



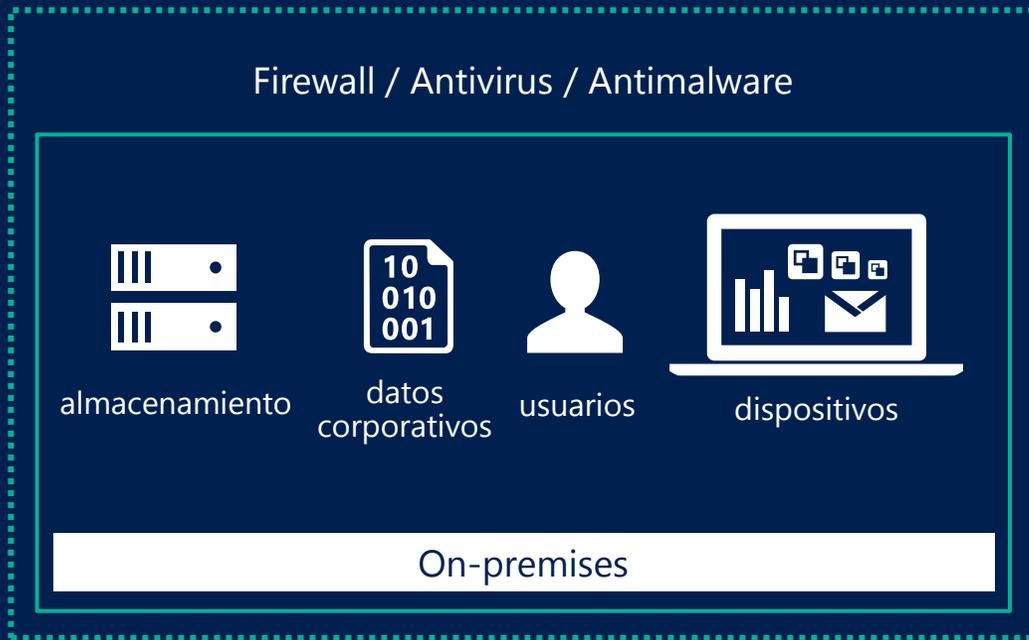
Microsoft Cloud Security Broker

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 acceder a los recursos desde cualquier lugar
- Los datos se comparten por los usuarios y las *cloud apps*
- TI tiene visibilidad y protección limitada

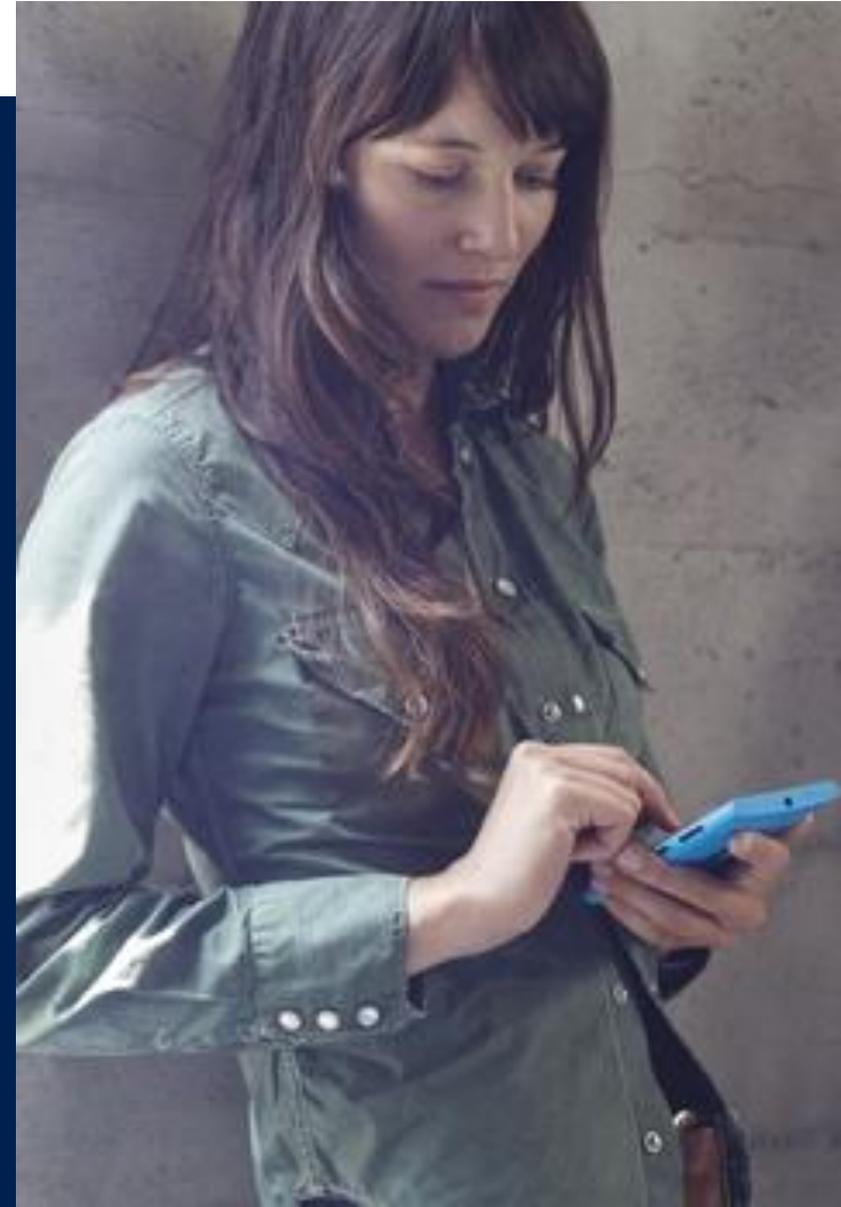
¿Qué está dirigiendo este cambio?

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 **



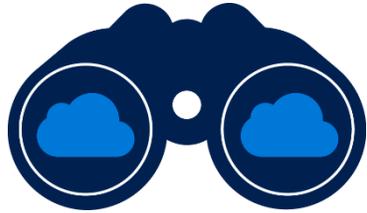
* Cloud Security Alliance (CSA) survey, Cloud Adoption, Practices and Priorities Survey Report

** <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



Microsoft Cloud Security Broker



Descubrimient



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



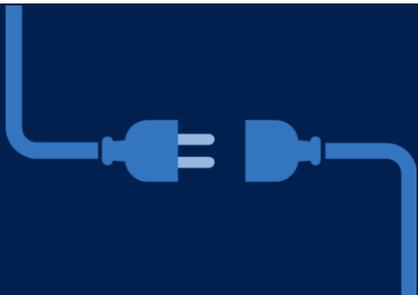
Control de los Datos

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



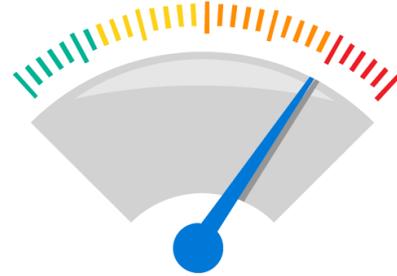
Descubrimiento

Descubrimiento *Shadow IT*



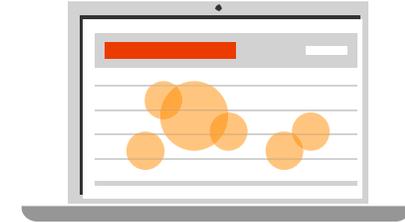
- Descubrir 13,000+ cloud apps en uso — no requiere agentes
- Identificar todos los usuarios, direcciones ip, top apps, tops users

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

Cloud App Security | Discover | Investigate | Control | Alerts **24** | Microsoft

Cloud Discovery | Global view | Last updated: Mar 22, 2016 | Last 90 days | Actions | Settings

Dashboard | Discovered apps | IP addresses | Users

31 all apps

15 sanctioned apps

0 unsanctioned apps

16 other apps

Filter by

Name

Activity timeframe

Risk factor

Score

Categories

Name	Traffic	Upload	Transactions	Score	Users	IP addresses	Last seen (UTC)
Caspio IT apps	190.9 MB	9.8 KB	98	6	96	20	Feb 22, 2016
Google Apps Collaboration	18.1 KB	4.7 KB	31 (2)	9	5	9	Mar 15, 2016
ANX Collaboration	73.4 MB	-	10	5	3	0	Jan 30, 2016
Do Project management	1.3 KB	400.0 B	3	6	2	2	Feb 20, 2016
The Web Pro Consumer	146.2 KB	58.6 KB	2	4	2	2	Feb 22, 2016
VK Social network	17.4 MB	-	4	5	2	0	Jan 28, 2016
YouTube Content sharing	8.8 KB	2.6 KB	26	7	2	2	Jan 30, 2016
Aconex Collaboration	49.5 KB	48.8 KB	1	6	1	1	Feb 7, 2016
Atlassian Jira Project management	49.5 KB	48.8 KB	1	7	1	1	Feb 10, 2016
Box Cloud storage	96.7 KB	9.8 KB	1	6	1	1	Feb 28, 2016

Investigación



Discover



Investigate



Control



Alerts

Cloud App Security Discover Investigate Control Alerts 24 Microsoft

Files

New policy from search | New user notification

APP: Select apps... | OWNER: Select users... | ACCESS LEVEL: Select access level... | FILE TYPE: Select type... | MATCHED POLICY: Select policy... Advanced

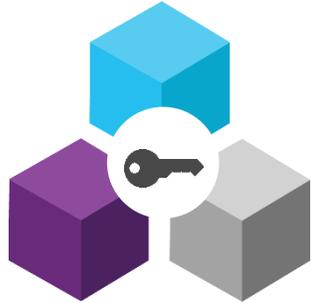
1 - 20 of 431 files

File name	Owner	App	Collaborators	Last modified
dealers protest picture burglaries	stacey	Google Apps	14 collaborators	Mar 1, 2016
guests independence percentages presentation	hortencia	Salesforce	14 collaborators	Mar 1, 2016
threats resource adaption loaves	mandy	Google Apps	28 collaborators	Mar 1, 2016
throttles differences reports replenishments	jeromy	Microsoft SharePoint Online	23 collaborators	Mar 1, 2016
rope frames interface tires	valentin	Box	4 collaborators	Mar 1, 2016
amount organs tone encounter	arthur	Salesforce	3 collaborators	Mar 1, 2016
stages chips response hooks	shirley	Box	9 collaborators	Feb 29, 2016
foods pans wells coil	jung	Microsoft SharePoint Online	14 collaborators	Feb 29, 2016
coordinate butter holddown ream	jody	Google Apps	27 collaborators	Feb 29, 2016



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 Forzado de políticas



- 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 extensión de políticas DLP existentes.



- 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

Cloud App Security Discover Investigate Control Alerts 24 Search Settings Help User Microsoft

Policy center

TYPE: Select type... SEVERITY: [Low] [Medium] [High] NAME: Policy name... RISK CATEGORY: Select risk category... Advanced

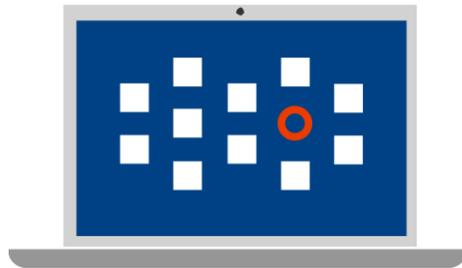
1 - 6 of 6 Policies Create policy Filter

Report	Count	Severity	Risk category	Action	Modified	
PCI COMPLIANCE: Publicly shared files with credit card info This policy identifies files containing credit card numbers and are publicly shared. Ate...	2 matches	[High]	Compliance	[Alerts]	Jul 22, 2015	[Settings] [More]
User logon from a non-categorized IP address Alert when a user logs on from an IP address that hasn't been included in a specific IP...	0 open alerts	[High]	—	[Alerts]	Mar 8, 2016	[Settings] [More]
Anomaly Detection Policy ADP	0 open alerts	[High]	—	[Alerts]	Mar 8, 2016	[Settings] [More]
Mass download by a single user Alert when a single user performs more than 30 downloads within 5 minutes.	0 open alerts	[High]	—	[Alerts]	Mar 14, 2016	[Settings] [More]
testing	0 open alerts	[Low]	—	[Alerts]	Mar 14, 2016	[Settings] [More]
Demo for bla	0 open alerts	[Low]	—	—	Mar 17, 2016	[Settings] [More]



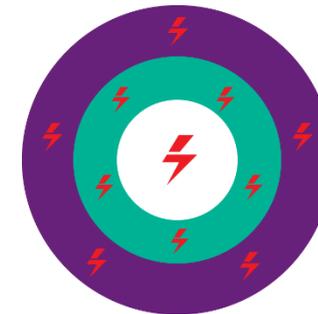
Protección de Amenazas

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 envío de ficheros frente a *malwares*

Protección de Amenazas



Discover



Investigate



Control



Alerts

Cloud App Security

Discover Investigate Control Alerts 24

Alerts

RESOLUTION STATUS: OPEN DISMISSED RESOLVED

RISK CATEGORY: Select risk category...

SEVERITY: [Progress indicators]

APP: Select apps...

USER: Select users...

POLICY: Select policy...

Advanced

1 - 20 of 24 alerts

Alert	App	Resolution	Severity	Date
Suspicious Activity / miah@acme.com	Google Apps	OPEN	High	21 days ago
New admin location / rolando@acme.com NL	Office 365	OPEN	Medium	21 days ago
Salesforce zombie account kenton@acme.com	Salesforce	OPEN	Medium	21 days ago
General Anomaly Detection / marianna@acme.com Google Apps	Exchange Online	OPEN	Medium	21 days ago
Suspicious Activity lavina@acme.com	Google Apps	OPEN	Medium	21 days ago
Suspicious Activity hiram@acme.com	Google Apps	OPEN	Medium	21 days ago

Integración probada para las Top SaaS apps



¿Quién lo está utilizando?





Gracias
Q&A

asantama@microsoft.com