WINDOWS DEFENDER
ADVANCED THREAT PROTECTION (**ATP**)

Un servicio que permite que los clientes empresariales **detecten, investiguen y respondan frente a ataques avanzados y dirigidos** en sus redes.

200+
días
el tiempo que los atacantes están presentes en la red de la víctima antes de la detección
Fuente: https://www2.fireeye.com/ATA

80
días
después de la detección hasta la recuperación total
Fuente: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/why-senior-leaders-arethe-front-line-against-cyberattacks

$3
billones
el impacto por pérdidas en la productividad y el crecimiento
Fuente: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/why-senior-leaders-arethe-front-line-against-cyberattacks

$3.5
millones
costo promedio de violación de datos (15% de aumento año tras año)
Fuente: https://www.ponemon.org/blog/ponemon-institute-releases-2014-costof-data-breach-global-analysis

Windows 10 es la **plataforma empresarial más segura** de la actualidad

Teniendo en cuenta las defensas de seguridad existentes hoy en Windows 10 (pre-ataque), desarrollamos Windows Defender Advanced Threat Protection (ATP), que ofrece a las empresas una capa de protección para implementar después de los ataques en la pila de seguridad de Windows 10.

Windows Defender Advanced Threat Protection

Proteger
El mundo actual, que privilegia la nube y la movilidad, exige el más alto nivel de identidad y seguridad para los datos.

Detectar
Herramientas integrales de monitoreo que ayudan a detectar anormalidades y responder a los ataques con mayor velocidad.

Responder
Tecnologías líderes para respuesta y recuperación, además de la mejor experiencia en consultoría.

Proteger a nuestros clientes empresariales nunca fue un desafío tan grande

Con el tiempo, hasta las mejores defensas para terminales se verán vulneradas por ciberataques, ya que éstos son cada vez más sofisticados y dirigidos. Este tipo de atacantes utiliza la ingeniera social, vulnerabilidades de día cero o hasta errores en la configuración para entrar en las redes.

MALWARE Y VULNERABILIDADES
no son las únicas preocupaciones

46%
de los sistemas comprometidos **no tenían malware**

99.9%
de las vulnerabilidades aprovechadas se usaron **más de un año después** de que se publicara el CVE

LOS ATAQUES VELOCES DE PHISHING
ofrecen poco tiempo de reacción

23%
de los receptores **abrieron mensajes de phisin**g (el 11% hicieron clic en los adjuntos)

50%
de los que abren y hacen clic en adjuntos lo **hacen en la primera hora**

SOLO 40%
DE LOS ATAQUES
utilizan malware como medio para llevar a cabo los objetivos de los atacantes. El resto está conformado por actividades perjudiciales que no utilizan malware para el cual se pueda insertar una firma. La mejor manera de detectar estos ataques es a través del análisis de comportamiento.

Fuente: Ponemon Institute, "The Post Breach Boom", 2013.
Ponemon Institute, "Informe Global 2014 sobre los costos de los ciberataques". Mandiant 2014 Threat Report Defender

Por qué **Windows Defender ATP**

Windows Defender ATP ofrece la capacidad de detectar, investigar y remediar ataques avanzados y violaciones de datos en sus redes.

Detectando lo indetectable
Sensores desarrollados en lo profundo del núcleo del sistema operativo, expertos en seguridad de Windows, y visión única de más de mil millones de máquinas y señales en todos los servicios de Microsoft.

Incorporado, no añadido
Sin agentes, con alto desempeño y bajo impacto, impulsado por la nube; fácil administración sin ningún tipo de despliegue.

"Single pane of glass" para seguridad en Windows
Explore 6 meses de valiosa línea de tiempo que unifica los eventos de seguridad de Windows Defender ATP, Windows Defender Antivirus y Device Guard.

El poder del gráfico de Microsoft
Aproveche el gráfico de seguridad de inteligencia de Microsoft e integre la detección y exploración con suscripción a Office 365 ATP para rastrear y responder a los ataques.

Windows Defender ATP tiene tres partes:

El cliente
El cliente registra los eventos y comportamientos de seguridad relevantes desde la terminal, utilizando el sensor de comportamiento de la terminal, integrado en Windows 10 (actualización de Windows 10 Anniversary, Windows Insider Preview Build número 14332 y posteriores) y activado al momento de la inscripción al servicio.

Servicio de análisis en la nube
El servicio de análisis en la nube se ejecuta en la plataforma de Big Data escalable de Microsoft y utiliza una combinación de indicadores de ataques (IOAs), análisis genérico y reglas de aprendizaje automático, así como indicadores de compromisos (IOC) reunidos en ataques anteriores. Procesa datos de terminales junto con datos históricos, más el amplio repositorio de datos de Microsoft para detectar comportamientos anómalos, técnicas de adversarios y similitudes con otros ataques conocidos.

Microsoft e inteligencia colaborativa
Nuestros especialistas e investigadores estudian los datos, buscando patrones de comportamiento nuevos y correlacionando esos datos con conocimiento existente de la comunidad de la seguridad.

PASE A LA OFENSIVA CONTRA ATAQUES CIBERNÉTICOS PROTEGIENDO A SU EMPRESA CON
WINDOWS DEFENDER ATP

Más infromación: : **aka.ms/windows-atp**

Microsoft