dynatrace

Runtime security for modern AI and cloud applications

Runtime vulnerability analytics

Claude Mythos is purpose-built for autonomous vulnerability discovery — collapsing the window from weeks to hours. Critically, it chains multiple low-impact flaws into sophisticated, weaponized attacks. Dynatrace Runtime Vulnerability Analytics acts on facts, anchoring every finding in live runtime context so you can fix what is truly exploitable in production.

742%
Increase in open-source supply chain attacks
— Sonatype, 2023

40%
Of all breaches occur at the application level
— Verizon DBIR, 2025

~77%
Less noise vs earlier pipeline scanning tools
— Dynatrace customer

4X
Faster vulnerability remediation
— Dynatrace customer

The challenge

How Mythos turns low-severity findings into a critical attack

1 LOW
Auth Bypass
Unauthenticated access to internal service

2 MEDIUM
Config Exposure
App misconfiguration exposes internal credentials

3 LOW
Dependency Flaw
Unpatched software component enables remote access

CRITICAL EXPLOIT
WEAPONISED
in under 4 hours

Illustrative example. Traditional scanners score each finding in isolation. Dynatrace Runtime Vulnerability Analytics sees the full chain — in runtime context

The Dynatrace difference

Unified risk view	Risk in context	Agentic remediation
Grail Data Lakehouse Centralizes all observability and security data — correlating logs, metrics, traces, and security events for unified risk decisions.	**Smartscape** Real-time dependency graph maps every component to its business services — enabling precise impact-radius analysis.	**Dynatrace Intelligence** Agentic system that routes confirmed findings to the right team with fix guidance and closed-loop validation.
Dynatrace Vulnerability Feed Patented feed with deepest coverage of open-source and AI frameworks — the primary target for Mythos-era discovery.	**Runtime Exposure Details** Focuses only on what you actually run. High-confidence critical findings based on what is reachable in production.	**Workflow Integration** Ready-made agents categorize by severity, map code to runtime context, and connect observability to security findings.

How it works

1. ALL CVEs
100,000s detected

2. RUNNING
Only loaded componets

3. REACHABLE
Real traffic paths only

4. REMEDIATE
4X faster. Agentic

What would Mythos find in your enviornment?

Switch on Runtime Vulnerability Analytics to see exactly what is exploitable in your environment — before an AI model does.