurations into real attack paths

Proof of exploitation

Validates that weaknesses are actually exploitable

Web application testing

Evaluates common web vulnerabilities and chains them into broader compromise paths

Rapid Response

Evaluates exposure to newly disclosed vulnerabilities and validates mitigations

Find-Fix-Verify loop

Enables immediate retesting to confirm remediation

Cloud and hybrid coverage

Pivots across on-prem and cloud environments

In Plain Language: NodeZero shows what attackers can actually do in your environment — not just what might be vulnerable.

How are they different?

While both Glasswing and NodeZero use AI, they operate at fundamentally different layers.

Dimension	Project Glasswing	NodeZero
Primary Purpose	Identify and work through vulnerabilities in software	Continuously test your environment
Target	Codebases, operating systems, open-source software	Your infrastructure: network, cloud, identities, applications
Output	Vulnerability insights and exploit development in controlled settings	Exploitable attack paths and validated impact
Access Model	Controlled, invitation-based	Self-service SaaS
Scope	Code-level analysis	Environment-level validation

Key Distinction

Glasswing shows what can be done at the code level.

NodeZero shows what will actually impact your environment.

How Do They Complement Each Other?

Project Glasswing and NodeZero operate at different layers of the security problem.

Together, they provide a more complete view of risk.

Project Glasswing Addresses

Vulnerabilities within software — including logic flaws and zero-days in the systems your environment depends on.

Think of Glasswing as improving the security of the underlying components.

NodeZero Addresses

Exploitable weaknesses in how your organization deploys and operates those systems — including misconfigurations, identity exposure, and lateral movement paths.

Think of NodeZero as testing whether your environment can actually be compromised.

The Reinforcing Reality

As capabilities like Mythos reduce the effort required to discover and exploit vulnerabilities:

- More vulnerabilities will be identified
- More potential attack paths will be explored
- More combinations of weaknesses will be tested

This increases pressure on security teams — not because the vulnerabilities are new, but because **the effort required to turn them into impact is decreasing.**

NodeZero ensures your organization can:

- Identify which exposures actually matter
- Validate whether they can be exploited
- Confirm that remediation reduces real risk

Key Takeaway

Project Glasswing and NodeZero represent two complementary approaches:

- Project Glasswing uses AI to identify and work through vulnerabilities in software systems
- NodeZero enables organizations to continuously test their own environments and validate real-world risk

Together, they address the lifecycle: From identifying weaknesses to validating whether those weaknesses can actually be used to compromise your environment

Security didn't break.
The model did.

What matters now is not how many vulnerabilities exist — but which ones can actually be exploited, how they connect, and what they enable.