



Proteggi i file CAD e previeni il furto di proprietà intellettuale in conformità della regolamentazione NIS2

Feliciano Intini, Data Security, Risk, Compliance & TrustedCloud Specialist, **Microsoft**

Davide Bertarelli, Head of Cybersecurity di **4wardPRO**

Blake Wood, Vice President Global Alliances, **Secude**

AGENDA

- **NIS2 Compliance journey: perchè Microsoft**
 - *Feliciano Intini, Data Security, Risk & Compliance Specialist*
- **Data security con Microsoft Purview**
 - *Davide Bertarelli, Head of Cybersecurity 4wardPRO*
- **Protezione dei file CAD con HaloCAD**
 - *Blake Wood, Vice President Global Alliances Secude*
- **Q&A**

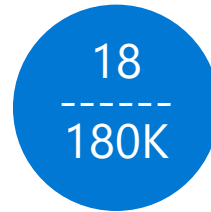


NIS2 Compliance journey: perchè Microsoft

Feliciano Intini
Data Security, Risk & Compliance Specialist



Overview of NIS2



NIS2 is the new European cybersecurity directive that will replace the existing NIS Directive as from **October 2024**.

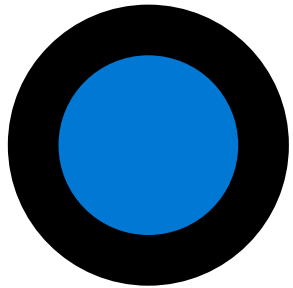
It is the most comprehensive EU cybersecurity legislation to date, covering 18 sectors and over 180K+ companies.

Its purpose is to establish a baseline of security measures for digital service providers and operators of essential services, to mitigate the risk of cyber attacks and to improve the overall level of cybersecurity in the EU.

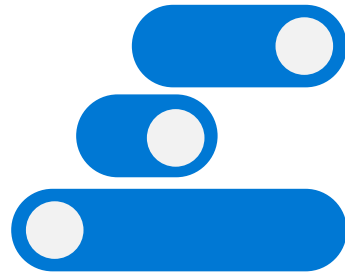
Member States have until October 17, 2024 to transpose the Directive into national law. This means that each organization encompassed by the Directive will be legally obligated to live up to its requirements by Q4 2024.

The Network Information Security Directive

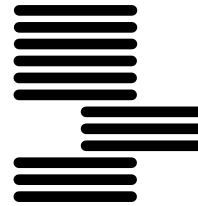
NIS2 vs. NIS1



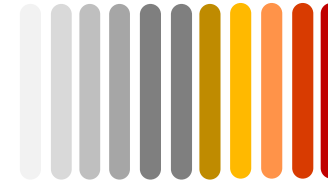
Stronger requirements and more affected sectors



Focus on securing and business continuity. This includes supply chain security.



Improving & streamlining the report obligations.



Worse Repercussions. Next to fines, NIS2 can lead to legal ramifications for management.



Enforcement localized in all European member states

NIS affects various sectors, including...

Essential Entity

Large companies are part of the sectors of high criticality listed in Annex I of the Directive.

A large entity is defined as a company with at least 250 employees

Or

with an annual turnover of at least 50 million euros or an annual balance sheet total of at least 43 million euros.

Failure to do so can result in:

Fine of >10 million Euro or 2% of global annual turnover for **essential entities** and >1.7 million Euro or 1.4% of global annual turnover for **important entities**

Important Entity

Medium-sized enterprises operating in the sectors of high criticality of Annex I of the Directive, Large or medium-sized enterprises in the sectors of Annex II of the Directive that do not fall into the essential entity category (due to their size or the type of entity involved).

A medium-sized enterprise is defined as one with at least 50 employees

Or


with an annual turnover (or balance sheet total) of at least 10 million euros, but with fewer than 250 employees

And








no more than 50 million euros annual turnover or 43 million euros balance sheet total.

Who?

Essential sectors:

-  Energy
-  Transport
-  Banking
-  Financial market infrastructure
-  Health sector
-  Drinking water
-  Wastewater
-  Digital Infrastructure
-  IT service management
-  Public administration
-  Space

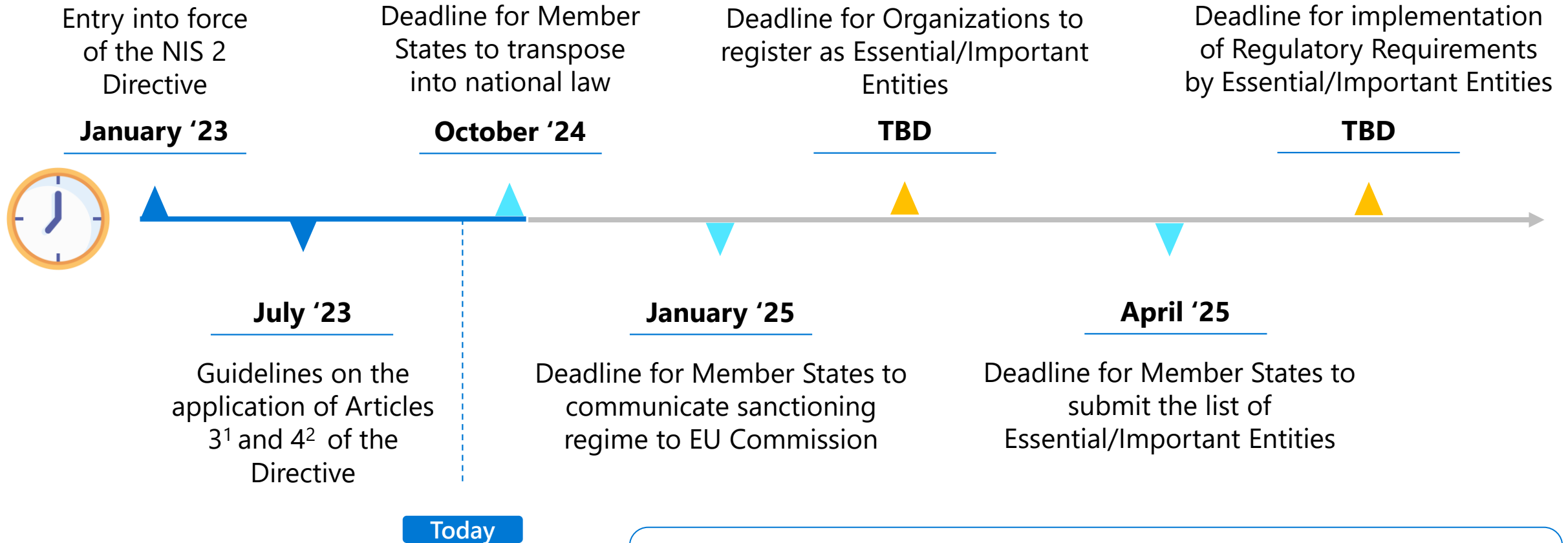
Important sectors:

-  Postal and courier services
-  Waste management
-  Chemicals
-  Food
-  Manufacturing of medical devices
-  Digital providers
-  Research organizations

New sectors included in NIS2

NIS2 Timeline

▲ Obligations to be fulfilled by Member States
▲ Obligations to be fulfilled by the Organizations



The NIS 2 Directive requires **organizations to identify themselves as essential/important entities, unlike the NIS Directive**, which gave Member States the responsibility for identifying entities in Scope

Notes: 1) Article 3 provides that Member States shall define, by 17 April 2025, a list of essential and important entities included in the scope of the Directive; 2) Article 4 provides that the provisions of the Directive do not apply to those entities that fall within the scope of sector-specific legal acts of the Union that define obligations at least equivalent to those of the Directive, in the field of Cyber risk management measures and notification of significant incidents

What does NIS2 mean for organizations?

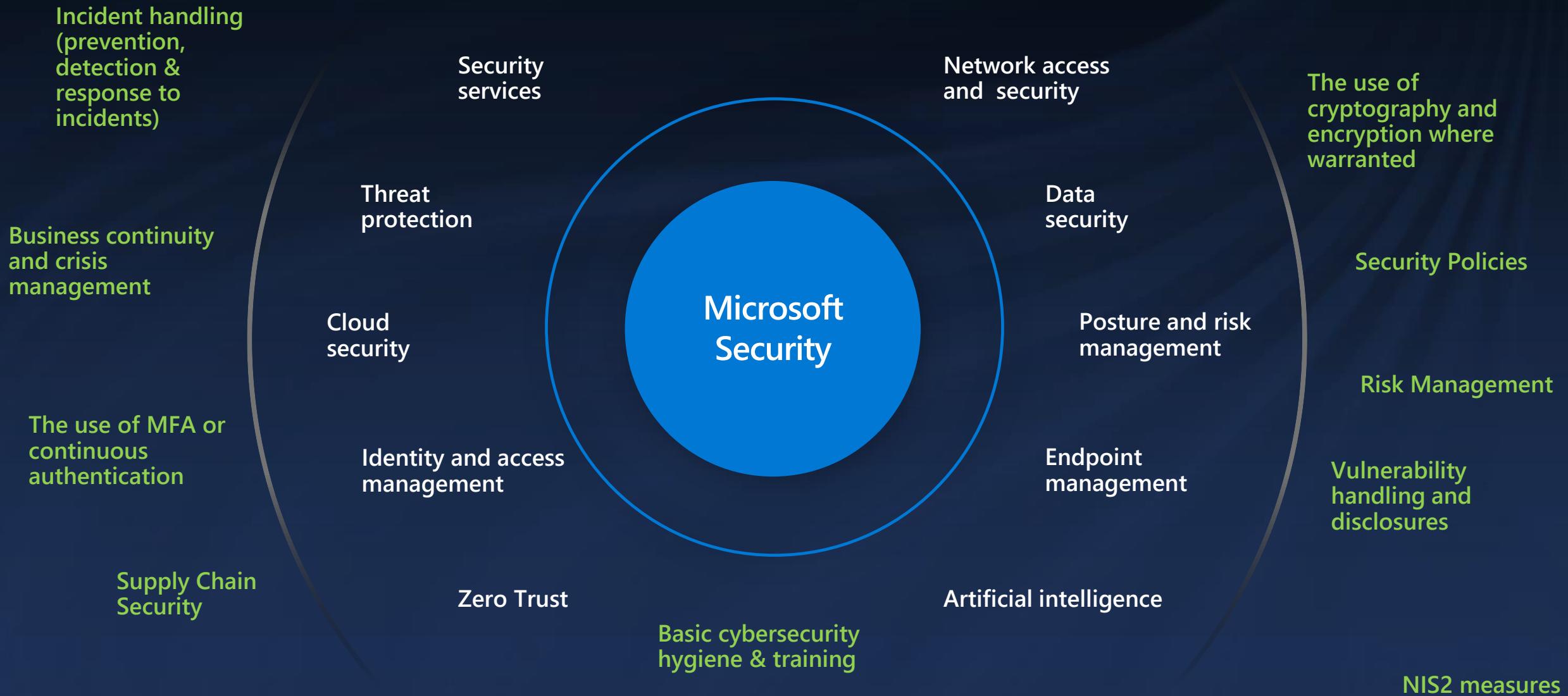
Cybersecurity Risk Management Measures

Risk Management	Security Policies	Incident handling (prevention, detection & response to incidents)	Business continuity and crisis management
Supply chain security consider supplier vulnerabilities	Vulnerability handling and disclosures	Regular assessments to determine the effectiveness of cybersecurity risk management measures (e.g., reflection of state of art – security posture)	
The use of cryptography and encryption where warranted	Basic cybersecurity hygiene & training	The use of MFA or continuous authentication	

Incident Reporting Obligations

Report incidents with significant* impact on the provision of services		
Within 24 hours	Within 72 hours an extensive report	Within 1 month a final report progress report
<p><i>*=An incident is significant if it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned or if it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage</i></p>		
Computer Security Incident Response Team (CSIRT)	Competent Authority	Recipients of services

Microsoft leads with end-to-end protection



Microsoft's integrated Security platform

Multicloud

Multiplatform



Cloud platforms



Microsoft Defender



Microsoft Sentinel



Microsoft Entra



Microsoft Intune



Microsoft Purview



Microsoft Priva

Device OSs



NIS Objectives & Principles vs Microsoft Technology

NIS Principles	Microsoft Solution	Comments
Governance	Defender CSPM, Entra	
Risk Management	Defender XDR and Purview Compliance Manager and Insider Risk Management	NIS2 template in Compliance Manager released
Asset Management	Defender CSPM, Defender for Endpoint	
Supply Chain	Defender XDR, Entra and DevOps	
Service Protection	Defender for API	In Preview
Identity & Access	Entra	
Data Security	Microsoft 365 Purview (Information Protection, Data Loss Prevention, Insider Risk Management)	
System Security	Defender for Endpoint, Defender for IoT and Intune	
Resilient Networks	Azure Network Security	3rd party integration with the major NDR vendors
Staff Awareness	O365 Phishing Simulation, Learning Paths, Policy Tips in Purview	
Security Monitoring	Microsoft Sentinel	
Proactive Security	Defender XDR	
Response and Recovery	Defender XDR, Azure Backup and Recovery	3rd party integration with major DR vendors

NIS2 Purview Compliance Manager Assessment template (New!)

The screenshot displays the Microsoft Purview Compliance Manager interface for Contoso Electronics. The breadcrumb trail is: Compliance Manager > Regulations > NIS2 Directive (EU) 2022/2555 of the European Parliament and of the Council. The main heading is "NIS2 Directive (EU) 2022/2555 of the European Parliame...". A "Service" dropdown menu is set to "Microsoft 365".

The left-hand navigation pane includes the following items:

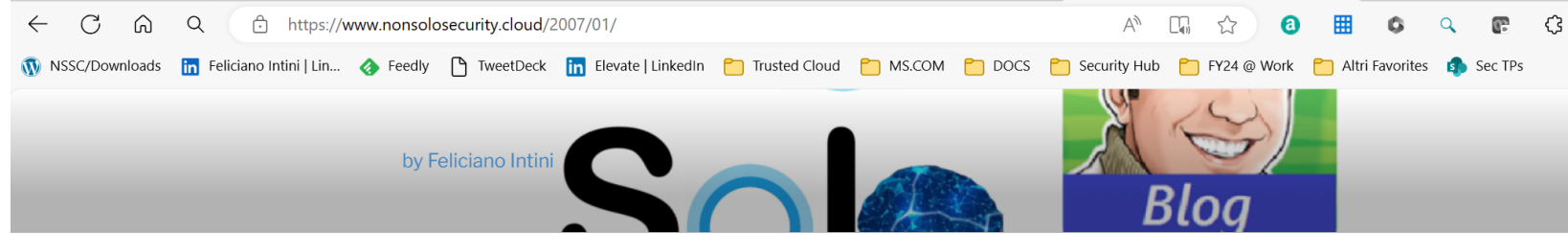
- Home
- Compliance Manager
- Data classification
 - Overview
 - Classifiers
 - Content explorer
 - Activity explorer
- Data connectors
- AI hub (preview)
- Alerts
- Policies
- Roles & scopes
- Trials
- Solutions
 - Catalog
 - App governance
 - Audit
 - Content search
 - Communication compliance
 - Data loss prevention

The main content area is divided into two sections:

- Overview**: Contains links for Details, About, and Feedback.
- Controls**: Shows 142 items with a search bar and a filter set to "Control family: Any". Below this is a table with columns: Control title, Control ID, Achievable points, and Improvement act.

Control title	Control ID	Achievable points	Improvement act
> Competent authorities and single points of contact	(5)		
> Computer security incident response teams (CSIRTs)	(10)		
> Cooperation at national level	(6)		
> Cooperation Group	(8)		
> Coordinated vulnerability disclosure and a European vulnerability database	(2)		
> CSIRTs network	(6)		
> Cybersecurity information-sharing arrangements	(5)		
> Cybersecurity risk-management measures	(5)		
> Database of domain name registration data	(6)		

At the heart of every cybersecurity hardening effort, there's always the DATA SECURITY



MONTH: JANUARY 2007

10 JANUARY 2007

"Piano dell'opera"

[This blog post has been republished as-is on February 2019]

So bene di non essere l'Oxford English Dictionary (... sapevate che la terza edizione verrà completata tra 20-25 anni e passerà dagli attuali 20 volumi a 40 tomi per un totale di circa 1.000.000 di parole ???), ma oggi parlare di *Microsoft Security* vuol dire toccare una serie di tecnologie, funzionalità, servizi e prodotti che spaziano a 360° sullo spettro del tema Sicurezza Informatica. Ritengo quindi opportuno dare un ordine ai temi che toccherò via via, e per farlo utilizzerò la tassonomia che utilizziamo nel nostro gruppo *Premier Center for Security* (il PCFS è il gruppo operativo di sicurezza di Microsoft Italia di cui faccio parte...seguirà post di approfondimento!), diretta estensione del modello **Defence-In-Depth (DiD)**, il quale prevede di operare delle attività di hardening a tutti i livelli che devono essere attraversati da un intrusore per tentare di accedere all'informazione da carpire/compromettere:

Network Security

Esempi: ISA Server, IPSEC, Soluzioni di Server&Domain Isolation, Wireless Security, VPN, NAP,...

Host Security

Esempi: hardening del sistema operativo di base, Security Update Management, Soluzioni Anti-Malware,...

Application Security

Esempi: hardening di applicazioni server (Exchange, SQL,...), ...

Data Security

Esempi: Rights Management Services, Encrypted File System, Bitlocker, Secure Messaging, ...

Security Foundations (Technology)

Esempi: Active Directory Security, Infrastrutture PKI (Smart Card, CLM, ...), Soluzioni di Identity Management, Forensic Analysis ...

Security Foundations (Processes)

Esempi: Security Policy aziendali e Compliance Management, Security Risk Management, Security Monitoring e Auditing, Security Incident Response

Search ...



MY PAGES

About Feliciano Intini

Downloads

Microsoft 365 Compliance readiness resources

Privacy Policy

RECENT POSTS

Benvenuta Microsoft Purview, la nuova

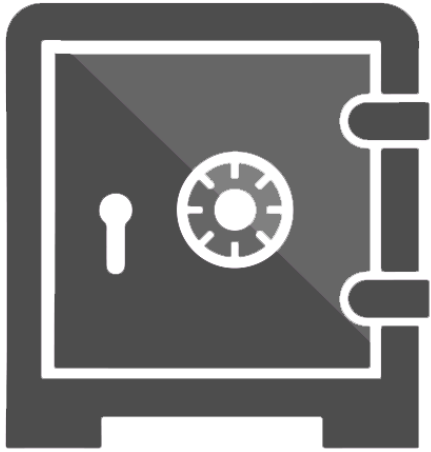


DATA SECURITY CON MICROSOFT PURVIEW

Davide Bertarelli
Head of Cybersecurity 4wardPRO



WHY DO WE NEED TO PROTECT DATA?



Confidentiality of information

Compliance with laws and regulations



What does NIS2 mean for organizations?

Cybersecurity Risk Management Measures

Risk Management	Security Policies	Incident handling (prevention, detection & response to incidents)	Business continuity and crisis management
Supply chain security consider supplier vulnerabilities	Vulnerability handling and disclosures	Regular assessments to determine the effectiveness of cybersecurity risk management measures (e.g., reflection of state of art – security posture)	
The use of cryptography and encryption where warranted	Basic cybersecurity hygiene & training	The use of MFA or continuous authentication	

Incident Reporting Obligations

Report incidents with significant* impact on the provision of services		
Within 24 hours	Within 72 hours an extensive report	Within 1 month a final report progress report
<p><i>*=An incident is significant if it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned or if it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage</i></p>		
Computer Security Incident Response Team (CSIRT)	Competent Authority	Recipients of services

TOP DATA SECURITY CONCERNS



Data security incidents are widespread

83%

of organizations experience more than one data breach in their lifetime¹

Malicious insiders account for 20% of data breaches, adding to costs

\$15.4M

Total average cost of activities to resolve insider threats over 12 month period²

Organizations are struggling with a fragmented solution landscape

80%

of decision makers purchased multiple products to meet compliance and data protection needs³

1. Cost of a Data Breach Report 2022, IBM

2. Cost of Insider Threats Global Report 2022, Ponemon Institute

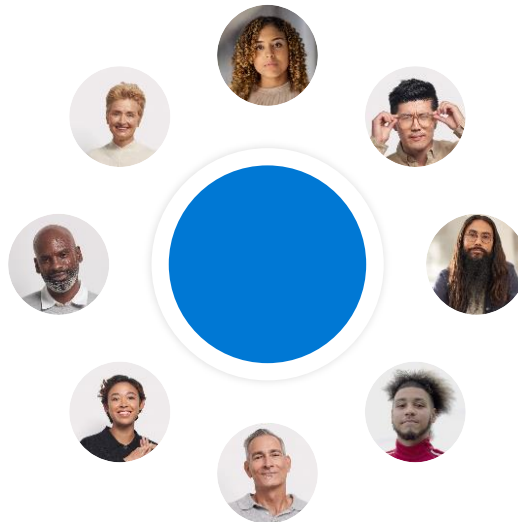
3. February 2022 survey of 200 US compliance decision-makers (n=100 599-999 employees, n=100 1000+ employees) commissioned by Microsoft with MDC Research

ORGANIZATIONS NEED TO...

Protect sensitive data wherever it lives throughout its lifecycle



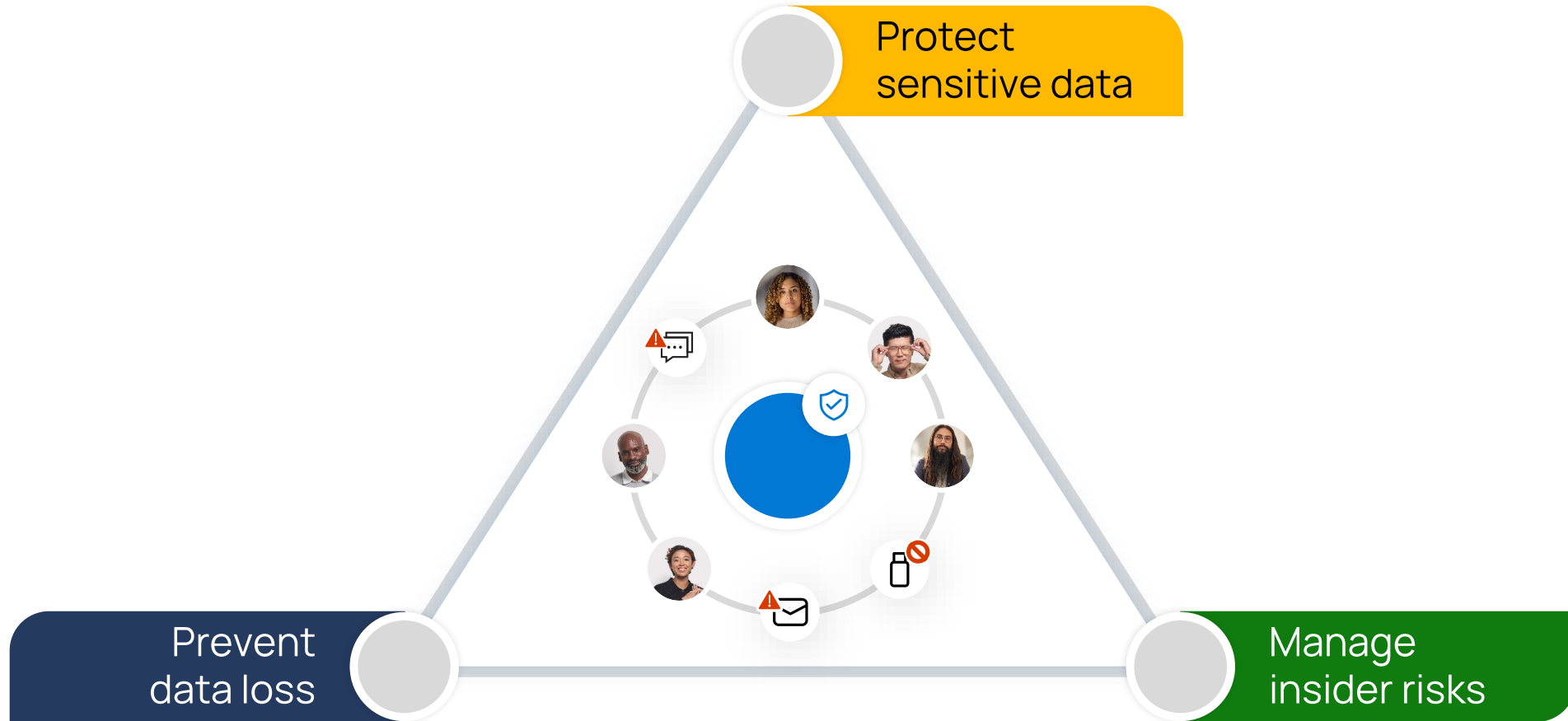
Understand user activity context around the data and identify risks



Prevent data from unauthorized use across apps, services, and devices



MICROSOFT'S APPROACH TO DATA SECURITY



PROTECT SENSITIVE DATA



Microsoft Purview Information Protection

Discover and classify data at scale using *automation and machine-learning*

Safeguard data throughout its lifecycle with labeling and encryption *built into* productivity tools

Extend the protection experience across environments to protect data wherever it lives





MANAGE INSIDER RISKS

Microsoft Purview Insider Risk Management

Protect *user trust* and build a holistic insider risk program with *pseudonymization* and strong privacy controls.

Identify hidden risks with 100+ *built-in machine-learning models* and indicators, requiring no endpoint agents.

Expedite mitigation with enriched investigations and *adaptive protection* that enforce controls dynamically.

PREVENT DATA LOSS



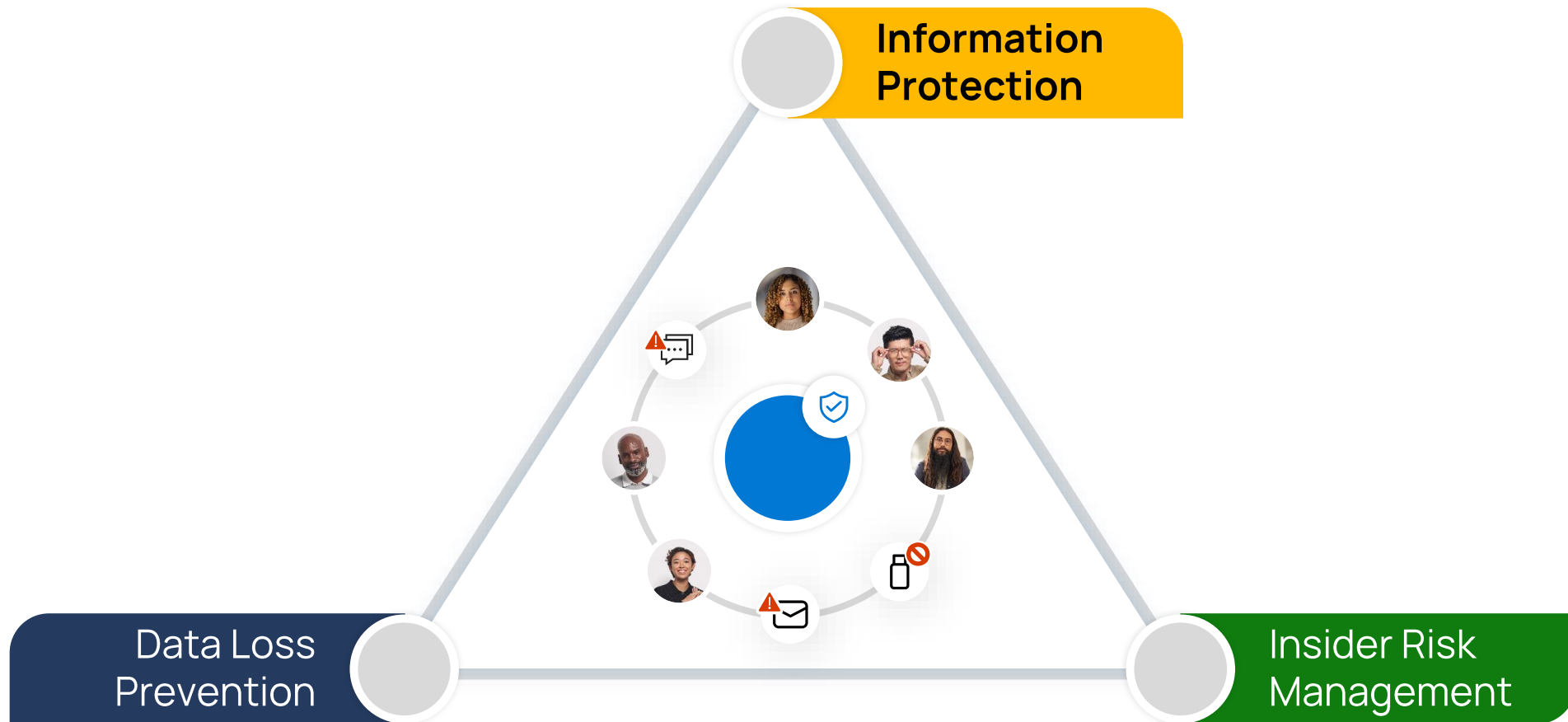
Microsoft Purview Data Loss Prevention

Cloud native with *built-in protection* in Microsoft 365 apps, services, and windows endpoints - *no on-premise infrastructure or agents needed*

Balance protection and productivity with granular policy controls and manage DLP policies all workloads from *a single location*

Leverage *classification and user activity* insights to better inform DLP polices and benefit from an *integrated incident management*

DATA SECURITY WITH MICROSOFT PURVIEW





FORTIFY DATA SECURITY WITH AN INTEGRATED APPROACH



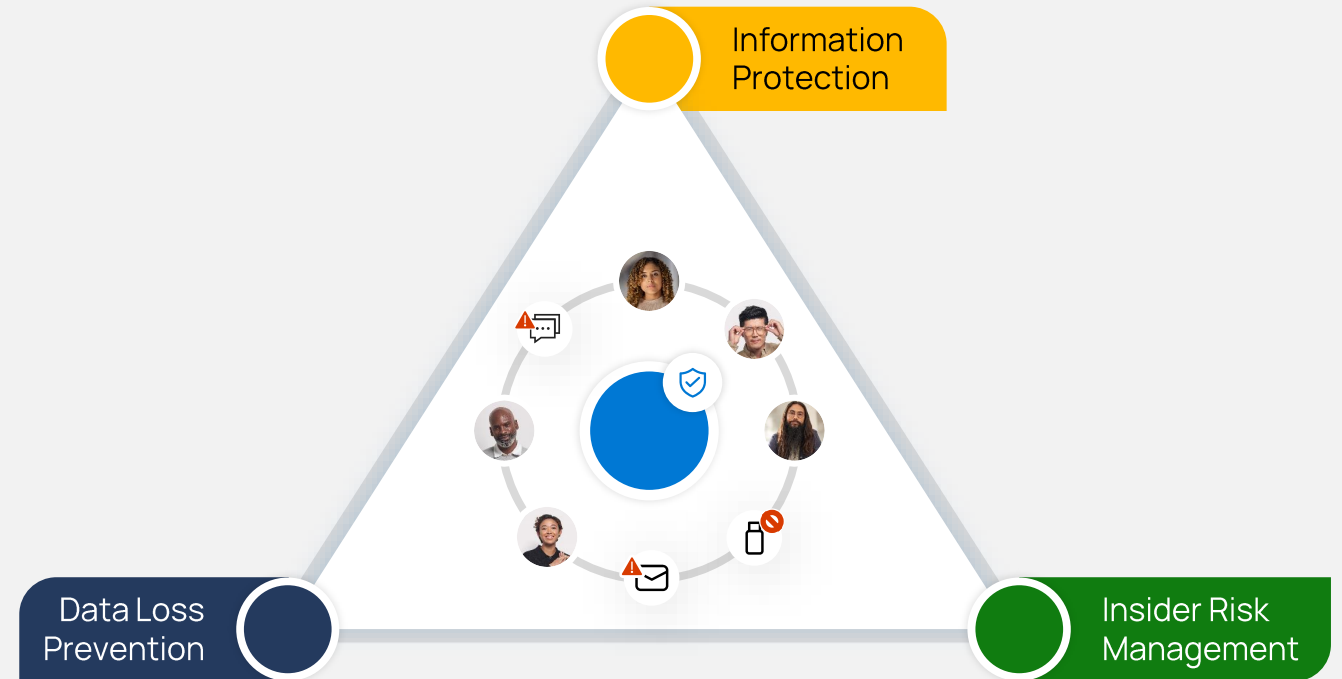
Discover and auto-classify data and prevent it from unauthorized use across apps, services, and devices



Understand the **user intent and context around sensitive data** to identify the most critical risks



Enable **Adaptive Protection** to assign appropriate DLP policies to high-risk users



Support for multi-cloud, hybrid, SaaS data | Partner ecosystem

Purview Information Protection platform coverage



Integrated configuration
management in the cloud



Microsoft 365 (aka Office)



Microsoft 365 for Mac



Microsoft 365 Apps for
Android
Viewer app



Microsoft 365 Apps for iOS
Viewer app



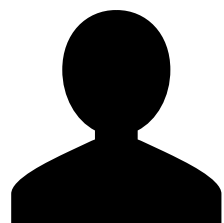
Web

Purview data classification



- Labels are **metadata** inside the document and readable from applications and services.
- They are **customizable**, to meet the specific needs of the organization
- Labels are **persistent** data that travels with the document
- Each document can have a maximum of **one label** at a time

Data classification usage



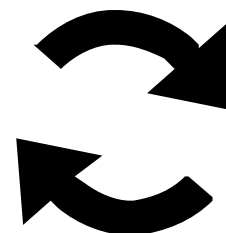
User set

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



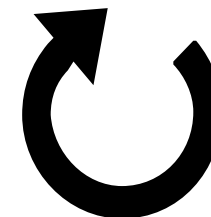
Recommended

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



Reclassification

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



Automatic

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

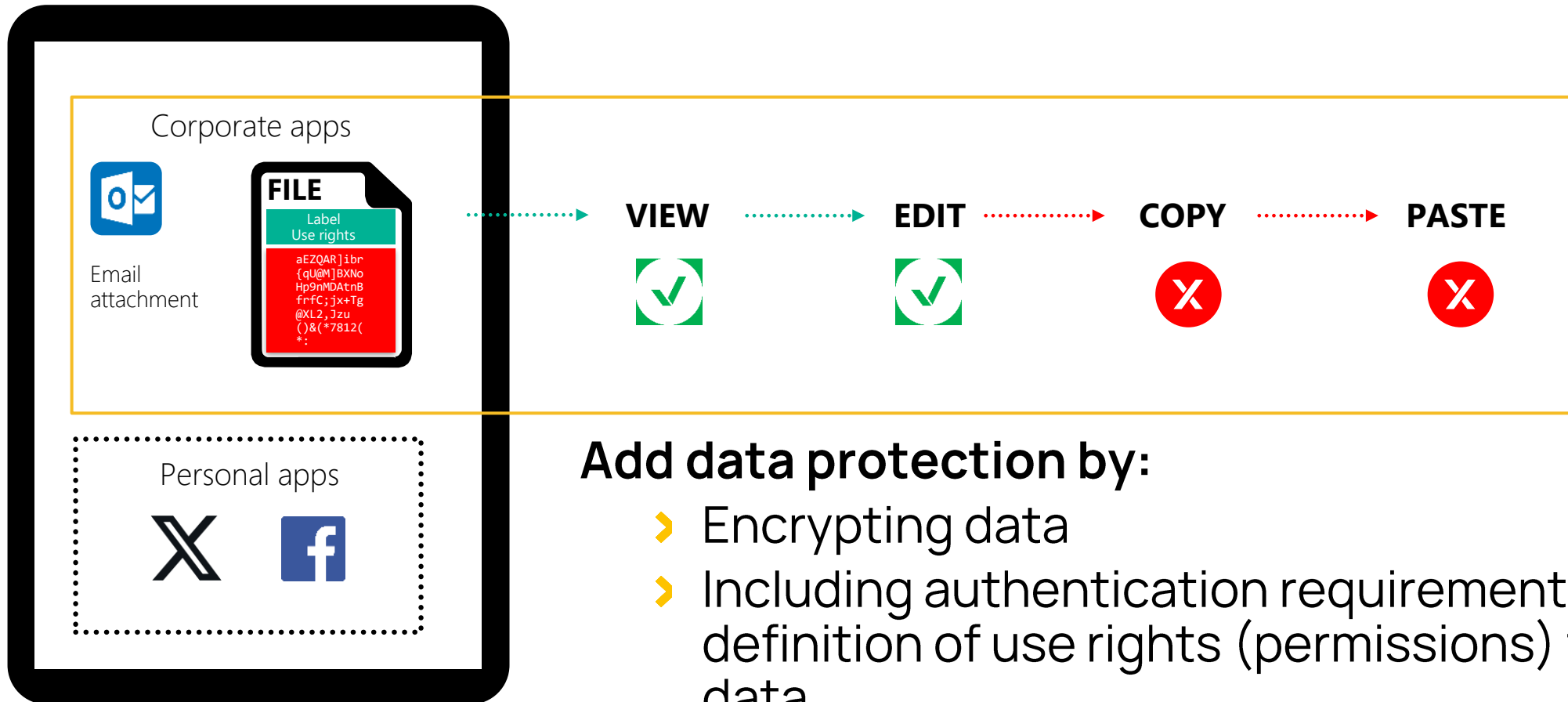
Manual Classification

User experience

The image shows a composite screenshot of Microsoft Office applications. On the left, a Microsoft Word document is open, displaying a 'Message' window with a 'Sensitivity Labels' section. The main content of the Word document is a financial summary table. In the center, a file save dialog box is open for 'Financial Summary.xlsx', with a red box highlighting the 'Sensitivity' dropdown menu. The dropdown menu is currently set to 'Confidential\All Employees' and lists other options: 'Personal', 'Public', 'General', 'Confidential', and 'Highly Confidential'. On the right, a Microsoft Excel spreadsheet is visible, showing a table with columns for 'Year 1' and 'Year 2' and rows for various financial metrics. The cell containing '44,574.00' is highlighted with a green border.

	Year 1	Year 2
Revenue	93,580.00	60,543.00
Gross margin	18,161.00	12,193.00
Operating income	1.48	1.24
Net income	96,526.00	174,303.00
Diluted earnings per share	1.44	1.44
Cash dividends declared	0.00	0.00
Cash, cash equivalents	0.00	0.00
Total assets	0.00	0.00
Long-term obligations	4.00	44,574.00

Protect data against unauthorized use



Add data protection by:

- Encrypting data
- Including authentication requirement and a definition of use rights (permissions) to the data
- Providing protection that is persistent and travels with the data

Supported and required formats

Coverage for popular formats + extensibility

Microsoft 365 Apps formats*



PDF



*file version "97-2003" and later

Extend sensitivity labeling with **File Explorer on Windows** for other supported file formats:



Microsoft Purview Information Protection client

Microsoft support

AutoCAD



SAP



Others



HaloCAD

HaloCore

Information Protecion Software Development Kit

Partners support

Information Protection **adoption**



CISO



Compliance Officer



Data Admin



Data owner



Help Desk



IW



DEFINE CLASSIFICATION
SCHEME



DEFINE ALL
CLASSIFICATION POLICY
CONDITIONS



CREATE/TEST AND
DEPLOY
CLASSIFICATION POLICY



ONGOING USAGE,
MONITORING AND
REMEDATION

Adoption strategy: where do I start?



Who owns my data?

Find your data owners. Start the with people responsible for the business process.



What types of data do I have?

Not file type. What business process produces the data? Why does it matter to your business?



Where is my data?

Strategy may differ depending on it. Think about how it travels.



Why is it a risk?

All data is not the same. Understand who is worried about what and why.



Keep it simple stupid

Don't create a hairball. Think of labels as segments based on agreed upon risk. Initially be conservative with policy/enforcement



Start Slow

Bring your people along. Limit confusion/mistakes by knowing the difference between one- and two-way doors

Protezione dei file CAD con HaloCAD

Proteggi i dati sensibili • Prevenire costose fughe di notizie • Garantire la conformità alle normative



Blake Wood, CISSP CCSP
VP of Global Alliances



Member of Microsoft
Intelligent Security Association



The NIS2 Regulation



Primary Goals

- To protect intellectual property – via data leakage or data breach
- To secure the manufacturing supply chain – Especially when sharing CAD files
- Achieve compliance by 17 October 2024

Affected Manufacturers

- >250 employees or > €50M
- Chemicals, food, medical devices, computers, electronics, machinery, and **motor vehicles**



VW Beetle



Porsche Macan



Toyota Land Cruiser



Ora Punk Cat



Zotye SR8



Hengtian L4600

Similar Regulations in the EU and Abroad

- Digital Operational Resilience Act - DORA (EU)
- Cybersecurity Maturity Model Compliance – CMMC 2.0 (US)

CAD Files

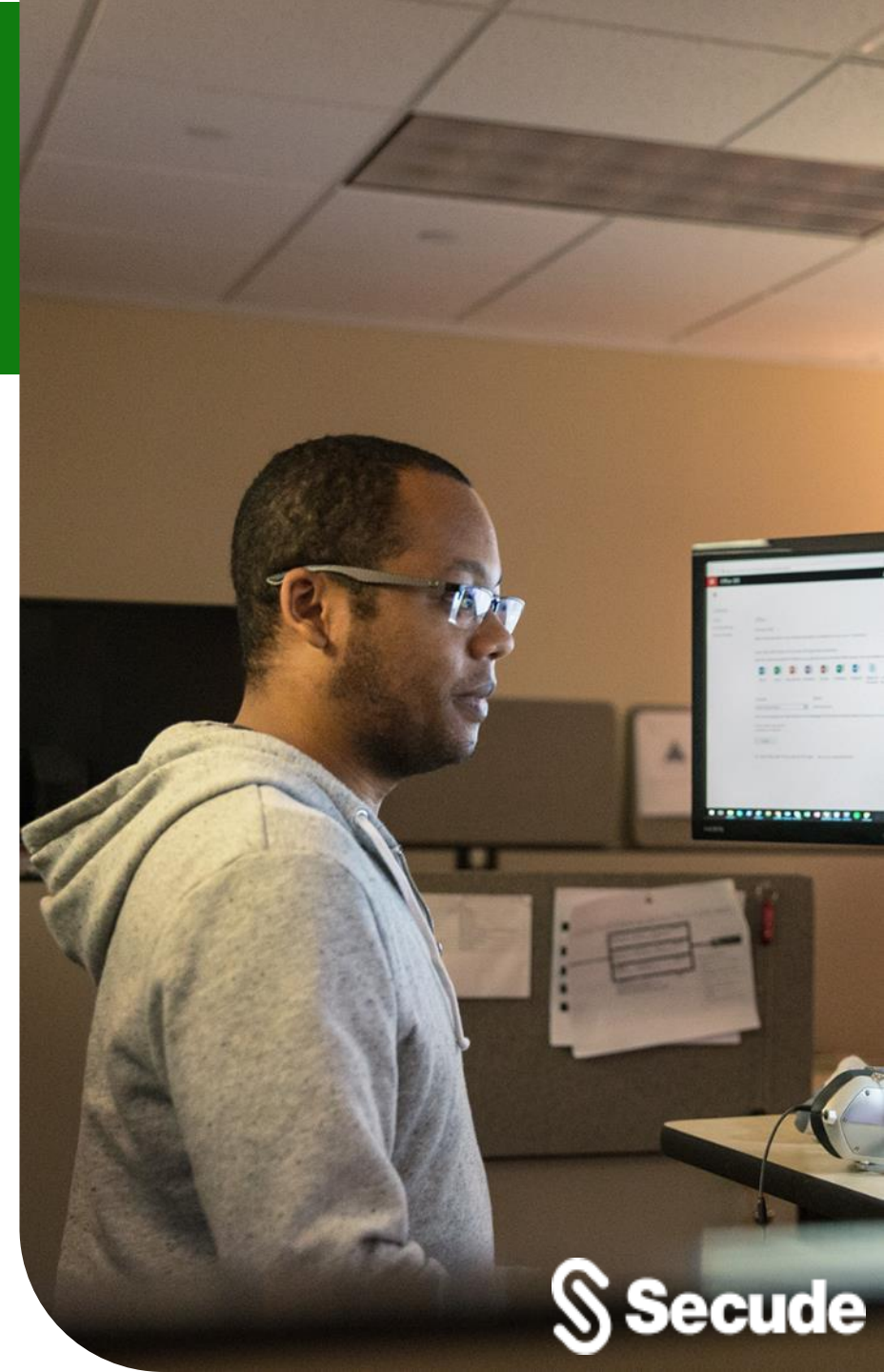
Challenges securing this intellectual property

Difficult to classify and protect CAD data

- Many software vendors and proprietary file formats to support
- Product Lifecycle Management (PLM) systems also complicate this
- A challenge for Off-The-Shelf DLP and Data Governance platforms like MS Purview

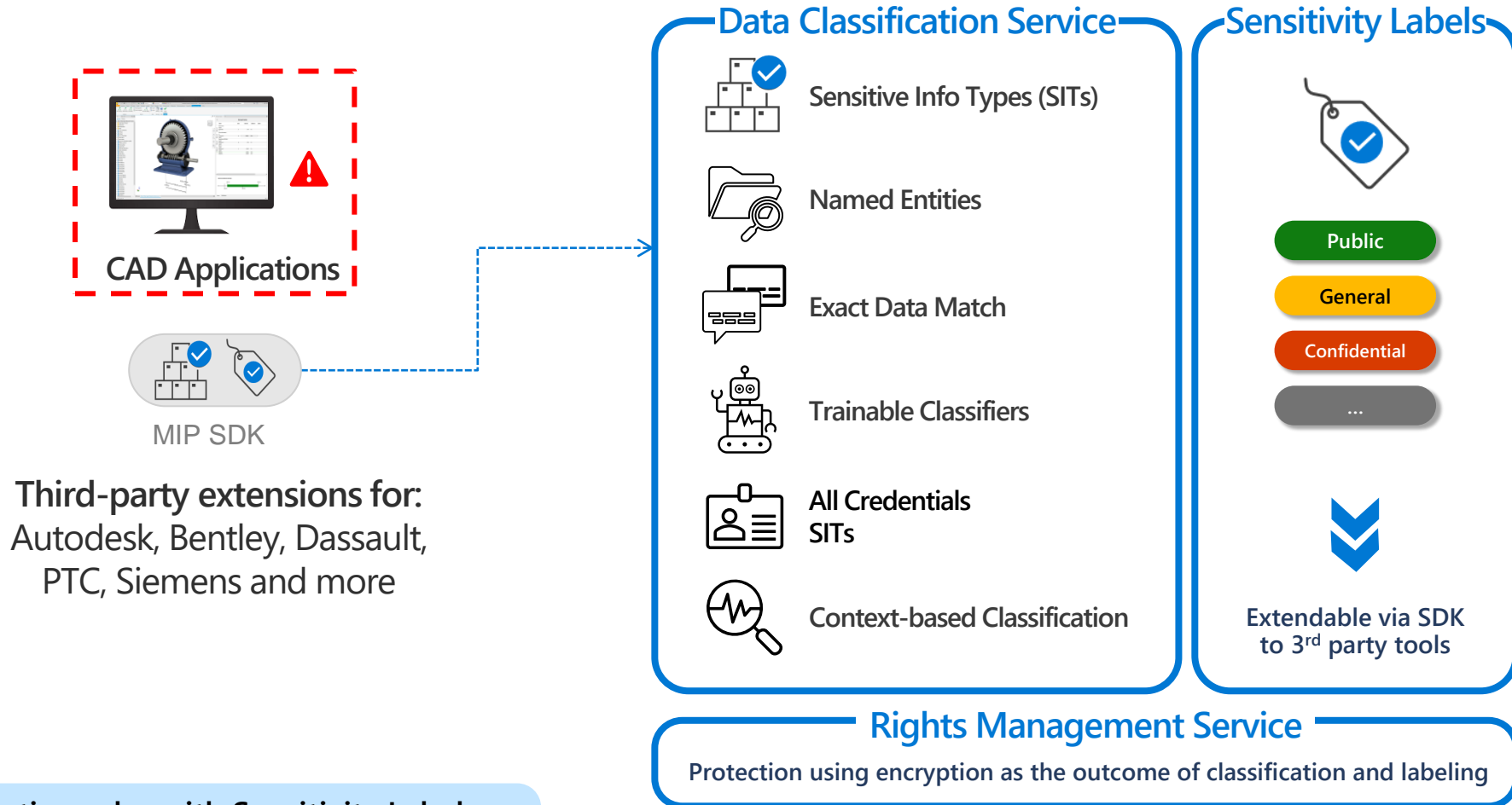
Software Vendor	CAD Product	HaloCAD Supported File Formats
Autodesk	AutoCAD	.dwg, .dxf
Autodesk	Inventor	.ipt, .iam, .idw, .ipn
Bentley	MicroStation	.dgn
Dassault	Solidworks	.sldprt, .sldasm, .slddrw, .sldprt
PTC	Creo	.asm, .prt, .mfg, .drw, .frm, .lay, .sec, .cem
Revit	Revit	.rvt, .rfa
Siemens	NX CAD	.prt, .jt
Siemens	Solid Edge	.par, .psm, .asm, .dft
N/A	CAD neutral formats	.step, .iges

Software Vendor	PLM System
Autodesk	Vault Basic
Autodesk	Vault Professional
Dassault	SolidWorks PDM
Keytech	PLM
PTC	Windchill
SAP	ECTR
Siemens	Teamcenter



Microsoft Purview Information Protection (MPIP)

Extending MPIP through CAD Application Integration



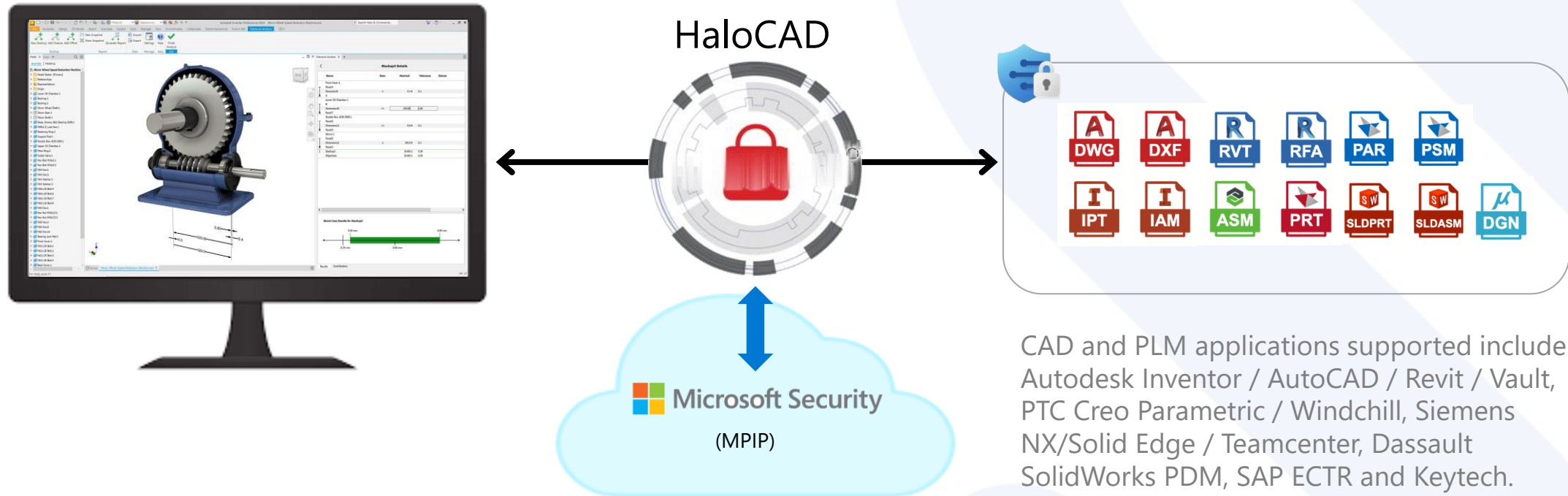
Enforce application rules with Sensitivity Labels

Enforce file access controls with Sensitivity Labels

Native integration with Microsoft 365 apps and services

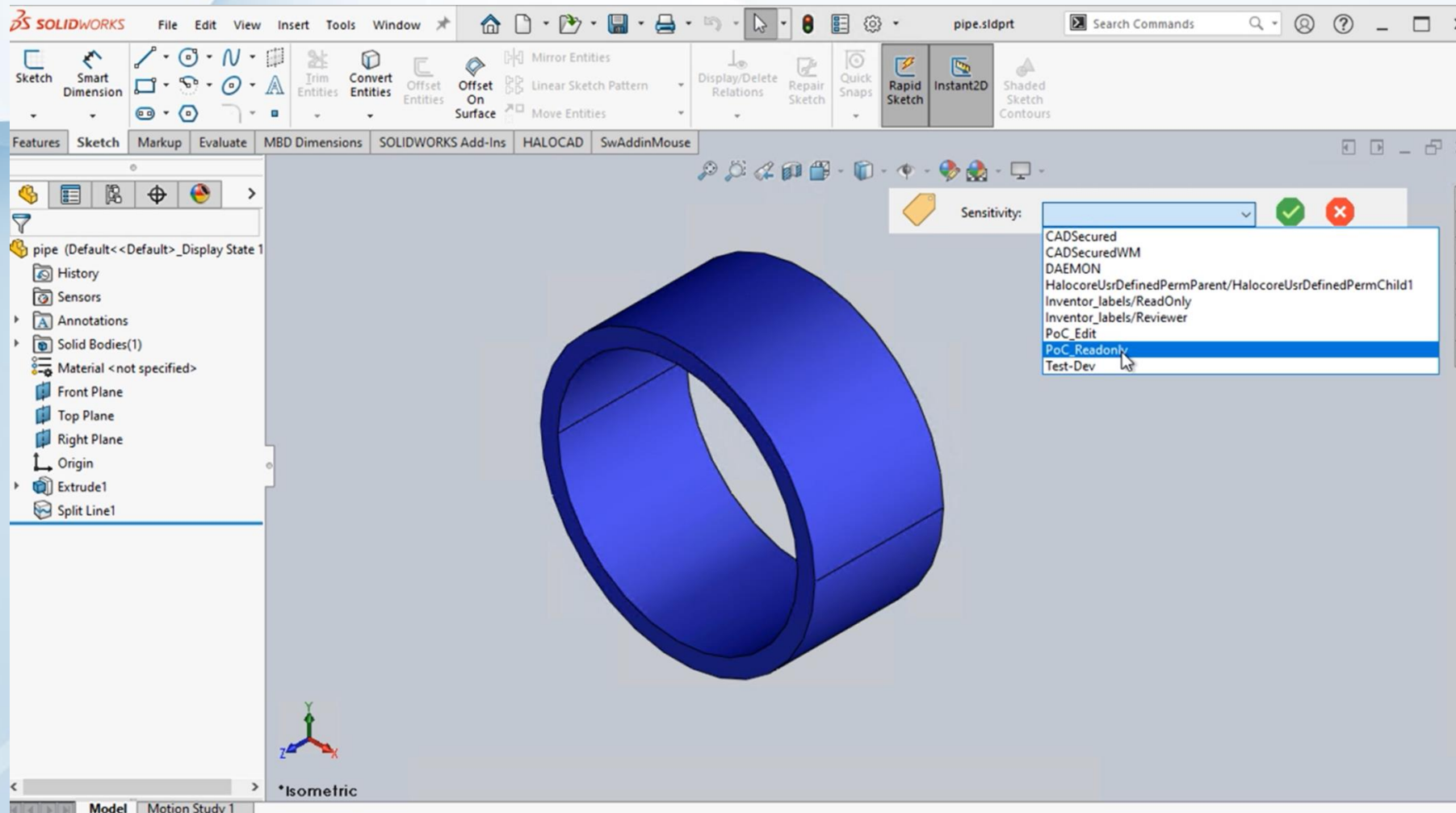
HaloCAD Plugs Directly into CAD and PLM Applications

Extend Microsoft Purview Information Protection to support multiple CAD file formats, automatically securing CAD/PLM data and **protecting your IP**

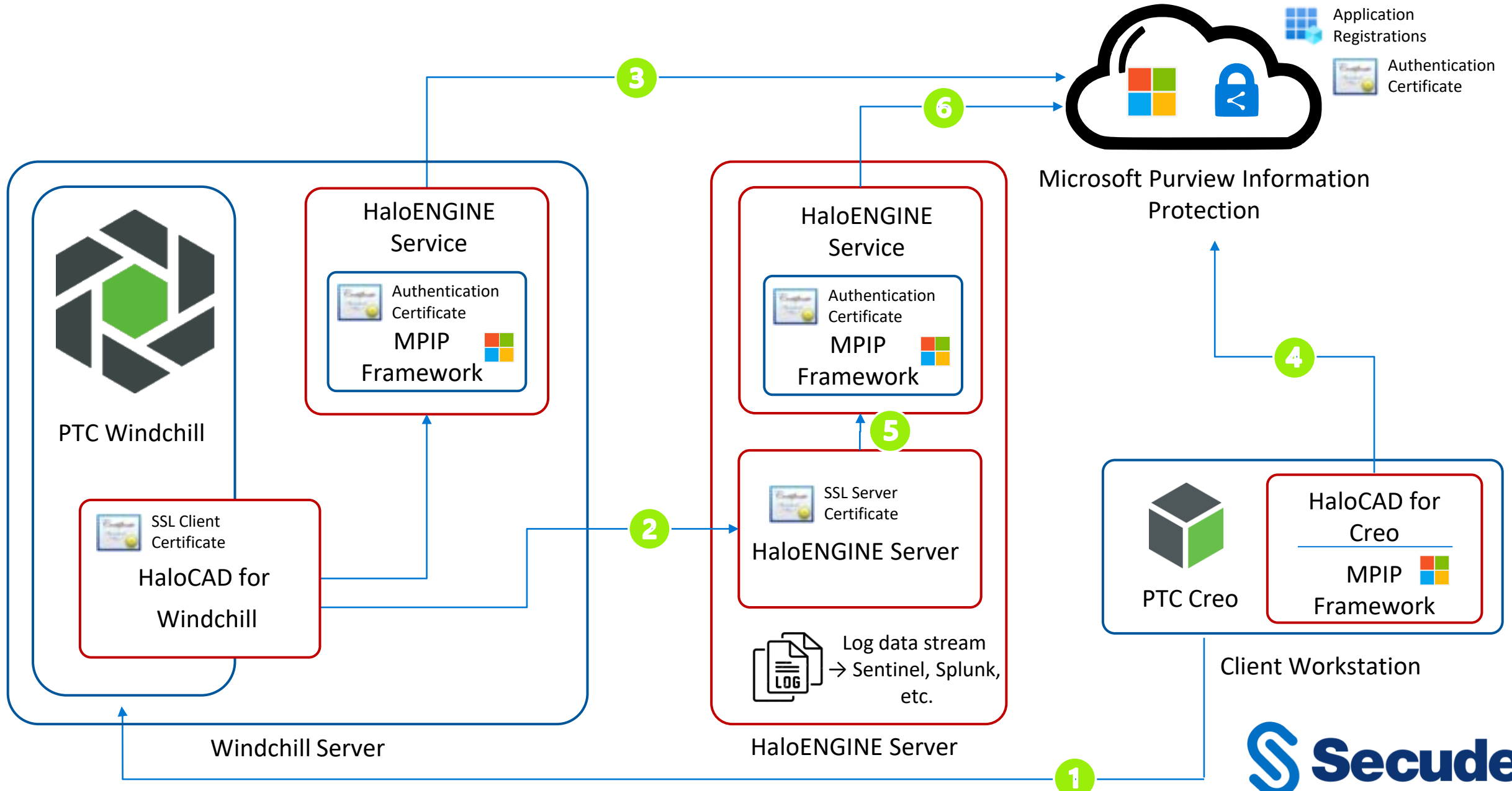


CAD and PLM applications supported include Autodesk Inventor / AutoCAD / Revit / Vault, PTC Creo Parametric / Windchill, Siemens NX/Solid Edge / Teamcenter, Dassault SolidWorks PDM, SAP ECTR and Keytech. Planned support : Dassault DraftSight and CATIA.

Example: HALOCAD for Dassault Solidworks



Halocad Architecture with Product Lifecycle Management (PLM)



HaloENGINE: Mapping Security Controls from Product Lifecycle Management (PLM) to MPIP Sensitivity Labels

The image displays two configuration panels in the HaloENGINE interface. The left panel, titled "Classification Rule", shows a rule configuration with the following details:

- Rule Result: CONFIDENTIAL
- System Type: WINDCHILL
- Construct Rule: A table with columns Metadata, Condition, and Value. It contains two rows: FILE_TYPE Equal *.prt and AND PRODUCT_NAME Equal new_product.
- Buttons: Deactivate Rule, SAVE, CANCEL.

The right panel, titled "Action Rule", shows an action configuration with the following details:

- Info: If the file only needs to be passed through, do not create an action for the file's classification.
- Choose Resulting Actions: A list with checkboxes for Block, Protect/Label, and Notify. The Protect/Label option is selected, and its value is set to HCAD Confidential. A "CHOOSE LABEL" button is visible next to it.
- Complete Action: Label
- System Type: WINDCHILL
- Construct Rules: A table with columns Property, Condition, and Value. It contains one row: Sensitivity Equal CONFIDENTIAL.
- Buttons: Deactivate Rule, SAVE, CANCEL.

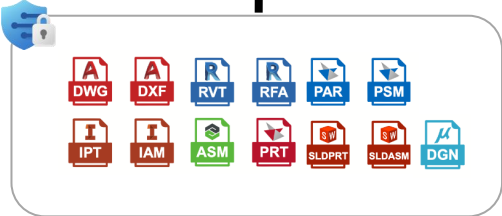
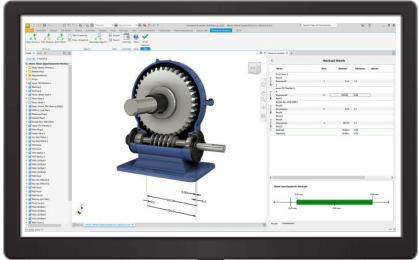
A red arrow points from the "CONFIDENTIAL" dropdown in the Classification Rule to the "HCAD Confidential" dropdown in the Action Rule. A red box highlights the "Protect/Label" action and its value field.

Automated mapping of access & usage controls to the corresponding MPIP label

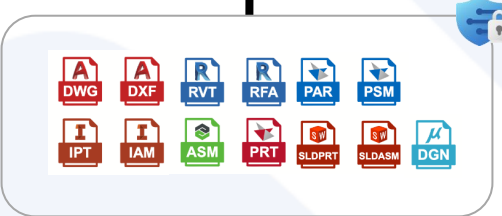
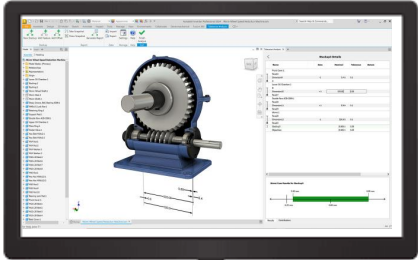
Secure CAD Collaboration

Extend Microsoft Purview Information Protection to CAD/PLM data and **secure the manufacturing supply chain**

Company 1
Designer



Company 2
Partner



File labeling, policies and access controls follow the file wherever it travels making it Zero Trust by default.



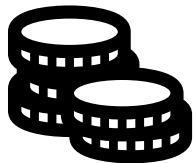
BOOK YOUR FREE POC NOW!

Scan the Qrcode to reserve your spot and receive a tailored complimentary PoC.

CSI Program
UP TO \$10K



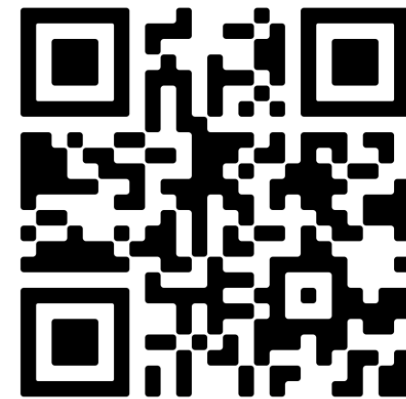
**PROTECT
SENSITIVE DATA**



**PREVENT COSTLY
LEAKS**



**ENSURE REGULATORY AND
NIS2 COMPLIANCE**



SCAN ME

Q&A

