SENTINELX

AGENTIC ENFORCEMENT SQUAD FOR SECURITY OPERATIONS

SentinelX is an autonomous enforcement squad that investigates security incidents, classifies risk, and executes real-time containment actions — locking down breaches in seconds with full compliance audit trails.

PROBLEM :

➤ **In Big enterprises, thousands of security alerts happen every day:**

1. Someone tries to hack a login
2. API keys get leaked
3. SQL injection attempts occur
4. Strange device or geo-location logins appear
5. Suspicious file downloads happen

Normally... Human SOC analysts must investigate these incidents manually.

That means:

1. 4–8 hours per incident
2. Severe alert fatigue
3. Many real attacks get missed
4. High financial + compliance risk

➤ The Problem :

Security teams don’t fail because they lack tools ,they fail because enforcement is too slow.
Most systems only detect and alert, but do not act immediately.

Enterprises need an autonomous enforcement workflow, not just another dashboard.

SOLUTION : SENTINELX SQUAD ENFORCEMENT

- **SentinelX is not another SOC dashboard.**
- **It is an autonomous enforcement workflow built on IBM watsonx Orchestrate.**

Instead of humans spending hours triaging alerts, SentinelX executes a full agentic loop:

Detect → Investigate → Decide → Enforce or Respond → Audit

1. Transforms all security logs into actionable intelligence
2. Produces an authorized security verdict
3. Enforces lockdown actions immediately
4. Documents every action for governance and compliance

- **The Game-Changer: Enforcement Authority**

Most security AI systems only say: "This looks suspicious."

SentinelX has standing authority to act:

- ✓ Lock compromised accounts
- ✓ Revoke stolen tokens
- ✓ Block hostile IPs
- ✓ Auto-generate audit + Jira ticket

SentinelX turns AI from advisor into SOC enforcer.


IBM watsonx Orchestrate
SENTINEL DETECTIVE
THREAT JUDGE
ENFORCEMENT OFFICER
COMPLIANCE CLERK
RISK SCORE: 85
ANOMALIES DETECTED
TARGET: user_id_123
KILL-SWITCH EXECUTE
AUDIT EVIDENCE RECORD
SENTINELX COMMANDER
THE SENTINELX AGENTIC SECURITY SQUAD

THE SENTINELX AGENTIC SECURITY SQUAD

IBM watsonx Orchestrate

SENTINEL DETECTIVE
(Evidence Extractor)

- ★ Ingests raw logs
- ★ Detects anomalies

THREAT JUDGE
(Verdict Authority)

- ★ **AUTHORIZED BREACH RESPONSE**
- ★ **ELEVATED** THREAT
- ★ **CLEARED**

SENTINELX COMMANDER
(Orchestration Brain)

IBM watsonx Orchestrate

DETECT → DECIDE → ACT → DOCUMENT

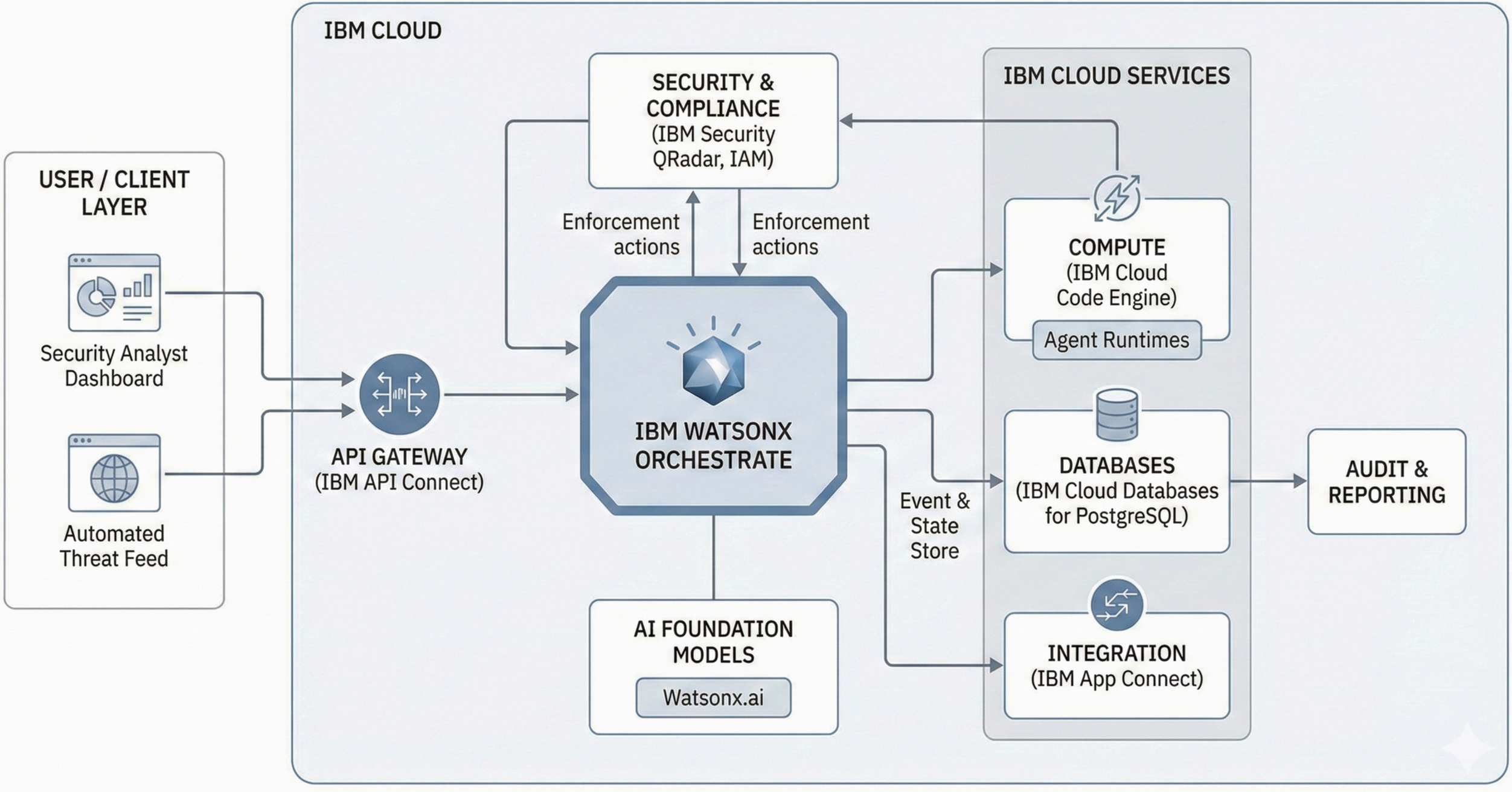
ENFORCEMENT OFFICER
(Kill-Switch Agent)

- ★ Revokes tokens
- ★ Locks accounts
- ★ Blocks IPs

COMPLIANCE CLERK
(Audit Closure Agent)

- ★ Creates audit report
- ★ Files Jira ticket
- ★ Provides traceability

THIS IS NOT A CHATBOT.
THIS IS AN AUTONOMOUS ENTERPRISE ENFORCEMENT WORKFLOW.


IBM CLOUD
USER / CLIENT LAYER
Security Analyst Dashboard
Automated Threat Feed
API GATEWAY
(IBM API Connect)
SECURITY & COMPLIANCE
(IBM Security QRadar, IAM)
Enforcement actions
Enforcement actions
IBM WATSONX ORCHESTRATE
AI FOUNDATION MODELS
Watsonx.ai
IBM CLOUD SERVICES
COMPUTE
(IBM Cloud Code Engine)
Agent Runtimes
DATABASES
(IBM Cloud Databases for PostgreSQL)
Event & State Store
INTEGRATION
(IBM App Connect)
AUDIT & REPORTING

WHY IBM WATSONX ORCHESTRATE + ENTERPRISE IMPACT

Why IBM Matters (Not Optional Tools)

➤ SentinelX is built around IBM watsonx Orchestrate because security enforcement requires:

1. Trusted enterprise orchestration
2. Agents must coordinate actions across IAM, SOC tools, and audit systems.
3. Tool execution with governance
4. Orchestrate allows agents to trigger real workflows — not just generate text.
5. Multi-agent delegation at scale
6. Detect → Judge → Enforce → Document happens as a structured pipeline.
7. Compliance-first automation
8. Every action is logged, ticketed, and traceable (SOC-ready).

Business Impact (What Changes)

➤ SentinelX converts security response from manual to autonomous:

1. From 4–8 hour manual triage → sub-10 second autonomous enforcement
2. Critical incidents neutralized instantly, not just flagged
3. Compliance closure generated automatically (ticket + evidence trail)
4. Analysts regain time by removing repetitive alert investigations
5. Attacks contained early — before data loss or disruption begins