Forcepoint | infodata PROFESSIONAL SERVICES

The Evolving Threat Landscape & Zero Trust Journey

Digvijay Pednekar
Territory Account Manager

Evolving Data Landscape

Data Sprawl and Fragmentation

“85%oforgsdon’tknowwheretheirsensitivedata lives.”
– Gartner

Gen AI Risk Explosion

"Dataleakage remains thetop threat. Close behind, however, is the insider threat supercharged by AI"

–Marcelo Amaral, CISO, Banco Safra

Governance and Regulatory Pressure

“Regulations evolvefast (GDPR,HIPAA,NIS2,PCIDSS)... need a shift from reactive to proactive data governance.”

–Enda Kyne, CISO, FBD Insurance

Security Stack Fatigue

“Standalone solutionscreatedinefficiencies and drained resources.”

– Gabe Guerra, Information Security, Mariner Finance

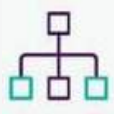
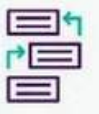
A Day in the Life of Sensitive Data

1	2	3	4	5
Sensitive Data	Endpoint Storage	SaaS Upload	AI Processing	Distribution
John runs SFDC report on top strategic accounts	Downloads a copy to local device	Uploads sensitive file to SharePoint	Asks ChatGPT to summarize report	Shares report via email and Slack

DATA	CRM PII, PCI, IP	.xlsx	Risky Prompt	Sensitive Information, Link
CHANNELS	Salesforce	Endpoint, SharePoint	SWG, Gen AI	Email, Slack

Without proper data security controls, a single sensitive document can proliferate across 5+ locations in minutes.

ANew Data Security Approach is Required

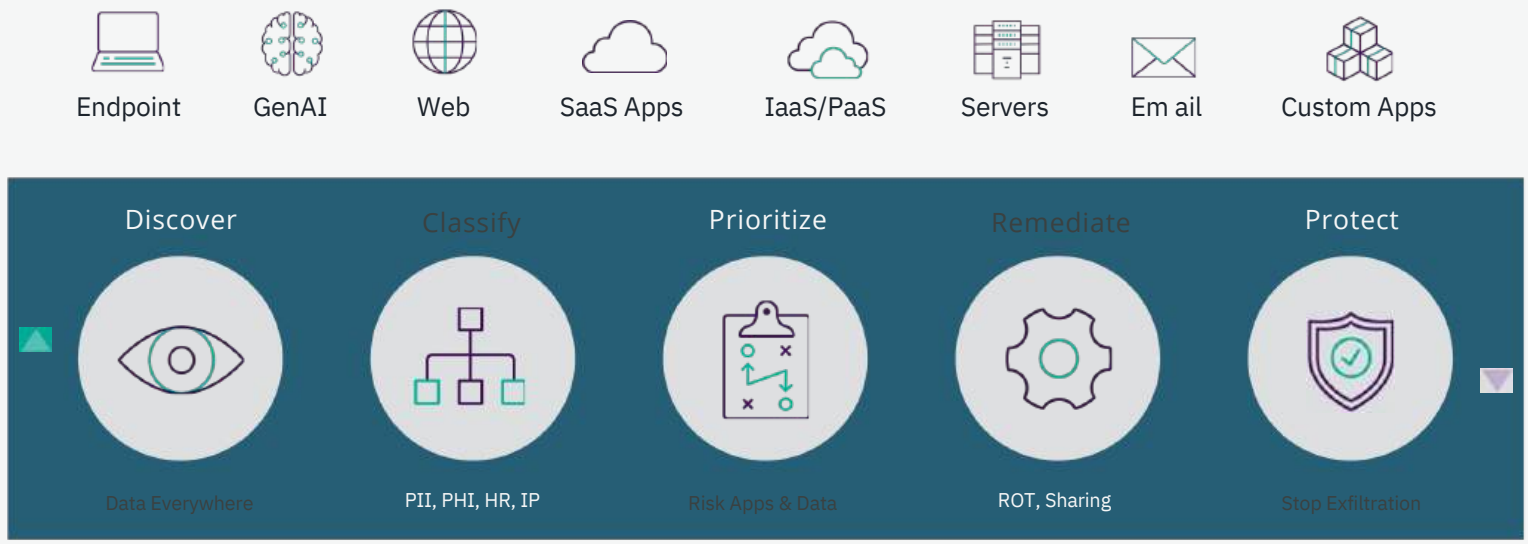




Discover	Classify	Prioritize	Remediate	Protect
Scan and map sensitive data across environment	Intelligent classification with context and sensitivity	Focus on high-impact data based on value, usage, and risk	Automate response to based on risk level and user behavior	Enforce real-time controls to prevent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

Forcepoint's mission is to enable effortless Data Security Everywhere

People can safely work anywhere with data everywhere



Data-at-Rest
Forcepoint DSPM

Data-in-Use
Forcepoint DDR

Data-in-Motion
Forcepoint DLP

Know
What youhave, where it lives, what's at stake

Dynamically Adapt
Protect in realtime as risk changes

Simplify
Eliminate complexity withautomation that scales

Across the entire data security lifecycle

The Challenges of Securing Sensitive Data

Data-at-Rest
Whereis it?

Data-in-Use
Howisitchanging?

Data-in-Motion
Do you have control?

Data Security Everywhere Brings DSPM, DDR, DLP Together

Comprehensive visibility and control

Data-at-Rest

ForcepointDSPM

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

Data-in-Use

ForcepointDDR

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

Data-in-Motion

ForcepointDLP

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

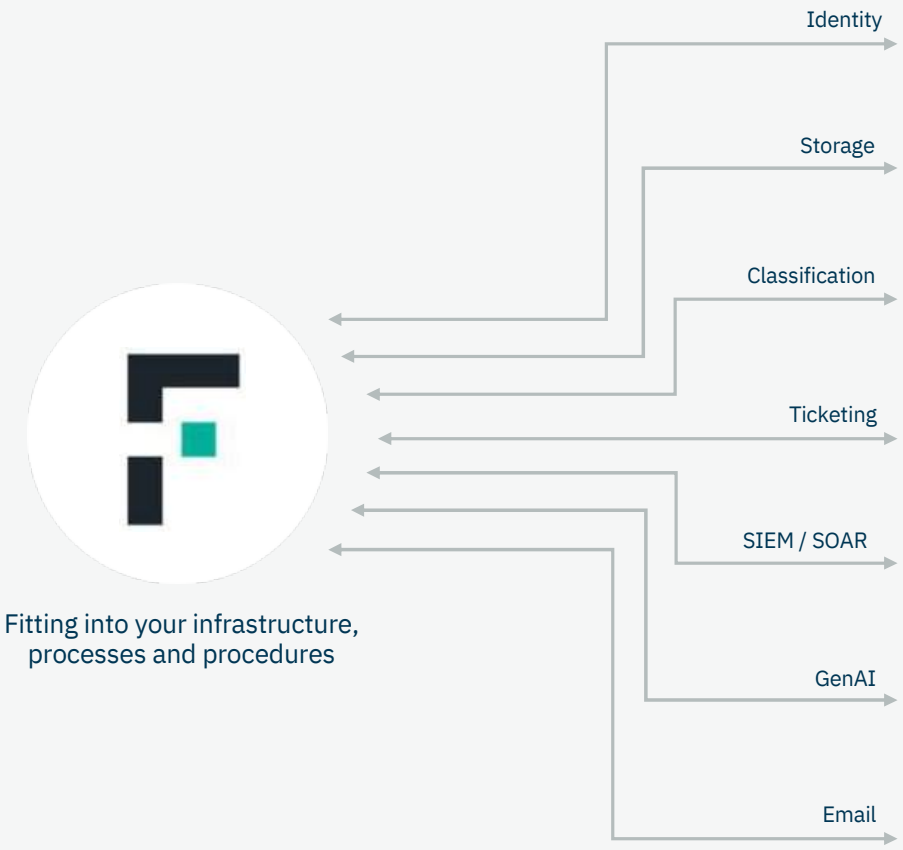
Forcepoint Data Security Everywhere

A framework solving for the most critical use cases

Compliance Readiness	Data Access Governance	Mitigate Data Risk	Breach Prevention
Copilot and M365 Data Security	Securely Enable Gen AI	Stop Ransomware	Email Security
Data Classification	BYOD Security	On-prem Support	Insider Risk Protection

Forcepoint Integrates with Your Environment

Simplifying operations



Examples

SAML
ADFS
PingIdentity
amazon S3
Azure Blob Storage
Microsoft Azure Information Protection
servicenow
splunk>
Radar
Microsoft Sentinel
ChatGPT
Copilot
Exchange
Google Workspace

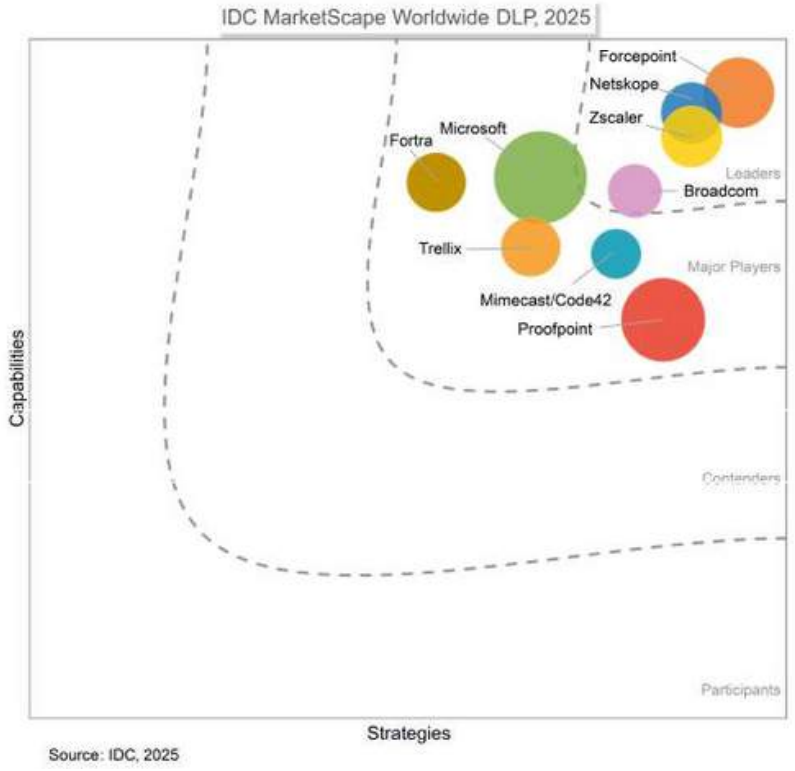
Forcepoint named a Leader in IDC MarketScape

Worldwide DLP 2025 Vendor Assessment

> Forcepoint DLP includes the full spectrum of DLP capabilities in its core offering. It can be used with unstructured and structured data, including images, and across data at rest, data in motion, and data in use.

> Adding AI-Mesh to DSPM shows customers where their specific data is, its protection status, and the ability to immediately add or adjust classification on that data.

> Customers appreciated the simplicity and user-friendliness of the product interface, the unified management of policies, and the stability of the product during updates.



Source: IDC, 2025

Source:"IDC MarketScape on Data Loss Prevention 2025 Vendor Assessment", doc #US53234325 April 2025

IDC MarketScape vendor analysis model is designed to provide an overview of the competitive fitness of technology and suppliers in a given market. The research methodology utilizes a rigorous scoring methodology based on both qualitative and quantitative criteria that results in a single graphical illustration of each vendor's position within a given market. The Capabilities score measures vendor product, go-to-market and business execution in the short-term. The Strategy score measures alignment of vendor strategies with customer requirements in a 3-5-year timeframe. Vendor market share is represented by the size of the icons.

Forcepoint: Where Trust Meets Tomorrow

Over two decades of trust to secure tomorrow's data landscape

Proven Foundation	Market Evolution	Continued Innovation
Leadership in Data Protection	Adapting to Modern Threats	Data Security Everywhere
20+ years securing the world's most sensitive data	Cloud-first transformation, securing sensitive data across new environments	AI-powered data security innovations AI Mesh, DSPM, DDR

From proven foundations to next-gen innovation. Forcepoint is driving the future of self-aware data security.

Forcepoint

The industry's onlyself-aware data security

"[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 rulesto actually start the learning curve of AI adoption."

– Marcelo Amaral, CISO, Banco Safra

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

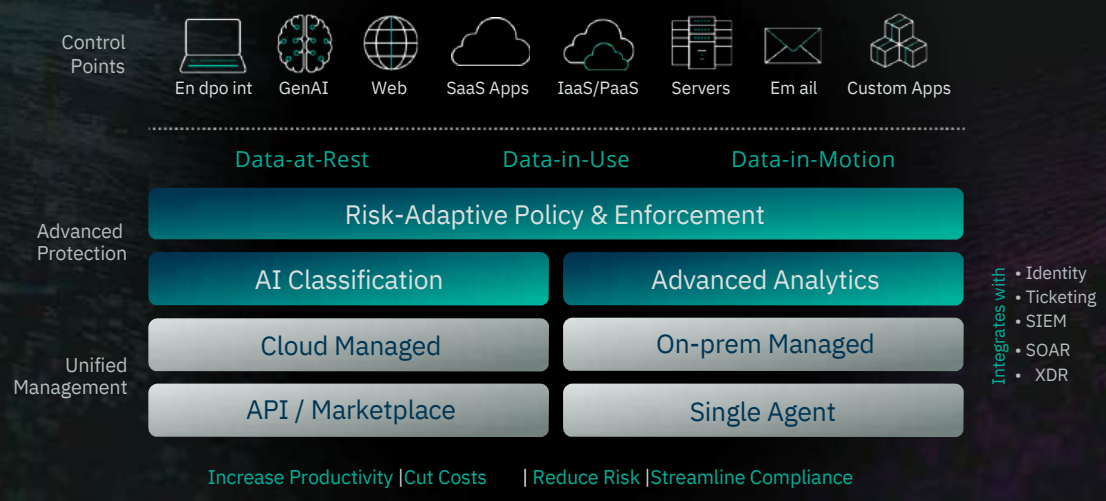
–EndaKyne,CISO, FBDInsurance

12,000+	160+	30M+	1700+	900+	1st	1st
Customers	Countries	Endpoints Secured	Built-in industry andgeo templates	File types recognized	To offer Risk-Adaptive Policies	Integration with ChatGPT, Copilot

Data Security Everywhere

Know. Dynamically Adapt. Simplify.

AI Mesh | DSPM |DDR |DLP |CASB |SWG |Email



Increase Productivity |Cut Costs | Reduce Risk |Streamline Compliance

Forcepoint Data Security Posture Management (DSPM)

powered by GetVisibility

Luke Otieno
SalesEngineer

AI Transformation is changing everything—and raising questions—even more than Digital Transformation

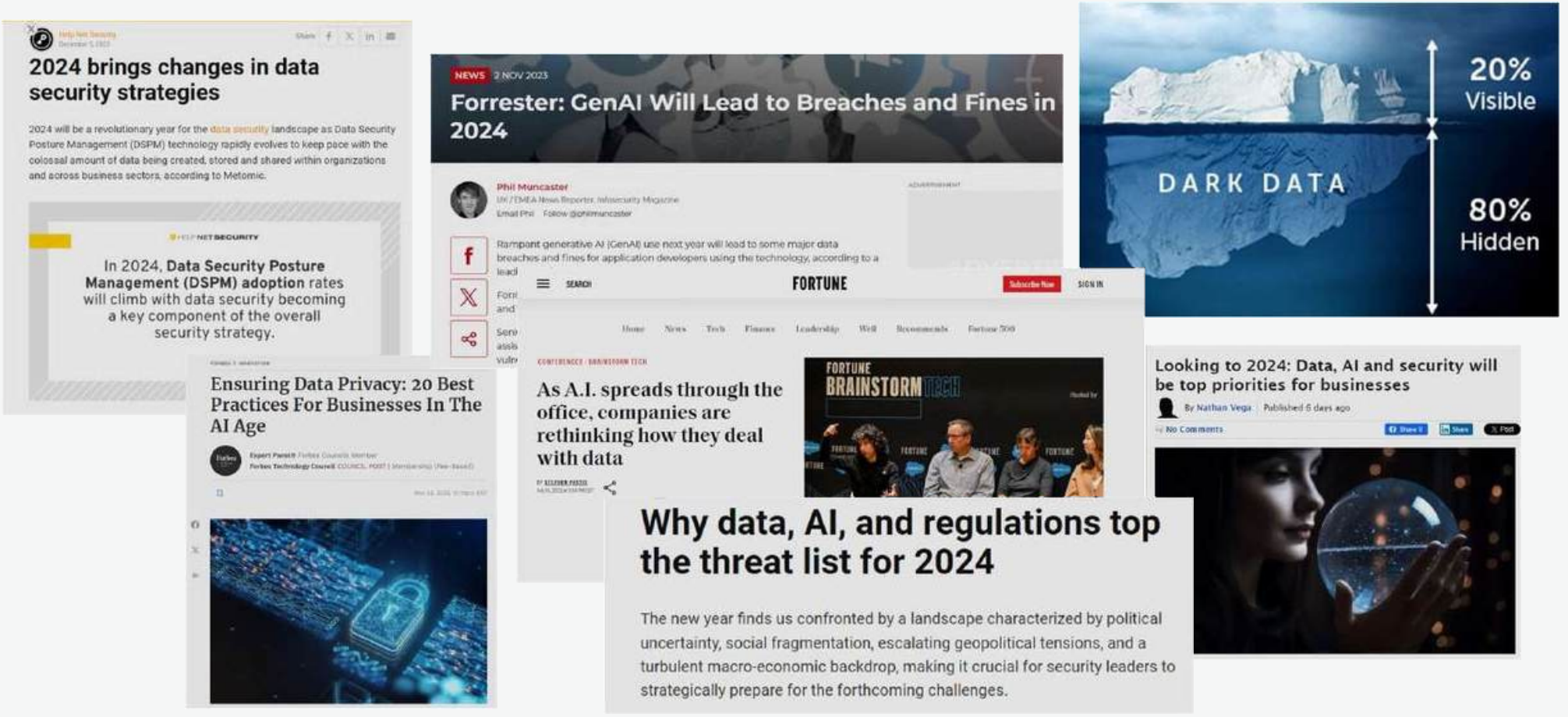
You need access to GenAI,
but how do you keep your data safe?

Who is using sensitive data?

What kinds? Where? How? Why?

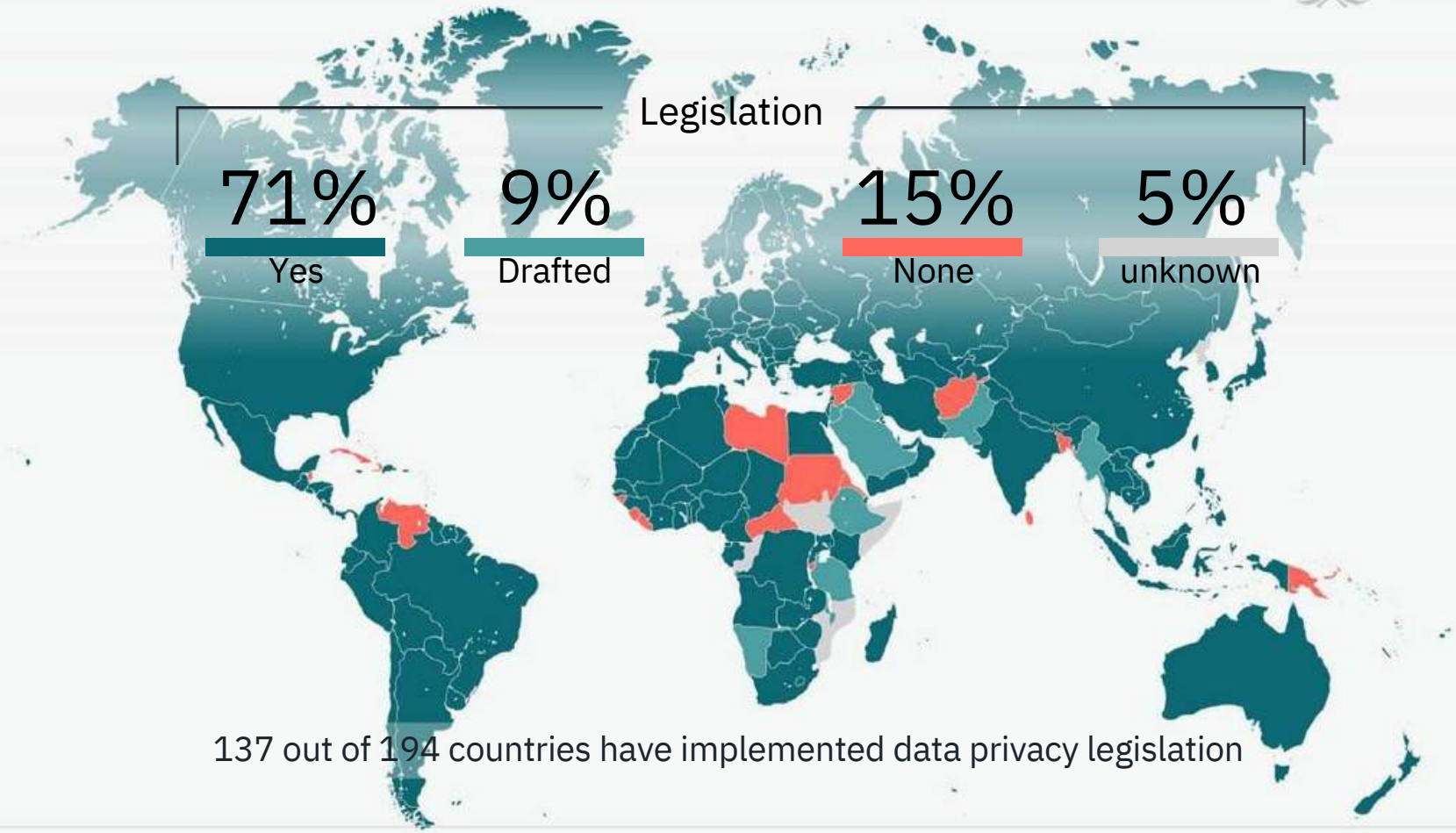
How do you seamlessly enforce data security everywhere?
(GenAI, SaaS apps, web, endpoints, email, your own apps, etc.)

GenAI: great power, even greater responsibility—and the tip of the iceberg



Data Security is now a business imperative

UNITED NATIONS
UNCTAD



137 out of 194 countries have implemented data privacy legislation

The growing threat of data breaches creating need for continuous data monitoring

Global average cost of a data breach reached an all-time high of $4.88 million in 2024, a 10% increase from 20231

In the third quarter of 2024, 422.61 million data records were leaked in data breaches2

It takes organizations an average of 258 days to identify and contain a data breach3

Region*	2024 Breach Cost(US $M)	Change from 2023
United	$9.36	–1%
States	$8.75	+8%
Middle East	$5.31	+14%
Germany	$4.73	+24%
Italy Canada	$4.66	–9%
UK Japan	$4.53	+8%
France	$4.19	–7%
LATAM	$4.17	+2%
ASEAN	$4.17	+2%
Australia	$3.23	+6%
India Br azil	$2.78	+3%
	$2.35	+8%
	$1.36	+11%

*IBM/PonemonCost of a Data Breach Report 2024

Forcepoint's mission is to enable Data Security Everywhere

so that people can safely work anywhere with data everywhere

Increase Productivity

Have peoplework anywhere with data everywhere—seamlessly, faster, easier—even from BYOD

Cut Costs

Replace fragmented infrastructure with more efficient, easier cloud service that cuts helpdesk calls too

Immediate Economic Impact

Reduce Risk

Use Zero Trust andenterprise-class security to continuously protect sensitive data wherever it is used

Streamline Compliance

Have consistent visibility & control everywhere

The Challenges of Securing Sensitive Data

Data-at-Rest

Where is it?

Data-in-Use

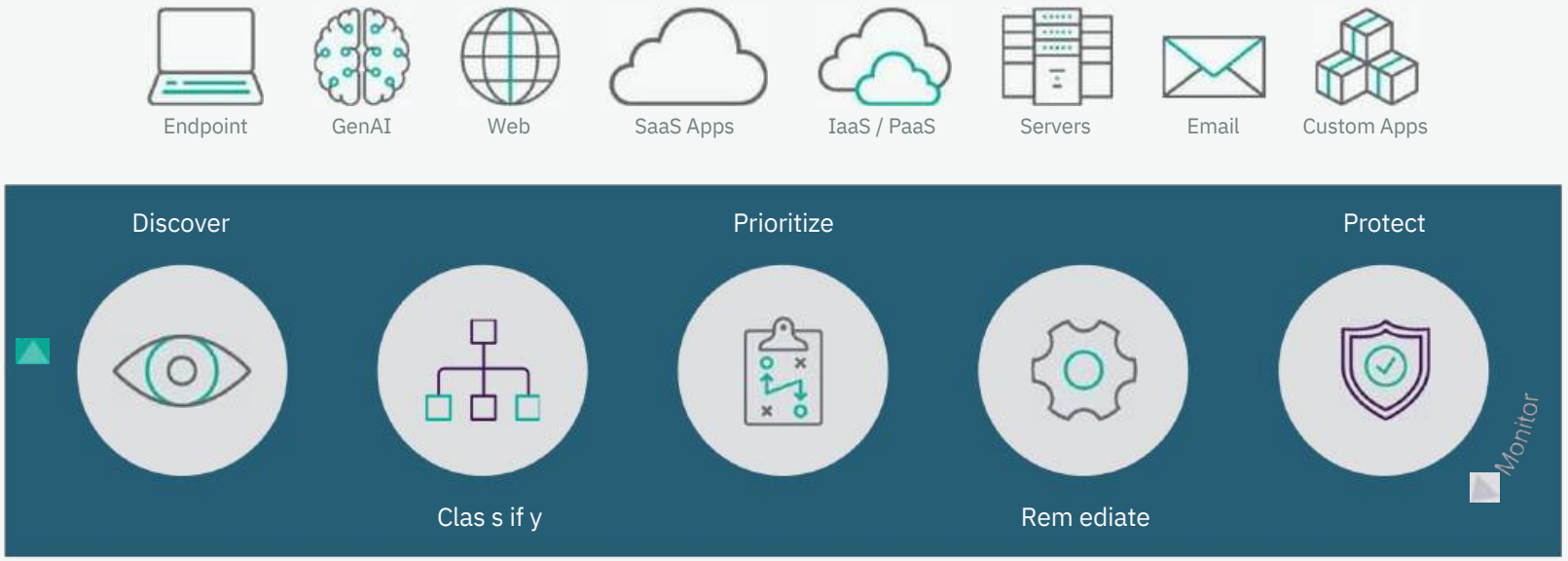
How is it changing?

Data-in-Motion

Do you have control?

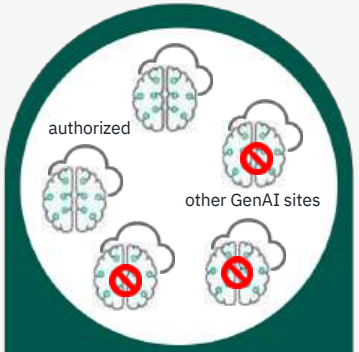
Forcepoint’s Data Security Everywhere

Fulllifecyclesecurityvisibility&controlfordataat rest, in use, in motion



Data-at-Rest	Data-in-Use	Data-in-Motion
Forcepoint DSPM	Forcepoint DDR	Forcepoint DLP

Gaining visibility and control over how GenAI sites are being used



Manage Access

See how GenAI sites 'in the wild' are used by your people

Block Uploading

Allow access to certain GenAI sites, but still prevent file uploads

Control Data Use

Inspect and control which data can be uploaded or pasted into sanctioned GenAI sites

Monitor

Track who, what, when sensitive data was uploaded
(ChatGPT Enterprise)

Forcepoint combines SSE, DLP, and DSPM to handle rapidly evolving GenAI needs

Modernize with Data Security Posture Management (DSPM)

AI-powered automation across the whole data security lifecycle

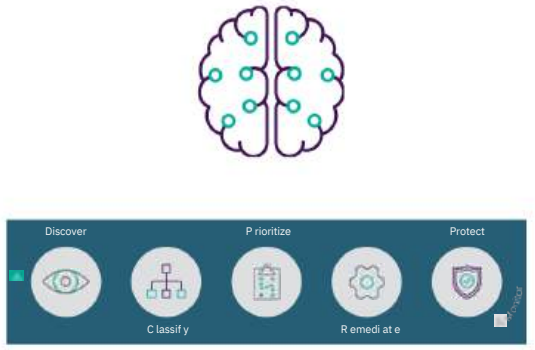
Discover sensitive data across important cloud and on-prem locations

Classify using AI Mesh engine for superior accuracy and efficiency

Prioritize where to focus efforts on securing the data posture efficiently

Remediate over-permissioned, redundant, and misplaced data

Protect sensitive information and regulated data everywhere



AI-powered Data Security Posture Management (DSPM)

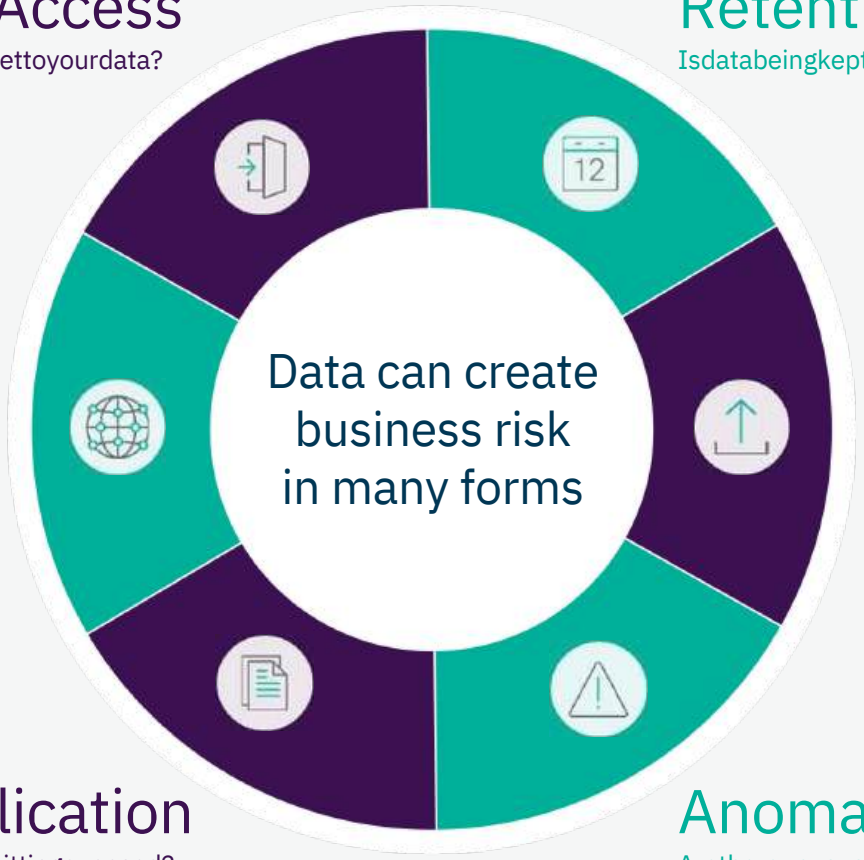
How well do you know your data?

Access

Can the wrong people/devices/appsgettoyourdata?

Retention

Isdatabeingkepttoolong (for compliance, cost, other reasons)?



Sovereignty

Whereisyour data?Isitsubjectto legal orcomplianceissues?

Over-sharing

Are protectionstoo loose?

Can filesbeshared tooeasily?

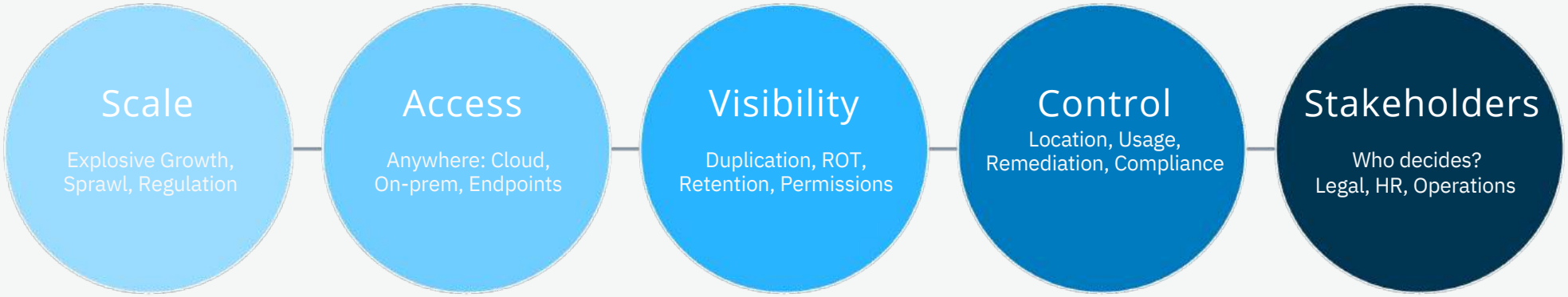
Duplication

Are redundant/obsoletecopiessittingexposed?

Anomaly

Arethereunusualpatterns in data access?

Data in a digital world presents new challenges



Old ways of protecting data don't work

Forcepoint DSPM

AI-powereddatadiscovery and classification with real-time risk reporting and orchestration

Com preh ens ive discovery

Inthe cloud (Amazon, Microsoft, Google) and on-prem; up to ~1Mfiles per hour.

AI Mesh-powered dataclassification

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

Real-time monitoring and risk assessment

Understanddata, access permissions andother data risks in near real-time

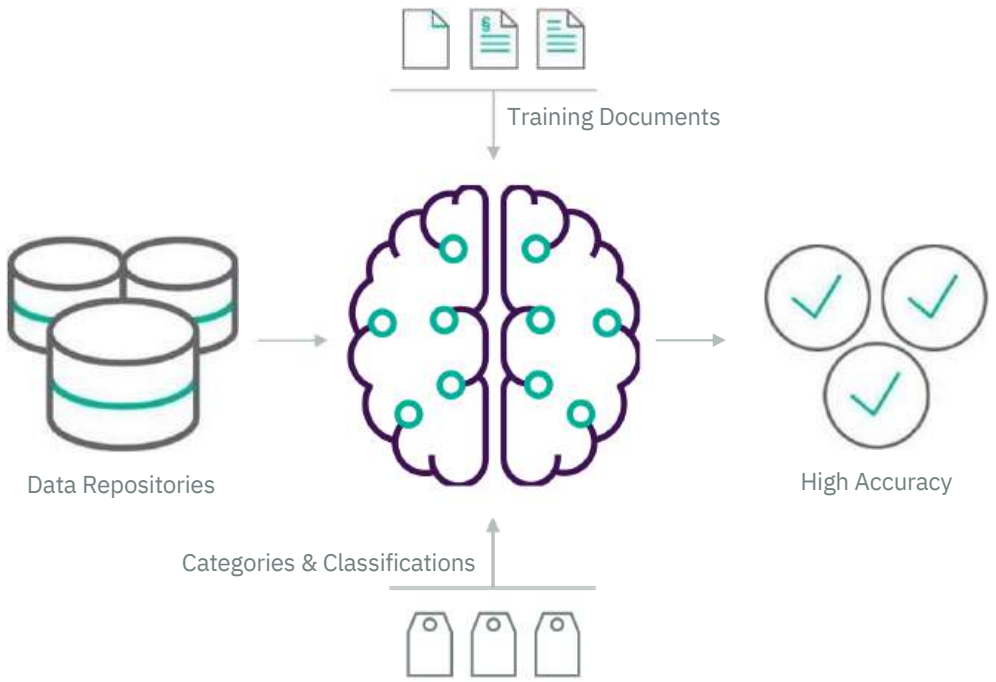
Workflow orchestration

Track data ownership and accountability to ensure actions taken are aligned with each s tak eholder

Extensive data sources

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

Discovery and classification create a foundation for applying controls to data



Contextualizing Data

Identifying

- SSN, Address, Account ID, TaxID, Drivers License, Age, Geo, Product Codes, and more

Categorizing

- PII,PCI, GLBA,ITAR, GDPR, CCPA, PHI, NPI, LGPD, PIPEDA, and more

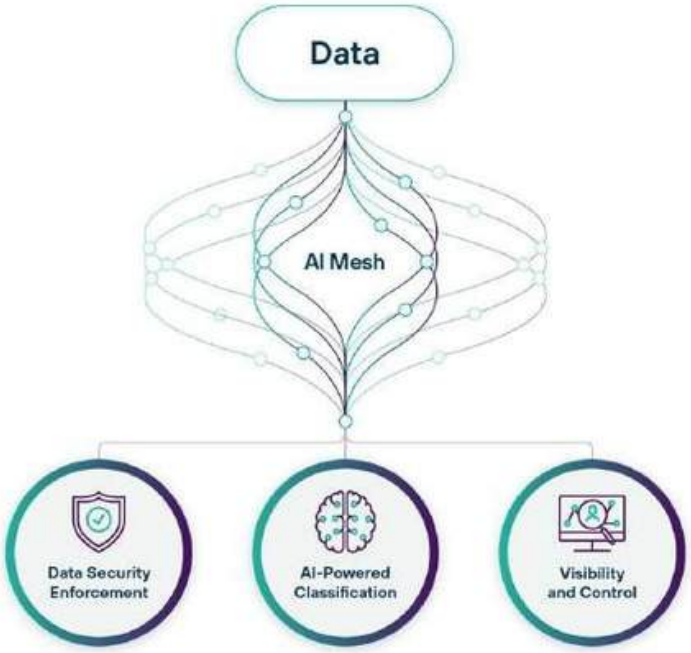
Classifying

- Sensitive,Secret, High Low, Public, Private, Confidential, and more

Labeling

- HR,Legal, Source Code, Intellectual Property, and more

Forcepoint DSPM is powered by the industry's first security AI Mesh



Forcepoint DSPM AI Mesh

Accurate, Fast, Explainable, Lower TCO

Smaller: SLM10Xsmaller than LLM models

Faster Classification: 200 milliseconds using regular CPUs

Lower TCO: smallernodes significantly lowers cost

Trainable:canbetuned to unique classification requirements

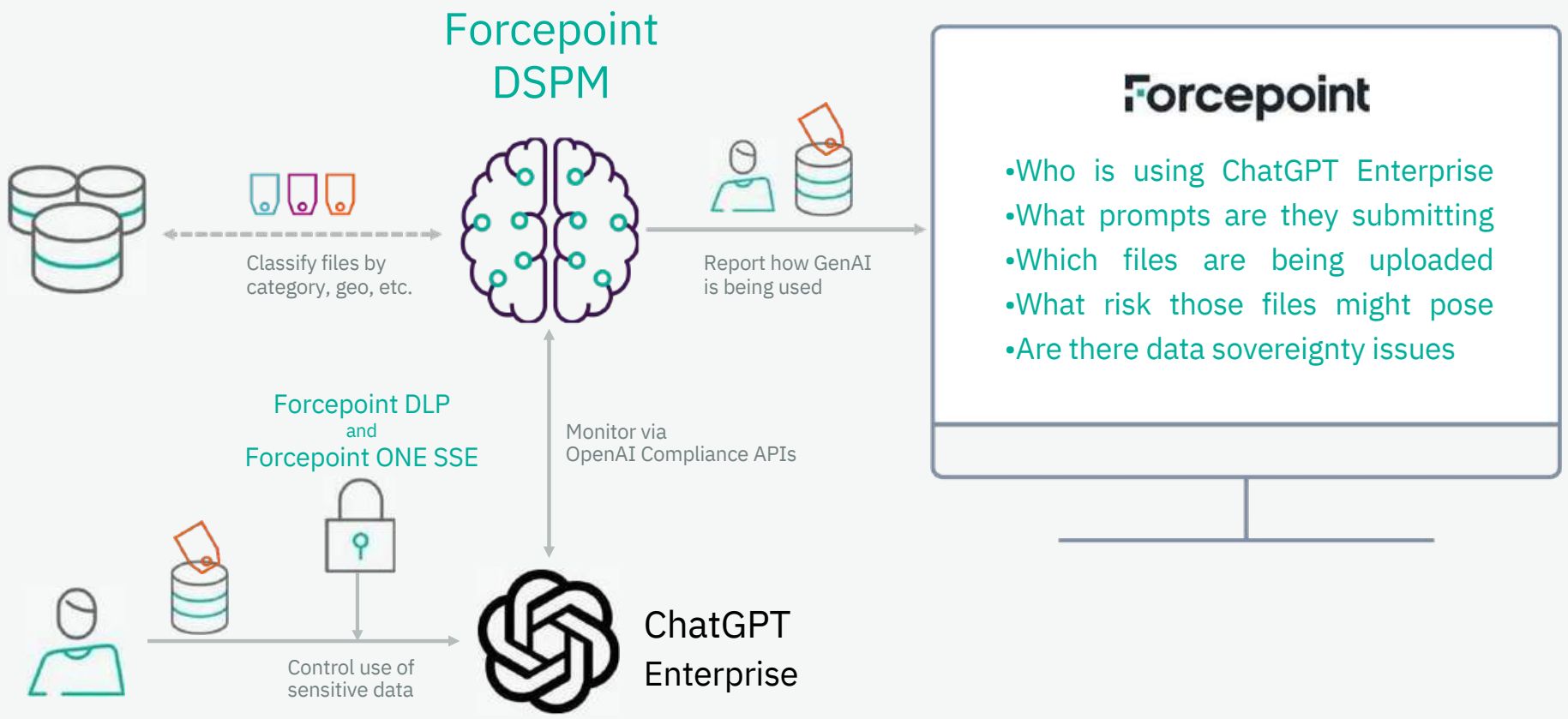
Explainable: Simplifies audit of AI for more transparency / trust

Forcepoint's AI Mesh is modular—uses focused, extensible architecture

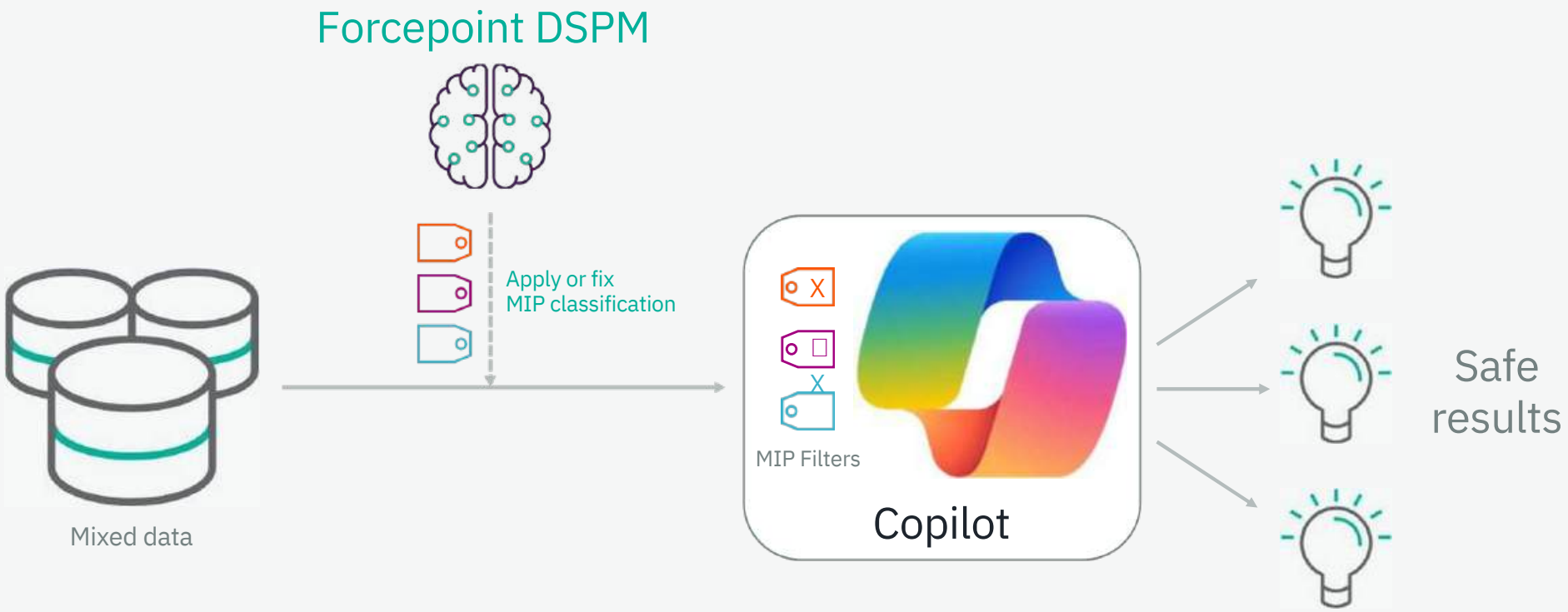
	Small Language Models (SLM)	Large Language Models (LLM)
Type of AI	Narrow AI	General AI
Focus	Tight, trained using specific, relevant data classes	Broad, potentially using inappropriate data
Extensibility	Easier to swap in optimized models	One size fits all
Accuracy	Higher due to more focused ties to right data	More prone to hallucinations
Eff icienc y	Smaller memory footprint, less compute intensive	Large compute and storage requirements
Reliability of Output	Clear justifications, more tracible to original input	Often opaque, creating security/business risk
Resilience to Bias & Manipulation	Less susceptible due to focused training	More susceptible to inheriting bias
Robustness against Attack	Less vulnerable to manipulated input	Easier to manipulate

Forcepoint's AI Mesh uniquely uses optimized SLM and focused AI techniques to deliver superior results

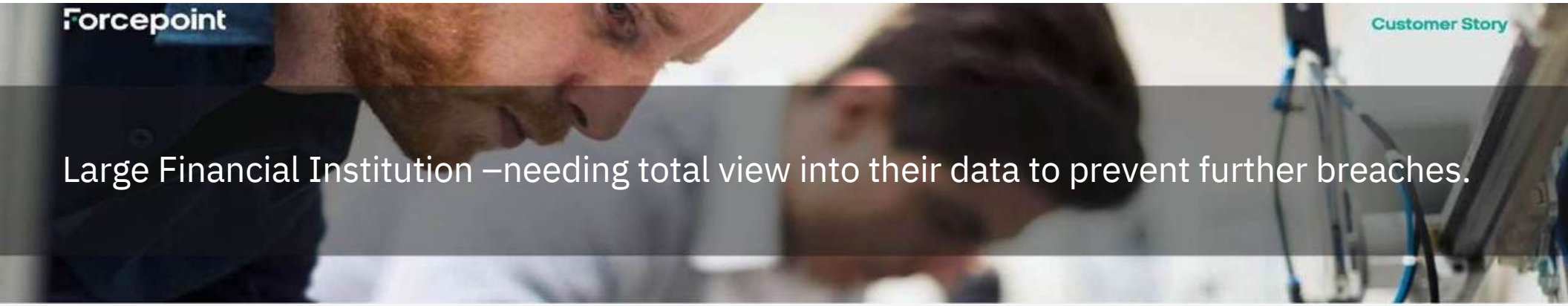
Example: giving visibility into how people are using ChatGPT Enterprise



Example: enabling safe use of GenAI



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



Large Financial Institution –needing total view into their data to prevent further breaches.

Challenges

- Stop leakage of sensitive data from employee's mailboxes. Breach had already taken place showing their email to be a large point of potential exfiltration.

Approac

h UseForcepoint to do a major scan before legal was to get involved.
. . 5 days to scan across 2.5TB of raw data, 9 million emails with attachments in 5 different languages.

Results

- Completed total scan of 2.5TB in just 2 ½ days!
- Were able to identify sensitive email content and remove sensitive data.
- Just one email had bank account details and screenshots of bank statements covering billions of dollars.


Forcepoint
"As part of Forcepoint's broader data security ecosystem, DSPM has integrated seamlessly with our existing solutions. It's an essential component of our overall data security strategy."
Indonesia Financial Group (IFG)

Modernize and automate the data security lifecycle with AI-powered DSPM technologies

Increase Productivity

Enable faster, safer data access and sharing for better innovation & collaboration

Cut Costs

Automate to save time/resources on investigations & remediation; save on cyber insurance

Reduce Risk

Prevent breaches by uncovering and fixing sensitive data misuse, exposure

Streamline Compliance

Gain visibility and control over sensitive data everywhere and mature your GRC program

Forcepoint does Data Security Everywhere better than anybody else

Recognized

Leader in ForresterWave for SSE
(March 2024)

Leader in Forrester Wave for
Data SecurityPlatforms
(March 2023)

Industry Firsts

Data-first SASE platform
(integrated CASB, SWG, ZTNA with DLP,
malwaredefenses, distributed enforcement)

Risk-Adaptive Protection

Secure SD-WAN

Expansive Protection

Broadest enforcement channels

APIs for adding to custom apps

Comprehensive threat protection

Easy to Use

1700+ built-in templates for industries
and 150+ geographies

Integrated into SSE/SASE gateways

Single-pane management
of policies and incidents

AI

AI mesh-based discovery, classification,
prioritization, orchestration

Granular visibility into ChatGPT Enterprise

Prevent inappropriate use of GenAI sites

Unparalleled Accuracy

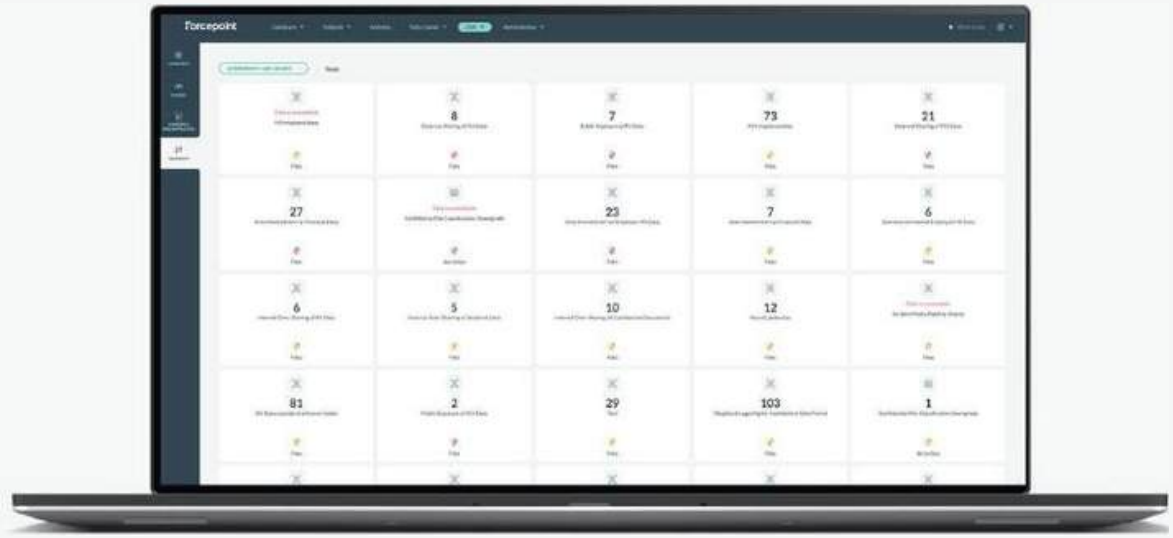
Detection of 900+ file types

ML-based content recognition

Structured & unstructured data

Forcepoint DDR: continuous monitoring to see and stop potential data breaches

DataDetection&Response



Continuous monitoring of file repositories

Continuousvisibility intodata creation, modification, movement and permission changes

AI-powered dataclassification

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

Dynamic incident alerts

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

Data lineage

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

Extensive cloud data sources

AWSS3, AzureAD,Azure Blob, AzureFiles,GoogleDrive,Confluence Cloud, Box (on-prem March)

*SharePoint Online, OneDrive, Google Drive, Azure Blob, Box

Detect Misuse of Data So You Can Fix it Before It Becomes a Breach

DataDetectionandResponse(DDR)

Discover file creations/modifications/movement, permission changes

Classify files whenever changes found

- Gather context and generate “multitag” classification

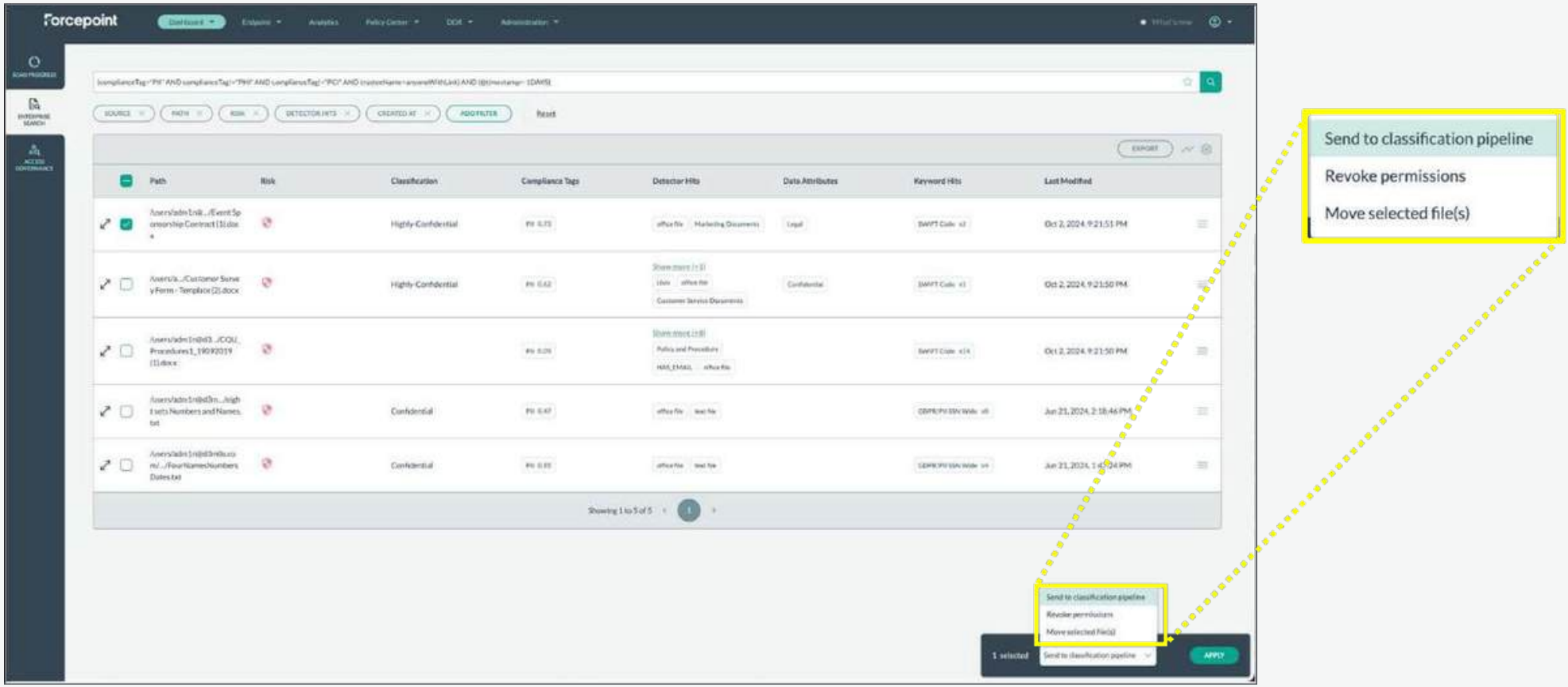
Prioritizepotential incidents for attention

Alert admins and simplify remediation

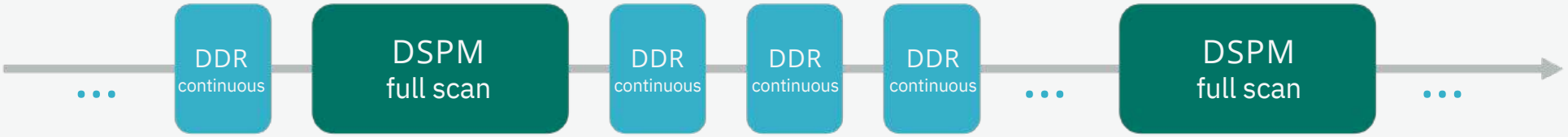
Identify risks so policies can be updated to protectagainst breaches

Continuously monitordata repositories for closed-loop security

Enables Remediation Actions to be Taken Directly from Console



DSPM and DDR work together to manage posture and reduce risk



Detect & respond to changes that introduce risk

Scan & classify to find ROT (redundant, obsolete, trivial) data

Address data risks

Detect & respond to changes

Update security posture

Show progress in fixing ROT data

Update for new compliance mandates, policies, repositories

DDR incidents only happen when the data is touched/used

Data Security Everywhere brings DSPM, DDR, DLP together

Comprehensive visibility & control

Data-at-Rest

Forcepoint DSPM

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

Data-in-Use

Forcepoint DDR

- Continuously monitor data repositories
- 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

Get started with a Forcepoint Data Risk Assessment (DRA)

Scan in your own environment

Forcepoint-certified personnel analyze scans, produce report

Highlights key issues

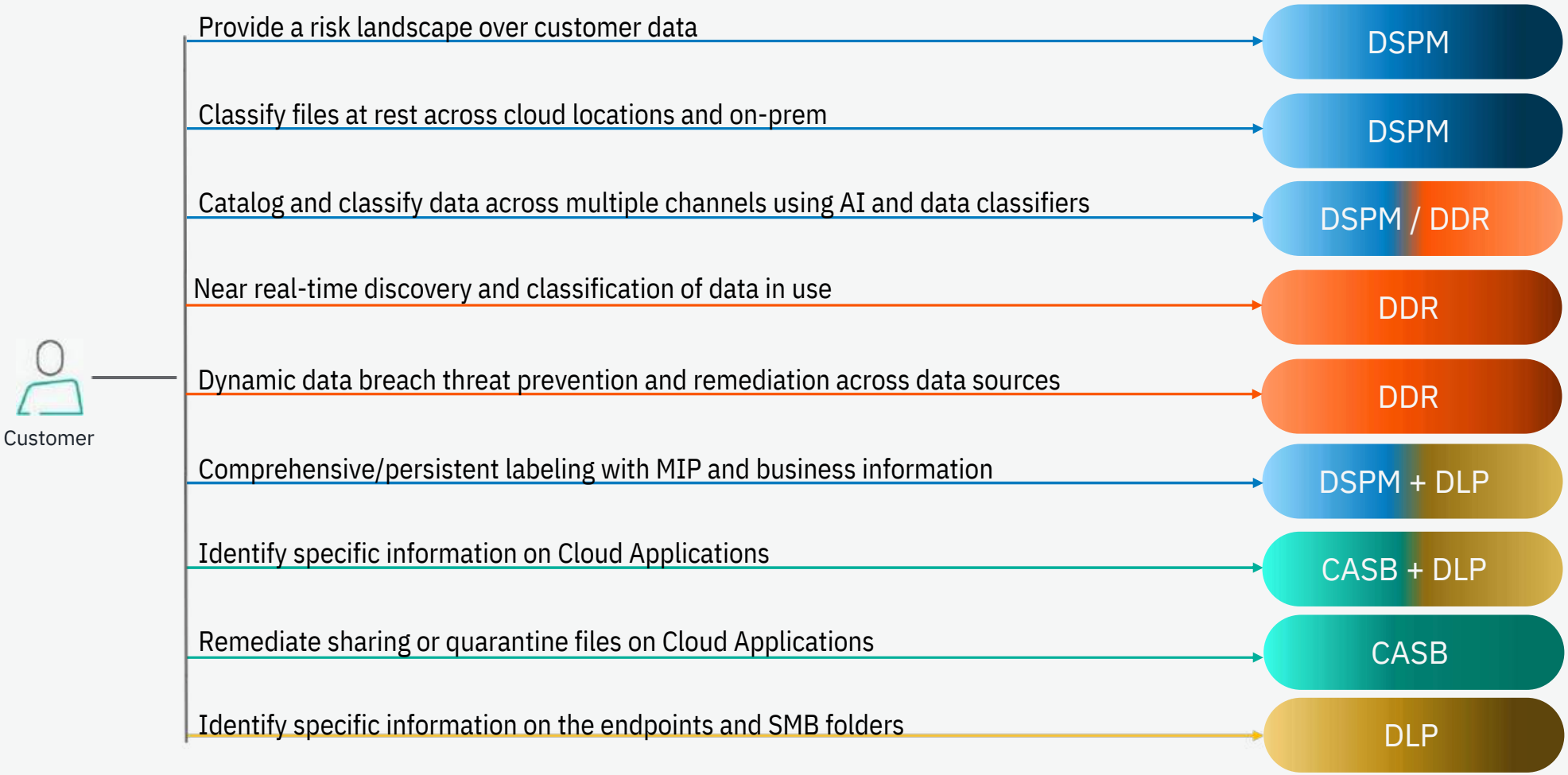
- Data assets
- Risk Impact
- Shadow data
- Overexposed data
- Over-privileged users
- Unprotected data
- Data sovereignty

See for yourself how Forcepoint DSPM helps you
See. Secure. Simplify.

Data Security Product Comparison

	DDR	DSPM	DLP	RAP	CASB API
Foc us	Seeing and stopping data breaches	Strengthening the data posture	Preventing senstive data exfiltration	Dynamic enforcement based on risky behavior	Discovering and protecting SaaS data
Proactive/ Reactive	Reactive	Proactive	Reactive	Proactive/ Reactive	Proactive
Continuous monitoring	yes	no	yes	yes	yes
Prevent Data Breaches	yes (primary focus)	yes	yes	yes	yes
Standalone or Add-on	Add-on to DSPM	Standalone	Standalone	Add-on to DLP	Part of ONECASB SKU

Forcepoint DSPM Selection Flowchart



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
Co m pliance

© 2025 Forcepoint

infodata
PROFESSIONAL SERVICES

Contact Us at
Infodata Professional Services

Let’s empower your people and your business with Forcepoint Data Security Solutions

+234 911 208 5425

info@infodataproserv.com

www.infodataproserv.com