WSO2CON AFRICA

SEPT 22 – 24, 2026 | NAIROBI, KENYA

From Regulatory Burden & Traditional Security to Strategic Advantage

Nevi Amunugama

VP & CISO
WSO2

What we'll cover today

01 **Introduction - WSO2 Security & Compliance**
Brief Overview of the function

02 **The Old Paradigm - Pre AI**
Compliance and security were considered to be an expense, gatekeepers and slowed down innovation.

03 **The AI Inflection Point**
What actually changed around us in regulation and in defense with the introduction of AI

04 **From Burden to Advantage with an Agentic Enterprise**
The journey, the maturity and the value AI adoption can unlock

05 **Getting There**
Guardrails, roadmap, and how you prepare

Introduction to WSO2 Security & Compliance

WSO2

WSO2 Security & Compliance

Innovation is a core value

- Fundamental to everything we do at WSO2.
- We are not just a software development leader. We deliver securely and at scale, open source technology.
- Innovation exists throughout the entire lifecycle of our products & services.
- It drives growth, attracts customers & investors, and established us as a leader in the market .

WSO2 Security & Compliance:
https://wso2.com/security/

WSO2

The WSO2 Approach

It's all about the balance!

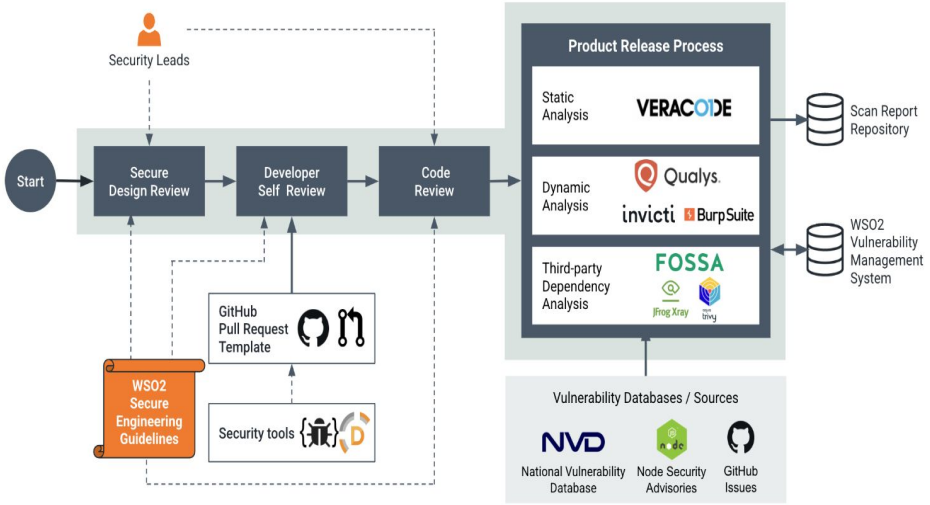
- Changed the perception and traditional ideology:
  - *"Security & Compliance does NOT slow down innovation"*
- Encourage adoption of new technologies,
  - A secure & governed agentic experience is NOT a risk
  - Innovation & flexibility can be achieved
- Security & compliance are building blocks of products and services which allows,
  - Stronger "Go To Market" strategy
  - Maintain customer confidence
  - Align with more customer needs.
- Maintain a healthy balance between security, operational, legal and business requirements.

WSO2

WSO2 Security

Secure Software Development Process (SSDLC)

Security is not an afterthought at WSO2. It's an integral part of each phase in the development life cycle. This ensures that security vulnerabilities are identified and mitigated as early as possible.



Secure engineering

01

Secure software development process

Security built into every phase of the lifecycle, from design through release and beyond.

Explore Process →

02

Secure engineering guidelines

Secure engineering practices for safer development throughout the lifecycle.

Explore Guidelines →

03

Secure deployment guidelines

Security guidelines and recommendations to deploy WSO2 products.

Explore Guidelines →

Vulnerability management

Vulnerability management

Program for continuous vulnerability management across all products and services.

Explore Program →

Responsible disclosure

Program for reporting vulnerabilities, with recognition and rewards for qualifying submissions

Explore Program → Report Security Issues →

Security announcements

Security advisories

Information on vulnerabilities affecting our products and services.

View Advisories →

Cloud security bulletins

Information on vulnerabilities affecting our cloud products and services.

View Bulletins →

CVE justifications

Justifications for non-impacting CVEs associated with our products and services.

View Justifications →

Incident clarifications

Analysis of widely discussed security events.

View Clarifications →

WSO2 Compliance

Global compliance

Independently audited certifications, attestations, and built-in capabilities to support global compliance and standards.

ISO 27001:2022 Certified

SOC 2® Type 2 Compliant

PCI DSS Certified

GDPR Compliant

CCPA Ready

DORA Compliant

HIPAA Compliant

OpenID® Certified™

Data privacy and protection

Transparent privacy and data protection resources to help you understand how your data is handled, protected, and governed.

View Data Privacy and Protection Details →

Laws/Regulations

African Union - African Union Convention on Cyber Security and Personal Data Protection, 2014 — View Details →

Egypt - Personal Data Protection Law No.151 of 2020 — View Details →

Ghana - Bank of Ghana Cyber & Information Security Directive, 2018 — View Details →

Ghana - Data Protection Act, 2012 — View Details →

Kenya - Central Bank of Kenya (CBK) Guidance Note on Cybersecurity, 2017 — View Details →

Kenya - Data Protection Act, 2019 — View Details →

WSO2

https://wso2.com/security/

The Old Paradigm - Pre AI

WSO2

The Old Paradigm - Pre AI: Built for defence, not for offence

Compliance and Security were considered to be an expense, gatekeepers and slowed down innovation.

Reactive
Risk is identified mostly after the fact — security reviews, audits, incident reports, breach post-mortems had some automation, but lacked scale that only AI could provide.

Slow to adapt
New regulation or a new attack pattern can take months to review, assess applicability & operationalize.

Manual & paper-heavy
Spreadsheets, templated populated, email trails, and point-in-time evidence collection was collated, but mostly manually.

Time and effort spent on coordination, follow-ups, status updates etc between teams and auditors was also very manual.

Pure cost center
Budgeted purely to avoid fines and breaches — It was difficult to create value, increase savings and reduce cost without agentic solutions.

Siloed
Legal, IT security, and Compliance teams work from separate systems and definitions. Teams often seen as blockers and not partners. Now you have far greater collaboration built in with AI based solutions.

WSO2

The Old Paradigm - Pre AI

Prior to AI driven,

- **Security & Compliance reviews were manual. Risks could be missed.**
- **Detection had automation built but still process heavy.**
- **Budget concerns have always been a focus**
- **Investment in Security & Compliance (resource & time) impacted growth in other areas.**

279
Days

Average breach detection & containment time in the most heavily regulated sectors (healthcare)

35% +

Of manual GRC audit workload that AI-era platforms are now built to remove

4.9 M

Average cost of breaches driven by malicious insiders — the most expensive attack vector

Source: IBM Cost of a Data Breach Report 2025 (Ponemon Institute)

The AI Inflection Point

WSO2

The AI Inflection Point

What actually changed in regulation and defence - Compliance has moved from periodic to continuous

Continuous control monitoring	24/7 scanning replaces point-in-time audits, catching drift the moment it happens instead of months later.
Predictive risk scoring	Models can flag the likelihood based on the publicly available breach notifications and exploits.
Natural-language regulatory, certification & attestation intelligence	AI reads new rules, controls & requirements as they publish and maps them directly to existing controls and policies.
Automated evidence collection	Audit trails assemble themselves in the background, cutting weeks of prep, coordination and follow up efforts to hours.

WSO2

The AI Inflection Point

The Security Journey / Make it measurable - Organizations have moved from mostly Reactive to largely Proactive & Adaptive

Faster detection & containment	AI-enhanced tools cut the time between intrusion and containment from months to weeks. Dynamic reporting which allows tailor-made, audience specific reports/dashboards etc.
Automated triage	Machine learning ranks alerts by real risk, so analyst hours can be used more efficiently.
Anomaly detection at scale	Behavioral baselines can catch novel attacks that signature-based tools were built to miss.
Adaptive defense	Defenses retrain on new attack patterns automatically, closing the gap with AI-powered attackers.

WSO2

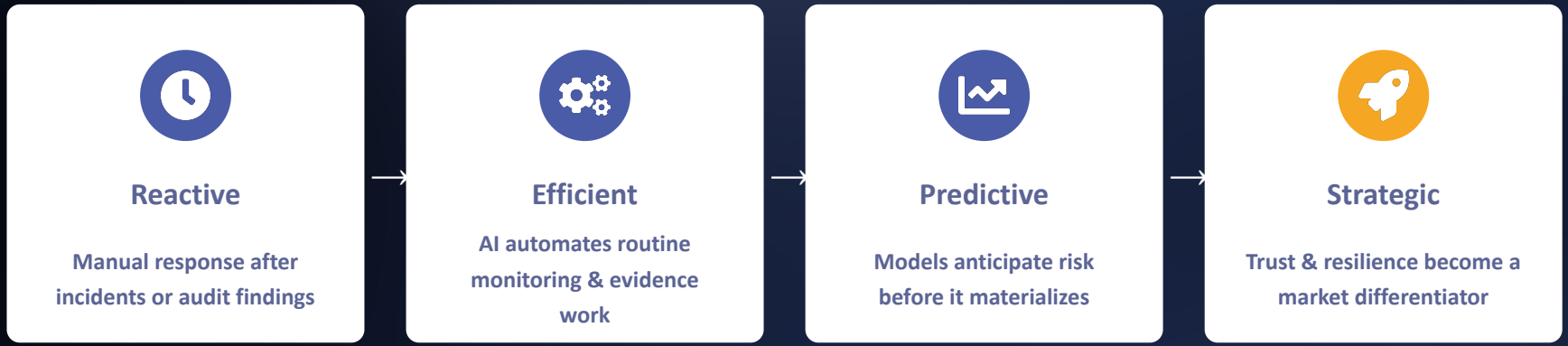
From Burden To Advantage

WSO2

From Burden To Advantage

The journey, the maturity and the value AI unlocks

Not just about reducing risk. Organizations need to optimize cost & readiness for what we anticipate next to execute effectively and efficiently



WSO2

Strategic Advantage with AI - Looks Like?

How AI is turning Regulatory Compliance & Security into a strategic growth engine across industry.

Faster time-to-market

New products and markets clear compliance review in days, not quarters.

Trust as brand equity

Demonstrable security posture & governance becomes a differentiator in RFPs and enterprise sales.

Capital reinvested

Budget freed from manual review funds product and growth instead.

Innovation velocity

Teams ship AI and data products confidently, with guardrails built in. Move from experimental to true impact.

M&A readiness

Continuous evidence means due diligence is a formality, not a scramble.

Board-level visibility

Real-time risk posture replaces quarterly snapshots in the boardroom.

WSO2

Old Paradigm (Prior to AI) vs Today (AI Enabled)

	The Old Paradigm	AI-ENABLED
Posture	Defensive — avoid fines & breaches	Offensive — enable growth safely
Cadence	Point-in-time audits, annual reviews	Continuous monitoring, real-time scoring
Evidence	Manually assembled, weeks of prep	Auto-collected, always audit-ready
Detection	Mean time to contain: 240–280+ days	Compressed by up to ~80 days with AI
Budget framing	Sunk cost of doing business	Investment with measurable ROI

WSO2

WSO2 Security

Agentic Enterprise

WSO2's shift from traditional compliance & security to AI enabled competitive advantage.

Not experimental anymore, but true AI adoption.

01 Delivering Compliant Product & Services leveraging AI

02 Ensure Data Security & Regulations are met with Agentic strategy

03 Approach Cybersecurity in the age of AI - For example Mythos

04 Security efficiency in an Agentic Enterprise

05 Security Training Refocus with AI

06 Risk & Compliance Platform initiatives that use AI

07 Incident Management - Detection and response readiness strategy

Getting There

WSO2

Getting There

Strategic advantage - Requires Guardrails, Governance, roadmap and a plan.

Shadow AI

Unsanctioned tools create blind spots outside existing access controls.

Data quality

Predictive models are only as good as the compliance and security data feeding them.

Human oversight

High-stakes decisions still need an accountable reviewer, not just a model score.

Explainability

Regulators and auditors expect to know why a model flagged — or cleared — something.

AI cuts both ways — 63% of organizations still lack formal AI governance policies, and ungoverned "shadow AI" was a factor in 1 of 5 breaches in 2025.

Source: IBM Cost of a Data Breach Report 2025 (Ponemon Institute)

WSO2

Getting There

Strategic advantage - Achieve reasonableness with practical approach.

1	**Baseline your posture**	Map current compliance & security workflows against a baseline target
2	**Target high-cost workflows**	Pick the most manual, most expensive & most error prone process — evidence collection or alert triage are common starts.
3	**Pilot with governance from day one**	Pair the AI pilot with an oversight owner, an audit log, and an explainability standard.
4	**Reinvest the savings visibly**	Redirect freed budget, resources and hours into a growth initiative the organization can see and measure.
5	**Scale & report to the board**	Move from quarterly snapshots to a real-time risk and resilience dashboard.

WSO2

Got There!

The Burden - It was never about regulation, compliance or security…It was about manual overhead, scale & volume

- Effective AI implementations successfully reduces detection, response, and audit cycles from months to hours.
- Time, effort & errors recovered from manual review can be re-invested in growth.
- Governance is what converts AI adoption into durable advantage, not new risk.

Questions?

WSO2

WSO2CON AFRICA

SEPT 22 – 24, 2026 | NAIROBI, KENYA

Thank You!

Nevi Amunugama

VP & CISO
WSO2