

HCLTech | Supercharging
Progress™

All-in-One AI Security Risk and Compliance Hub

Safeguarding AI initiatives across cloud,
on-prem and SaaS environments

IBM

Platinum Partner

Overview

As organizations increasingly adopt AI to drive innovation, efficiency and decision making, securing these AI systems has become paramount. With ever-growing multicloud environments, diverse AI deployments and stringent compliance requirements, safeguarding these initiatives is no longer optional, it's essential for success and trust in the digital age.

The **HCLTech All-in-One AI Security Risk and Compliance Hub powered by IBM Guardium AI** provides an innovative, holistic approach to AI security. This powerful solution ensures protection, governance and compliance for AI deployments operating in heterogeneous environments, encompassing cloud, on-prem and SaaS systems.

Challenges

While revolutionary, AI brings a unique set of challenges that organizations must address to secure their operations and maintain compliance in an evolving regulatory landscape. Below are some of the key challenges organizations face:

- 1 Shadow AI risks:**
Shadow AI refers to the unsanctioned development or use of AI systems within an organization often without the knowledge of IT or security teams. Shadow AI can include rogue models, third party APIs, or experimental tools deployed without proper security controls. These rogue deployments expose an enterprise to risks such as mismanagement of sensitive data, bias in decision making and breaches in compliance.
- 2 Complex, distributed environments:**
Modern organizations operate across multicloud ecosystems, utilizing diverse vendors and solutions. This fragmented landscape makes it increasingly challenging to consistently detect, monitor and secure AI assets, leaving vulnerabilities unaddressed and compliance unmonitored.
- 3 Exposure to adversarial threats:**
AI systems are vulnerable to adversarial inputs and cyberattacks. For instance, prompt injections, data manipulation and malicious use of AI-generated outputs can degrade model integrity, exploit systems and lead to unintended or harmful consequences.
- 4 Evolving regulatory compliance:**
Organizations increasingly grapple with complex compliance requirements as governments and regulatory authorities around the world pass new laws governing AI systems. Frameworks such as the NIST AI 600-1 GOVERN, ISO 42001 and the EU AI Security Act demand ongoing monitoring, governance and adherence all of which can be difficult to operationalize and scale.

These challenges illustrate the need for a robust solution to holistically secure enterprises' AI initiatives.



Our Solution

The HCLTech All-in-One AI Security Risk and Compliance Hub offers a tailored, robust and future-proof approach to solving organizations' compliance and security challenges. Powered by IBM Guardium® AI Security, this solution acts as a centralized framework for managing AI security risks, AI lifecycle transparency and regulatory compliance with global standards. Our solution helps organizations to:

Discover AI assets:

Gain a comprehensive view of your organization's AI systems across various environments, whether in development or operation.

Evaluate AI security posture:

Assess vulnerabilities in AI systems to safeguard against adversarial attacks and misconfigurations.

Enhance regulatory alignment:

Ensure global compliance with frameworks such as NIST AI 600-1 GOVERN, ISO 42001 and the EU AI Security Act.

Mitigate shadow AI risks:

Eliminate unauthorized or unsanctioned AI deployments (aka "shadow AI"), which can lead to security gaps and compliance issues.

Our solution enables enterprises to implement responsible and secure AI initiatives through advanced features like adversarial testing, regulatory compliance assessments and policy controls for AI input-output monitoring.

Key features

The platform delivers high-impact capabilities tailored to meet enterprise AI security and compliance priorities:



Comprehensive AI asset

discovery: Automatically discover AI systems (shadow AI, sanctioned deployments and beyond) across code repositories, cloud accounts, multi-vendor platforms and on-prem deployments.



AI security posture

management: Evaluate and map the security posture of your AI systems, identifying vulnerabilities and misconfigurations. Proactively secure models against data and adversarial attacks, such as prompt injection or rogue usage.



Real-time adversarial testing:

Simulate adversarial attacks to test and strengthen AI system assumptions, algorithms and edge scenarios. Prevent harmful security breaches from emerging as an operational risk.



Input/output gateway

policies: Implement security guardrails for prompt input/output handling, restricting inappropriate prompts and securing interfaces from malicious usage. Policymaking is automated but customizable.



Multi-environment visibility:

Gain complete control and observability over AI deployments and assets across distributed environments, including hybrid or multicloud platforms featuring services from Azure, AWS, IBM Cloud and others.



Streamlined regulatory

compliance: Simplify adhering to AI-specific governance standards like the EU AI Security Act while staying aligned with broader global frameworks like ISO 42001 and NIST.

By seamlessly integrating AI asset discovery, observability and proactive testing, the Hub reduces AI-related security risks and enables enterprises to accelerate their adoption of responsible, trust-first AI solutions.

Benefits / Value Delivered

The **HCLTech All-in-One AI Security Risk and Compliance Hub** delivers tremendous value, creating a secure and compliant AI ecosystem for modern enterprises. Here's why its benefits stand above the competition:



Comprehensive shadow AI detection: Shadow AI, a significant risk factor for many enterprises, is fully addressed with 360-degree visibility of your environment. By detecting unsanctioned deployment of datasets, models, or AI services, the hub ensures that no rogue initiative escapes scrutiny. This eliminates unexpected vulnerabilities and aligns usage with your organizational policies.

Enhanced compliance and governance: Keep pace with rapidly changing regulations and standards. With automated regulatory alignment for frameworks like NIST, ISO and EU AI directives, your teams can focus on innovation. At the same time, the hub ensures complete adherence to local and international compliance requirements.



Proactive security measures: Prevent attacks before they occur. The hub acts as a resilient safeguard by identifying risks, such as adversaries exploiting insecure outputs or compromised models. Employing thorough adversarial testing and prompt protection ensures a long-term, sustainable security posture.

Reduced operational complexity: Simplify the challenges of managing AI deployments across a distributed and hybrid environment. With centralized monitoring and insights, teams spend less time manually securing systems while achieving optimized operational efficiency.



Scalable for enterprise growth: The hub is designed to meet the needs of growing enterprises with expanding AI initiatives. It seamlessly adjusts to increases in AI deployments' volume, scope and diversity without jeopardizing security or compliance.

Take the first step toward Responsible AI adoption.

For more information, visit the [solution page](#) on IBM

Learn more about our joint solutions here: [HCLTech and IBM Software for Security](#)

HCLTech | Supercharging
Progress™

hcltech.com