



# Cómo proteger tus datos críticos de negocio en Microsoft 365



SaaS Level Up

Impulsa tu negocio SaaS



# Agenda

Secure Critical Data with Zero Trust

Identity Governance and Security

Microsoft Information Protection

Microsoft 365 Backup with Barracuda Cloud-to-Cloud Backup

Microsoft Defender

Microsoft Cloud App Security

Barracuda Sentinel

Data Security Audit with ArexData



SaaS Level Up

## Zero Trust

**Isabel Gómez**  
SaaS Level Up CEO

plain  
concepts 



# Microsoft Zero Trust Principles

## Guidance for technical architecture



### Verify explicitly

Always validate all available data points including

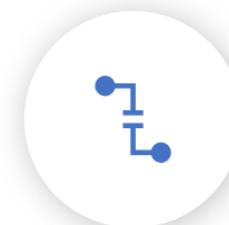
- User identity and location
- Device health
- Service or workload context
- Data classification
- Anomalies



### Use least privilege access

To help secure both data and productivity, limit user access using

- Just-in-**time** (JIT)
- Just-**enough**-access (JEA)
- Risk-based **adaptive** policies
- Data protection against **out of band** vectors



### Assume breach

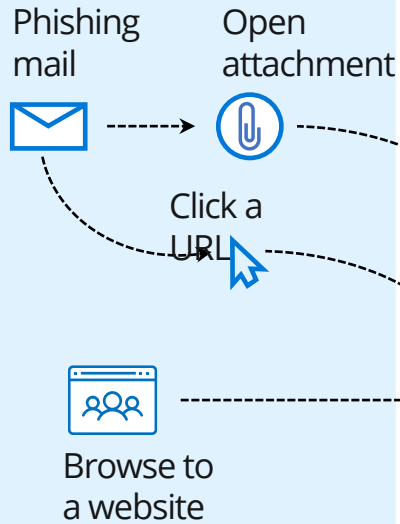
Minimize blast radius for breaches and prevent lateral movement by

- **Segmenting access** by network, user, devices, and app awareness.
- **Encrypting** all sessions end to end.
- **Use analytics** for threat detection, posture visibility and improving defenses

# Protection across the attack kill chain

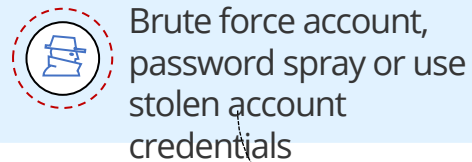
## Microsoft Defender for Office 365 (MDO)

Malware detection, safe links, and safe attachments

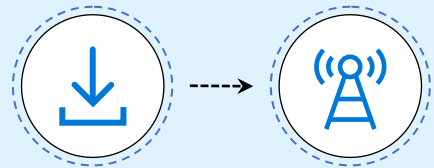


## Azure AD Identity Protection

Identity protection & conditional access

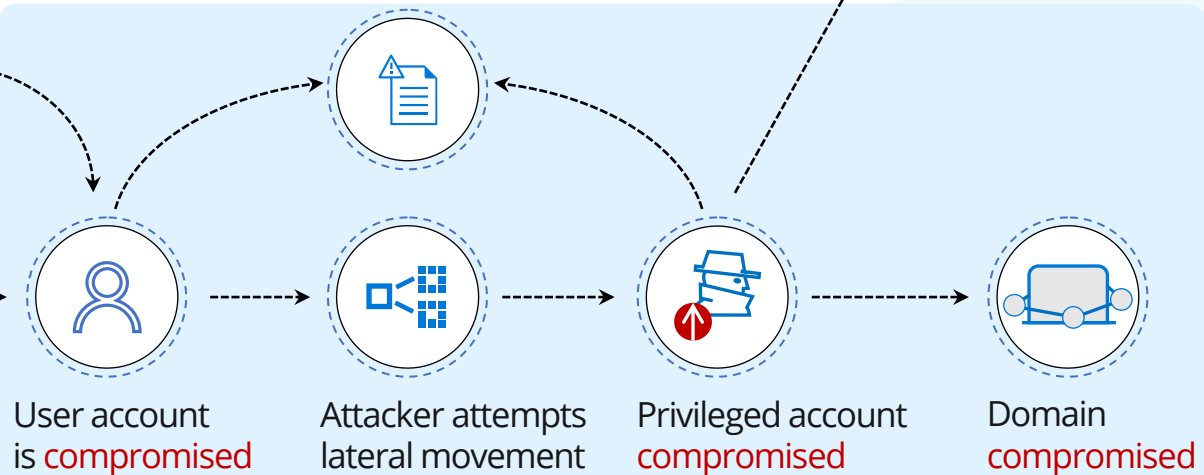


Exploitation & Installation → Command & Control



## Microsoft Defender for Endpoint (MDE)

Endpoint Detection and Response (EDR) & End-point Protection (EPP)



## Microsoft Defender for Identity (MDI)

Identity protection

## Microsoft Cloud App Security

Extends protection & conditional access to other cloud apps





SaaS Level Up

# Identity Governance and Security

**Ivan Bravo**

SaaS Level Up Cloud Engineer

plain  
concepts 



# Azure AD: Microsoft 365 Authentication

Azure Active Directory (Azure AD) is an online directory instance

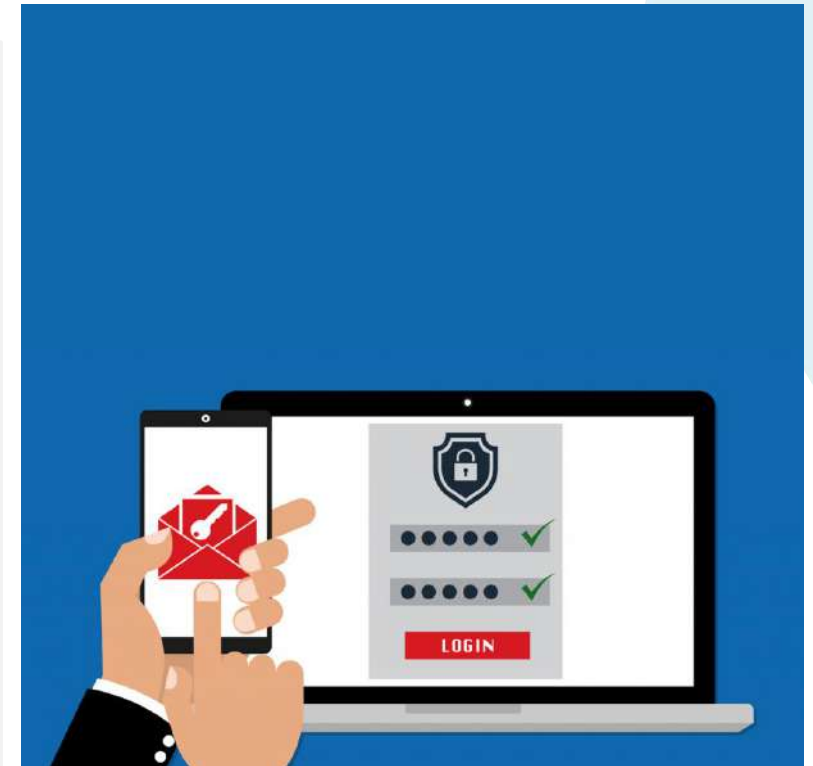
Azure AD provides authentication and authorization for Microsoft 365 and for other Microsoft cloud offerings, including Azure

Authentication options in Microsoft 365 fall into one of the following categories (each of which is covered in the following slides):

Cloud-only

Directory Synchronization with Pass-through authentication (PTA) + Password Hash Sync (PHS)

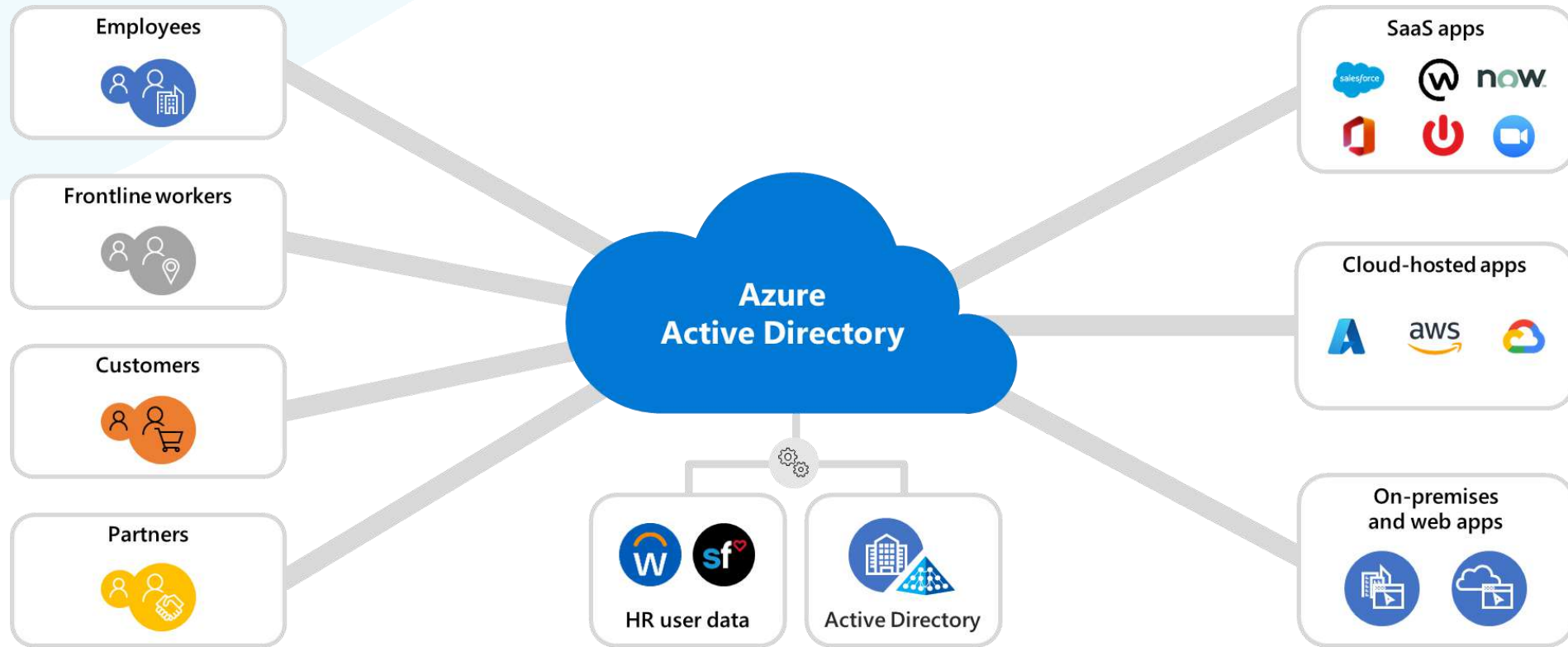
Single Sign-On (SSO) with Active Directory Federation Services (AD FS)





SaaS Level Up

# Unified identity management



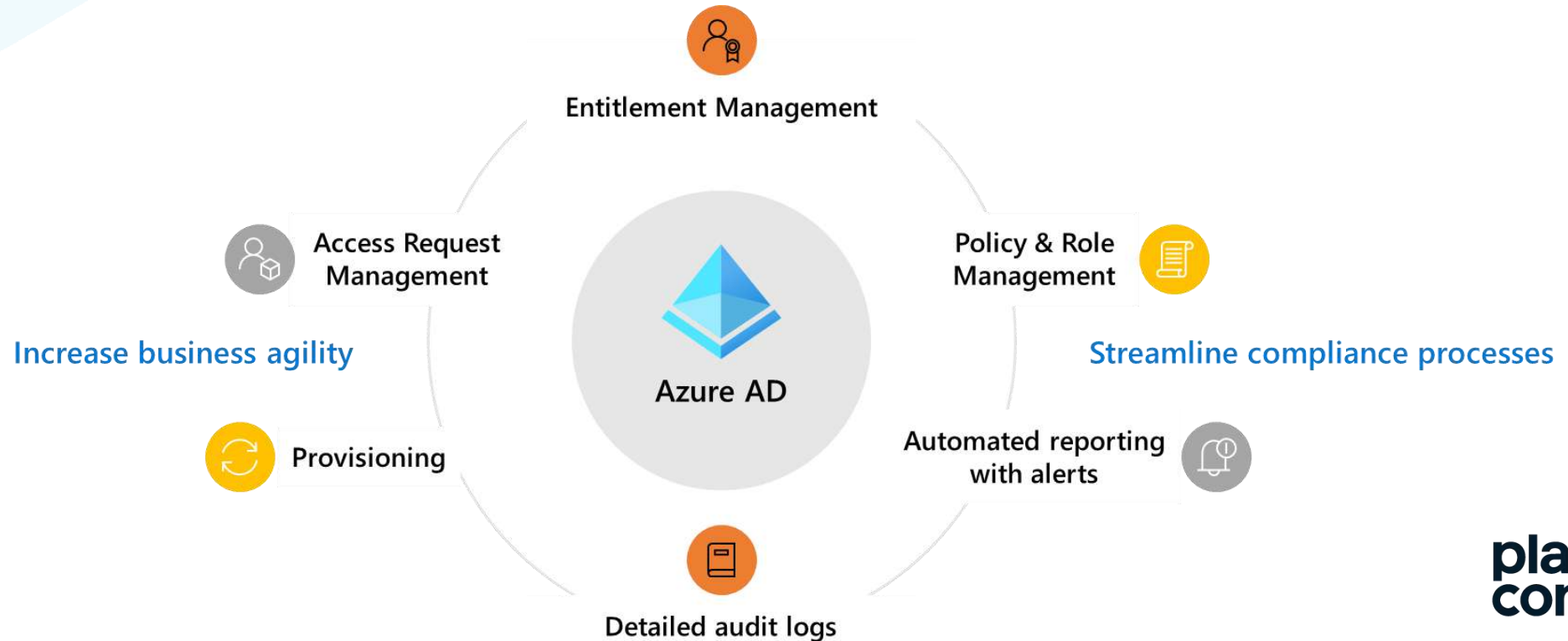




# Azure AD identity and access lifecycle management

Strengthen security while maintaining productivity

Increase business agility while strengthening security and compliance posture at scale





# Identity governance in Azure AD

## The tasks of Azure AD identity governance

### Govern the identity lifecycle

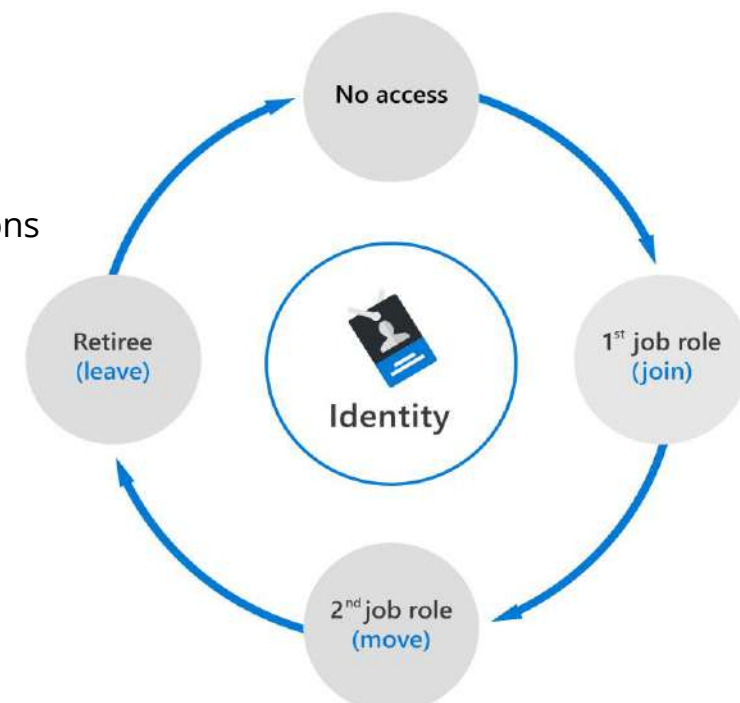
Azure AD Premium & Identity Manager: users coming from HCM cloud and on-prem solutions  
Entitlement Management

### Govern access lifecycle

Dynamic Groups  
Azure AD Access Reviews

### Secure privileged access for administration

Azure AD Privileged Identity Management (PIM)  
Azure Access Reviews to recertificate Admin roles



- Join: A new digital identity is created.
- Move: Update access authorizations.
- Leave: Access may need to be removed.



# Entitlement management and access reviews

## Entitlement management

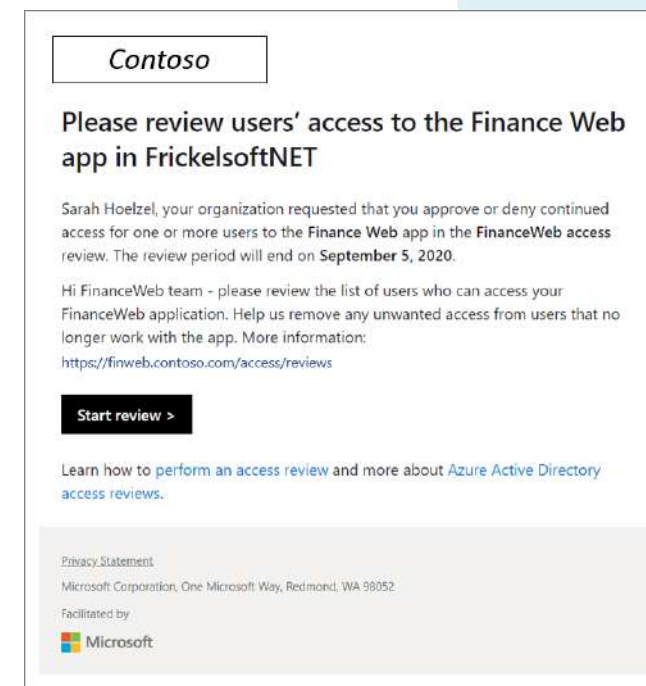
- It is an identity governance feature that enables organizations to manage identity and access lifecycle at scale.
- **Access Packages:** It automates access request workflows, access assignments, reviews, and expiration.

## Access reviews

- Enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignment.
- Ensure that only the right people have access to resources
- Used to review and manage access for both users and guests

## Terms of use

- Allow information to be presented to users, before they access data or an application.
- Ensure users read relevant disclaimers for legal or compliance requirements.





# Securing Identities in Microsoft 365

## Best Practices

- Security Defaults (MFA, block legacy auth protocols, protect privileged Access)
- Block legacy authentication protocols
- Multi-Factor Authentication
- Conditional Access
- Protect Privileged Access (PIM)
- Password management:
  - Self-Service password reset and periodic password reset
  - Banned Password list
  - Account Lockout Threshold
- Sign-out Inactive Users
- Azure Identity Protection



# Multi-Factor Authentication (MFA)

Enable Zero Trust with strong authentication and adaptive policies



**We support a broad range of multi-factor authentication options**

## Including passwordless technology



Microsoft Authenticator



Windows Hello



FIDO2 security key



Biometrics



Push notification



Soft tokens OTP



Hard tokens OTP



SMS, Voice

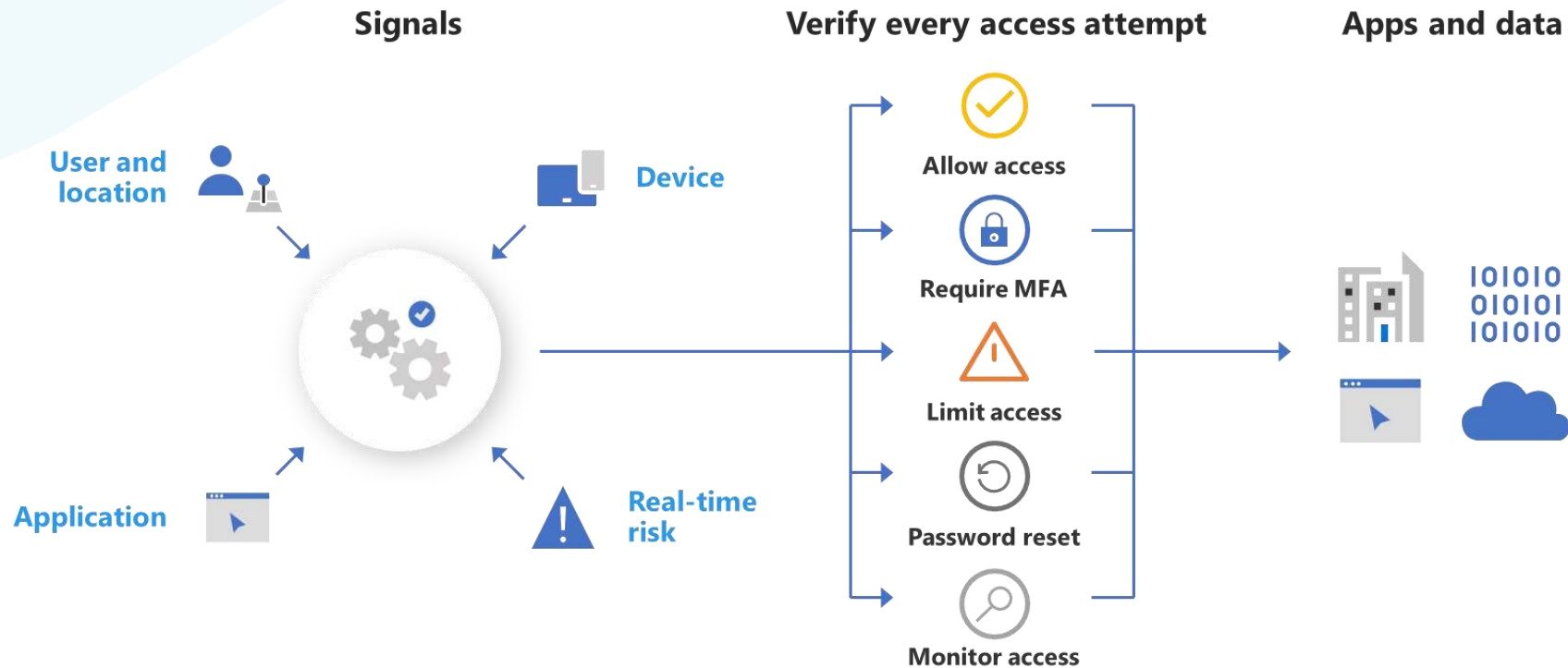


**Multi-factor authentication prevents 99.9% of identity attacks**



# Protect identities with Conditional Access

Enable Zero Trust with strong authentication and adaptive policies





# Identity protection

Intelligently detect and respond to compromised accounts



Enhanced logging



Threat alerts



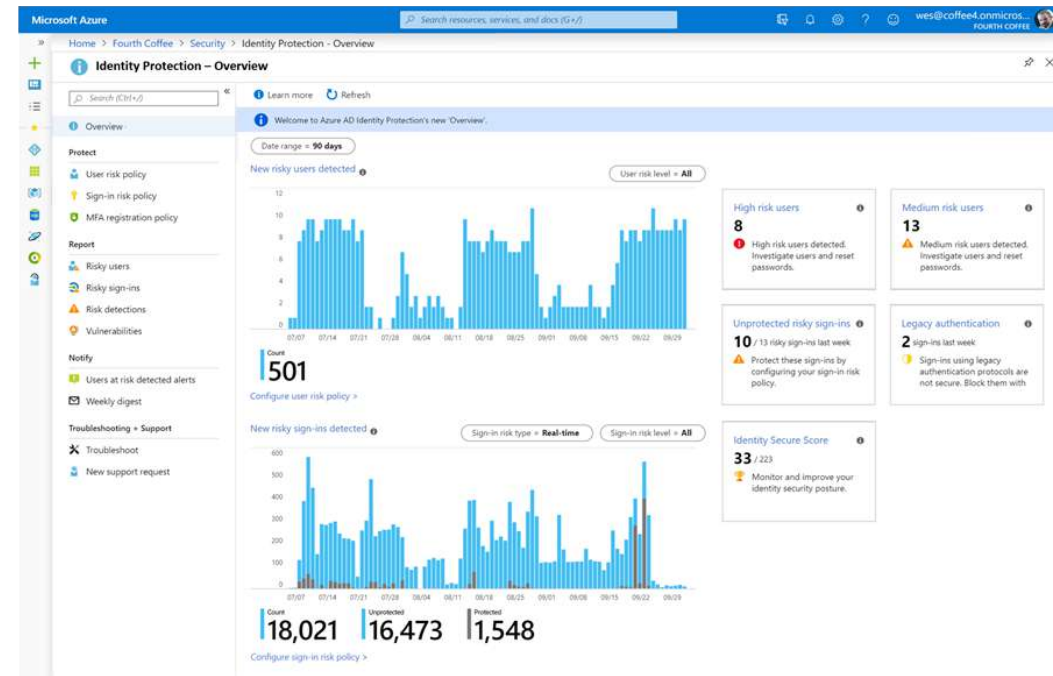
Risk scores



Sign-in reports



Privileged access insights





# Azure Identity Protection

Azure AD Identity Protection flags “Risk Events” based on anomalous activities involving user accounts. The following Risk Events are currently evaluated:

- Leaked credentials
- Impossible travel to atypical locations
- Sign-ins from infected devices
- Sign-ins from anonymous IP addresses
- Sign-ins from IP addresses with suspicious activity
- Signs in from unfamiliar locations

**Conditional Access policies** can be used to block or grant access based on level of risk for sign in-events.

Examples:

- Policy to mitigate risky sign-ins by blocking sign-ins or requiring multi-factor authentication challenges
- Policy to block or secure risky user accounts
- Policy to require users to register for multi-factor authentication

- **Azure AD P2** license is required





# Privileged Identity Management (PIM)

PIM enables you to manage, control, and monitor access to important resources in your organization.



Just in time, providing privileged access only when needed, and not before.



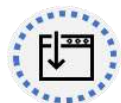
Time-bound, by assigning start and end dates that indicate when a user can access resources.



Approval-based, requiring specific approval to activate privileges.



Visible, sending notifications when privileged roles are activated.



Auditable, allowing a full access history to be downloaded.



SaaS Level Up

# Microsoft Information Protection

**José Gallardo**  
Plain Concepts Cloud Solutions Engineer

plain  
concepts 



# Discovering and managing data is challenging



1. Forrester. Security Concerns, Approaches and Technology Adoption. December 2018

2. IBM. Future of Cognitive Computing. November 2015

3. Microsoft GDPR research, 2017



# Microsoft Information Protection



Integrated  
into user apps



Rich & Intelligent  
classification



Extensible  
to other systems



Unified  
management

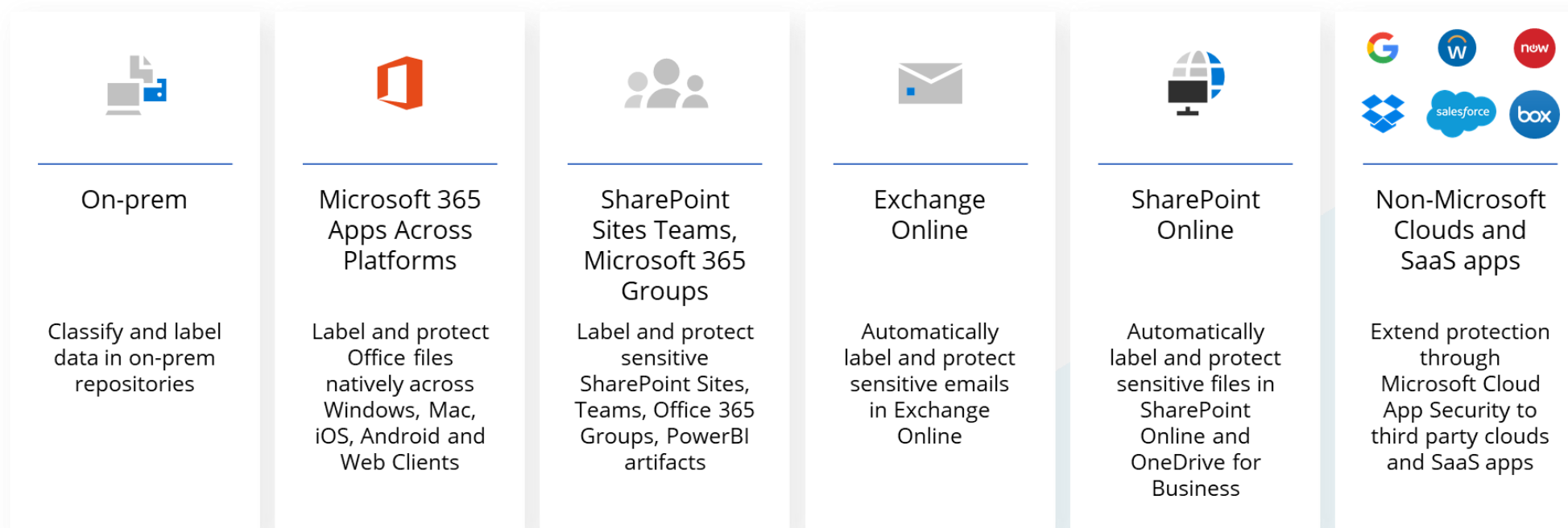


User-centered  
balances security  
with productivity



# Microsoft Information Protection

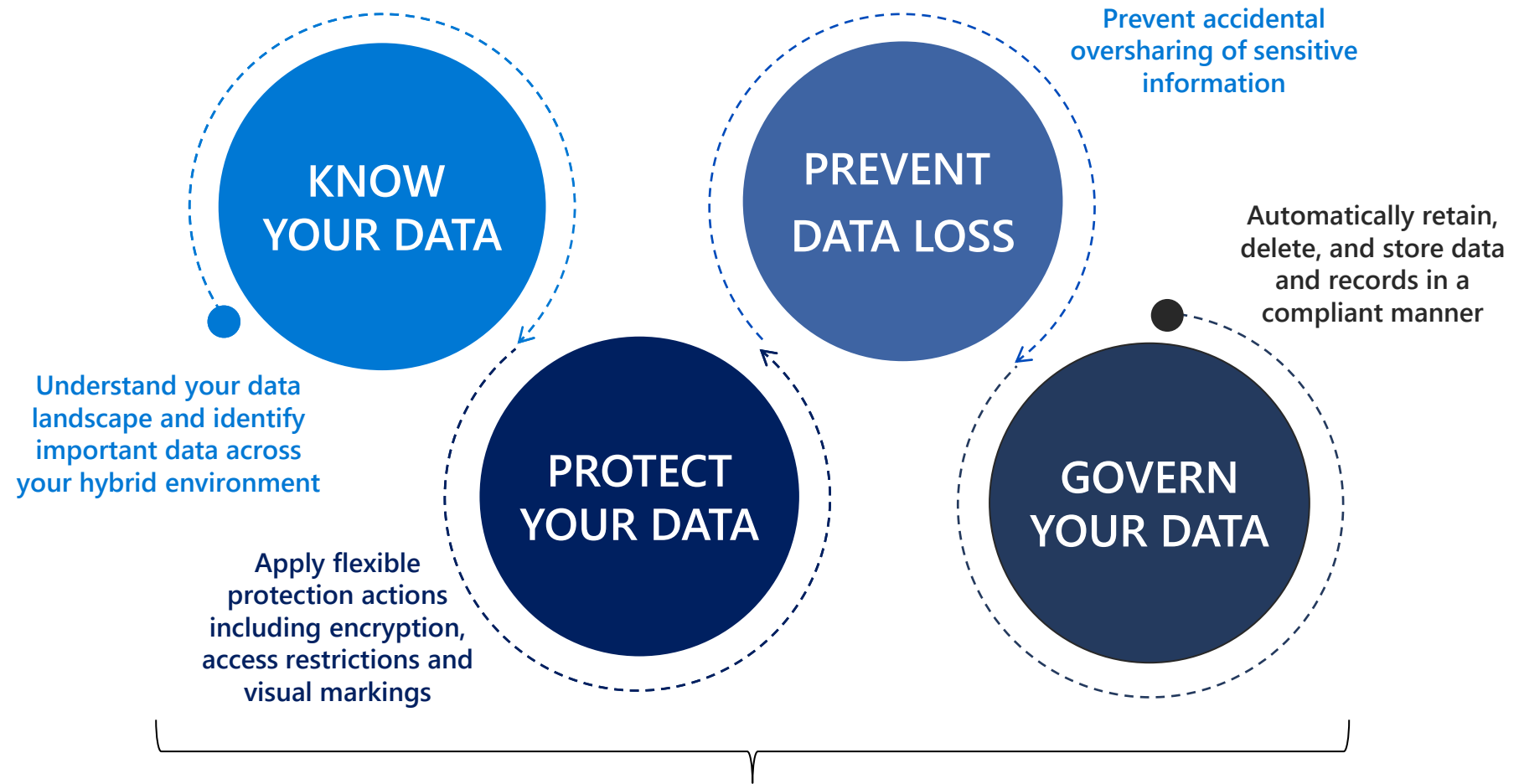
## Discover and protect your data across all environments



Unified Management in Microsoft 365 compliance center

# Microsoft Information Protection

Protect and govern data – **wherever** it lives



**Powered by an intelligent platform**

Unified approach to automatic data classification, policy management, analytics and APIs

- ☰
- 🏠 Home
- 📊 Compliance score
- 🔗 Data classification
- 🔌 Data connectors
- ⚠️ Alerts
- 📈 Reports
- 📜 Policies
- 🔍 Permissions

---

- Solutions**
- 🗃️ Catalog

---

- ⚙️ Settings
- 📄 More resources

---

- Internal Engineering Tools**
- 🛠️ Tools ▾
- 📄 Prototypes ▾
- 🛠️ Common controls ▾

---

- ✎ Customize navigation
- ⋮ Show all

## Data classification

Overview Trainable classifiers (preview) Sensitive info types Content explorer Activity explorer

The sensitive info types here are available to use in your security and compliance policies. These include a large collection of types we provide, spanning regions around the globe, as well as any custom types you have created.

+ Create info type ↻ Refresh

207 items 🔍 Search

Name ↑	Type	Publisher
Portugal Citizen Card Number	Entity	Microsoft Corporation
Portugal Tax Identification Number	Entity	Microsoft Corporation
Profanities	Entity	Contoso electronics
Project Jupiter	Entity	Contoso electronics
Project Obsidian	Entity	Contoso electronics
Regex DIT	Entity	Contoso electronics
res.csv	Entity	Contoso electronics
Romania Personal Numerical Code (CNP)	Entity	Microsoft Corporation
Russian Passport Number (Domestic)	Entity	Microsoft Corporation
Russian Passport Number (International)	Entity	Microsoft Corporation
Saudi Arabia National ID	Entity	Microsoft Corporation
sensitive info type 1	Entity	Contoso electronics
sensitive-info-1	Entity	Contoso electronics
SimpleCustomType	Entity	Contoso electronics
Singapore National Registration Identity Card (NRIC) Number	Entity	Microsoft Corporation
Slovakia Personal Number	Entity	Microsoft Corporation



# Data classification

Overview | Trainable classifiers (preview) | Sensitive info types | **Content explorer** | Activity explorer

Data visualization

Search for specific categories or labels

All locations > SharePoint Online > PO Contract documents > **Project\_Obsidian\_chip\_design.docx**

Sensitive info types

Australia Passport Number	345
<b>Project Obsidian</b>	<b>600</b>
Turkish National Identification number	34
U.K. Driver's License Number	789
U.K. Electoral Roll Number	245
U.K. National Health Service Number	689
U.K. National Insurance Number (NINO)	235
U.S. / U.K. Passport Number (0)	1,567
U.S. Bank Account Number	244
U.S. Social Security Number (SSN)	350
U.S. Driver's License Number	692

Export report ... 45 items

Name	Sensitive info type	Sensitive label
<input checked="" type="checkbox"/> Project_Obsidian_chip_design.docx	Project Obsidian +1	-
<input type="checkbox"/> Project_Obsidian_MSA_Draft_1.docx	Project Obsidian +1	-
<input type="checkbox"/> Project_Obsidian_MSA_Draft_2.docx	Project Obsidian +1	-
<input type="checkbox"/> Project_Obsidian_MSA_Draft_3.docx	Project Obsidian +1	-
<input type="checkbox"/> Project_Obsidian_MSA_Draft_4.docx	Project Obsidian +1	-
<input type="checkbox"/> Project_Obsidian_MSA_Draft_5.docx	Project Obsidian +1	-
<input type="checkbox"/> Project_Obsidian_MSA_Final_for_review.docx	Project Obsidian +1	-
<input type="checkbox"/> Project_Obsidian_MSA_Final_tobe_Signed.docx	Project Obsidian +1	-
<input type="checkbox"/> Project_Obsidian_MSA_Final_Signed.docx	Project Obsidian +1	-
<input type="checkbox"/> Project_Obsidian_Contract_Obligation.docx	Project Obsidian +1	-
<input type="checkbox"/> PO_Team_chart_v1.pdf	Project Obsidian +1	-
<input type="checkbox"/> PO_Team_chart_v2.pdf	Project Obsidian +1	-
<input type="checkbox"/> PO_Team_chart_Final.pdf	Project Obsidian +1	-
<input type="checkbox"/> PO_Leaders_conference_notes.docx	Project Obsidian +1	-

**Project Obsidian Spec. docx**

Source view | Details

**Project Obsidian**

**Updated Engine Chip Design**

Automated Car Team  
October 21, 2019

Contacts	Email	Timeline
Lidia Holloway	lidia@contosoelectronics.com	Q4 FY 22

With our new investments in automated cars we need to redesign the AI500 chip to pull more

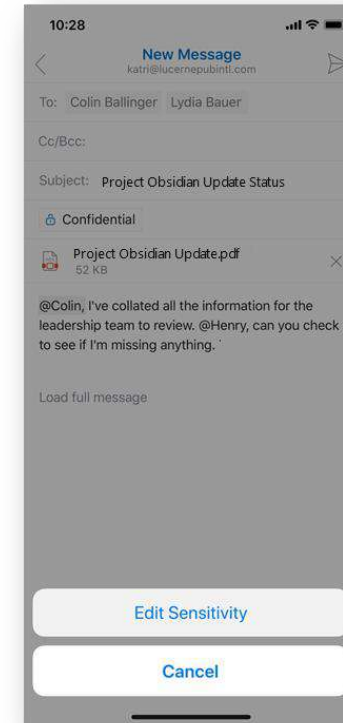
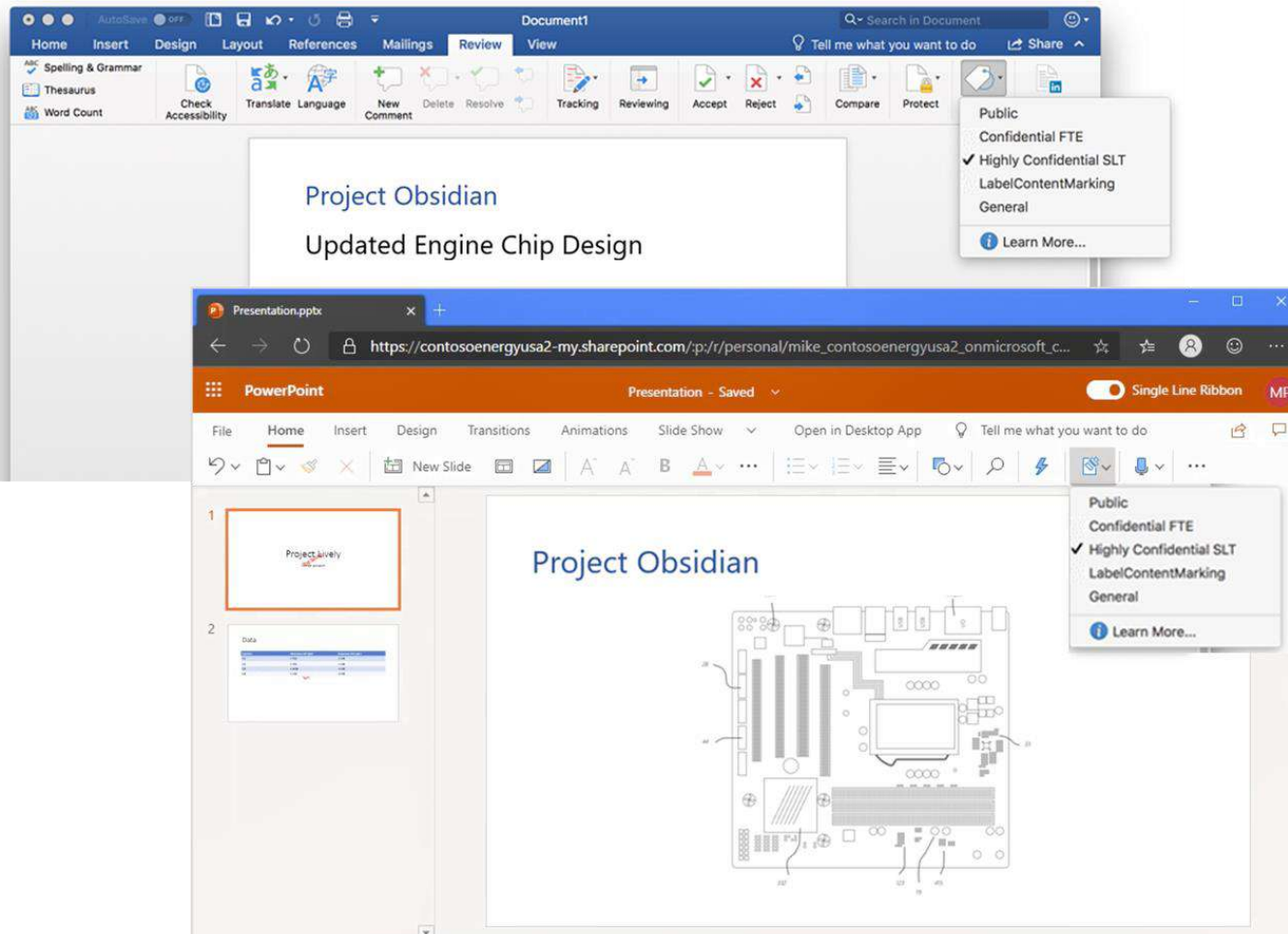
Provide feedback | Cancel





SaaS Level Up

# Native manual labeling in Office apps across all platforms



plain  
concepts

# Data classification

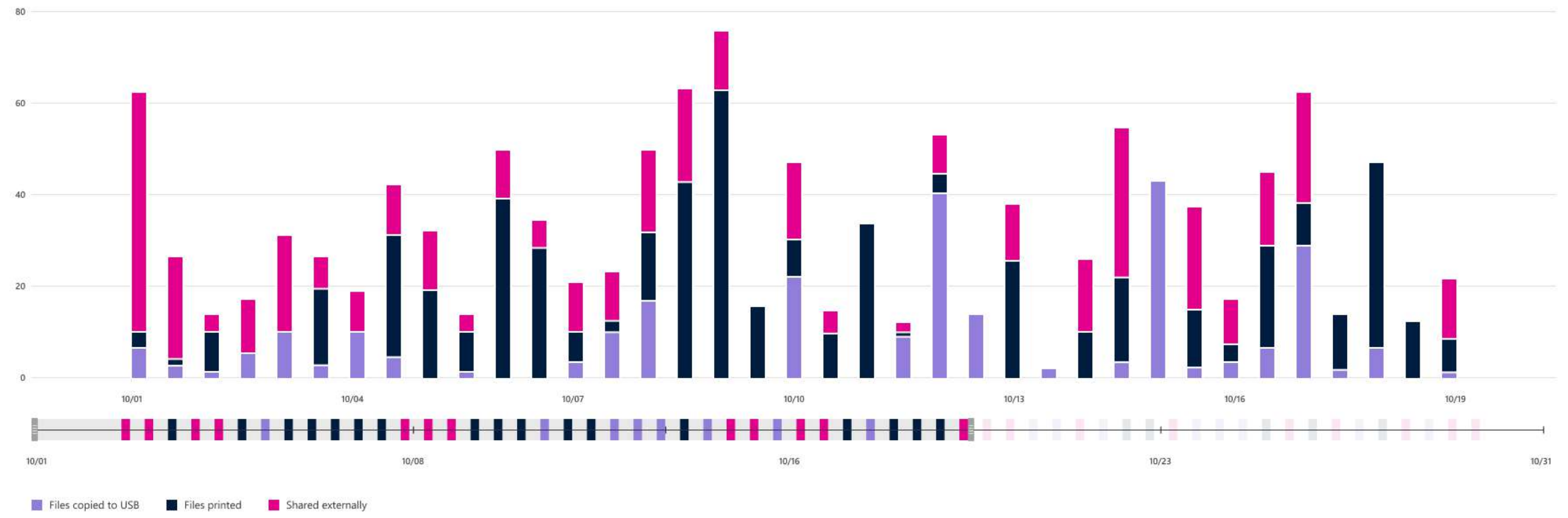
Overview | Trainable classifiers (preview) | Sensitive info types | Content explorer | **Activity explorer**

List view | **Data visualization**

**Filter by** Save query Filters Customize columns

Date range: **Last 30 days** | Activities: **Any** | Sensitive info types: **Any** | Sensitivity label: **Any** | Enforcement Mode: **Any** | Location: **Any**

Create alert | New DLP policy from results | **9,550 activities**





SaaS Level Up

# Microsoft 365 Backup

plain  
concepts 



# Microsoft 365 Data Retention policies

- Exchange “deleted folders” aren’t a backup option
  - Deleted mailboxes’ data has limited retention
  - Restoring from these folders isn’t straightforward
- Teams’ conversations aren’t retained
  - Only 30 days for conversations and chats
- SharePoint and OneDrive aren’t backed-up
  - Users can inadvertently delete data
  - In the case of security breaches, no roll-back capability



## Microsoft says that you need 3<sup>rd</sup> party backup for O365

### **Microsoft Service Agreement (MSA):**

We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. **We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps.**

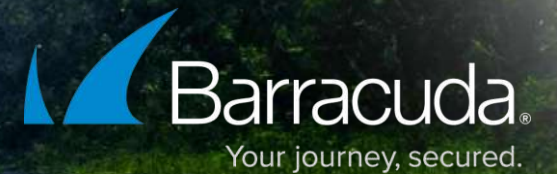
- -Microsoft Services Agreement, Section 6B

# Barracuda & M365 Backup

Miguel López

Country Manager – Iberia

[mlopez@barracuda.com](mailto:mlopez@barracuda.com)



# What does CCB add to Office 365 capabilities?

	Incl. in O365	CCB
Independent copy of the data		✓
Unlimited storage and unlimited retention	Limited	✓
Ease of use for protecting data and setting up options		✓
Ease of use for recovering data		✓
Cross restore of data to other users, mailboxes, folders or sites		✓
Granular restore for SharePoint and OneDrive		✓
Ability to restore after corruption, malware or ransomware	Limited	✓



# Microsoft Retention Policies vs CCB

Office 365 Application	Microsoft Default Retention	Microsoft Maximum Retention after Deletion	Barracuda CCB Retention
Exchange Mail, Calendars, Contacts, and Tasks	30 days after soft delete	Unlimited after Soft Delete	Unlimited
	14 days after hard delete	30 days after Hard Delete	Unlimited
SharePoint Online / OneDrive for Business	User Deleted items go into Site recycle Bin for 93 days	93 days	Unlimited
	Admin Deleted items go into Site Collection Recycle bin folder for 30 days	93 days	Unlimited
Teams	Deleted Teams will be retained for 30 days	30 days	Unlimited

1: Soft Delete occurs when an item is moved to a temporary recycle bin (example: right-click and delete in Outlook)

2: Hard Delete occurs when an item is removed entirely from the source (example: SHIFT+Delete an item in Outlook)

3: After an item is cleared from the site recycle bin, the item will be moved to the Site Collection recycle bin for the remainder of the 93 days.

4: There is a unlimited retention option with Office 365 with E3 and E5 for OneDrive - <https://www.microsoft.com/en-us/microsoft-365/business/compare-more-office-365-for-business-plans>. It is much more expensive - \$20 user/month or \$35 user/month vs \$8 user/month for E1.





# Complete Protection for Office 365



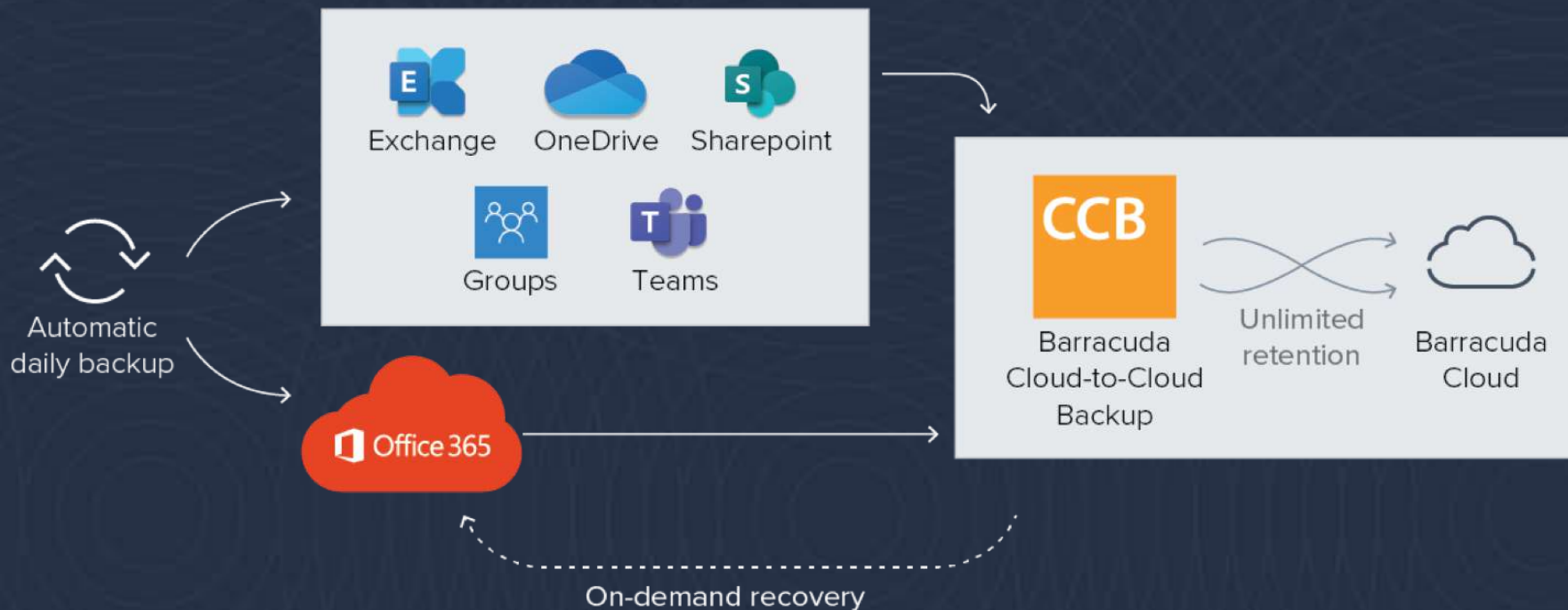
## Backup, Recovery & Business Continuity for Office 365

- Direct Cloud to Cloud backup
- Protects Exchange / SharePoint Online / Teams and OneDrive against data loss
- Provides granular recovery options
- Unlimited Storage
- Comprehensive feature set

The screenshot displays the Barracuda Cloud-to-Cloud Backup (CCB) web interface. The top navigation bar includes 'DASHBOARD', 'PROTECT', 'REPORTS', and 'SETTINGS'. The main content area shows a list of protected services with their status. A 'Teams' service is highlighted, showing 'Next backup scheduled for Sep 9, 2020, 12:00:00 AM' and 'BACKUP NOW' button. Below this, a 'Microsoft Services Agreement' is displayed, with a red circle highlighting a specific paragraph in the 'Service Availability' section. The interface also shows a 'SharePoint' service and a 'Restore' button for a specific backup.

# Barracuda Cloud-to-Cloud Backup (CCB)

Unlimited storage and retention for Office 365 Exchange Online, SharePoint, OneDrive for Business and Teams/Groups. Delivered as a SaaS.





SaaS Level Up

# Microsoft Defender

**David Fernández**

Plain Concepts Cloud Solutions Engineer

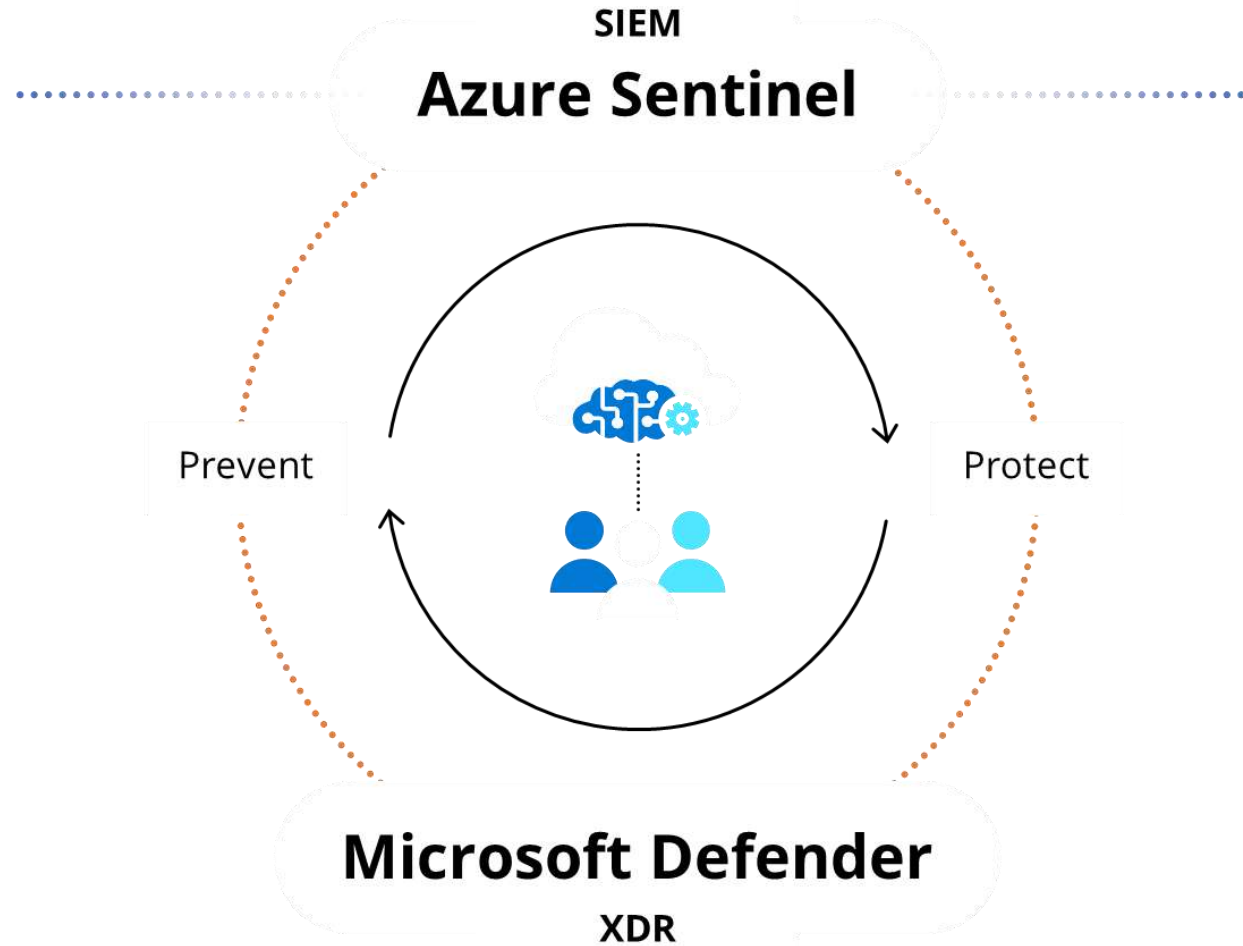
plain  
concepts 



SaaS Level Up



Multi-cloud



Partnerships



SaaS Level Up

← Cross-domain protection →

### Microsoft 365 Defender

- Identities
- Endpoints
- Apps
- E-mail
- Cloud Apps
- Docs

### Azure Defender

- SQL
- Server VMs
- Containers
- Network
- IoT
- Azure App Services

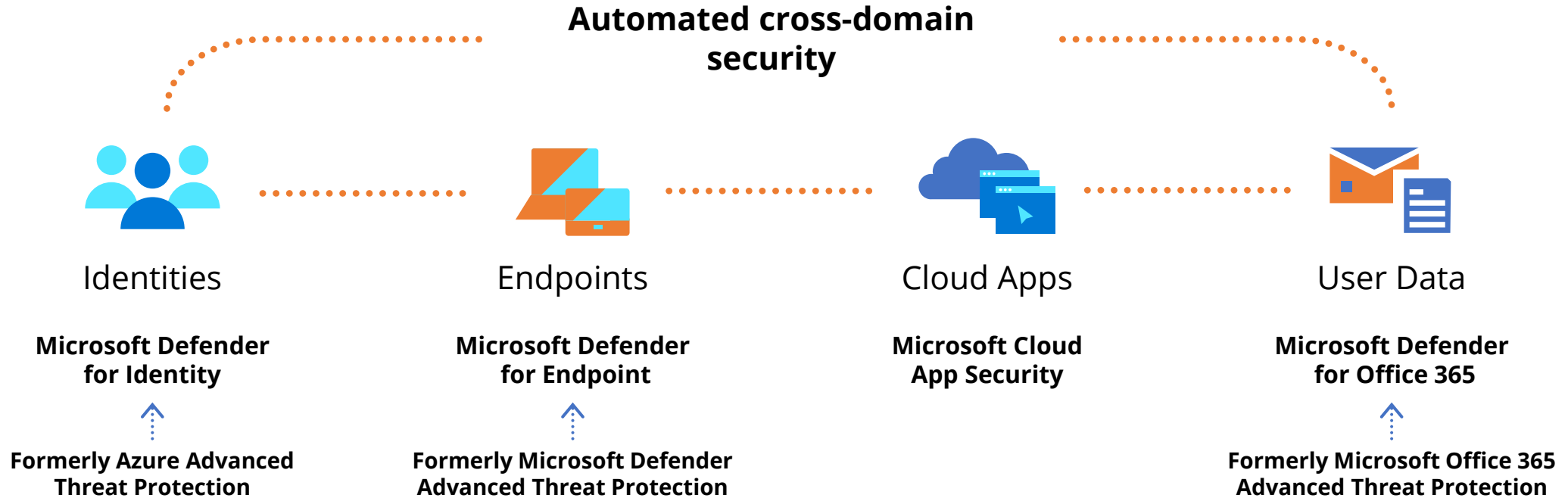
# Microsoft Defender

XDR



SaaS Level Up

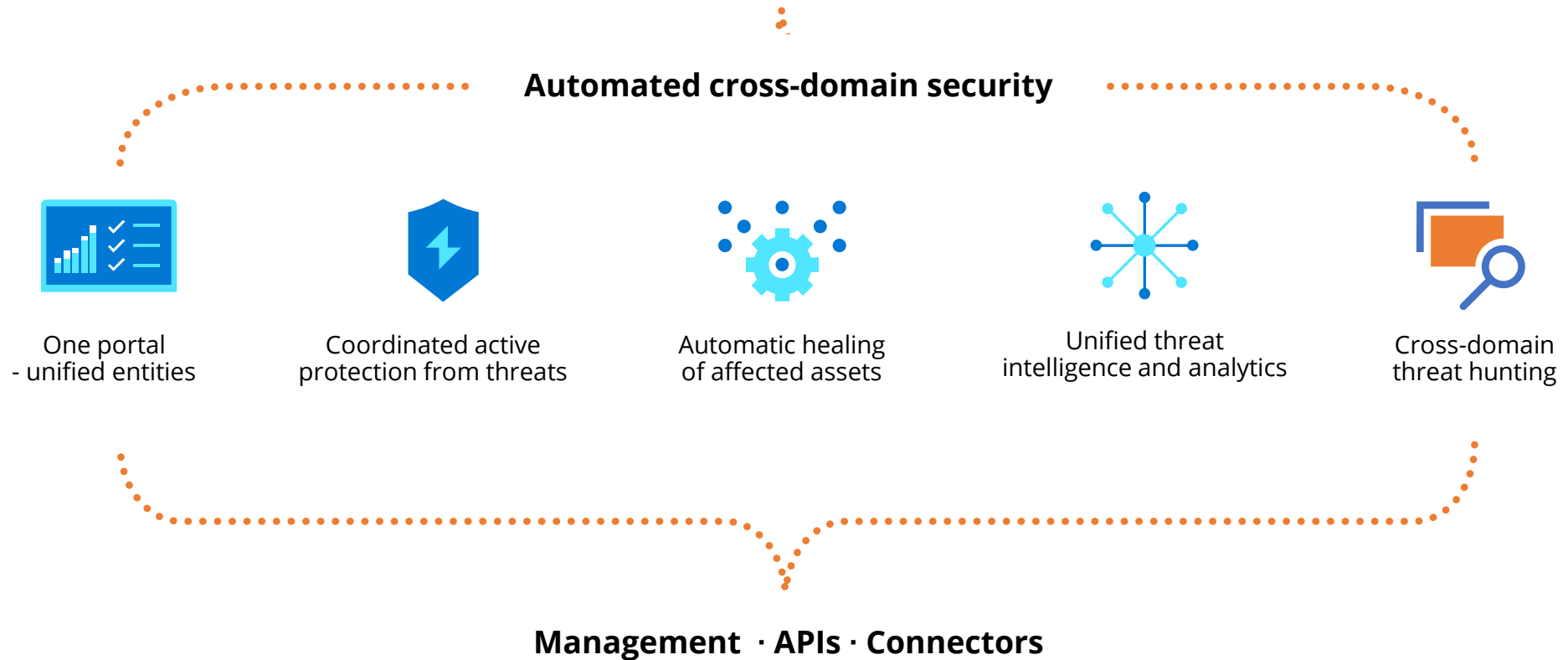
# Microsoft 365 Defender



Shift from individual silos to coordinated cross-domain security



# Microsoft 365 Defender



- ☰
- 🏠 Home
- 🏆 Secure score
- 🛡️ Incidents & alerts ^
- Unified queue
- Endpoint alerts
- Email & collaboration alerts
- 🔍 Hunting v
- 📄 Action center
- Endpoint
- 🔍
- 📄 Dashboard
- 📄 Device inventory
- 🔧 Vulnerability management v
- 📄 Threat analytics
- 🔗 Partners & APIs v

## Good morning, Rob

Active Incidents

### 35 Active incidents

**21 Unassigned incidents**

■ High (5) ■ Medium (8) ■ Low (16) ■ Informational (6)

**incident and alert trend**

Incident name	Severity	Active alerts	Scope	Last activity	Tags
Multi-stage incident...	High	123/138	📄 4 👤 2 🗨️ 117	Sep 4, 06:32:45 AM	HIGH RISK THREAT EXPERT
'Dirtelti' backdoor wa...	High	132/132	📄 44 👤 0 🗨️ 0	Sep 4, 06:41:45 AM	
Office process droppe...	High	132/132	📄 4 👤 0 🗨️ 0	Sep 4, 06:42:45 AM	

[View all active incidents](#)

Action Center

### 20 actions pending approval

**Users** 5/35

**Mailboxes** 15/30

**Devices** 10/16

■ Pending approval ■ Remediated ■ Timed out ■ Failed

[Approve in Action Center](#)

Threat Analytics

### 1 Active threat in your org

**Human operated ransomware attack**

**Cobalt Strike: Hiding in the Red** No active alerts

**Qakbot blight lingers, seeds ransomware** No active alerts

■ Active Alert ■ Resolved alerts

[See More](#)

Security Blogs and News

Tammay Ganachaya @tanmayg

In continuing to diminish the chances of sophisticated threats slipping through defenses, we have expanded behavioral blocking and containment capabilities to get even broader visibility into malicious behavior by using a rapid protection loop...

[See on Twitter](#)

**Microsoft Defender ATP**

Next-generation protection

↔️

Endpoint detection and response

March 9th, 2020 - 6:32PM 👍 157

● ● ● ● ●

[Next](#) [Need help?](#) [Give feedback](#)

### Microsoft 365 Defender Unified Portal

Microsoft 365 E5 license or any individual product E5 license  
 Use Microsoft 365 Defender even if you only have one E5 product, expand over time to get cross-product value

### Microsoft 365 Defender Dashboard

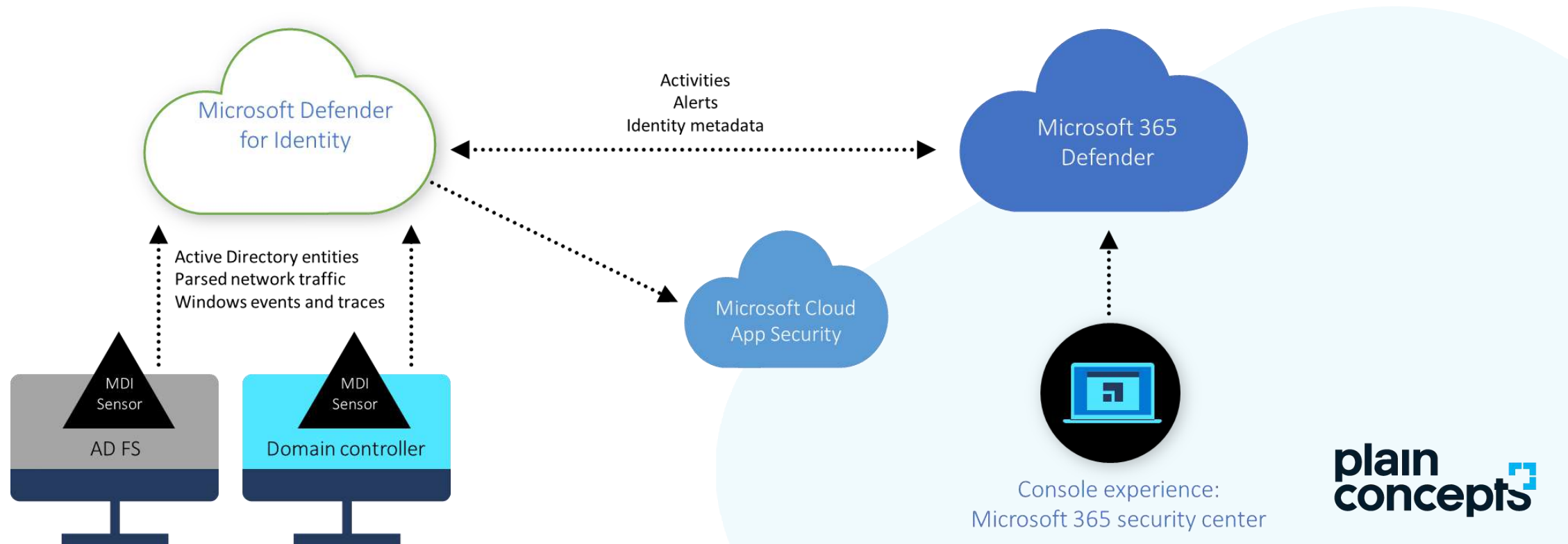
My organization's overall security state  
 What's the next highest priority SOC work item





# Microsoft Defender for Identity architecture

Defender for Identity learns about your network, enables detection of anomalies, and warns you of suspicious activities





# Microsoft Defender for Identity

Microsoft Defender for Identity helps security operations teams protect user identity as part of on-premises and cloud enterprise environments



## Prevent



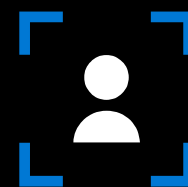
Proactive identity security posture assessments



## Detect



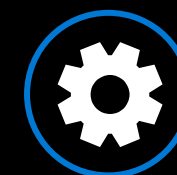
Real-time analytics and data intelligence



## Investigate



User investigation priority



## Respond



Automatic response to compromised identities

Cloud scale, continuous updates



SaaS Level Up

# Microsoft Defender for Endpoint

## Delivering endpoint security across platforms



 Windows



macOS



iOS



 Windows 365

Azure Virtual Desktop



Cisco  
Juniper Networks

HP Enterprise  
Palo Alto Networks

Endpoints and servers

Mobile device OS

Virtual desktops

Network devices

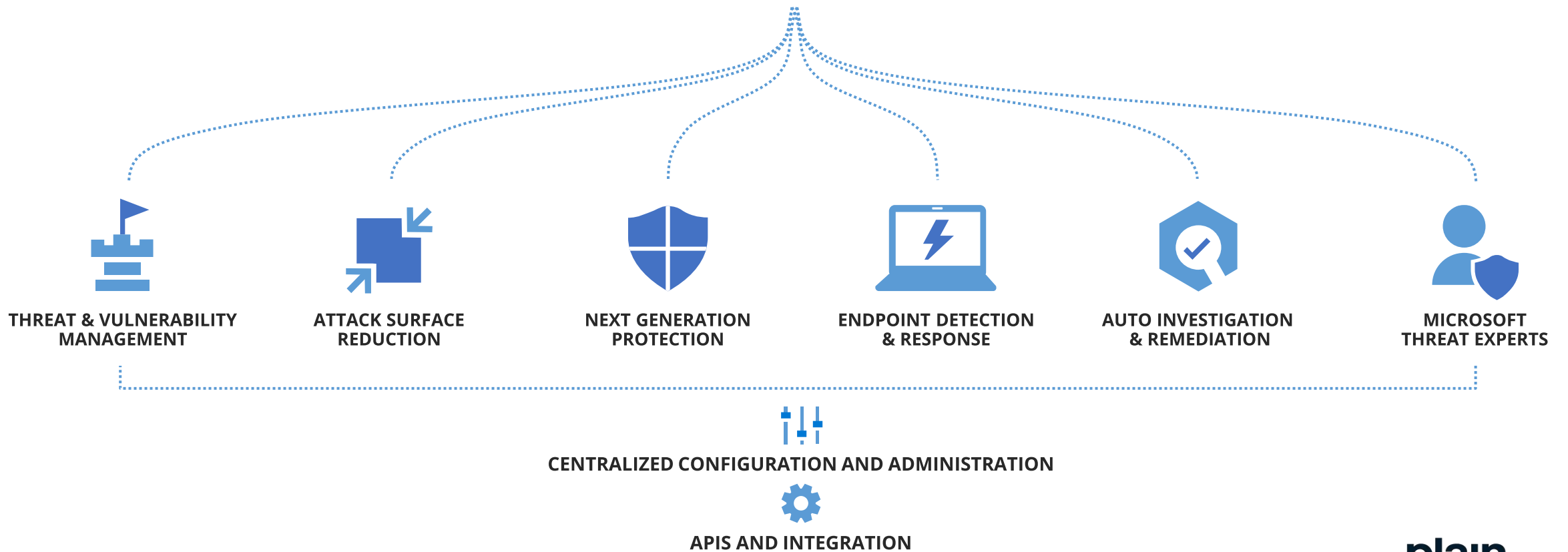


SaaS Level Up



# Microsoft Defender for Endpoint

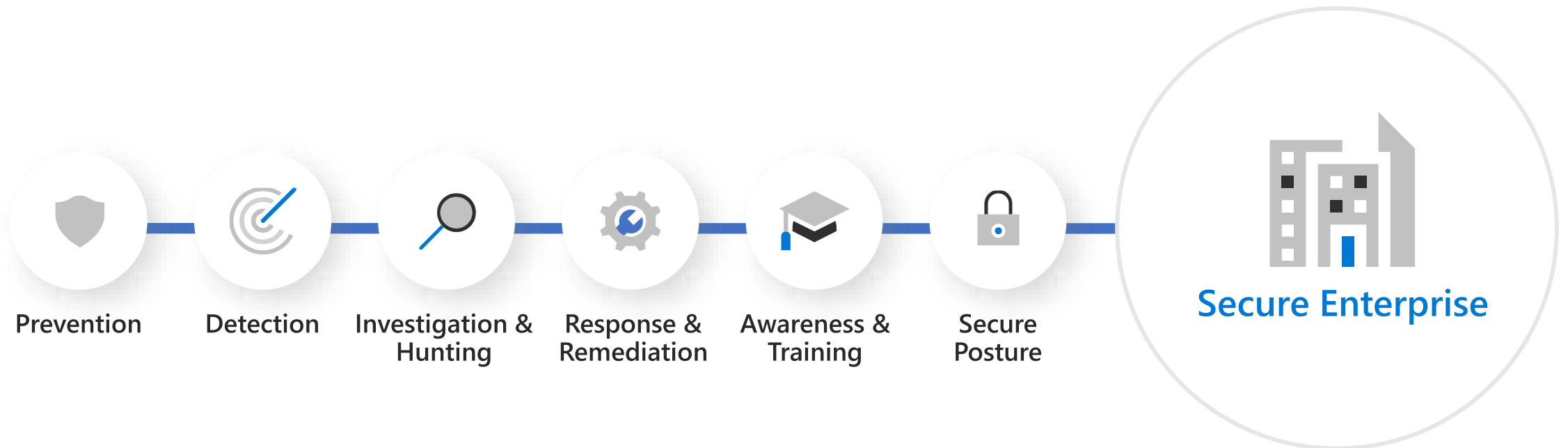
Threats are no match.





# Microsoft Defender for Office 365

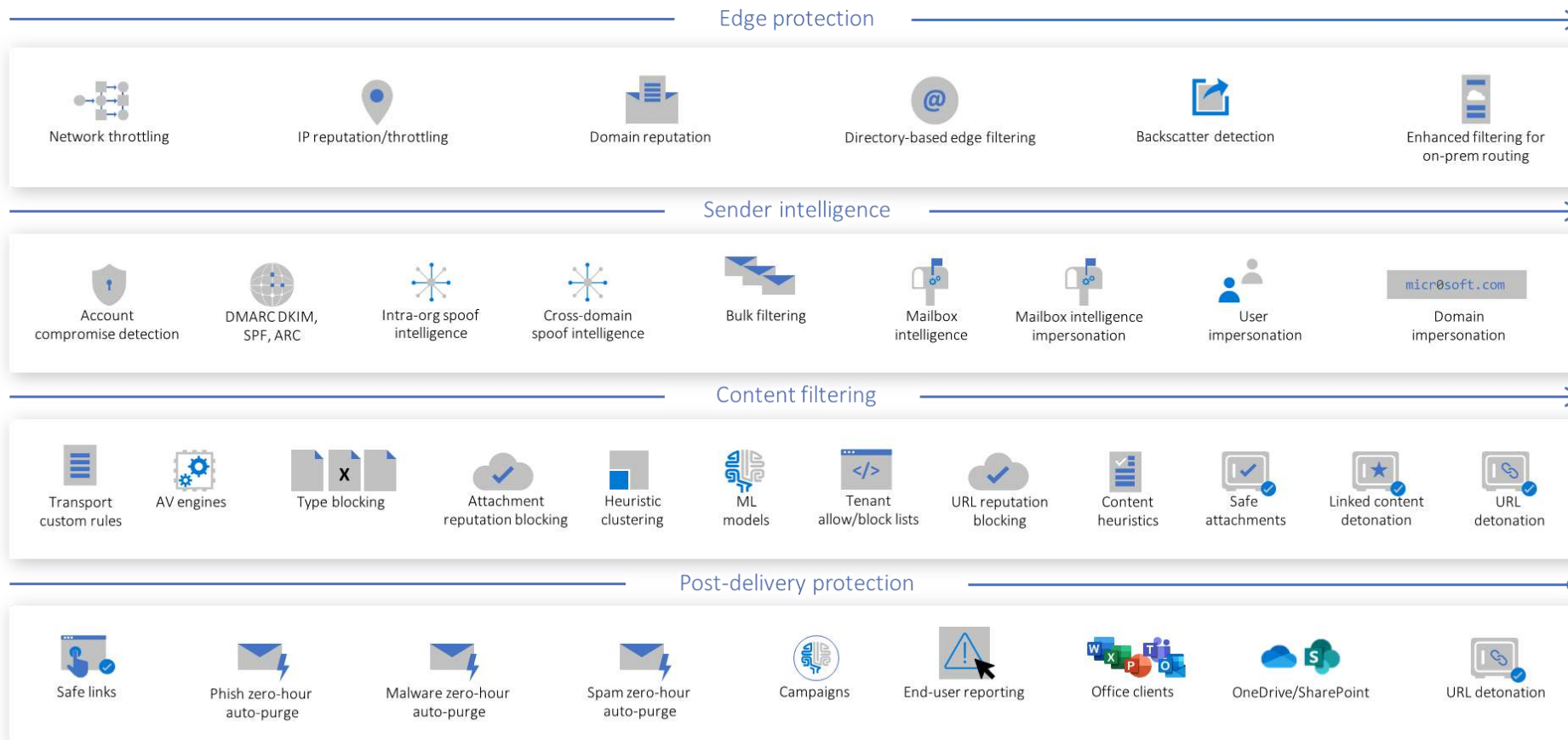
Securing your enterprise requires more than just prevention





# Microsoft Defender for Office 365

## Multi-Layered protection stack





SaaS Level Up

# Microsoft Cloud Apps Security

**Eduardo Recio**  
SaaS Level Up Cloud Engineer

plain  
concepts 



# ¿Qué es un Cloud App Security Broker?

Agente que se sitúa entre los usuarios y las aplicaciones en la nube, y supervisa toda la actividad y aplica las políticas de seguridad.



Acceso y gestión de la identidad



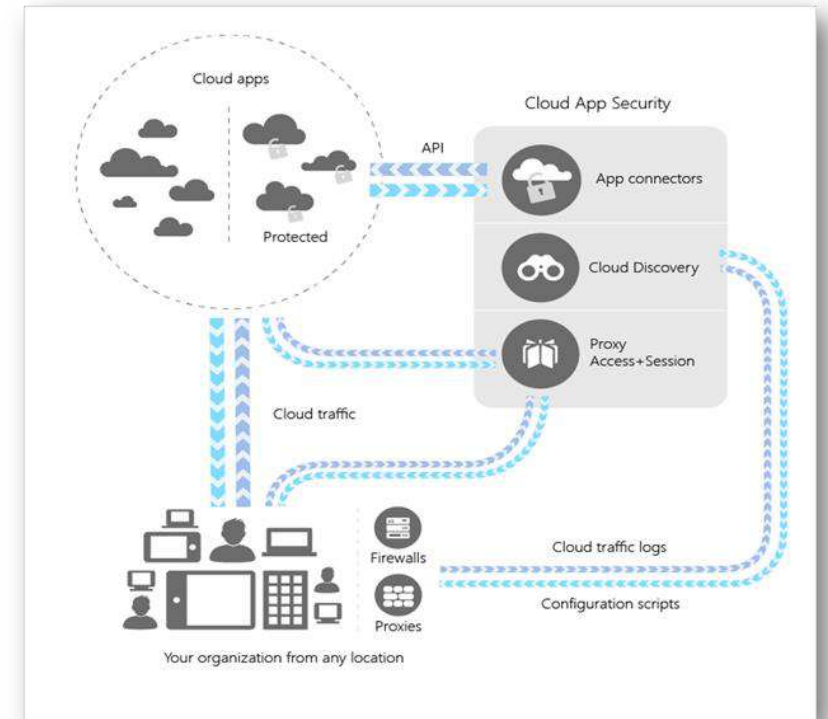
Protección contra amenazas



Administración de la seguridad



Protección de la información







# Microsoft Cloud Apps Security

¿Por qué necesitamos uno si queremos proteger nuestros datos en Office 365?

## Top casos de uso

- Descubrir y gobernar apps
- Detectar filtración y tener visibilidad de los datos corporativos
- Aplicar políticas DLP, incluso en corporativos no gestionados
- Identificar cuentas de usuario comprometidas



# Descubrir y gobernar apps

Cloud App Security

### Cloud Discovery

Dashboard | Discovered apps | Discovered resources | IP addresses | Users | Devices | 27, 2021, 7:22 PM

Queries: Select a query | Save as | Advanced filters

Apps: Apps... | App tag: None | Risk score: 0 - 10 | Compliance risk factor: Select factors... | Security risk factor: Select factors...


Browse by category: Search for category...

App	Score	Traf...	Uplo...	Tran...	Users	IP ad...	Devices	Last ...	Actions
Azure CDN E... Hosting services	10	1.8 GB	409 KB	426	2	16	2	Oct 27,...	☑ ☒ ⋮
Microsoft 365... Collaboration	10	16 MB	8 MB	63	2	10	2	Oct 26,...	☑ ☒ ⋮
Microsoft Tec... Forums	10	55 MB	3 MB	58	2	10	2	Oct 27,...	☑ ☒ ⋮
Microsoft Su... Customer support	10	3 MB	642 KB	13	2	2	2	Oct 21,...	☑ ☒ ⋮
Azure Front D... Hosting services	10	36 MB	—	8	2	5	2	Oct 21,...	☑ ☒ ⋮

News and entertainment 34  
IT services 18  
Productivity 17  
Security 16  
Marketing 15  
Advertising 15  
Accounting and finance 15



# Descubrir y gobernar apps

**Netflix**  
Web app  
News and entertainment • Netflix

Last 30 days Win10 Endpoint Users App actions

**Overview** Info Cloud app usage

Cloud app score

### Cloud app score: 8/10

General	10/10
Security	8/10
Compliance	4/10
Legal	10/10

[View score breakdown](#)

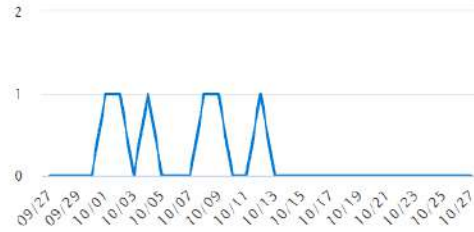
Usage

Users	1	Traffic	4.3 GB
IPs	2	Devices	1

[View usage details](#)



Usage trend Users

### Users: 1




[View usage details](#)

Top entities (Cloud app) Users

User	Investigat...	Traffic
		906 MB

Recent alerts

  
**Phew, there are no open alerts**  
Over the last 30 days  
[View all alerts](#)



# Detectar filtración y tener visibilidad de los datos corporativos

Files

FILES MATCHING ALL OF THE FOLLOWING Basic

- Access level equals External, Public
- Last modified earlier than (days) 180 Days ago

1 - 20 of 632 files New policy from search

File name	Owner	App	Collaborators	Policies	Last modified
templates	! superadmin@test2... test2...	b Test2	👤	1 policy match	May 10, 2018
README.md	! superadmin@test2... test2...	b Test2	👤 3 collaborators	1 policy match	May 10, 2018
attributes	! superadmin@test2... test2...	b Test2	👤	1 policy match	May 10, 2018



# Aplicar políticas DLP, incluso en corporativos no gestionados

The screenshot shows the Microsoft 365 compliance console. The left sidebar contains navigation options: Home, Compliance Manager, Data classification, Data connectors, Alerts, Reports, Policies, Permissions, Solutions, Catalog, Settings, More resources, Customize navigation, and Show all. The main area is titled "Data loss prevention > Create policy". A progress indicator shows the current step: "Locations to apply the policy".

The "Choose locations to apply the policy" section includes a table of locations with their status:

Status	Location	Ind
<input checked="" type="checkbox"/> On	Exchange email	All
<input checked="" type="checkbox"/> On	SharePoint sites	All
<input checked="" type="checkbox"/> On	OneDrive accounts	All
<input checked="" type="checkbox"/> On	Teams chat and channel messages	All
<input checked="" type="checkbox"/> On	Devices (preview)	All
<input checked="" type="checkbox"/> On	Microsoft Cloud App Security	All

A "Microsoft Cloud App Security" dialog box is open on the right, showing a search bar and a list of selected locations:

- 2 of 12 selected
- Box - Box - US
- Box - Box - General
- Salesforce - Salesforce - US
- Salesforce - Salesforce - EU
- Salesforce - Salesforce - General
- Dropbox - Dropbox - US

At the bottom of the dialog, there are buttons for "Done", "Cancel", "Need help?", and "Give feedback".



# Identificar cuentas de usuario comprometidas

The screenshot displays the Microsoft Cloud App Security user risk dashboard for Jonathan Walcott. The interface includes a left-hand navigation pane with sections for User threat, User exposure, and Contact info. The main content area shows the user's risk score of 127, broken down into Alerts (70), Risky activities (55), and Blast radius (12). A comparison bar indicates the user's score is in the top 90% of the organization. Below this, a timeline of alerts and risky activities is shown, including a mass download alert, log on, resource access, and risky sign-in.

**User risk** Lateral movement

**Investigation priority score** 127

Score is based on the last 7 days | [How do we score?](#)

**User risk in the last two weeks**

Score: 70 (Alerts)  
Score: 55 (Risky activities)  
Score: 12 (Blast radius)

**User score compared to the organization** 91% (Top 90% in your organization)

**Alerts and risky activities that contributed to the score (last 7 days)** | [View all user alerts \(12\)](#)

- Yesterday
- +20 Today at 4:28 PM High **Mass download alert**
- +8 Yesterday at 7:11 PM Medium **Log on**
- Last week
- +12 Thursday at 2:22 AM Medium **Resource access - Device: WK-Win10-PC**  
Device: WK-Win10-PC
- +18 Thursday at 1:28 AM Medium **Risky sign-in**
- There aren't any more alerts on risky activities for this user over the last 7 days  
[View all user alerts](#)

**User threat**

Open incidents 4 Investigation priority 127

Open alerts 107 Identity risk level Medium

Lateral movement paths 3

**User exposure**

Accounts 25	Devices 15
Logon types 3	Locations 3
Matched files 12	Groups 12
Mailboxes 12	

**Contact info**

Email [jonathanwalcott@contoso.com](mailto:jonathanwalcott@contoso.com)



SaaS Level Up

## Barracuda Sentinel

Protección avanzada contra amenazas

plain  
concepts 

# Barracuda & the Public Cloud

Miguel López

Country Manager – Iberia

[mlopez@barracuda.com](mailto:mlopez@barracuda.com)





# Comprehensive email protection

## Gateway Defense and Resiliency

Cloud Backup and Archiving

Email Continuity

Encryption and DLP

In/Outbound Security

## API-Based Inbox Defense

AI for Social Engineering

Brand Protection  
DMARC Reporting

Account Takeover

## Security Awareness

Phishing Simulation

User Awareness Training

Automated Reporting

## Incident Response

Automation

Post Delivery Remediation

Threat Hunting

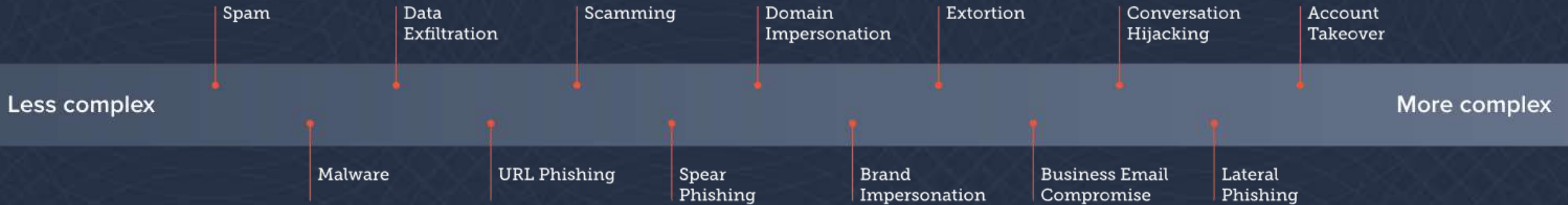


Barracuda

Total Email Protection™



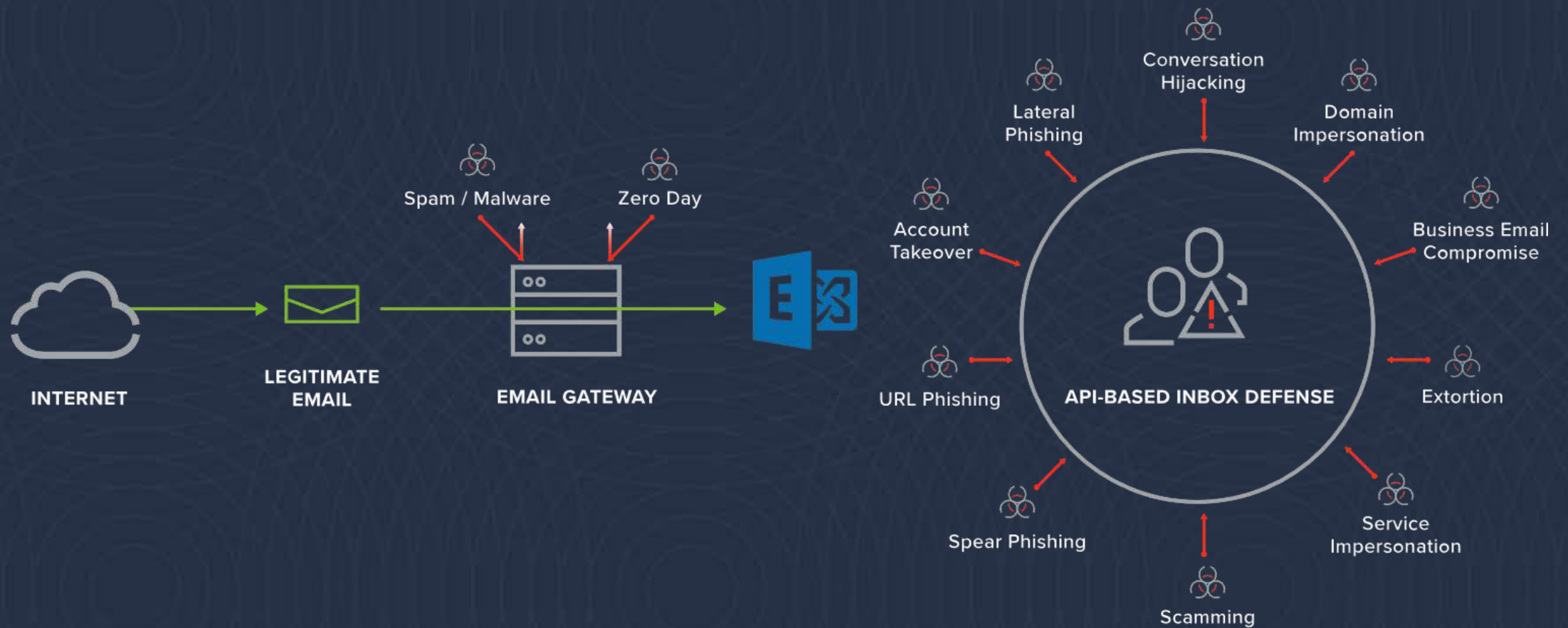
# Email attacks are evolving



<https://www.barracuda.com/13-threats-report>



# Email security – two forms of prevention



# The 13 Known Threat Types

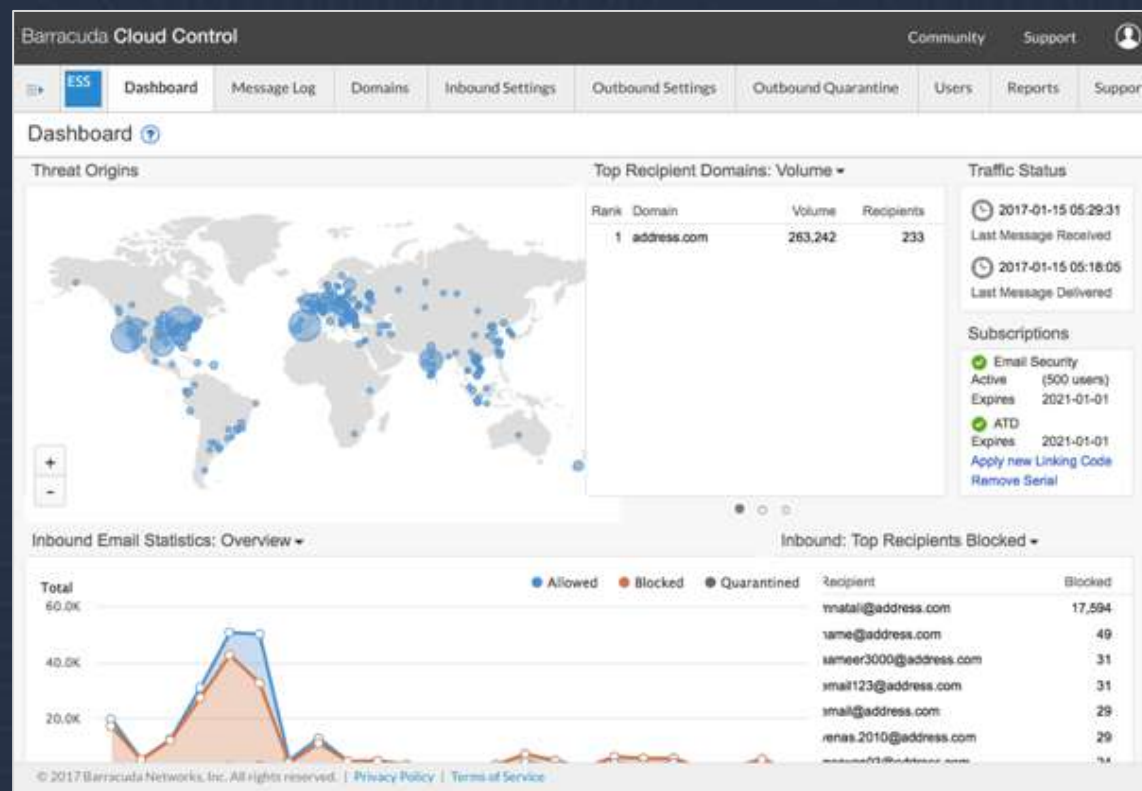
		Threat type	Barracuda TES	Gateway Solutions
Total email Security	Essential	Spam	Green	Yellow
		Malware	Green	Yellow
	Sentinel	Data Exfiltration	Green	Green
		URL Phishing	Green	Green
		Lateral Phishing	Green	Red
		Spear Phishing	Green	Red
		Service Impersonation	Green	Yellow
		Domain Impersonation	Green	Yellow
		Business Email Compromise	Green	Red
		Scamming	Green	Yellow
		Blackmail	Light Green	Yellow
		Account Takeover	Green	Red
		Conversation Hijacking	Green	Red

# Complete Protection for Office 365



## Essentials Advanced Email Security Service

- Protects inbound & outbound email
- Spam & viruses are blocked
- Advanced Threat Detection (Sandboxing)
- Email spooling and Emergency Inbox
- DLP and Encryption
- Comprehensive reporting





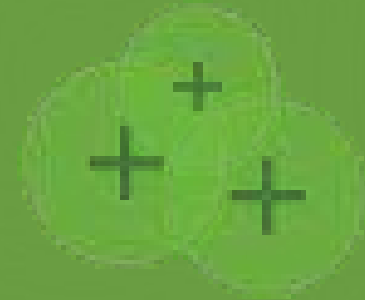
# Sentinel: Fraud prevention and inbox defense

The letters 'AI' in a light blue, sans-serif font, centered on a dark blue background.

AI for  
Real-Time  
Spear Phishing  
Prevention



Domain Fraud  
Visibility and  
Protection with  
DMARC



Account  
Takeover  
detection and  
remediation



# Inbox defense technology



Understands abnormal behavior based on an **identity graph**



**Machine learning/IA analysis -  
Barracuda Security Insights**





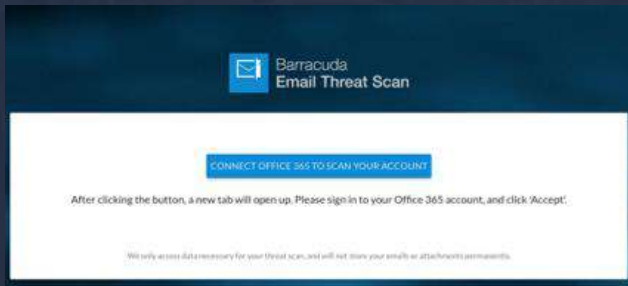
# Barracuda Email Threat Scanner

## Barracuda Email Threat Scanner (ETS)

- Cloud service that scans O365 mailboxes
- Find advanced threats at rest
- Identifies owners of said threats
- Provides detailed reports and recommendations

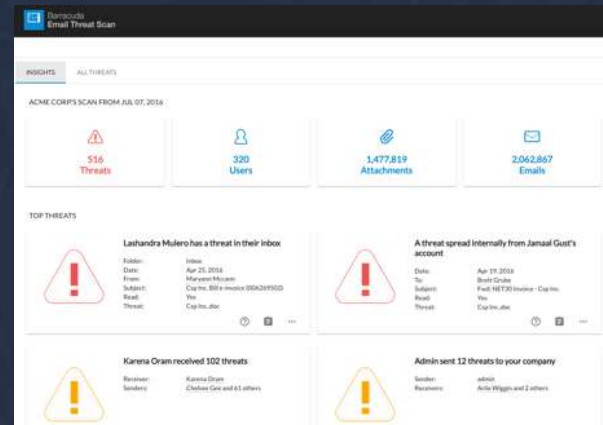
### 1) Scan

Send customer link to [scan.barracuda.com/signup](http://scan.barracuda.com/signup)



### 2) Educate

Educate customer on their top risks



### 3) Remediate

Provide remediation checklist & sign up for Essentials





SaaS Level Up

## Data Security Audit

**Alberto Gonzalez**  
ArexData CTO

plain  
concepts 

*Arexdata, la manera simple de proteger tus datos*



**AREXDATA**

PROTECT YOUR MOST VALUABLE ASSET - YOUR DATA

Alberto Gonzalez  
CTO, ArexData

**Alberto González**  
**CTO, Arexdata**

[www.arexdata.com](http://www.arexdata.com)

© 2021 Arexdata.

# Auditoría de Datos

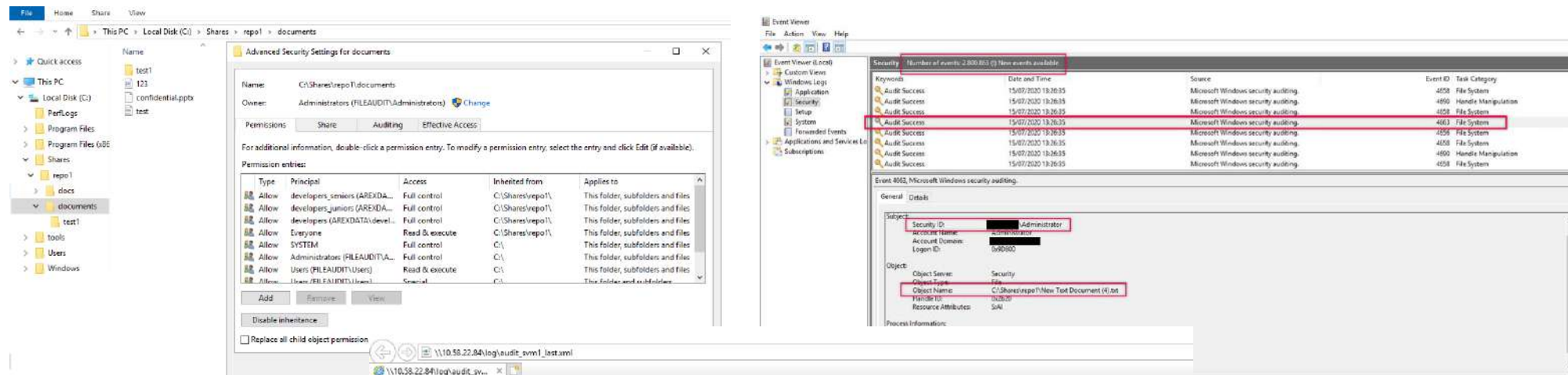
## El problema: ¿dónde están mis datos?

*El activo más importante de tu compañía es tus datos... pero están desperdigados en múltiples sitios*

- Los datos los generas en un sitio, como en tu disco local... y rápidamente se diseminan sin control en otros repositorios como la cloud, en almacenes de datos, sharepoint, copias locales....etc...
- Y las amenazas actuales son cada vez mayores: intrusiones, ransomware, fugas de información... en todas partes, todos los días
- Controlar los datos es complicado: aproximadamente 90% de las compañías no tienen implementados procesos para gestionar el dato. Saber donde estan y quien accede a los datos es una de las principales dificultades

# No es simple conseguir la visión completa

*Multiples herramientas, con información complicada de entender*



The image shows two screenshots from a Windows environment. The left screenshot displays the 'Advanced Security Settings for documents' dialog box, showing a list of permission entries for the folder 'C:\Shares\repo1\documents'. The right screenshot shows the Windows Event Viewer, displaying a list of security events. A table of events is visible:

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	15/07/2020 19:26:55	Microsoft Windows security auditing	4658	File System
Audit Success	15/07/2020 19:26:55	Microsoft Windows security auditing	4658	Handle Manipulation
Audit Success	15/07/2020 19:26:55	Microsoft Windows security auditing	4658	File System
Audit Success	15/07/2020 19:26:55	Microsoft Windows security auditing	4663	File System
Audit Success	15/07/2020 19:26:55	Microsoft Windows security auditing	4656	File System
Audit Success	15/07/2020 19:26:55	Microsoft Windows security auditing	4658	File System
Audit Success	15/07/2020 19:26:55	Microsoft Windows security auditing	4600	Handle Manipulation
Audit Success	15/07/2020 19:26:55	Microsoft Windows security auditing	4658	File System

Below the event list, the details for Event 4663 are shown, including the subject (Administrator) and object (C:\Shares\repo1\New Text Document (1).txt).

```
<?xml version="1.0"?>
<Events xmlns="http://www.netapp.com/schemas/ONTAP/2007/AuditLog">
  <System>
    <Provider Guid="{3CB2A168-FE19-4A4E-BDAD-DCF422F13473}" Name="NetApp-Security-Auditing"/>
    <EventID>4656</EventID>
    <EventName>Open Objects</EventName>
    <Version>101.3</Version>
    <Source>CIF5</Source>
    <Level>0</Level>
    <Opcode>0</Opcode>
    <Keywords>0x0020000000000000</Keywords>
    <Result>Audit Success</Result>
    <TimeCreated SystemTime="2020-07-10T09:17:06.83299000Z"/>
    <Correlation/>
    <Channel>Security</Channel>
    <Computer>ontapselect97/svm1</Computer>
    <ComputerUUID>5476018a-6a9e-11ea-ae3b-0050568ca3cf/2a75bde7-6aa8-11ea-b68d-00a0b8960088</ComputerUUID>
    <Security/>
  </System>
  <EventData>
    <Data Name="SubjectIP" IPVersion="4">10.58.22.200</Data>
    <Data Name="SubjectUnix" Local="false" Gid="1" Uid="0"/>
    <Data Name="SubjectUserSid">S-1-5-21-1843849653-2909494909-3618756610-500</Data>
    <Data Name="SubjectUserName" Administrator</Data>
    <Data Name="SubjectDomainName" AREXDATA</Data>
    <Data Name="SubjectUserLocal" false</Data>
    <Data Name="ObjectServer" Security</Data>
    <Data Name="ObjectType" Directory</Data>
    <Data Name="HandleID" 000000000040d0d00001422316ca62d</Data>
    <Data Name="ObjectName" [engineering]/osd</Data>
    <Data Name="AccessList" %964123 %961538</Data>
    <Data Name="AccessMask" 2080</Data>
    <Data Name="DesiredAccess" Read Attributes; Read ACL</Data>
    <Data Name="Attributes"/>
  </EventData>
</Events>
</Event>
```

# Así que resulta complicado obtener respuestas a preguntas básicas

*... y cuando las consigues es a costa de que tu departamento IT invierta mucho tiempo y esfuerzo*

*¿Quién tiene acceso a esta carpeta?*

*¿A qué carpetas puede un usuario o grupo acceder?*

*¿Quién ha estado accediendo a estos ficheros durante el último más? ¿Y para qué?*

*¿Hay datos sensibles o privados en mis carpetas? (HIPAA, PCI, GDPR)*

*¿Que datos y accesos hay en mis carpetas públicas?*

*¿Cómo puedo arreglar todo esto?*

# Necesidades típicas

- “Necesito cumplir con la **regulación**, en particular con GRPD”
- “Tengo que poner **orden en mi AD**: revisar permisos, limpiar grupos, etc..”
- “Queremos revisar el **estado de cumplimiento** de regulaciones internas y externas”
- “Soy **responsable de los datos** asociados a mi **departamento de negocio**, pero no puedo depender de TI para controlar los accesos”
- “Hemos de revisar los accesos a ficheros para poder **prevenir y eliminar cyber-amenazas** a la compañía”



# Endpoint Audit

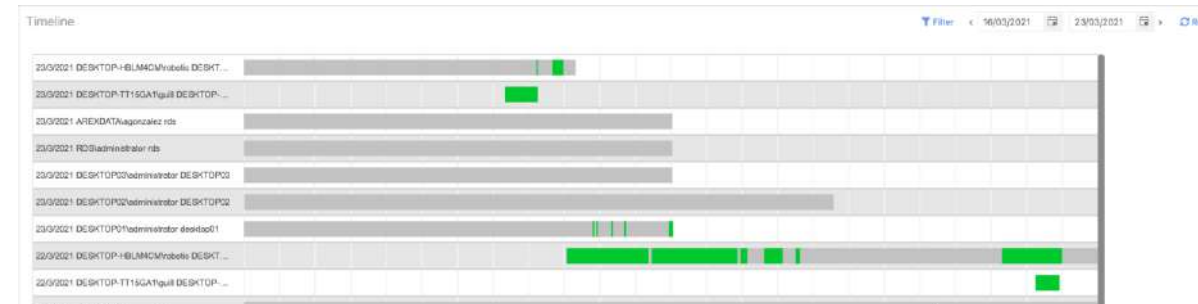
controla los datos que residen en las estaciones de trabajo de los usuarios

- Proporciona una **vision central** de la actividad en las estaciones de trabajo de sus usuarios
- Controlar accesos y modificaciones a ficheros
- Monitorizar los trabajos de impresión
- Ver la actividad de sus usuarios: aplicaciones usadas, tiempo trabajado, software instalado
- **Detectar y alertar situaciones de riesgo** como borrados masivos, copios de discos, muchas impresiones, etc... Reaccionar ante ellas a través de la ejecución automática de de los scripts que defina el cliente



Missing Hours

Date	User	Desktop	Start	End	Activity	Min	Protection	Registration	Updated	Offline
2023/03/21	DESKTOP-TT15GATqj48	DESKTOP-TT15GATqj48	07:28	18:13	Idle				0h	7h 45m
2023/03/21	DESKTOP-HBLMACMvrbobc	DESKTOP-HBLMACMvrbobc	08:18	08:38	Idle	0%	100%	0h 0m	0h 0m	1h 10m
2023/03/21	DESKTOP03administrator	DESKTOP03	08:08	10:00	Idle	75%	100%	0h 0m	0h 0m	1h 52m
2023/03/21	DESKTOP-42H4L2FJagonzalez	DESKTOP-42H4L2FJagonzalez			Idle					0h 0m
2023/03/21	DESKTOP01administrator	DESKTOP01			Idle					0h 0m
2023/03/21	DESKTOP02administrator	DESKTOP02	17:43	18:00	Idle	100%	100%	0h 0m	0h 0m	0h 16m
2023/03/21	DESKTOP-TT15GATqj48	DESKTOP-TT15GATqj48	07:28	18:13	Idle					7h 45m
2023/03/21	AREXDATAagonzalez	AREXDATAagonzalez			Idle					0h 32m
2023/03/21	RDSAdministrator	RDSAdministrator			Idle					0h 0m
2023/03/21	DESKTOP03administrator	DESKTOP03			Idle					0h 0m
2023/03/21	DESKTOP02administrator	DESKTOP02			Idle					0h 0m
2023/03/21	DESKTOP01administrator	DESKTOP01			Idle					0h 0m
2023/03/21	DESKTOP-HBLMACMvrbobc	DESKTOP-HBLMACMvrbobc			Idle					0h 0m
2023/03/21	DESKTOP-TT15GATqj48	DESKTOP-TT15GATqj48			Idle					0h 0m
2023/03/21	AREXDATAagonzalez	AREXDATAagonzalez			Idle					0h 0m
2023/03/21	RDSAdministrator	RDSAdministrator			Idle					0h 0m
2023/03/21	DESKTOP03administrator	DESKTOP03			Idle					0h 0m
2023/03/21	DESKTOP02administrator	DESKTOP02			Idle					0h 0m
2023/03/21	DESKTOP01administrator	DESKTOP01			Idle					0h 0m
2023/03/21	DESKTOP-HBLMACMvrbobc	DESKTOP-HBLMACMvrbobc			Idle					0h 0m
2023/03/21	DESKTOP-TT15GATqj48	DESKTOP-TT15GATqj48			Idle					0h 0m

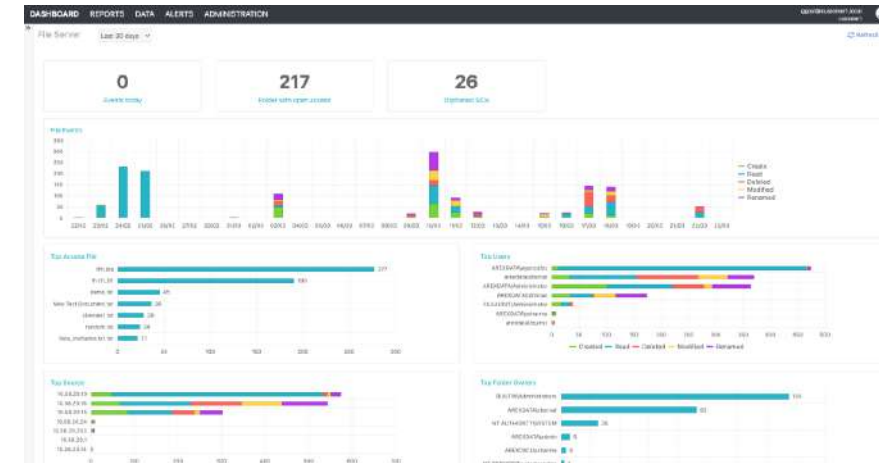




# Enterprise Audit

protege los datos en repositorios centrales, almacenamiento, y cloud

- Obtener una **vision única de la acciones** en sus ficheros, sin importar el repositorio donde ocurran
- **Visualizar la actividad en los ficheros** almacenados en Fileservers, Office365, Google Suite, y en sus cabinas NetApp (1)
- **Muestra los permisos de cada fichero**, permitiendo detectar situaciones de riesgo como permisos excesivos o “shares” abiertos sin autenticación
- **Obtenga una vista común de todos sus Active Directories y Azure AD**, visualizando los eventos de todos sus dominios. Detecte malas prácticas como cuentas inactivas, grupos de seguridad vacios, contraseñas no cambiadas, etc...

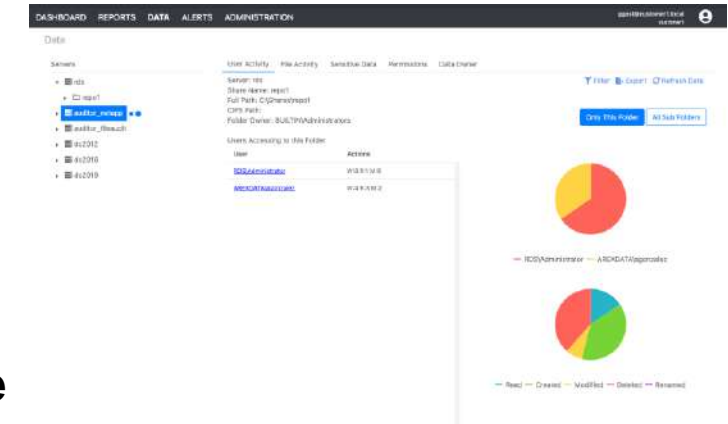


Date	Server	Operation	Source	User	Path	File
29/09/2021 19:01:22	netapp	Created	10.58.20.24	AREXDATA\magarwal	vol_root_path\qa_path\magarwal	New Text Document.txt
29/09/2021 19:01:13	netapp	Created	10.58.20.24	AREXDATA\magarwal	vol_root_path\qa_path\New folder	
28/09/2021 17:35:35	SharePoint	Created	47.61.246.201	ggost@arexdata.com	Arexdata\Shared Documents\Marketing\Templates	
22/09/2021 09:02:26	OneDrive	Created	87.221.137.125	agonzalez@arexdata.com	Documents\QA\Test Cases	
22/09/2021 09:01:47	OneDrive	Created	87.221.137.125	agonzalez@arexdata.com	Documents\New folder	
22/09/2021 09:01:14	OneDrive	Created	87.221.137.125	agonzalez@arexdata.com	Documents\Engineering\New folder	
21/09/2021 14:03:00	netapp	Created	10.58.20.10	AREXDATA\agonzalez	vol_root_path\qa_path\agonzalez	New Text Document.txt
20/09/2021 15:58:11	fileaudit	Created	10.58.20.253	AREXDATA\rey	C:\Shares\qa	arabic.txt

# Enterprise Management

delegar la protección de datos en los responsables de departamento u otros expertos

- Aproveche el conocimiento que sus **responsables de líneas de negocio** tienen de los datos de sus departamentos para mejorar la protección y control de los datos
- **Reduzca la complejidad técnica** que la Seguridad de los Datos implica a sus responsables operacionales.
- Revise y analice la **actividades de usuarios** sobre los ficheros bajo su responsabilidad
- Visualice y gestione los permisos desde **una única vista con un interface simple de usar**



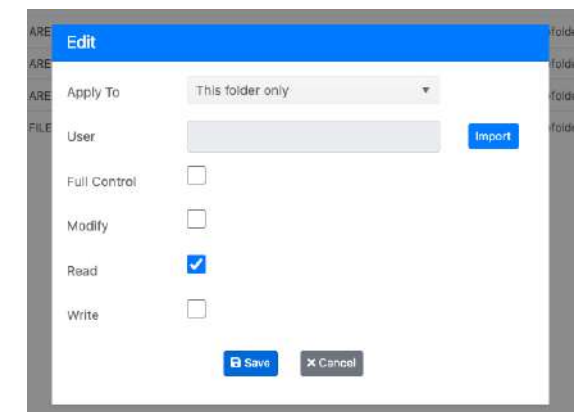
User Activity | File Activity | Sensitive Data | **Permissions** | Data Owner

Server: auditor\_fileaudit  
Share Name: qa  
Full Path: C:\Shares\qa\agonzalez  
CIFS Path: C\$\Shares\qa\agonzalez  
Folder Owner: BUILTIN\Administrators

Refresh Data

**+ Add**

User	NTFS Permissions	Apply To	Actions
AREXDATA\developer_junior_1	R X L	This folder subfolders and files	Inherited
AREXDATA\agonzalez	R X L	This folder subfolders and files	Inherited
AREXDATA\Administrator	F W R M X L	This folder subfolders and files	Inherited
FILEAUDIT\Administrator	F W R M X L	This folder subfolders and files	Inherited







SaaS Level Up

Demo ArexData

plain  
concepts 



SaaS Level Up

# Questions?

plain  
concepts 

plain  
concepts



SaaS Level Up