Cómo proteger tus datos críticos de negocio en Microsoft 365

Barracuda. AREXDATA plain concepts SaaS Level Up

Impulsa tu negocio SaaS

SaaS Level Up

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

plain concepts

SaaS Level Up

Zero Trust

Isabel Gómez
SaaS Level Up CEO

plain concepts

SaaS Level Up

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** polices
- Data protection against **out of band** vectors

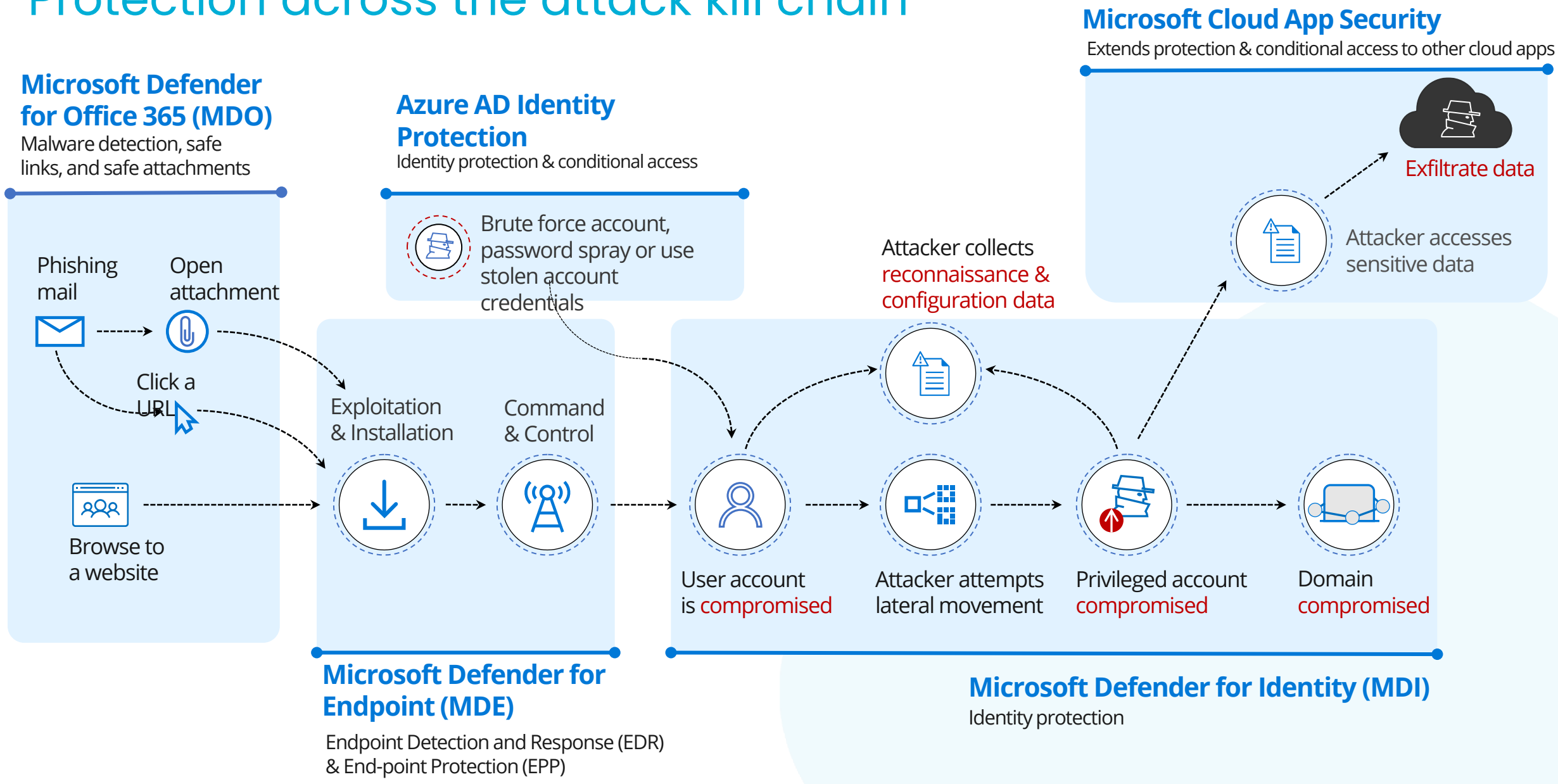
Assume breach

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

plain concepts

Protection across the attack kill chain



SaaS Level Up

Identity Governance and Security

Ivan Bravo
SaaS Level Up Cloud Engineer

plain concepts

SaaS Level Up

Azure AD: Microsoft 365 Authentication

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

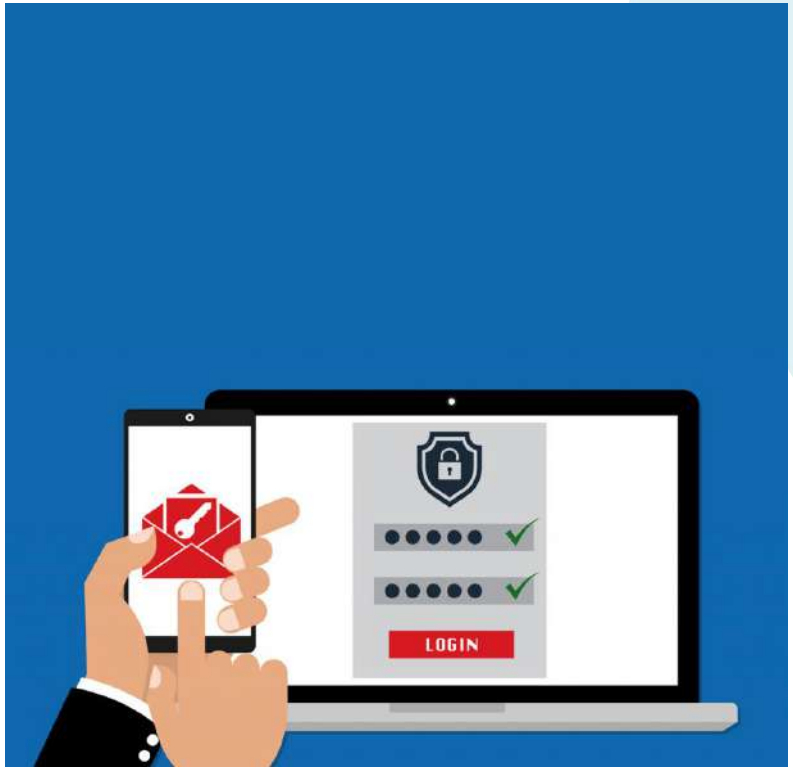
Azure AD provides authentication and authorization for Microsoft 365 and for other Microsoft cloud offerings, including Azure

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)



plain concepts

SaaS Level Up

Unified identity management

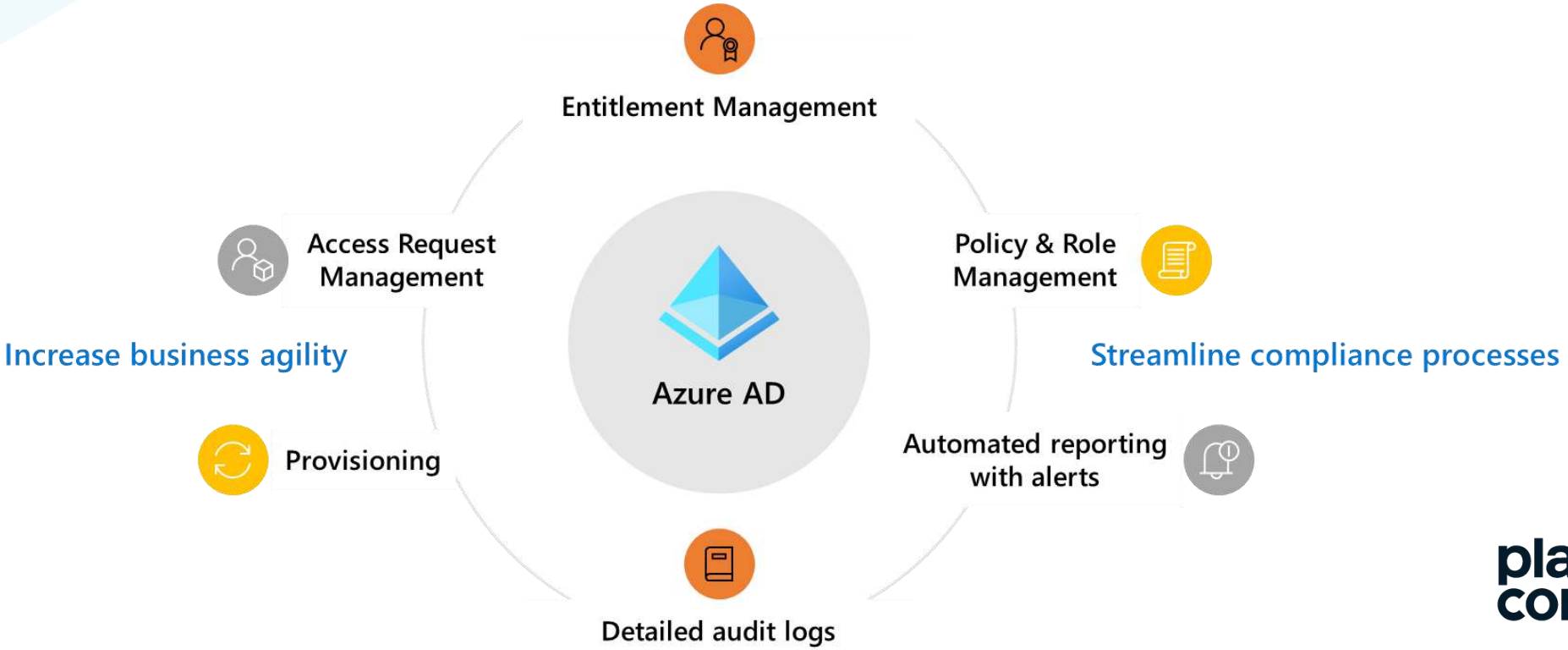
plain concepts

SaaS Level Up

Azure AD identity and access lifecycle management

Strengthen security while maintaining productivity

Increase business agility while strengthening security and compliance posture at scale



plain concepts

SaaS Level Up

Identity governance in Azure AD

The tasks of Azure AD identity governance

Govern the identity lifecycle

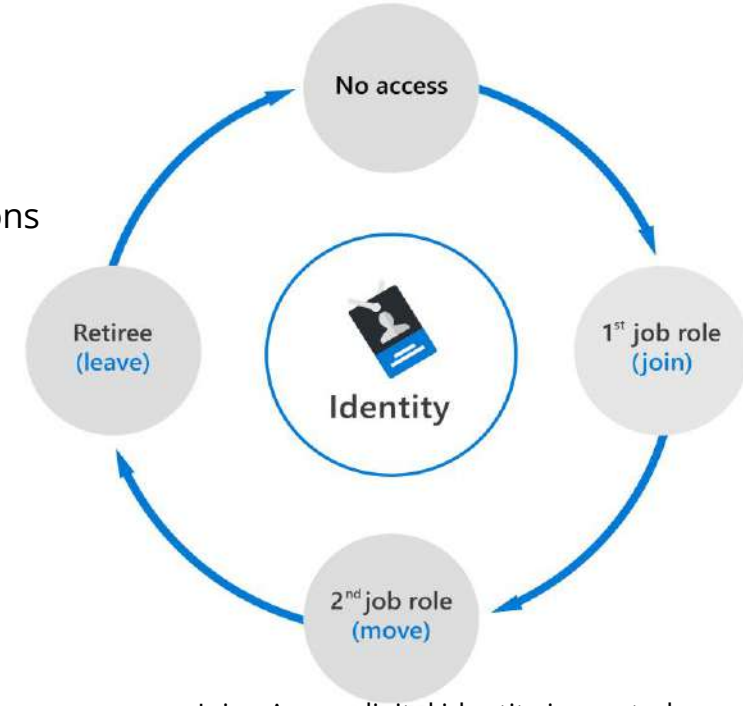
Azure AD Premium & Identity Manager: users coming from HCM cloud and on-prem solutions
Entitlement Management

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.

plain concepts

SaaS Level Up

Entitlement management and access reviews

Entitlement management

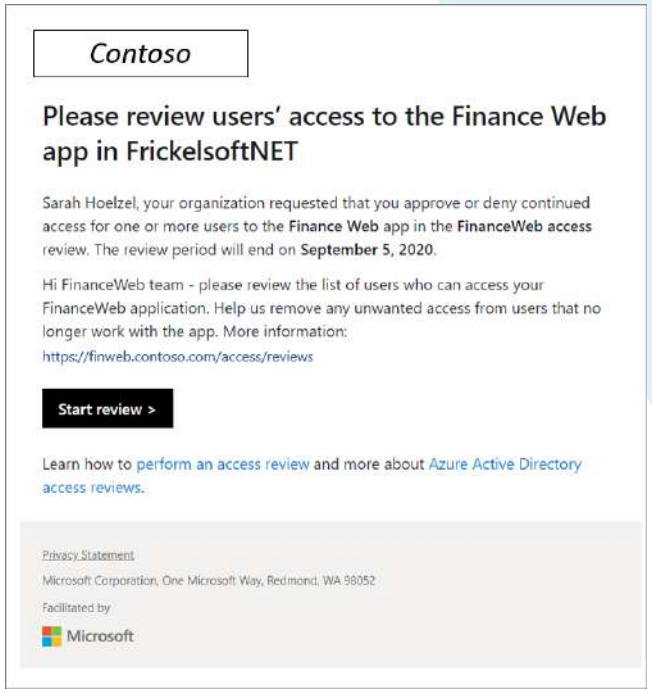
- It is an identity governance feature that enables organizations to manage identity and access lifecycle at scale.
- **Access Packages**: It automates access request workflows, access assignments, reviews, and expiration.

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.


Contoso

Please review users' access to the Finance Web app in FrickelsoftNET

Sarah Hoelzel, your organization requested that you approve or deny continued access for one or more users to the **Finance Web** app in the **FinanceWeb access** review. The review period will end on **September 5, 2020**.

Hi FinanceWeb team - please review the list of users who can access your FinanceWeb application. Help us remove any unwanted access from users that no longer work with the app. More information:
https://finweb.contoso.com/access/reviews

Start review >

Learn how to perform an access review and more about Azure Active Directory access reviews.

Privacy Statement
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052
Facilitated by
Microsoft

plain concepts
SaaS Level Up
Impulsa tu negocio SaaS

SaaS Level Up

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

plain concepts

SaaS Level Up

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

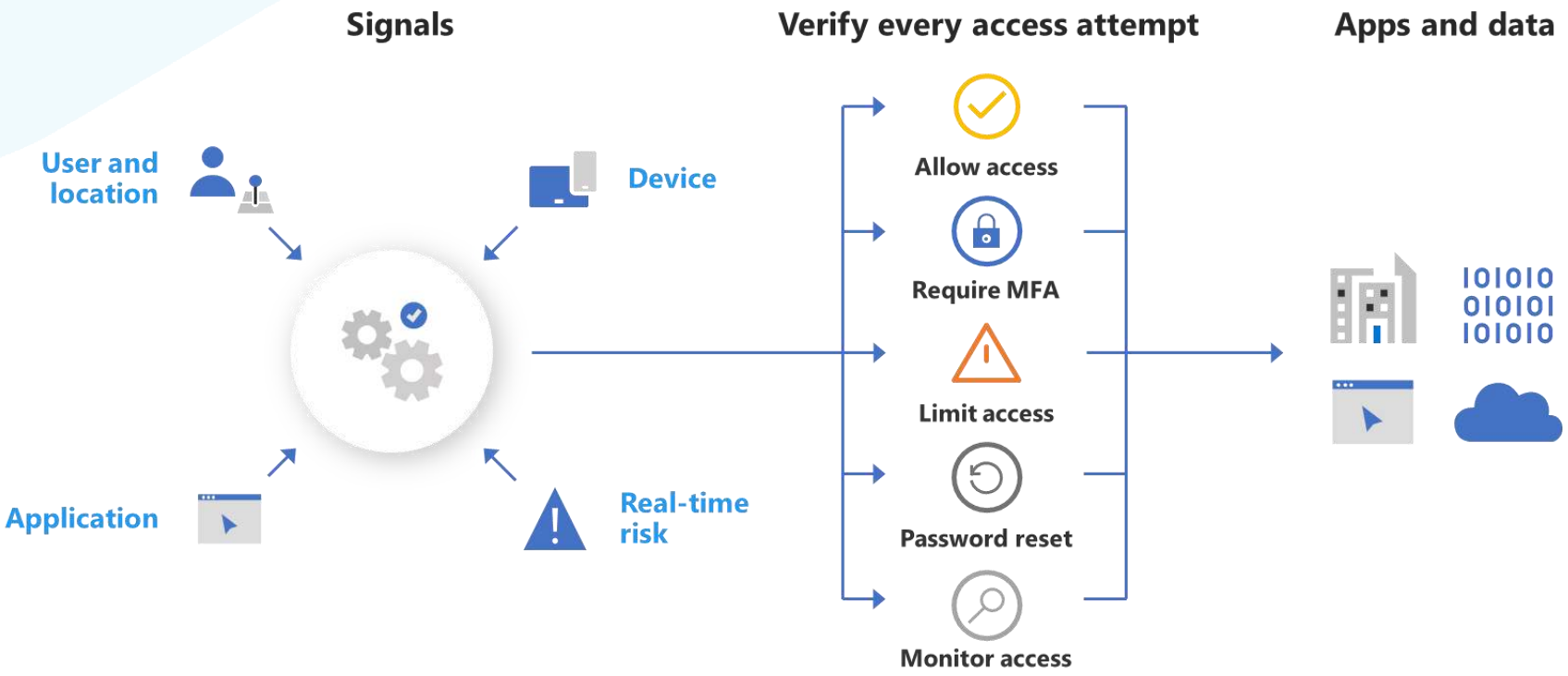
Multi-factor authentication prevents 99.9% of identity attacks

plain concepts

SaaS Level Up

Protect identities with Conditional Access

Enable Zero Trust with strong authentication and adaptive policies



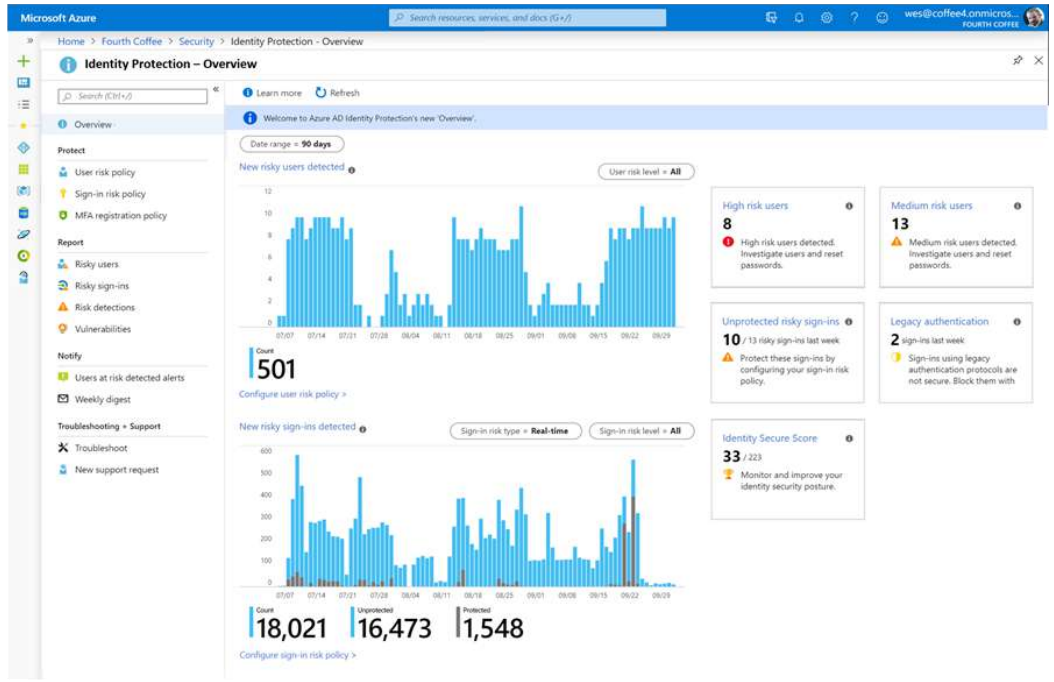
plain concepts

SaaS Level Up

Identity protection

Intelligently detect and respond to compromised accounts

- Enhanced logging
- Threat alerts
- Risk scores
- Sign-in reports
- Privileged access insights



plain concepts

SaaS Level Up

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

plain concepts

- **Azure AD P2** license is required

SaaS Level Up

Privileged Identity Management (PIM)

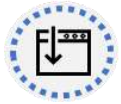
PIM enables you to manage, control, and monitor access to important resources in your organization.

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.

plain concepts

SaaS Level Up

Microsoft Information Protection

José Gallardo
Plain Concepts Cloud Solutions Engineer

plain concepts

SaaS Level Up

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

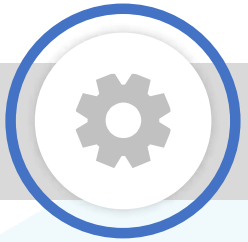
plain concepts

SaaS Level Up

Microsoft Information Protection

Integrated
into user apps

Rich & Intelligent
classification



Extensible
to other systems

Unified
management

User-centered
balances security
with productivity

plain concepts

SaaS Level Up

Microsoft Information Protection

Discover and protect your data across all environments

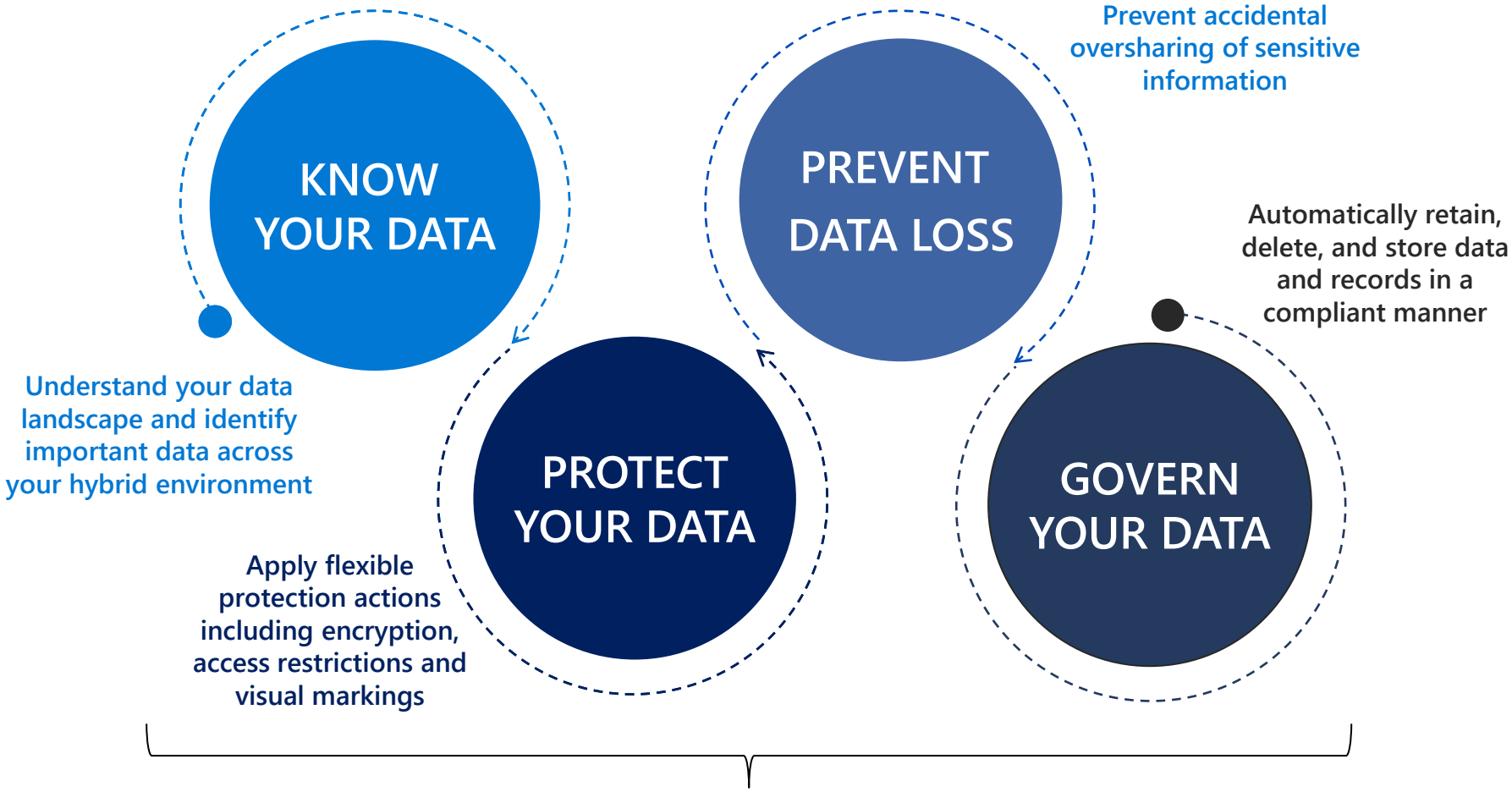
On-prem	Microsoft 365 Apps Across Platforms	SharePoint Sites Teams, Microsoft 365 Groups	Exchange Online	SharePoint Online	Non-Microsoft Clouds and SaaS apps
Classify and label data in on-prem repositories	Label and protect Office files natively across Windows, Mac, iOS, Android and Web Clients	Label and protect sensitive SharePoint Sites, Teams, Office 365 Groups, PowerBI artifacts	Automatically label and protect sensitive emails in Exchange Online	Automatically label and protect sensitive files in SharePoint Online and OneDrive for Business	Extend protection through Microsoft Cloud App Security to third party clouds and SaaS apps

Unified Management in Microsoft 365 compliance center

plain concepts

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

Admin Center | Compliance Center

https://compliance.microsoft.com

Microsoft 365 compliance

Search

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
Project Obsidian	600
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

Retention labels

Sensitive labels

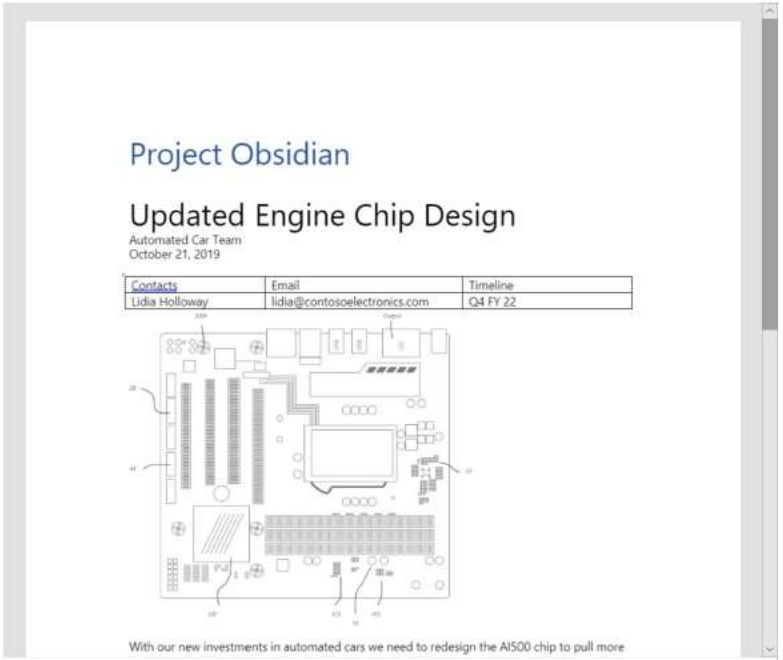
Export report ...

45 items

Name	Sensitive info type	Sensitive label
Project_Obsidian_chip_design.docx	Project Obsidian +1	-
Project_Obsidian_MSA_Draft_1.docx	Project Obsidian +1	-
Project_Obsidian_MSA_Draft_2.docx	Project Obsidian +1	-
Project_Obsidian_MSA_Draft_3.docx	Project Obsidian +1	-
Project_Obsidian_MSA_Draft_4.docx	Project Obsidian +1	-
Project_Obsidian_MSA_Draft_5.docx	Project Obsidian +1	-
Project_Obsidian_MSA_Final_for_review.docx	Project Obsidian +1	-
Project_Obsidian_MSA_Final_tobe_Signed.docx	Project Obsidian +1	-
Project_Obsidian_MSA_FInal_Signed.docx	Project Obsidian +1	-
Project_Obsidian_Contract_Obligation.docx	Project Obsidian +1	-
PO_Team_chart_v1.pdf	Project Obsidian +1	-
PO_Team_chart_v2.pdf	Project Obsidian +1	-
PO_Team_chart_Final.pdf	Project Obsidian +1	-
PO_Leaders_conference_notes.docx	Project Obsidian +1	-

Project Obsidian Spec. docx

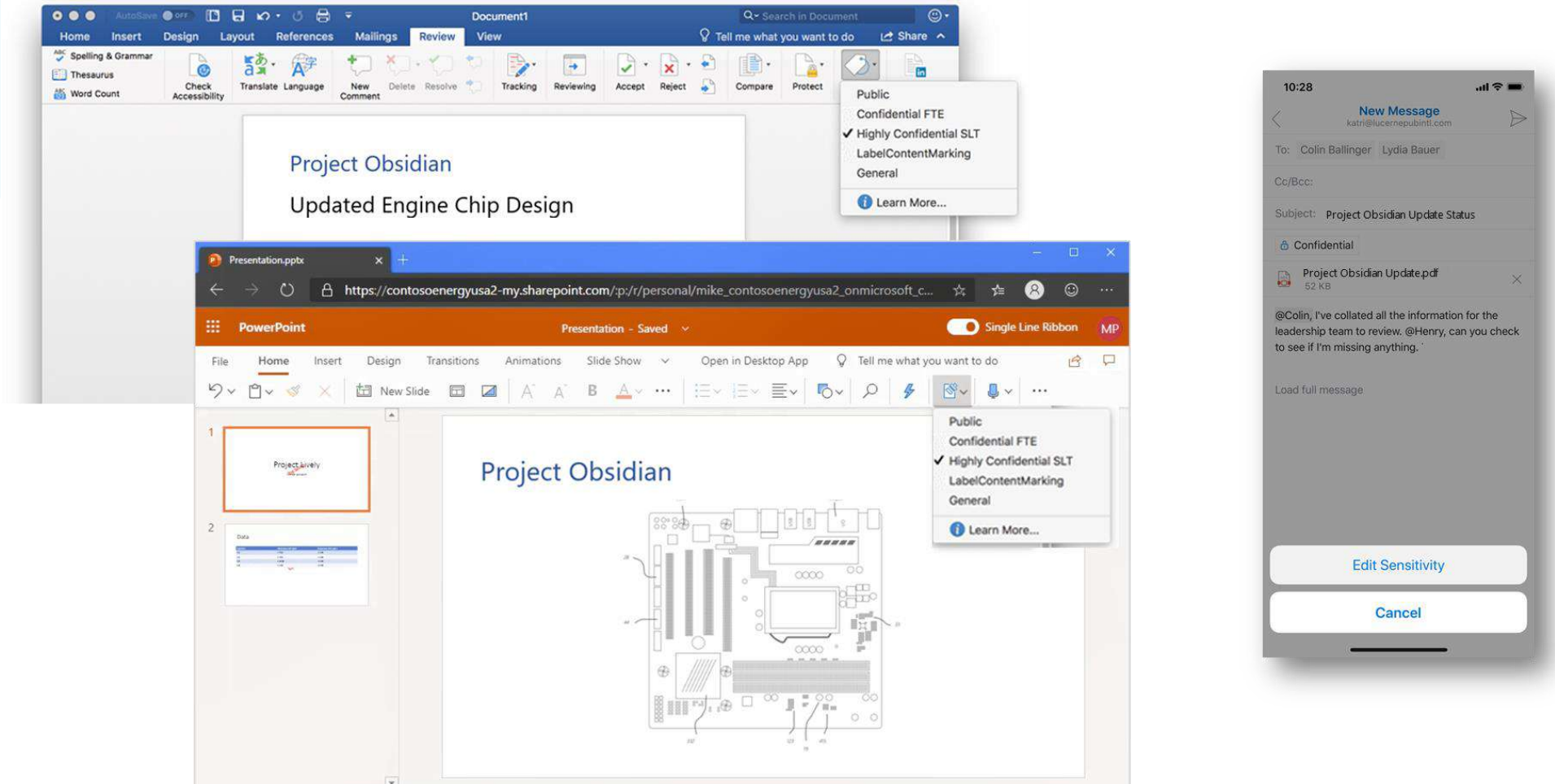
Source view | Details



Provide feedback | Cancel

SaaS Level Up

Native manual labeling in Office apps across all platforms



plain concepts

Admin Center | Compliance Center

https://compliance.microsoft.com

Microsoft 365 compliance

Search

Data classification

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

List view | Data visualization

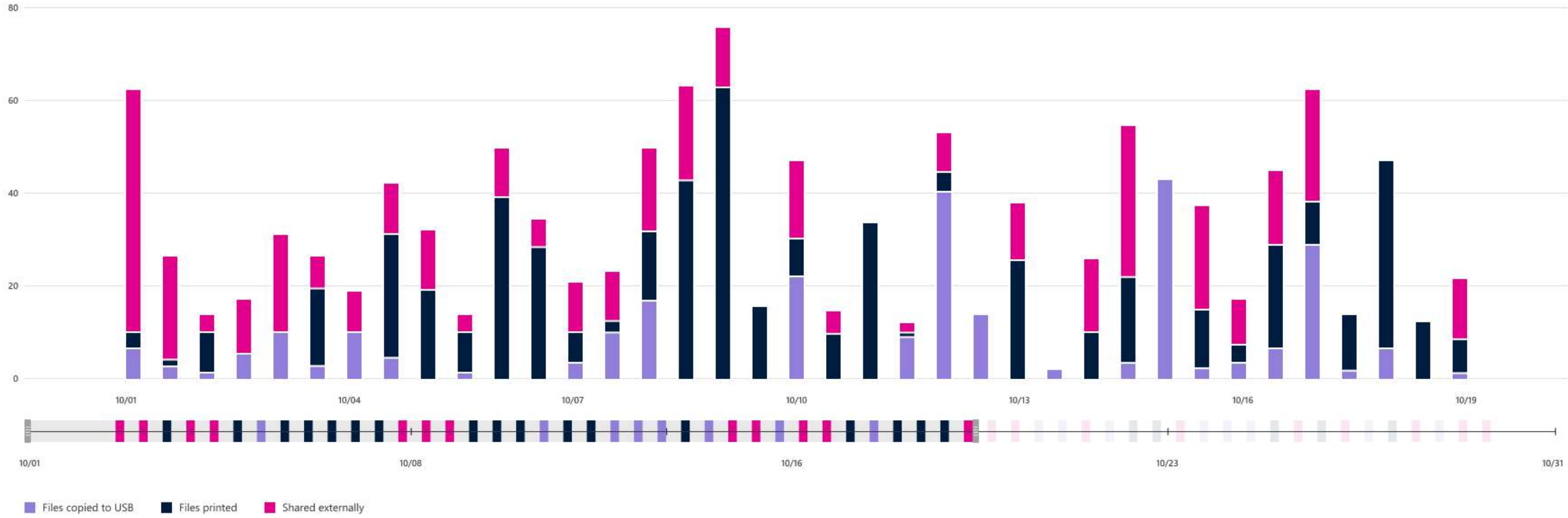
Filter by

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

SaaS Level Up

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

plain concepts

SaaS Level Up

Microsoft says that you need 3rd 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

plain concepts

Barracuda & M365 Backup

Miguel López
Country Manager – Iberia
mlopez@barracuda.com

Barracuda
Your journey, secured.

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

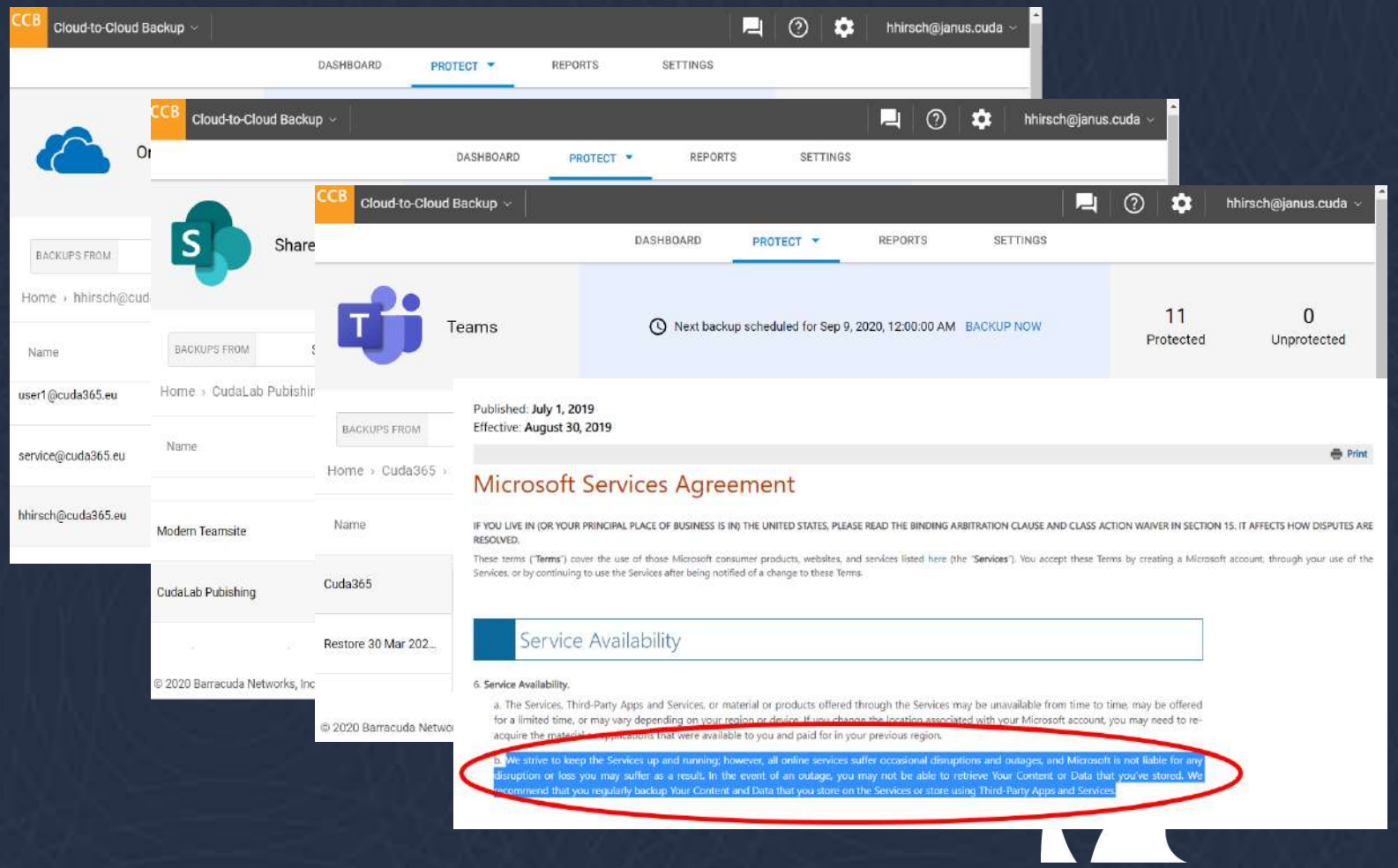
1: Soft Delete occurs when an item is moved to a temporary recycle bin (example: right-click and delete in Outlook)
2: Hard Delete occurs when an item is removed entirely from the source (example: SHIFT+Delete an item in Outlook)
3: After an item is cleared from the site recycle bin, the item will be 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

Barracuda
Essentials
for Microsoft Office 365

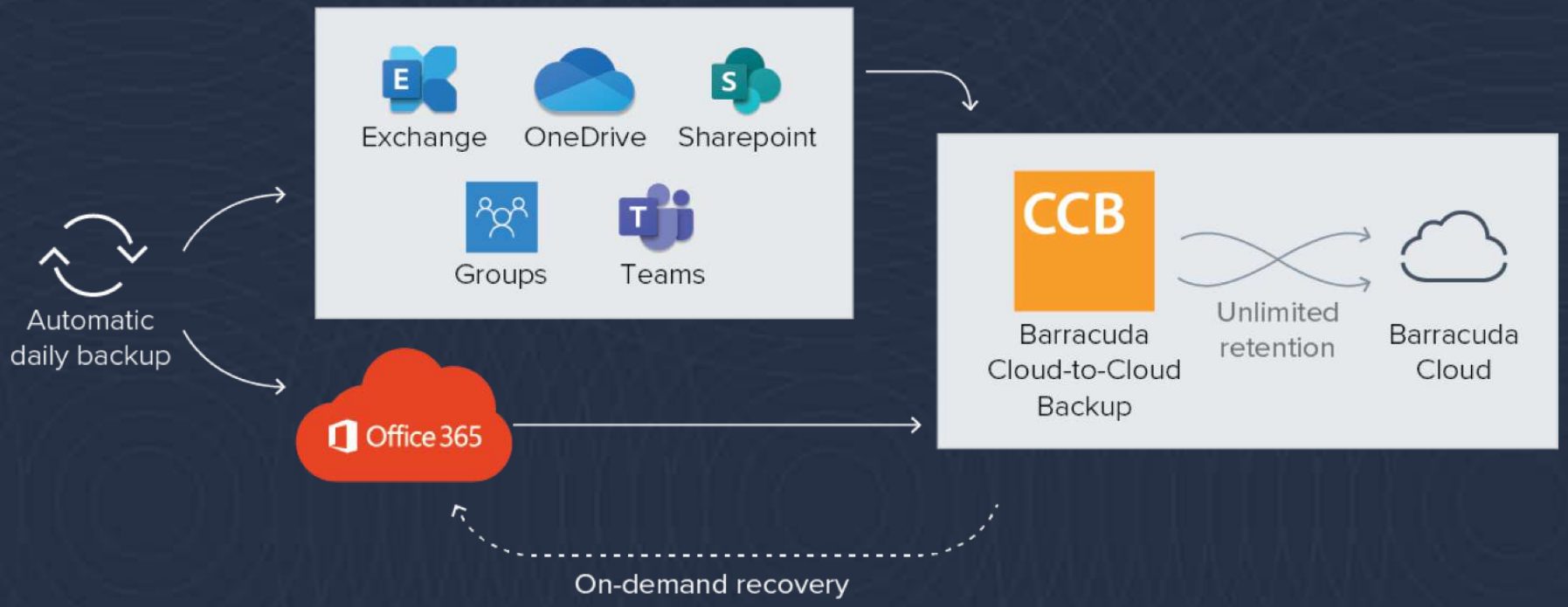
Backup, Recovery & Business Continuity for Office 365

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



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.



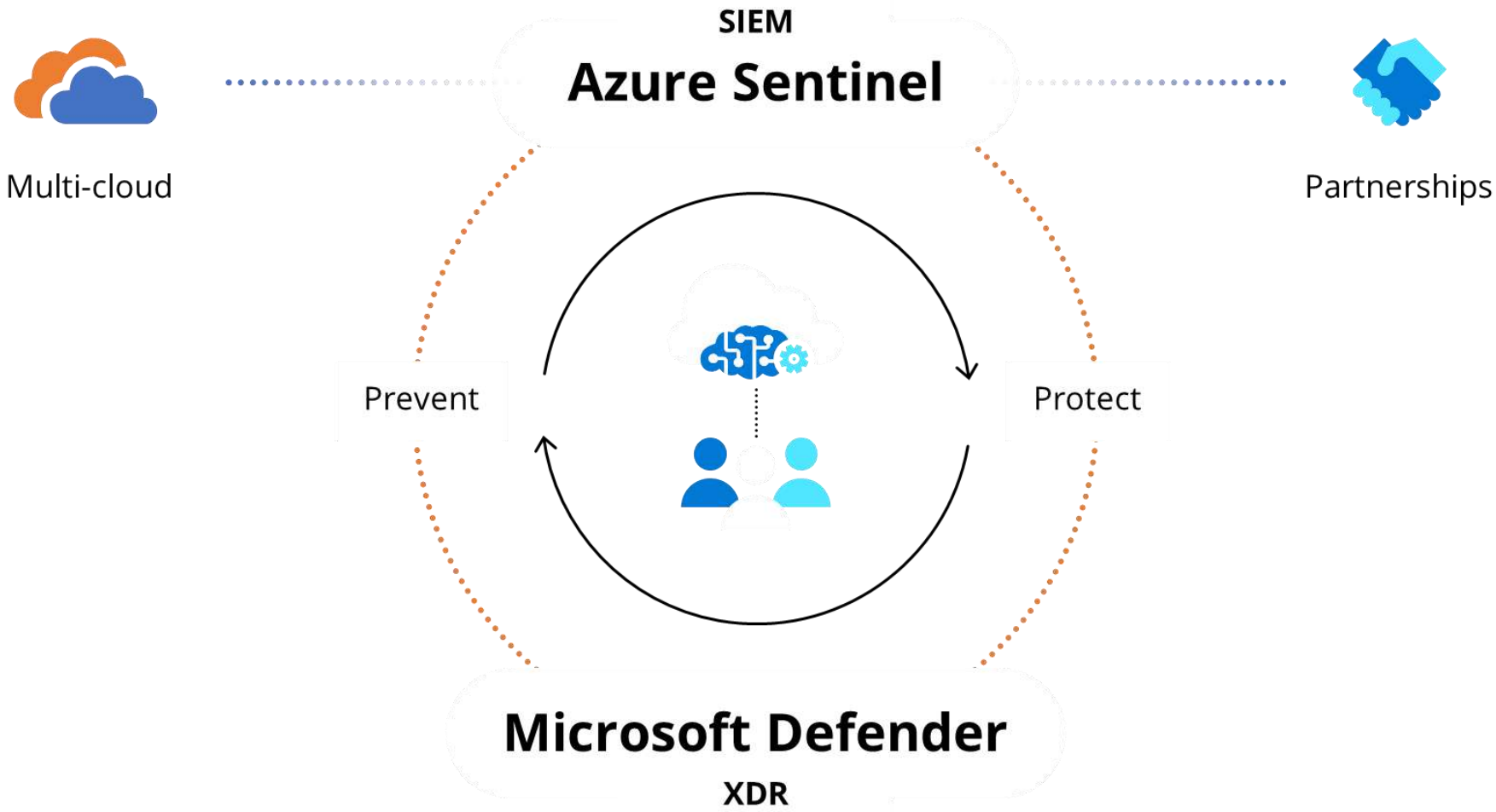
SaaS Level Up

Microsoft Defender

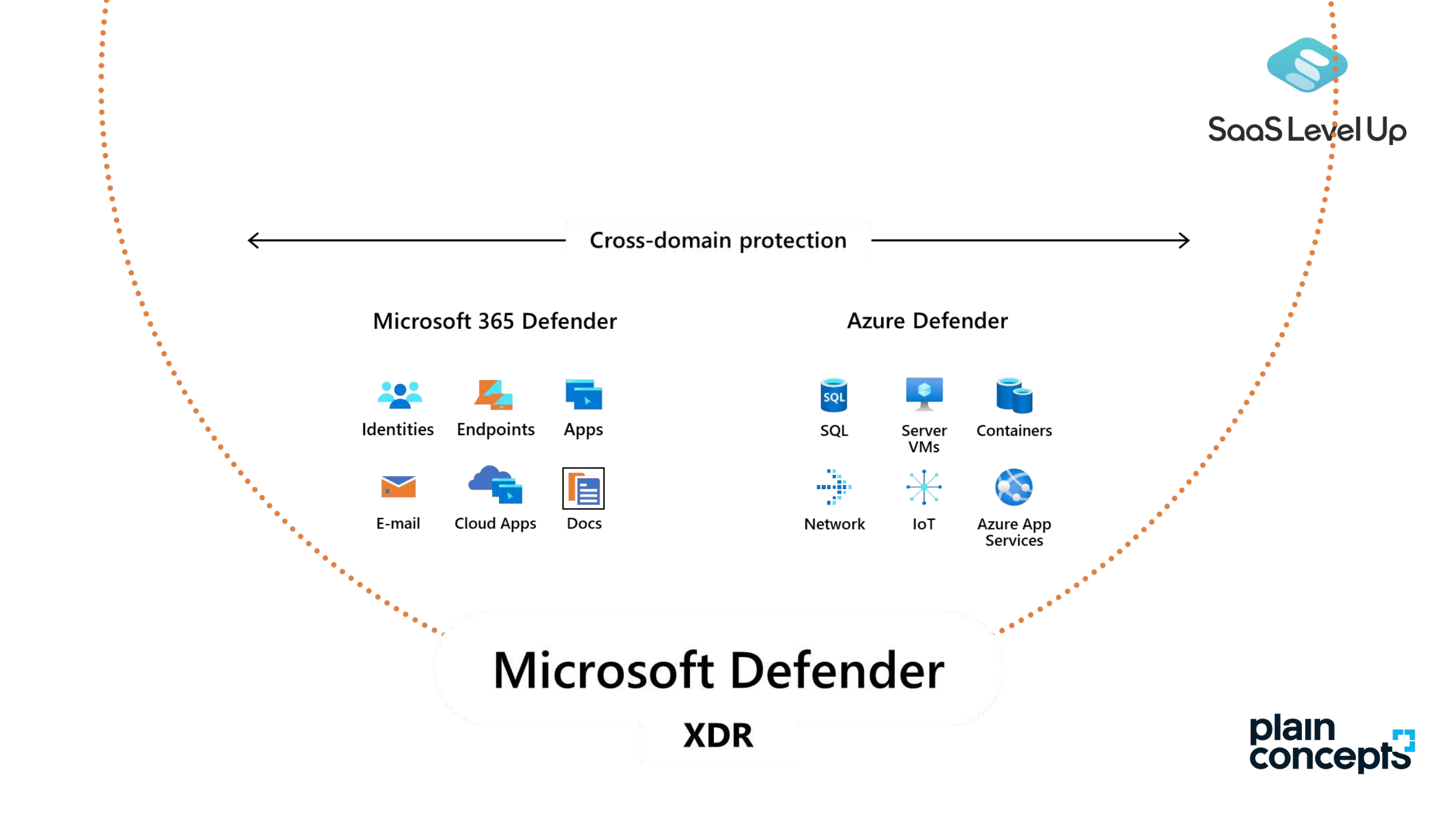
David Fernández
Plain Concepts Cloud Solutions Engineer

plain concepts

SaaS Level Up



plain concepts


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
plain concepts

Microsoft 365 Defender

SaaS Level Up

Automated cross-domain security

Identities	Endpoints	Cloud Apps	User Data
Microsoft Defender for Identity	**Microsoft Defender for Endpoint**	**Microsoft Cloud App Security**	**Microsoft Defender for Office 365**
Formerly Azure Advanced Threat Protection	**Formerly Microsoft Defender Advanced Threat Protection**		**Formerly Microsoft Office 365 Advanced Threat Protection**

Shift from individual silos to coordinated cross-domain security

plain concepts

SaaS Level Up

Microsoft 365 Defender

Automated cross-domain security

One portal
- unified entities

Coordinated active
protection from threats

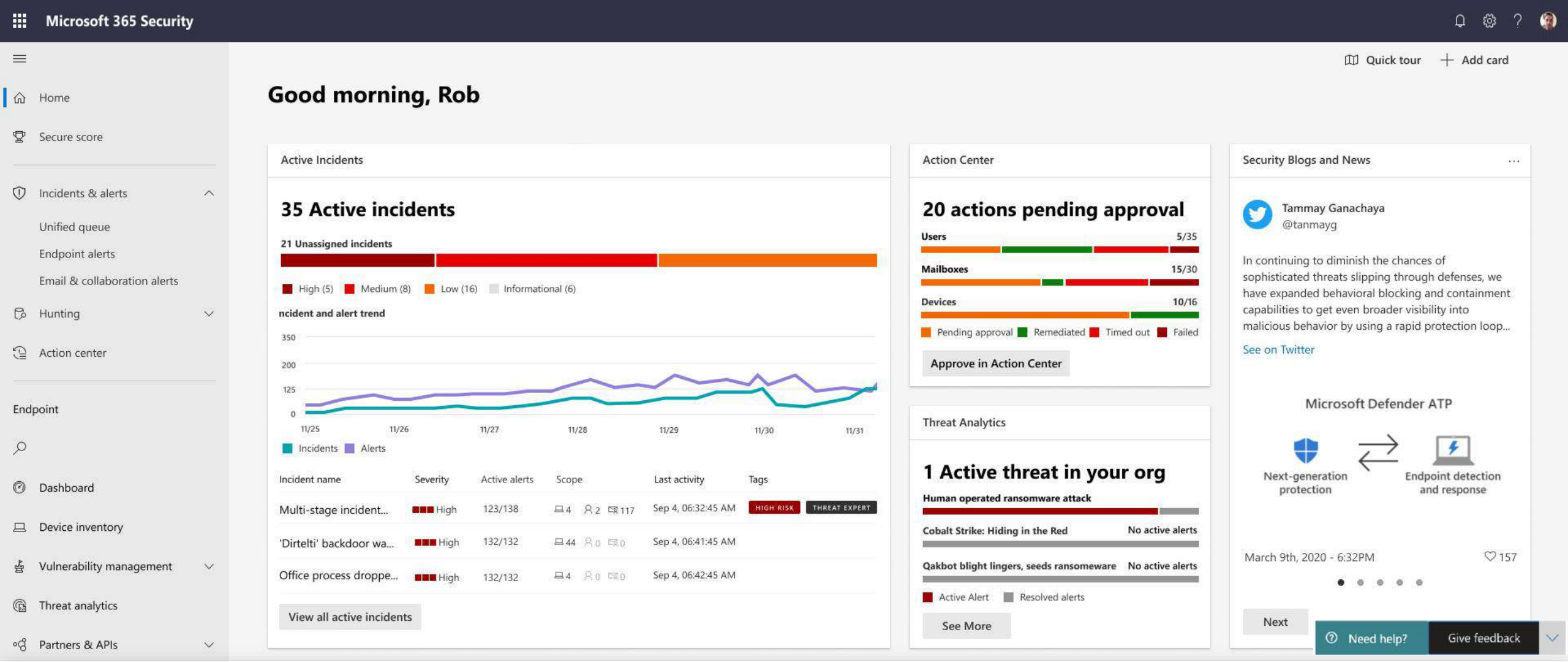
Automatic healing
of affected assets

Unified threat
intelligence and analytics

Cross-domain
threat hunting

Management · APIs · Connectors

plain concepts



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

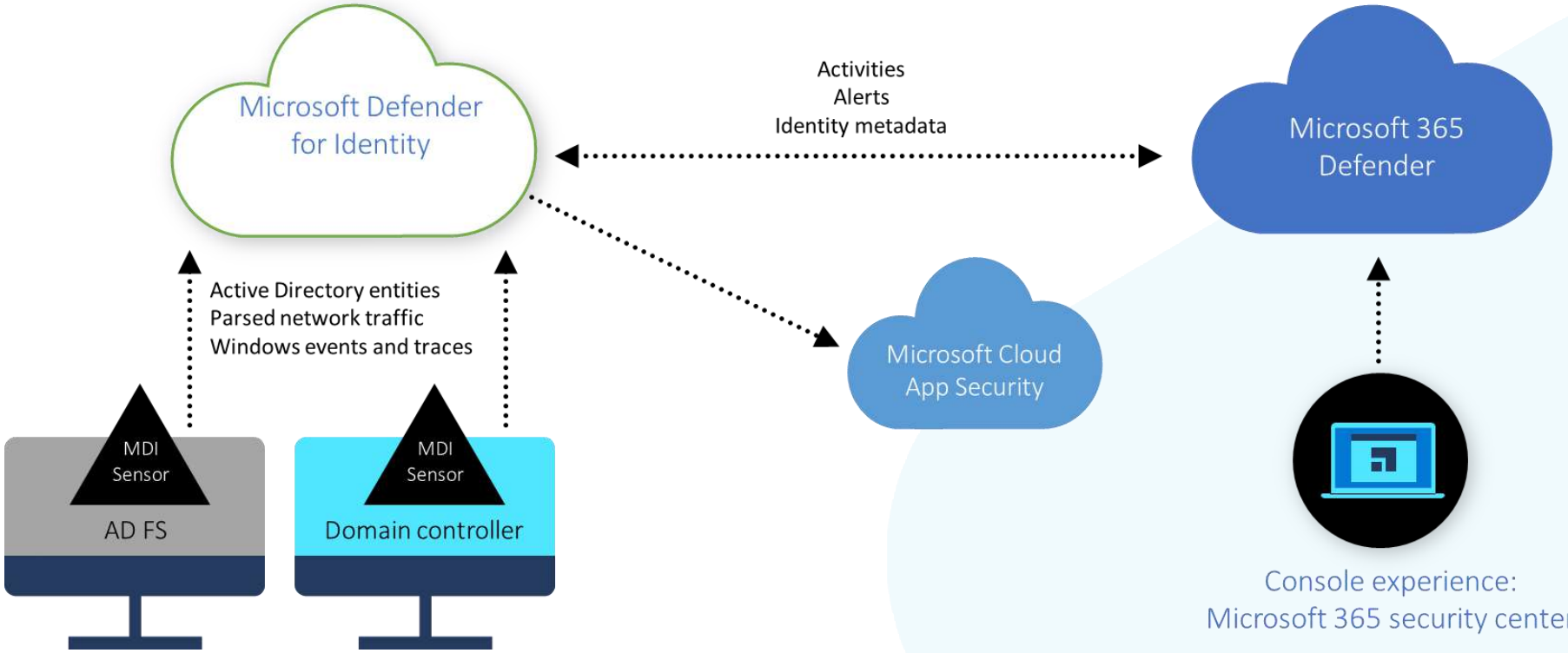
My organization's overall security state

What's the next highest priority SOC work item

SaaS Level Up

Microsoft Defender for Identity architecture

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



plain concepts

Microsoft Defender for Identity

SaaS Level Up

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

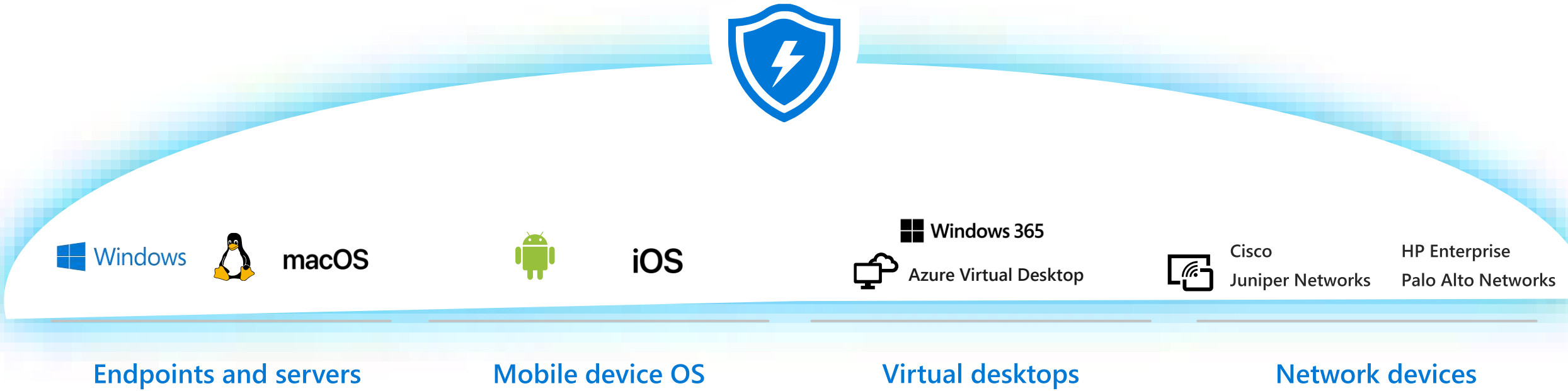
Cloud scale, continuous updates

plain concepts

SaaS Level Up

Microsoft Defender for Endpoint

Delivering endpoint security across platforms

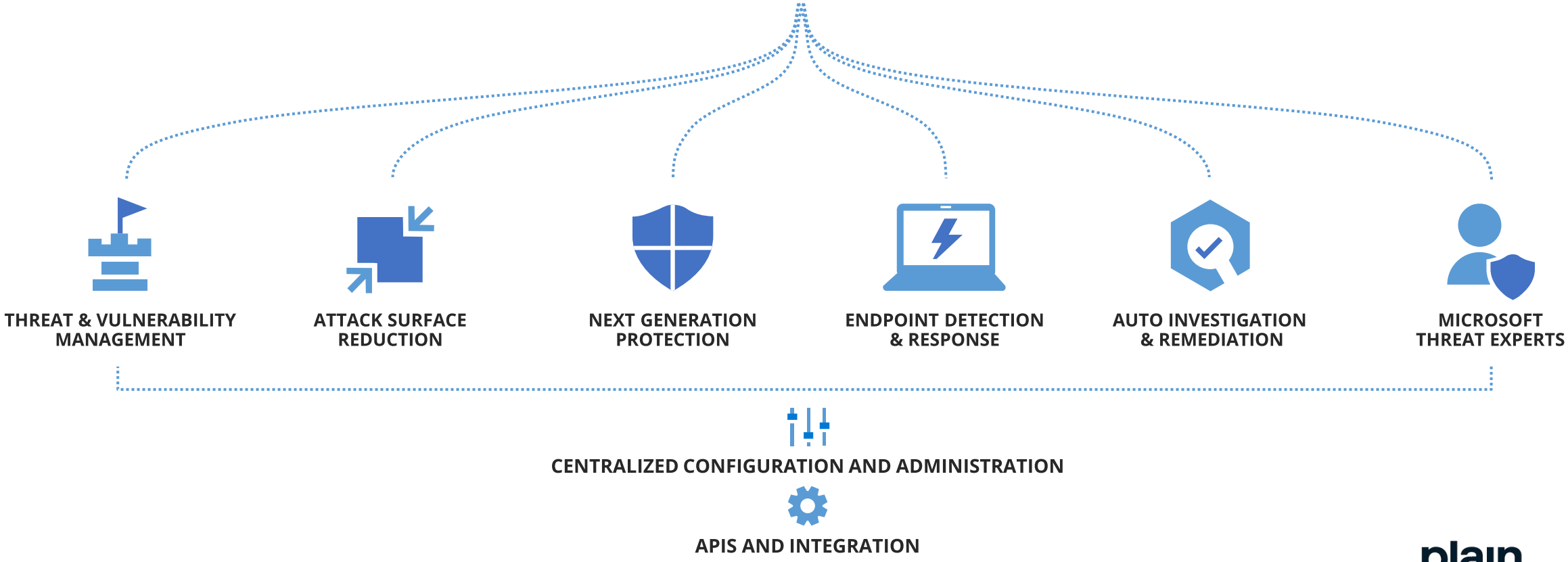


plain concepts

Microsoft Defender for Endpoint

SaaS Level Up

Threats are no match.

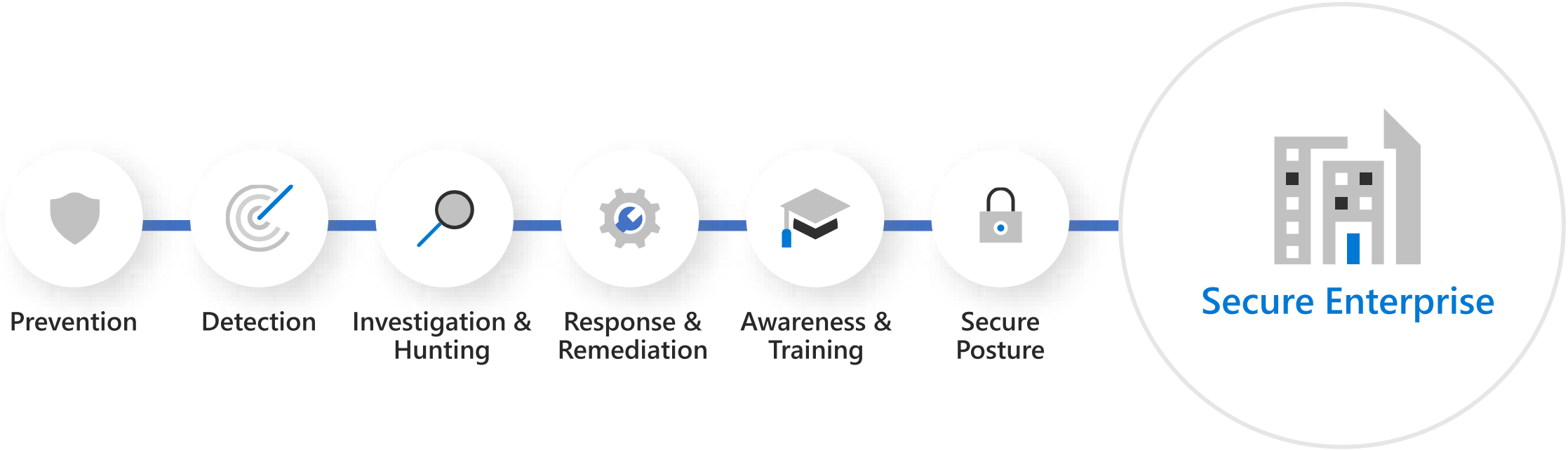


plain concepts

SaaS Level Up

Microsoft Defender for Office 365

Securing your enterprise requires more than just prevention

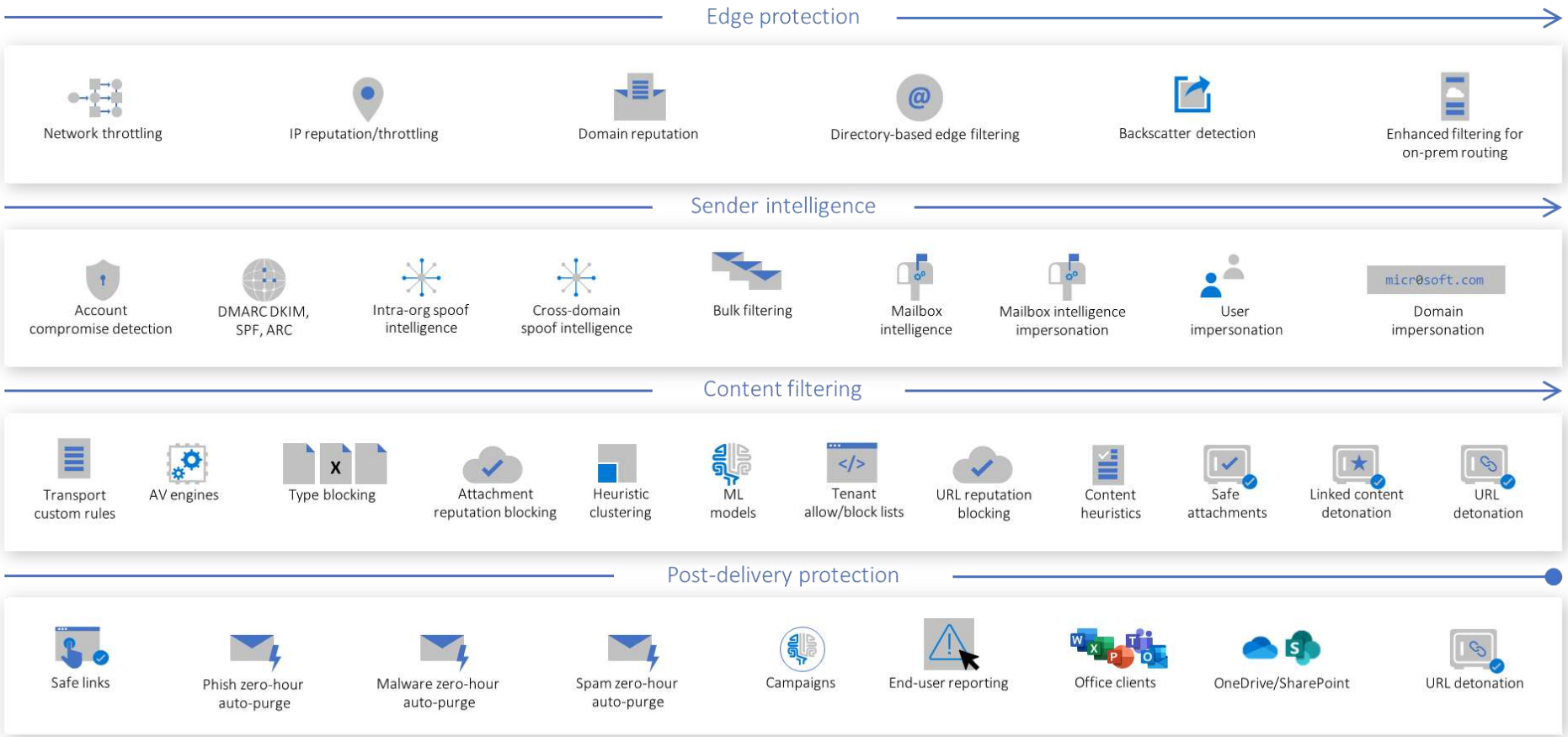


plain concepts

SaaS Level Up

Microsoft Defender for Office 365

Multi-Layered protection stack



plain concepts

SaaS Level Up

Microsoft Cloud Apps Security

Eduardo Recio
SaaS Level Up Cloud Engineer

plain concepts

SaaS Level Up

¿Qué es un Cloud App Security Broker?

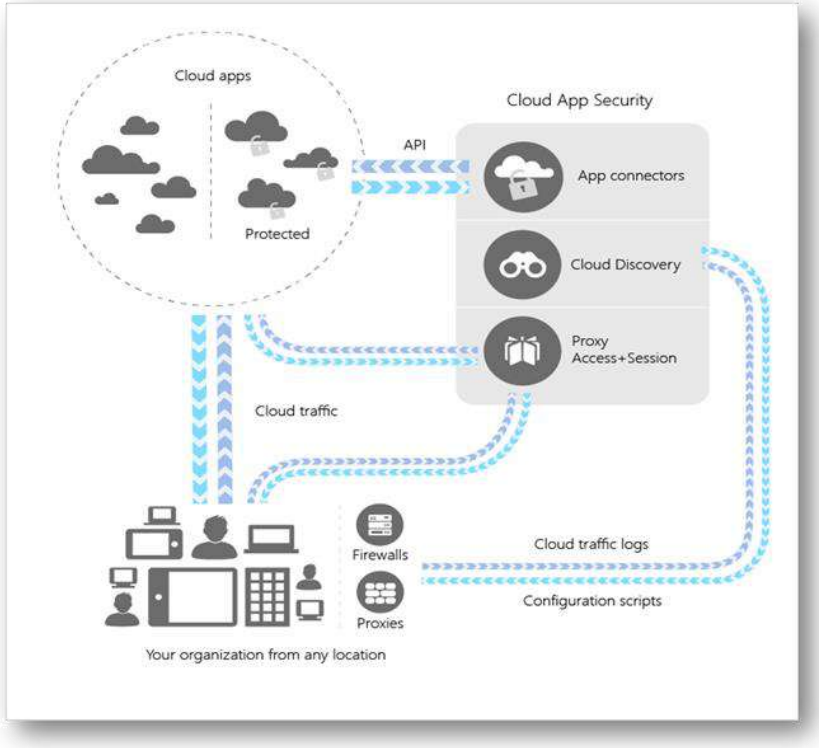
Agente que se sitúa entre los usuarios y las aplicaciones en la nube, y supervisa toda la actividad y aplica las políticas de seguridad.

Acceso y gestión de la identidad

Protección contra amenazas

Administración de la seguridad

Protección de la información



plain concepts

SaaS Level Up

Microsoft Cloud Apps Security

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

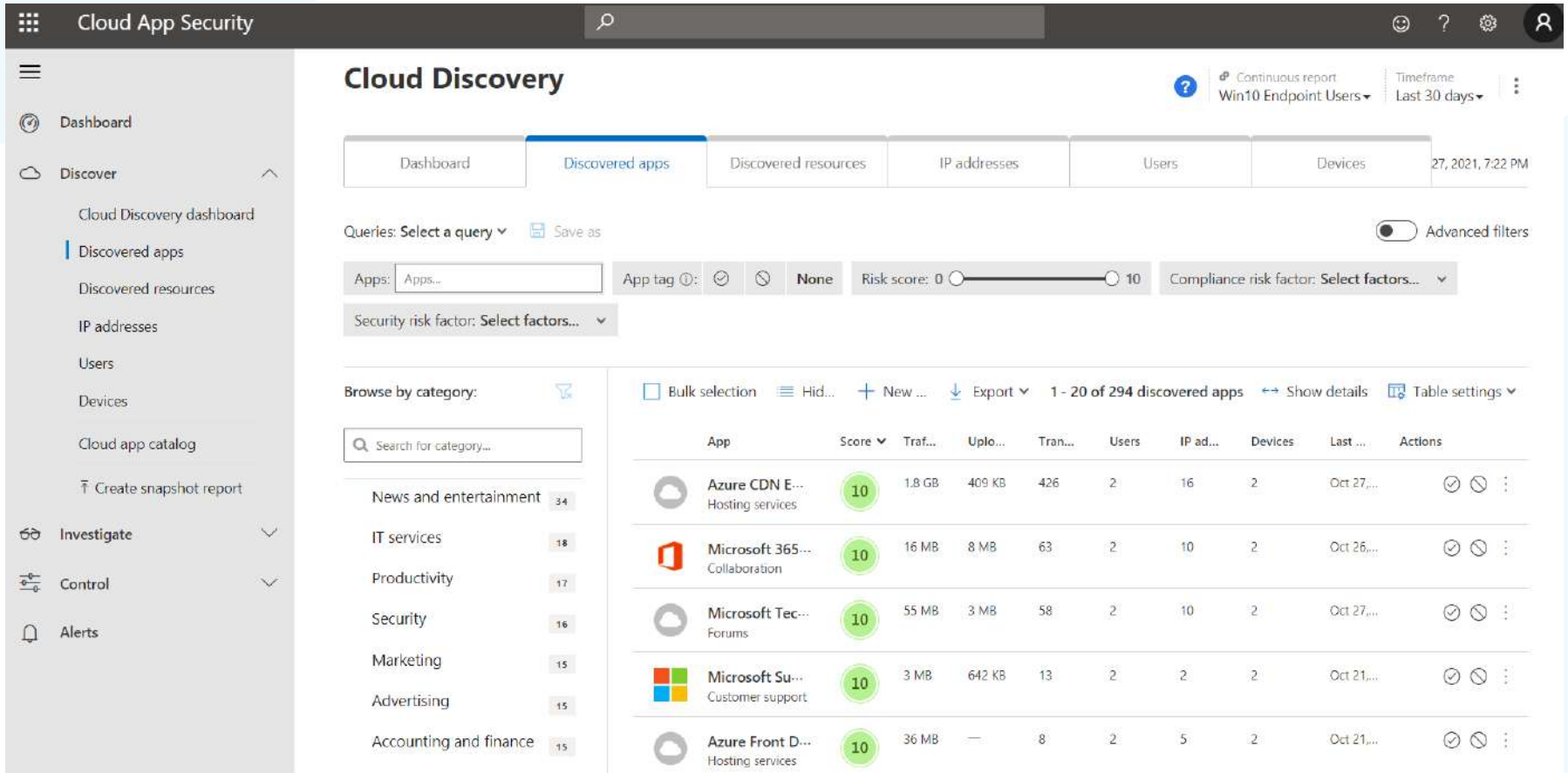
Top casos de uso

- 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

plain concepts

SaaS Level Up

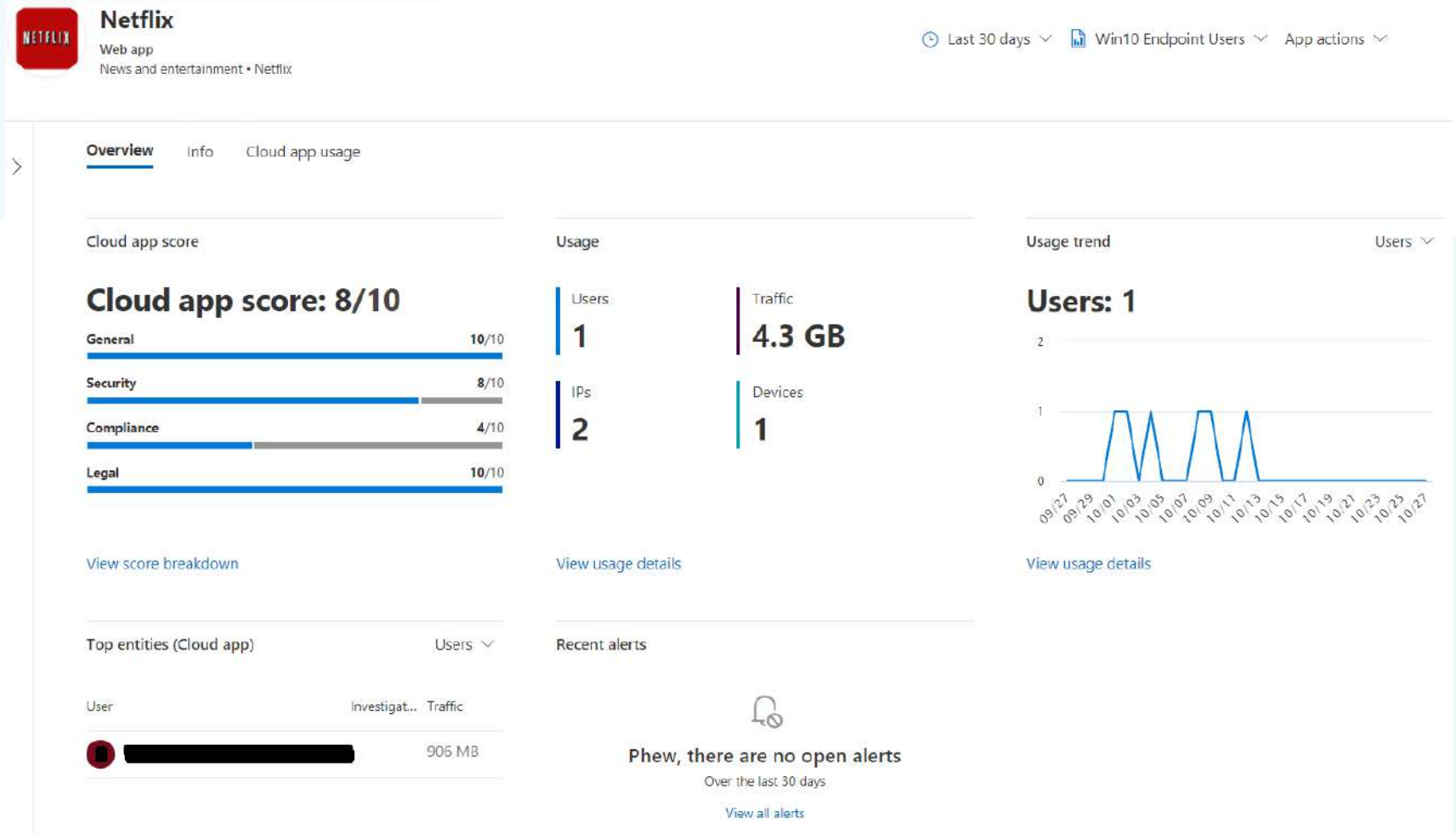
Descubrir y gobernar apps



plain concepts

SaaS Level Up

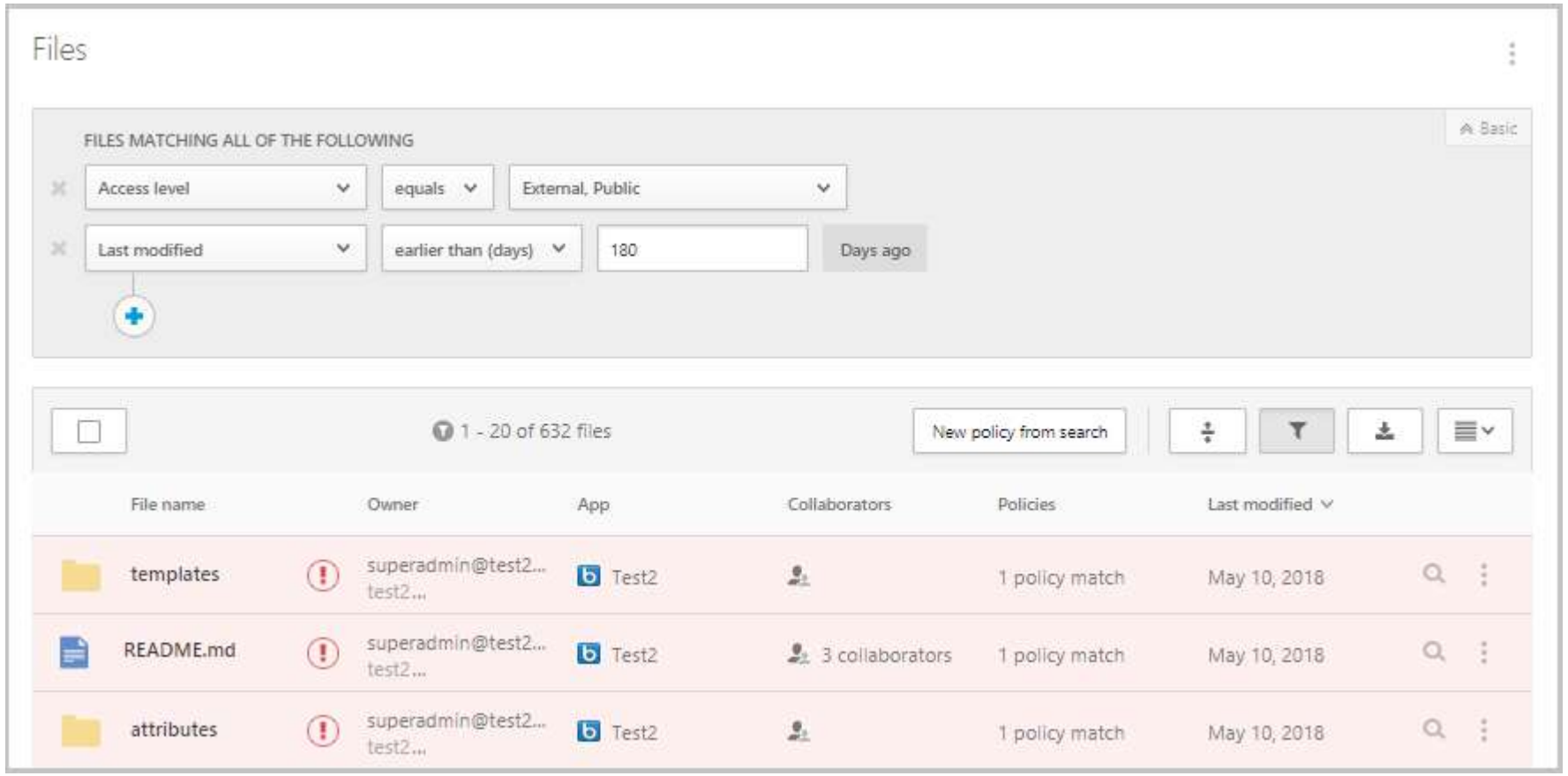
Descubrir y gobernar apps



plain concepts

SaaS Level Up

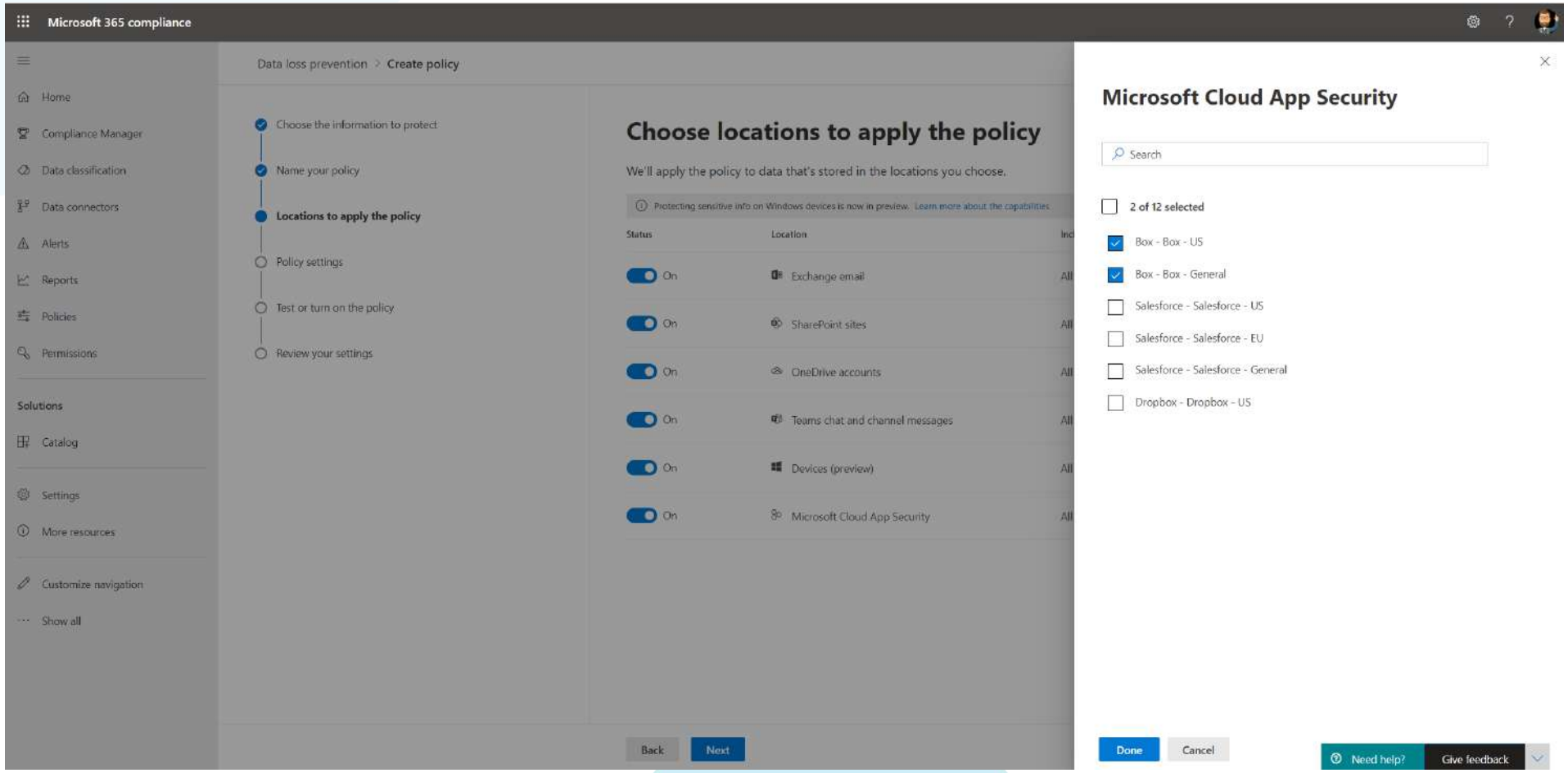
Detectar filtración y tener visibilidad de los datos corporativos



plain concepts

SaaS Level Up

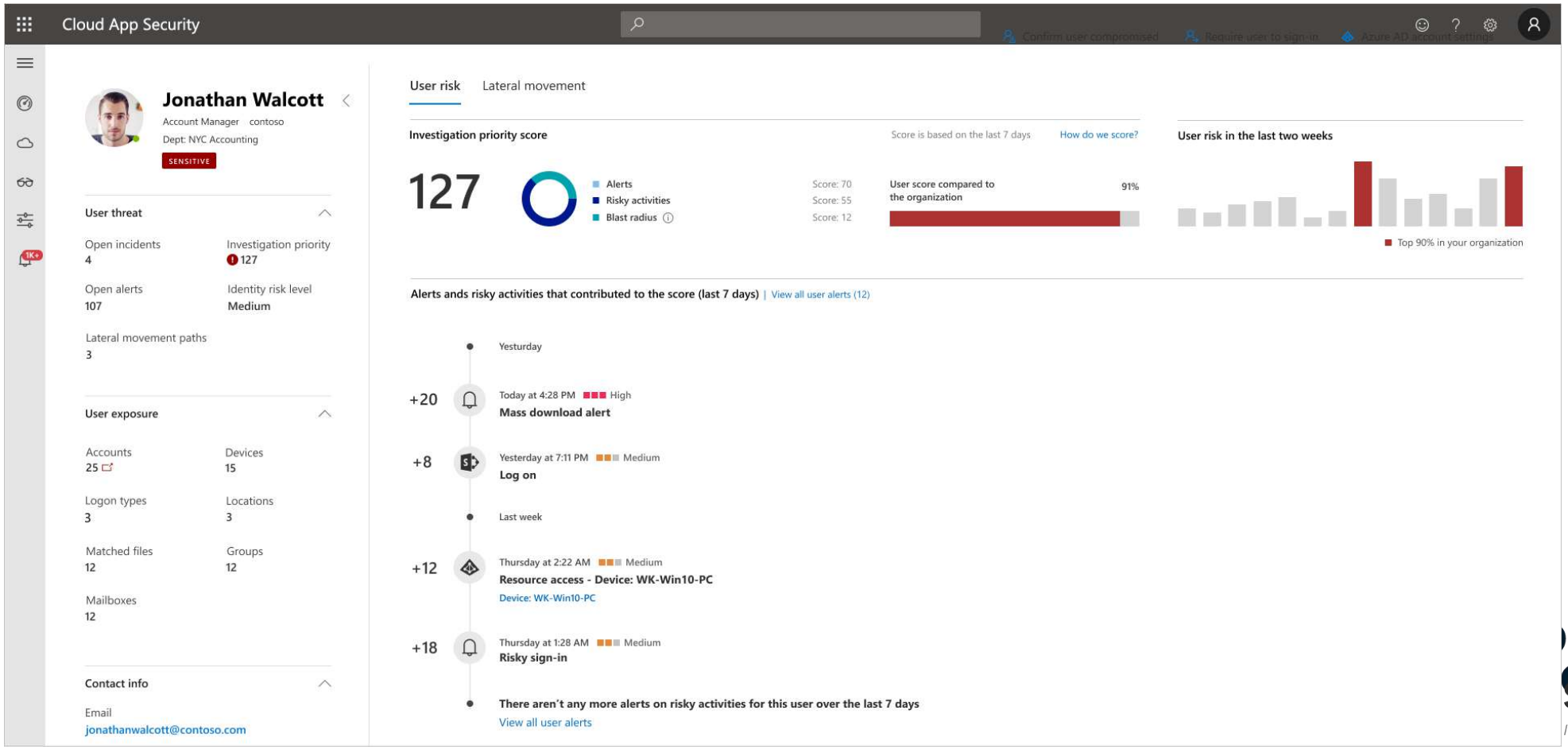
Aplicar políticas DLP, incluso en corporativos no gestionados



plain concepts

SaaS Level Up

Identificar cuentas de usuario comprometidas



SaaS Level Up

Barracuda Sentinel

Protección avanzada contra amenazas

plain concepts

Barracuda & the Public Cloud

Miguel López
Country Manager – Iberia
mlopez@barracuda.com

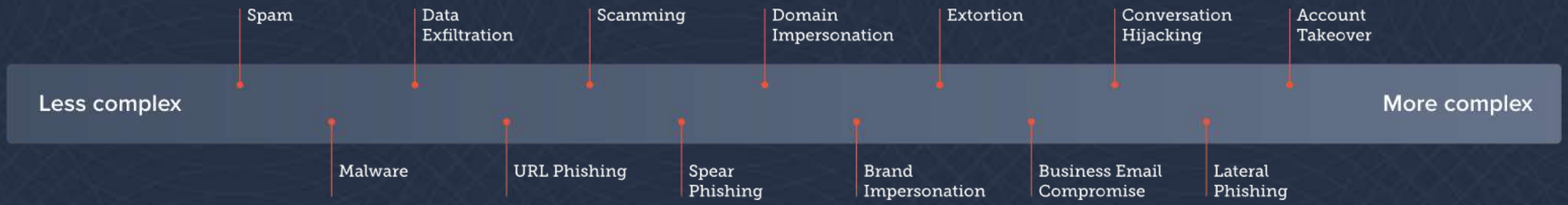
Barracuda
Your journey, secured.

Comprehensive email protection

Gateway Defense and Resiliency	API-Based Inbox Defense	Security Awareness	Incident Response
Cloud Backup and Archiving	AI for Social Engineering	Phishing Simulation	Automation
Email Continuity	Brand Protection DMARC Reporting	User Awareness Training	Post Delivery Remediation
Encryption and DLP	Account Takeover	Automated Reporting	Threat Hunting
In/Outbound Security			

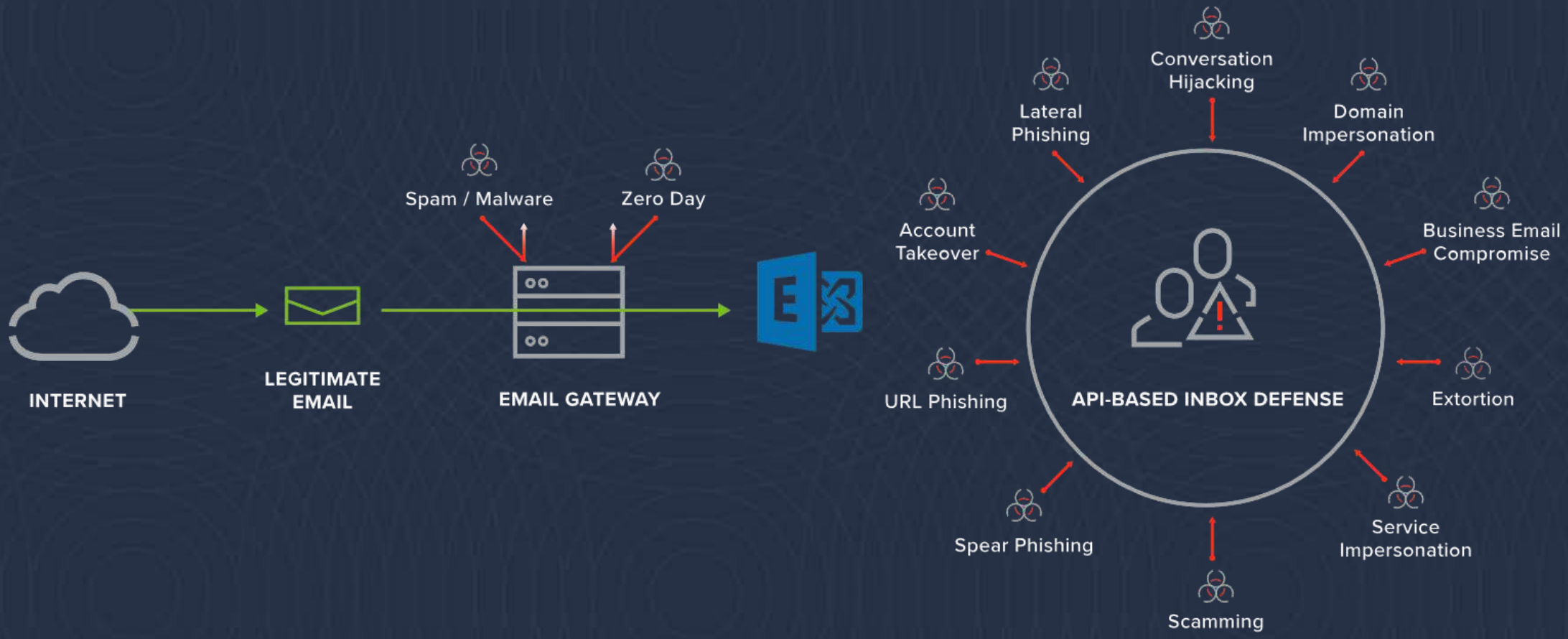
Barracuda
Total Email Protection™

Email attacks are evolving

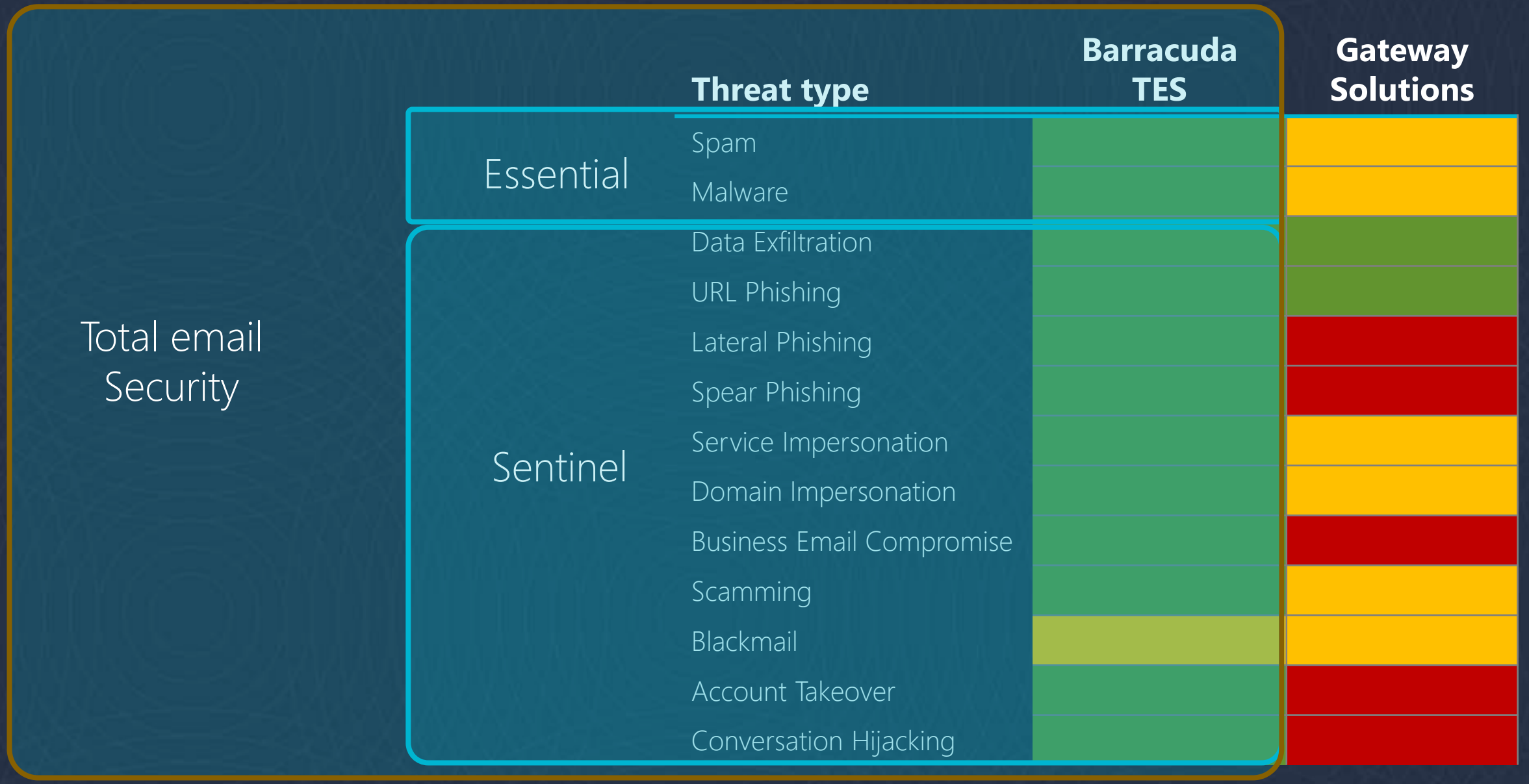


https://www.barracuda.com/13-threats-report

Email security – two forms of prevention



The 13 Known Threat Types

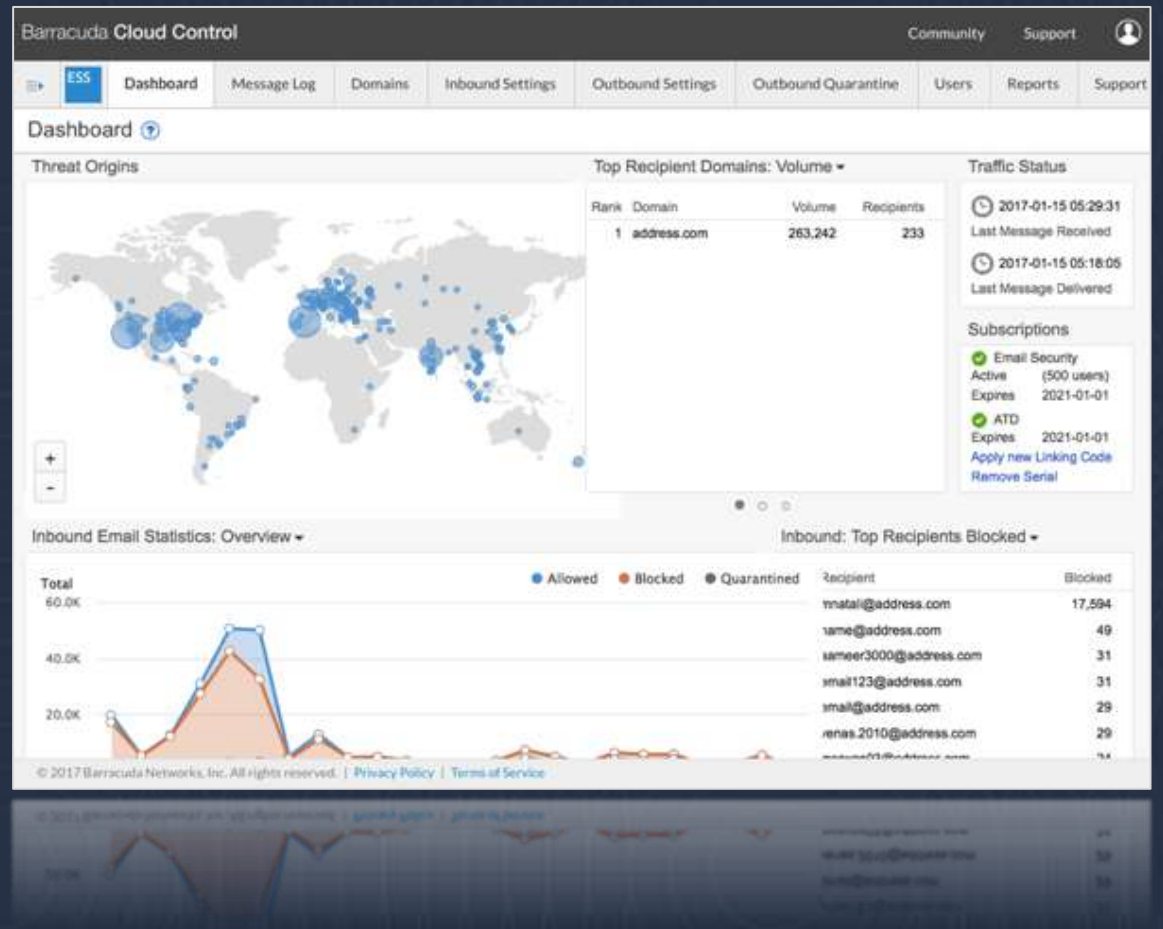


Complete Protection for Office 365

Barracuda
Essentials
for Microsoft 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



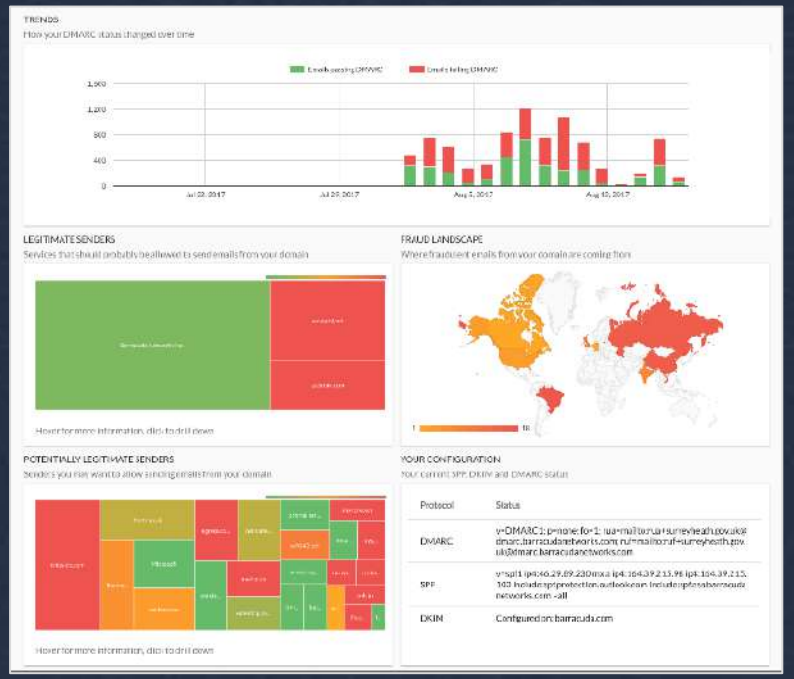
Barracuda Sentinel for O365

Barracuda
Essentials
for Microsoft Office 365

AI for Real-Time Spear Phishing & Cyber Fraud Defense for Office 365

- Learns each organization's unique communications patterns & Identifies anomalous signals in message metadata and content
- Quarantines spear phishing attacks in real time
- Protects from domain spoofing and brand hijacking. Helps easily set up DMARC authentication
- Provides visibility and analysis of DMARC reports. Utilizes AI to identify high-risk individuals

Detail	Phishing	Spear Phishing
Contains a link(s) to a malicious site	✓	✗
Sent to many people	✓	✗
Personalized	✗	✓
Primary goal	Steal credentials	Wire transfer, SSNs
Barracuda Product	Barracuda Essentials	Barracuda Sentinel

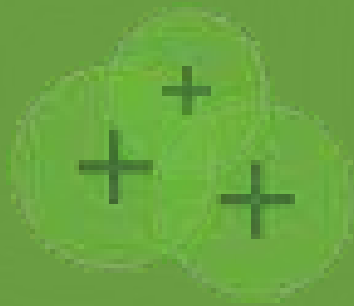


Sentinel: Fraud prevention and inbox defense

AI

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

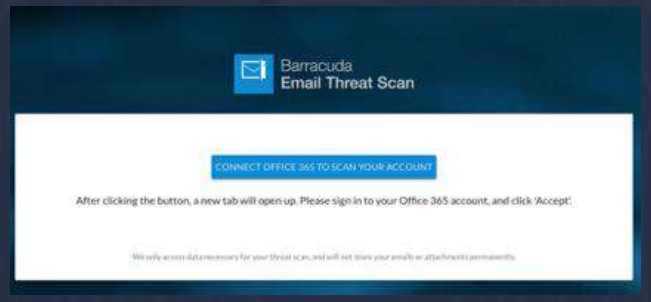
Barracuda Email Threat Scanner

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

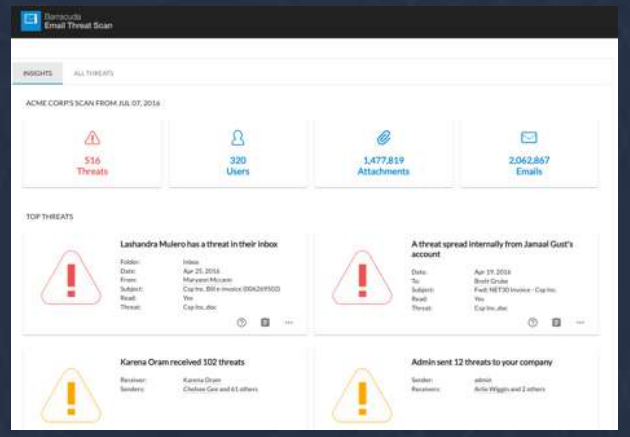
1) Scan

Send customer link to scan.barracuda.com/signup



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

Alberto Gonzalez
CTO, ArexData

Alberto Gónzalez
CTO, Arexdata

www.arexdata.com

Auditoría de Datos

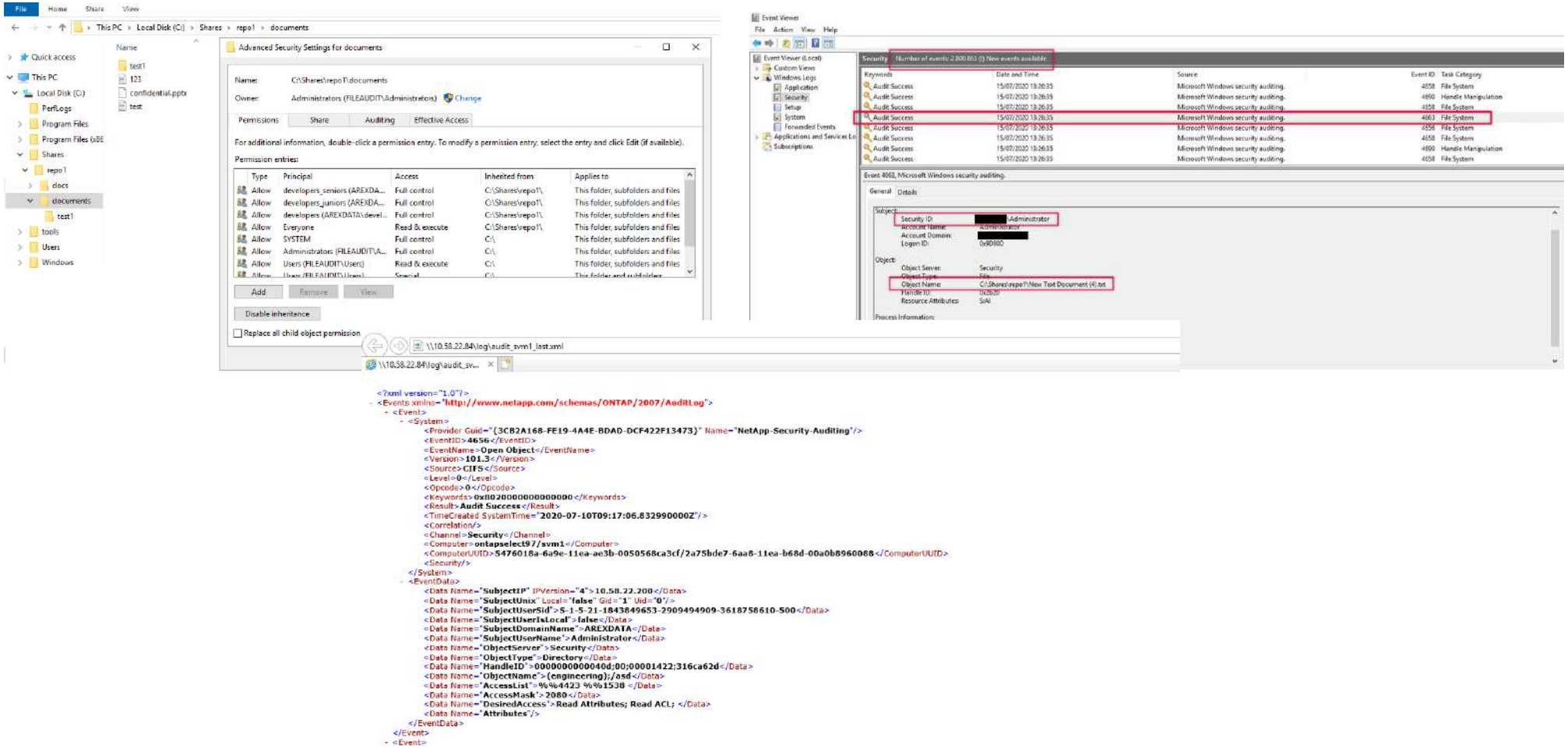
El problema: ¿dónde están mis datos?

El activo más importante de tu compañía es tus datos... pero están desperdigados en multiples 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



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 ultimo más? ¿Y para qué?

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

¿Que datos y accesos hay en mis carpetas publicas?

¿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

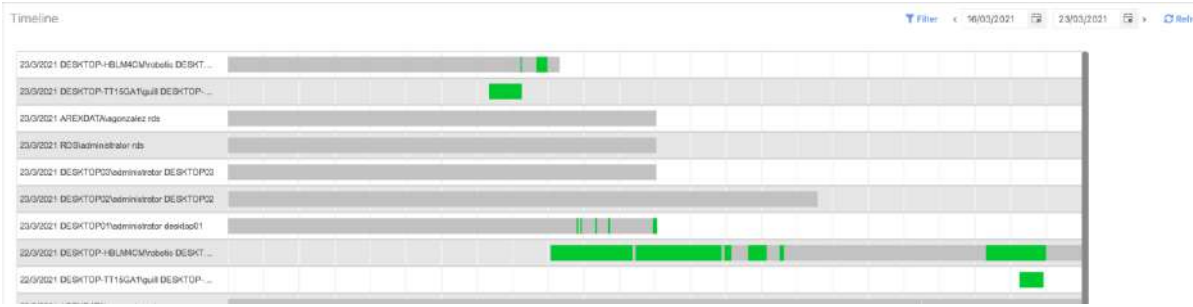
controla los datos que residen en las estaciones de trabajo de los usuarios

AREXDATA
PROTECT YOUR MOST VALUABLE ASSET - YOUR DATA

Arexdata Data Security Platform

Endpoint Audit | Enterprise Audit | Enterprise Management | Data Classification

- 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, copiados de discos, muchas impresiones, etc…Reaccionar ante ellas a través de la ejecución automática de de los scripts que defina el cliente



Enterprise Audit

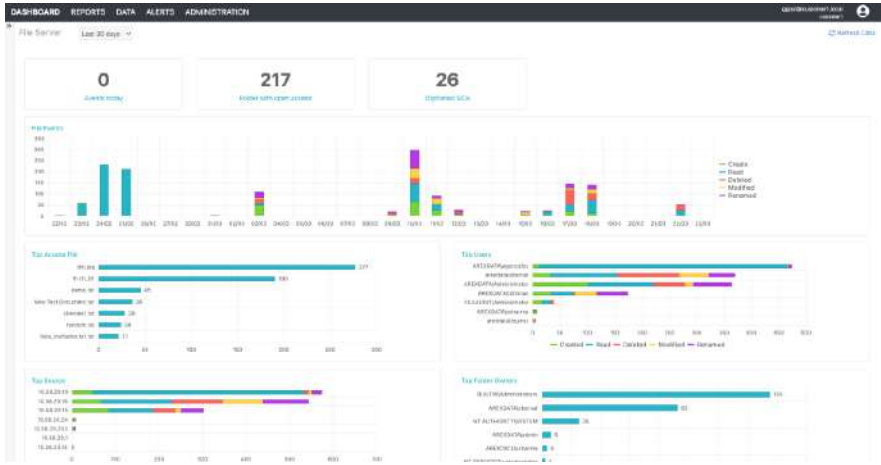
protege los datos en repositorios centrales, almacenamiento, y cloud

AREXDATA
PROTECT YOUR MOST VALUABLE ASSET - YOUR DATA

Arexdata Data Security Platform

Endpoint Audit | **Enterprise Audit** | Enterprise Management | Data Classification

- 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…



77

1. *Otras marcas y tecnologias en roadmap*

Enterprise Management

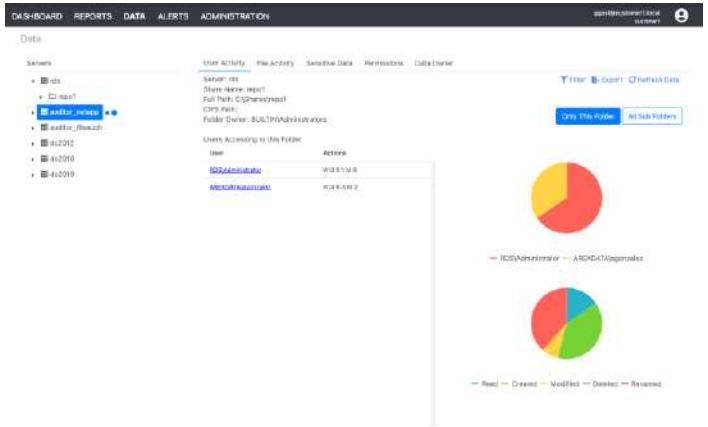
delegar la protección de datos en los responsables de departamento u otros expertos

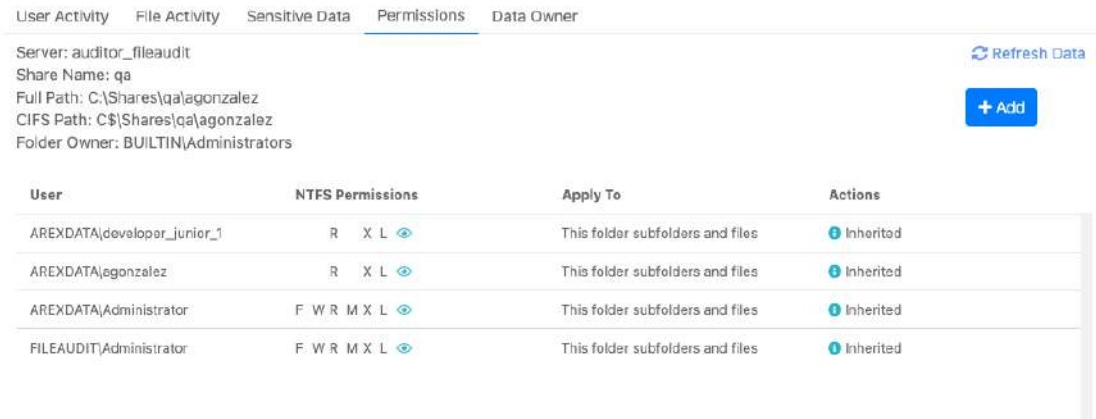
AREXDATA
PROTECT YOUR MOST VALUABLE ASSET - YOUR DATA

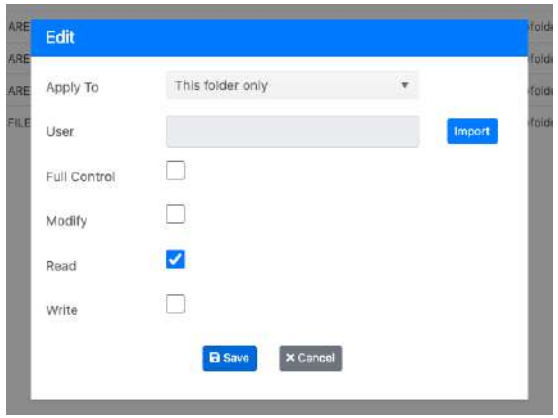
Arexdata Data Security Platform

Endpoint Audit | Enterprise Audit | Enterprise Management | Data Classification

- Aproveche el conocimiento que sus **responsables de lineas 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**







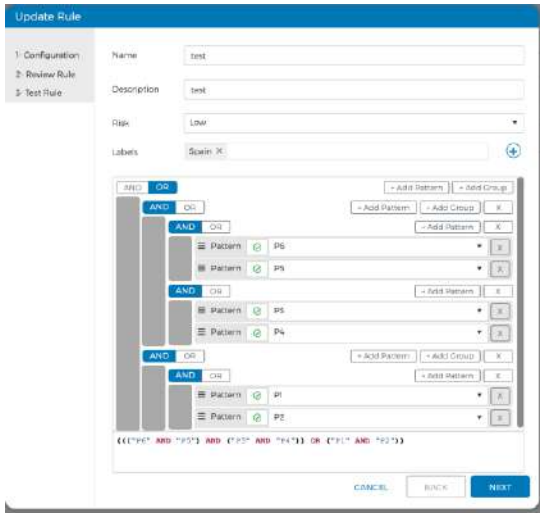
Data Classification

encontrar y controlar la información sensible existente dentro de sus ficheros

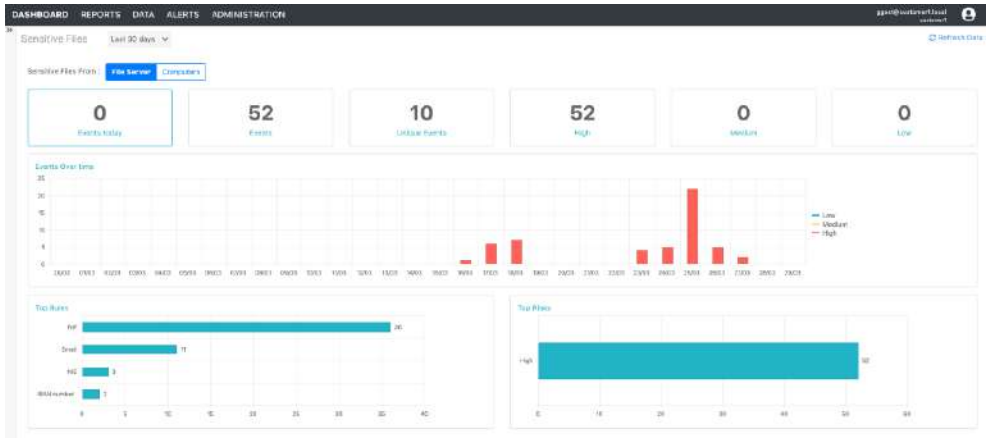
AREXDATA
PROTECT YOUR MOST VALUABLE ASSET - YOUR DATA

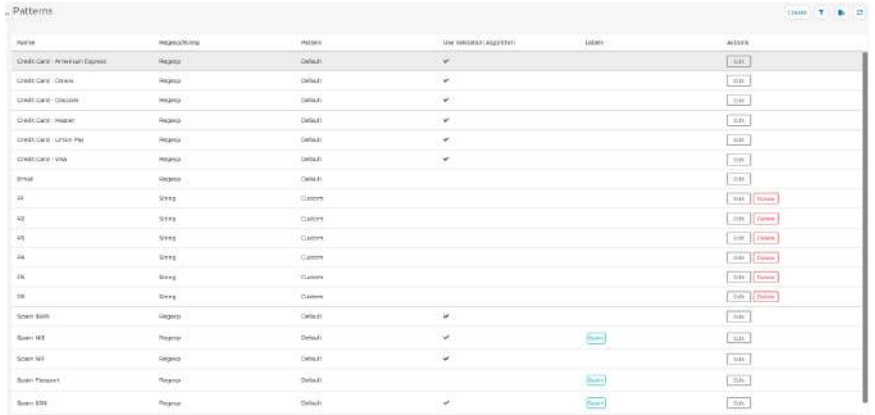
Arexdata Data Security Platform

Endpoint Audit | Enterprise Audit | Enterprise Management | Data Classification



- **Detectar información sensible** (DNI, Seguridad Social, tarjetas de crédito, etc…) o **información clasificada** en todos sus tipos de ficheros, incluyendo imágenes
- Añade fácilmente **nuevos patrones a detectar**, por ejemplo tus códigos de facturas, o los nombres internos de proyectos críticos. Refínelos con términos de proximidad y listas de términos a excluir
- **Combina** los patrones usando **operaciones lógicas** construyendo reglas para detectar situaciones o términos específicos
- **Monitoriza las actividades** en ficheros con datos sensibles, encuentra **quien accede** a ellos, revisa sus permisos. Todo ello desde una vista única
- **Controlar donde residen** estos ficheros sensibles, incluso en estaciones de trabajo de los usuarios





SaaS Level Up

Demo ArexData

plain concepts

SaaS Level Up

Questions?

plain concepts


plain
concepts
SaaS Level Up