Forcepoint

Neznalosť dát neospravedlňuje Ilúzia ochrany dát v dobe AI

Igor Urban
Territory Account Manager

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 2023[1]

In the third quarter of 2024, ***422.61 million*** data records were leaked in data breaches[2]

It takes organizations an average of ***258 days*** to identify and contain a data breach[3]

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

**IBM/Ponemon Cost of a Data Breach Report 2024*

1. IBM/Ponemon Cost of a Data Breach Report 2024
2. Statista, Data breaches worldwide – statistics & facts, 2024
3. IBM/Ponemon Cost of a Data Breach Report 2024

© 2024 Forcepoint

Why Data Protection now? Lets talk about compliance…

ISO 27001:2022

A.5.12	Data Classification
A.8.10	Information deletion
A.8.12	Preventing data leaks
A.8.16	Monitoring of activities
A.5.23	Information security for the use of cloud services

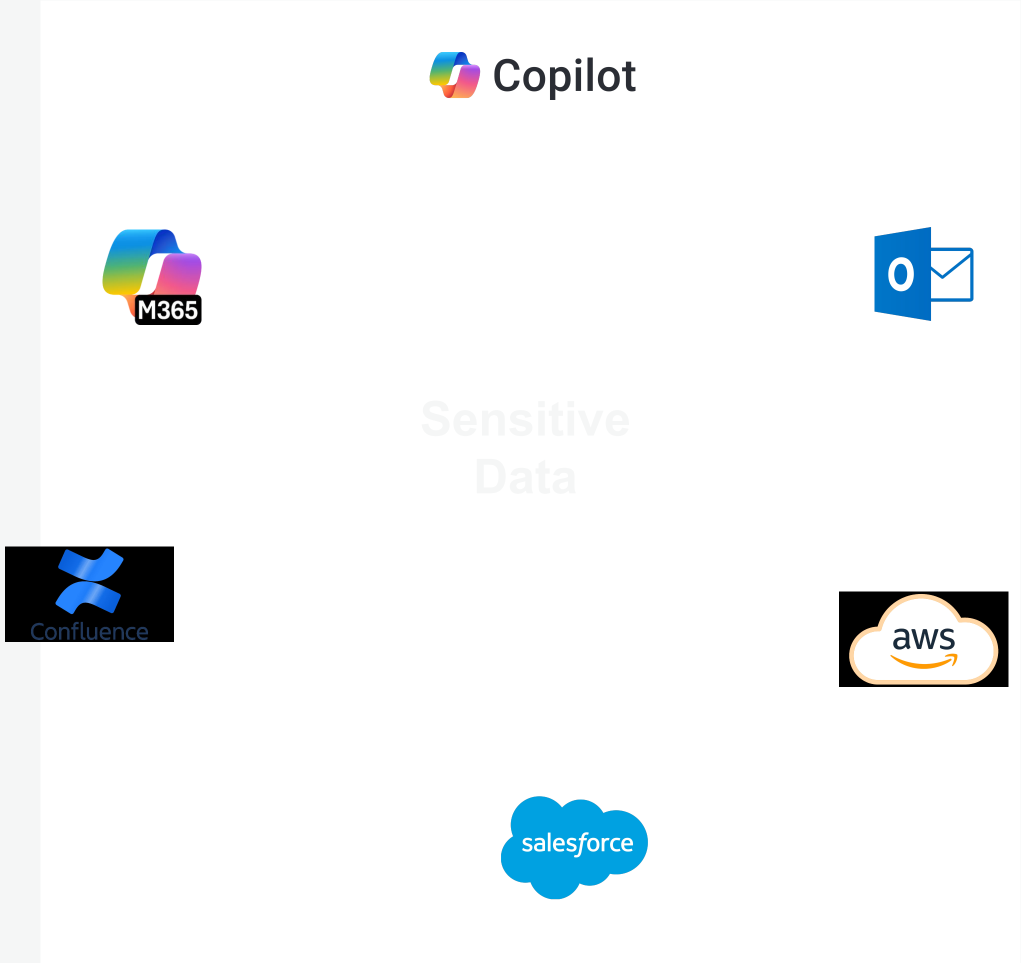
NIS 2.0

- Establishing security controls for information systems and measuring their effectiveness
- Enforcement of encryption policies
- Limiting authorized access to sensitive data based on contextual factors such as the location of the login, the time of the login, and the action in question
- Providing real-time visibility and control over sensitive data

DORA

- ICT risk management
- ICT third-party risk management
- Digital operational resilience testing
- ICT-related incidents
- Information sharing
- Oversight of critical third-party providers

Evolving Data Landscape



Data Sprawl and Fragmentation

“85% of orgs don’t know where their sensitive data lives.”
– **Gartner**

Gen AI Risk Explosion

“The one constant with all flavors of AI is that they require access to your data.”

– **Chief Data Strategy Officer**

Governance and Regulatory Pressure

“Regulations evolve fast (GDPR, HIPAA, NIS2, PCI DSS)… need a shift from reactive to proactive data governance.”

– **Analyst, Data Security**

Security Stack Fatigue

“Patchwork of tools that don’t talk to each other… drained time and focus.”

– **Healthcare provider**

© 2025 Forcepoint

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 don’t work in order, 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

Streamline Compliance and Governance

Consistent, reportable visibility and protection across all channels

Safely Enable Gen AI

Innovate and mitigate risks of GenAI and new tools

Consolidate Fragmented Infrastructure

Reduce OpEx up to 31%

Copilot and M365 Data Security

AI Data Classification

BYOD Security

Insider Risk Protection

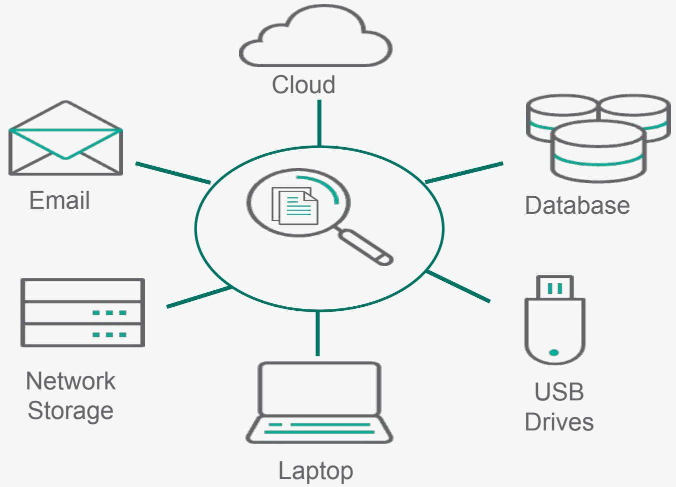
Email Security

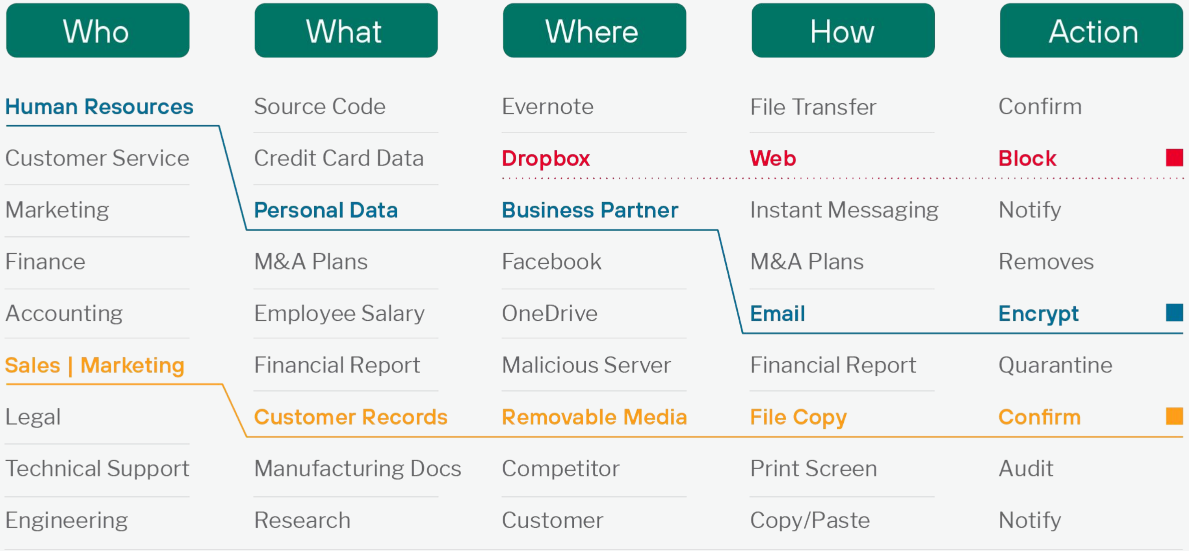
Unified Breach and Incident Readiness

© 2025 Forcepoint

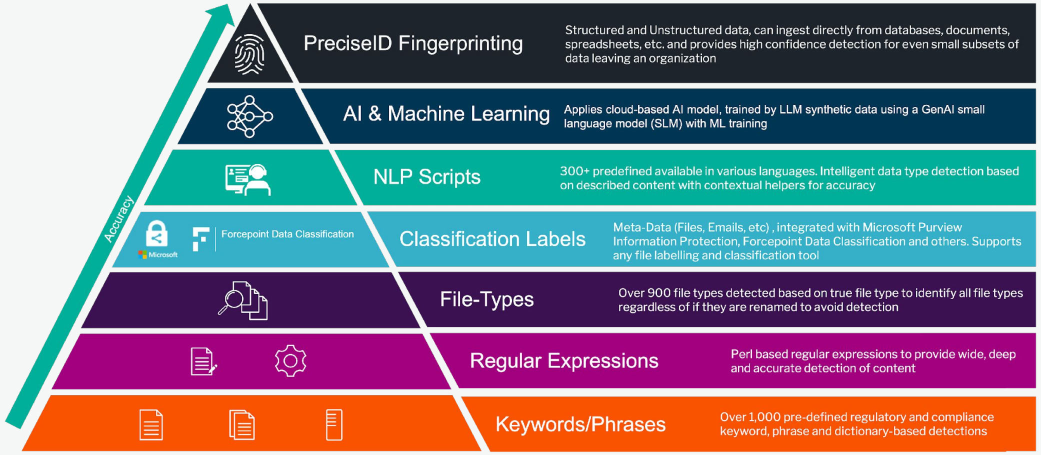
DATA IN MOTION

Map and Manage Sensitive Data Flows





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



PreciseID Fingerprinting	Structured and Unstructured data, can ingest directly from databases, documents, spreadsheets, etc. and provides high confidence detection for even small subsets of data leaving an organization
AI & Machine Learning	Applies cloud-based AI model, trained by LLM synthetic data using a GenAI small language model (SLM) with ML training
NLP Scripts	300+ predefined available in various languages. Intelligent data type detection based on described content with contextual helpers for accuracy
Classification Labels	Meta-Data (Files, Emails, etc) , integrated with Microsoft Purview Information Protection, Forcepoint Data Classification and others. Supports any file labelling and classification tool
File-Types	Over 900 file types detected based on true file type to identify all file types regardless of if they are renamed to avoid detection
Regular Expressions	Perl based regular expressions to provide wide, deep and accurate detection of content
Keywords/Phrases	Over 1,000 pre-defined regulatory and compliance keyword, phrase and dictionary-based detections

© 2025 Forcepoint 10

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

DATA AT REST

What is DSPM

Data security posture management (DSPM) provides visibility as to **where** sensitive data is & **who** has access to that data

It does that by assessing the current state of data security, **identifying and classifying potential risks** and vulnerabilities & implementing **security controls** to mitigate these risks

Forcepoint DSPM

- One-stop Solution for Data governance and risk management
- Streamlines data Governance process
- Provides monitoring and remediation
- Enables organizational autonomy
- Enhances and strengthens data governance for the organization

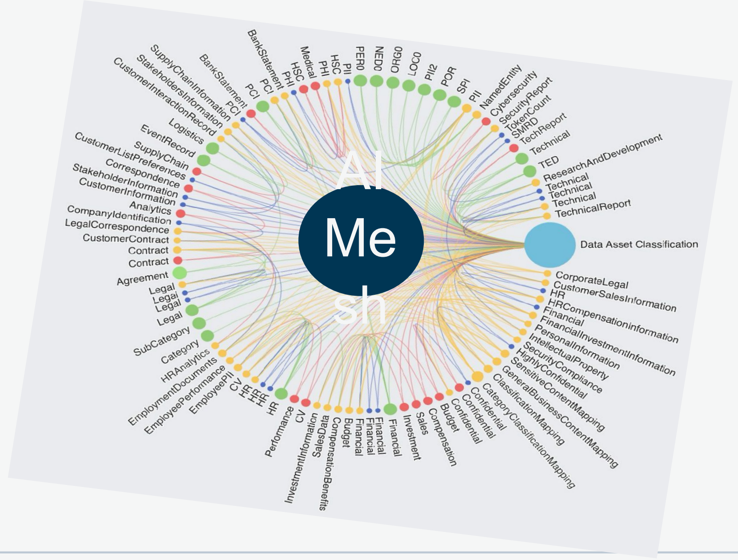
DSPM Use cases

Sensitive Data Discovery & AI Classification

Risk Assessment and Priorities

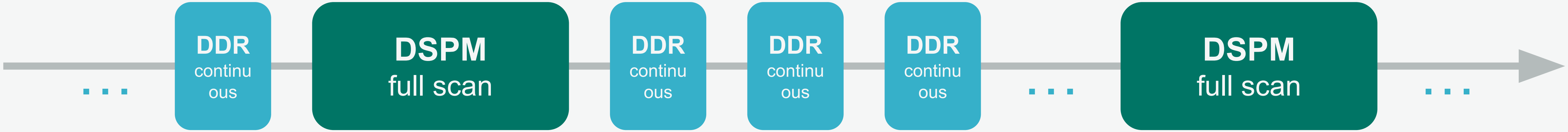
Access and Permission Management

ROT Data



DATA IN USE

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

© 2024 Forcepoint

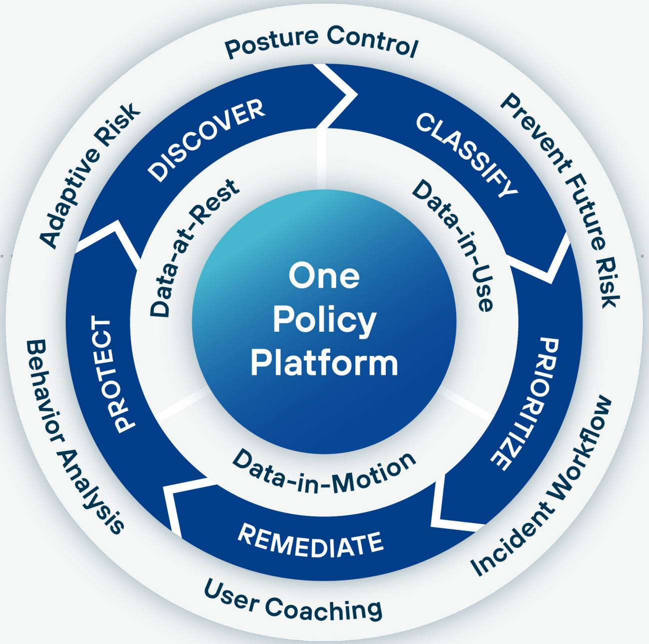
Forcepoint

Data Security Everywhere

Know | Adapt | Protect

Technology Stack

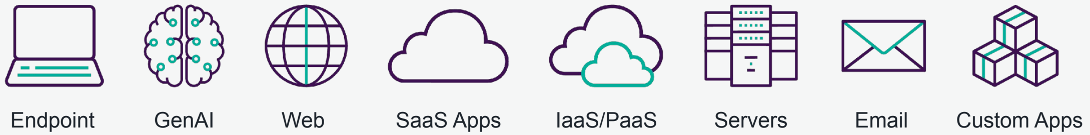
- AI Mesh
- DSPM
- DDR
- DLP
- CASB
- SWG
- Email



Platform Integrations

- Identity
- Ticketing
- SIEM
- SOAR
- XDR

Any Device, Any App, Any Location



© 2025 Forcepoint

Ďakujem

iurban@forcepoint.com
+421 905 274 378

© 2025 Forcepoint