

Microsoft Security



Security Specialist
Mauricio Betancourt

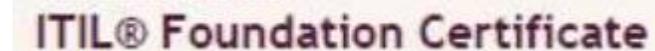


Perfil. Ingeniero de Sistemas Especialista Ciberseguridad



Security
Specialist

Mauricio Betancourt



33%

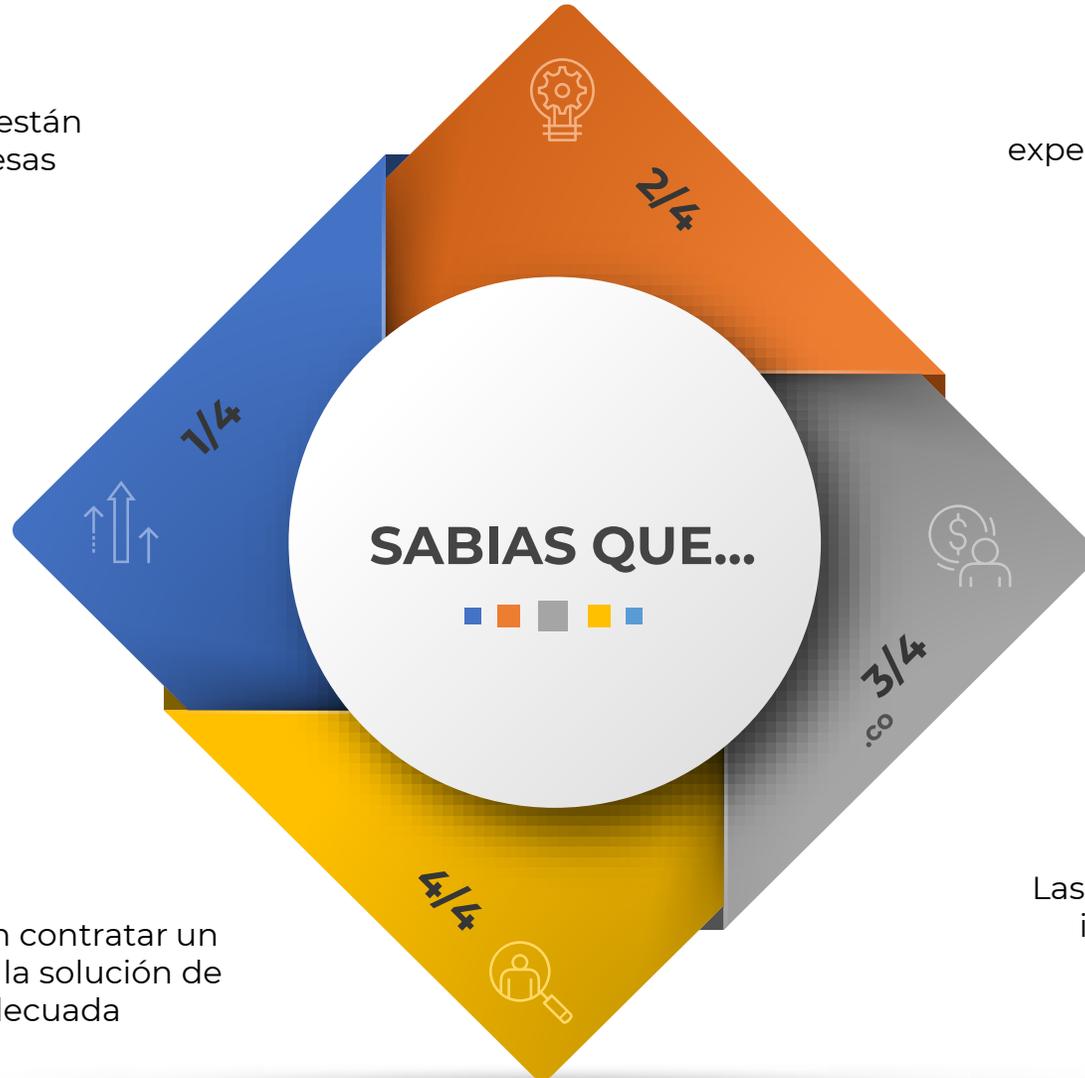
1/3 de todos los ciberataques están dirigidos a pequeñas empresas



coste medio de una violación de datos de pymes.

90%

Las pymes considerarían contratar un nuevo MSP si ofrecieran la solución de ciberseguridad adecuada



61%

De las pequeñas empresas que experimentan un ciberataque reciente no pudieron operar

60%

Las pymes carecen de competencias internas para hacer frente a los ciberataques



¿Fecha de la aparición del malware tipo Ransomware?

¿Empresa que fue afectada por el ataque mas conocido del Ransomware?

Historia del Ransomware

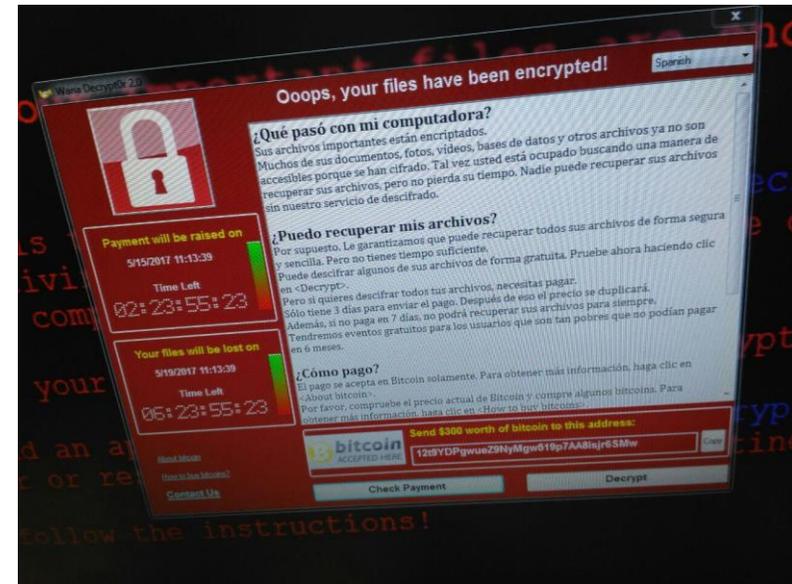


Ataques de Ransomware.



En **1989** se pensó qué había en un disquete que había recibido de la OMS. Se esperaba una investigación médica sobre el SIDA, se encontró con un hackeo que le pedía **189 dólares**.

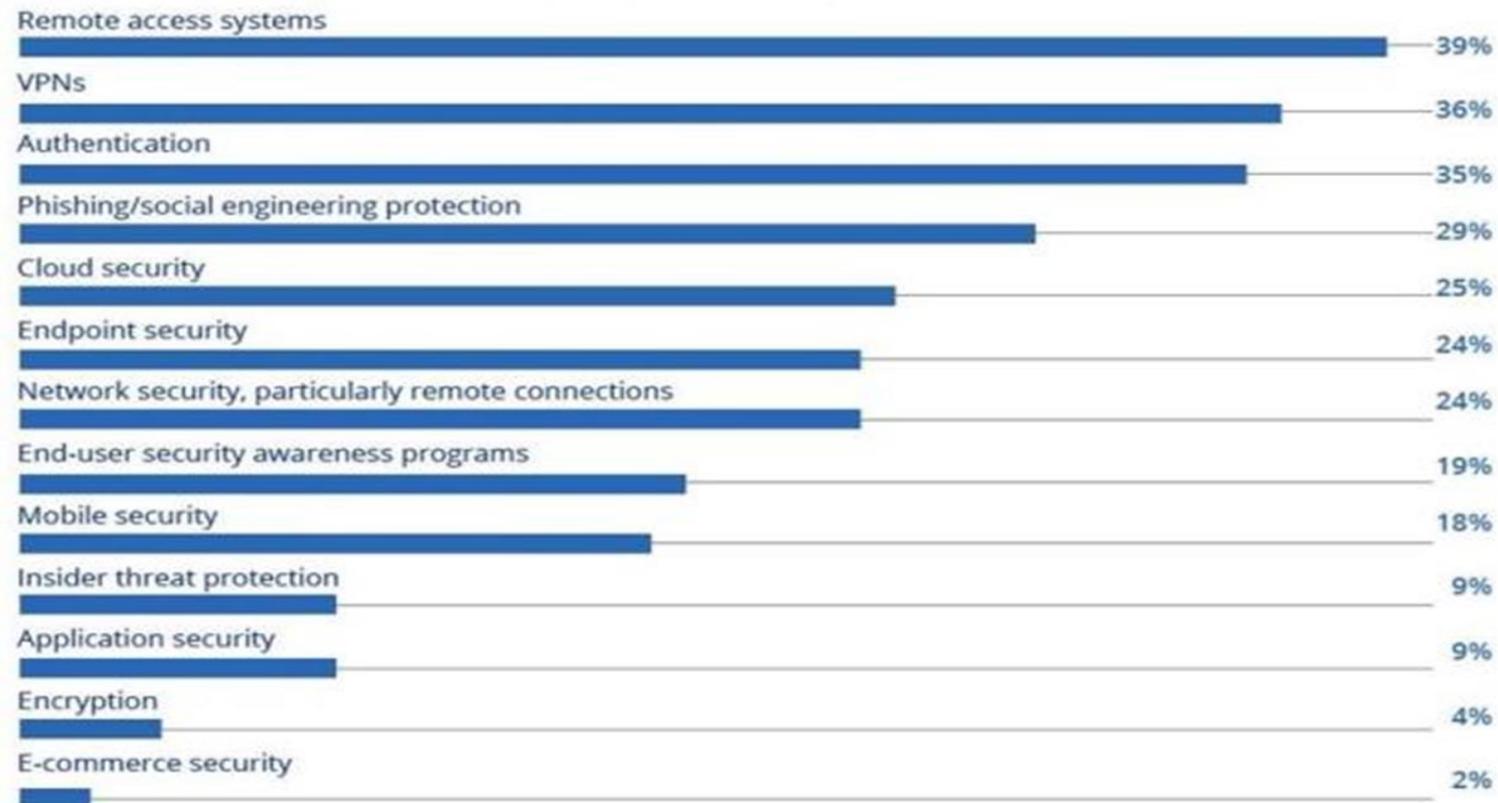
En **2017** Los servicios de sistemas de la operadora han explicado a través de mensajes de correo electrónico a la plantilla que se ha detectado en la red de **la empresa de telecomunicaciones** el ingreso de un malware que afecta a los datos y a los ficheros de los empleados y ha conminado a éstos a que los apaguen y no los enciendan hasta nuevo aviso. También se ha pedido que se desconecten los teléfonos móviles de la red WiFi.



¿Y cómo ha cambiado la seguridad en la nueva realidad?

Prioritization of Security Projects

Which security projects or tasks will get highest priority as a result of the COVID-19 outbreak?



Note: Maximum of three responses allowed

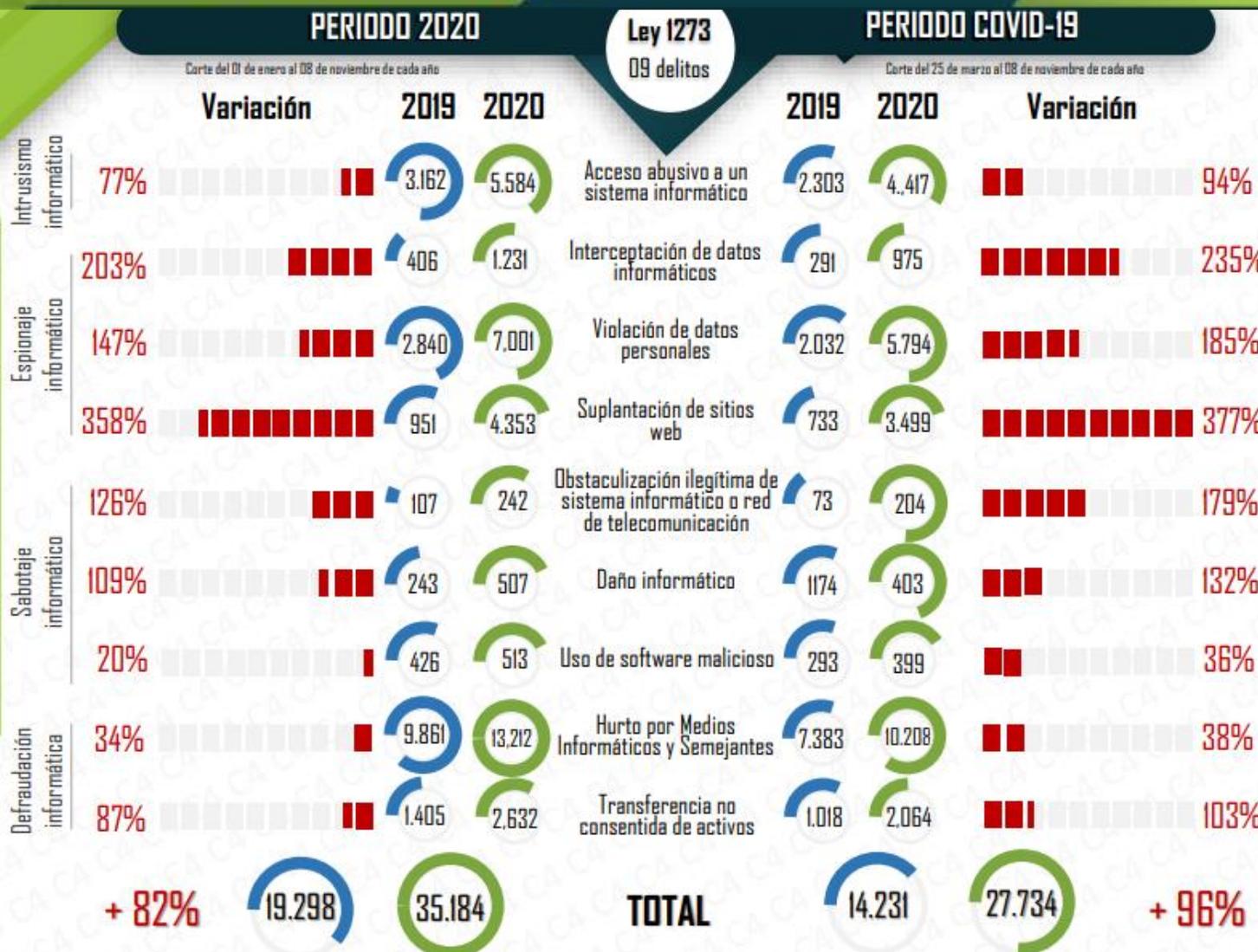
Data: Dark Reading survey of 190 technology and cybersecurity professionals at organizations with 100 or more employees, July 2020

BALANCE CIBERCRIMEN 2020



La ciberdelincuencia a nivel global crece a un ritmo considerable con nuevas tendencias emergiendo permanentemente. Los ciberdelincuentes cada vez se especializan más, siendo capaces de hacer uso de las nuevas tecnologías en pro de sus intereses, adaptan sus ataques utilizando nuevos métodos y establecen redes de cooperación, dándoles la capacidad de materializar un ataque en cuestión de minutos. El incremento del uso de Internet y las tecnologías de la información y las comunicaciones, abren con ello una enorme ventana de oportunidades para que los ciberdelincuentes ataquen

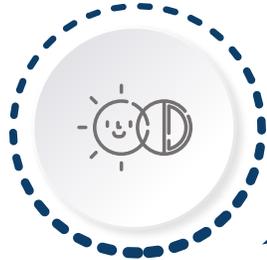
Estadística Ley 1273 de 2009



Microsoft Security

Seguridad en nube

- Microsoft Defender for Cloud
- Microsoft Defender for Cloud apps
- Seguridad avanzada de GitHub



Administración de riesgos

- Administración de riesgos internos
- Cumplimiento de comunicaciones
- eDiscovery



Administración de acceso e identidades

- Azure Active Directory
- Administración de permisos de CloudKnox



SIEM y XDR

- Microsoft 365 Defender
- Microsoft Defender for Cloud
- Microsoft Sentinel



Gobierno y protección de la información

- Protección de la información
- Gobierno de la información
- Prevención de pérdida de datos



Confianza cero una seguridad proactiva



A group of business professionals are seated around a conference table in a meeting room. The scene is overlaid with a semi-transparent blue filter. The word "Seguridad" is centered in white text, with a thin yellow horizontal line underneath it. The background shows a whiteboard with some faint text and a lamp hanging from the ceiling.

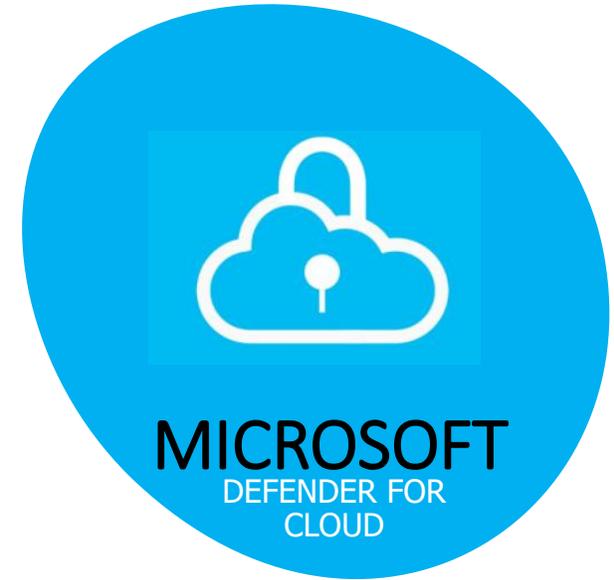
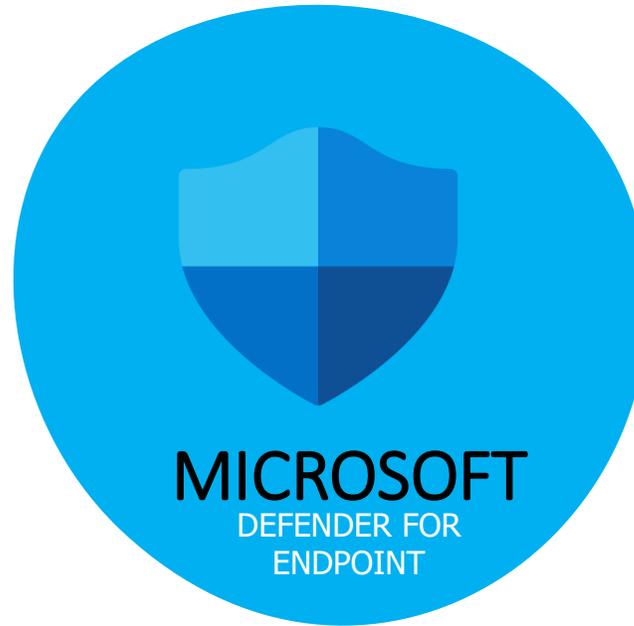
Seguridad



¿Como **controlas** el acceso de los dispositivos a tu compañía y evitas que haya **fugas de información**?

¿Cuentas actualmente con una **solución de seguridad 360** que permita mitigar al máximo las amenazas informáticas?

Microsoft Defender



Señales de seguridad de Microsoft Volumen y diversidad de señales procesadas por Microsoft



July 1, 2020 through June 30, 2021

Microsoft Defender for office 365

Microsoft 365



INTELIGENCIA SOBRE AMENAZAS



Una visión integral de la protección contra amenazas

The screenshot shows the Microsoft 365 Defender Home dashboard. Key metrics include:

- Threat analytics:** 2 active threats, including "MOBILE/M mail email campaign" and "Living off the land binaries".
- Active incidents:** 112 active incidents, with a list of recent events such as "Unauthenticated cloud app access was blocked on multiple endpoints".
- Users at risk:** 88 users at risk, categorized by risk level (High, Medium, Low).
- Device health:** Active Devices: 682, with 10 device(s) at risk.
- Discovered devices:** Total discovered devices: 14.1k, including 1 IoT device, 14085 endpoints, and 3 high value devices.

The screenshot shows the Configuration analyzer page in Microsoft 365 Defender. It displays a table of 39 strict recommendations for the Anti-phishing policy group.

Policy group/setting name	Policy	Applied to	Current configuration	Last modified	Recommendations
Anti-spam	10 recommendations				
Anti-phishing	24 recommendations				
If email is sent by someone who's not allowed to sp...	Office365 AntiPhish ...	Move to Junk Email E...	Mar 29, 2021 5:00 PM	Quarantine message	Adopt
Automatically include the domains I own	Office365 AntiPhish ...	False	Mar 29, 2021 5:00 PM	True	Adopt
Include custom domains	Office365 AntiPhish ...	False	Mar 29, 2021 5:00 PM	True	Modify
If email is sent by an impersonated user	Office365 AntiPhish ...	Move to Junk Email E...	Mar 29, 2021 5:00 PM	Quarantine message	Adopt
If email is sent by an impersonated domain	Office365 AntiPhish ...	Move to Junk Email E...	Mar 29, 2021 5:00 PM	Quarantine message	Adopt
Enable intelligence for impersonation protection (...)	Office365 AntiPhish ...	False	Mar 29, 2021 5:00 PM	True	Adopt
Show tip for impersonated users	Office365 AntiPhish ...	False	Mar 29, 2021 5:00 PM	True	Adopt
Show tip for impersonated domains	Office365 AntiPhish ...	False	Mar 29, 2021 5:00 PM	True	Adopt
Show tip for unusual characters	Office365 AntiPhish ...	False	Mar 29, 2021 5:00 PM	True	Adopt
If email is sent by an impersonated user who's prot...	Office365 AntiPhish ...	No action	Mar 29, 2021 5:00 PM	Quarantine message	Adopt
Advanced phishing thresholds	Office365 AntiPhish ...	1	Mar 29, 2021 5:00 PM	3	Adopt

The screenshot shows an investigation graph for a "Weaponized URL in mail discovered by Defender for Office 365". The investigation is complete and remediated. The graph details the following:

- Triggering Alerts:** Automated investigation of a weaponized URL in mail.
- Emails Investigated (5):** 1 email (viva.org/Phish (5)).
- Users Investigated (5):** 1 user impacted (1), 4 suspicious logins (1), and 4 mail downloads (1).
- Threats Found:** 3 threats identified: "Compromised User - Sending email phish", "User - Activity Anomalies detected", and "Compromised Device - Malware".
- Actions Remediated:** 3 actions completed: "URL Blocked (1)" and "Emails Deleted (2)".



¿Cómo Protege el **correo electrónico, los archivos** y las **aplicaciones de office 365** frente ataques desconocidos y elaborados.?

OFFICE ADVANCED THREAT PROTECTION

- ❖ PROTECCION FRENTE A VINCULOS MALINTENCIONADOS
- ❖ PROTECCION CONTRA DATOS ADJUNTOS PELIGROSOS
- ❖ PROTECCION DE BUZONES
- ❖ INFORMES



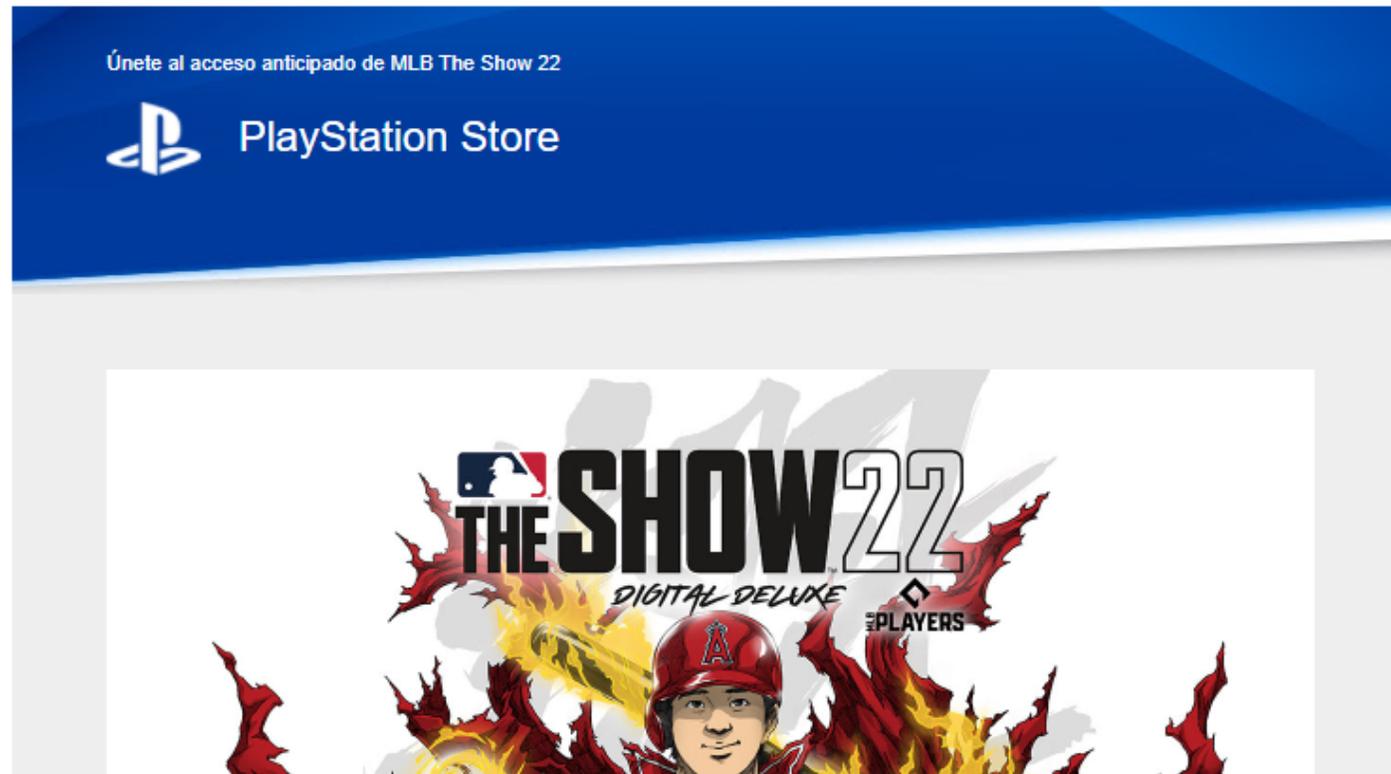
OFFICE ADVANCED THREAT PROTECTION

❖ PROTECCION FRENTE A VINCULOS MALINTENCIONADOS

 Aduéñate del espectáculo con la actualización de esta semana de PS Store   Recibidos x

PlayStation <email@email.playstation.com> [Anular suscripción](#)
para mí ▾

mié, 23 mar, 20:11 (hace 10 horas)



OFFICE ADVANCED THREAT PROTECTION

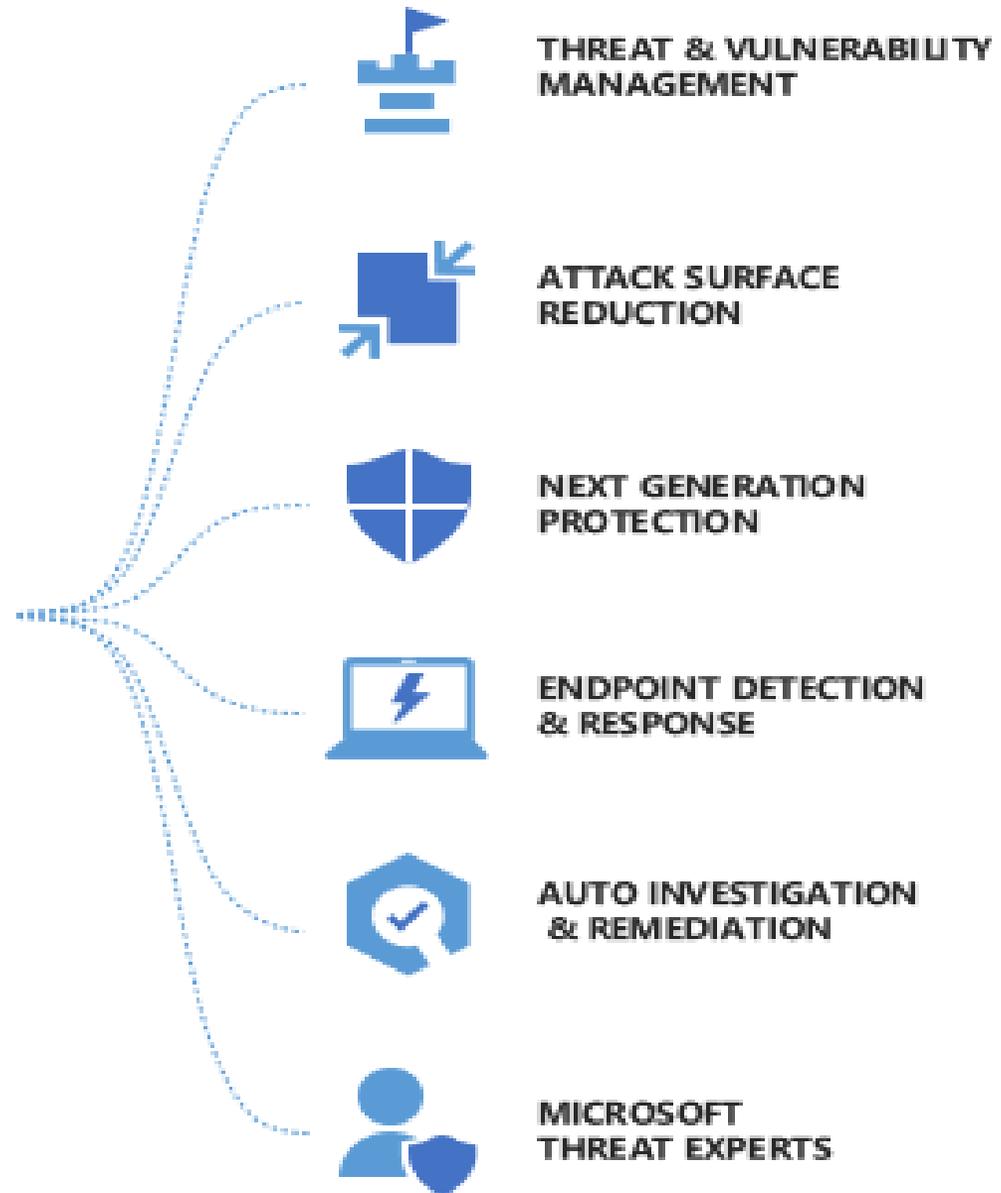
❖ PROTECCION FRENTE A VINCULOS MALINTENCIONADOS

Delivered-To: mbetanco82@gmail.com
Received: by 2002:a05:6512:10c1:0:0:0 with SMTP id k1csp30926861fg;
Wed, 23 Mar 2022 18:11:20 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJyb53c1MJAFK1VN9pC/X2xSBKLqQZiW2V1IcwnRHy19+/krSspwS0dBB/wNe272U18arxCM
X-Received: by 2002:a05:6214:2467:b0:441:406d:b007 with SMTP id im7-20020a056214246700b00441406db007mr2455038qvb.55.1648084280420;
Wed, 23 Mar 2022 18:11:20 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1648084280; cv=none;
d=google.com; s=arc-20160816;
b=F/BkzX6ZmZHcp5HmONCcUmvCGGatvIDJa7W47+oPUVIV5un7QxNC5RsZaaGVDiuwKc
v4P5WdXAW8jye/2yHv13P0JEtB+RVJVMOUJB1X2u/GvaRLJJOK40YzDuUTjf+n0XvNyk
rBuCXH1HqnDjAWGHih+5zDkGVbjgI4cNfTu1Qv0yQbF4A/RXcpwZjpou57BkrTopYfId
yYh2M7UmfwEiZttz4mfemt3QpzDLvrSw5FfdCqrc/kOW9nNiSV/oEShhsP0hAjCDSvY
VHFPPF0DKCnDgSVAFGimuEjnjoShe6Z2AQ59Yfm68q5xKUUkPaUCKYrpIRdGZi1bOdR0
AgYg==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
h=feedback-id:message-id:list-id:reply-to:mime-version
:list-unsubscribe-post:list-unsubscribe:date:subject:to:from
:dkim-signature;
bh=m11mQq1q+qvD+epRUvFuclCg9+v9s7+qs/PMWujrvaQ=;
b=ryWXKN/jTcWdtjMEew6KdMHSgjEoYGVxvJpJoo3T1Iag8RBm7TbY2W6WdNMQSHyiD
KHPZ/zzq/IaPXYo1BaE8EJZro8uNP2qh9TuLRGCw0vKwVu8BQAmVcJnrz4LwjZUDGLr5
ZM4Bg2TDkdXsQzOy70YkL0kn4LjRdZJlHatHfOQu4bMxv80Md2C/Hqye7qwXvukH6XQn
Wy2YlGdSjNlFkaXikcPweJLteOM0z/gLI0YBW5Ak623cVfdy6ztd0tM414gAC6YI8pB
2MJWg7noNZaHNngBxPzBw7Jgl+HL2KpCNTbS/eGz0xL6LliEXM1zZPLXNwd18ETgo5n
Dhiw==
ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@email.playstation.com header.s=200608 header.b=gkERX0Aj;
spf=pass (google.com: domain of bounce-19_html-289807781-450998-6151033-11068@bounce.email.playstation.com designates
13.111.27.214 as permitted sender) smtp.mailfrom=bounce-19_HTML-289807781-450998-6151033-11068@bounce.email.playstation.com;
dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=email.playstation.com
Return-Path: <bounce-19_HTML-289807781-450998-6151033-11068@bounce.email.playstation.com>
Received: from ea214.mta.exacttarget.com (mta21.playstationemail.com. [13.111.27.214])
by mx.google.com with ESMTPS id h12-20020a05620a284c00b0067ec6a6bb07si2578621qkp.556.2022.03.23.18.11.19
for <mbetanco82@gmail.com>
(version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
Wed, 23 Mar 2022 18:11:20 -0700 (PDT)
Received-SPF: pass (google.com: domain of bounce-19_html-289807781-450998-6151033-11068@bounce.email.playstation.com designates
13.111.27.214 as permitted sender) client-ip=13.111.27.214;



Microsoft Defender for Endpoint

Built-in. Cloud-powered.



Microsoft Defender ATP next generation protection engines



Metadata-based ML

Stops new threats quickly by analyzing metadata



Behavior-based ML

Identifies new threats with process trees and suspicious behavior sequences



AMSI-paired ML

Detects fileless and in-memory attacks using paired client and cloud ML models



File classification ML

Detects new malware by running multi-class, deep neural network classifiers



Detonation-based ML

Catches new malware by detonating unknown files



Reputation ML

Catches threats with bad reputation, whether direct or by association



Smart rules

Blocks threats using expert-written rules



ML

Spots new and unknown threats using client-based ML models



Behavior monitoring

Identifies malicious behavior, including suspicious runtime sequence



Memory scanning

Detects malicious code running in memory



AMSI integration

Detects fileless and in-memory attacks



Heuristics

Catches malware variants or new strains with similar characteristics



Emulation

Evaluates files based on how they would behave when run



Network monitoring

Catches malicious network activities

- Acciones y envíos
- Centro de actividades
- Entregas
- Análisis de amenazas
- Puntuación de seguridad
- Centro de aprendizaje
- Pruebas
- Extremos
- Inventario de dispositivos
- Administración de vulnerabi...
- Panel
- Recomendaciones
- Corrección
- Inventario de software**
- Puntos débiles
- Escala de tiempo del evento

Inventario de software

Aplicaciones
46

Exportar

Nombre	Plataforma de sist...	Proveedor	P
<input checked="" type="checkbox"/> Windows 10	Windows	Microsoft	9
Edge	Windows	Microsoft	7
Defender For Endpoint	Windows	Microsoft	1
Workstation	Windows	Vmware	9
Jdk	Windows	Oracle	1
Jre	Windows	Oracle	1
Postman	Windows	Postman	0
Chrome	Windows	Google	0

Windows 10

Versiones de EOS

[Abrir página de software](#) [Informar de imprecisión](#)

Detalles del software **Dispositivos instalados**

Exportar

3 elementos

Buscar

Nombre	Sistema operativo	Última visualiz
testvmdesktop	Windows 10	23/3/2022
desktop-82cbhmp	Windows 10	22/3/2022
desktop-c2c84lh	Windows 10	22/3/2022

Panel de administración de amenazas y vulnerabilidades

Puntuación de exposición de la organización

Puntuación de exposición

Esta puntuación refleja la exposición actual asociada a los dispositivos de su organización. Las excepciones activas pueden afectar a la puntuación.



16/100

■ Bajo 0 a 29 ■ Medio 30 a 69 ■ Alto 70 a 100

Puntuación de exposición en el tiempo



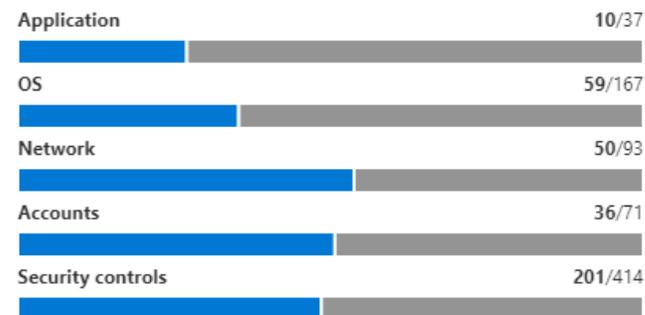
Mejorar puntuación

Puntuación de seguridad de Microsoft para dispositivos

Su puntuación para los dispositivos: 46 %

Esta puntuación refleja la postura de configuración de seguridad colectiva de sus dispositivos a través de los controles de seguridad del sistema operativo, de las aplicaciones, de la red y de las cuentas. La puntuación puede quedar afectada por excepciones activas.

356/782 puntos obtenidos



Puntuación para dispositivos a lo largo del tiempo



Mejorar puntuación

Exportar

Nombre	Gravedad
CVE-2021-35564	Medium
CVE-2021-3522	Medium
CVE-2021-35567	Medium
CVE-2021-35603	Low
CVE-2021-35561	Medium
CVE-2021-35556	Medium
CVE-2020-3987	Medium
<input checked="" type="checkbox"/> CVE-2020-3999	Low
CVE-2020-3981	High
CVE-2021-35550	Medium
CVE-2021-35565	Medium
CVE-2020-3989	Low
CVE-2020-4004	Critical
CVE-2020-3990	Low
CVE-2020-3988	Medium
CVE-2020-3982	Medium
CVE-2021-35588	Low
CVE-2021-35550	...

privilege access to a virtual machine can crash the virtual machines vmx process leading to a denial of service condition.

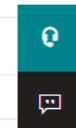
Detalles de la vulnerabilidad

Nombre de vulnerabilidad	Gravedad
CVE-2020-3999	Low
CVSS	Publicado el
3.3	16/12/2020
Actualizado el	Antigüedad
21/7/2021	un año
Software relacionado	
Vmware Workstation (y 2 más)	
Detalles de amenaza	
Público	Comprobado
No	No
Kits de vulnerabilidades	Tipo
No	-
Referencia	
-	

Dispositivos expuestos para todo el software relacionado (1)

Exportar

Nombre	Plataforma de sistema op...	Última visualización
desktop-82cbhmp	Windows 10	21/3/2022



- Acciones y envíos
- Centro de actividades
- Entregas
- Análisis de amenazas
- Puntuación de seguridad
- Centro de aprendizaje
- Pruebas
- Extremos
- Inventario de dispositivos
- Administración de vulnerabi...
- Panel
- Recomendaciones**
- Corrección
- Inventario de software
- Puntos débiles
- Escala de tiempo del evento
- Asociados y API

Recomendaciones Actualizar VMware Workstation

Corrección necesaria

[Abrir página de software](#) [Informar de imprecisión](#)

General Dispositivos expuestos Dispositivos instalados CVE asociados

Exportar

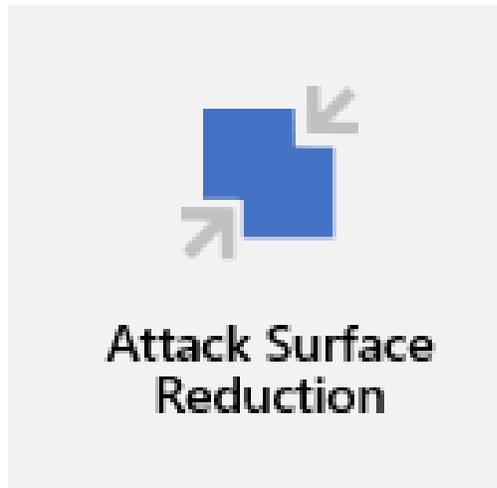
9 elementos

Nombre	Gravedad	Publicado el	Dispositivos expuestos
CVE-2020-3986	Medium	13/9/2020	1
CVE-2020-3989	Low	13/9/2020	1
CVE-2020-4004	Critical	18/11/2020	1
CVE-2020-3999	Low	16/12/2020	1
CVE-2020-3981	High	19/10/2020	1

Solicitar corrección

Opciones de excepción

Microsoft Defender for End point



web Control

 Eliminar

Categorías

- Ancho de banda alto [^]
 - Descargar sitios
 - Punto a punto
 - Transmisión multimedia y descargas
 - Uso compartido de imágenes
- Contenido para adultos [^]
 - Apuestas
 - Cultos
 - Desagradable
 - Desnudez
 - Educación sexual
 - Pornografía/Sexualmente explícito
 - Violencia

web Control

+ Agregar elemento

✓ Nombre de la dirección

Guardar

Microsoft Defender for End point



Endpoint Detection
& Response



Expertos en
amenazas de Microsoft

Microsoft Defender for End point

Ofrecer seguridad de endpoints en todas las plataformas



Microsoft Defender for End point

Microsoft Defender calificó consistentemente como el mejor AV

1

AV-TEST: Protection score of 6.0/6.0 in the latest test

2

AV-Comparatives: Protection rating of 99.7% in the latest test

3

SE Labs: AAA award in the latest test

4

MITRE: Industry-leading optics and detection capabilities

 **6.0/6.0**

**Protection score
in AV-TEST**

Achieved perfect protection
score in the past 8 cycles

 **99.7%**

**Real-world protection
in AV-Comparatives**

Scored consistently high in
Real-World Protection Rates

 **AAA**

**Award from SE Labs
in past 4 cycles**

Achieved 97% cycles total
accuracy in latest cycle

Microsoft Defender for Cloud

Microsoft Defender for Cloud | Overview

Showing 73 subscriptions

[Subscriptions](#) [What's new](#)

73 Azure subscriptions

4 AWS accounts

4 GCP projects

5984 Assessed resources

209 Active recommendations

7336 Security alerts

Secure score

Unhealthy resources
4101 To harden these resources and improve your score, follow the security recommendations

Current secure score

54% 3137 POINTS

- COMPLETED Controls: 1/16
- COMPLETED Recommendations: 24/110

[Improve your secure score >](#)

Workload protections

Resource coverage
98% For full protection, enable 11 resource plans

Alerts by severity

High	4.6k
Medium	2K
Low	682

[Enhance your threat protection capabilities >](#)

Regulatory compliance

Azure Security Benchmark **None**

1 of 40 passed controls

Lowest compliance regulatory standards by passed controls

CMMC Level 3	0/55
NIST SP 800 53 R5	2/55
ISO 27001	1/20

[Improve your compliance >](#)

Insights

Most prevalent recommendations (by resources)

Audit diagnostic setting	1025
Append a tag and its value to resou...	549
Storage account should use a privat...	447
Storage accounts should restrict net...	446

New security alerts

145 new alerts were detected by Defender for Cloud in the last 48 hours.

[View full alerts list >](#) 5

[Azure Defender for SQL on machine...](#) 7

Controls with the highest potential increase

Remediate vulnerabilities	+10%	(6pt)
Remediate security configurations	+6%	(4pt)
Enable MFA	+6%	(10pt)

[View controls >](#)

Firewall Manager

5 Firewalls **3** Firewall policies **4** Regions with firewalls

Network protection status by resource

Virtual hubs	0/0
Virtual networks	8/249

[Improve your network security >](#)

Inventory

Unmonitored VMs
134 To better protect your organization, we recommend installing agents

Total Resources
5984

Unhealthy (4101)
Healthy (1435)
Not applicable (448)

[Explore your resources >](#)

Information protection **Preview**

Integrated with Purview

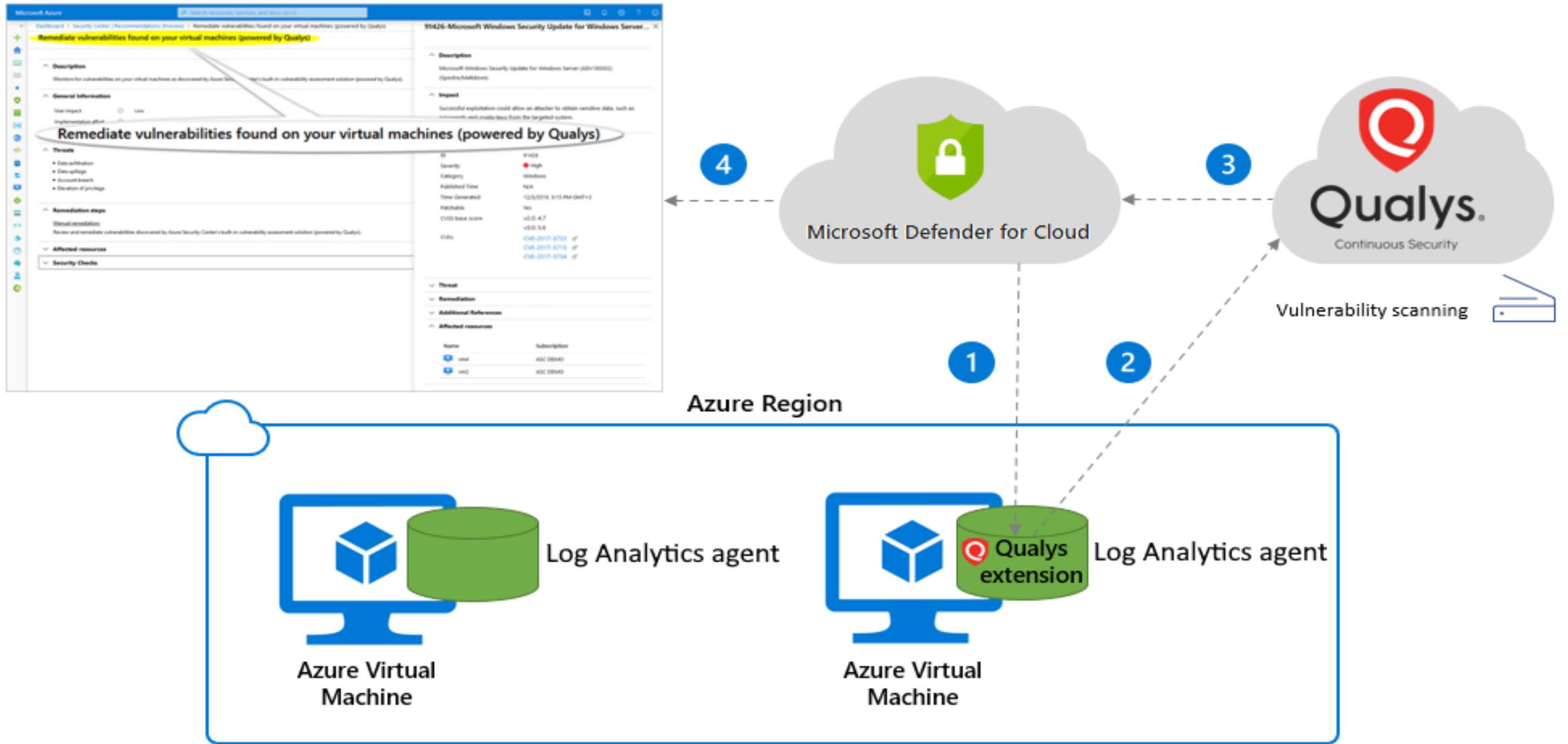
Resource scan coverage
1% For full coverage [scan](#) additional resources

Recommendations & Alerts by classified resources

Storage Accounts	Alerts: 1, Recommendations: 12
SQL Databases	Alerts: 2, Recommendations: 3
SQL Servers	Alerts: 1, Recommendations: 4

[View classified resources in inventory >](#)

Microsoft Defender for Cloud



Process flow diagram for Microsoft Defender for Cloud's built-in vulnerability scanner.



¿Cómo les podemos apoyar en temas de **ciberseguridad** ?

ASSESSMENT



+ ¿QUE ES?

+ ¿QUE BUSCA?

+ ¿QUE VALOR GENERA
EN EL CLIENTE?

¿QUE ES UN ASSESSMENT?

Cuando se habla de ciberseguridad, es el análisis de riesgos informáticos, es la evaluación de los distintos peligros que afectan a nivel de seguridad y que pueden producir situaciones de amenazas al negocio, como robos o intrusiones que comprometan los datos de la empresa o también pueden ser ataques externos que impidan el funcionamiento de los sistemas.



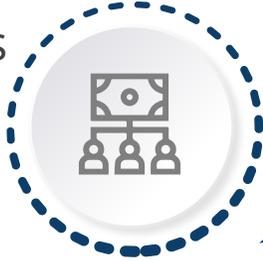
¿TIPOS DE EVALUACION?

- Análisis de vulnerabilidades. Escaneos
- Test de intrusión.
- Ejercicios Red Team
- GAP (ISO 27001 SGSI, Zero Trust (Microsoft), Buenas Practicas seguridad, hardening)
- Entre 40 a 50 usuarios.
- Mas de 50 usuarios.



¿QUE BUSCA?

• Identificar activos que requieren protección



• Construir el Plan de Acción



• Valorar las amenazas

• Identificar amenazas y debilidades



• Determinar el impacto en el negocio *



• Identificar vulnerabilidades



• Determinar el nivel de riesgo aceptado por la organización*



• Valorar el CiberRiesgo *

¿QUE VALOR GENERA EN EL CLIENTE?



GRACIAS