Work safer. Live safer.

DesktopToWork Security

DESKTOP TO WORK

DesktopToWork **Security**

Una suscripción a la seguridad

Cada vez más, los negocios son más digitales y estamos constantemente en línea. No podemos imaginarnos una vida sin Internet. Sin embargo, trabajar digitalmente no solo ofrece comodidad, sino que también conlleva riesgos. Es por eso que DesktopToWork ofrece la mejor seguridad para tu organización.

El mundo digital atrae a delincuentes, piratas informáticos y personas no deseadas. Constantemente buscando oportunidades para robar a personas y organizaciones, roban tu identidad (digital), cometen fraudes o simplemente buscan querer avergonzarte. Es por eso que la ciberseguridad es de suma importancia.

En DesktopToWork ayudamos a las organizaciones a aumentar su seguridad. Con un enfoque exhaustivo, investigamos y analizamos las vulnerabilidades digitales. A través de las herramientas de software adecuadas y el conocimiento avanzado relacionado con las amenazas cibernéticas, combatimos potenciales peligros.

En este folleto, echamos un vistazo detallado a la seguridad de los datos digitales y la seguridad cibernética. También proporcionamos una definición detallada de lo que realmente significan estos términos y cómo DesktopToWork puede proteger su información digital.

Citrix Partner Service Provider

Microsoft Tier-1 Cloud Soultions Provider

Gold Microsoft Partner

Cisco Select Partner

ISAE 3402 CERTIFIED

Management System Certificate DNV ISO 27001

DESKTOP TO WORK

Contacto

+34 93 271 16 44
info@desktoptowork.com
www.desktoptowork.com

Carrer de la Marina 16-18, Mapfre Tower,
Barcelona 08005, España

DTW Security

Empecemos con lo básico. ¿Qué es la seguridad digital?

La seguridad de los datos digitales es el término utilizado para proteger la identidad y la seguridad en línea de un negocio o persona, así como datos personales o financieros. Con la ayuda de soluciones de gestión de identidades y accesos, seguridad biométrica, y también mediante un sólido plan de copias de seguridad podemos protegernos contra los ciberataques. Además, es muy importante que las personas obtengan una correcta educación y que sean conscientes de los peligros potenciales que hay en Internet.

¿Cuál es la diferencia entre seguridad de datos digitales y ciberseguridad?

Es probable que haya oído hablar del término "ciberseguridad". Sin embargo, existe una diferencia entre la seguridad de los datos digitales y la ciberseguridad.

La seguridad de los datos digitales incluye la protección de la identidad en línea, y el acceso a los datos, así como todos tus datos personales y financieros.

La ciberseguridad cubre varias áreas. Protege toda la red, sistemas informáticos y otros componentes digitales y los datos almacenados en ellos.

Por lo tanto, la seguridad de los datos digitales protege la información. La ciberseguridad protege la infraestructura, los sistemas, las redes y la información.

Entonces, ¿Por qué es tan importante la ciberseguridad?

Recientes estudios muestran que más de 7 millones de sistemas son atacados con éxito todos los días y que la cantidad de incidentes de malware ha incrementado en 358% y los ataques ransomware aumentó un 435% en 2020.

En 2021, 6 organizaciones por minuto fueron víctimas de un ataque de ransomware y hubo 1,095 ataques DDoS (denegación de servicio). De media, el crimen digital organizado costo más de 1.7 millones de dólares por minuto.

El valor que ofrece unas buenas prácticas sobre la ciberseguridad se traduce en menor riesgo y menores costes. Si implementamos un plan de contingencia robusto, los costes de un ataque se podrían ver reducidos desde un 65%.

Se prevé que los costes del cibercrimen aumentaran más de un 50% en los próximos dos años, superando así 1 trillón de dólares en perdidas.

¿Cuáles son nuestros módulos de ciberseguridad?

Hemos definido seis módulos relacionados con la ciberseguridad que representan las TIC. Además, creemos que analizar y optimizar continuamente la seguridad en línea es esencial. Las personas son, por lo tanto, el séptimo pilar.

Seguridad de redes

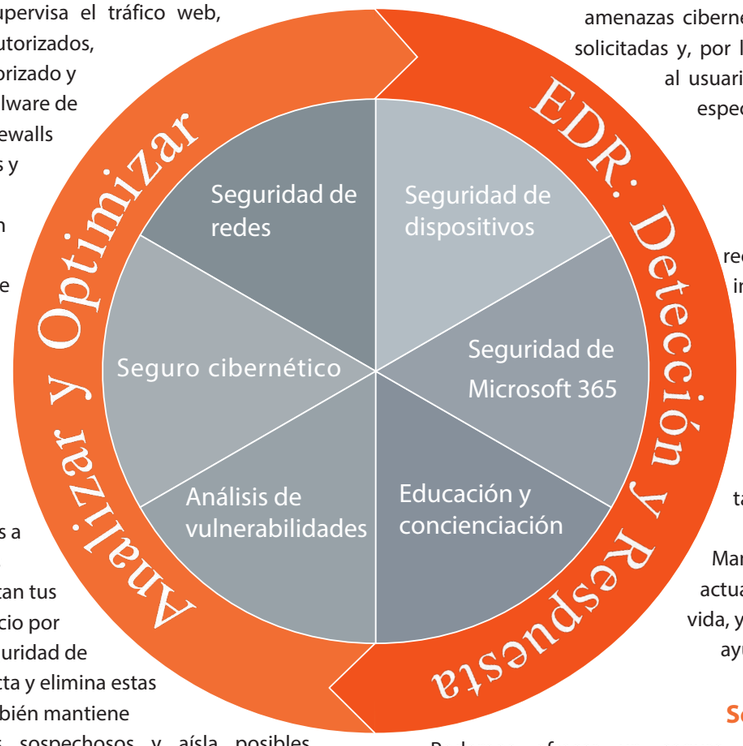
La seguridad de red (también conocida como seguridad perimetral) supervisa el tráfico web, identifica a los usuarios autorizados, bloquea el acceso no autorizado y protege contra virus y malware de última generación. Los firewalls han existido durante años y son esenciales para la seguridad empresarial. Un firewall NextGen es un dispositivo increíblemente útil para mantener alejados a los usuarios no deseados y las amenazas de red.

Seguridad de dispositivos

Las amenazas propagadas a través de malware y otros sistemas maliciosos infectan tus datos y paralizan tu negocio por completo. Una buena seguridad de dispositivos no solo detecta y elimina estas infecciones, sino que también mantiene alejados los programas sospechosos y aísla posibles amenazas. Ofrecemos soporte a todo tipo de dispositivos. Estos pueden ser servidores y ordenadores portátiles, pero también dispositivos móviles y dispositivos virtuales dentro de la red.

Seguridad de Microsoft 365

Con la ayuda de Microsoft Defender y Microsoft Azure, garantizamos una seguridad muy completa de todas tus aplicaciones en la nube y dispositivos. Proporcionamos autenticación multifactor (MFA) y nos aseguramos de que tu identidad digital esté protegida. Además, con la herramienta de Microsoft Compliance, podemos calificar y asegurar la información de tu organización en función de su importancia.



Educación y concienciación

¡Un buen ambiente comienza contigo mismo! Y en este caso con los usuarios de los diversos sistemas TIC dentro de una organización. A través de la educación periódica a corto plazo con la ayuda de e-learning, folletos y horas de preguntas, ayudamos a los usuarios finales a armarse mejor contra las amenazas externas. Ser capaz de reconocer e ignorar las amenazas juega un papel importante en esto. Además, podemos «simular» amenazas cibernéticas solicitadas y no solicitadas y, por lo tanto, proporcionar al usuario final conocimientos específicos si es necesario.

Análisis de vulnerabilidades

Es el módulo donde recogemos y analizamos información que pueda vulnerar tu negocio. Con herramientas automatizadas, somos capaces de proteger tu entorno a casi tiempo real y también corregimos las vulnerabilidades. Mantener tu organización actualizada es tu seguro de vida, y en DesktopToWork te ayudamos a conseguirlo.

Seguro cibernético

Podemos ofrecer un seguro cibernético para tu organización, puedes transferirnos la responsabilidad de tu empresa por daños sufridos por terceros (como un ataque cibernético), incluyendo los daños consecuentes al ataque. Estos riesgos digitales pueden consistir en la pérdida de datos debido a la piratería, pero también la pérdida o el robo de, por ejemplo, ordenadores portátiles, tabletas o memorias USB. La gestión de los daños en nombre del asegurado y los gastos de defensa y asistencia jurídica también están asegurados.

Ilustración: Los seis pilares de DTW Security

Seguridad de redes

Debido a un inmenso crecimiento del tráfico en Internet en los últimos años, también ha habido un crecimiento de ciberdelincuentes que quieren aprovecharse de las vulnerabilidades. Esto hace que el despliegue y mantenimiento de una red segura sea obligación.
En DesktopToWork empleamos equipos de red de última generación (NGFW) que ofrecen muchas funcionalidades y características que te mantendras protegido. Ofrecemos soluciones de ciberseguridad con un método perimetral, estableciendo diversas líneas de defensa y llegando a segurizar las redes de tu organización, datos empresariales, identidades y accesos, entre otros.

Funcionalidades extra

Mientras que un firewall estándar filtra el tráfico entrante y saliente de una red en función del puerto del Protocolo de Internet y las direcciones IP, un firewall NextGen agrega funciones adicionales. Mediante la inspección inteligente del tráfico de paquetes de red, nuevas solicitudes de conexión que pueden asociarse con posibles amenazas cibernéticas. Las características adicionales que ofrece el equipo de red de última generación incluyen seguridad para aplicaciones, prevención de intrusiones y capacidades de prevención de amenazas más avanzadas, como malware y acceso no autorizado.

Prevención de robos

Con IDS, que significa sistema de detección de intrusos, puede establecer reglas para el tráfico que está y no está permitido en la red. Esto no es un lujo superfluo porque cada red es un posible objetivo para los atacantes. Por eso es importante que podamos detectar los ataques con anticipación (detección y prevención). Todas las amenazas conocidas, como el malware, se almacenan en una base de datos.

Los equipos NextGen se actualizan diariamente para qué las amenazas más nuevas se prevengan.

Protección avanzada contra malware

No basta con bloquear el malware. Es importante obtener una imagen completa del tráfico total de la red. Advanced Malware Protection (AMP) comprueba cada archivo descargado en una base de datos de malware y bloquea automáticamente las amenazas ya conocidas. Sin embargo, también puede determinar en un momento posterior que un archivo ha resultado ser una amenaza. Esto es posible porque todo el tráfico de la red es monitorizado y rastreado en una base de datos global. De esta manera, también se pueden tomar medidas con efecto retroactivo para contrarrestar la amenaza.

Análisis de malware con Threat Grid

Threat Grid analiza lo que está haciendo el malware potencial en la red y lo traduce en informes legibles. Para ello se utilizan 950 indicadores, que además imitan las acciones humanas.

Geolocalización en el firewall

La última generación de equipos de red también se puede utilizar para bloquear el tráfico en función del país de origen o el país de destino. Así que tienes la opción de bloquear todo el tráfico desde o hacia ciertos países. Por ejemplo, si su organización no necesita permitir el tráfico de Rusia o China, puede ajustarlo y bloquearlo fácilmente.

Filtrar contenido web

Con equipos NextGen podrás filtrar contenidos de forma avanzada. Se pueden filtrar por categorías o sitios web específicos para que ya no sean accesibles para los empleados en la red de la empresa.
Por ejemplo, juegos y apuestas en línea o sitios web para mayores de 18 años. Estos sitios web no solo son malos para la productividad, sino que también son conocidos por distribuir malware. Esto permite que los usuarios de su red continúen disfrutando de los beneficios de Internet, pero al mismo tiempo están protegidos contra contenido inapropiado o dañino sin comprometer la productividad.

Filtrado de búsquedas

Cuando un dispositivo intenta acceder a una página web, la dirección web se compara con una gran cantidad de URLs en una base de datos. Esto hace posible permitir el acceso a una URL específica a un sitio web, mientras se excluyen otras. Por ejemplo, se pueden agregar direcciones URL específicas a una lista blanca para que el filtro no las bloquee.

Monitorización e informes

La monitorización nos ayuda a reconocer retroactivamente incidentes no deseados y a trabajar proactivamente para proteger el entorno para futuros ataques.
Es muy importante saber exactamente lo que está sucediendo en tu red. Por eso te enviamos informes semanales o mensuales con todos los posibles ataques que han sido derrotados. El informe muestra en qué ubicación se encontraba, de qué país provino el ataque, qué tipos de ataques fueron e incluso a qué dispositivos y sistemas operativos se accedió con mayor frecuencia.

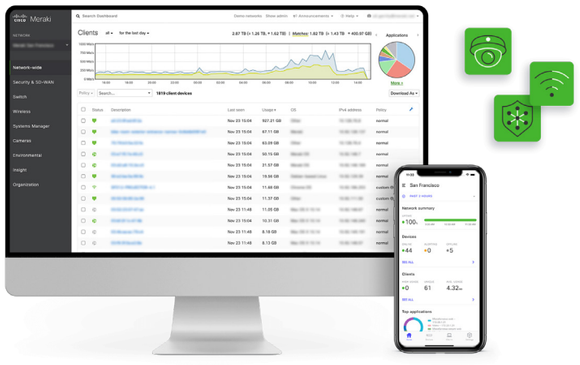


Ilustración: Portal de Meraki Firewall

Seguridad de dispositivos

Protección y administración de dispositivos

Si deseas evitar que los dispositivos de tu red, como PCs, portátiles y teléfonos móviles, corran un alto riesgo de convertirse en víctimas de ransomware, malware o correos electrónicos de phishing, necesitas una protección completa para todos los dispositivos. La única solución para proteger a tu organización y a tus empleados frente a robos, pérdidas y malas intenciones. Hoy en día, la seguridad de dispositivos, merece toda nuestra atención. DesktopToWork proporciona una solución de seguridad completa para dispositivos, los datos e identidades corporativas.

Datos más seguros

Cuando hablamos de datos, nos referimos a todo tipo de información sensible del negocio o los empleados. Es importante proteger la información digital, y esto empieza protegiendo los dispositivos por los cuales podemos acceder a dicha información. Con el Mobile App Management (MAM) de Microsoft podemos evitar accesos no deseados, descarga de archivos e incluso copiar y pegar contenido a aplicaciones externas.

El eslabón más débil

Un dispositivo suele ser el caballo de troya para muchos atacantes, suele ser el punto débil de una organización conjuntamente con la poca concienciación de los empleados sobre ciberseguridad. Por lo tanto, debemos blindar los dispositivos con la tecnología y herramientas de última generación, por ejemplo, el cifrado de discos con BitLocker, filtrar contenido web, y actualizaciones periódicas del software.

Todo esto está integrado en Mobile Device Managament (MDM) de Microsoft, creando una solución muy completa ante ataques a dispositivos en la red.

¿Qué es el ransomware?

Un ransomware (del inglés ransom, 'rescate', y ware, acortamiento de software) o secuestro de datos en español. Es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción.

Los incidentes de malware ha incrementado en 358% desde el último periodo. Más de 6 organizaciones por minuto son víctimas de estos ataques. La media del coste de un ataque ransomware en 2020 fue de 170,404 dólares.

La solución de DesktopToWork

En DesktopToWork ofrecemos una solución completa de seguridad para dispositivos. No solo detectamos y resolvemos ciberataques, sino que también observamos y analizamos el comportamiento de usuarios y archivos para prevenir posibles incidentes.

Zero Trust es una estrategia de seguridad basada en un proceso estricto de verificación de identidad, accesos y dispositivos, además de un componente de análisis y revisión proactiva. Es una estrategia muy robusta, y es por eso que nos hemos querido juntar con los mejores productos del mercado. Crowdstrike nos provee de un servicio de detección y respuesta (EDR) junto a una potente herramienta de Antivirus y Anti-Malware de última generación, además de un Security Operations Center (SOC) para proteger todos tus dispositivos.

¿Quieres saber más sobre nuestra solución?

- **Antivirus de última generación (NGAV)**

NGAV elimina las deficiencias de las soluciones antivirus tradicionales. NGAV verifica el sistema operativo y muchos más componentes, utiliza el aprendizaje automático ('machine learning' en inglés) y la inteligencia artificial. Entre otras cosas, NGAV analiza el comportamiento de los procesos y archivos y, por lo tanto, puede responder a ataques conocidos y desconocidos.

- **Detección y Respuesta (EDR)**

EDR proporciona una visión completa de la protección y las amenazas potenciales en los dispositivos, y puede intervenir de inmediato cuando sea necesario. El objetivo de EDR es monitorizar, analizar, identificar y prevenir continuamente ataques avanzados. Antes de que el malware se instale, ya podemos detectar dónde ha entrado, qué ruta ha tomado en la red y los dispositivos presuntamente infectados. EDR puede detenerlo a tiempo.

- **Centro de Operaciones de Seguridad (SOC)**

Además de todas las medidas de prevención que tomamos con NGAV y EDR, es importante estar activo 24/7 con monitorización y caza de amenazas. Un SOC es un equipo externo de especialistas en seguridad cibernética que no hace más que buscar vulnerabilidades y ataques.

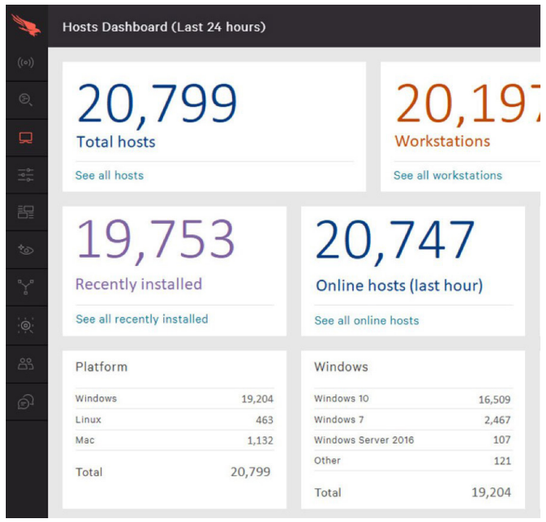
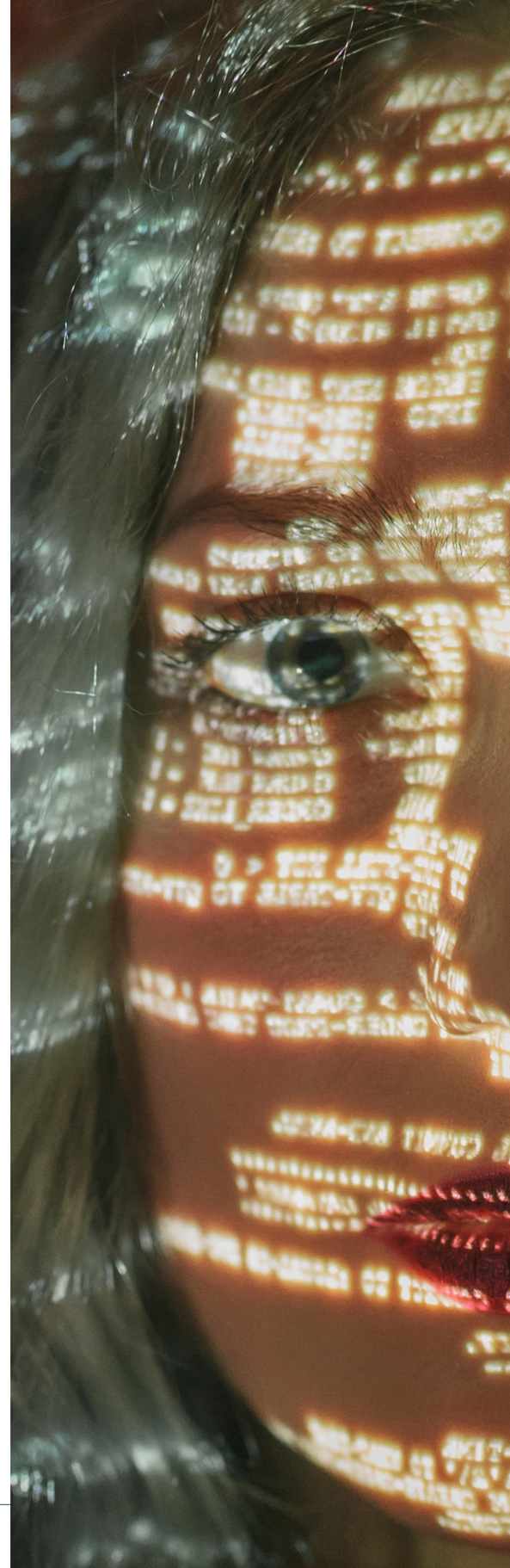


Ilustración: Portal de CrowdStike Falcon



Seguridad de Microsoft 365

Solución integrada para la seguridad en Microsoft 365

Microsoft 365 no solo es una herramienta colaborativa, es también el líder en seguridad. Los sistemas digitales están creciendo, asimismo, el número de cibercriminales está creciendo. Con Microsoft 365 Security and Compliance te ayudamos a protegerte.

Garantizamos una seguridad muy completa de todas tus aplicaciones en la nube. Proporcionamos autenticación multifactor y nos aseguramos de que tu identidad digital esté protegida. Además, con la ayuda de la gestión de cumplimiento, podemos calificar y asegurar la información en función de su importancia.

Solución integrada

Varios factores juegan un papel en la seguridad de tu entorno digital. Microsoft 365 ofrece una solución de seguridad integrada con Microsoft Defender for Endpoint, Office 365, Identity y Cloud Apps que permiten una vista general y especifica al mismo tiempo de las amenazas. También ofrecemos servicios en la nube para la protección y gestión de identidades y accesos a través de Azure Active Directory.
De esta forma se puede determinar cómo ha entrado una amenaza en el sistema, cuál es el impacto y qué consecuencias tiene para la organización. Para prevenir o detener ataques cibernéticos, las herramientas de Microsoft 365 y Azure AD toman medidas automáticamente.

Algunas funcionalidades de Microsoft 365

¿Para qué sirven exactamente las diversas funcionalidades de Microsoft 365 Security y qué pueden significar para tu organización? Enumeramos las partes más importantes:

Microsoft Defender for Endpoint

Esta es una plataforma de seguridad para puntos finales empresariales. Ayuda a las redes corporativas a prevenir y detectar amenazas avanzadas. Pero también para (automáticamente) investigar y responder a ellos. La plataforma verifica continuamente las vulnerabilidades y las configuraciones incorrectas, lo que permite una detección rápida de las vulnerabilidades de seguridad.

Defender for Endpoint utiliza sensores que recopilan y procesan señales de comportamiento del sistema operativo. Se analizan los datos de este sensor. Los conocimientos que esto genera contribuyen a una lucha eficaz contra las amenazas avanzadas.

Microsoft Defender for Office 365

Esta parte de Microsoft 365 protege a tu organización de amenazas como enlaces malintencionados (URL) o archivos adjuntos con programas dañinos, a través del correo electrónico, Teams, OneDrive o SharePoint. Podemos blindar el entorno del usuario con políticas antiphishing, pero también comprobar si hay indicios de malware, ransomware entre otros ataques. Tambien podemos proteger del spam en los correos electrónicos, que suelen ser una carga para los administradores, así como también la encriptación de correos electrónicos. Defender for Office 365 hace de él, un paquete de herramientas muy útiles con capacidad para prevenir y detectar amenazas, investigar y responder a estas.

Microsoft Defender for Identity

Es una solución de seguridad basada en la nube que aprovecha las señales de Active Directory local para identificar, detectar e investigar amenazas avanzadas, identidades puestas en peligro y acciones malintencionadas dirigidas a la organización por parte de usuarios internos.

Microsoft Defender for Cloud Apps

Con esta completa solución SaaS (software como servicio), tenemos mucho más control sobre el entorno en la nube y podemos identificar y combatir las ciberamenazas en todos sus servicios en la nube. Defender para Cloud Apps se integra de forma nativa con soluciones de Microsoft líderes y está diseñado pensando en los profesionales de seguridad.
Es un agente de seguridad de acceso a la nube que admite distintos modos de implementación, entre los que se incluyen la recopilación de registros, los conectores de API y el proxy inverso.

Protección de identidad de Azure AD (IAM)
Asegurar las identidades y el acceso al entorno empresarial es una parte esencial de la ciberseguridad. Utilizamos las múltiples funcionalidades de Microsoft Azure Active Directory (AAD), como por ejemplo, el acceso condicional.

El perímetro de seguridad moderno ahora se extiende más allá de la red de una organización, incluye tanto la identidad del usuario como la del dispositivo. Las organizaciones pueden usar patrones de accesos basados en identidades como parte de sus decisiones de control de acceso.

El acceso condicional investiga los accesos para tomar decisiones y aplicar las directivas de control de acceso de manera automatizada.

Multi Factor Authentication (MFA)

La configuración de MFA agrega una capa adicional de seguridad cuando iniciamos sesión en una cuenta de Microsoft 365.
Con MFA, las contraseñas son menos importantes. No solo ingresa una contraseña, sino también un código de verificación generado aleatoriamente que se envía a tu teléfono móvil o a través de una aplicación de autenticación.

Copias de seguridad de Microsoft 365

Además de todas las precauciones que tome para proteger su entorno de TI, por supuesto, siempre es necesario tener una buena copia de seguridad en caso de que algo salga mal. DesktopToWork ofrece una solución de copia de seguridad en la que se realiza una copia de seguridad del correo electrónico, OneDrive, SharePoint y Teams todos los días. Estas copias de seguridad se mantienen durante 1 año.

Educación y concienciación

La ciberseguridad empieza por una buena educación y concienciación.

¡Un entorno seguro comienza con las personas! Y en este caso, con los usuarios que tienen acceso a múltiple sistemas dentro de la organización. A través de una educación periódica (plataformas e-learning, folletos informativos, preguntas de examen y simulaciones) ayudamos a los usuarios finales a armarse mejor contra las amenazas externas. Ser capaz de reconocer, ignorar y reportar las amenazas juega un papel muy importante.
Es por eso que la educación y concienciación de la seguridad informática es una estrategia a futuro, maximizamos y garantizamos el retorno de tu inversión (ROI).

El factor humano

Una línea de defensa solo puede funcionar de manera óptima si también se tiene en cuenta el factor humano. Por lo tanto, los empleados son una parte importante de tu línea de defensa. Incluso si has pensado en implementar la mejor tecnología y las herramientas más sofisticadas del mercado, los ataques como los correos electrónicos de phishing o el ransomware aún pueden colarse. En ese momento, debes poder confiar en tus empleados para identificar una ciberamenaza y notificar a tu equipo de IT. Para eso, la formación y la concienciación es imprescindible.
Cada vez más, las organizaciones se dan cuenta de que este 'cortafuegos humano' juega un papel fundamental. Es más probable que los ataques cibernéticos se dirijan a los empleados, cada vez son más sofisticados y difíciles de identificar.

¿Qué es un cortafuegos humano?

Un firewall humano consta de un grupo de colaboradores que respaldan las defensas, observando activamente amenazas sospechosas en el entorno. Informan de todo lo que encuentran peligroso. Cuantos más empleados tengas a bordo, más fuerte puede volverse el cortafuegos humano.

La mayoría de las filtraciones de datos a menudo comienzan por un error de un empleado. Por eso es importante que sean conscientes de que es posible marcar la diferencia informando de actividades sospechosas directamente al equipo de seguridad. Los errores pueden ocurrir en cualquier momento, especialmente porque los vectores de ataque pueden ser complejos y sofisticados, pero con cursos y simulaciones que enseñen a las personas a identificar e informar toda actividad sospechosa, puede minimizar los riesgos de un ataque exitoso.

Más información sobre los ataques

Cuando los empleados comienzan a denunciar correos electrónicos que les parecen sospechosos, se obtiene una gran cantidad de datos. Las soluciones automatizadas basadas en inteligencia artificial y aprendizaje automático (del inglés, machine learning) permiten evolucionar dichas soluciones para mejorar la detección de amenazas, que a su vez necesitan tu atención inmediata.

Suscripción a formación empresarial

DesktoptoWork ofrece varios cursos de formación sobre seguridad en los que orientamos a tus empleados lo mejor posible en este ámbito.

Como hemos visto, Microsoft 365 Defender protege a tu organización contra las amenazas maliciosas a través del correo electrónico, los vínculos (URL) y otras herramientas de colaboración.

Prevenir. Detectar. Investigar.

Trabajamos con una ruta estandarizada para la gestión de posibles incidentes cibernéticos. Revisamos las capacidades de cada producto en lo que respecta a prevención, detección e investigación de amenazas.

Simulación de ataques

DesktopToWork ofrece una solución personalizada que ejecuta escenarios de ataque realistas en tu organización. Estos ataques simulados pueden ayudar a identificar y encontrar usuarios vulnerables antes de que un ataque real afecte tu entorno. Hemos separado la simulación de ataque en dos simulacros:

- **Campañas**
  Notificamos a la organización que está a punto de realizarse un simulacro.
  Lanzamos una serie de simulaciones de ataque. Observamos la actividad de la simulación.
  Tenemos como objetivo sensibilizar a los empleados durante un largo periodo de tiempo.
- **Ataque**
  Lanzamos una simulación de ataque realista sin previo aviso. Supervisamos la reacción en tiempo real de la simulación.
  Tenemos como objetivo identificar usuarios vulnerables y ayudarlos con formaciones específicas

Threat Explorer & Threat Trackers

Threat Explorer es una poderosa herramienta en tiempo real para ayudar a los equipos de operaciones de seguridad a investigar y responder a las amenazas.
Threat Trackers son widgets y vistas informativas que te brindan inteligencia sobre diferentes problemas de ciberseguridad que pueden afectar a tu empresa.

Algunos ejemplos de cursos que ofrecemos:

- Introducción a la conciencia sobre la seguridad informática
- Cómo reconocer ataques de phishing e ingeniería social?
- Como proteger mi lugar de trabajo
- Gestionar y mejorar la privacidad

Análisis de vulnerabilidades

Explorar vulnerabilidades

Como su nombre indica, identificamos las vulnerabilidades dentro de tu empresa con un análisis automatizado de vulnerabilidades. Hacemos un inventario de cómo funciona la infraestructura de IT y qué objetivos, dentro del contexto de tu organización, pueden ser interesantes para los criminales informáticos.
Escaneamos cualquier plataforma, con más de 60.000 dispositivos diferentes. La información recogida por este gran volumen de dispositivos nos ayuda a protegernos de manera más extensa y desde diferentes ángulos. También corregimos las vulnerabilidades.

Implementamos una solución de evaluación de vulnerabilidades estándar de la industria digital para los profesionales de la seguridad. Inteligencia de última generación, actualizaciones rápidas, una interfaz fácil de usar.

Fácil de implementar, fácil de usar

Una solución totalmente portátil que se puede implementar prácticamente en cualquier lugar. La creación de políticas es simple y solo requiere unos pocos clics para escanear una red corporativa completa.

Detección avanzada significa más protección

65000 CVE en nuestra base de datos, la mayor cantidad en la industria. Con Nessus, analizamos más tecnologías y descubrimos más vulnerabilidades.

Rentable para empresas de todos los tamaños

Para culquier porposito, proporcionamos un análisis completo de vulnerabilidades con evaluaciones ilimitadas.

Visibilidad precisa en tus redes

Con Nessus, identificamos las vulnerabilidades que necesitan atención con un análisis preciso y de alta velocidad, y destacamos qué vulnerabilidades deben abordarse primero.

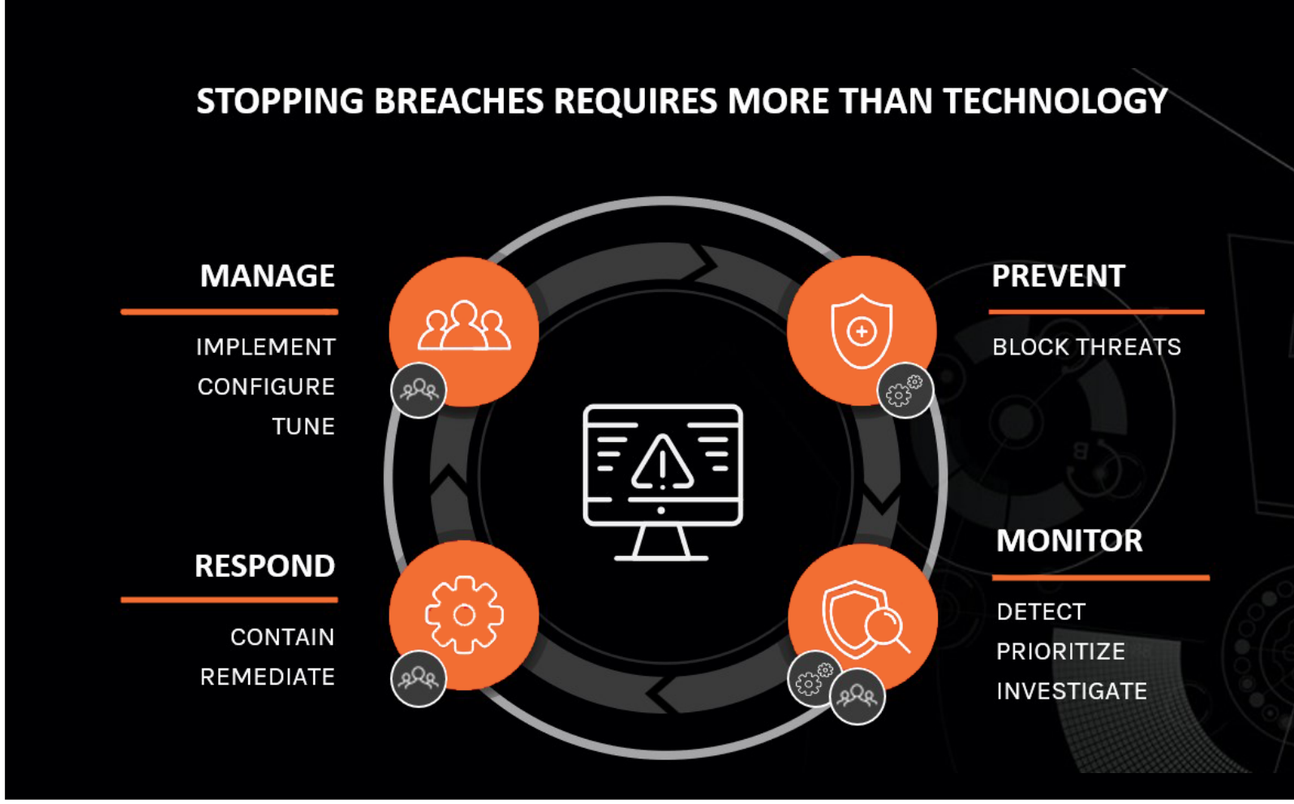
Protección contra ataques Zero-day

Un ataque de día cero (en inglés zero-day) es un ataque contra una aplicación o sistema que tiene como objetivo la ejecución de código malicioso gracias al conocimiento de vulnerabilidades que son desconocidas para los usuarios y para el fabricante del producto.

Aprovechamos nuestras fuentes de inteligencia para encuentrar y brindar protección contra estas amenazas de forma muy rapida.

Crecimiento y la escalabilidad

Con la operatividad en toda la cartera de productos de Tenable, migre fácilmente a Tenable.io, aproveche los conocimientos adicionales de Tenable.ot para su entorno industrial o combine las soluciones con el resto de Tenable a medida que aumentan sus necesidades de gestión de vulnerabilidades.



Los beneficios de un análisis de vulnerabilidades:

- Obten información sobre vulnerabilidades de tu entorno
- Identificamos y mostramos las prioridades claramente
- También corregimos las vulnerabilidades.
- Escaneamos cualquier plataforma, con más de 60.000 endpoints diferentes
- No es un análisis puntual, empleamos una monitorización continua.

Muchas organizaciones se centran en la prevención. Organizaciones maduras entienden que la ciberseguridad no es solo un proyecto, es un activo continuo y en desarrollo que no solo se centra en la tecnología, pero también en personas y el proceso.
En DesktopToWork tenemos un proceso muy comprometido con la seguridad informática y su continua evolución:

Administrar
El proceso de implementación, configuración y afinación de la tecnología. Nos apoyamos de profesionales y empresas líder en el sector.

Prevenir
La acción de prevenir, como ya sabemos, es muy importante en el proceso. Recopilamos mucha información sobre amenazas en la red para una rápida identificación y bloquearlas a tiempo.

Respuesta
Es un componente crítico del proceso. Una vez identificado un incidente real, debemos contener y remediar el problema de manera efectiva y rápida. Gracias a nuestro equipo, podemos mitigar cualquier amenaza a tiempo real.

Monitorización
Creemos que monitorización es una necesidad básica para comprender tu seguridad, es por eso que empleamos muchos esfuerzos en detectar, priorizar e investigar tu entorno de manera proactiva.

Seguro cibernético

¿Alguna vez te has preguntado si es necesario contratar un ciberseguro? En este artículo explicamos por qué es aconsejable contratar un seguro cibernético es importante. Podemos enfrentarnos a altos costes si tu organización no tiene un seguro cibernético adecuado o inexistente.

No existe un entorno de IT 100% seguro

Si tu organización ha invertido mucho en seguridad informática y el personal también ha recibido formaciones que los hace más conscientes frente a las amenazas cibernéticas, el negocio ha dado un paso importante para no convertirse en una víctima del creciente número de ciberdelincuentes activos en Internet. Pero a pesar de los mejores esfuerzos, lamentablemente no existe un entorno de TI 100% seguro.

Aun habiendo invertido muchos recursos en un entorno seguro de IT, y a pesar de poner nuestro mayor esfuerzo para evitar ataques, nadie puede garantizar al 100% la seguridad de tu negocio. El seguro cibernético es una opción que puede ayudarte a proteger tu negocio contra las pérdidas causadas por un ataque cibernético.

El cibercrimen está a la orden del día. Por ejemplo, solo en el territorio español, el último año se produjeron más de 40.000 ciberataques al día. Ya sea una caja registradora que ha sido hackeada, datos de tu base de clientes que u otra información sensible con la que el ciberdelincuente puede aprovechar.

No solo tiene consecuencias económicas para tu empresa, sino también para tu imagen.

Daño financiero y de imagen

El cibercrimen está a la orden del día. Por ejemplo, una investigación internacional muestra que el 68% de empresas fueron víctimas de ciberdelincuencia en 2020. Ya sea que se trate de una caja registradora que ha sido pirateada, base de datos de clientes que terminan en manos equivocadas u otra información confidencial con la que el ciberdelincuente puede salirse con la suya, no solo tiene consecuencias financieras para su empresa, sino también para su imagen.

Además, un ataque cibernético crea muchas molestias. Por ejemplo, si estamos lidiando con una violación de datos en la que se robaron datos personales, estamos obligados de informar a la Autoridad de Protección de Datos española y europea. Además de poder ser multado si no ha tomado o ha tomado pocas medidas para evitar una violación de datos.

Consecuencias financieras

¿Sabías que las sanciones por no cumplir la ley de protección de datos pueden alcanzar hasta los 20 millones de euros o el 4% del volumen de facturación anual? Además de otros costes que puede incurrir una filtración de datos:

- Trabajos de configuración posteriores: 7.000€
- Experto legal para ayuda con la presentación de informes: 240 € por hora
- Investigación forense del incidente: 4.000€ por día
- Coste de datos robados o perdidos: 185€ por archivo
- Experto para reparar el problema: 125€ la hora
- Especialista en relaciones públicas para la comunicación de control de daños: 100€ por hora

Entonces, un seguro de ciberseguridad es una excelente opción para cubrir estos costes. Para poder contratar dicho seguro, debe cumplir una serie de condiciones con respecto a la seguridad informática de la organización. Las compañías de seguros quieren saber qué tan buena o mala es tu ciberseguridad.

En DesktopToWork, no solo te ayudamos a cumplir esos requisitos, sino también ofrecemos un seguro para tu negocio. Hay varias aseguradoras en el mercado, pero ¿por qué contratar un seguro cibernético por separado cuando también puedes hacerlo a través de nosotros?

No solo estarás asegurado contra las consecuencias económicas de un ciberataque y poder reclamar una indemnización, también recibirás ayuda de profesionales. Este seguro cubre, entre otras cosas, lo siguiente:

- Daños sufridos por terceros
- Gastos de defensa por responsabilidad en caso de no gestionar adecuadamente los datos de privacidad y otros riesgos digitales
- Costes de investigación
- Costes de consultoría de relaciones públicas para proteger la imagen
- Costes de notificación al cliente
- Tarifas de monitorización de crédito
- Multas impuestas por el gobierno (si están permitidas)
- Costes de reconstrucción de datos
- Extorsión cibernética
- Cierre de negocio por riesgos digitales

Work safer.
Live safer.

DesktopToWork Security

DESKTOP TO WORK

Contacto

+34 93 271 16 44
info@desktoptowork.com
www.desktoptowork.com

Carrer de la Marina 16-18, Mapfre Tower,
Barcelona 08005, España