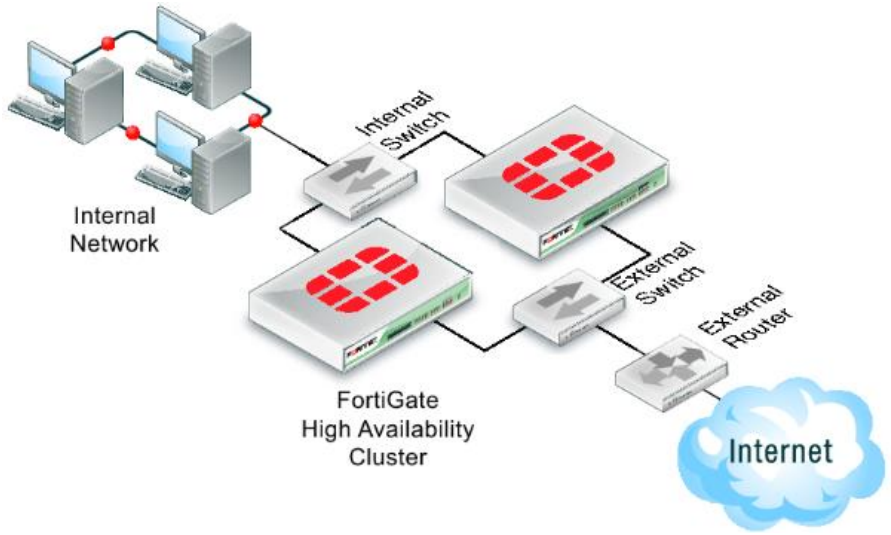
Modelo de seguridad con Fortinet

Como muestra el grafico este es un modelo simplificado de seguridad con Firewall Fortinet, para proteger su red empresarial, y proveerle conexión segura.

- La misma constituye dos (2) Appliance Fortinet en modo cluster Activo Activo.
- La configuración proporciona alta disponibilidad y distribución de carga, de las sesión activas.
- FortiOS, es el sistema operativo de los equipos Fortinet, seguro y de fácil administración.
- Fortinet le provee administración con un panel web y además una consola CLI.
- Bloquee sitios web maliciosos, y de contenido indebido mediante unos pasos muy sencillos de configuración.
- Proteja su red interna con IDS (Intruder Detection System) & IPS (Intruder Prevention System).
- Firmas actualizadas de virus provistas por Fortinet.
- Fortinet provee una eficiente y robusta solución SD-WAN.
- VPN Site-2-Site con túnel IPSec y Client-2-Site mediante un agente y túnel SSL.
- Acceda a reportes a reportes y gráficos útiles para el análisis de vulnerabilidades y detección de eventos no deseados.



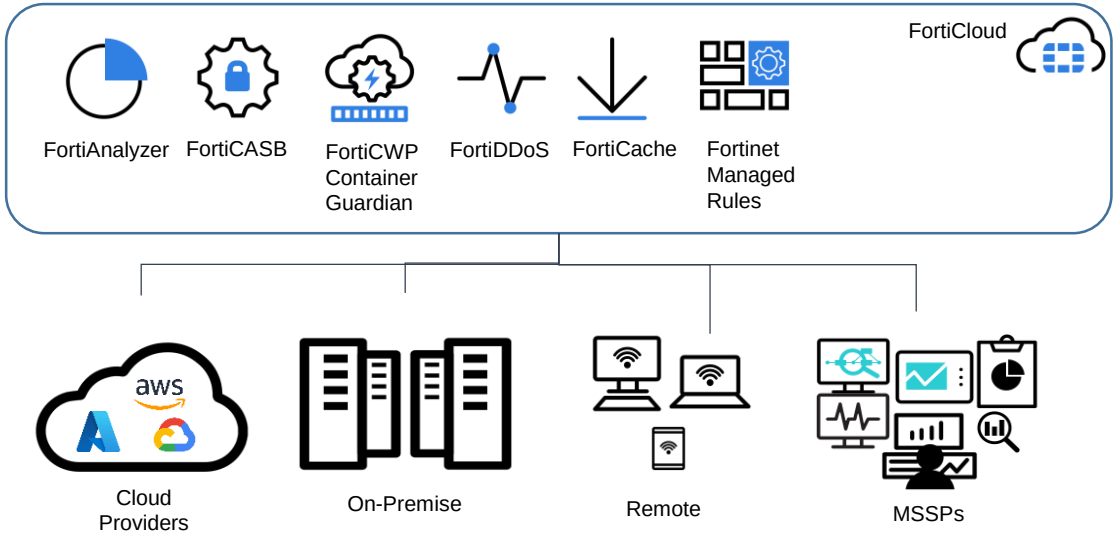
Fortinet provee una gama de dispositivos físicos y virtuales de gestión unificada contra amenazas de seguridad para su empresa.

Además ofrece un conjunto de servicios en la nube en modo SaaS, para administrar y gobernar sus dispositivos.

También puede utilizar otros servicios en la nube para proteger sus aplicaciones e infraestructura cloud.

También puedes tener un entorno totalmente segurizado y con alta disponibilidad.

Fortigate utiliza su propio sistema operativo FortiOS, que provee, una amigable UI, y un conjunto se características que facilitan la administración de los equipos.



FortiCloud

FortiCloud es una plataforma de Fortinet para entregar seguridad y servicios de administración de seguridad. FortiCloud proporción a los clientes una manera simple de conectar, proteger y, entregar sus datos y aplicaciones tanto On-Premise como Cloud. La Suite de FortiCloud ofrece un conjunto de portales y servicios en la nube que permite acceder y administrar un rango de las soluciones de Fortinet y un sitio de servicios de fácil acceso. Ademas proporciona acceso a FortiCare para la gestión de dispositivos y cuentas Fortinet.

FortiCloud Suite

Assets and Accounts

- Assets Management
- IAM

Cloud Management

- FortiGate Cloud
- FortiExtender Cloud
- FortiManager Cloud
- FortiAnalizer Cloud
- FortiLAN Cloud
- FortiClient EMS
- FortiSOAR Cloud

Cloud Management

- FortiPresence
- FortiToken Cloud
- FortiCASB
- FortiPenTest
- FortiMail
- FortiSandbox
- FortiPhish
- FortiWeb
- FortiInsight
- OCVPN Portal
- FortiGSLB
- FortiCWP

Kaspersky
Small Office Security (Datasheet)

Protección continua para su negocio. Simple y fácil de usar.

Kaspersky Small Office Security combina la simplicidad de la protección de los equipos personales con funciones especiales para mantener su empresa segura mientras los empleados realizan su trabajo. Con una seguridad que se "configura una sola vez", protege sus PC y laptops Windows y Mac, además de sus servidores de archivos Windows, para resguardar los archivos más importantes para el usuario.

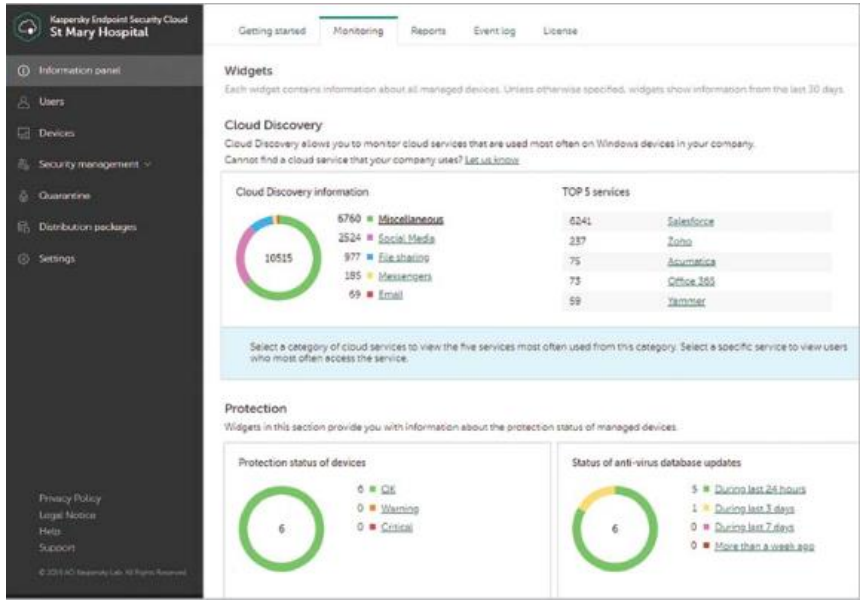
- **Protección contra ransomware avanzada** y reversión de acciones maliciosas para evitar que un clic accidental bloquee los equipos
- **Cifrado y copia de seguridad de archivos** para proteger su propiedad intelectual y secretos comerciales
- **Pago Seguro** para pagar las facturas y los impuestos online con confianza
- **Protección de dispositivos Android** para que sus empleados puedan trabajar de forma segura desde sus smartphones y tablets personales
- **Análisis de vulnerabilidades integrado** para garantizar que las aplicaciones empresariales que utilice estén protegidas frente a intrusiones

KASPERSKY lab

Kaspersky es una empresa que se dedica a proteger a los recursos informáticos de su compañía.

Protege a su empresa de ciberamenazas con soluciones de fácil implementación y de administración directa. Así tendrá tiempo para concentrarse en asuntos más importantes, como desarrollar sus negocios.

Kaspersky protege la mayoría de los asuntos que son importantes para su empresa, independiente del nivel de conocimientos de TI.



Kaspersky
Endpoint Security Cloud (Datasheet)

Protección sin complicaciones para su empresa, a donde sea que vaya.

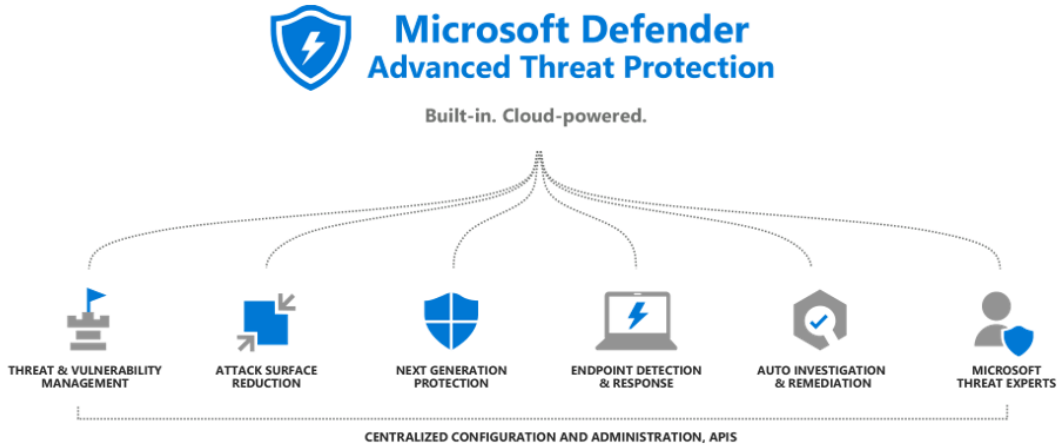
Kaspersky Endpoint Security Cloud proporciona una única solución para todas las necesidades de seguridad de TI de su organización. Asegúrese de que su empresa funcione sin problemas mientras Kaspersky se encarga de bloquear el ransomware, el malware sin archivos, los ataques de día cero y otras amenazas emergentes.

El enfoque basado en la nube permite que los usuarios puedan trabajar a salvo en cualquier dispositivo y colaborar de forma segura en línea, en el trabajo o en casa, desde oficinas remotas y en terreno. Además, nuestra consola basada en la nube permite administrar la seguridad desde cualquier lugar y en cualquier momento.

Kaspersky Endpoint Security Cloud fomenta la adopción segura de la nube con la detección de TI invisible y la protección para MS Office 365. Comenzar es rápido y fácil, no se necesita configurar un servidor ni políticas de seguridad, y sus usuarios están protegidos desde el momento en que se conectan en línea. Además de estar más protegido, con Kaspersky Endpoint Security Cloud dedicará menos tiempo a administrar su seguridad de TI, de modo que podrá concentrarse en las tareas empresariales de alta prioridad.

Microsoft Defender para punto de conexión usa la siguiente combinación de tecnologías integrada en Windows 10 y el robusto servicio en la nube de Microsoft:

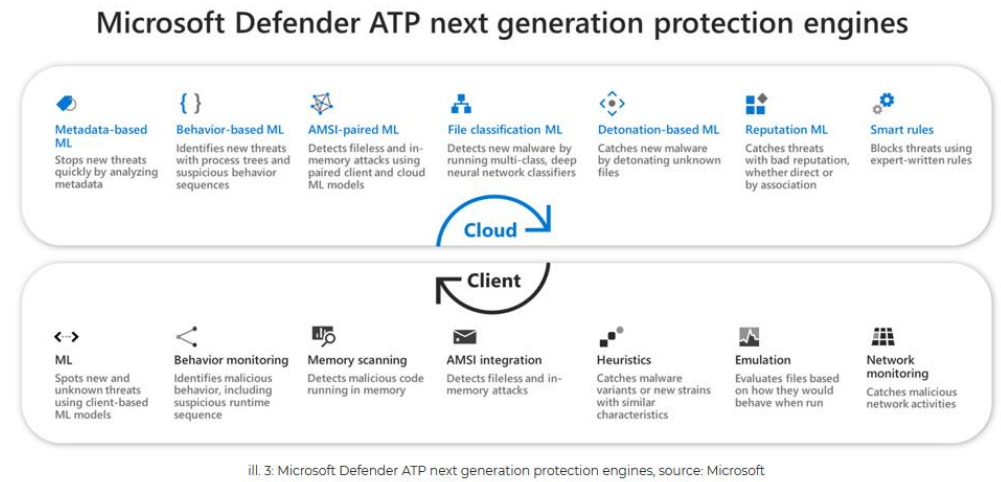
•**Sensores de comportamiento del punto de conexión**. Integrados en Windows 10, estos sensores recopilan y procesan señales de comportamiento desde el sistema operativo. Los sensores envían estos datos a la instancia de nube privada aislada de Microsoft Defender para punto de conexión.
•**Análisis de seguridad en la nube**. Al aprovechar los macrodatos, el aprendizaje de dispositivos y la óptica exclusiva de Microsoft en todo el ecosistema de Windows, los productos empresariales en la nube (como Office 365) y los activos en línea, las señales de comportamiento se traducen en conocimientos, detecciones y respuestas recomendadas a amenazas avanzadas.
•**Inteligencia sobre amenazas**. Generada por cazadores de Microsoft, equipos de seguridad y aumentada por la inteligencia de amenazas proporcionada por los socios, la inteligencia de amenazas permite a Microsoft Defender para punto de conexión identificar herramientas, técnicas y procedimientos de atacantes, y generar alertas cuando se observan en los datos de sensores recopilados.



ill. 1: Microsoft Threat Protection, source: Microsoft

Microsoft Defender para Endpoints es una plataforma empresarial para la seguridad de puntos de conexión concebida para ayudar a impedir, detectar e investigar las amenazas avanzadas, y responder a ellas.

Es una solución de seguridad para Endpoints que ofrece administración de amenazas y vulnerabilidades, protección de puntos de conexión, detección y respuesta de puntos de conexión, defensa contra amenazas móviles y servicios administrados en una única plataforma unificada.



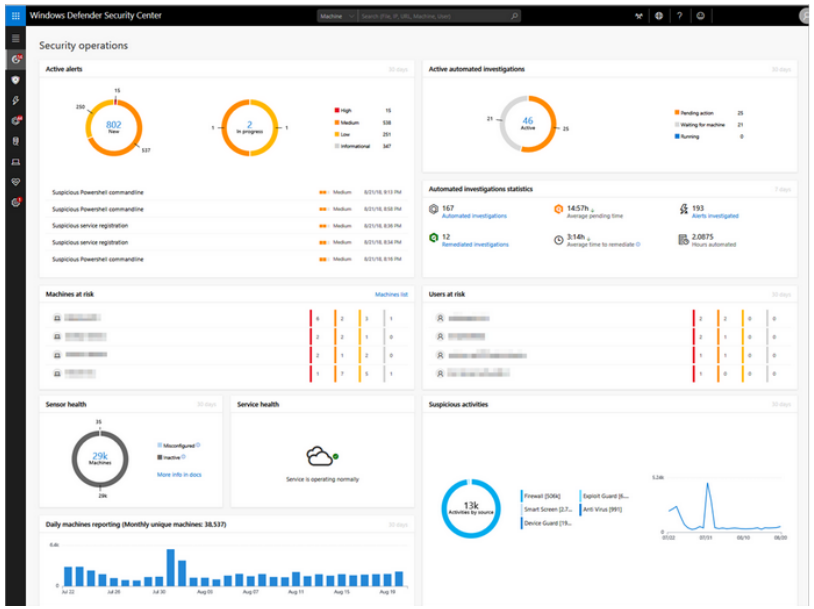
ill. 3: Microsoft Defender ATP next generation protection engines, source: Microsoft

El motor de protección ATP de próxima generación de Microsoft Defender permite que Microsoft Defender AV proteja al cliente contra amenazas que aún no se detectan o conocen.

Además, se utilizan algoritmos de aprendizaje automático e inteligencia artificial para identificar y eliminar amenazas nuevas y no detectadas.

Microsoft Defender for Endpoint ayuda al departamento de IT a administrar eficazmente la red de la empresa, ofreciéndole un portal de administración y gestión centralizado de todas las alertas y medidas de seguridad de los equipos.

- Paneles de navegación
- Gestion de alertas
- Control y gestión de invertigacion automáticas.
- Busqueda Avanzada,
- Inventario de equipos
- Estado del servicio.
- Configuracion personalizada.



Rho.

Seguridad con Suricata IDS & IPS

Características

Motor IDS & IPS

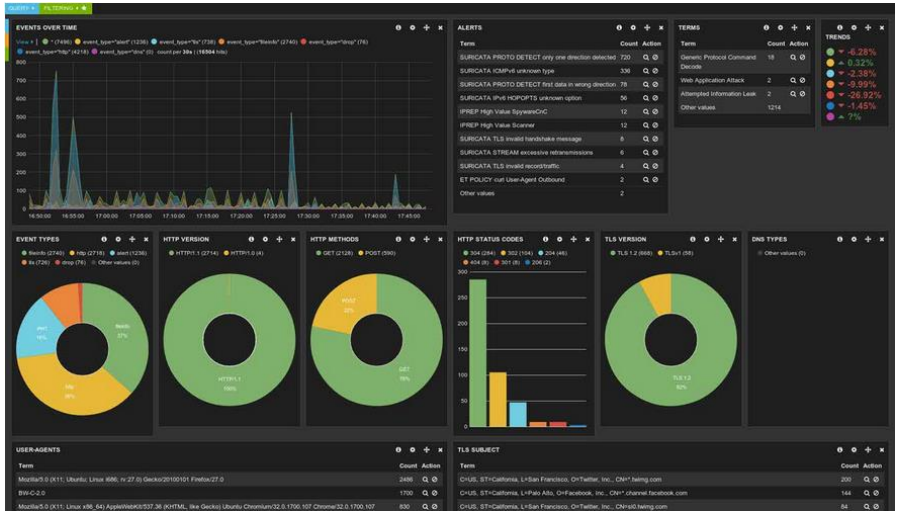
- Motor de sistema de detección de intrusos en la red (NIDS)
- Motor de sistema de prevención de intrusiones en la red (NIPS)
- Motor de monitoreo de seguridad de red (NSM)
- Análisis fuera de línea de archivos PCAP
- Grabación de tráfico usando **pcap logger**
- Modo de socket Unix para el procesamiento automatizado de archivos PCAP
- Integración avanzada con cortafuegos **Linux Netfilter**

Alertas

- Filtrado de alertas por regla.
- Filtrado de alertas globales.
- Por host/subred umbral y configuración de limitación de velocidad

Reputación IP

- Carga de grandes cantidades de datos de reputación basados en el host
- Coincidencia de datos de reputación en el lenguaje de reglas utilizando la palabra clave **"iprep"** soporte de recarga en vivo
- Admite rangos CIDR



SURICATA

Suricata es el principal motor independiente de detección de amenazas de código abierto.

Al combinar detección de intrusiones (IDS), prevención de intrusiones (IPS), monitoreo de seguridad de red (NSM) y procesamiento PCAP, Suricata puede identificar, detener y evaluar rápidamente incluso los ataques más sofisticados.

Suricata se integra a la perfección con su red y puede integrarse en numerosas soluciones comerciales y de código abierto respetadas.

El proyecto y el código de Suricata son propiedad y están respaldados por **Open Information Security Foundation** (OISF), una organización sin fines de lucro que se compromete a mantener el código abierto de Suricata para siempre.

Integración

Plataformas de visualización

Suricata le permite integrar con diferentes plataformas de código abierto o bajo licencia. Para poder crear paneles y visualizaciones de los Logs que recopila cuando protege su red.

Puede alojar estas plataformas en la nube o en un VM dentro de DataCenter.

Las mismas se acceden mediante su navegador preferido de internet, esto le permite poder monitorizar su red empresarial desde cualquier lugar.