

Information Protection

Protect and manage your sensitive data throughout its lifecycle

Mirad Maglic
Microsoft CEE



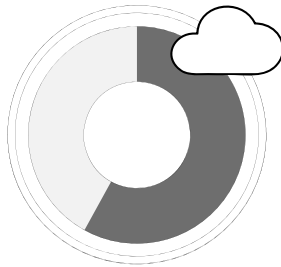
NEW WORLD OF WORK IS DRIVING CHANGE

41% of employees say mobile business apps change how they work

85% of enterprise organizations keep sensitive information in the cloud

88% of organizations no longer have confidence to detect and prevent loss of sensitive data

58% Have accidentally sent sensitive information to the wrong person



COMPLIANCE IS TOP-OF-MIND

50% year over year growth rate in electronic data

41% of organizations state enforcing of governance is their biggest issue

45% of organizations state lack of governance opens them to security and compliance risks

"My data is **scattered across sources** and the data continues to grow"

"I can't apply **unified policies across various data sources** or to a specific repository"

"When enforcing compliance our **business users' productivity is disrupted**"

"I want **data governance to be automatic** - not something I have to think about"

"How do I **protect sensitive information** such as sensitive PII data across my enterprise?"

"How do I **find only relevant data** when I need it?"

Providing clarity and consistency for the protection of personal data

The **General Data Protection Regulation** (GDPR) imposes new rules on organizations in the European Union (EU) and those that offer goods and services to people in the EU, or that collect and analyze data tied to EU residents, no matter where they are located.

- **Enhanced** personal privacy rights
- **Increased** duty for protecting data
- **Mandatory** breach reporting
- **Significant** penalties for non-compliance

Microsoft believes the GDPR is an important step forward for clarifying and enabling individual privacy rights

What are the key changes to address the GDPR?

Personal privacy

Individuals have the right to:

- Access their personal data
- Correct errors in their personal data
- Erase their personal data
- Object to processing of their personal data
- Export personal data

Controls and notifications

Organizations will need to:

- Protect personal data using appropriate security
- Notify authorities of personal data breaches
- Obtain appropriate consents for processing data
- Keep records detailing data processing

Transparent policies

Organizations are required to:

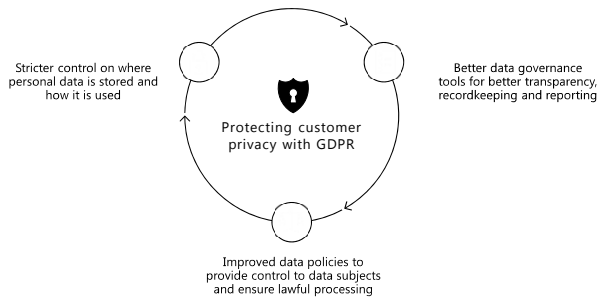
- Provide clear notice of data collection
- Outline processing purposes and use cases
- Define data retention and deletion policies

IT and training

Organizations will need to:

- Train privacy personnel & employees
- Audit and update data policies
- Employ a Data Protection Officer (if required)
- Create & manage compliant vendor contracts

What does this mean for my data?



How do I get started?

1 Discover	Identify what personal data you have and where it resides
2 Manage	Govern how personal data is used and accessed
3 Protect	Establish security controls to prevent, detect, and respond to vulnerabilities & data breaches
4 Report	Keep required documentation, manage data requests and breach notifications



GENERAL DATA PROTECTION REGULATION (GDPR)





- Enhanced personal privacy rights
- Increased duty for protecting data
- Mandatory breach reporting
- Significant penalties for non-compliance

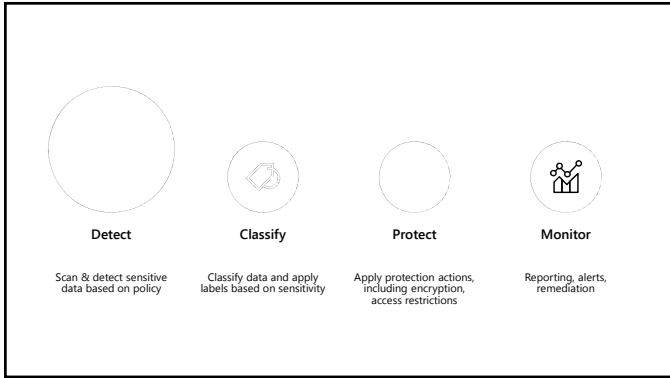
HOW YOU GET STARTED:

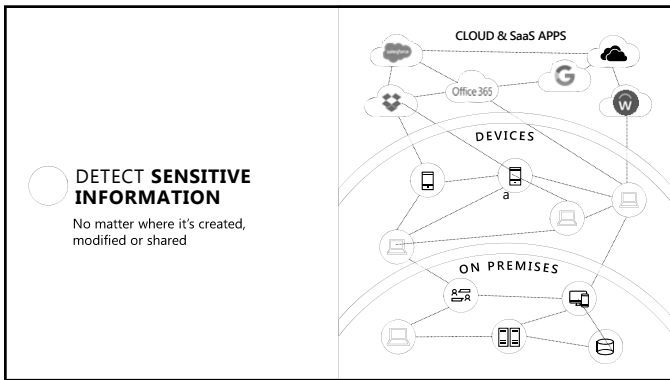
1 Discover	Identify what personal data you have and where it resides
2 Manage	Govern how personal data is used and accessed
3 Protect	Establish security controls to prevent, detect, and respond to vulnerabilities & data breaches
4 Report	Keep required documentation, manage data requests and breach notifications

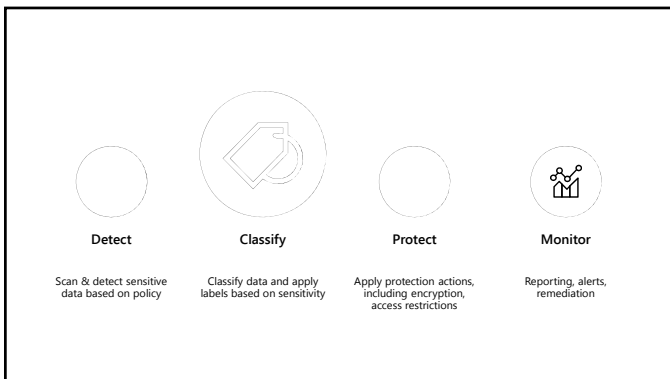
HOW DO I PROTECT SENSITIVE INFORMATION?

INFORMATION PROTECTION LIFECYCLE

			
Detect	Classify	Protect	Monitor
Scan & detect sensitive data based on policy	Classify data and apply labels based on sensitivity	Apply protection actions, including encryption, access restrictions	Reporting, alerts, remediation







CLASSIFY INFORMATION BASED ON SENSITIVITY

Automatic classification
Policies can be set by IT Admins for automatically applying classification and protection to data

Recommended classification
Based on the content you're working on, you can be prompted with suggested classification

Manual classification
You can override a classification and optionally be required to provide a justification

User-specified classification
Users can choose to apply a sensitivity label to the email or file they are working on with a single click

SENSITIVITY LABELS PERSIST WITH THE DOCUMENT

Document labeling – what is it?
Metadata written into document files

Travels with the document as it moves

In clear text so that other systems such as a DLP engine can read it

Used for the purpose of apply a protection action or data governance action – determined by policy

Can be customized per the organization's needs

CLASSIFICATION & LABELING EXAMPLE – SENSITIVE DATA

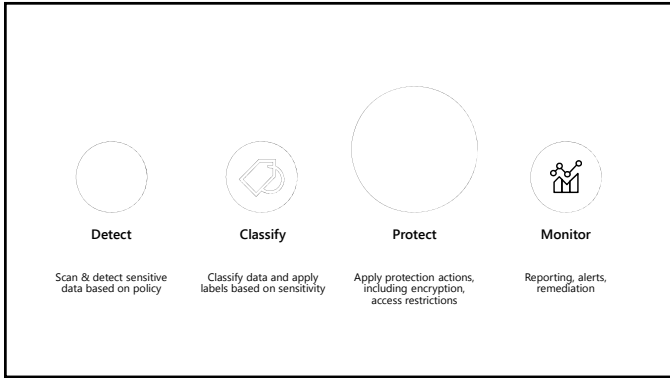
Discover personal data and apply persistent labels

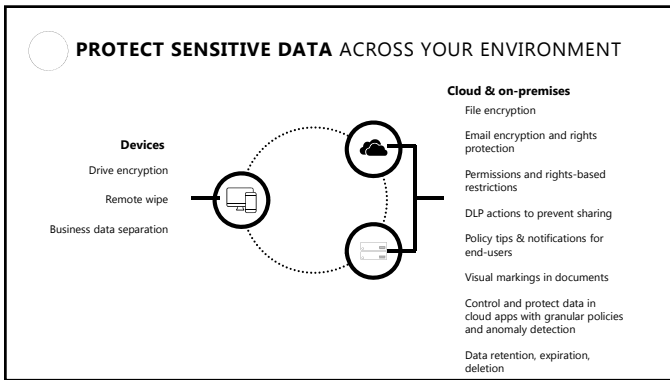
Labels are persistent and readable by other systems e.g. DLP engine

Label is metadata written to data

Sensitive data is automatically detected

Date	Description	Amount	Merchant	Transaction date	Transaction fees	Balance
7/1/2018	Ending balance	\$2,450.00	Woodgrove Bank			\$2,450.00
7/2/2018	Payment for June	-334.00	Woodgrove Bank		\$2.00	\$2,116.00
7/3/2018	Pickup Home	348.00	Homebased Trade			\$2,464.00
7/3/2018	Wine	\$600.00	Cobo Winery		\$20.00	\$3,083.00
7/6/2018	Ticket to Maui	\$489.00	Blue Yonder Air			\$3,572.00
7/12/2018	Cash withdrawal	\$654.00	Woodgrove Bank			\$2,918.00
7/3/2018	Wine	\$600.00	Cobo Winery		\$20.00	\$2,318.00








MONITOR INFORMATION PROTECTION EVENTS FOR GREATER CONTROL

Visibility

- Policy violations
- Document access & sharing
- App usage
- Anomalous activity
- End-user overrides
- False positives

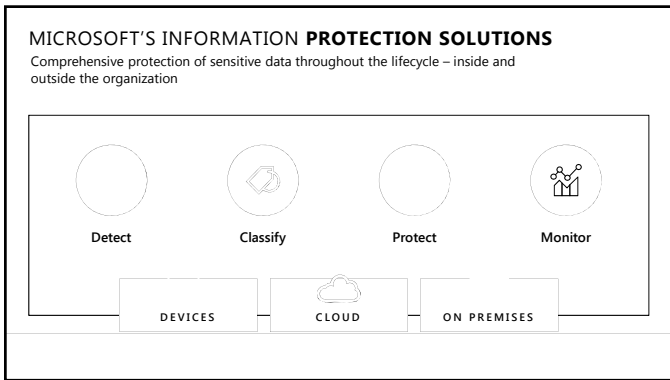
Take Action

- Tune & revise policies
- Revoke access
- Quarantine file
- Quarantine user
- Integrate into workflows & SIEM



MICROSOFT'S INFORMATION PROTECTION SOLUTIONS

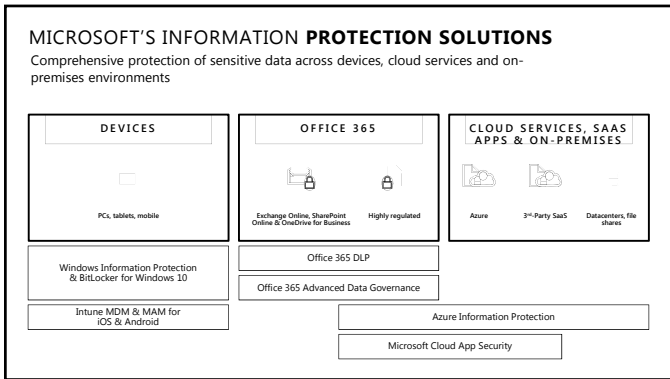
Comprehensive protection of sensitive data throughout the lifecycle – inside and outside the organization



The diagram illustrates the lifecycle of information protection across three environments: DEVICES, CLOUD, and ON PREMISES. The lifecycle consists of four stages: Detect, Classify, Protect, and Monitor. Each stage is represented by an icon: a circle for Detect, a magnifying glass for Classify, a shield for Protect, and a person with a magnifying glass for Monitor.

MICROSOFT'S INFORMATION PROTECTION SOLUTIONS

Comprehensive protection of sensitive data across devices, cloud services and on-premises environments



The diagram details Microsoft's Information Protection Solutions across three categories: DEVICES, OFFICE 365, and CLOUD SERVICES, SAAS APPS & ON-PREMISES.

- DEVICES:** Includes Windows Information Protection & BitLocker for Windows 10, and Intune MDM & MAM for iOS & Android.
- OFFICE 365:** Includes Exchange Online, SharePoint Online & OneDrive for Business (Highly regulated), Office 365 DLP, and Office 365 Advanced Data Governance.
- CLOUD SERVICES, SAAS APPS & ON-PREMISES:** Includes Azure, 3rd-Party SaaS, and Datacenters, file shares. Solutions include Azure Information Protection and Microsoft Cloud App Security.

5 Steps Program

Best Practice - Start small, do it now, and move quickly

- | | |
|-------------|--|
| 1. Classify | Take simple steps, it generates high-impact quickly (i.e. 'Do Not Forward' for HR and Legal) |
| 2. Label | Test, phase the roll out, and learn – IT can't know it all |
| 3. Protect | Control sensitive internal email flow across all PCs/Devices |
| 4. Monitor | 'Share Protected' files with business partners (B2B) |
| 5. Respond | Teach and enable users to revoke access |

Thank you!
