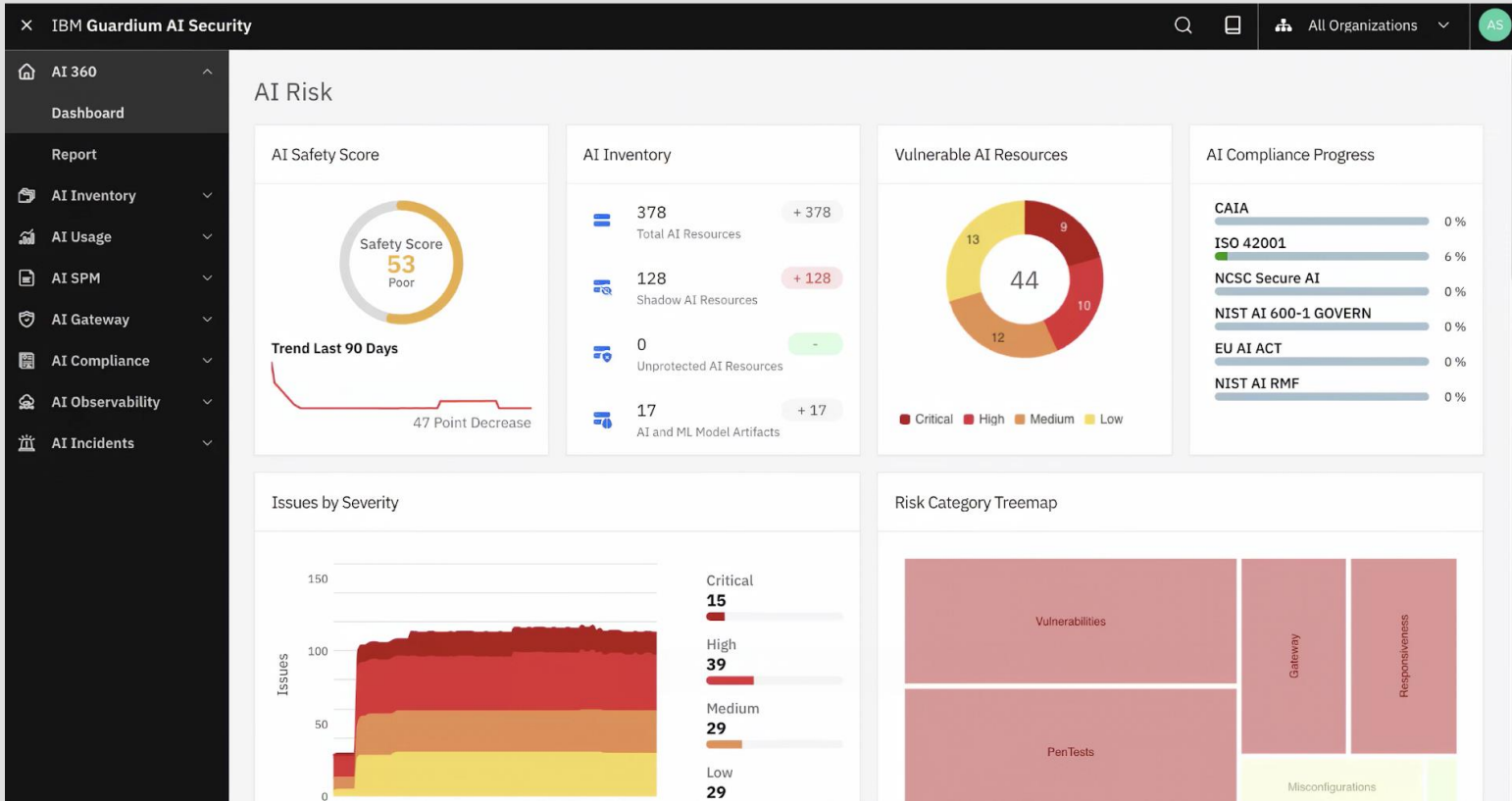
IBM Guardium AI Security Assessment Services Platform

Kuber Saraswat
Program Director, Product Management, BP Channel,
Cross Sell Data Security (Guardium) & Identity (Verify)
Kuber@ibm.com

Raninder Bhandari
Data Security Product Management
Business Partner Channel
raninder.bhandari@ibm.com



Build Multi-Million AI Security Services Deals

WHY

Low Investment, High-Service Potential
Unlock significant value with minimal upfront cost.

Recurring-Service Revenue Potential
Drive strong returns due to recurring service revenue business.

Rapid Onboarding & cost effective AIBOM Delivery
Get up and running fast with a streamlined onboarding process and rapid AI Bill of Materials generation

Expose Shadow AI Instantly
Quickly identify unauthorized or unmanaged
AI usage across the organization.

AI Trust, Risk and Security Management Market

21.3%
Global Market CAGR 2025-2034. Estimated Growth 16.379.66 M

HOW

Phase 1	Phase 2	Phase 3
Create Awareness Scan	**Develop Need**	**Manage Service Engagement**
Scan and Generate AIBOM	Service Engagement for AI use case development and prioritization	Secure AI Use case, regulatory compliance, pen testing, continuous monitoring and AI firewall
Two weeks	Four weeks	1-3 years

- 01 **AI Assessment as-a-service**
- 02 **AI Resource Mapping as-a-service**
- 03 **AI Compliance as-a-service**
- 04 **AI Security Manage Service**

Source : Polaris Market Research

Organizations are struggling to secure AI assets

81%

of executives say secure and trustworthy AI is essential to the success of their business[1]

Only 24%

of current generative AI projects are being secured[1]

51%

of executives cite unpredictable risks and new security vulnerabilities arising because of generative AI[1]

$4.88 million

average cost of a data breach in 2024, both a new record and a 10% increase year-on-year[2]

47%

of executives see new attacks targeting existing AI models, data and services[1]

At-scale attacks predicted

once a single generative AI technology reaches 50% market share[3]

[1] Securing Generative AI: What matters now - IBM and AWS, 2024
[2] Cost of a Data Breach 2024
[3] X-Force Threat Intelligence Index 2024

AI Security Managed Services

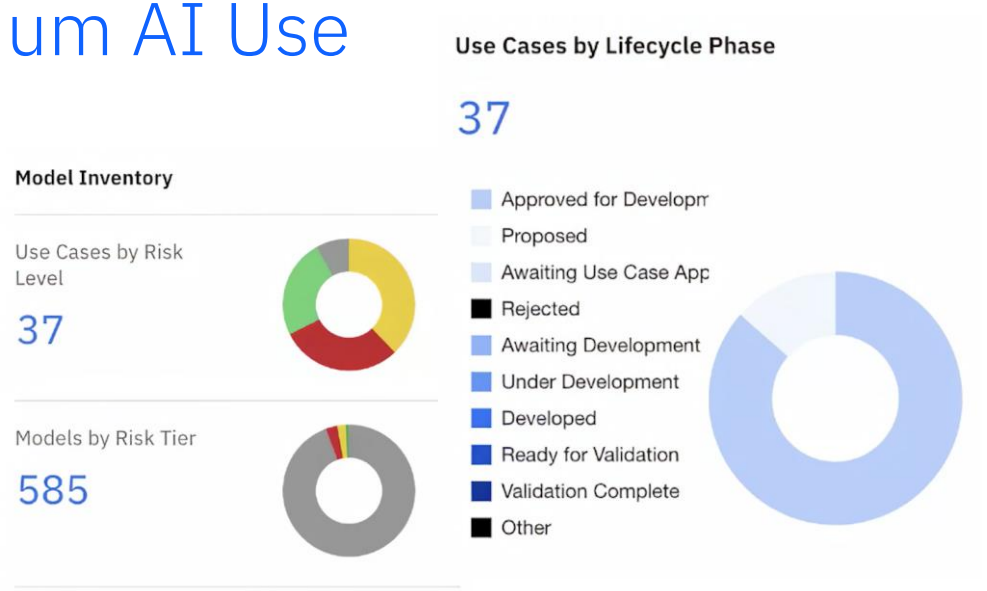
as-a-Service

- AI Assessment
- AI Resource Mapping
- AISPM
- AI Compliance

AI Security Services Phases and Outcome

Phase	Task	What Product Will Do	Partner Service Delivery	Outcome
AI Discovery & Inventory	1 2 3	- Agentless scanning of environments - Shadow AI detection - AI asset catalog creation	- Conduct stakeholder interviews to validate discovered assets - Classify AI systems by risk and business criticality	Verified AI inventory with risk tiers
Compliance Assessment	9 10	- Automated mapping to ISO 42001, EU AI Act, NIST AI RMF - Generate compliance posture score - Prebuilt auditor-ready templates	- Interpret compliance gaps in business context - Prioritize remediation based on regulatory exposure	Compliance roadmap with actionable priorities
Risk Modeling and Governance Design	4 5	- Risk scoring engine - Governance workflow automation - Integration with SIEM and IAM	- Design governance policies aligned with enterprise risk appetite - Define escalation paths and approval workflows	Governance blueprint integrated with enterprise processes
Secure Deployment and Guardrail Enforcement	6 7 8	- Runtime guardrails - Policy enforcement SDK - Drift prevention controls	- Implement guardrails in AI pipelines - Validate enforcement through penetration testing	Hardened AI systems with documented security posture
Continuous Monitoring and Observability	2 4 5	- AI-SPM (Security Posture Management) - AI Data Lake for telemetry - Real-time alerts and anomaly detection	- Configure dashboards for CISO/CAIO visibility - Conduct periodic compliance audits	Continuous compliance assurance and proactive threat detection
Remediation & Optimization	4 8	- Automated governance triggers - Risk re-scoring after remediation - Integration with ticketing systems	- Execute remediation plans - Optimize AI lifecycle for compliance and performance	Closed compliance gaps and improved operational resilience

Guardium AI Use cases



Unknown AI deployments is a business risk.

AI 360 View

Detects shadow AI and discovers all AI assets including chatbots, embedded systems, models.

AI deployment environment hardening

AI-SPM

Scans AI systems, LLM's for vulnerabilities, misconfigurations, and drift. Pentest homegrown and open-source models to identify ambiguities.

Ingest AI activities into threat detection system.

AI Observability

Activity log monitoring across AI models, pipelines etc. to create
AI 'data lake' to further integrate with SIEM, SOAR.

AI Gateway to inspect inbound and outbound interactions

AI Firewall

Policy controlled detection of advance threats such as prompt injection, jailbreaks etc. to prevent
sensitive data leakage.

Audit & Compliance to meet global regulations

AI Compliance

Pre-built workflows aligned to
NIST AI 600-1 GOVERN,
EU AI Act, ISO 42001 and other Global regulations

AI models life-cycle management and governance

AI Security + Watsonx.Gov

Exchange information on model discovery to support model lifecycle management.

IBM Guardium AI Security (SaaS)

MSP Services Catalogue

AI Discovery Assessment

Assessment Service (One time)

Automated discovery for AI deployments:

– Enabling organizations to identify AI use cases, including shadow AI running in the organization

Detection of AI vulnerabilities and misconfigurations

– Allowing organizations to identify vulnerabilities in AI use cases and map them to common assessment frameworks (OWASP, MITRAE, NIST etc.)

Risk scoring and Recommendations

– Provide your security expertise to the customer to prioritize the identified AI vulnerabilities and misconfigurations.

AI Security Services

Managed Services

Discovery and Continuous Monitoring of AI deployments

– Cloud Accounts on-boarding
– Comprehensive discovery of AI assets in code repositories, cloud workloads to identify shadow AI.
– Visibility on AI deployments across multi-cloud and multi-vendor services.

AI Security Posture Management

– Detect and fix security vulnerabilities and misconfigurations with automated penetration tests
– Assign and initiate auto remediation tasks as per the priority and risk scoring.
– Map the vulnerabilities to assessment frameworks like OWASP Top 10, NIST RMF etc.
– Safeguard model Integrity and authenticity.

AI Gateway

- Runtime protection of AI models and applications.
- Secure the prompts by configure the proxy
- Restrict un-authorized inputs / outputs.

AI PenTest Services

Managed Services

AI Posture Services

– Develop ML and LLM's inventory for Pen testing and Red teaming
– Onboard the required models
– Help prepare strategic roadmap to address critical findings and misconfigurations
– Execute the scans as per the business requirements

Incident Management

– Execute the remediation as per the severity of the Pentest Findings

AI Gateway

Managed Services

AI Gateway Proxy Configuration

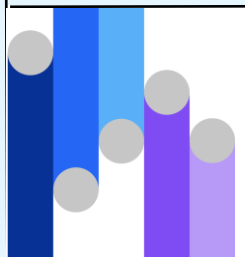
– Onboard the required LLM provider on AI Gateway.
– Assess attack vectors like code injection, code leakage, prompt injection, output tampering, model abuse.
– Identify risks of data poisoning, unauthorized data access for input and output prompts.
– Streamline the response as per business requirements / standards.
– Pre-requisite : Discovery of AI landscape.

AI Compliance (Add-on)

Managed Services

Compliance Configuration

– Perform a Comprehensive AI Security Audit to assess the maturity of current AI systems against prominent libraries (EU AI Act, ISO 42000, NIST AI -600 etc.)
– Leverage IBM's AI Security Framework to strengthen AI security across models, data, and applications.
– Adapt AI systems to meet industry and regional requirements as per evolving regulations.



What MSP Can Accomplish

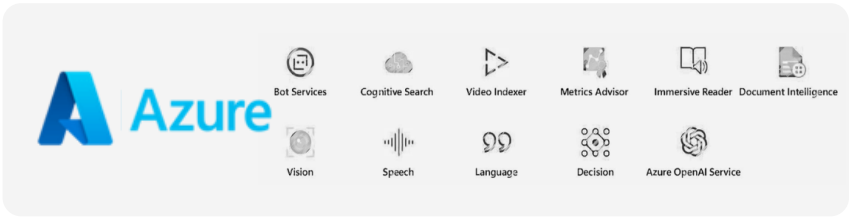
- ✓ Discovery of Shadow AI
- ✓ AI Firewall (Proxy)
- ✓ AI SPM (Pentest, Code Scan etc.)
- ✓ Accomplish Compliance.

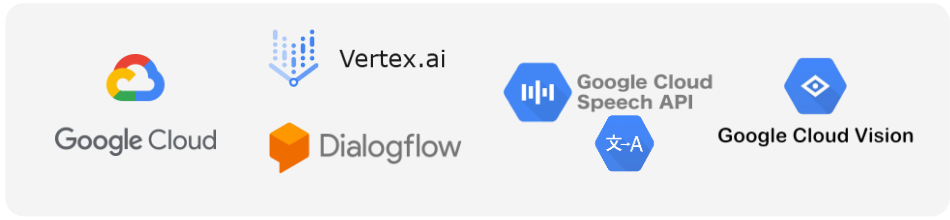
Benefits to customer

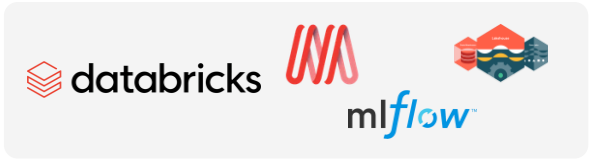
- ✓ Un-interrupted AI Security Coverage
- ✓ Regulatory Readiness
- ✓ Minimize Risk Exposure
- ✓ Trust development into AI

Supported platforms

AI Platforms







LLMs

ML Frameworks, Vectors DBs, and more

Pricing and Packaging

Guardium AI Security

Primary Parts

Part	Name	Purpose	Metric
D111CZX	IBM Guardium AI Security Subscription permonth	Discovery of AI assets including shadow AI, protecting AI models and endpoints (AI SPM, AI Pentest, AI Gateway)	Application
D111EZX	IBM Guardium AI Security Audit Assistant Add-on	Collecting compliance evidence to report on	Application
D0R6TZX	Configure & Assist Guardium (SaaS)	Base implementation plan from TEL	Services

Counting Logic

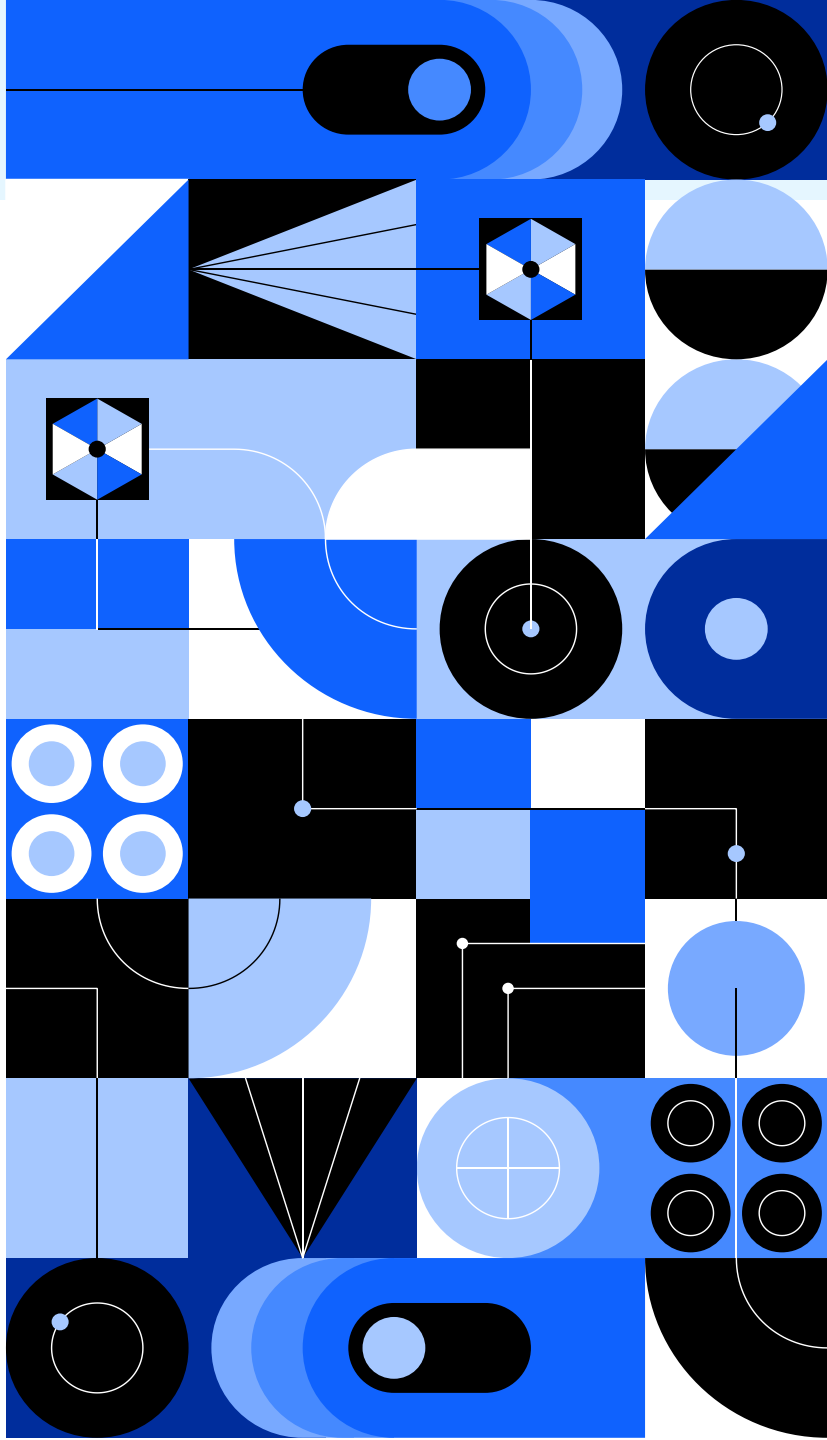
An AI Use Case (also, AI System) is an application developed by an application team and owned by a single business owner. If it serves one business goal, has one stakeholder, and delivers one type of AI -powered outcome, it's one AI Use case (AI system)
—and that's what we count and price. (ref : How to count AI Use case)

Unified Taxonomy

Part Code (D111CZX)	UT Codes	
	UT 30	UT 35
Guardium AI Security	UT30AUW	UT35AAN

Details

- Available as a SaaS subscription part
- Charge metrics: Application (AI use case/project)
- Max discount allowed by OEM is 20%
- Min term: 12 months
- #Emp Base : Assumption has been made to baseline the organization size across T-shirt sizing.
- *Pricing is list price in USD as on June '25. Please user IBM Quoting tool for latest pricing
- 80 Hours mandatory expert lab efforts.
  Link to AI Security Sales Kit and IBM Quoting Tool




IBM