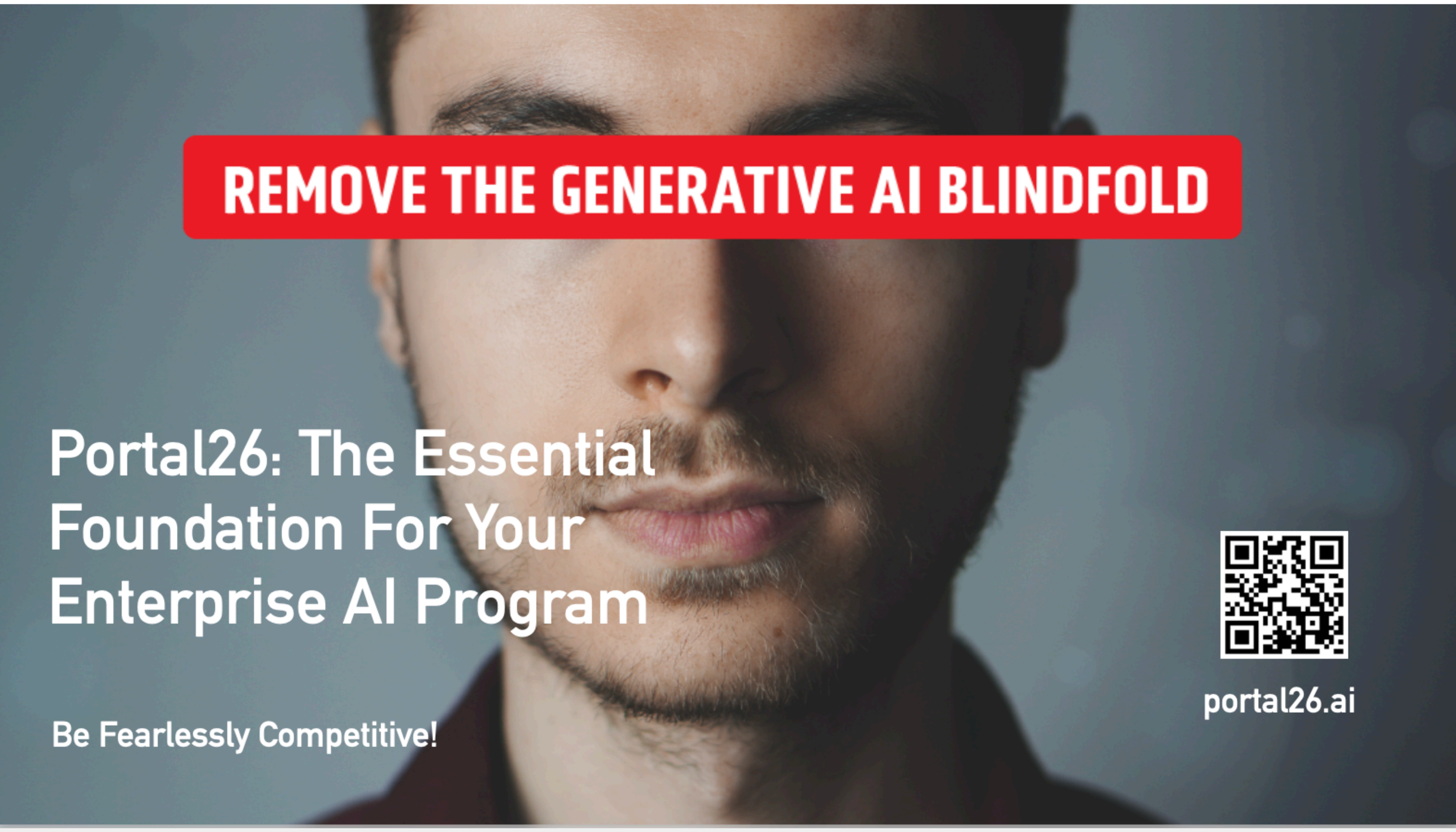


The Portal26 AI TRiSM Platform Provides Invaluable GenAI Visibility and Insight While Mitigating Critical Enterprise Risks

The GenAI Genie has left the proverbial bottle! Employee productivity as well as business flows are rapidly evolving. As the use of generative AI has skyrocketed, companies are finding that there is minimal visibility into who is using generative AI and for what purpose. In addition, widespread and unmonitored generative AI usage has introduced legal, data privacy, intellectual property, and compliance risks that are challenging to monitor and mitigate.

Even as employees are untrained on GenAI tools and policy, IT and security teams are faced with “Shadow AI” which is growing fast and can be dangerous. Security teams are unable to investigate generative AI related incidents, and business teams have no tools by which to discern the true impact of generative AI on productivity and process.

For these reasons it is urgent and important for organizations to implement governance, risk management, and appropriate guardrails for employee use of generative AI.

The Portal26 AI TRiSM (AI Trust, Risk, Security Management) addresses the above concerns by enabling enterprises to both gain visibility into usage and also to create and enforce generative AI governance policies that mitigate compliance, IP, privacy and other related risks. Further, Titaniam supports employee education by usage based policy distribution and also supports security investigations by connecting GenAI to the broader security stack.

Contact us at: info@portal26.ai Visit us at: https://portal26.ai

Enterprise GenAI Challenges

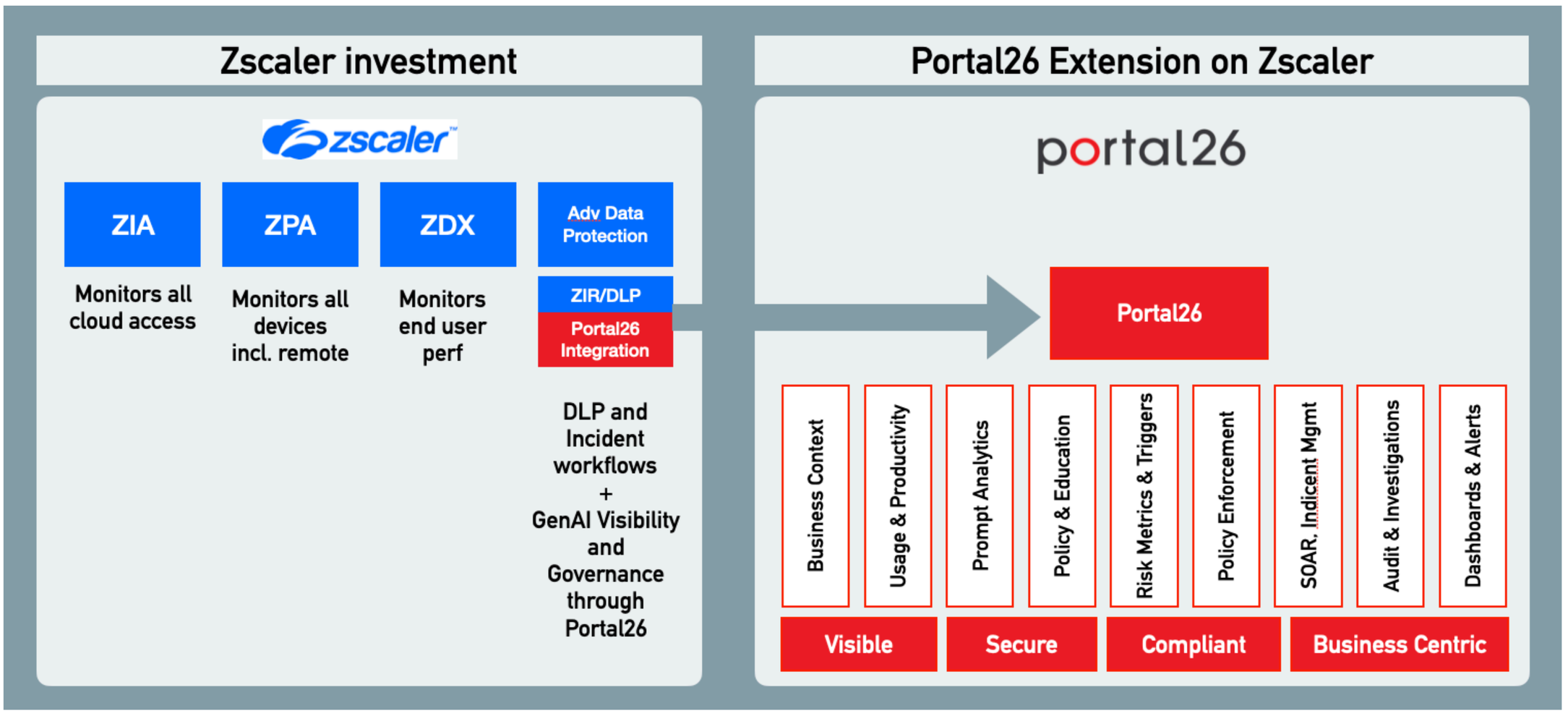
- Too visibility to who is using GenAI and for what
- Productivity and business flows are evolving
- Transparency is critical and as yet non-existent
- Employees are untrained but adopting GenAI fast
- External exposure is massive: IP/Compliance/Security/ Data Privacy
- Security teams are ill-equipped to monitor or investigate and cannot safely enable

Portal26 Solution

- Eliminate Shadow AI
- Observe, audit, and investigate
- Analyze usage, prompts, and productivity
- Create, educate, enforce policy
- Measure and Mitigate GenAI risk
- Deliver security, privacy, and compliance
- Understand GenAI impact on business and enable responsible adoption

Seamless Extension for Risk-Free GenAI Adoption

Extend your existing security investments for network monitoring and DLP, your SIEM and SOAR, incident management, alerting, and notification. Titaniam seamlessly connects enterprise GenAI into your security stack so that security can become an efficient enabler for risk-free GenAI adoption across the enterprise



1. Configure Gateway to connect to Portal26
2. Get immediate ROI via instant and real-time usage, prompt, productivity, and data privacy analytics
3. Leverage existing DLP, SIEM, and Email to create guardrails, enforce security and privacy controls
4. Create and manage GenAI risk scorecards and GenAI usage policies
5. Create compliance, audit, and governance artifacts regarding responsible use of GenAI
6. Create and enforce security and privacy policies
7. Define, refine, distribute and train against GenAI acceptable use policies
8. Enable GenAI related look backs and investigations
9. Gain insight into usage and productivity patterns to enable efficient business process to leverage GenAI
10. Maintain regulatory compliance
11. Easy onboarding via pre-built integrations

Contact us at: info@portal26.ai Visit us at: https://portal26.ai

Enormous Benefits from Incremental Investment

Portal26's AI TRiSM Platform allows enterprises to manage GenAI Risks by gaining visibility into GenAI Usage, implementing security and privacy guardrails, enforcing GenAI policy, and enabling GenAI related monitoring and investigations.

VISIBILITY

Get immediate and real-time visibility into GenAI usage, prompts, and productivity

GOVERNANCE

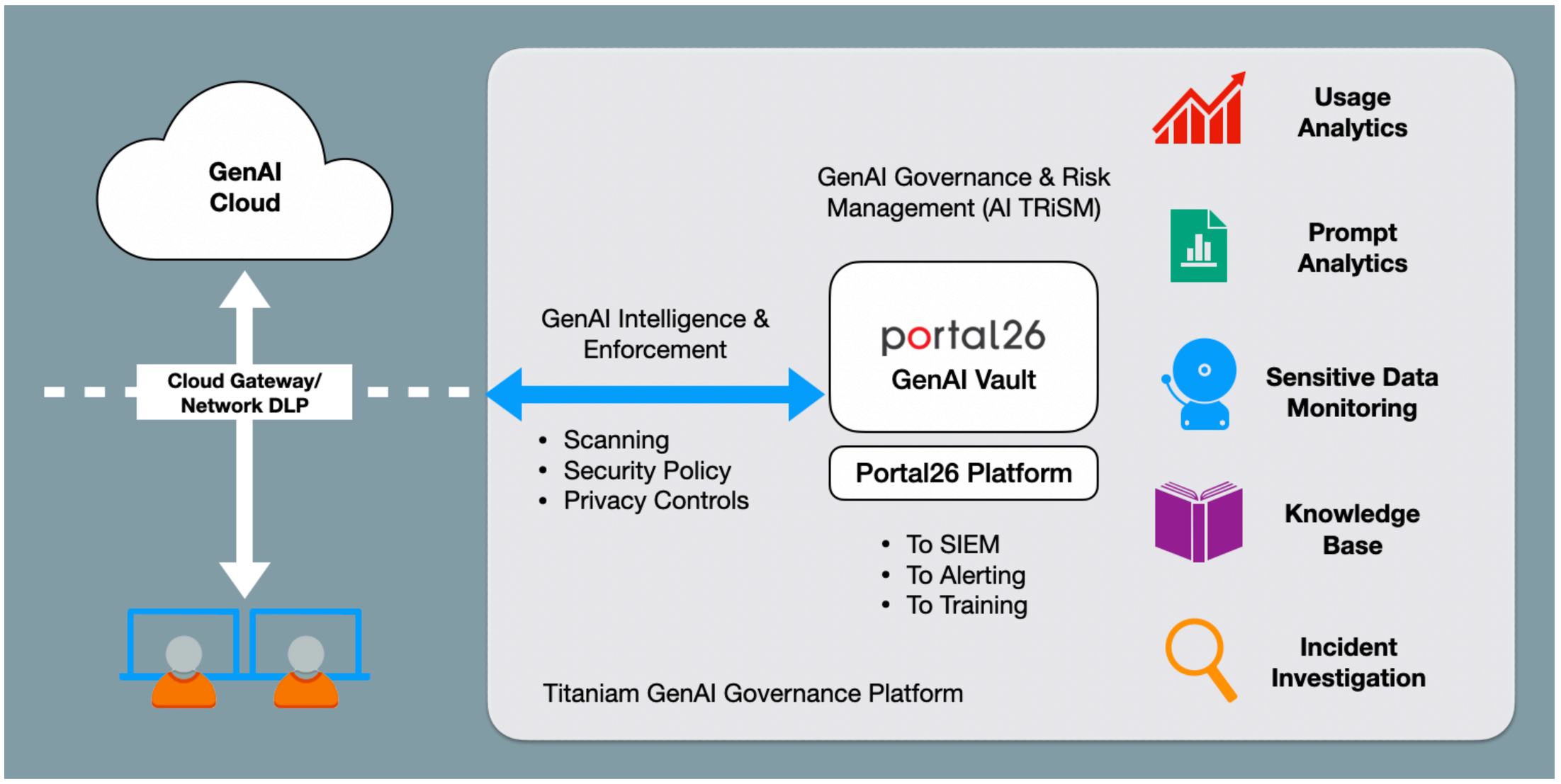
Create and enforce GenAI usage policy. Measure, monitor, and mitigate GenAI risks

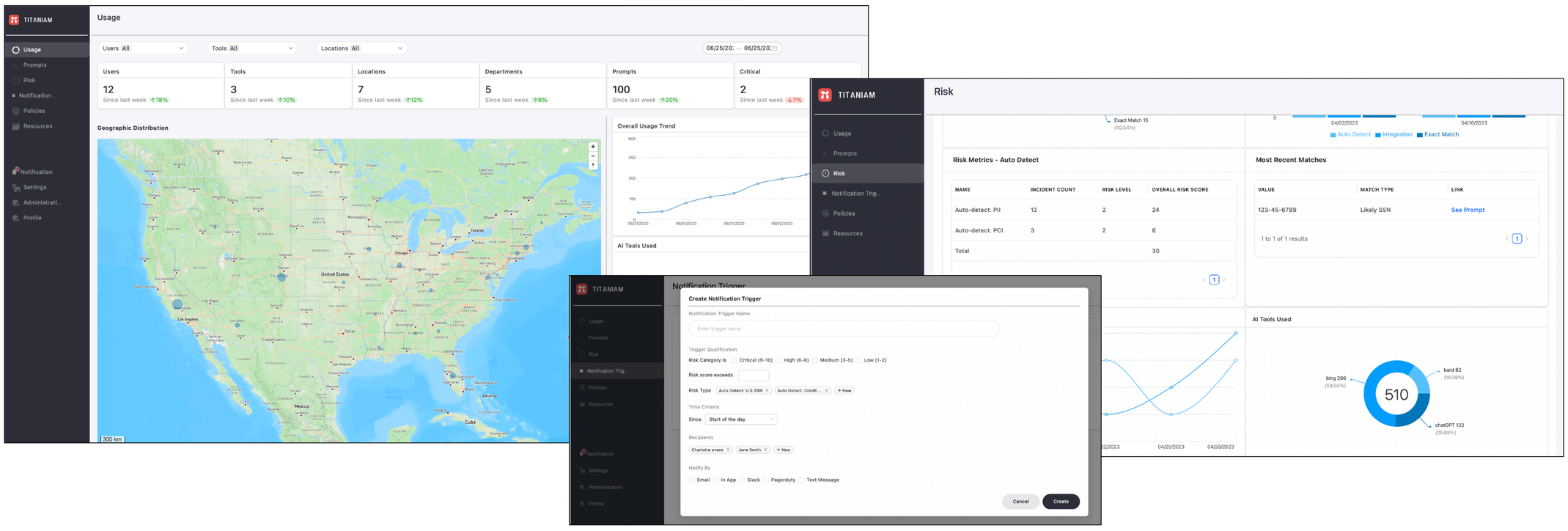
EDUCATION

Educate employees on acceptable use guidelines. Notify/attest based on usage

SECURITY

Implement security, privacy, compliance. Audit and Investigate GenAI incidents





portal26.ai

TRANSPARENCY TO UNDERSTAND. GOVERNANCE TO MANAGE