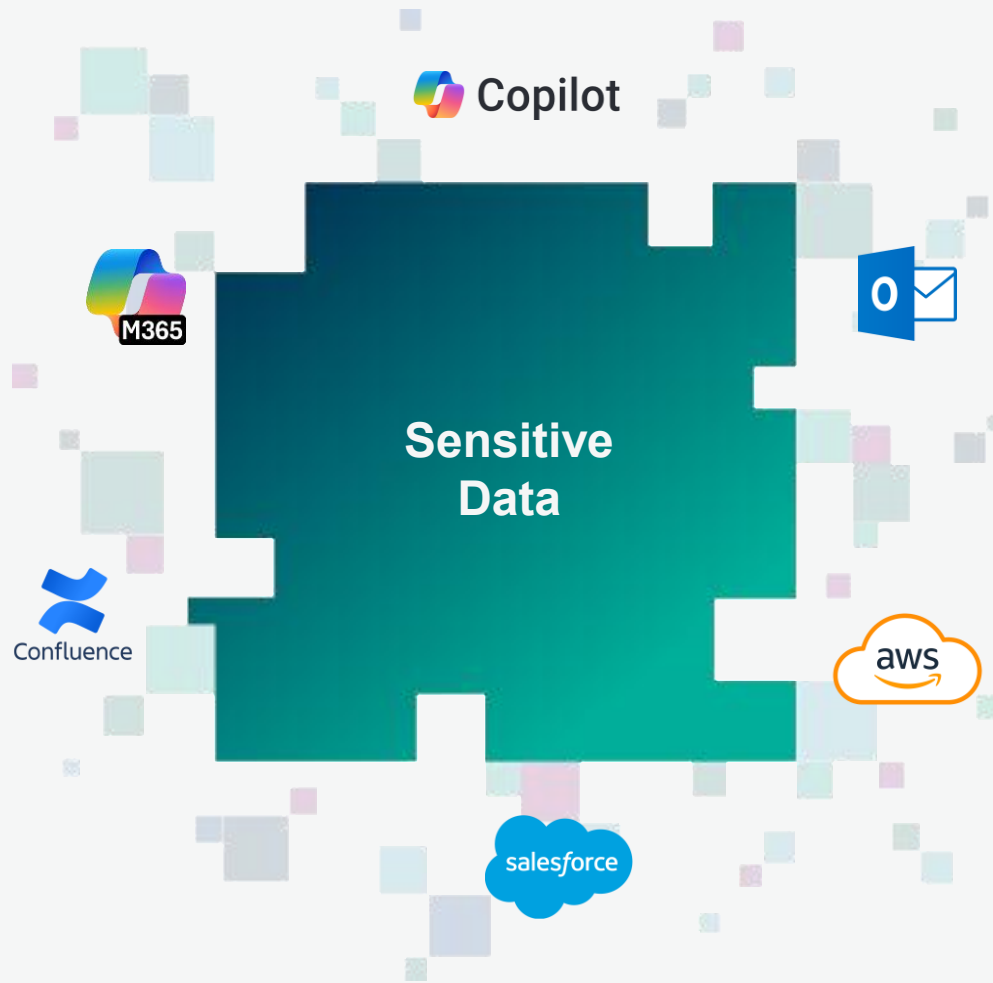




Securing an AI-Powered Business

Kemal ARTIKARSLAN
Se Lead

Evolving Data Landscape



Data Sprawl and Fragmentation

"85% of orgs don't know where their sensitive data lives." – Gartner

Insider Risk

82% of data breaches involve the human element – Verizon DBIR

AI Risk Explosion

"Data leakage remains the top threat. Close behind, however, is the insider threat supercharged by AI" – Marcelo Amaral, CISO, Banco Safra

Governance and Regulatory Pressure

"Regulations evolve fast (GDPR, HIPAA, NIS2, PCI DSS)... need a shift from reactive to proactive data governance." – Enda Kyne, CISO, FBD Insurance

Security Stack Fatigue

"Standalone solutions created inefficiencies and drained resources." – Gabe Guerra, Information Security, Mariner Finance

Sensitive Data Risks Take Many Forms

Access

Can the wrong people/devices/apps get to your data?

Sovereignty

Where is your data?
Is it subject to legal or compliance issues?

Duplication

Are redundant/obsolete copies sitting exposed?



Retention

Is data being kept too long (for compliance, cost, other reasons)?

Over-sharing

Are protections too loose? Can files be shared too easily?

Anomaly

Are there unusual patterns in data access?

A New Data Security Approach is Required



Discover	Classify	Prioritize	Remediate	Protect
Scan and map sensitive data across environment	Intelligent classification with context and sensitivity	Focus on high-impact data based on value, usage, and risk	Automate response to based on risk level and user behavior	Enforce real-time controls to prevent data loss across all channels

Proper data security requires these answers, not as a point in time, they are not sequential, but continuously, across all channels

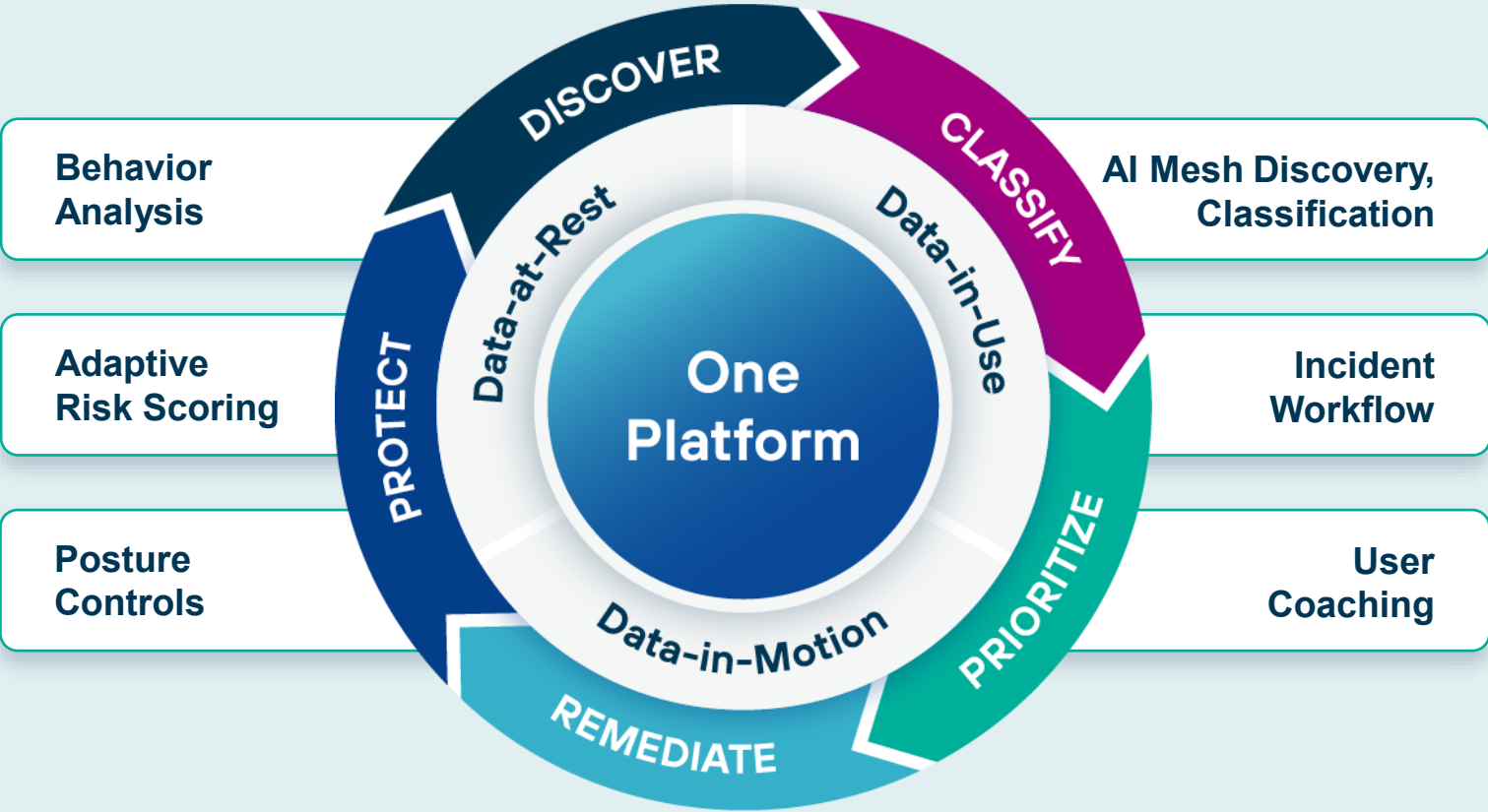
With Forcepoint, Data Security Becomes a Business Accelerator

See and Protect Data Everywhere

Consolidate policies by as much as 90% and automate classification

Safely Enable Gen AI

Innovate and mitigate risks of Gen AI and new tools



Streamline Compliance, Governance

Consistent, reportable visibility and protection across all channels

Consolidate Fragmented Infrastructure

*Reduce Op Ex up to 31%

Securely Enable AI

Unlock AI productivity while mitigating data risks

Securely and confidently enable AI innovation



Shadow AI & managing employee access

See which AI apps employees are using and control access so shadow AI does not introduce risk



Control user interaction

Allow employees to use approved AI apps while stopping sensitive uploads, downloads, and risky prompts



Data access guardrails

Make sure AI assistants can only access approved data while sensitive repositories stay protected



Monitor & report AI usage

Track who, what, and when sensitive data was shared in AI apps to deliver compliance-ready insights

The average company
uses 20-90 unique AI apps
every week

- Forcepoint¹

Business Outcomes

Unlock AI productivity
without risk

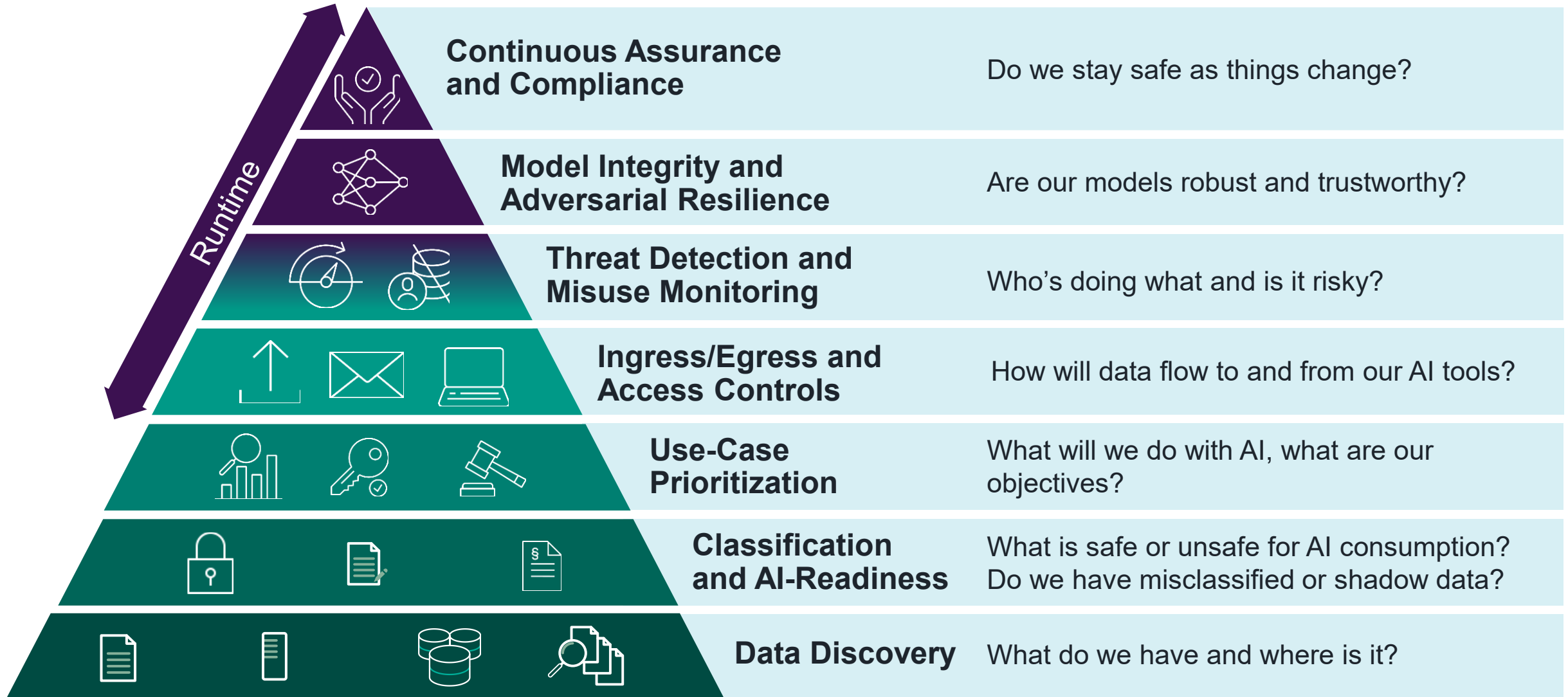
Prevent regulatory
non-compliance

Easily enforce company
policies around AI

Prevent data loss

AI Security Maturity Framework

At Forcepoint we believe organizations should secure AI projects in clear logical phases



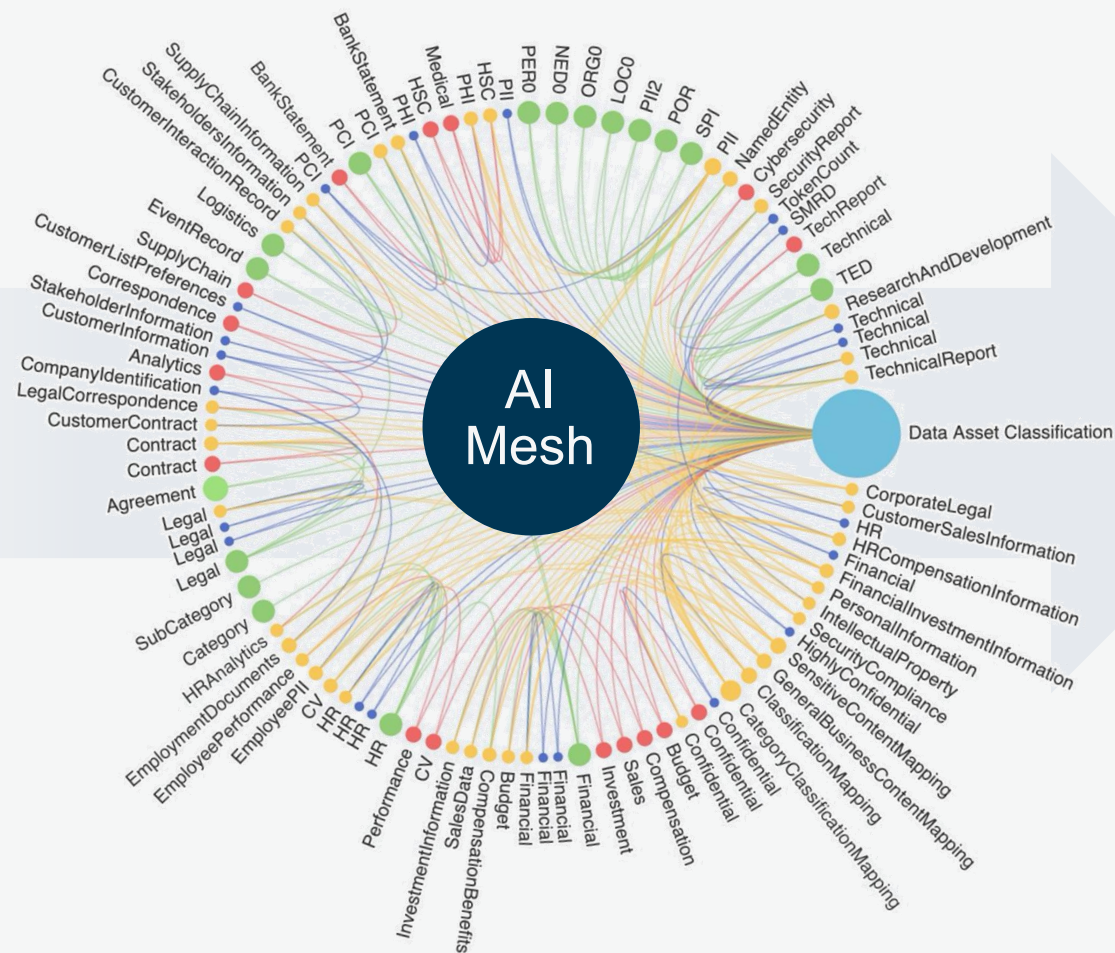
Forcepoint AI Mesh Provides Highest-Accuracy Understanding of Data



Smaller: SLM 10X
smaller than LLM models

Lower TCO: smaller nodes significantly lowers cost

Explainable: Simplifies audit of AI for transparency / trust



AI-powered Accuracy



Speed



Completeness

Example: Giving Visibility Into How People Are Using ChatGPT Enterprise

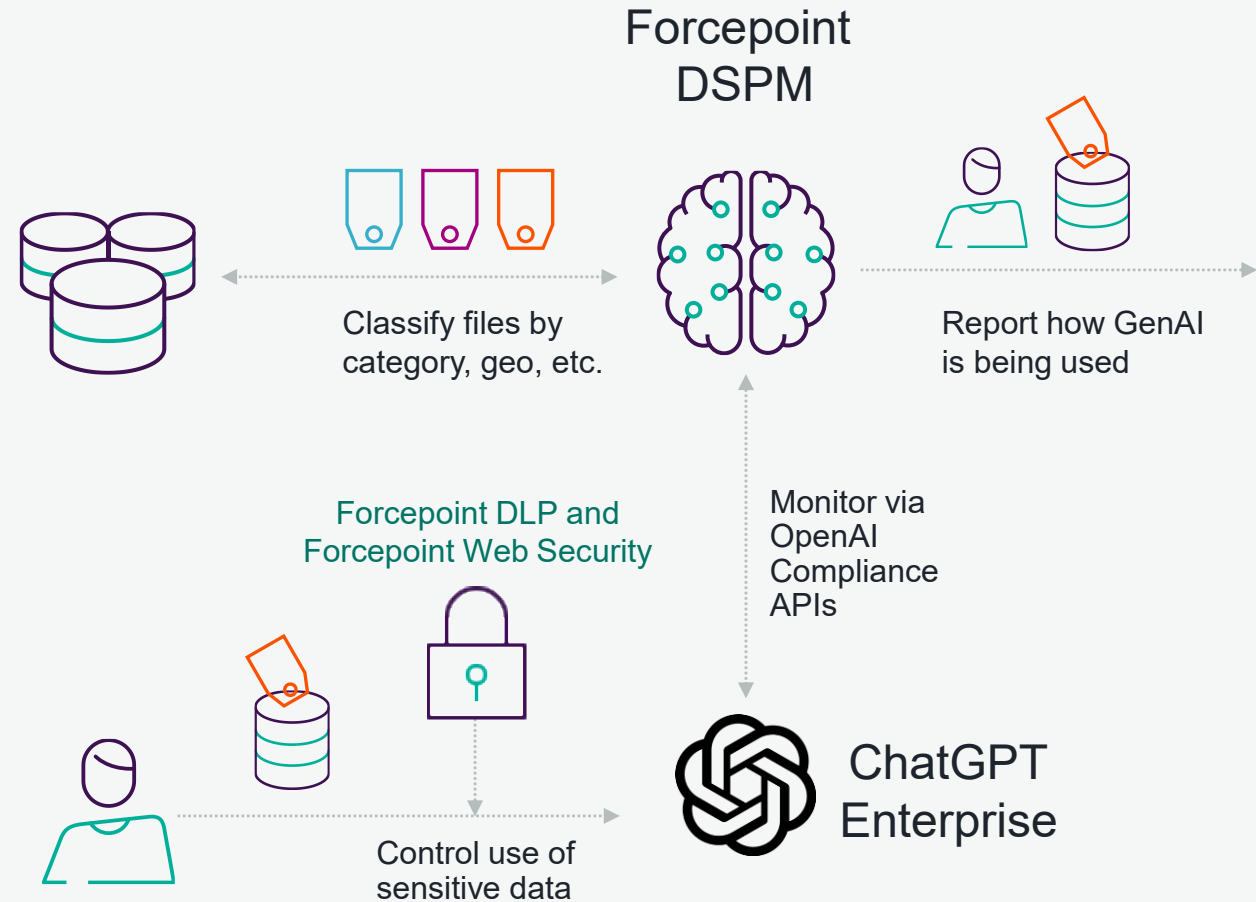
Who is using ChatGPT Enterprise

What prompts are they submitting

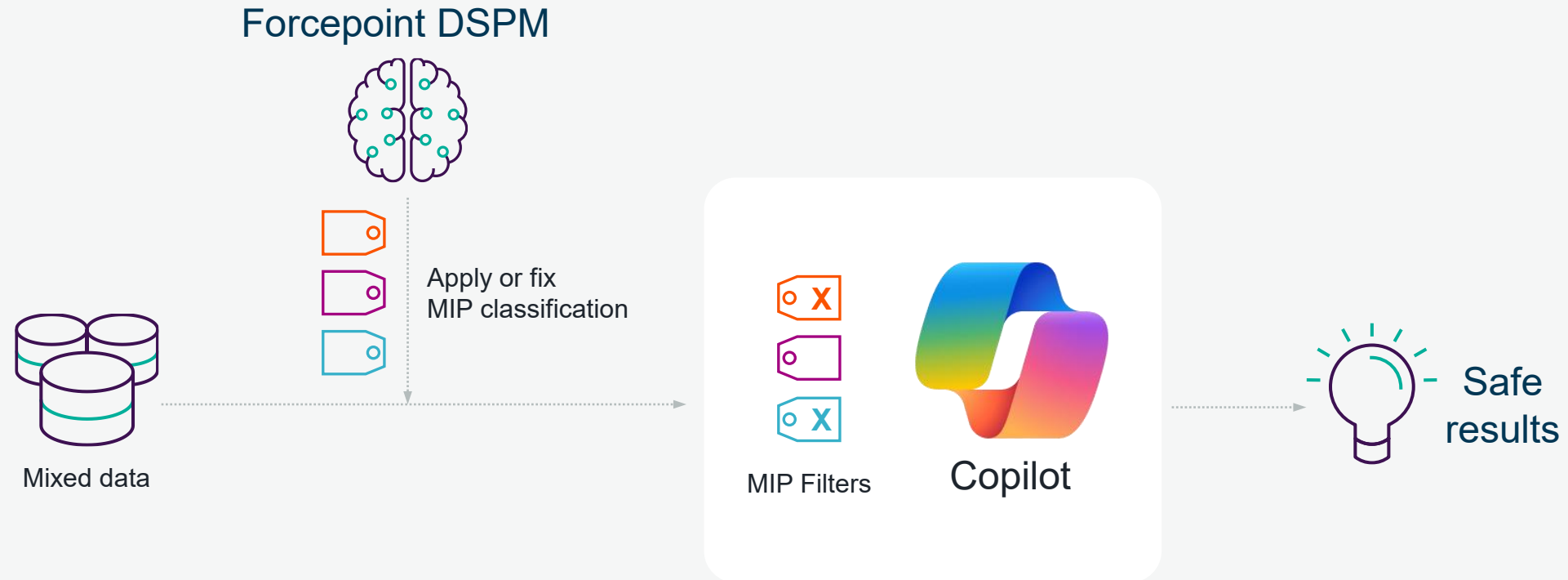
Which files are being uploaded

What risk those files might pose

Are there data sovereignty issues



Example: Controlling What Data Is allowed – or Prohibited – With Microsoft Copilot



High-accuracy, AI-powered classification enables blocking of unauthorized data usage by Copilot

AI Security Dashboards

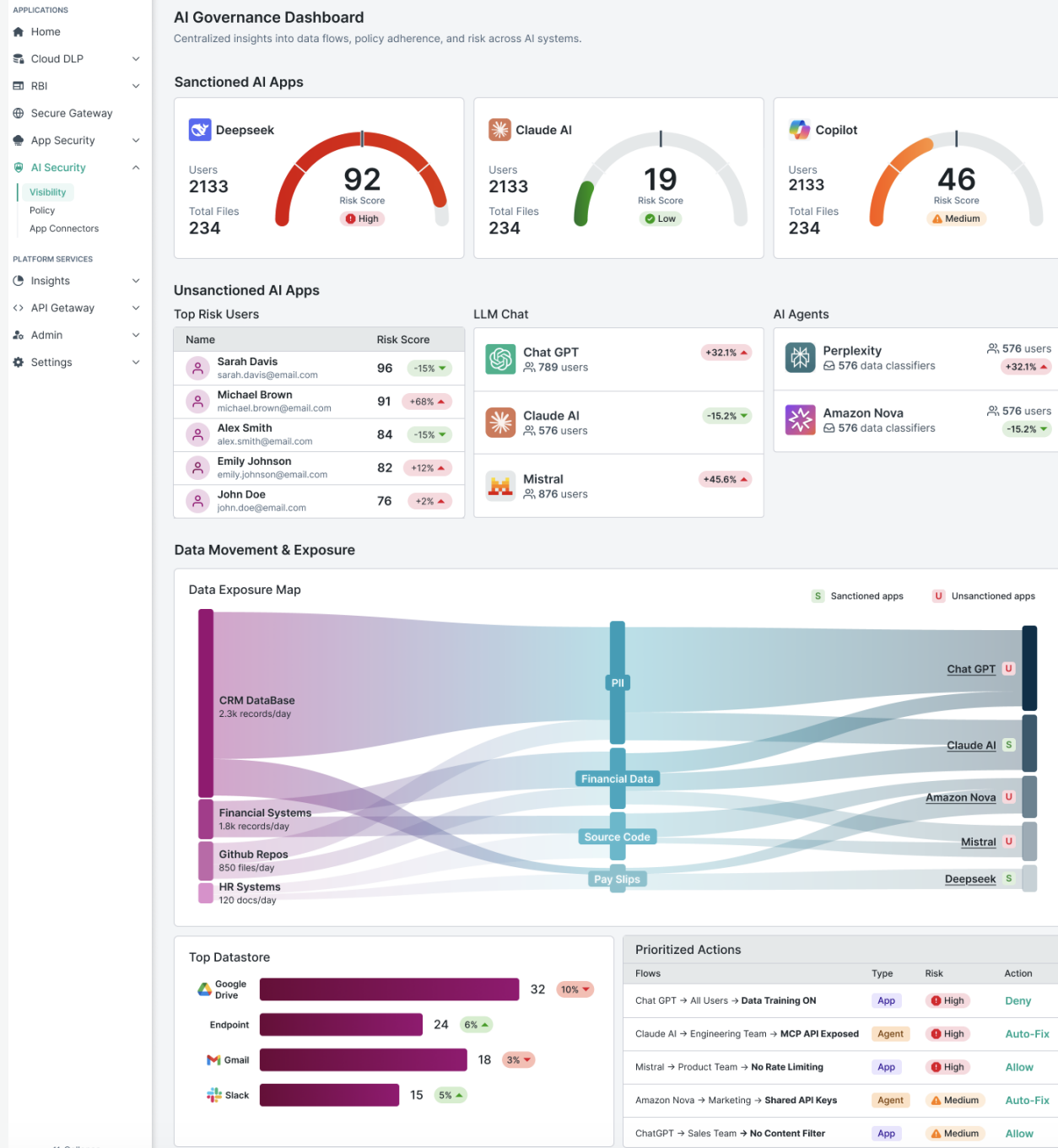
Thin UI layer that creates unified visibility

Unified/Streamlined Experience

- Single-entry point for administrators to view and control AI activity. No need to jump between various products.

Unified Reporting

- Policy audit logs centralized across all enforcement points.
- Event logs from sanctioned and unsanctioned AI apps, aggregated for a unified operational view.



Empower your people and your business with Forcepoint

Forcepoint

Data Security Everywhere

AI | Zero Trust | DSPM | Risk-Adaptive | DLP | Email | CASB | ZTNA | SWG | RBI | CDR | SD-WAN



Increase
Productivity



Cut
Costs



Reduce
Risk



Streamline
Compliance