



WE DO NOT FOLLOW
THE TREND - WE ARE
CREATING IT

Igor Urban
Territory Account Manager



Security that enables
today's global business

"[Forcepoint is] defining wide values, data security, classification, having the appropriate tools to actually monitor what is going on... you have the data in a container that is so well designed and protected, and you have appropriate DLP and access control rules to actually start the learning curve of AI adoption."

– Marcelo Amaral, CISO, Banco Safra

"Forcepoint DSPM and DDR tools have been very much embraced by our teams because they're easy to use, modern, and actually fit for purpose. It's allowed teams to act on real issues."

– Enda Kyne, CISO, FBD Insurance



>
accenture

12,000+
Customers

160+
Countries

30M+
Endpoints
Secured

1700+
Built-in industry
and geo templates

900+
File types
recognized

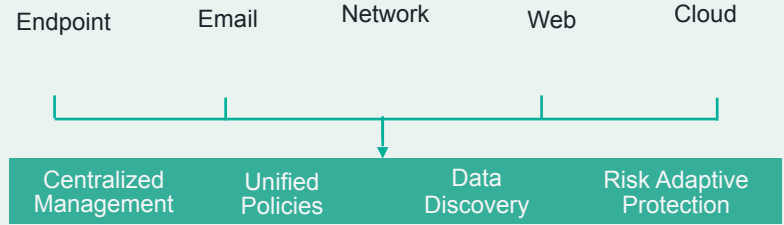
1st
To offer Risk-
Adaptive Policies

1st
Integration with
ChatGPT, Copilot

Data Security

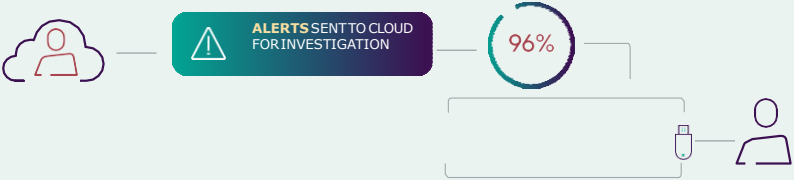
DLP - Data Loss Prevention

The industry's most trusted DLP solution providing sensitive data protection across all channels: endpoint, network, cloud, web & email



Risk Adaptive Protection

Dynamically adjust data protection enforcement based on real-time user risk



DLP for Cloud Email

Precisely monitor & prevent sensitive data loss via external and internal email

Classification / Governance

Leverage AI to deliver highly accurate data classification and/or Data Governance for Forcepoint DLP

Security Service Edge

Forcepoint ONE

Securely connect users to business applications and the web, seamlessly

- ONE cloud-native, Zero Trust platform
- ONE set of policies for web, cloud, apps
- ONE unified way to secure data
- ONE integrated cloud console

Cloud Access Security Broker (CASB)

Enforce access control & data security for cloud apps

- Features**

 - Secure any SaaS application
 - Unmanaged & managed device coverage
 - Shadow IT visibility & control
- Benefits**

 - Apply Zero Trust controls to managed cloud apps
 - Prevent misuse or loss of data from cloud apps

Zero Trust Network Access (ZTNA)

Enforce access control & data security for private apps

- Features & Benefits**
- Secure access to private web apps, SSH, RDP & more
 - Unmanaged & managed device coverage
 - Inline DLP & malware scanning
 - Prevent misuse or loss of data from private apps

Secure Web Gateway (SWG)

Securely connect users to business applications & the web

- Features & Benefits**
- Shadow IT visibility & inline control
 - Endpoint enforcement for up to 2x faster performance
 - Prevent misuse or loss of data on the web

ZT RBI /CDR

Enforce access control & data security for cloud apps

- Features**

 - Zero Trust web browsing isolates all web code from the device
 - Content Disarm & Reconstruction (CDR) for file downloads & uploads
- Benefits**

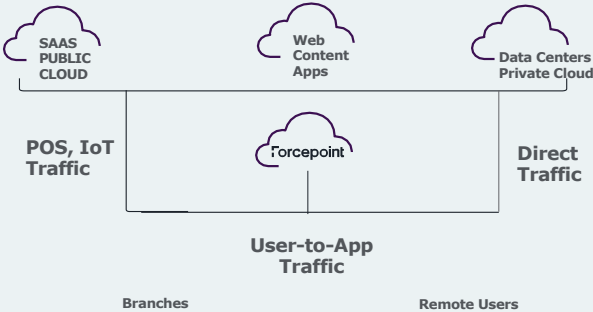
 - Safe interaction with unsafe sites
 - Clean file downloads even from known malicious sites
 - Elevated protection with seamless user experience

Networking (SASE)

FlexEdge Secure SD-Wan

Easily connect & protect branch offices everywhere

Security Service Edge Integration



Next-Generation Firewall

Fast, resilient security for edge & cloud that scales easily

- Features**

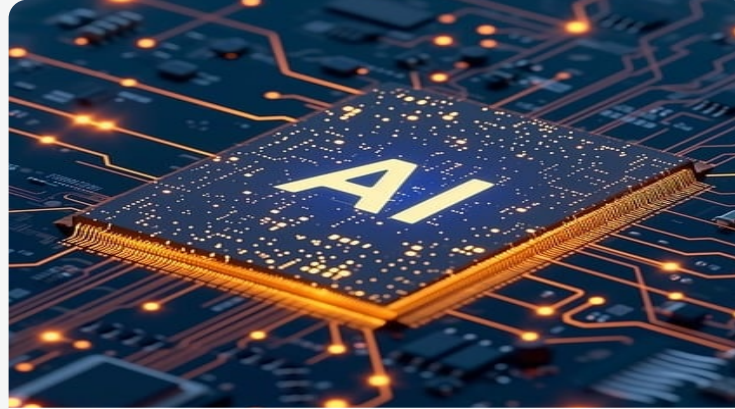
 - Fast anti-intrusion security for edge & cloud
 - Centralized visibility & control of 6000 sites
- Benefits**

 - Safeguard site to site communications
 - Control access to private clouds (AWS, Azure, Google)

Modern Trends Have Increased Data Breach and Compliance Risks



Cloud and hybrid work
have led to data protection
and privacy concerns



Organizational data
can sprawl across SaaS apps,
Gen AI apps and internet



Data
can be accessed from
managed or unmanaged
devices



**60% of the world's corporate
data is stored in the cloud ¹**

¹ [2022 Thales Data Threat Report](#)

**Organizations maintain an average
of over 125 SaaS apps - IT is aware
of only a third of those ²**

² [Gartner](#)

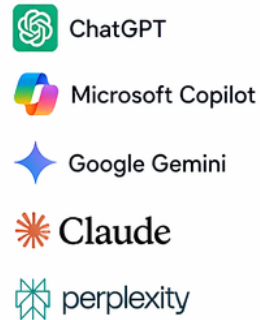
**67% of people use personal
devices at work ³**

³ [CBS News](#)

AI NÁSTROJE V MODERNÝCH ORGANIZÁCIÁCH

NAJPOUŽÍVANEJŠIE AI NÁSTROJE V SPOLOČNOSTIACH, ORGANIZÁCIÁCH A VO VEREJNEJ SPRÁVE

CHATBOTY & ASISTENTI



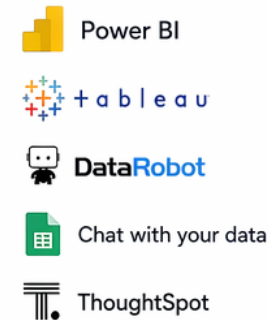
KREATIVITA & OBSAH



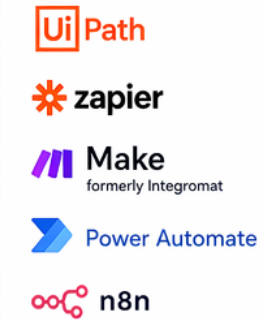
PÍSANIE & DOKUMENTY



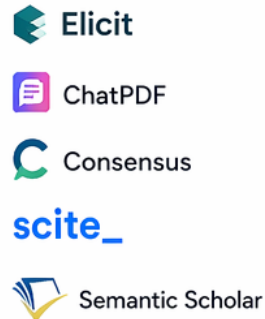
ANALÝZA DÁT & BI



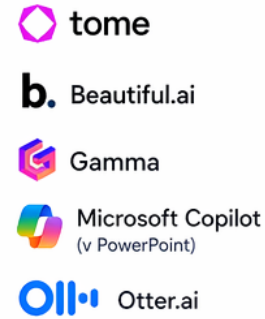
AUTOMATIZÁCIA & PROCESY



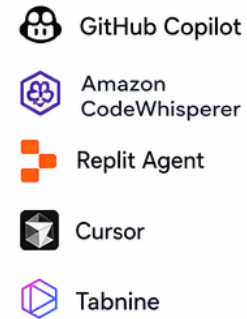
VYHLADÁVANIE & POZNATKY



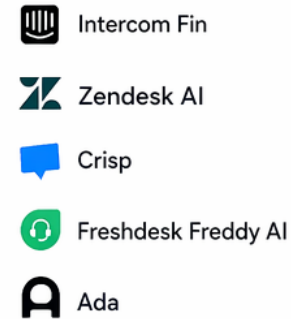
PREZENTÁCIE & KOMUNIKÁCIA



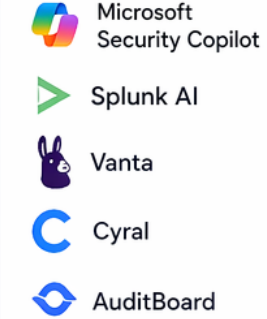
VÝVOJ & IT



ZÁKAZNÍCKA PODPORA



BEZPEČNOSŤ & COMPLIANCE



VYUŽITIE V
ORGANIZÁCIÁCH



ZVYŠOVANIE
PRODUKTIVITY



LEPŠIE ROZHODOVANIE
NA ZÁKLADE DÁT



AUTOMATIZÁCIA
RUTINNÝCH ÚLOH



ÚSPORA ČASU
A NÁKLADOV



INOVÁCIE & KONKURENCIESCHOPNOSŤ

AI NÁSTROJE SA RÝCHLO VYVÍJAJÚ. PREHĽAD JE AKTUÁLNY K MÁJU 2024.

—
What any AI needs?

Data, data and then data...





Data Security Everywhere Innovations

Comprehensive data security that unifies intelligent visibility, automated remediation, and adaptive enforcement to secure sensitive data across all channels

1

What **sensitive data** do you have?

2

Where is your **sensitive data**?

3

What are the risks to your **data**?

4

How to remediate **data risk**?

5

How to protect against **data loss**?

Data Security Everywhere Brings DSPM, DDR, DLP Together

Comprehensive visibility and control



Data-at-Rest Forcepoint DSPM

- Full scanning
- Find and fix ROT data risks
- Track security posture for compliance, policies, repositories

Data-in-Use Forcepoint DDR

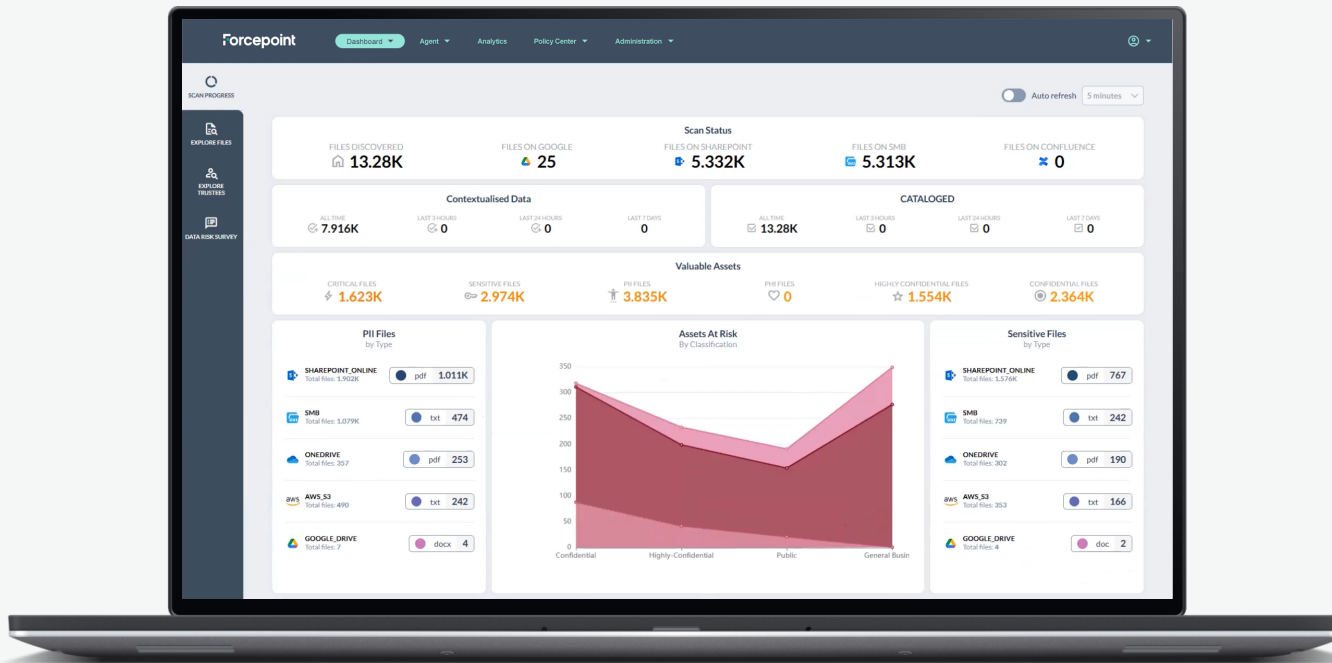
- Continuously monitor data repositories for changes
- Enables continuous security posture updates
- Alert and remediate potential breaches

Data-in-Motion Forcepoint DLP

- Prevent theft of data
- Single set of policies across all channels

Forcepoint DSPM

AI-powered data discovery and classification
with real-time risk reporting and orchestration



Fast, comprehensive discovery

In the cloud (Amazon, Microsoft, Google) and on-prem;
scan ~1M files per hour

AI Mesh-powered data classification

Powered by a highly trained, high-efficiency AI Mesh
for greatest accuracy and speed

Real-time monitoring and risk assessment

Understand data, access permissions and other data
risks in near real-time

Workflow orchestration

Track data ownership and accountability to ensure actions
taken are aligned with each stakeholder

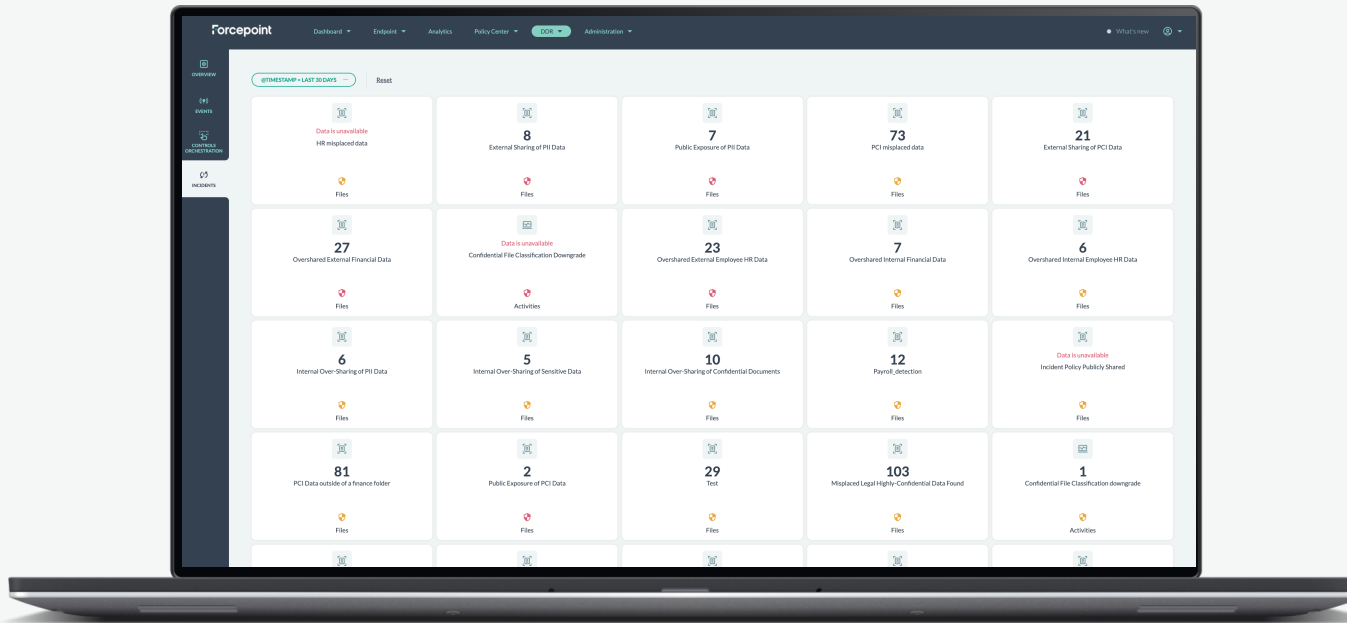
Extensive data sources

Cloud collaboration (O365), cloud file stores (SharePoint, Gdrive, Box), GenAI (ChatGPT Enterprise), IaaS (AWS, Azure), SaaS apps, IAM, on-prem storage (SMB, SharePoint)

Forcepoint DDR

Continuous monitoring to see and stop potential data breaches

Data Detection and Response



Continuous monitoring of file repositories

Continuous visibility into data creation, modification, movement and permission changes

AI-powered data classification

Powered by a highly trained, high-efficiency AI Mesh for greatest accuracy and efficiency

Dynamic incident alerts

Automated alerts and dashboards show data, access permissions and other data risks

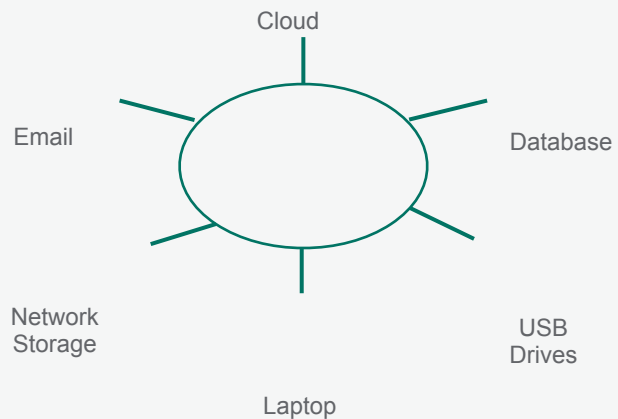
Data lineage

Track unstructured data as it moves and changes for stronger investigations*

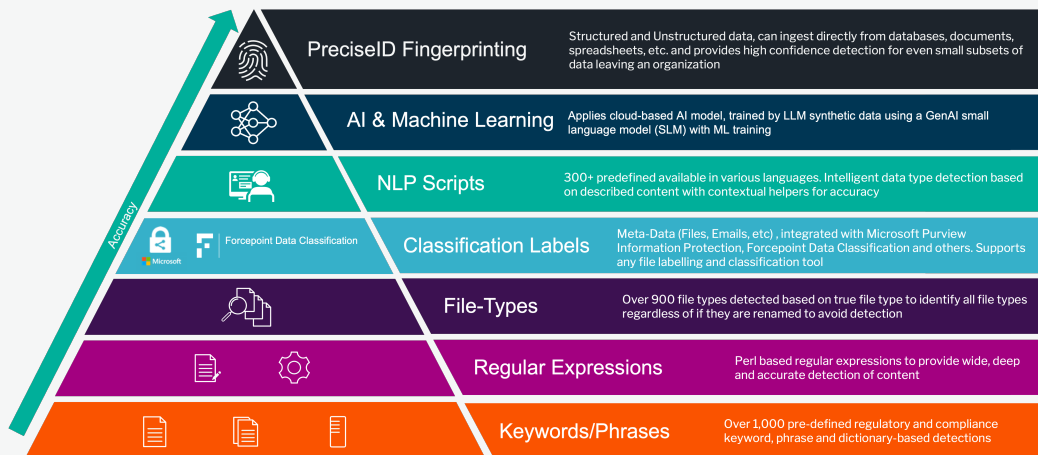
Extensive cloud data sources

AWS S3, Azure AD, Azure Blob, Azure Files, Google Drive, Confluence Cloud, Box (on-prem March)

Forcepoint DLP



Who	What	Where	How	Action
Human Resources	Source Code	Evernote	File Transfer	Confirm
Customer Service	Credit Card Data	Dropbox	Web	Block
Marketing	Personal Data	Business Partner	Instant Messaging	Notify
Finance	M&A Plans	Facebook	M&A Plans	Removes
Accounting	Employee Salary	OneDrive	Email	Encrypt
Sales Marketing	Financial Report	Malicious Server	Financial Report	Quarantine
Legal	Customer Records	Removable Media	File Copy	Confirm
Technical Support	Manufacturing Docs	Competitor	Print Screen	Audit
Engineering	Research	Customer	Copy/Paste	Notify



Forcepoint Risk-Adaptive Protection

Simplify data security via a behavior-centric approach



- Level of risk continuously assessed for each user
- Policies enforced automatically according to risk
- Progressively stronger enforcement minimizes data security friction and false positives
 - Most stringent action, blocking, can be reserved for when risk is proven, like in the real world
- Automated incident management

The Problem Customers Have Right Now

AI is moving faster than your security controls

AI Security
market by 2028*

01



What AI is running in my environment right now?

Employees are using a mix of AI tools, from code assistants to GenAI apps and early agent frameworks, often without IT visibility. Without a complete, accurate inventory across sanctioned, shadow, and emerging AI, security teams can't set the right controls.

02



Is sensitive data reaching AI systems it shouldn't?

PII, intellectual property, and regulated data are flowing into AI tools every day. Most organizations lack real-time visibility into these interactions, making it difficult to understand or prevent accidental exposure.

03



Are my AI agents operating within safe boundaries?

AI agents operate autonomously, executing multi-step actions, connecting to external services, and inheriting user permissions with no security oversight. Teams have no way to know which agents are running in their environment, what they're authorized to access, or how to stop them when something goes wrong.

*Source: Morgan Stanley

Example: Giving Visibility Into How People Are Using ChatGPT Enterprise

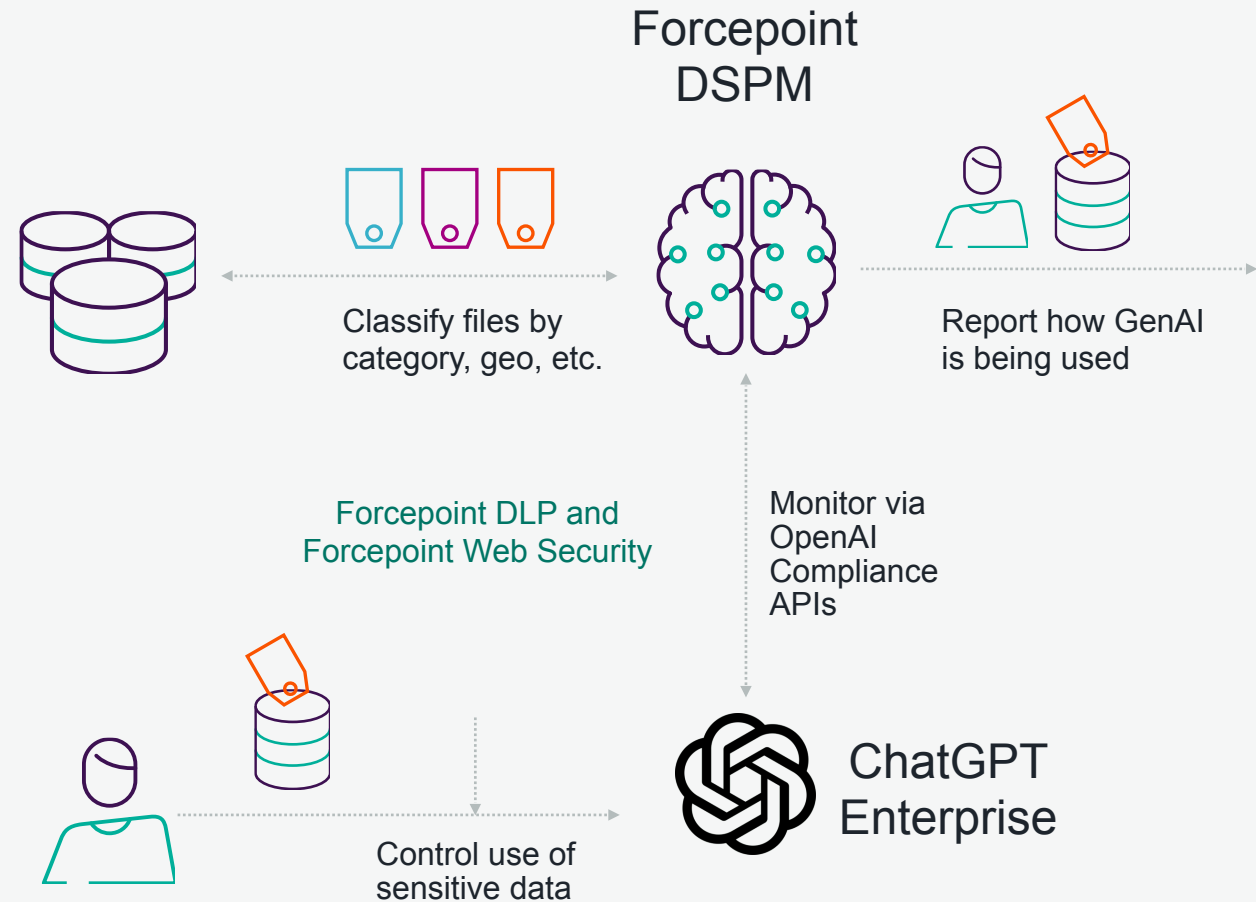
Who is using ChatGPT Enterprise

What prompts are they submitting

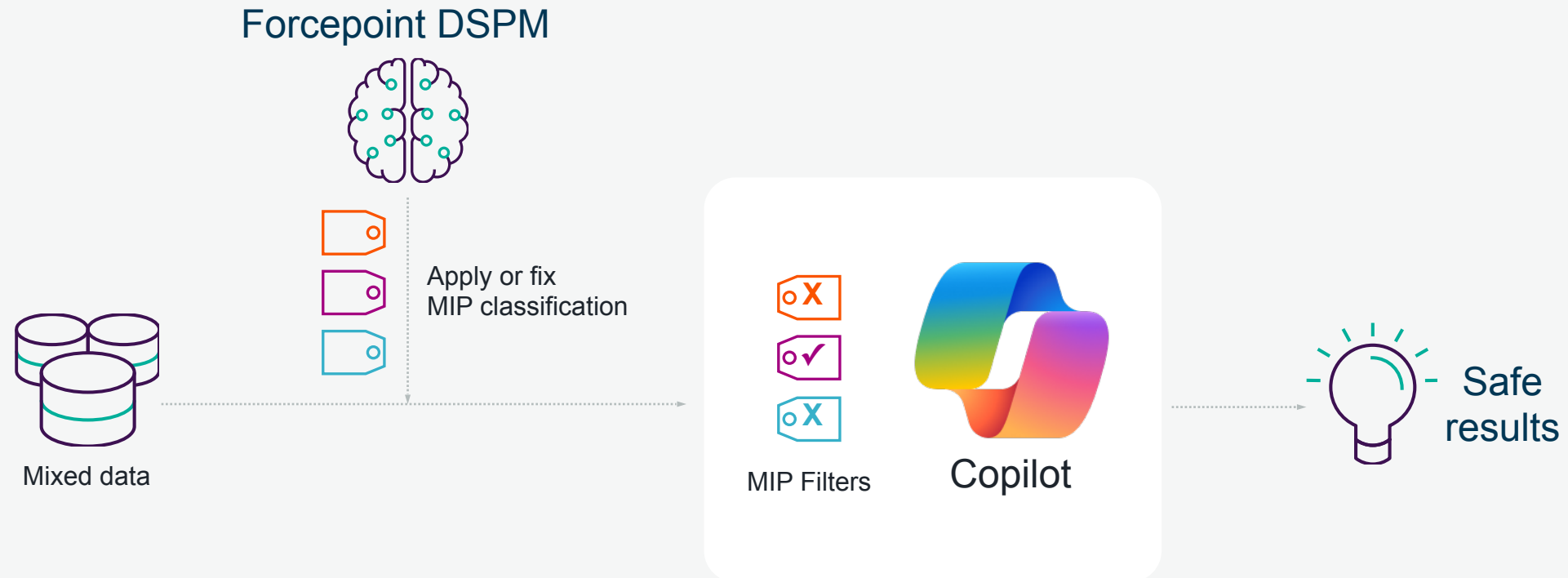
Which files are being uploaded

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

Forcepoint

AWARE

The virtual summit for security pros who need to implement smarter, more adaptive data security strategies now.
Learn how to tap into the power of AI to control AI.

Live AWARE Event

ANNOUNCING

Forcepoint AI Security

Launch Event: **AWARE: Decoding Agentic AI Security**

June 3rd, 2026

Registration Link

<https://www.forcepoint.com/aware>

What We Are Launching At AWARE

Forcepoint AI Security

One platform

- A single console for sanctioned AI, shadow AI, and agents, replacing fragmented product coverage.

Broader AI coverage

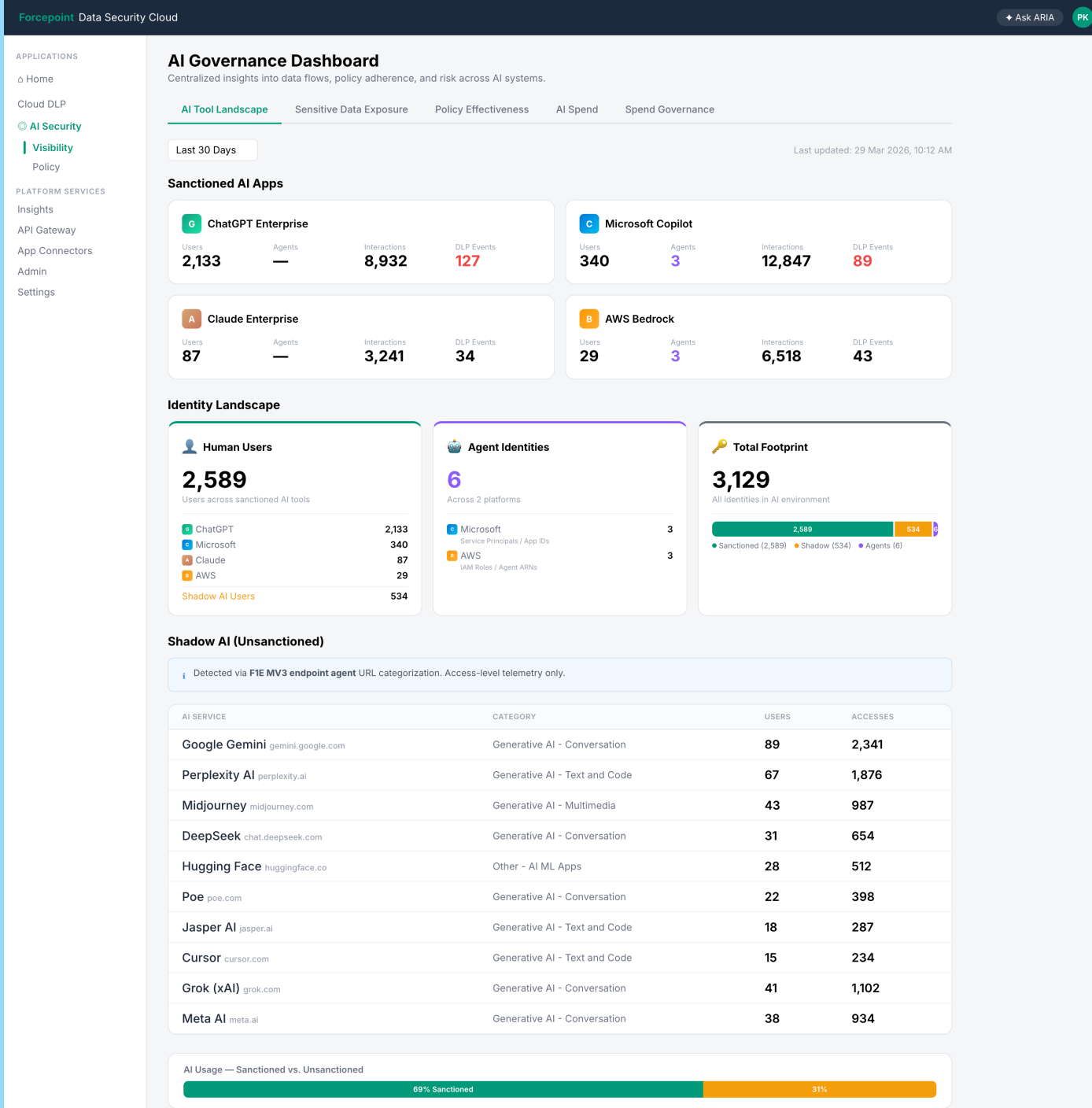
- ChatGPT, Copilot, Claude, Gemini, plus agentic AI across Copilot Studio, ChatGPT, AWS Bedrock, and more.

ARIA-guided setup

- From first login to governed environment in minutes.

Zero reclassification

- Existing DLP policies apply to AI prompts and responses from day one. No rebuild required.



Thank You



iurban@forcepoint.com
+421 905 274 378