HCL BigFix

# AI Can Find Vulnerabilities Faster Than Most Organizations Can Fix Them

AI has fundamentally changed the economics of vulnerability discovery. Models such as Mythos demonstrate that vulnerabilities can now be identified at a speed and scale that far exceeds traditional human-led approaches. As discovery accelerates, the challenge is no longer finding vulnerabilities, it is remediating them before they can be exploited. Organizations that succeed will identify exposure faster, prioritize what matters, remediate quickly, and continuously prove risk reduction.

## The numbers that define the threat

**31%**

Exploited vulnerabilities are now the #1 initial access vector in breaches, surpassing credential theft.

**8 hours**

Average time from public disclosure to first confirmed in-the-wild exploitation

**26%**

Only 26% of known exploited vulnerabilities were fully remediated.

**<9%**

of published CVEs are ever weaponised in real attacks, but those are the ones that matter.

Source : Verizon DBIR 2026, https://zerodayclock.com/

## Speed Is the New Battleground

AI has removed the historic constraint of finding vulnerabilities at scale. The new bottleneck is remediation. Anthropic's Mythos model demonstrated this at scale, uncovering more than 10,000 critical vulnerabilities within weeks, often before vendor patches exist. In the Mythos era, resilience depends on one thing: reducing exposure faster than threats can evolve.

### What security leaders now face

- **Exploitation velocity**
  CVE disclosure to active exploitation now measured in hours. Monthly patch cycles cannot keep pace.
- **Compliance without continuity**
  Point-in-time audits miss drift. Posture changes the moment a scan completes. Continuous enforcement is the only defensible model.
- **Noise vs. signal**
  Thousands of CVEs are published monthly. Fewer than 9% are ever weaponised. Knowing which ones to prioritise is the challenge.
- **Defend before a patch exists**
  Misconfiguration is the attack surface AI exploits first. Enforcing secure baselines closes exposure before a vendor fix ships.

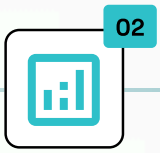
HCLSoftware

## How HCL BigFix responds

HCL BigFix operates as a continuous loop, every remediation feeds the next detection cycle, closing exposure windows in near real-time.

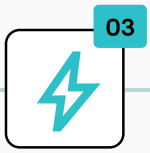

### Detect

Identify vulnerable endpoints and security exposures across your environment.




### Prioritize

Focus on the vulnerabilities most likely to be exploited.




### Act

Patch, disable, reconfigure, quarantine, or remediate endpoints at scale.


### Prove

Demonstrate measurable risk reduction with board-ready reporting.

**Continuous loop: every Act feeds the next Detect.**

## What Makes HCL BigFix Operationally Different

### Unified Endpoint Management

A unified platform for patching, compliance, inventory, remediation, and endpoint management.

### On-Premise Control

Maintain complete control of your data, infrastructure, and sovereignty requirements.

### Legacy Systems Support

Manage legacy operating systems and applications that other vendors no longer support.

### Largest Remediation Library

630K+ Fixlets and native scanner integrations help prioritize and remediate critical exposures without manual handoffs.

### Governed at Scale

Every Fixlet is human-reviewed with staged deployment and rollback safety. Speed without operational risk.

### Autonomous Agent

Patching, enforcement, and compliance reporting continue across air-gapped, OT, and branch environments without persistent connectivity.

**Mythos finds the vulnerability.**
**HCL BigFix closes the exposure.**

Glasswing is a signal, not a crisis. The organisations that act on it will be better positioned than those that wait.

Schedule a Demo

HCLSoftware