Microsoft Cloud Security Broker

Seguridad a nivel empresarial para *Cloud Apps*

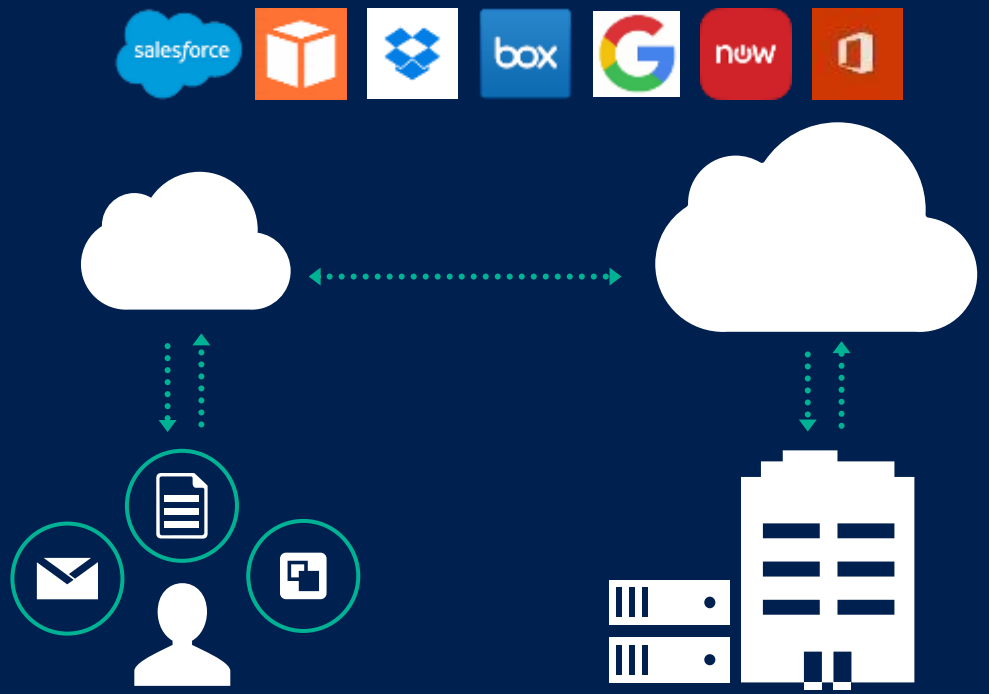
Agustín Santamaría –
asantama@microsoft.com
Azure & Security Solutions Specialist

¿Qué está dirigiendo este cambio?

LA VIDA **ANTES DEL CLOUD**

- Sólo son instaladas aplicaciones autorizadas
- Se acceden a los recursos a través de las redes/dispositivos gestionados
- Se disponen de las capas para la protección de las aplicaciones internas
- TI tiene un perímetro de seguridad conocido

LA VIDA **CON EL CLOUD**



- Los usuarios eligen sus aplicaciones (no autorizadas – *shadow IT*)
- Los usuarios pueden accede a los recursos desde cualquier lugar
- Los datos se comparten por los usuarios y las *cloud apps*
- TI tiene visibilidad y protección limitada

¿Qué está dirigiendo este cambio?

73%

de las organizaciones indican que la seguridad es el primer reto para la adopción de SaaS apps*

80%

>80% de los empleados admiten que utilizan en su trabajo SaaS apps no aprobadas **

- Cloud Security Alliance (CSA) survey, Cloud Adoption, Practices and Priorities Survey Report

** http://www.computing.co.uk/ctg/news/2321750/more-than-80-per-cent-of-employees-use-non-approved-saas-apps-report

Cuestiones a las que se deben dar respuesta

CONTROL DE ACCESO

¿Cómo aseguro acceso apropiado a mis *Cloud apps*?

SHADOW IT

¿Cómo sé que apps se están utilizando en mi entorno?

PREVENCIÓN DE AMENAZAS

¿Cómo sé si mis usuarios han sido "infectados"?

PROTECCIÓN DE DATOS

¿Cómo prevengo la fuga de información?

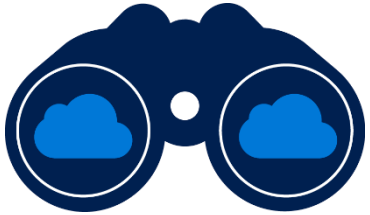
VISIBILIDAD/INFORMES

¿Cómo obtengo visibilidad sobre la utilización de *Cloud apps*?

CUMPLIMIENTO

¿Cómo puedo cumplir con las exigencias regulatorias?

Microsoft Cloud Security Broker



Descubrimiento

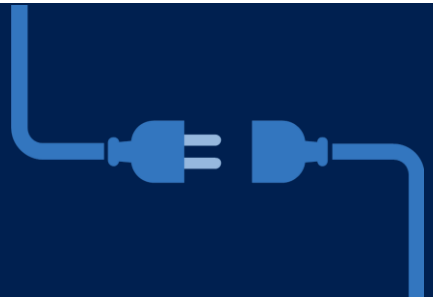
Visibilidad completa y contexto de uso del cloud y *Shadow IT*

Control de los Datos

Adapta tu entorno de *cloud* con políticas y controles de acceso, compartición de datos y DLP

Protección Amenazas

Identificación de los riesgos de uso, incidentes de seguridad, comportamientos anómalos de los usuarios y prevención de amenazas



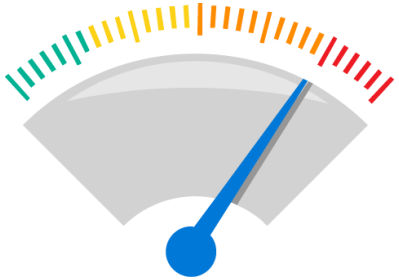
Integrado con las soluciones de seguridad, movilidad y cifrado

Descubrimiento

Descubrimiento *Shadow IT*

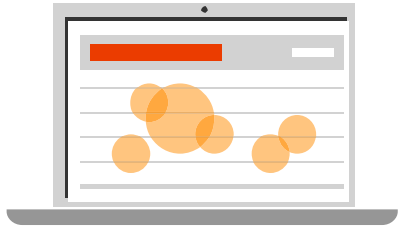
- Descubrir 13,000+ cloud apps en uso — no requiere agentes
- Identificar todos los usuarios, direcciones ip, top apps, tops users

Scoring del riesgo



- *Score* automatic basado en más de 60+ parameters
- Analiza el Riesgo de cada aplicación basado en sus mecanismos de seguridad y cumplimiento de regulaciones

Análisis *Ongoing*



- Detección del Riesgo *ongoing, informes, análisis de los usuarios, patrones de comportamiento y uso, tráfico de subida/bajada y transacciones.*
- Detección *Ongoing* de aplicaciones discovered apps

Integrado con las soluciones de seguridad, Movilidad y cifrado

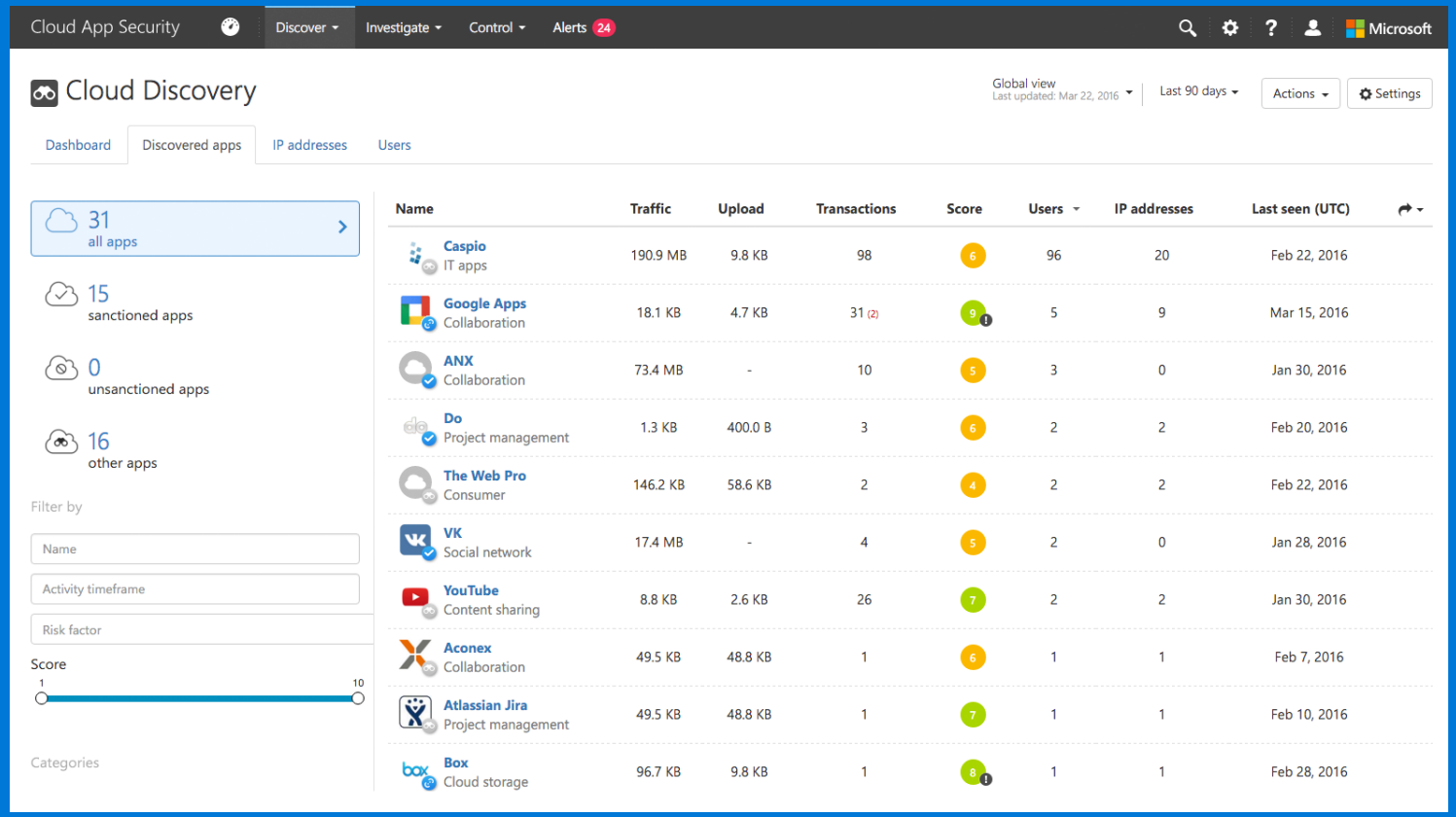
Descubrimiento

Discover

Investigate

Control

Alerts



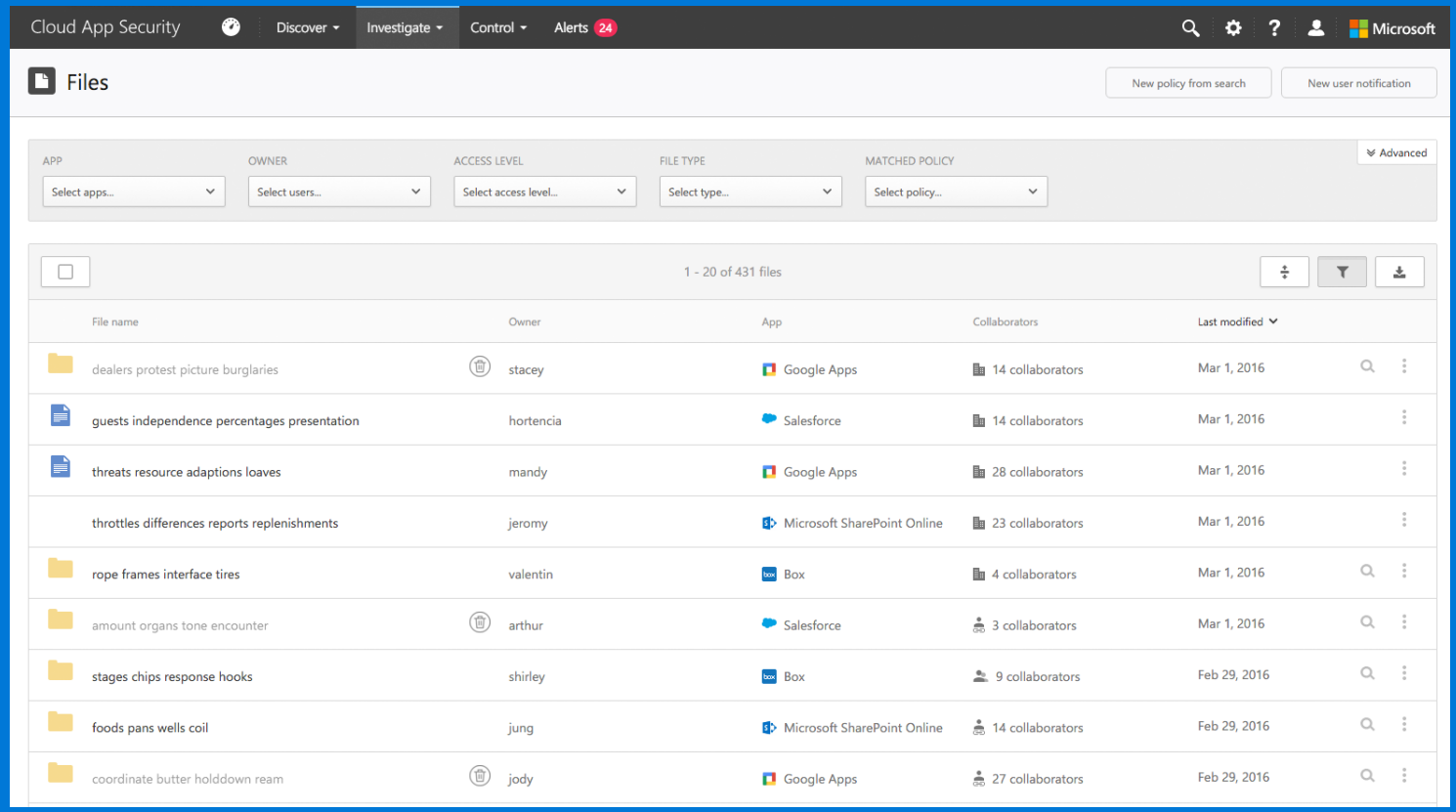
Investigación

Discover

Investigate

Control

Alerts



Control de los datos

Definición Políticas

- Políticas granulares de seguridad para las aplicaciones aprobadas
- Utilización de políticas *out-of-the-box* o personalizadas

DLP y compartición de datos

- DLP *inlines* y *at rest*
- Gobierno de los datos en cloud: ficheros en unidades de *cloud,* attachments o en *cloud apps.*
- Utilización de plantillas predefinidas o extension de políticas DLP existentes.

Forzado de políticas

- Identificación de violación de políticas – usuarios, ficheros, nivel de actividad
- Forzar acciones: cuarentena y eliminación de permisos
- Bloquear transacciones sensibles, limitar sesiones para dispositivos no gestionados

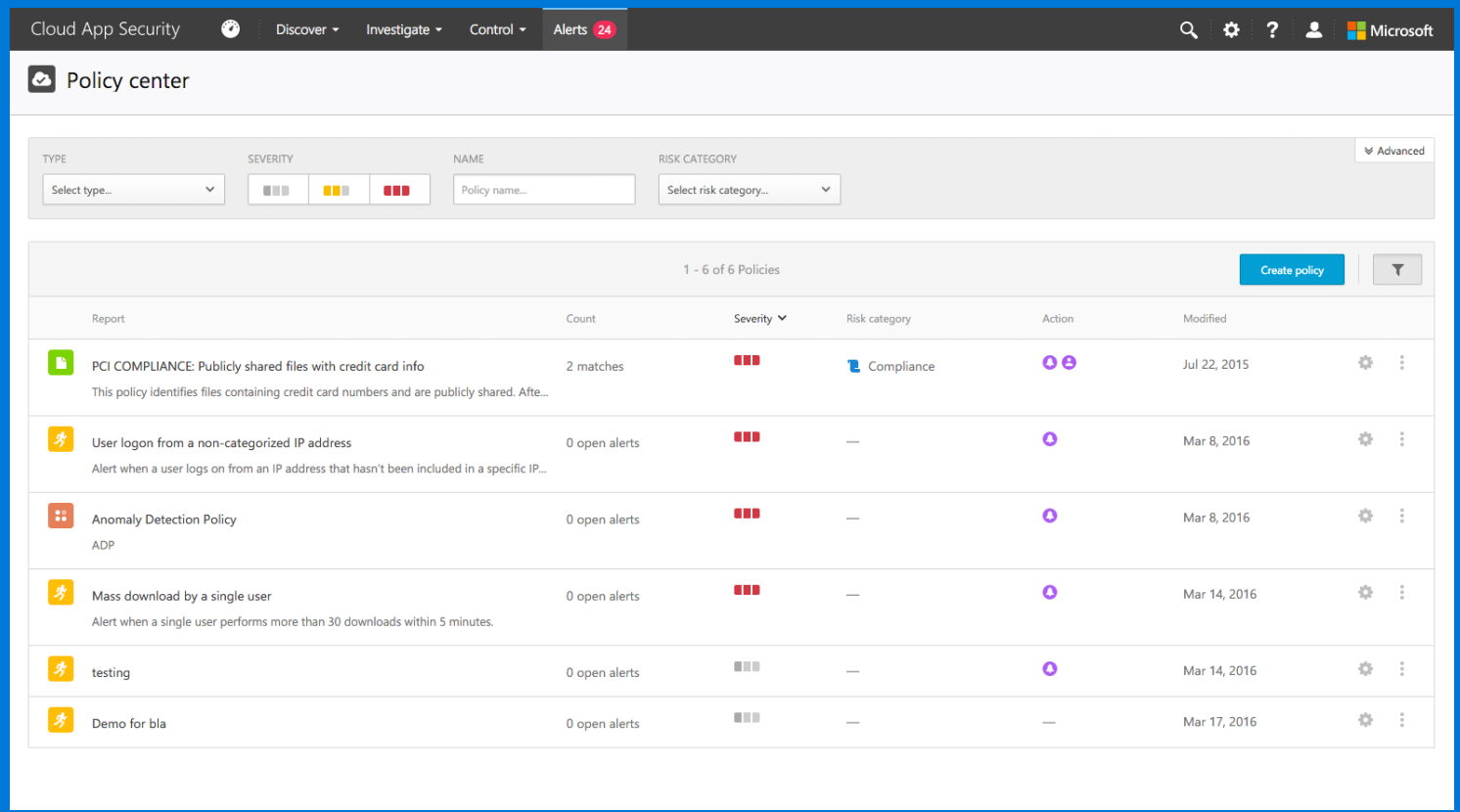
Control

Discover

Investigate

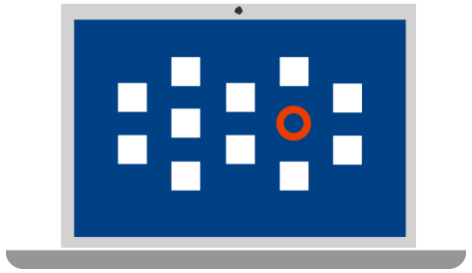
Control

Alerts



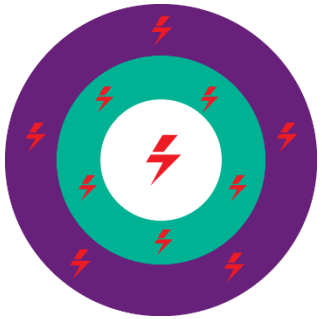
Protección de Amenazas

Behavioral analytics



- Identificación de anomalías en el entorno de *cloud* que podrían ser indicativo de una posible brecha
- *Behavioral analytics* que determina el Riesgo de cada transacción

Attack detection



- Identificar patrones de ataque de origen para mejorar la prevención frente amenazas utilizando la ingente información de cyber-inteligencia de Microsoft
- Análisis en tiempo real de envio de ficheros frente a *malwares*

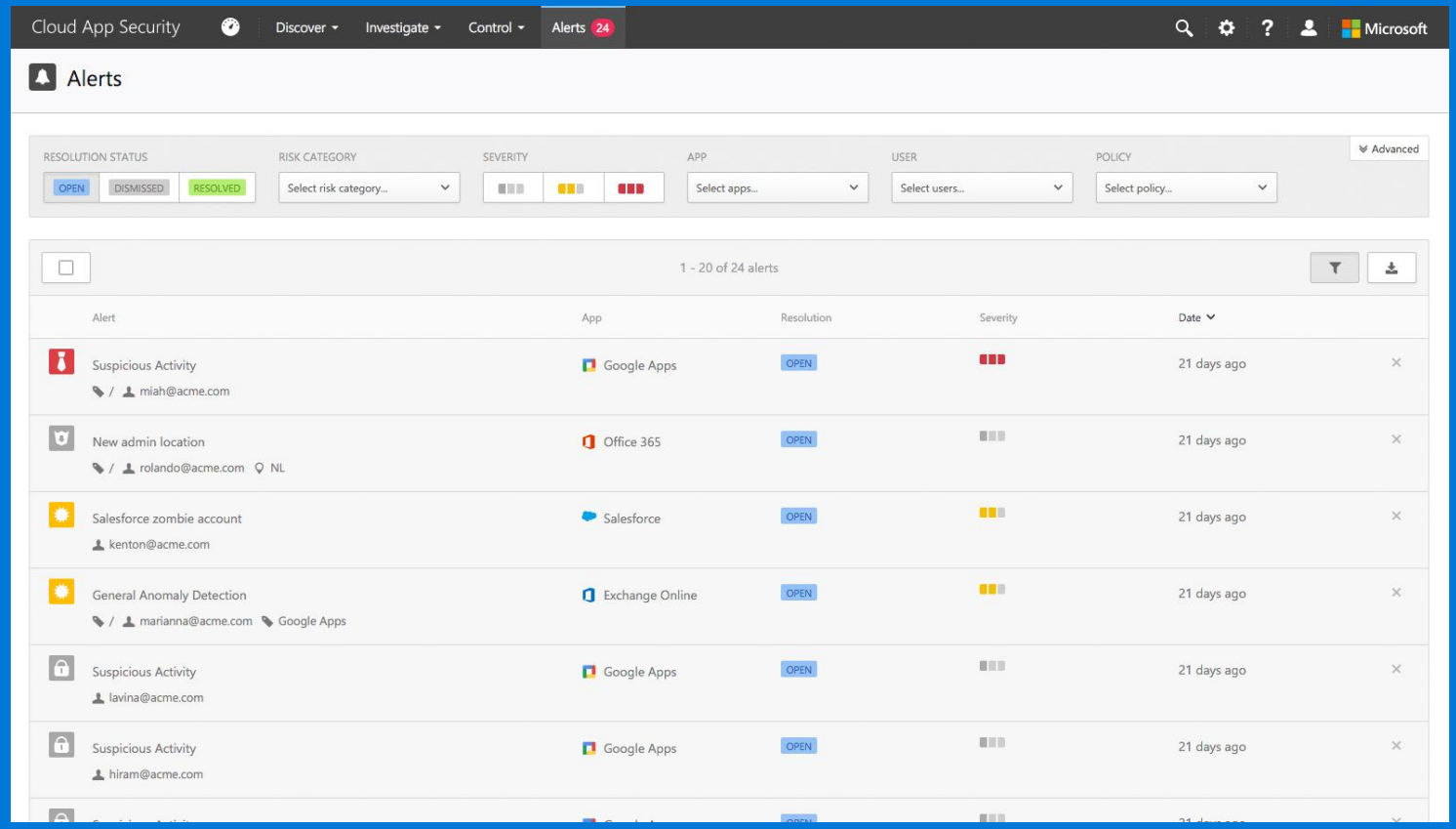
Protección de Amenazas

Discover

Investigate

Control

Alerts



Integración probada para las Top SaaS apps

¿Quién lo está utilizando?

Gracias
Q&A

asantama@microsoft.com