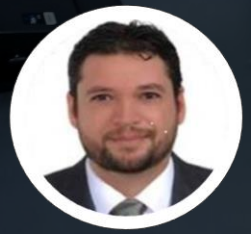
Microsoft

Microsoft Security



Security Specialist
Mauricio Betancourt

Perfil.
Ingeniero de Sistemas
Especialista Ciberseguridad

Security
Specialist

Mauricio Betancourt

Microsoft Specialist

Microsoft CERTIFIED Professional

Microsoft CERTIFIED Solutions Associate

McAfee Product Specialist CERTIFIED

C|EH Certified Ethical Hacker

C|ND Certified Network Defender

Qualys.

FORTINET NSE Institute

CISCO CERTIFIED CCNA ROUTING & SWITCHING

Check Point Certified

digium The Asterisk Company

icontec

PROFESSIONAL CERTIFICATE CertiProf Professional Knowledge SCRUM FOUNDATION SFPC

ICSI | CNSS Certified Network Security Specialist

ITIL® Foundation Certificate

33%

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

61 %

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

coste medio de una violación de datos de pymes.

90%

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

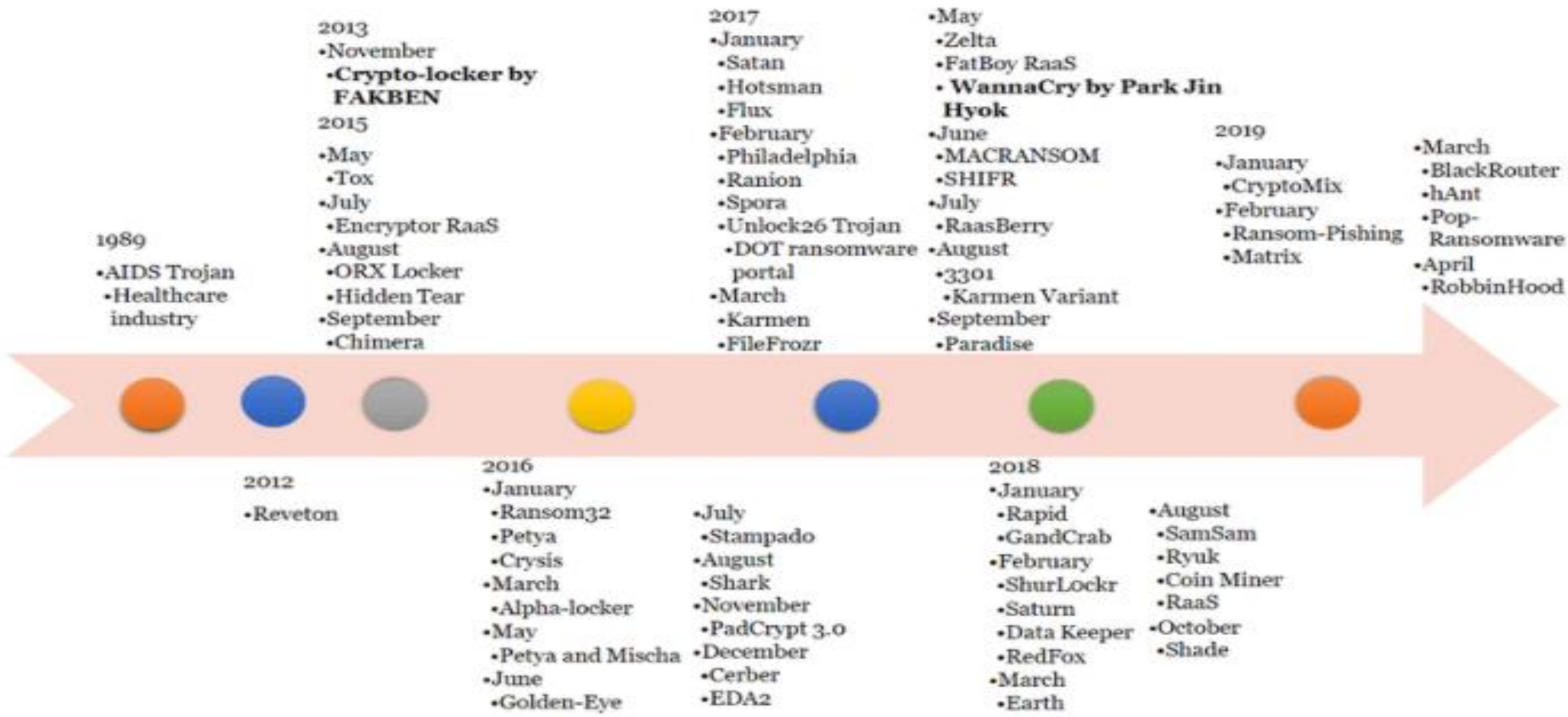
60%

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?

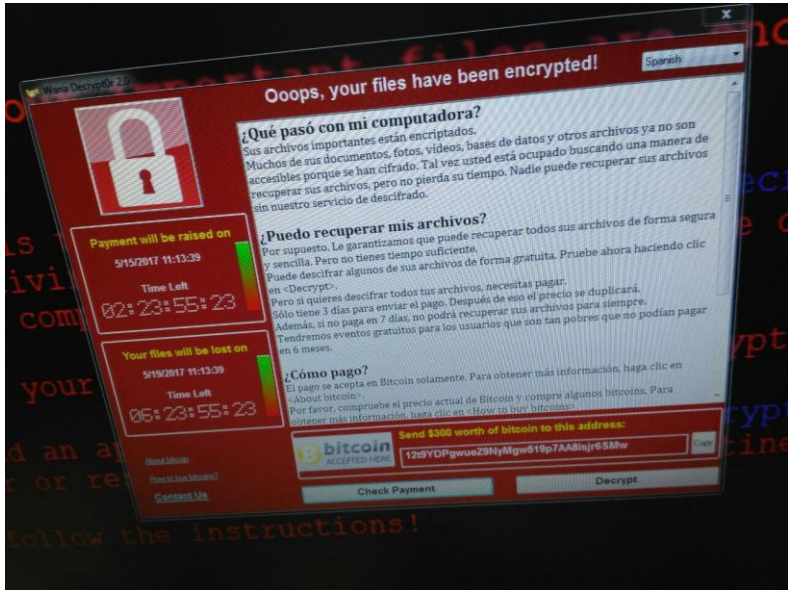
Historia del Ransomware



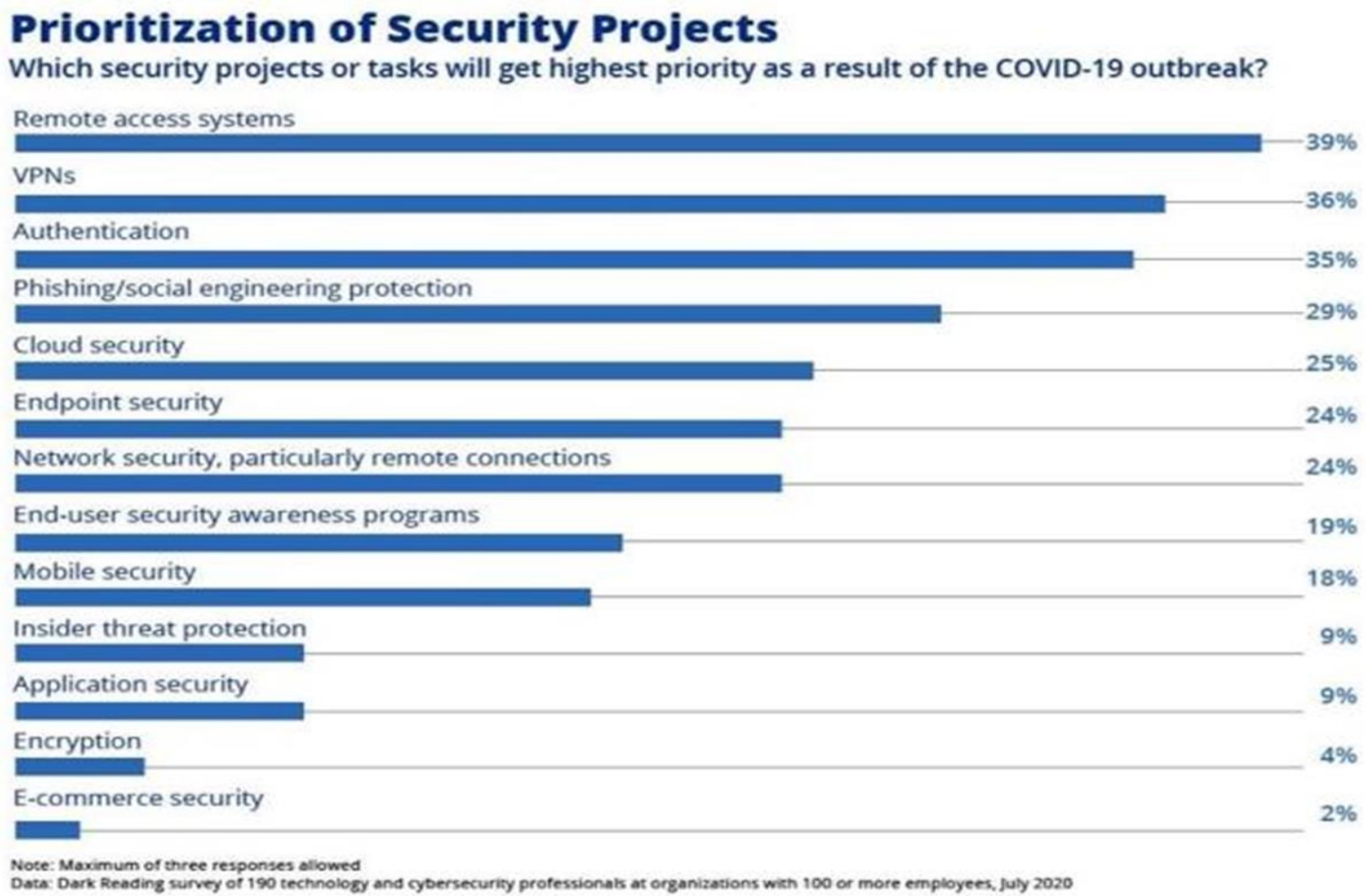
Ataques de Ransomware.

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.

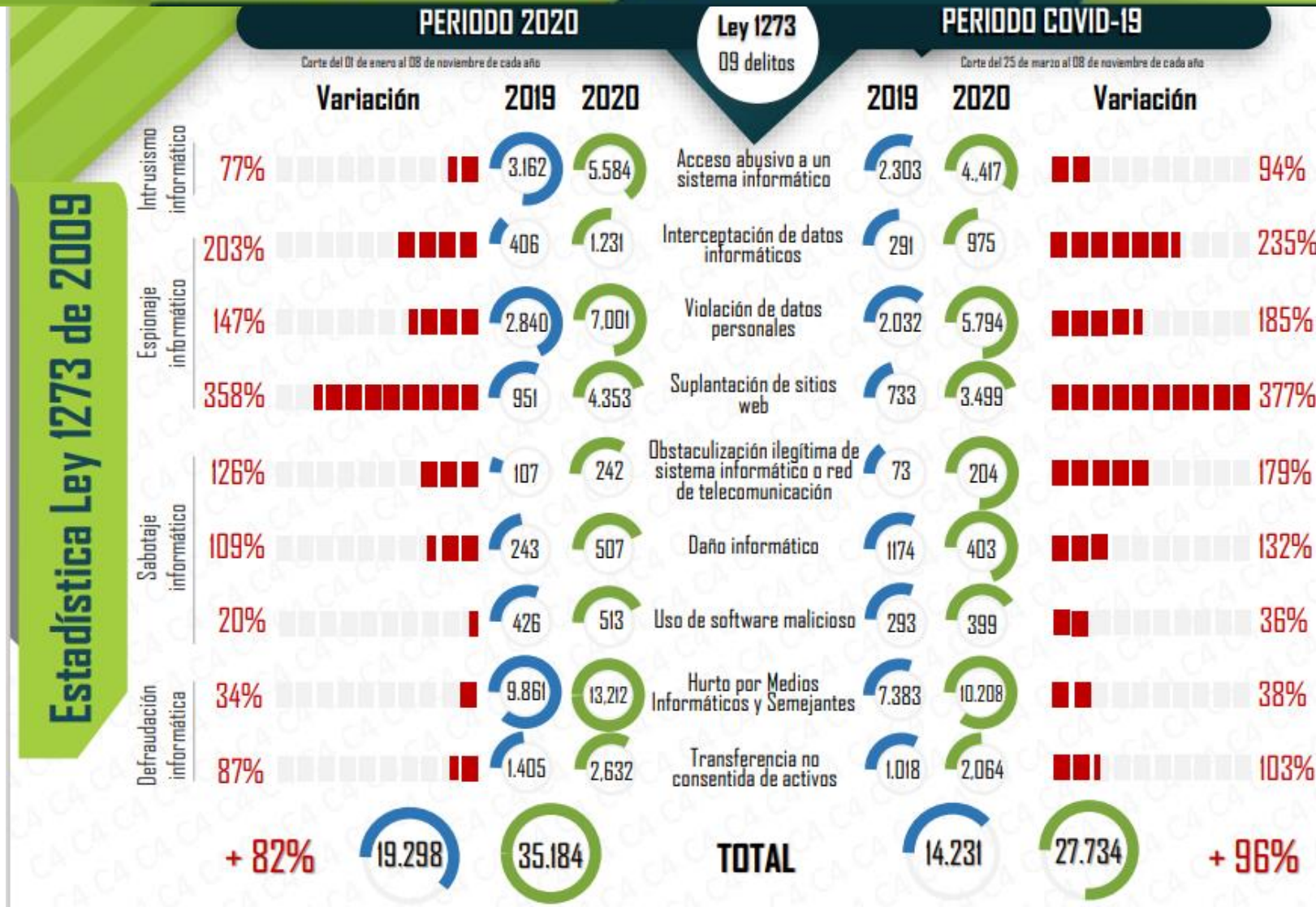


¿Y cómo ha cambiado la seguridad en la nueva realidad?



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 paraque los ciberdelincuentes ataquen



Seguridad en nube

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

Administración de acceso e identidades

- Azure Active Directory
- Administración de permisos de CloudKnox

Gobierno y protección de la información

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

Administración de riesgos

- Administración de riesgos internos
- Cumplimiento de comunicaciones
- eDiscovery

SIEM y XDR

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

Confianza cero

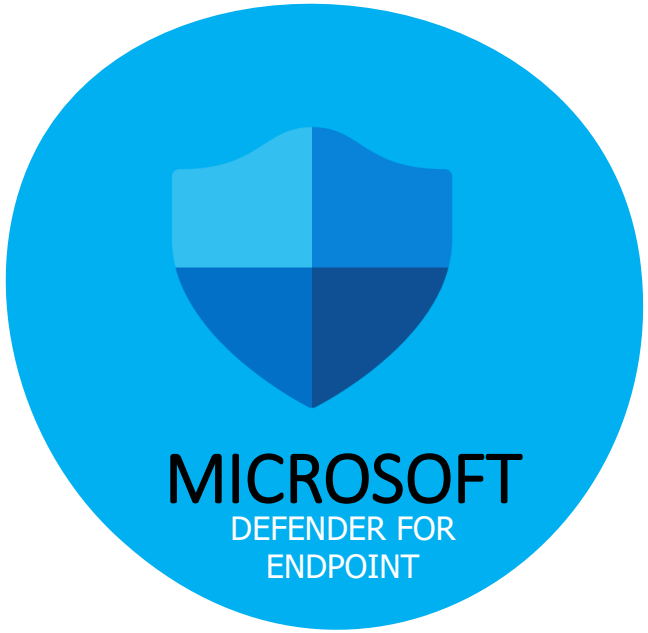
una seguridad proactiva

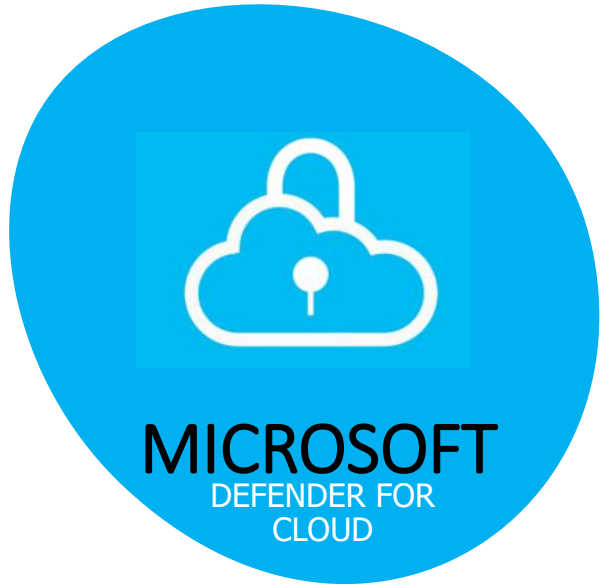
Seguridad

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

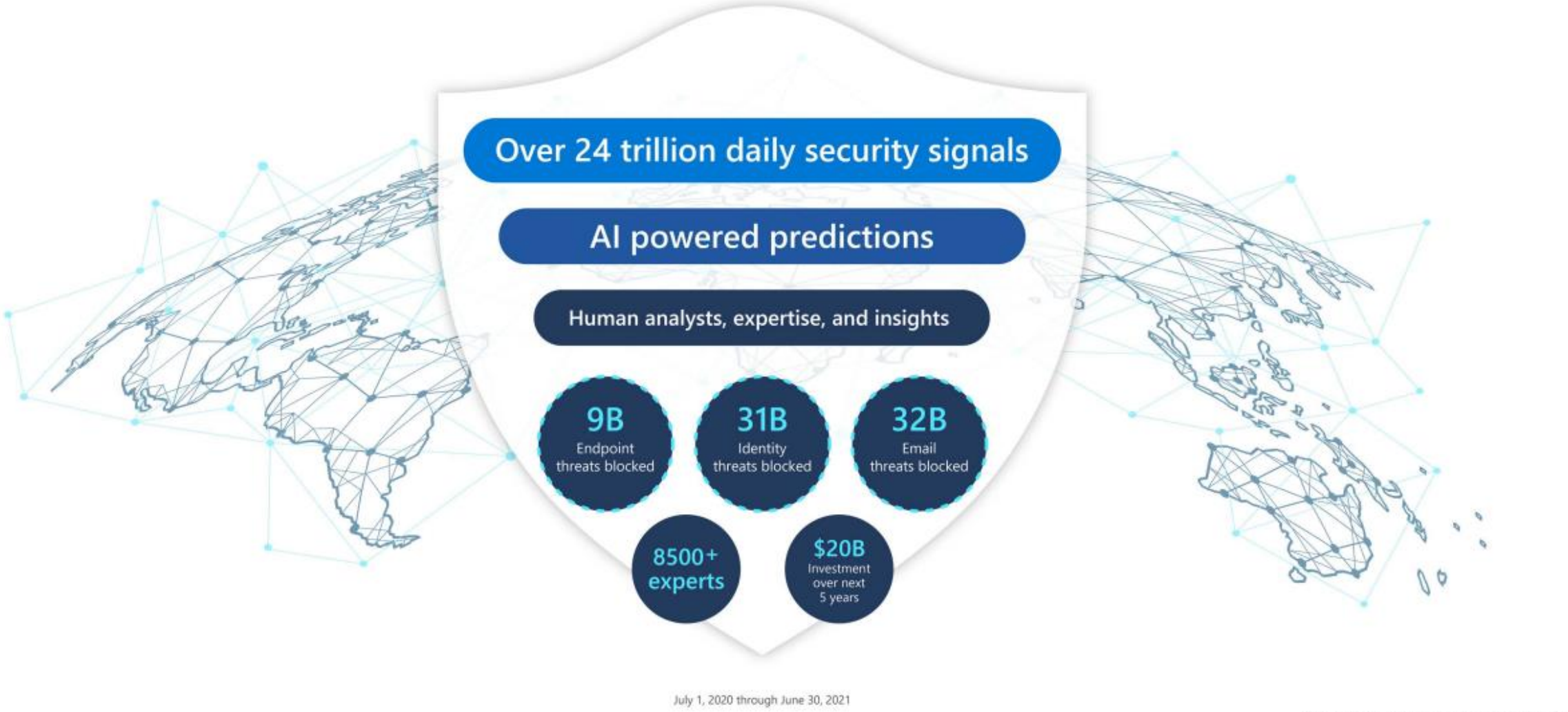
¿Cuentas actualmente con una solución de seguridad 360 que permita mitigar al máximo las amenazas informáticas?

Microsoft Defender





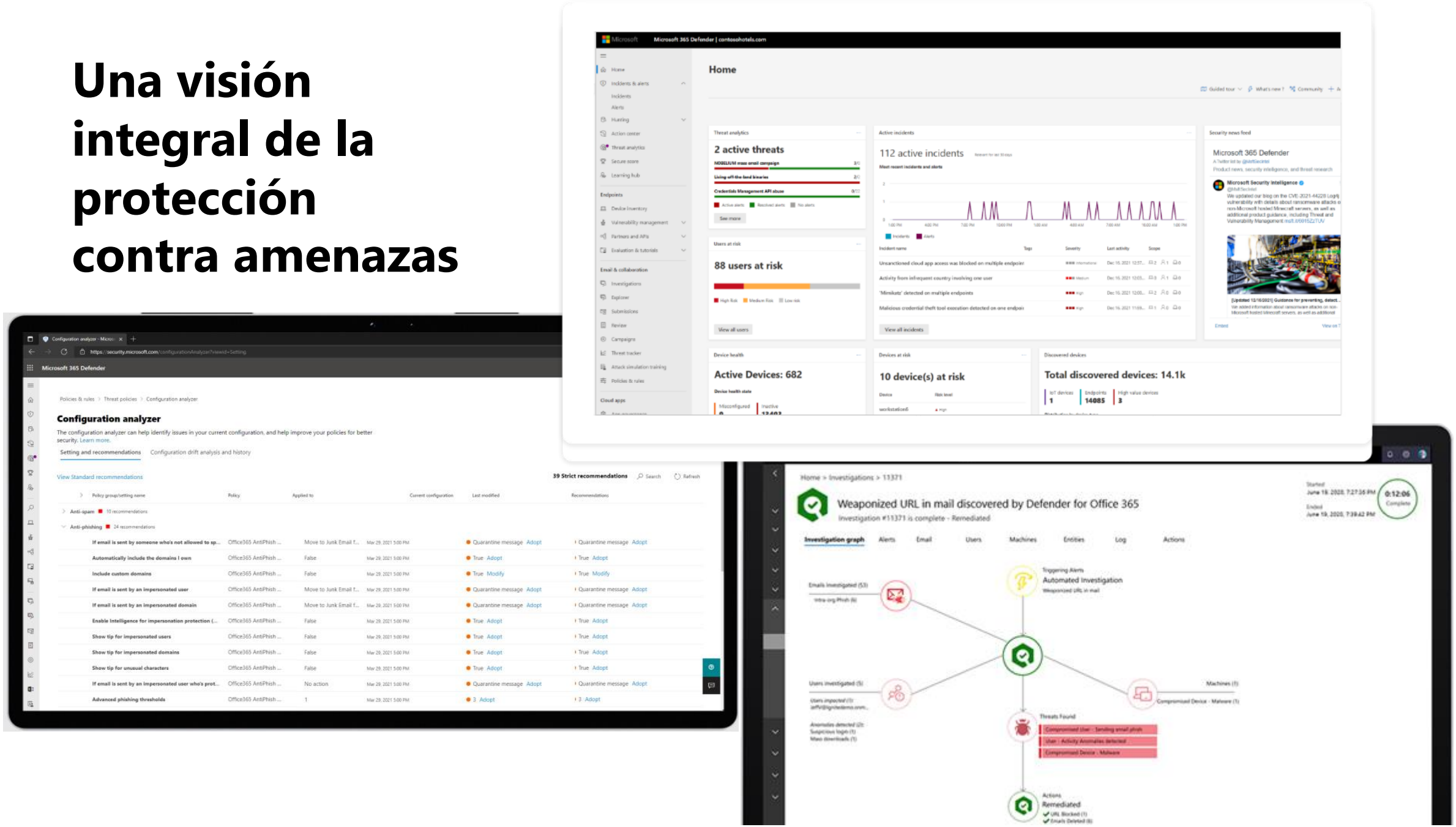
Señales de seguridad de Microsoft Volumen y diversidad de señales procesadas por Microsoft



Microsoft Defender for office 365

INTELIGENCIA SOBRE AMENAZAS

Una visión integral de la protección contra amenazas



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

OFFICE ADVANCED THREAT PROTECTION

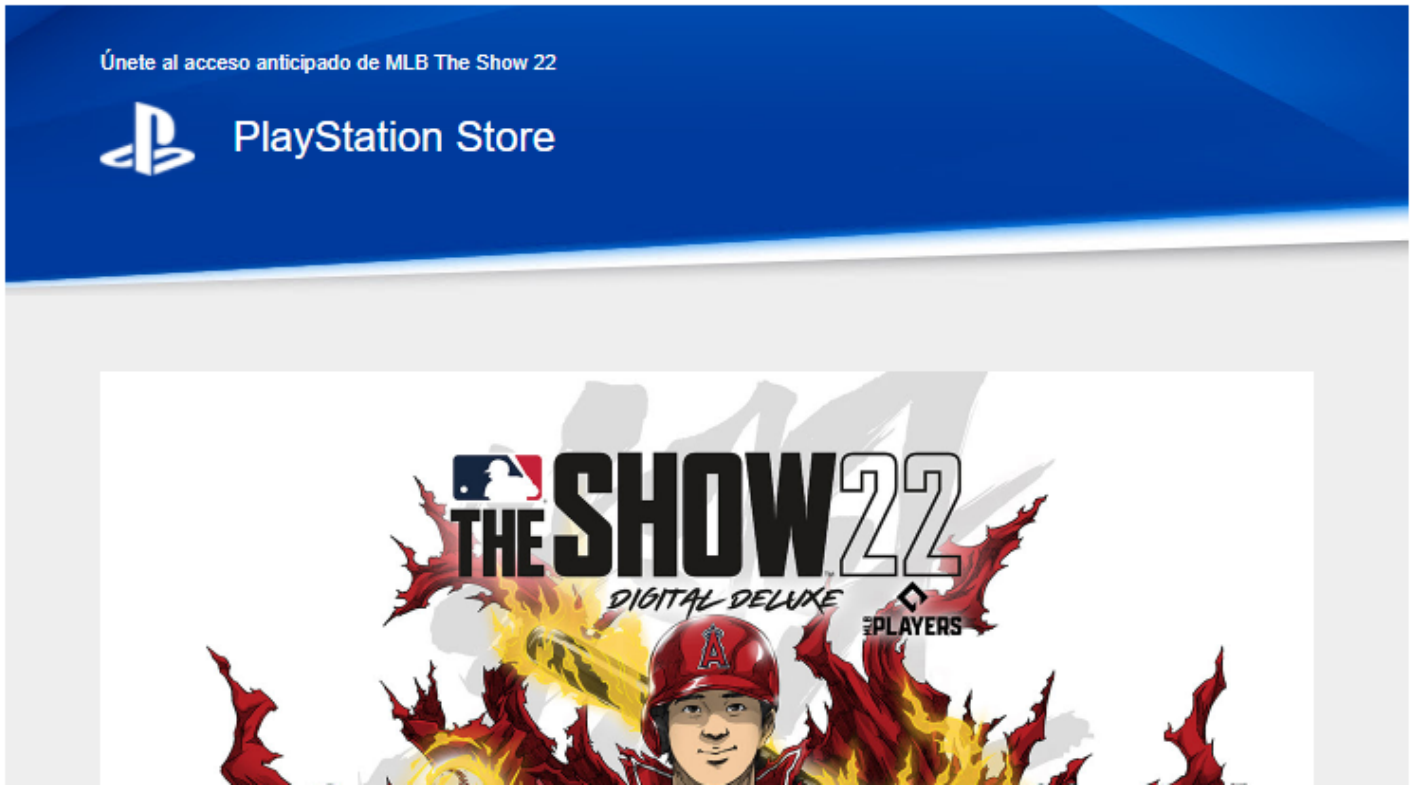
- PROTECCION FRENTE A VINCULOS MALINTENCIONADOS
- PROTECCION CONTRA DATOS ADJUNTOS PELIGROSOS
- PROTECCION DE BUZONES
- INFORMES

OFFICE ADVANCED THREAT PROTECTION

- **PROTECCION FRENTE A VINCULOS MALINTENCIONADOS**

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

PlayStation <email@email.playstation.com> Anular suscripción mié, 23 mar, 20:11 (hace 10 horas)
para mí



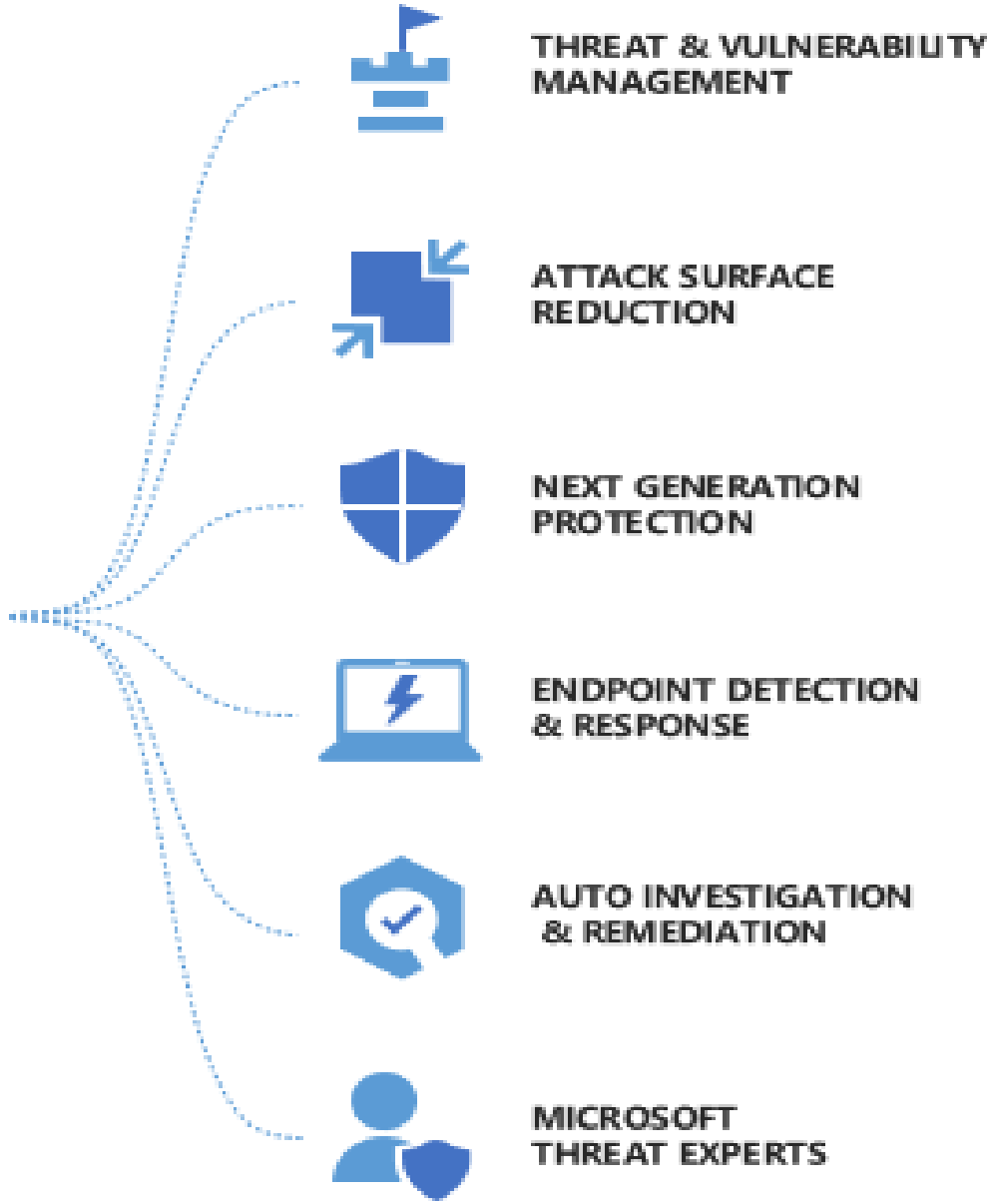
OFFICE ADVANCED THREAT PROTECTION

- **PROTECCION FRENTE A VINCULOS MALINTENCIONADOS**

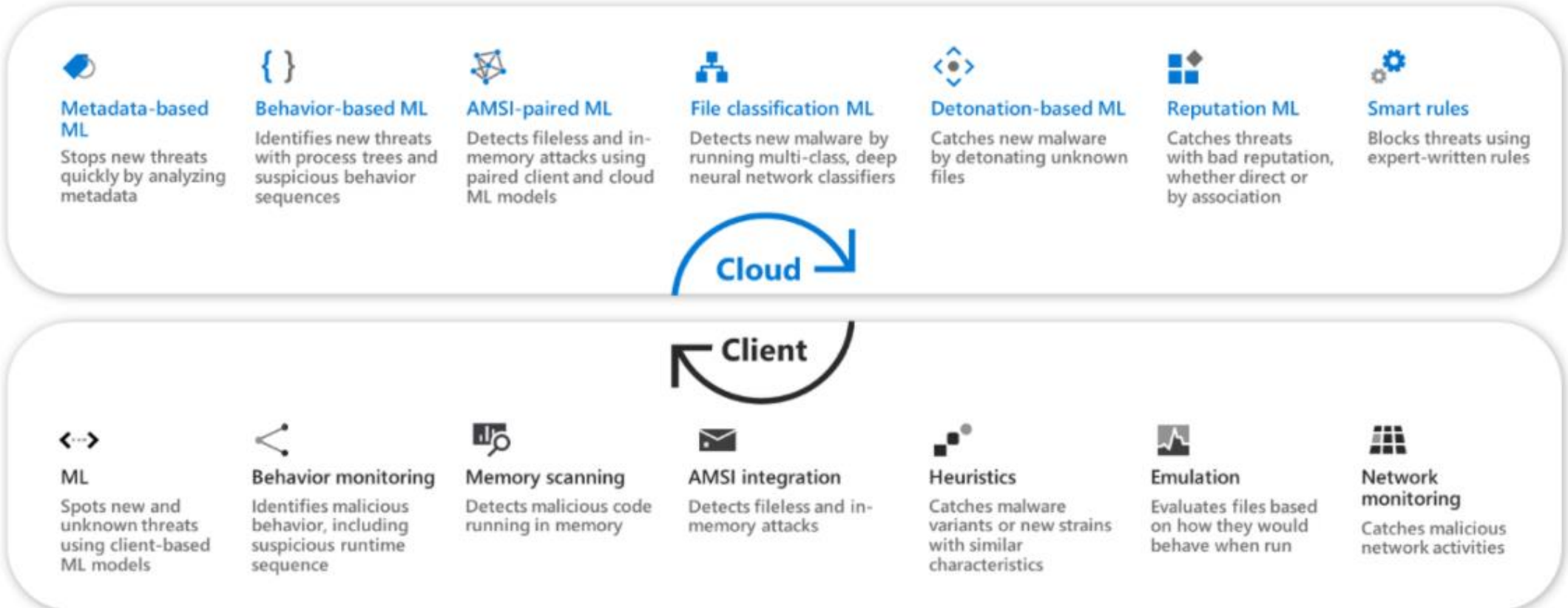
```
Delivered-To: mbetanco82@gmail.com
Received: by 2002:a05:6512:10c1:0:0:0:0 with SMTP id k1csp3092686lfg;
        Wed, 23 Mar 2022 18:11:20 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJyb53c1MJAFK1VN9pC/X2xSBKLqqZIw2V1IcwnRHy19+/krSspwSOdBB/WNe272U18arxCM
X-Received: by 2002:a05:6214:2467:b0:441:406d:b007 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/2yHv13POJEtB+RVJVMOUJBlX2u/GvaRLJJOK40YzDuUTjf+n0XvNyk
         rBuCXH1HqnDjAWGHih+5zDkGVbjgI4cNfTu1Qv0yQbF4A/RXcpwZjpou57BkrTopYfId
         yYh2M7UmfwEiZttzm4mfemt3QpzDLvrSw5FfdCqrc/kOW9nNiSV/oEShhspOhAjCDSvY
         VHfPPF0DKCnDgSVAFGimuEjnjoShe6Z2AQS9Yfm68q5xKUUKPaUCKYrpIRdGZi1bOdR0
         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=m11mQqiq+qvD+epRUvFuclCg9+v9s7+qs/PMWujrvaQ=;
        b=ryWXKN/jTcWdtjMEeW6KdMHSgjEoYGVxvJpJoo3T1Iag8RBm7TbY2W6WdNHMQSHyiD
         KHPZ/zzq/IaPXYo1BaE8EJZro8uNP2qh9TuLRGCw0vKWVu8BQAmVcJnrz4LwjZUDGLr5
         ZM4Bg2TDkdXsQzOy70YkL0kn4LjRdZJlHatHfOQu4bMxV80Md2C/Hqye7qwXvukH6XQn
         Wy2YlgdSjNlFkaXikcPWejLteOM0z/gLId0YBW5Ak623cVfdy6ztd0tM414gAC6YI8pB
         2MJWg7noNZaHNgngBxPzBW7Jgl+HL2KpCNTbS/eGz0xL6LliEXM1zZPLXNWd18ETgoSn
         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;
```

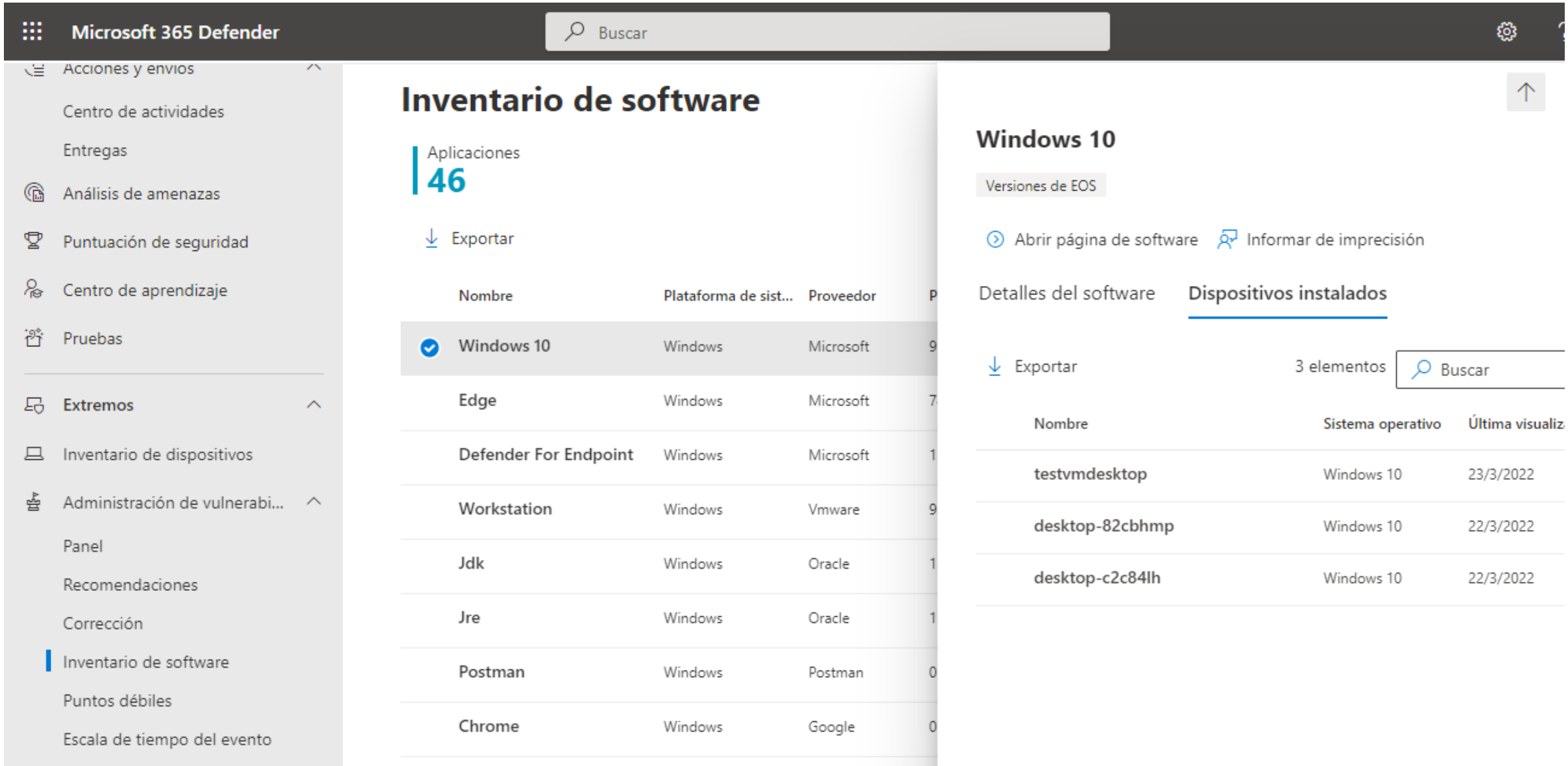
Microsoft Defender for Endpoint

Built-in. Cloud-powered.



Microsoft Defender ATP next generation protection engines




Microsoft 365 Defender
Buscar
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
Windows 10
Windows
Microsoft
Edge
Windows
Microsoft
Defender For Endpoint
Windows
Microsoft
Workstation
Windows
Vmware
Jdk
Windows
Oracle
Jre
Windows
Oracle
Postman
Windows
Postman
Chrome
Windows
Google
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 %

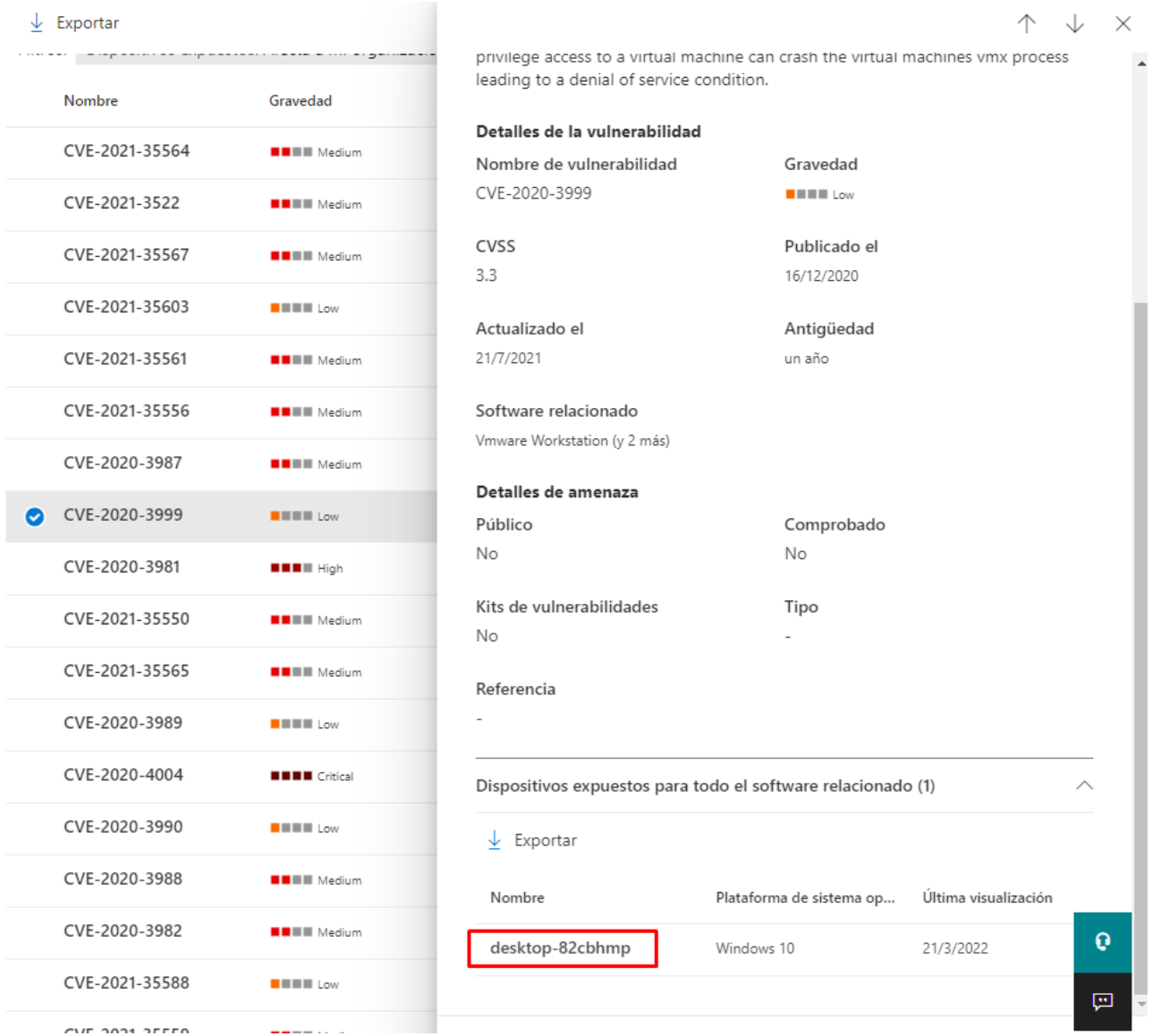
Esta puntuación refleja la postura de configuración de seguridad colectiva de sus dispositivos a través de los controles de seguridad del sistema operativo, de las aplicaciones, de la red y de las cuentas. La puntuación puede quedar afectada por excepciones activas.

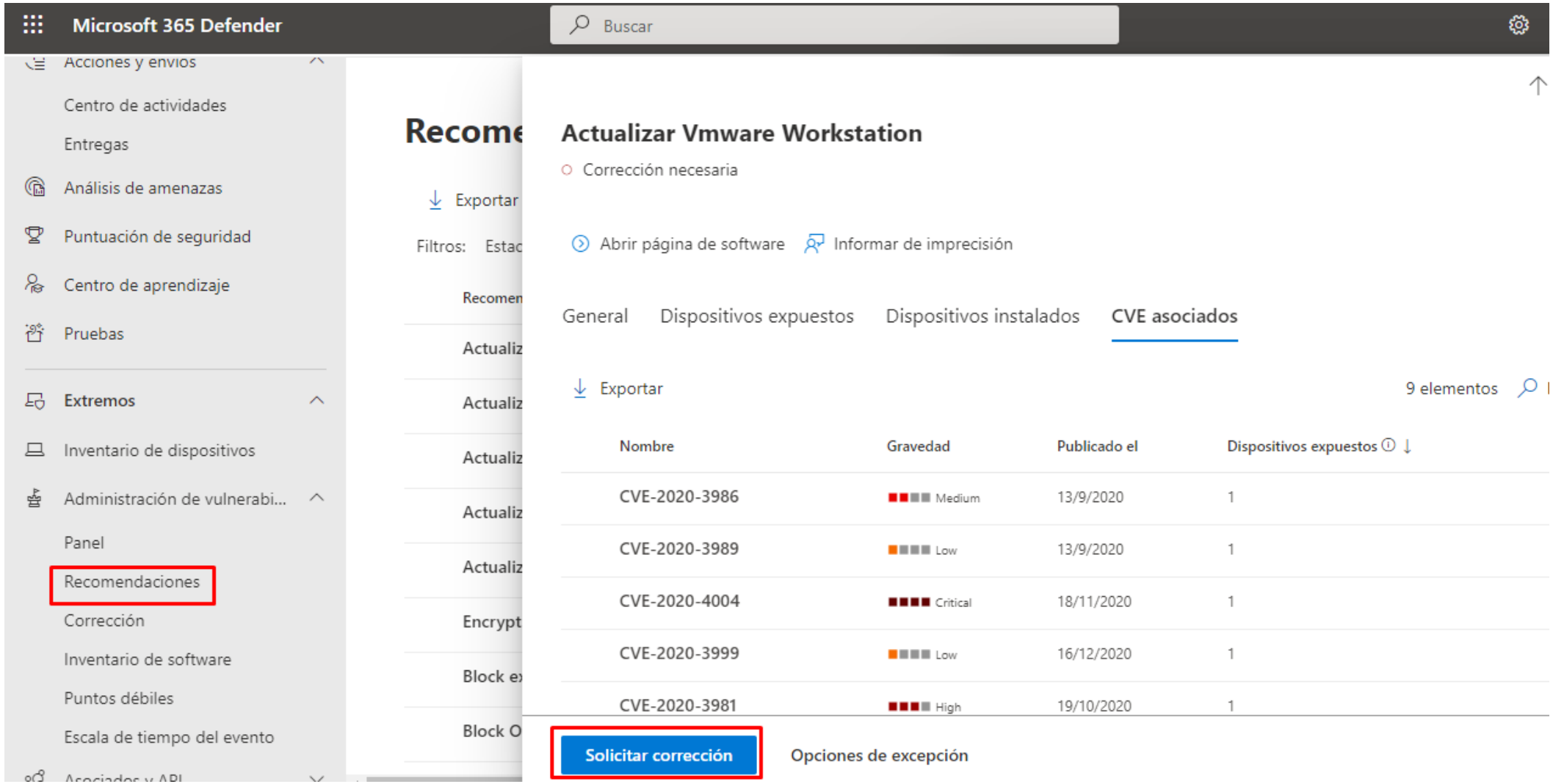
356/782 puntos obtenidos

Application	**10**/37
OS	**59**/167
Network	**50**/93
Accounts	**36**/71
Security controls	**201**/414

Puntuación para dispositivos a lo largo del tiempo

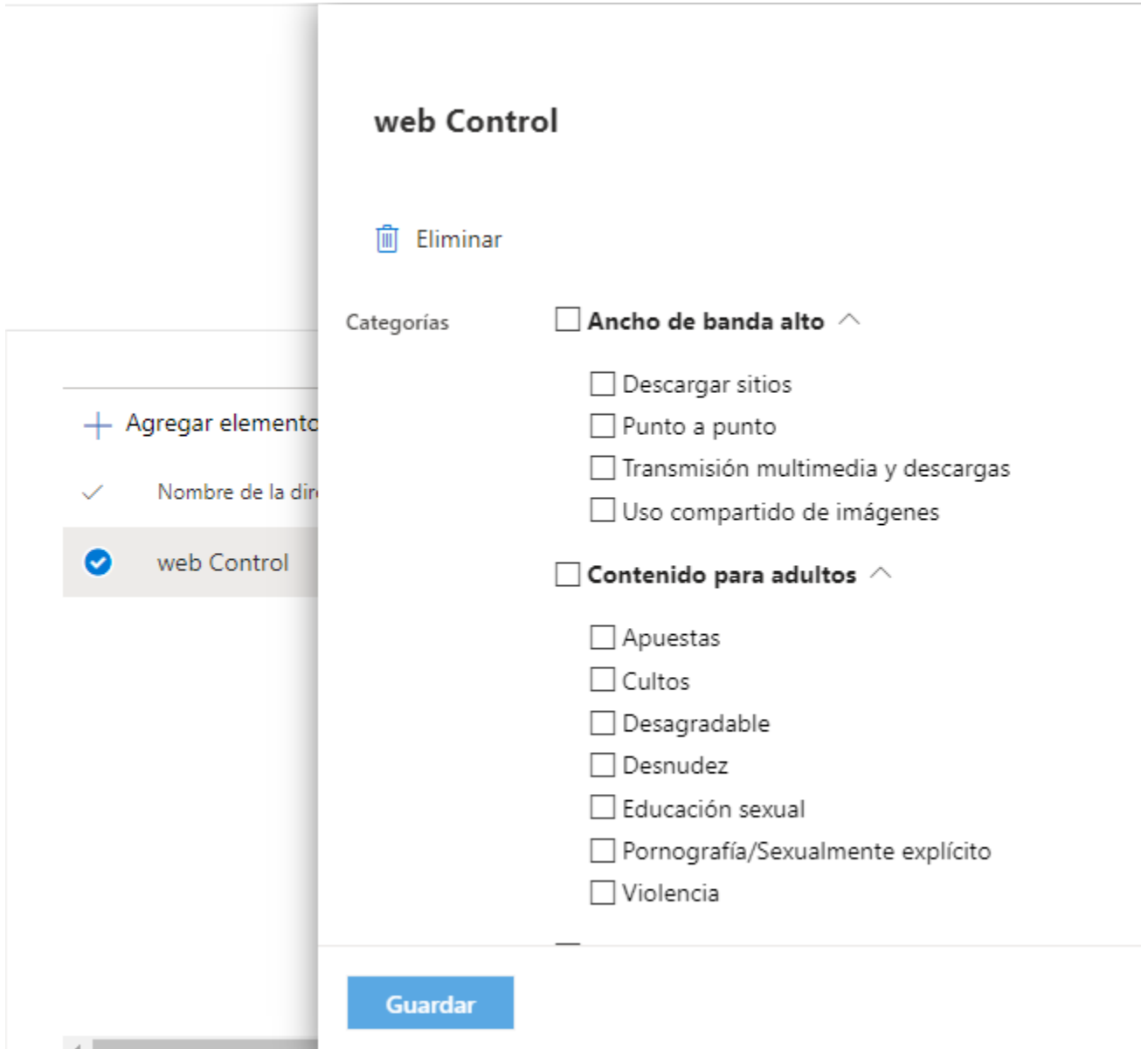
Mejorar puntuación


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
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
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
CVE-2020-3999
Gravedad
Low
CVSS
3.3
Publicado el
16/12/2020
Actualizado el
21/7/2021
Antigüedad
un año
Software relacionado
Vmware Workstation (y 2 más)
Detalles de amenaza
Público
No
Comprobado
No
Kits de vulnerabilidades
No
Tipo
-
Referencia
-
Dispositivos expuestos para todo el software relacionado (1)
Exportar
Nombre
Plataforma de sistema op...
Última visualización
desktop-82cbhmp
Windows 10
21/3/2022

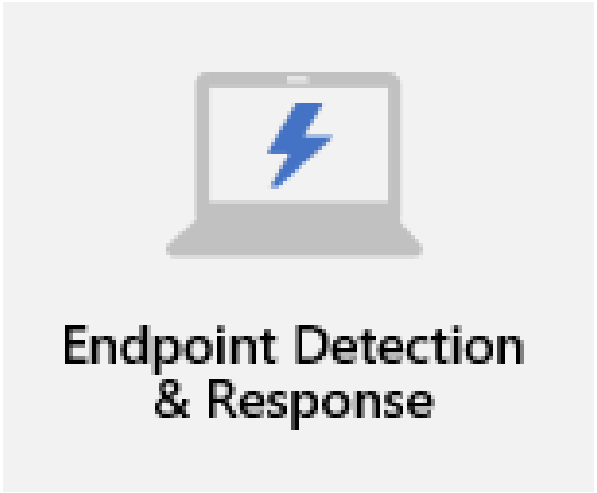

Microsoft 365 Defender
Buscar
Acciones y envíos
Centro de actividades
Entregas
Análisis de amenazas
Puntuación de seguridad
Centro de aprendizaje
Pruebas
Extremos
Inventario de dispositivos
Administración de vulnerabi...
Panel
Recomendaciones
Corrección
Inventario de software
Puntos débiles
Escala de tiempo del evento
Recome
Exportar
Filtros:
Actualiz
Encrypt
Block ex
Block O
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

Attack Surface Reduction



Microsoft Defender for End point



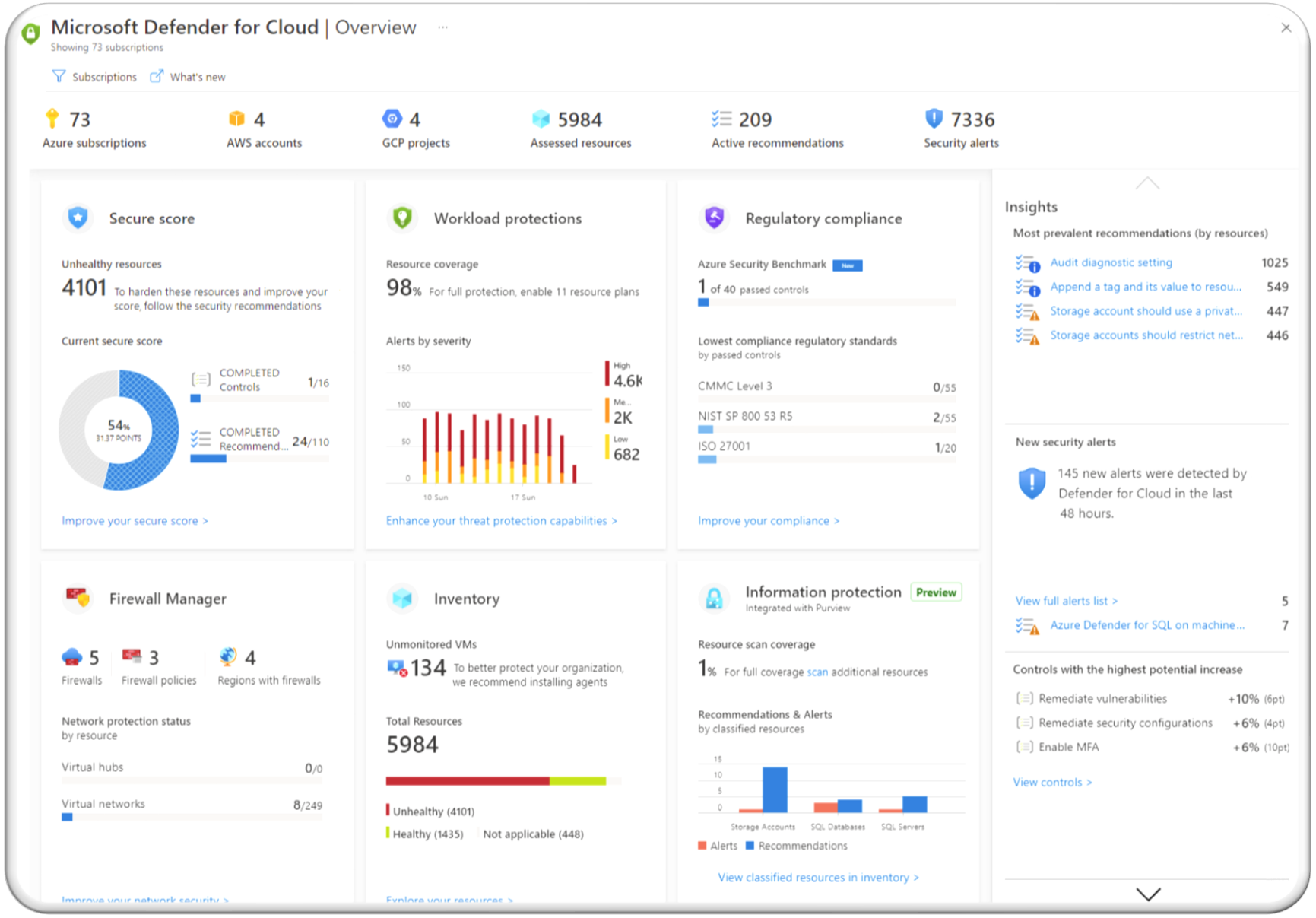
Microsoft Defender for End point

Microsoft Defender for End point

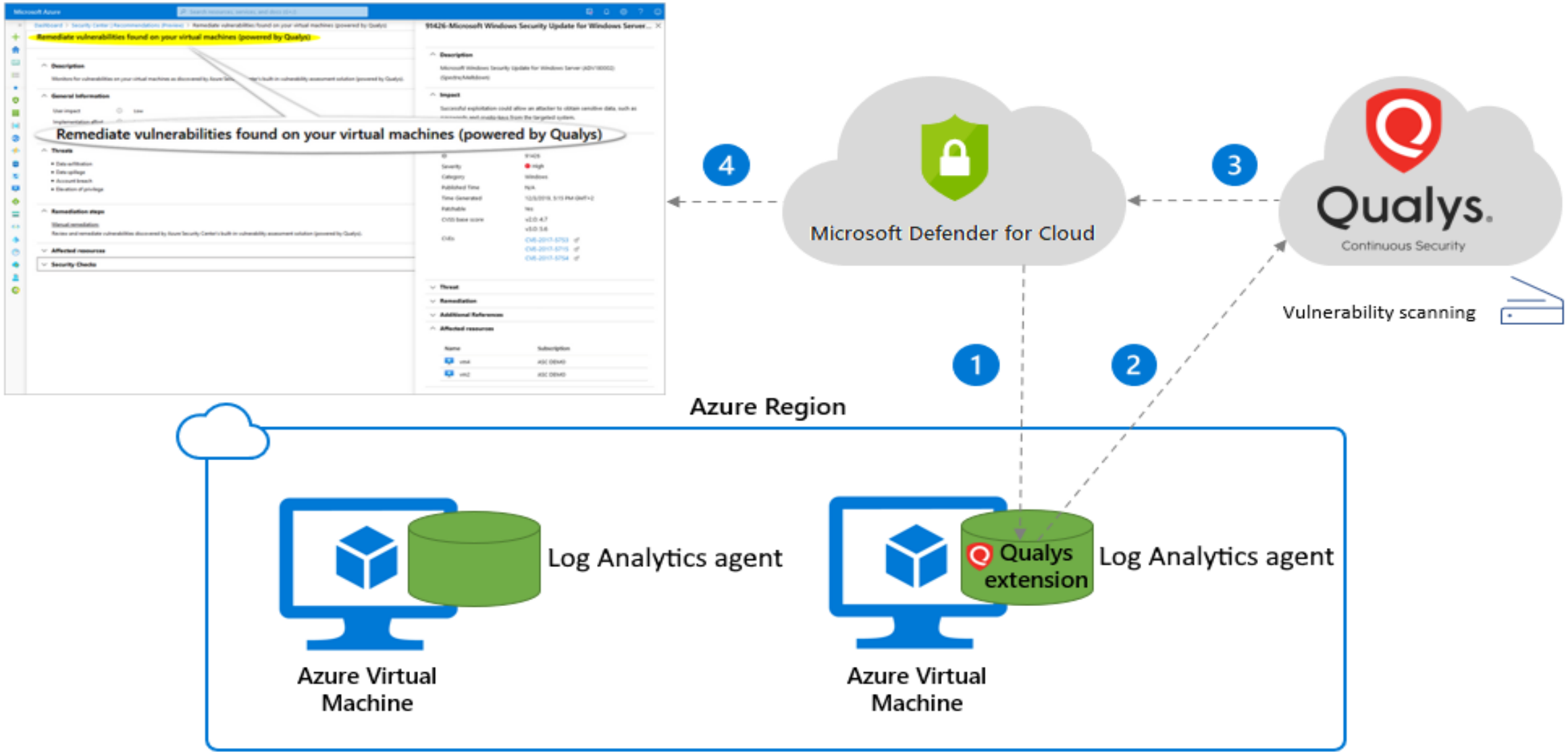
Microsoft Defender calificó consistentemente como el mejor AV

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

Microsoft Defender for Cloud



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