iSentinel

Protegemos el éxito de su negocio

SOLUCIONES INTEGRALES DE TECNOLOGÍA

EN CIBERSEGURIDAD
E INFRAESTRUCTURA

iSentinel
Protegemos el éxito de su negocio

NUESTRO
NEGOCIO

Nuestra propuesta se basa en una amplia experiencia de buenas prácticas y proyectos exitosos.

Somos una empresa que entrega Soluciones Integrales de Tecnología, en el ámbito de Ciberseguridad, Infraestructura, Servicios Profesionales, Servicios Gestionados y Consultorías.

Contamos con amplia experiencia apoyando a diversas empresas del rubro financiero, industrial, retail, telecomunicaciones, gobierno, entre otras, en la entrega de soluciones que permiten responder a necesidades, requerimientos y problemáticas de nuestros clientes, mejorando su experiencia tecnológica y asegurar la continuidad operativa de su negocio.

Nuestro servicio está enfocado en un modelo de gestión en base a un punto de contacto escalable automáticamente, capaz de entregar soluciones de manera ágil, flexible y eficaz, asegurando la continuidad del servicio y negocio de nuestros clientes.

iSentinel es parte de AJ Corp, un holding de empresas con más de 35 años en Latinoamérica.

iSentinel
Protegemos el éxito de su negocio

NUESTRAS
SOLUCIONES

01 SERVICIOS GESTIONADOS

02 HARDWARE

03 SOFTWARE Y LICENCIAS

04 SERVICIOS PROFESIONALES

iSentinel

Protegemos el éxito de su negocio

SOFTWARE Y LICENCIAS

iSentinel
Protegemos el éxito de su negocio

03

SOFTWARE Y
LICENCIAS

BACKUP

- kaspersky
- veeam

SEGURIDAD ENDPOINT

- kaspersky
- CHECK POINT
- TREND MICRO
- vicarius
- BeyondTrust
- safetica

VIRTUALIZACIÓN

- veeam
- SANGFOR
- TREND MICRO

iSentinel
Protegemos el éxito de su negocio

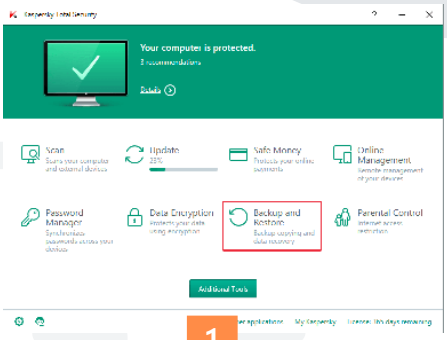
BACKUP

kaspersky

Establece copias de seguridad automáticas con Kaspersky Total Security

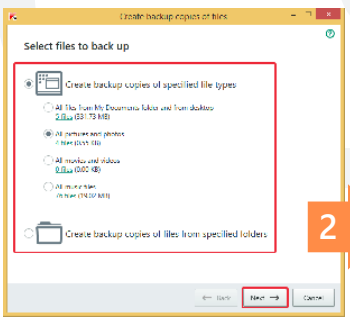
KLbackup es una utilidad de **Kaspersky Security Center** que permite hacer copias de seguridad y restaurar datos del Servidor de administración. Se puede ejecutar en modo interactivo o no interactivo. Al realizar una copia de seguridad, se guardan:

- Base de datos del Servidor de administración (directivas, tareas, configuración de la aplicación, eventos guardados en el Servidor);
- Información de configuración sobre la estructura de la red lógica y los dispositivos cliente;
- Almacenamiento de paquetes de instalación de aplicaciones para la instalación remota (contenido de la carpeta Packages);
- Certificado del Servidor de administración.

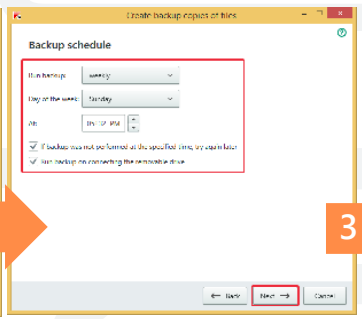


Elegir “Copia de seguridad y Restauración” en la ventana principal.

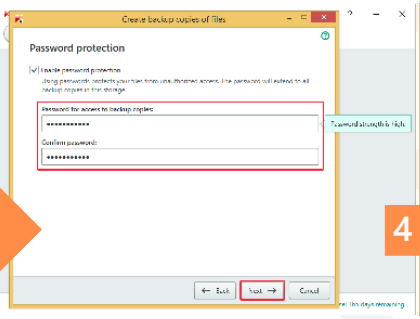
Luego hacer click en “Seleccionar archivos para una copia de seguridad”.



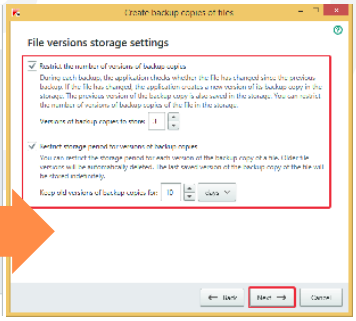
En la ventana “Crear copias de seguridad de archivos”, elegir el tipo de documentos de los cuáles quiere hacer una copia de seguridad o indicar una carpeta en particular.



Fijar un horario para la ejecución de copia de seguridad automática.



Crea una contraseña para proteger tu carpeta de almacenamiento.

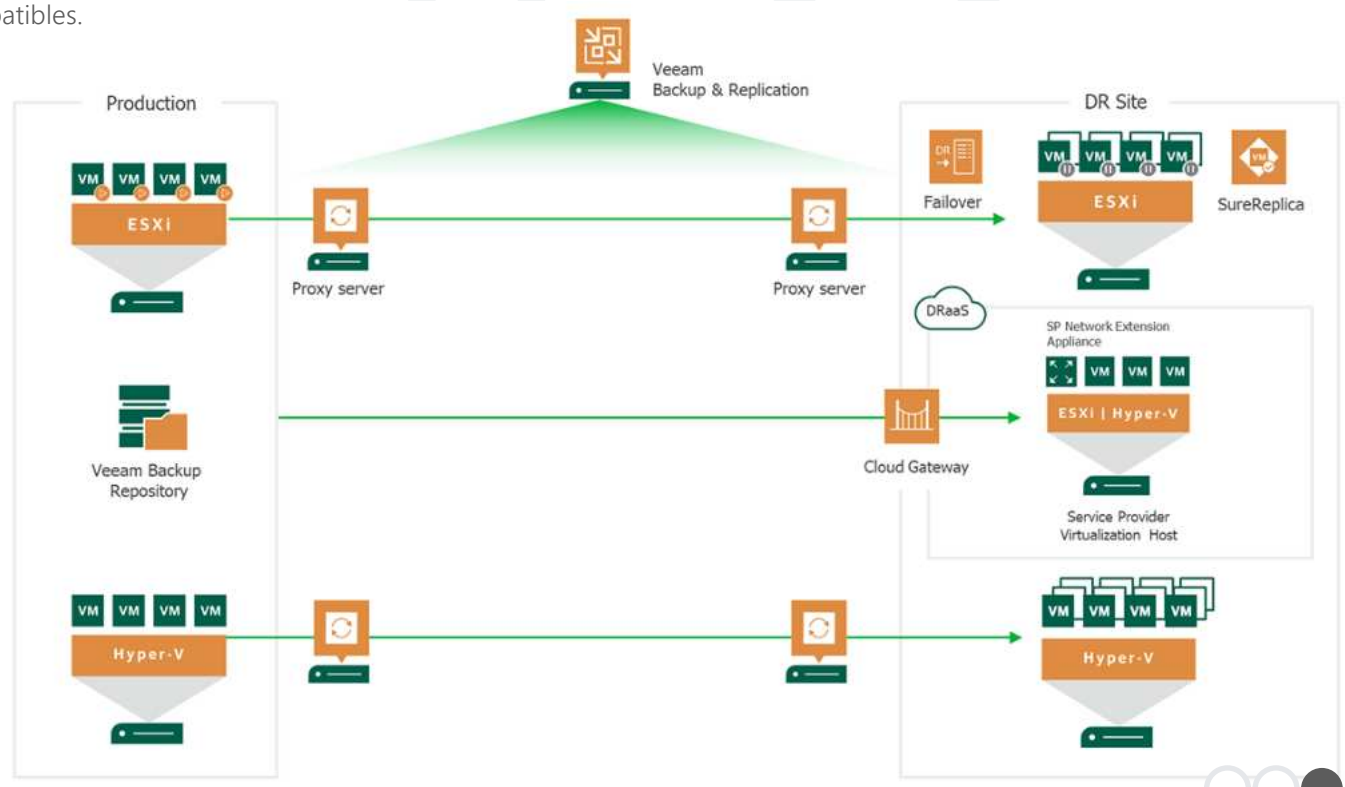


Define los parámetros para almacenamiento de la copia de seguridad.

BACKUP

Veeam Backup & Replication es una solución de protección de datos probada que ofrece backup y recuperación fiable y eficiente para entornos virtuales, físicos, NAS y nativos de la nube.

Una tecnología de recuperación ante desastres como servicio (DRaaS), como Veeam Backup , ofrece una variedad de capacidades de protección de datos. La solución permite la expansión de cargas de trabajo virtuales, físicas y en la nube, facilitando la gestión de los procesos de TI y minimizando las posibilidades de tiempos de inactividad y caídas . El sistema se ejecuta en la capa de virtualización y no tiene agentes, lo que ofrece protección de datos integral para todas las cargas de trabajo. AWS , IBM Cloud , VMware , Microsoft Hyper-V , Sap Hana , Oracle , Exchange y MySQL son solo algunos de los entornos compatibles.



iSentinel
Protegemos el éxito de su negocio

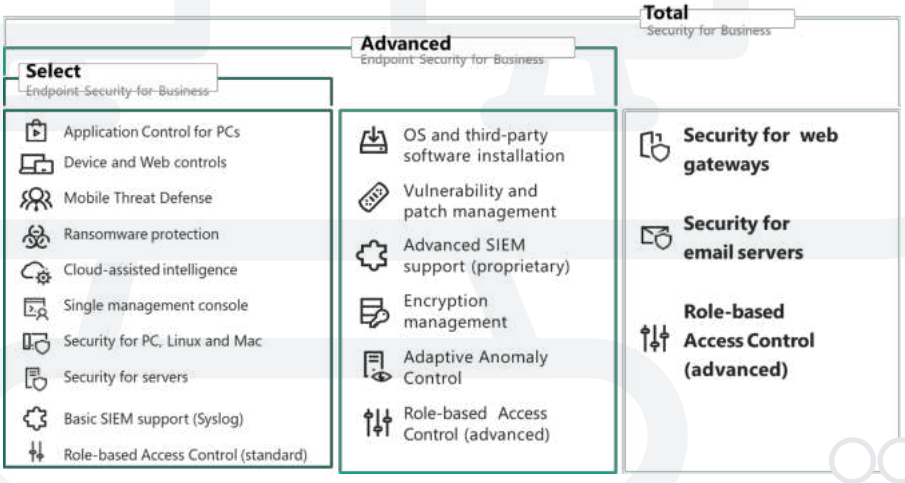
SEGURIDAD ENDPOINT

kaspersky

kaspersky
Endpoint Security

Kaspersky Endpoint Security for Business Select y Advanced son ambos Productos de seguridad de endpoints que protegen contra ciberataques. La principal diferencia es que Advanced incluye más tecnologías de seguridad y un modelo basado en roles para dividir responsabilidades.

Con la creciente digitalización de sus operaciones comerciales, necesita proteger cada servidor, portátil y dispositivo móvil de su red. El nivel Select combina tecnologías multicapa con una gestión flexible de la nube y controles centralizados de aplicaciones, web y dispositivos para proteger sus datos confidenciales en cada punto final.



iSentinel
Protegemos el éxito de su negocio

SEGURIDAD ENDPOINT

TREND MICRO™

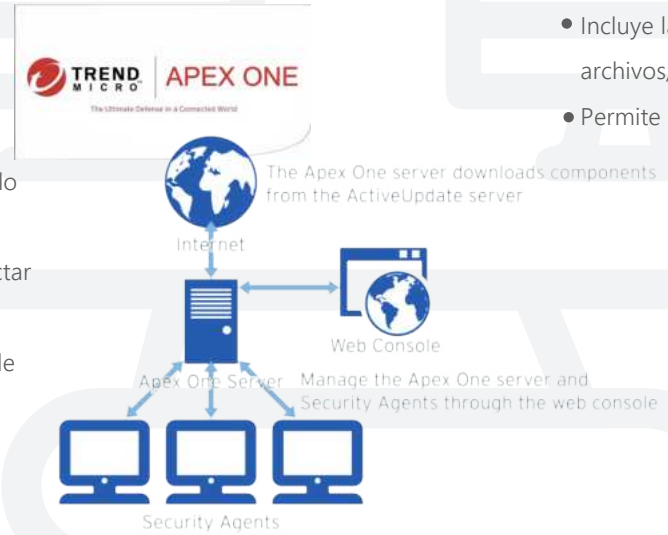
Trend Micro ofrece soluciones de seguridad para endpoints, como Trend Vision One, Apex One, y Endpoint Encryption. Estas soluciones protegen dispositivos como laptops, computadoras de escritorio, y dispositivos móviles.

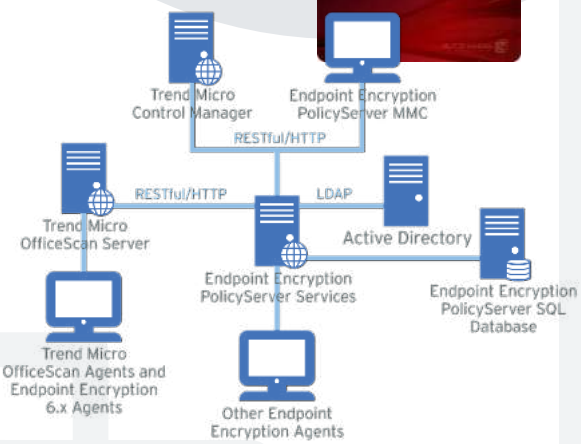
Trend Vision One

- Ofrece protección contra amenazas en múltiples etapas de un ataque
- Centraliza la información para detectar eventos y el camino del ataque
- Permite responder más rápido y aumentar la eficiencia operativa
- Incluye XDR nativo para extender las defensas hacia el correo, las redes, y máss o acciones autorizadas.

Apex One

- Ofrece detección de amenazas, investigación, y respuesta en un solo agente.
- Utiliza machine learning para detectar malware avanzado.
- Incluye un sistema de prevención de intrusiones basado en host (HIPS).





Endpoint Encryption

- Encripta los datos en una amplia gama de dispositivos
- Incluye la encripción de disco completo, de archivos/carpetas, y de medios extraíbles.
- Permite administrar holísticamente a los usuarios.

iSentinel
Protegemos el éxito de su negocio

SEGURIDAD ENDPOINT

BeyondTrust

BeyondTrust Endpoint Privilege Management protege los dispositivos y el acceso de los usuarios mediante la gestión de los privilegios. Le permite crear listas blancas pragmáticas para administrar aplicaciones confiables y bloquear versiones no autorizadas o antiguas de software.

Seguridad de confianza cero

Elimine los derechos de administrador local y administre el acceso root para eliminar los privilegios permanentes. Controle lo que los usuarios pueden instalar o ejecutar mediante privilegios justo a tiempo, sin afectar la productividad ni generar sobrecarga de administración.

Auditoría y gobernanza

Simplifique el cumplimiento y la investigación forense con un registro de auditoría único e impecable de toda la actividad del usuario, al que se puede acceder fácilmente desde una consola central segura.

Privilegio Justo a Tiempo

Asigne privilegios solo a la tarea, comando o aplicación y no al usuario, solo cuando el privilegio sea necesario y solo durante el tiempo que sea necesario.

Informes de actividad

Optimice continuamente la postura de seguridad y la experiencia del usuario final a través de paneles e informes personalizables.

Integraciones potentes

Optimice los flujos de trabajo con integraciones nativas con ServiceNow, herramientas SIEM, VirusTotal, herramientas MFA, Microsoft Entra ID y una API flexible.

Despliegue rápido

Utilice plantillas de políticas de inicio rápido prediseñadas basadas en información de miles de implementaciones para lograr avances rápidos y de alto impacto en la reducción de riesgos.

Experiencia flexible del usuario final

Cree una experiencia de usuario final personalizada para tipos específicos de usuarios dentro de sus organizaciones, desde usuarios técnicos como desarrolladores o administradores de servidores hasta roles no técnicos más estándar.

Protección unificada

Proteja todo su patrimonio de puntos finales, ya sean computadoras de escritorio Windows y Mac, servidores Windows o servidores Linux locales o en la nube.

iSentinel
Protegemos el éxito de su negocio

SEGURIDAD ENDPOINT

CHECK POINT™

Check Point Endpoint Security es una solución de seguridad que protege los dispositivos de los usuarios finales, como laptops, smartphones, o tablets. Esta solución protege contra amenazas como ransomware, phishing, o malware no autorizado.

Check Point Endpoint Security, incluye seguridad de datos, seguridad de red, prevención avanzada de amenazas, análisis forense, detección y respuesta de terminales (EDR), y soluciones de VPN de acceso remoto. Para ofrecer una gestión de seguridad sencilla y flexible, todo el paquete de seguridad del endpoint de Check Point puede administrarse de forma centralizada utilizando una única consola.

Características de Check Point Endpoint Security:

- Seguridad de datos
- Seguridad de red
- Prevención avanzada de amenazas
- Análisis forense
- Detección y respuesta de terminales (EDR)
- VPN de acceso remoto
- Soporte para todas las SO y VDI

SOLUCIONES

Harmony Endpoint

HARMONY ENDPOINT

La protección de Harmony Endpoint ofrece una gestión simple y unificada y el cumplimiento de políticas de seguridad para entornos Windows y Mac OS X.

Harmony Mobile

HARMONY MOBILE

Harmony Mobile es la solución líder para la defensa de amenazas en seguridad para dispositivos iOS y Android.

CAPSULE WORKSPACE

Capsule Workspace es una solución eficiente para proteger los entornos empresariales en los dispositivos móviles.

iSentinel
Protegemos el éxito de su negocio

SEGURIDAD ENDPOINT

vicarius

La gestión de parches no es suficiente. vRx ofrece aplicación de parches automática, secuencias de comandos personalizadas y protección sin parches para garantizar que no haya brechas de seguridad en su infraestructura.

Vicarius vRx es una plataforma avanzada de análisis de vulnerabilidades y gestión de parches diseñada para proteger aplicaciones, sistemas operativos y software de terceros. Su enfoque único en la protección predictiva permite identificar debilidades antes de que sean explotadas, todo sin necesidad de acceso al código fuente.

¿Para que sirve?

En un entorno digital en constante evolución, las organizaciones necesitan herramientas proactivas que aseguren la continuidad operativa y protejan los datos sensibles.

El papel de vRx de Vicarius en el etiquetado de endpoints

Al utilizar vRx de Vicarius , las organizaciones pueden optimizar el etiquetado de endpoints. vRx proporciona una vista consolidada de todos los activos, lo que permite el etiquetado y la segmentación en tiempo real según factores de riesgo, uso de aplicaciones y más. Sus funciones de gestión automatizada de parches mejoran aún más la eficacia del etiquetado, garantizando que las medidas de remediación se ajusten a los niveles de riesgo identificados.

Vicarius vRx te ayuda a:

Identificar vulnerabilidades críticas en tiempo real.

Automatizar la implementación de parches y soluciones.

Priorizar riesgos en función del impacto potencial en tu organización.

Proteger aplicaciones sin acceso al código fuente a través de tecnología patentada.

iSentinel
Protegemos el éxito de su negocio

SEGURIDAD ENDPOINT

safetica

La defensa contextual impulsada por IA clasifica con precisión los datos confidenciales, identifica con precisión el comportamiento riesgoso y adapta de forma proactiva las defensas para aplicar la seguridad cuándo y dónde sea necesaria.

Descubra cómo Safetica utiliza Control de dispositivos para gestionar riesgos internos y proteger los datos.

El control de dispositivos, significa establecer políticas y medidas para supervisar y gestionar el uso de dispositivos dentro de la red o entorno de una organización. Ayuda a realizar un seguimiento de quién puede conectarse a ellos, a qué datos pueden acceder y qué acciones pueden realizar.

El control de dispositivos desempeña un papel crucial a la hora de mitigar los riesgos internos y proteger los datos dentro de una empresa.

Escanea, identifica y clasifique automáticamente los dispositivos externos conectados utilizados por los empleados.

Previene y bloquea el uso no autorizado de dispositivos.

Establece políticas granulares de control de dispositivos y supervisa todos los puertos y dispositivos USB en todos los endpoints.

Envía notificaciones e informes sobre la actividad USB en todos los puntos finales.

VIRTUALIZACIÓN

Veeam es un proveedor especialista en la gestión de sistemas y protección de datos de entornos virtualizados, que con sus soluciones de Backup permite maximizar el rendimiento de la inversión en virtualización minimizando los riesgos ante pérdidas o crisis imprevistas.

On premises

Por más de una década, Veeam ha lanzado numerosas características disruptivas para la gestión y protección de ambientes virtuales on premises como, por ejemplo, los basados en VMware vSphere, Microsoft Hyper-V y Nutanix AHV. Hoy en día, además soportamos backup de servidores físicos o virtuales con sistemas operativos AIX, SOLARIS, LINUX y WINDOWS, además de estaciones de trabajo Windows, Linux y MAC.

Nube pública

Con **Veeam** puede replicar, tomar copias de sus datos y respaldar las cargas de trabajo que tenga en las distintas nubes públicas como Amazon AWS, Microsoft Azure y Google Cloud Platform.

Veeam cuenta con soluciones nativas para AWS, Azure y GCP. La interfaz gráfica está basada en la web y es posible integrarla con Veeam Backup & Replication mediante la utilización de plug-ins.

Además, los respaldos de máquinas virtuales o servidores físicos realizados on premises pueden restaurarse a Azure o AWS y viceversa, por lo que al utilizar **Veeam Backup & Replication** para integrar los respaldos realizados en las nubes, podrá gestionar la movilidad de sus máquinas virtuales entre las distintas nubes o tener la capacidad de realizar una recuperación ante desastres.

Nubes múltiples

Puede que su organización hoy cuente con una nube on premises o con servidores en una nube de algún proveedor público (AWS, GCP, Azure). De ser así, seguramente en el corto o mediano plazo contará con un ambiente de nubes múltiples o híbrido. Es decir, por ejemplo, un centro de datos on premises más un ambiente en AWS, y otro en Azure.

Contenedores

Hoy en día es crítico que pueda contar con respaldo nativo de Kubernetes. **Kasten by Veeam** es una solución que no solo realiza respaldo de forma nativa de Kubernetes, sino que también facilita la portabilidad de las aplicaciones y provee de recuperación ante desastres.

VIRTUALIZACIÓN

SANGFOR

Sangfor es un proveedor de soluciones de virtualización e hiperconvergencia que ayudan a optimizar los recursos de TI y reducir costos.

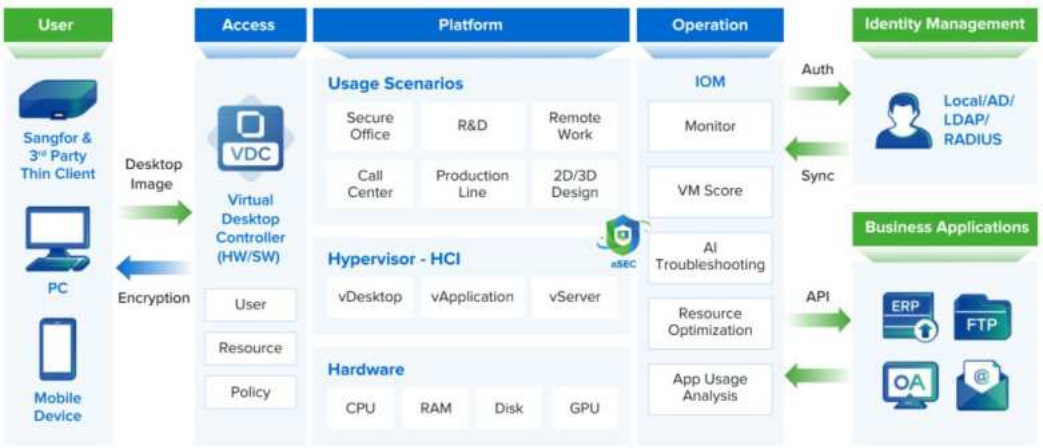
SOLUCIONES

Sangfor ofrece una variedad de productos y servicios, incluyendo:

- Virtualización de servidores, escritorios, y aplicaciones.
- Infraestructura de escritorio virtual (VDI).
- Infraestructura hiperconvergente (HCI).
- Firewall de nueva generación.
- Protección de endpoints.
- Protección contra ransomware.
- Detección y respuesta gestionada.
- Optimización WAN.
- SD-WAN.

Las soluciones de Sangfor están diseñadas para:

- Optimizar el uso de espacio y recursos.
- Simplificar la gestión de la infraestructura.
- Reducir la complejidad.
- Converger computación, almacenamiento, redes, y seguridad en una única pila de software.
- Mejorar la flexibilidad y escalabilidad de la infraestructura.



iSentinel
Protegemos el éxito de su negocio

VIRTUALIZACIÓN

TREND MICRO™

TREND MICRO | Deep Security

Trend Micro ofrece soluciones de seguridad para virtualización, como Deep Security, parches virtuales, y XDR, que ayudan a proteger servidores y aplicaciones en entornos virtuales.

SOLUCIONES

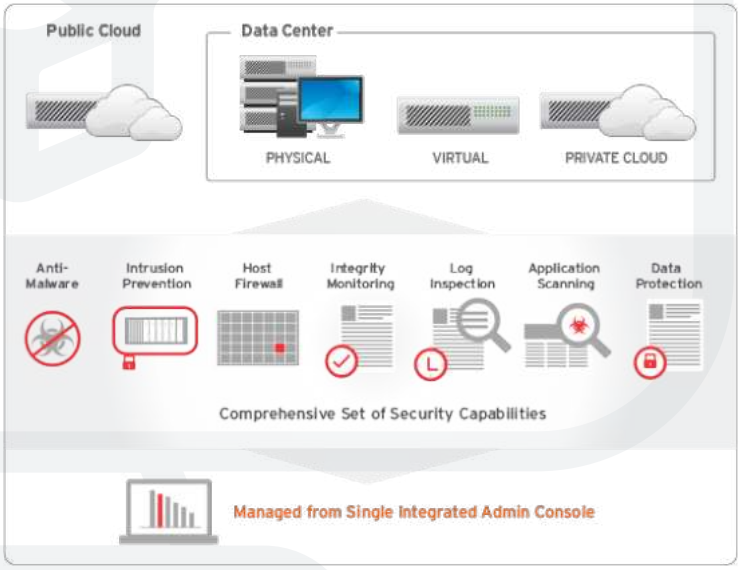
Trend Micro Deep Security

- Protege aplicaciones y datos empresariales contra filtraciones e interrupciones
- Se integra con soluciones de virtualización como VMware, Citrix, y Microsoft
- Ofrece protección sin agente o basada en agente
- Incluye características de antimalware, detección y prevención de intrusiones
- Permite simplificar las operaciones de seguridad
- Ofrece visibilidad centralizada para una mejor y más rápida detección y respuesta

Parcheo virtual

- Protege contra vulnerabilidades conocidas y desconocidas
- Utiliza reglas del sistema de prevención de intrusiones (IPS) para bloquear el tráfico malicioso
- Entrega la protección de vulnerabilidades más puntual a lo largo de una variedad de endpoints

La solución de Trend Micro se extiende a todo el ámbito de los servidores, ya sean físicos, virtuales o Cloud y es que Deep Security es la solución completa y recomendada para los servidores corporativos de cualquier Sistema Operativo.



CONTÁCTENOS

DIRECCIÓN: Av La Divisa 340. San Bernardo.
Santiago, Chile
FONO: +56 2 2488 6550
CORREO:ventas@isentinel.cl


iSentinel
Protegemos el éxito de su negocio