HCL BigFix

AI Management across the Enterprise

Closing the Visibility, Compliance, and Control Gaps That Shadow AI Has Opened

HCLSoftware

AI Has Become an Enterprise Governance Problem

Employees are adopting AI tools faster than most organizations can govern them. The average enterprise now sees employees accessing **60** AI applications per week, and adoption is happening bottom-up, often faster than IT, security, and finance can track. **94%** of organisations lack complete visibility into AI activity (Netskope AI Index, 2026). The tools are genuine productivity accelerators, but without oversight, they introduce new categories of risk that traditional endpoint and SaaS management tools may not fully see.

Fragmented tools and point-in-time checks leave organizations unable to answer three critical questions: which AI tools are in use, whether they are compliant, and whether their usage and spend can be controlled. This brief examines the three gaps redefining AI risk, how they translate into business exposure, and how HCL BigFix AI Management helps organizations discover, assess, and control AI tools from one platform.

The Structural Challenges

AI adoption is no longer moving through one approved path. Employees are using AI in browsers, code editors, desktop tools, local models, and SaaS applications, often before IT, security, or finance teams know it exists. This creates three structural gaps that every enterprise must close: the ability to see which AI tools are in use, assess whether they are safe and compliant, and control them before they create risk or waste.

The Three Gaps Redefining AI Risk

AI adoption is no longer moving through one approved path. Employees are using AI in browsers, code editors, desktop tools, local models, and SaaS applications, often before IT, security, or finance teams know it exists.
This creates three structural gaps that every enterprise must close: the ability to see which AI tools are in use, assess whether they are safe and compliant, and control them before they create risk or waste.

The Visibility Gap

(You can't govern what you can't see)

Traditional endpoint tools were built to manage software installed on machines. AI now appears in places traditional inventory tools may not fully detect: browser-based tools such as ChatGPT, Claude, and Gemini; local model files such as .gguf and .safetensors; and developer environments with MCP servers and AI coding assistants. Only 6% of organizations report complete visibility into AI usage across their environment. (Netskope AI Index, 2026). Everything outside formal procurement is invisible, and invisible risk cannot be quantified or defended.

The Compliance Blind Spot

Seeing a tool is not knowing if it's safe

Discovery is only the first step. Enterprise IT also needs to know whether each tool is approved for use: whether it is FedRAMP and ISO 42001 certified, whether it is policy compliant, where the data is stored, and what happens to customer prompts and enterprise data when the tool is used.

Many discovery tools report raw software data without the governance context needed for policy decisions. 63% of breached organizations had no AI governance policy, or were still drafting one (IBM, 2025). Under the EU AI Act, penalties reach up to €35M or 7% of global annual revenue (whichever is higher) for prohibited AI practices, and the rules can apply to any organization doing business in the EU regardless of where the organization is headquartered.

The Control & Cost Gap

A policy you cannot enforce is not control

Most governance failures are action failures, not detection failures. When a tool is found to be non-compliant with internal policy, customer requirements, or regulatory expectations, there is no fast path to find and remove every instance; manual processes take weeks and still miss some of the endpoints. The cost problem is the same: organizations pay for AI subscriptions that sit idle while employees use unsanctioned alternatives. A shadow AI breach costs roughly $670K more than a standard incident (IBM cost of data breach, 2025). Such examples show that most AI governance failures stem from a lack of control, not a lack of technology.

How the gaps translate into business risk

Three Gaps. One Business Risk.

These gaps do not stay contained within IT. They show up as business risks that affect security posture, audit readiness, operational response, and AI investment decisions

Data leakage.

Source code, customer records, and strategy documents may be entered into AI tools IT has not approved. Once that data leaves the organization, teams may lose control over where it is stored, who can access it, and whether it is used for model training.

Audit and control failure.

When auditors or regulators ask which AI tools are in use, whether they are compliant, and how violations are remediated, teams need more than a raw inventory. Without enriched context and enforcement, there is no defensible answer and unmanaged AI continues to create risk, waste, and accountability gaps.

Reputation risk.

An AI-related incident can surface before IT has a complete picture of the tool, user, data, or exposure involved.

This is no longer a technical control issue. It is a business continuity and resilience issue.

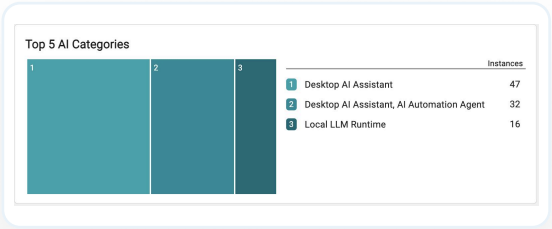
The Solution

How HCL BigFix Addresses These Challenges

AI Management is built into HCL BigFix, using the infrastructure and HCL BigFix agent deployed in 155+ million endpoints. It runs on a combined UEM + SAM foundation, uniting endpoint management with software asset intelligence to close the full loop so teams can discover AI tools, assess governance attributes, enforce policy, and understand AI spend from one platform. Each capability maps directly to one of the three governance gaps.

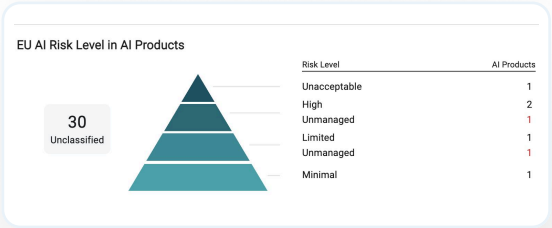
Total AI Visibility

Discovers AI across endpoints and browsers from a single platform, with out-of-the-box reporting and no new agents. It helps surface AI tools that traditional registry-based discovery can miss. It covers multiple AI categories, including browser-based AI, IDE plugins, AI automation agents, and other emerging AI tools. It can detect tools that may train on user prompts, local model files, and MCP server connections, helping organizations identify and reduce potential data leakage paths.



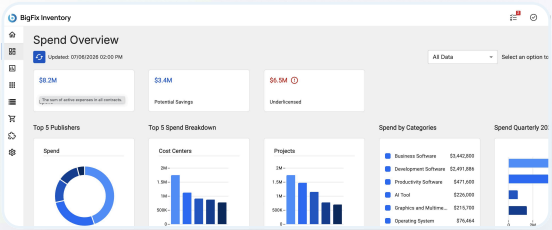
AI Compliance Intelligence

Enriches detected AI tools with governance attributes such as FedRAMP and ISO 42001 certification, data residency, vendor origin, EU AI Act risk classification, and data-training risk. These attributes help teams move from raw inventory to policy-ready decisions without custom scripting or separate data collection. This gives IT, security, and compliance teams a clearer view of which AI tools are approved, which require review, and which may need restriction or removal.



Governed AI Control and Spend Intelligence

Enables action from one console: redirect users to approved alternatives, uninstall endpoint-based tools, and revoke SaaS access for non-compliant or orphaned accounts. It supports uninstall actions for 30+ AI titles, giving teams a practical path to enforce policy across endpoint and SaaS environments.. Because it is built on a SAM foundation, it also surfaces license utilization, renewal exposure, and total AI spend, turning the governance problem and the cost problem into one workflow.



What HCL BigFix AI Management Delivers by Role

Security and risk leadership

(CISO, Head of Cybersecurity, Security Operations)

Reduce shadow AI data exposure.

Identify unsanctioned AI tools and usage paths that may expose source code, customer data, or confidential business information.

Answer audit and executive questions faster.

Produce an enriched inventory of sanctioned and unsanctioned AI tools instead of assembling evidence manually during an audit or incident.

IT operations and infrastructure

(IT Operations Head, Endpoint and Infrastructure Teams)

Complete discovery without adding tool sprawl.

Provides a single source of truth for AI across endpoints and browsers, using the HCL BigFix agent and Inventory server to reduce the need for additional discovery tools or endpoint overhead.

Enforce policy at scale.

When a tool is restricted, locate affected endpoints and take action across the environment from one console.

Compliance, risk and audit

(Chief Risk Officer, Compliance Head, Internal Audit)

Maintain continuous AI governance evidence.

Enrich each detected tool with FedRAMP, data residency, vendor origin, and EU AI Act risk attributes for ongoing review.

Regulatory readiness.

Demonstrate oversight of every AI tool in use, aligned to evolving requirements such as certifications or policy changes.

Executive and scale owners

(CIO, CFO, COO)

Improve AI spend discipline.

Identify idle licenses, redundant subscriptions, and renewal exposure so finance and procurement can make defensible consolidation decisions.

Make AI spend accountable.

Enable executives and finance teams to connect AI usage, ownership, compliance status, renewals, and spend, so they can reduce waste, consolidate tools, and defend AI investment decisions.

HCL BigFix: A Single Foundation for Enterprise AI Governance

HCL BigFix provides one trusted platform to see, assess, and govern AI across the enterprise. It enables organizations to reduce risk, demonstrate compliance, and optimize AI investment while building on the endpoint and software asset management foundation they already trust. AI adoption is already happening across the enterprise. Governance now needs to catch up. Discover every AI tool, assess compliance instantly, and control or remove it at scale.

Ready to discover, assess, and control AI across your environment?

Contact us to speak with an HCL BigFix expert, or book a 30-minute discovery session.

Sources:

Netskope AI Index, 2026 · IBM Cost of a Data Breach Report, 2025 · EU AI Act · Security Reports, 2025 · Forbes ("Why 95% of AI Pilots Fail").

HCLSoftware

hcl-software.com

About HCLSoftware

HCL Software is a global leader in software innovation, dedicated to powering the Digital+ Economy. We develop, market, sell, and support transformative solutions across business and industry, intelligent operations, total experience, data and analytics, and cybersecurity. Built on a rich heritage of pioneering spirit and unwavering commitment to customer success, we deliver best-in-class software products that empower organizations to achieve their goals. Our core values of integrity, inclusion, value creation, people centricity, and social responsibility guide everything we do. HCL Software serves more than 20,000 organizations, including a majority of the Fortune 100 and almost half of the Fortune 500. 02FEB2026.