ABOX

Catálogo de seguridad 2026
Distribuidores

Índice

Antivirus | Avast CloudCare 3
Antivirus MTD | Zimperium 4
Antivirus MTD | Lookout 5
Antivirus MTD | Harmony Mobile Security 6
Firewall | Clavister Netwall – NGFW 7
Monitorización | Fastvue 8
Monitorización | WebSpy 9
Monitorización | Promodag 10
Filtrado de contenidos | ContentKeeper 11
Filtrado de contenidos | Cleanmail 12
Gestión de identidades | HelloID 13
Gestión de identidades | MobilityGuard 14
Gestión de identidades | PhenixID 15
Auditorias y migraciones | AvePoint Fly 16
Backups y restauración | AvePoint Cloud Backup 17
Backups y restauración | Vembu BDR Suite 18
Movilidad | Workspace One UEM 19
Movilidad | SOTI MOBICONTROL 20
Movilidad | Ivanti Endpoint Manager 21
Movilidad | Ivanti Neurons for MDM 22
Movilidad | MaaS360 23
Movilidad | Samsung Knox 24
Movilidad | Microsoft Intune 25

Antivirus | Avast CloudCare

Potentes servicios de seguridad en línea por capas para pequeñas y medianas empresas

Avast CloudCare es una solución de seguridad cibernética en la nube que protege a empresas de cualquier tamaño. Ofrece características como antivirus, protección de correo electrónico y seguridad de red, con administración centralizada para facilitar la gestión y monitoreo desde cualquier lugar. Su tecnología avanzada detecta y elimina virus, malware y otras amenazas. La protección de correo electrónico incluye filtro antispam y prevención de phishing, mientras que la seguridad de red abarca cortafuegos y detección de intrusiones para salvaguardar la red empresarial contra amenazas externas.

➢ Panel de Control Intuitivo

Visualice todas las alertas de un vistazo, aborde los problemas y obtenga la información que necesita para tomar decisiones informadas, agregue servicios y ejecute acciones rápidas de cara a aumentar la disponibilidad, la estabilidad y la seguridad.

➢ Informes completos

Recopile datos a partir de múltiples servicios y resúmenes de alertas y genere informes detallados de actividad de fácil lectura haciendo clic en un solo botón.

➢ Gestión de dispositivos y política

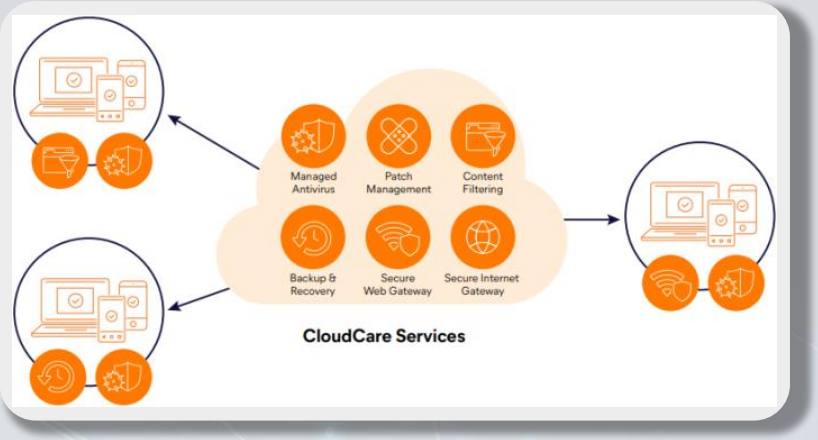
Dimensione las operaciones empresariales y reduzca el mantenimiento con unos cambios de política que se configuran automáticamente, en tiempo real, en los dispositivos controlados por agentes.

➢ Alertas en tiempo real

Configure alertas para problemas importantes que requieren su atención y envíe inmediatamente correos electrónicos o mensajes SMS a las partes implicadas, mejorando el tiempo de reacción y limitando la exposición.

➢ Control remoto de TI gratuito

Conexión segura a dispositivos de cliente desde cualquier ubicación para solucionar problemas, llevar a cabo tareas, reiniciar equipos, transferir archivos y chatear con los clientes de forma remota.



➢ Administración de parches

Identifique e implemente con facilidad los parches críticos, y supervise la actividad en curso desde un panel central.

➢ Filtrado de contenidos

Aumente la productividad y bloquee el acceso a sitios web no seguros y distracciones en línea, para que los empleados estén protegidos y mantengan su productividad durante el horario de trabajo.

➢ Copia de seguridad

Evite costosos períodos de inactividad con una variedad de soluciones de copias de seguridad y recuperación de datos, locales y en línea, que protegen archivos, aplicaciones, servidores, etc.

➢ Puerta de enlace Web segura

Bloquee el acceso a sitios web, descargas y ubicaciones maliciosas para evitar ataques que dañen su red o roben cualquier dato.

➢ Pasarela de internet segura

Ofrezca mayor seguridad y escalabilidad y reduzca los costes con nuestra revolucionaria solución de gestión unificada de amenazas basada en la nube.

Antivirus MTD | Zimperium

ZIMPERIUM

Proteja sus endpoint móviles

Zimperium Mobile Threat Defense (MTD), antes conocida como zIPS, es una aplicación de seguridad móvil para empresas que protege dispositivos corporativos y BYO contra amenazas avanzadas en cuatro áreas: dispositivos, redes, phishing y ataques a aplicaciones. Utiliza detección basada en aprendizaje automático para prevenir malware, incluyendo el de día cero. Zimperium ha demostrado detectar más del 99 % de malware y aplicaciones maliciosas en evaluaciones realizadas por AV-TEST GmbH. Además, ofrece cobertura completa en Android, iOS y ChromeOS, tanto en tablets como smartphones.

➢ Desarrollado por aprendizaje automático

A medida que la superficie de ataque móvil continúa expandiéndose y evolucionando, también lo hace el motor basado en aprendizaje automático de Zimperium. Zimperium MTD detecta amenazas conocidas y desconocidas analizando el comportamiento de un dispositivo móvil y puede identificar con precisión desviaciones del sistema móvil, aplicaciones que se comportan como malware, tráfico de red anómalo y ataques de phishing avanzados. Además, el aprendizaje automático se entrega en el dispositivo, lo que lo protege incluso si el endpoint no está conectado a la red.

➢ Seguridad móvil empresarial escalable

Zimperium MTD se puede utilizar como herramienta independiente o integrarse con un MDM/EMM para dispositivos administrados. Cuando se integra con un MDM/EMM, Zimperium MTD envía alertas sobre amenazas detectadas al MDM/EMM, y el MDM/EMM soluciona el riesgo basándose en reglas predefinidas. Zimperium MTD funciona a la perfección con las principales soluciones MDM/EMM y es la única solución de defensa contra amenazas móviles que puede integrarse simultáneamente con múltiples MDM/EMM, lo que resulta especialmente útil a la hora de realizar la transición de soluciones.

Zimperium MTD también se puede utilizar para dispositivos no administrados con administración de aplicaciones móviles (MAM). Con las aplicaciones habilitadas para MAM, cuando un usuario inicia una aplicación de trabajo, como Microsoft O365, en un dispositivo móvil, la aplicación solo permite el acceso cuando la defensa contra amenazas móviles se está ejecutando en el dispositivo.

➢ Seguridad móvil empresarial centrada en la privacidad

Con un enfoque de privacidad por diseño, Zimperium MTD brinda a los usuarios una experiencia transparente con configuraciones personalizables e información sobre qué datos se recopilan y utilizan para la inteligencia sobre amenazas. Debido a que la detección de Zimperium MTD se realiza en el dispositivo, la información privada nunca se envía a la nube.

➢ Componente vital de la ciberseguridad integral

Zimperium MTD ofrece análisis forense móvil crucial para que los equipos de seguridad respondan rápidamente a incidentes, reduciendo el tiempo de reparación. Mediante integraciones con sistemas MDM/EMM/UEM, SIEM, SOAR y XDR, los equipos de respuesta obtienen visibilidad de amenazas móviles. Los análisis forenses evitan que dispositivos comprometidos causen brotes, permitiendo a los equipos revisar datos sobre dispositivos, conexiones de red y aplicaciones maliciosas para minimizar riesgos.

➢ Implementación Zero Touch

Implemente y active Zimperium MTD en los terminales móviles Endpoint de sus empleados y contratistas sin complicaciones en los pasos de activación por parte del usuario final.

➢ Acceso a datos críticos

La certificación integral de dispositivos permite a las empresas tener una imagen completa de la seguridad de sus móviles y refuerza las arquitecturas Zero Trust a través de integraciones existentes.

Antivirus MTD | Lookout

Protege los dispositivos móviles de tus empleados de cualquier ciber-amenaza

Lookout Mobile Threat Defense es una aplicación que se instala en los dispositivos móviles (iOS, Android y Chrome OS) protegiéndolos contra todo tipo de amenazas y preservando la privacidad del empleado.
Protege tu empresa en tres niveles: **protección de aplicaciones, protección de red, protección de sistemas operativos y dispositivos.**

Funciones de Lookout Mobile Threat Defense: Asegura tanto los dispositivos propiedad de la empresa como los de los empleados, es adecuado para empresas de todos los tamaños: SOHO a corporaciones multinacionales, despliegue sin fricciones, experiencia simple de usuario, y preserva y respeta la privacidad de los usuarios.

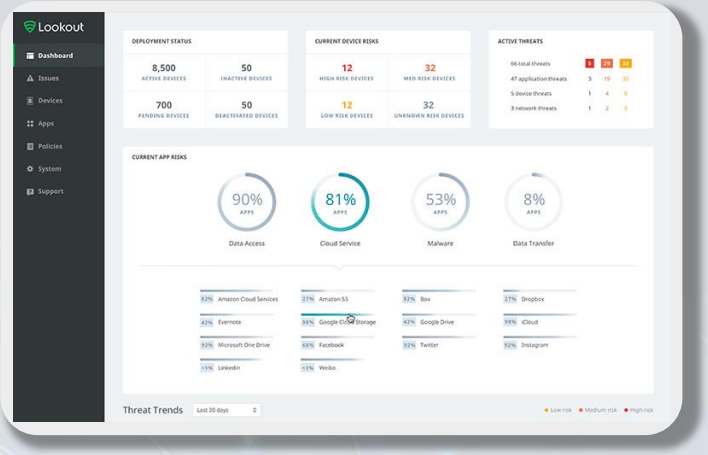
➢ ¿Por qué es vital tener el servicio de Lookout en dispositivos de tu empresa?

Detección de phishing: Lookout detecta y bloquea la navegación del usuario a un sitio de phishing en todos los puntos de entrada manteniendo seguros el dispositivo, el usuario y la organización, todo esto sin acceder a los datos del usuario ni enrutar el tráfico a la nube para su inspección.

Detección de malware: Tras la detección, Lookout notifica al usuario de la detección y proporciona instrucciones sobre la solución recomendada. Junto con una integración de MDM, los administradores pueden bloquear automáticamente el acceso del usuario a los recursos corporativos hasta que solucionen el problema. Además, con Lookout Essentials se le pueden integrar dos funciones adicionales: “Integración con productos MDM” e “Integración con soluciones de Gestión de identidades y Monitorización SIEM”.

➢ Consola basada en la nube

Con completa visibilidad y control de todos los dispositivos de la organización y aplicación móvil para proteger el dispositivo sin afectar su rendimiento.



➢ Protege contra amenazas web y contenido

Ataques de Phishing, sitios web y archivos maliciosos. Protección integral de la navegación web.

➢ Protección a nivel de Aplicaciones

Protege contra aplicaciones maliciosas, software espía y troyanos, aplicaciones desactualizadas y vulnerables o aplicaciones que incumplen normativas y políticas de seguridad de la organización.

➢ Protección de las conexiones de Red de la empresa

Previene de amenazas ocultas en las redes a las que se conecta el dispositivo: Wifis y redes móviles maliciosas, e identifica vulnerabilidades potenciales en el software y configuraciones del dispositivo.

➢ Protección física del dispositivo

Protege contra amenazas provenientes de la manipulación no autorizada del dispositivo, modificación del sistema operativo, (Jailbreak o rooting) para evadir controles de seguridad o instalar aplicaciones no permitidas o maliciosas (software espía).

Antivirus MTD | Harmony Mobile Security

Harmony Mobile

Seguridad móvil: robusta, ágil y transparente

Harmony Mobile, diseñado para reducir los gastos generales de los administradores y aumentar la adopción de los usuarios, se adapta perfectamente a su actual entorno móvil, se implementa y escala rápidamente y protege los dispositivos sin afectar al usuario experiencia ni privacidad.

➢ Una solución de defensa contra amenazas móviles líder en el mercado

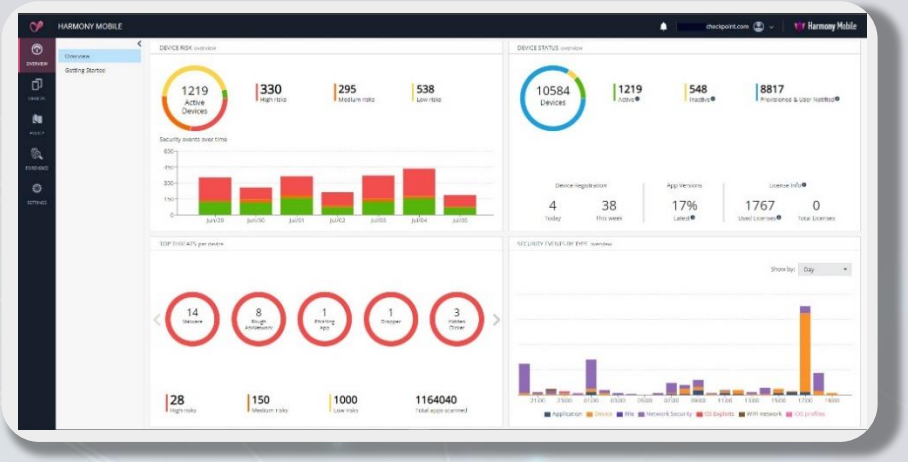
Harmony Mobile mantiene a salvo los datos de su empresa protegiendo los dispositivos móviles de los empleados en todos los vectores de ataque: aplicaciones, archivos, red y SO. Diseñado para reducir los gastos generales y aumentar la adopción por parte de los usuarios, se integra perfectamente en los entornos móviles existentes y protege el dispositivo sin afectar a la experiencia del usuario ni a su privacidad.

- **Protección completa**: Proteja sus datos corporativos en todas las superficies sujetas a sufrir ataques móviles: aplicaciones, redes y SO.
- **Administración sencilla**: Seguridad escalable y fácil de gestionar para cualquier tipo de personal móvil.
- **Fácil de usar**: Rápida adaptación de los usuarios sin incidencia en su experiencia o privacidad.

➢ Protege contra el sofisticado panorama de amenazas

Los ciberataques aumentan constantemente en volumen y sofisticación, con un incremento del 38% en el número de ciberataques de un año a otro. Harmony Mobile protege contra las amenazas más inminentes:

- Protege contra el malware y los intentos de phishing bloqueando las descargas de aplicaciones y archivos maliciosos.
- Evita los ataques Man-in-the-Middle
- Bloquea el acceso del dispositivo infectado a los activos y recursos de la empresa
- Reconoce y bloquea las técnicas avanzadas de jailbreak y rooting.
- Detecta la vulnerabilidad SO (CVE) y la desinformación.



➢ Protección de terminales a 360° con funciones avanzadas, todo en un único cliente

Harmony Endpoint es una solución completa y consolidada de seguridad de terminales con funciones avanzadas de EPP, EDR y XDR, creada para proteger al personal remoto del complejo panorama actual de amenazas.

- **Protección de aplicaciones y archivos**: Harmony Mobile impide que el malware infecte el dispositivo de los empleados detectando y bloqueando la descarga de aplicaciones maliciosas en tiempo real.
- **Protección de red**: La exclusiva infraestructura de seguridad en red de Harmony Mobile -Protección de Red en Dispositivo- mantiene a las empresas por delante de las amenazas emergentes al extender las tecnologías de seguridad en red líderes del sector a los dispositivos móviles.
- **SO y dispositivo Protección**: Garantiza que los dispositivos no estén expuestos a un peligro mediante evaluaciones de riesgos en tiempo real que detectan ataques, gestión de vulnerabilidades (CVE), cambios de configuración o ajustes de seguridad débiles y rooting y jailbreaking avanzados.

Firewall | Clavister Netwall - NGFW

Connect, Protect.

Clavister es una empresa líder en seguridad cibernética que ofrece soluciones como Next-Generation Firewalls (NGFW), los cuales proporcionan seguridad avanzada mediante inspección profunda de paquetes, prevención de intrusiones, filtrado de contenido y protección contra malware. Los NGFW de Clavister utilizan tecnologías como aprendizaje automático e inteligencia artificial para detección y prevención proactivas de amenazas. Además, son personalizables y escalables, permitiendo a las empresas adaptar la seguridad a sus necesidades, con una plataforma de gestión centralizada para monitorear y administrar la seguridad de red de manera eficiente.

Características principales:

- Firewall de próxima generación que proporciona protección avanzada contra amenazas de red, como malware, ataques DDoS y hacking.
- Interfaz fácil de usar y capacidad de configuración para adaptarse a diferentes requisitos de seguridad de red.
- Funciones avanzadas de gestión de tráfico, incluyendo control de ancho de banda y priorización de tráfico.
- Capacidad para implementar políticas de seguridad granulares y personalizadas para diferentes partes de la red.
- Soporte para múltiples protocolos y aplicaciones, lo que permite un mayor control sobre el tráfico de red.
- Funciones de seguridad avanzadas, como VPN y autenticación de usuarios.
- Enfoque en la escalabilidad, compatibles con entornos virtuales lo que permite que la solución crezca con el negocio.
- Alta disponibilidad, sin interrupciones de servicio en caso de fallo o actualización del sistema.
- Integración con otras soluciones de seguridad y tecnologías, como Clavister InControl y SIEM.

¿Qué incluye los NGFW de Clavister?

Clavister InControl

➢ GESTIÓN Y CONTROL CENTRALIZADO

Todos los dispositivos Clavister se pueden administrar individualmente a través de una interfaz web, pero se incluye una licencia para usar la gestión centralizada Clavister InControl. La solución ofrece implementación sin intervención, formas simplificadas de aprovisionar y administrar una implementación de SD-WAN seguro y capacidades de gestión de actualización de firmware.

Clavister InCenter

➢ ANALÍTICA EN LA NUBE EN TIEMPO REAL

Clavister InCenter permite a los administradores de TI obtener información sobre sus redes. Clavister InCenter proporciona todas las historias de usuario, incluyendo la investigación forense con búsqueda de registros, paneles de control e informes, así como el monitoreo de la salud. Se incluye una versión alojada de Clavsiter InCenter Cloud con cada suscripción de seguridad, y alternativamente InCenter está disponible para implementación local.

Clavister OneConnect

➢ TRABAJO REMOTO SIMPLE Y SEGURO

Clavister OneConnect es el cliente SSL VPN para Windows, iOS/iPad OS y macOS que ofrece una solución simple y fácil de usar para acceso remoto y está incluido en la solución NetWall de Clavister.

CyberSecurity Score

➢ ANÁLISIS DE SEGURIDAD SIMPLIFICADO Y ACCIONABLE

Ayuda a los gerentes de TI y sus ejecutivos a comunicarse sobre el estado de su infraestructura de seguridad y garantiza que los fondos y esfuerzos se gasten donde más importan: esta herramienta se incluye en Clavister InCenter, disponible para todos los Clavister NetWall con una suscripción de seguridad.

Monitorización | Fastvue

Ve lo que está sucediendo en su red

Fastvue es una solución de análisis y generación de informes para redes de internet y seguridad que permite a los administradores de TI monitorear el uso de internet en su organización. Ofrece informes detallados y en tiempo real sobre el tráfico de internet, ayudando a identificar problemas de seguridad, optimizar el ancho de banda y mejorar la productividad de los empleados.

Compatible con dispositivos de seguridad web y firewall de marcas como Sophos, Barracuda, Fortinet y Cisco Meraki, Fastvue es fácil de implementar y personalizar, permitiendo la creación de informes y alertas a medida. Además, brinda un excelente servicio al cliente y soporte técnico.

Monitoreo del tráfico de internet
Monitorice el uso de Internet por parte de los empleados o estudiantes e identifique cualquier actividad inapropiada o riesgosa. La herramienta proporciona informes detallados y en tiempo real sobre el uso de Internet, como los sitios web visitados, el ancho de banda utilizado, las aplicaciones utilizadas, entre otros.

Control de acceso a internet
Fastvue también puede ayudar su empresa para implementar políticas de uso de Internet y controlar el acceso a sitios web específicos. Los administradores pueden configurar restricciones de acceso para ciertos sitios web y categorías, y pueden bloquear el acceso a sitios web maliciosos o inapropiados.

Cumplimiento de políticas
Las organizaciones pueden utilizar Fastvue para cumplir con las políticas y regulaciones internas y externas relacionadas con el uso de Internet. La herramienta ayuda a las organizaciones a demostrar que están tomando medidas para garantizar un uso adecuado y seguro de Internet.

Análisis forense
Fastvue puede ser útil para la investigación de incidentes de seguridad y la resolución de problemas. Los administradores usan dicha herramienta para buscar registros de tráfico web y obtener una visión detallada de la actividad en la red.

Mejora de la productividad
Fastvue puede ayudar a las empresas a mejorar la productividad al identificar sitios web y aplicaciones que consumen mucho tiempo y ancho de banda. Los administradores pueden establecer políticas para limitar el acceso a estos sitios y aplicaciones y, por lo tanto, mejorar la eficiencia del trabajo.

Identificación de amenazas
Identifique posibles amenazas a la seguridad informática, como malware, virus y phishing. Los administradores pueden configurar alertas para ciertos patrones de actividad en la red y tomar medidas para mitigar los riesgos.

Seguimiento del uso de aplicaciones
Monitorice el uso de aplicaciones en la red e identifique cualquier uso no autorizado o inapropiado. Los administradores pueden ver informes detallados sobre las aplicaciones utilizadas y el ancho de banda que consumen.

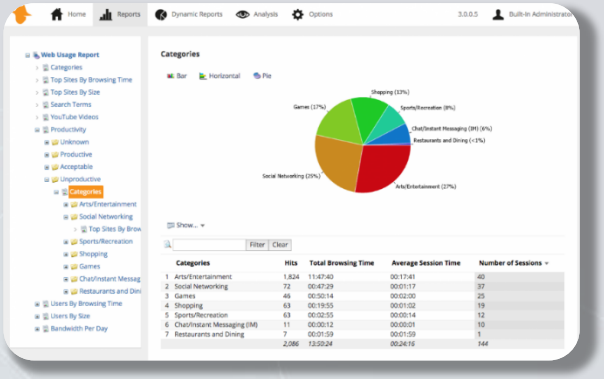
Gestión de ancho de banda
Gestione el uso del ancho de banda y optimizar el rendimiento de la red. Los administradores pueden ver informes detallados sobre el uso del ancho de banda y tomar medidas para equilibrar el tráfico de la red y evitar cuellos de botella.

Monitorización | WebSpy

Controla tu red, protege tu negocio con WebSpy

WebSpy es una herramienta de análisis de tráfico de Internet que permite a las empresas monitorear y gestionar su uso de Internet. Ofrece informes detallados sobre el tráfico de la red, incluyendo el uso de ancho de banda, actividad de navegación, correo electrónico y más, y ayuda a detectar actividades maliciosas como el acceso a sitios peligrosos o la descarga de malware.

Altamente personalizable y escalable, WebSpy se adapta a las necesidades específicas de las empresas y es compatible con una amplia gama de dispositivos y plataformas, lo que facilita su integración en cualquier infraestructura de red existente.



Seguridad de la red
Monitorice la actividad de la red en busca de posibles amenazas y vulnerabilidades, lo que ayuda a los administradores de la red a tomar medidas de seguridad para proteger la red contra posibles ataques.

Cumplimiento de políticas
Webspy ayuda a las organizaciones a garantizar el cumplimiento de las políticas de uso de la red y de seguridad, supervisando el uso de la red y detectando cualquier actividad que viole las políticas de la organización.

Optimización del uso de la red
Utilice Webspy para analizar el tráfico de la red y detectar cuellos de botella y otros problemas de rendimiento, lo que permite a los administradores de la red tomar medidas para mejorar la eficiencia de la red y optimizar el uso de los recursos.

Supervisión de la productividad
Supervise la actividad de los empleados en la red, lo que ayuda a los gerentes a identificar a los empleados que pueden estar utilizando la red de manera inapropiada o que pueden estar perdiendo tiempo en actividades no relacionadas con el trabajo.

Análisis del tráfico de la red
Analice el tráfico de la red y genere informes detallados sobre el uso de la red y el comportamiento de los usuarios. Estos informes pueden ayudar a los administradores de la red a tomar decisiones informadas sobre la gestión de la red y la optimización de los recursos.

Monitorización del tráfico en línea
Monitorice y analice el uso de aplicaciones en línea, lo que permite a los administradores de la red tomar medidas para mejorar el rendimiento y la eficiencia de las aplicaciones.

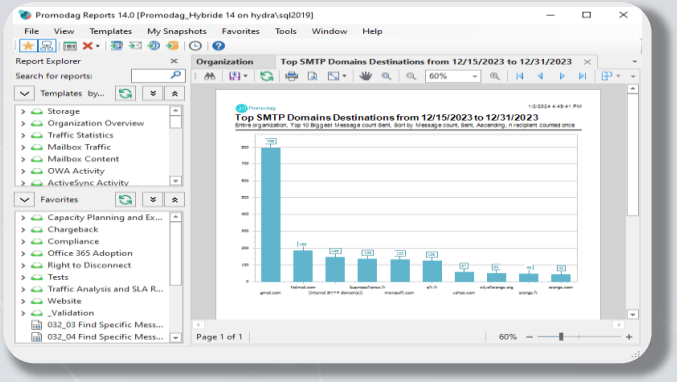
Supervisión de la actividad del servidor
Webspy se utiliza para monitorear la actividad de los servidores y detectar problemas de rendimiento y otros problemas que puedan afectar la disponibilidad de la red.

Investigación de incidentes de seguridad
Con Webspy puede investigar incidentes de seguridad, lo que permite a los administradores de la red identificar la causa raíz del problema y tomar medidas para prevenir futuros incidentes de seguridad.

Monitorización | Promodag

Informes de Exchange para Office 365 y Exchange On-premises

Promodag Reports for Exchange es una herramienta que cubre todas las necesidades de informes de Exchange, compatible con Exchange Online (Office 365), híbrido y On-premise. Facilita la auditoría del correo electrónico, asegura el cumplimiento de las normas comerciales y optimiza el rendimiento del sistema de correo. Ayuda a cumplir obligaciones legales como el RGPD y optimiza el uso de recursos. Además, permite generar indicadores útiles para la gestión diaria del contenido del buzón. Con más de 20 años de preferencia entre los administradores de Exchange Server, es ideal para auditar mejores prácticas, cumplir con el RGPD y prepararse para migraciones a otras versiones de Exchange o Office 365.



➢ Informes de almacenamiento

Utilice informes de almacenamiento para sacar a la luz los 10 buzones de correo más grandes o para enumerar cuotas para grupos completos de buzones.

➢ Informes de estadísticas de tráfico

Los informes de estadísticas de tráfico proporcionan métricas destinadas a permitirle realizar un análisis en segundo plano de la actividad de mensajería, principalmente en formato gráfico.

➢ Informes de contenido de buzones y carpetas públicas

Utilice toda la potencia de los informes del servidor Exchange para filtrar elementos individuales de Outlook según propiedades específicas dentro de un grupo de buzones o carpetas públicas.

➢ Informes de tráfico global

Da un paso atrás con los informes de tráfico global y genera informes cualitativos y cuantitativos de Exchange Server sobre el tráfico de mensajes a nivel de servidor.

➢ Informes de optimización del tráfico

Ejecute informes de optimización del tráfico para estimar el uso de direcciones SMTP antiguas o para enumerar NDR. Utilice este conjunto de herramientas de informes del servidor Exchange para descubrir quién usa direcciones secundarias y enumerar los mensajes devueltos.

➢ Informes de inventario

Los informes de inventario se han diseñado para enumerar objetos relacionados con Exchange, es decir, servidores y los diferentes tipos de destinatarios que alojan, junto con sus atributos.

➢ Informes de actividad ActiveSync y OWA

Los informes ActiveSync y OWA le ayudan a medir la actividad de los usuarios hasta la hora y la dirección IP utilizada.

➢ Informes de entrega de mensajes internos

Los informes de entrega de mensajes internos le ayudan a ofrecer informes precisos de Exchange Server sobre la calidad real del servicio que se entrega a los usuarios finales.

➢ Informes de facturación

Utilice informes de facturación para facturar a departamentos o sucursales internos en función del volumen de correo electrónico que envían o reciben, el tamaño de sus buzones de correo o ambos.

Filtrado de contenidos | ContentKeeper

Seguridad, control y confianza

Content Keeper permite a los administradores monitorear y registrar el uso de Internet, asegurando el cumplimiento de las políticas y evitando el acceso a sitios no autorizados. También ayuda a reducir riesgos legales y cumplir con regulaciones de privacidad de datos. En resumen, es esencial para proteger a la organización contra amenazas en línea.

➢ Filtrado de contenido
Content Keeper se utiliza para filtrar el contenido de la web y bloquear el acceso a sitios web maliciosos, inapropiados o no autorizados. Los administradores pueden personalizar las políticas de filtrado para adaptarse a las necesidades de su organización y pueden bloquear categorías de sitios web específicas, como redes sociales, juegos en línea, videos, etc.

➢ Seguridad de la red
Content Keeper ofrece una solución de seguridad de red integral que protege contra amenazas en línea, incluidos virus, malware, phishing y ataques de hackers. Los administradores pueden configurar políticas de seguridad personalizadas para evitar la entrada de virus y otras amenazas.

➢ Cumplimiento de la política de uso aceptable
Content Keeper se utiliza para hacer cumplir las políticas de uso aceptable de la organización. Los administradores pueden definir las políticas de uso de Internet y bloquear el acceso a sitios web no autorizados o inapropiados para garantizar que los empleados sigan las directrices de la organización.

➢ Monitoreo y registro
Content Keeper ofrece capacidades de monitoreo y registro detalladas para ayudar a los administradores a supervisar el uso de Internet. Los administradores pueden generar informes sobre el uso de Internet y el cumplimiento de las políticas de uso aceptable.

➢ Control parental
Content Keeper también se puede utilizar como una herramienta de control parental para bloquear el acceso a sitios web inapropiados y garantizar la seguridad en línea de los niños y adolescentes.

➢ Acceso remoto seguro
Content Keeper puede utilizarse como un proxy de seguridad para permitir un acceso remoto seguro a la red de la organización. Esto es especialmente útil para los trabajadores que necesitan acceder a los recursos de la red de la organización desde ubicaciones remotas.

➢ Reducción del riesgo de responsabilidad
Content Keeper ayuda a reducir el riesgo de responsabilidad de la organización al bloquear el acceso a contenido ilegal o inapropiado. Esto es especialmente importante en organizaciones que trabajan con información sensible o que tienen regulaciones de cumplimiento estrictas.

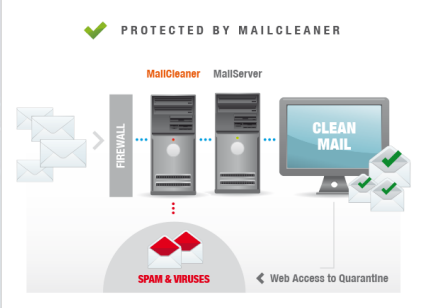
➢ Protección contra amenazas de phishing y ataques de malware
Content Keeper puede utilizarse para bloquear el acceso a sitios web y correos electrónicos maliciosos que contienen virus y malware, lo que ayuda a proteger la red de la organización contra amenazas de seguridad.

➢ Cumplimiento de las regulaciones de privacidad de datos
Content Keeper puede utilizarse para garantizar que los empleados no accedan a sitios web o descarguen archivos que violen las regulaciones de privacidad de datos. Esto es especialmente importante en organizaciones que manejan información personal confidencial.

Filtrado de contenidos | Cleanmail

¡Mantén tu bandeja de entrada limpia y organizada con Cleanmail!

Cleanmail es una herramienta para organizar y limpiar tu bandeja de entrada, eliminando spam, clasificando correos por prioridad, y gestionando suscripciones y correos duplicados. Permite personalizar la bandeja de entrada y enviar respuestas automáticas. Su interfaz fácil de usar ayuda a ahorrar tiempo y encontrar correos importantes rápidamente, mientras protege tu privacidad. Es una opción eficiente para gestionar correos electrónicos.



Eliminación de correos electrónicos no deseados
Cleanmail puede ayudarte a eliminar correos electrónicos no deseados o spam de tu bandeja de entrada. Esto te permitirá reducir la cantidad de correos electrónicos no importantes y te ayudará a centrarte en los correos electrónicos importantes.

Organización de correos electrónicos
Organice sus correos electrónicos en diferentes carpetas o etiquetas para encontrar rápidamente los correos electrónicos que necesitas. Puedes crear reglas de clasificación personalizadas para que los correos electrónicos sean clasificados automáticamente.

Eliminación de correos electrónicos antiguos
Con el tiempo, tu bandeja de entrada puede llenarse con correos electrónicos antiguos y sin importancia. Cleanmail puede ayudarte a eliminar estos correos electrónicos para que puedas mantener tu bandeja de entrada limpia y ordenada.

Identificación de correos electrónicos importantes
Cleanmail puede ayudarte a identificar los correos electrónicos importantes que requieren tu atención inmediata. Puedes crear reglas personalizadas para etiquetar o marcar los correos electrónicos importantes y asegurarte de que no se pierdan entre los correos electrónicos menos importantes.

Administración de suscripciones
Si recibes muchos correos electrónicos de suscripciones a boletines informativos o promociones, Cleanmail puede ayudarte a administrar estas suscripciones. Puedes utilizar la función de eliminación masiva de Cleanmail para eliminar todos los correos electrónicos de suscripción de una sola vez.

Limpieza de archivos adjuntos
Los archivos adjuntos pueden ocupar mucho espacio en tu bandeja de entrada y hacer que sea difícil encontrar los correos electrónicos importantes. Cleanmail puede ayudarte a limpiar los archivos adjuntos eliminando los archivos innecesarios y archivando los archivos importantes.

Optimización del rendimiento del correo electrónico
Si tu bandeja de entrada está llena de correos electrónicos, esto puede afectar al rendimiento de tu aplicación de correos electrónicos. Cleanmail puede ayudarte a optimizar el rendimiento de dicha aplicación al reducir la cantidad de correos electrónicos en tu bandeja de entrada y mejorar la velocidad de carga y búsqueda de nuevos que te lleguen.

Reducción del tamaño de la bandeja de entrada
Si tienes una gran cantidad de correos electrónicos en tu bandeja de entrada, puede ser difícil encontrar los que sean importantes. Cleanmail puede ayudarte a reducir el tamaño de tu bandeja de entrada al eliminar correos electrónicos no importantes o antiguos, lo que te permitirá centrarte en aquellos que sean de importancia y prioritarios.

Gestión de identidades | HelloID

Automatiza la gestión de identidad y acceso de tu empresa con HelloID Provisioning

HelloID Provisioning es una solución de automatización para la gestión centralizada de identidades y accesos. Permite administrar altas, cambios y bajas de usuarios, así como su acceso a recursos empresariales, integrando sistemas locales y en la nube para mantener la sincronización de datos. Ofrece flujos de trabajo personalizados, reduciendo tiempo y costos, e incluye funciones de auditoría e informes para supervisar el uso y asegurar el cumplimiento de políticas de seguridad.

➢ Onboarding de empleados

Automatice el proceso de creación de cuentas de usuario, asignación de permisos y provisionamiento de recursos para nuevos empleados, lo que agiliza el proceso de incorporación y garantiza que los nuevos empleados tengan acceso a los recursos que necesitan desde el primer día.

➢ Offboarding de empleados

HelloID Provisioning puede desactivar automáticamente las cuentas de usuario y revocar los permisos de acceso para los empleados que se van, lo que garantiza que los recursos de la empresa estén protegidos después de que un empleado deja la organización.

➢ Actualización de roles y permiso

HelloID Provisioning permite a los administradores de TI actualizar rápidamente los roles y permisos de los usuarios en todos los sistemas y aplicaciones, lo que asegura que los usuarios tengan el acceso correcto a los recursos según sus funciones y responsabilidades en la organización.

➢ Automatización de flujos de trabajo

Automatice flujos de trabajo y procesos de aprobación para la creación de cuentas de usuario y asignación de permisos, lo que ayudará a reducir la carga de trabajo de los administradores de TI y garantice la precisión de los permisos asignados.

➢ Creación y gestión de grupos de usuarios

HelloID Provisioning puede crear automáticamente grupos de usuarios y asignar permisos a esos grupos, lo que simplifica la gestión de permisos de usuario a nivel de grupo.

➢ Cumplimiento de requisitos de auditoría

Mantenga un registro detallado de todas las actividades de aprovisionamiento y desprovisionamiento, lo que ayuda a las organizaciones a cumplir con los requisitos de auditoría y seguridad.

➢ Cumplimiento de normativas de privacidad de datos

HelloID Provisioning puede ayudar a las organizaciones a cumplir con las regulaciones de privacidad de datos, como GDPR y CCPA, al controlar y auditar el acceso a los datos personales de los usuarios.

➢ Integración con sistemas de gestión de proyectos

HelloID Provisioning puede integrarse con sistemas de gestión de proyectos, como Jira y Trello, para automatizar la asignación de permisos de usuario y recursos en función de los proyectos y las tareas asignadas.

➢ Gestión de contraseñas

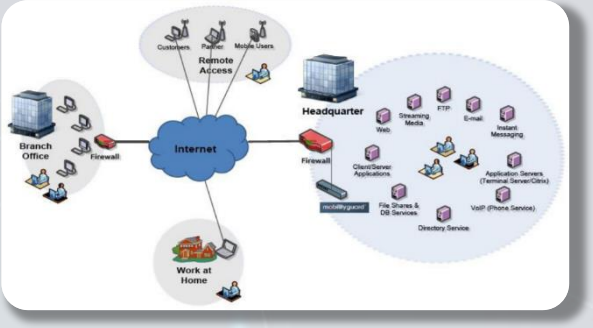
Sincronice automáticamente las contraseñas de los usuarios en todos los sistemas y aplicaciones que utilicen, lo que reduce el riesgo de vulnerabilidades de seguridad y facilita a los usuarios tener una única contraseña para recordar.

Gestión de identidades | MobilityGuard

mobilityguard®
Unified Access Management

Acceda con confianza, proteja con MobilityGuard

MobilityGuard es una solución de seguridad en la nube que ofrece autenticación multifactor, control de acceso basado en roles y análisis de riesgos para proteger dispositivos móviles y aplicaciones. Permite gestionar el acceso de usuarios y dispositivos autorizados, integrándose con diversas soluciones de autenticación y adaptándose a las necesidades de cada organización. Los administradores pueden establecer políticas personalizadas y monitorear el acceso desde una consola centralizada, simplificando la gestión de la seguridad y garantizando una experiencia segura.



Autenticación multifactor (MFA)

MobilityGuard puede integrarse cona una variedad de soluciones de MFA para proporcionar una autenticación sólida en el inicio de sesión. Los usuarios pueden utilizar diferentes métodos de autenticación, como contraseñas, tokens, huellas dactilares o reconocimiento facial, para aumentar la seguridad de la cuenta.

Seguridad del dispositivo

Implemente políticas de seguridad de dispositivo para garantizar que solo los dispositivos aprobados puedan acceder a la red. Esto ayuda a proteger contra amenazas de malware, phishing y otros ataques.

Control de acceso basado en roles

Con MobilityGuard puede permitir a los administradores definir roles de usuario y permisos para acceder a aplicaciones y datos. Los usuarios solo pueden acceder a las aplicaciones y datos que tienen permiso para ver, lo que reduce el riesgo de fugas de datos y otros incidentes de seguridad.

Análisis de riesgos y prevención de amenazas

Realice análisis de riesgos en tiempo real para identificar y prevenir amenazas a la seguridad de la red. Los administradores pueden establecer políticas para bloquear el acceso de dispositivos o usuarios que presenten riesgos de seguridad.

Gestión centralizada

Proporcione una plataforma centralizada para administrar usuarios, dispositivos y aplicaciones con MobilityGuard. Los administradores pueden implementar políticas de seguridad y monitorear el acceso de los usuarios desde una única consola, lo que simplifica la administración de la seguridad de la red.

Cumplimiento normativo

MobilityGuard ayuda a las empresas a cumplir con las regulaciones de privacidad y seguridad de datos, como GDPR y HIPAA. Al proporcionar controles de acceso y autenticación avanzados, MobilityGuard Control de Accesos ayuda a garantizar que los datos confidenciales de la empresa estén protegidos y que se cumplan las regulaciones de privacidad y seguridad.

Auditoría y seguimiento de accesos

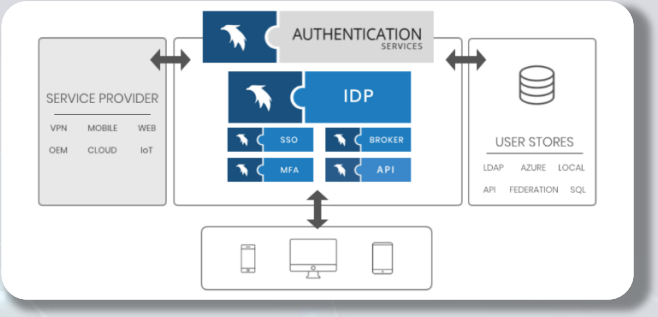
MobilityGuard proporciona herramientas avanzadas de auditoría y seguimiento de accesos, que permiten a los administradores de TI supervisar el acceso a los recursos empresariales. Esto incluye la capacidad de registrar y analizar los intentos de acceso, identificar posibles amenazas y tomar medidas de seguridad proactivas para proteger los recursos empresariales.

Gestión de identidades | PhenixID

PhenixID

Una gestión de identidad y acceso segura y sin complicaciones con PhenixID

PhenixID es una solución de gestión de identidad y acceso (IAM) que permite administrar usuarios, recursos y privilegios en una organización. Ofrece funcionalidades como autenticación, gestión de contraseñas, federación de identidades y seguridad de la información, cumpliendo con normativas de privacidad y protección de datos. Es personalizable y escalable, lo que permite adaptarla a las necesidades específicas de cada organización, mejorando la seguridad y el cumplimiento normativo.



- **Autenticación de usuario**
  PhenixID se emplea para verificar la identidad de los usuarios y habilitarles el acceso a recursos concretos según sus permisos.

- **Gestión de identidades**
  PhenixID sirve para gestionar las identidades de los usuarios, lo que incluye crear, modificar y eliminar cuentas de usuario.

- **Autorización de usuario**
  PhenixID se emplea para dar acceso a los usuarios a recursos particulares de acuerdo con sus funciones y autorizaciones.

- **Gestión de contraseñas**
  Con PhenixID se realiza la gestión de las contraseñas de los usuarios, que incluye la reconfiguración de las contraseñas perdidas y la configuración de políticas para estas.

- **Gestión de acceso**
  PhenixID se usa para gestionar el acceso de los usuarios a recursos concretos, lo cual engloba la definición de reglas de acceso y la auditoría de los accesos.

- **Gestión de privilegios**
  Como herramienta, PhenixID se emplea para administrar los privilegios de los usuarios, lo que implica que estos solo pueden acceder a aquellos recursos que necesitan para desempeñar sus labores.

- **Gestión de grupos**
  PhenixID se emplea para gestionar grupos de usuarios, lo que comprende la creación, modificación y supresión de estos, así como la asignación de usuarios a grupos en particular.

- **Federación de identidades**
  Con PhenixID permite que los usuarios accedan a recursos en otros sistemas utilizando sus credenciales de la misma plataforma/aplicación.

- **Seguridad de la información**
  PhenixID se utiliza para mejorar la seguridad de la información mediante la implementación de políticas de autenticación y autorización más estrictas y la monitorización de las actividades de los usuarios.

- **Single Sign-On (SSO)**
  PhenixID permite la autenticación única con SSO, lo que quiere decir que los usuarios pueden acceder a varios servicios y aplicaciones con un solo inicio de sesión.

- **Cumplimiento normativo**
  Para satisfacer las exigencias normativas, PhenixID cumple con los requisitos de la RGPD y de la LOPD.

- **Integración de aplicaciones**
  PhenixID se utiliza para la integración de aplicaciones, lo que significa que se pueden conectar aplicaciones y sistemas en una organización.

Auditorias y migraciones | AvePoint Fly

AvePoint
AvePoint Fly

Migración a la nube para archivos, correo electrónico y otros contenidos

Consolide fácilmente los inquilinos de Microsoft 365; Google, Slack, Dropbox y Box; o incluso correo autohospedado, SharePoint y archivos compartidos en Microsoft 365 o SharePoint.

- **Fuentes de migración previas al escaneo:**
Descubra cuánto contenido tiene y las personalizaciones y elementos no compatibles que se deben corregir para Microsoft 365 o SharePoint.

- **Migración de correo sencilla:**
Mueva archivos de Exchange, Gmail, IMAP/POP3, PST y otros inquilinos de Exchange Online a Exchange Online.

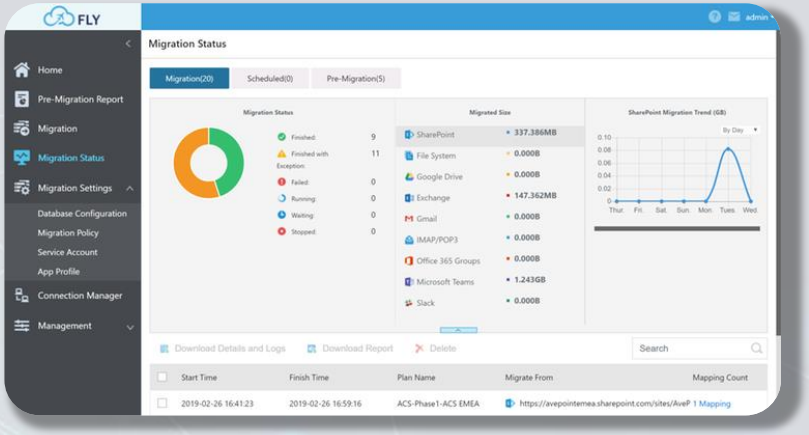
- **Progreso de monitorización:**
Supervise de cerca la limitación, el rendimiento y más con nuestros informes de progreso integrados o plantillas de Power BI.

- **Transforme Microsoft Teams:**
Consolide canales, archivos, sitios u otros equipos para que los usuarios puedan encontrar fácilmente la información que necesitan, en el momento que necesitan.

- **Dominio en la proliferación de datos:**
Limpie su entorno de Teams en rápido crecimiento asegurándose de tener los metadatos, los permisos y los datos adecuados.

- **Impulso de una mayor coherencia:**
Optimice la arquitectura de la información en su entorno de trabajo digital moderno, incluida la fácil actualización de las convenciones de nomenclatura.

- **Migrar únicamente el contenido necesario:**
El modo de migración a la nube de alta velocidad puede mover terabytes de contenido por día.



- **Transición fluida a Microsoft 365:**
Con descubrimiento detallado y análisis de alcance dinámico a través de Power BI, organice su migración por fases utilizando filtros, programaciones e implementaciones por etapas para los usuarios finales

- **Limpie y proteja sus datos:**
Etiquete, organice y clasifique datos por motivos de seguridad e intención.

- **Mapear y transformar:**
Cree políticas para asociar filtros y asignaciones, de modo que los metadatos, los usuarios y los permisos se transfieran sin problemas.

- **Programe según sus términos:**
Ejecutar planes fuera del horario laboral reduce el riesgo de limitación y minimiza la amenaza de interrupción del negocio para sus usuarios.

- **Código en el que puede confiar:**
Utilizamos API de importación de Azure de alta velocidad para garantizar que su contenido llegue a la nube a la velocidad del rayo.

Backups y restauración | AvePoint Cloud Backup

La solución más completa de copias de seguridad de nube a nube

AvePoint Cloud Backup es la solución de copias de seguridad de nube a nube para Microsoft 365 más completa del sector. Gracias a sus copias de seguridad automatizadas e ilimitadas y a su almacenamiento seguro en el Azure Storage de AvePoint o en su propia nube, usted solo tiene que decidir cuántos datos quiere recuperar y cuándo.

Las recuperaciones de datos bajo demanda y granulares a nivel de elemento le dan acceso en todo momento a sus archivos, e-mails, conversaciones, grabaciones, proyectos, tareas, Groups, Teams, Planner y sitios cruciales para el negocio. Ayude a sus usuarios a encontrar su contenido perdido automatizando la restauración con AVA, el asistente virtual de AvePoint.

➢ Copias de seguridad integrales

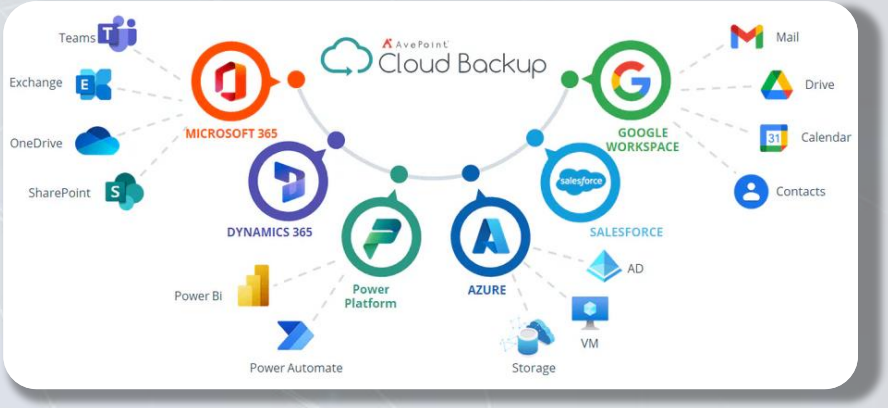
Un servicio de copias de seguridad ilimitadas para sus archivos de Microsoft 365 en SharePoint Online, Exchange Online, Project Online, OneDrive for Business, Groups, Teams, Planner y carpetas públicas.

➢ Recuperación en minutos, en vez de días

Programe restauraciones sin tener que coger el teléfono o ejecute reversiones a nivel de sitio y restaure fácilmente sus archivos de Microsoft 365 en sitios, bibliotecas, OneDrive, buzones de correos, Groups o Teams.

➢ Copias de seguridad sin dolores de cabeza

Se ejecutan copias de seguridad automáticas hasta 4 veces al día y se conservan e 100% de sus datos durante un año. Las suscripciones de copias de seguridad ilimitadas le dan la flexibilidad que usted necesita y la protección que desea.



➢ Copias de seguridad a su gusto

Almacene con toda seguridad sus datos de M365 en nuestro Azure Storage escalable, nube privada, o centro de datos de un proveedor de su elección.

➢ Cumplimiento de normativas y regulaciones

Veeam Backup cumple con los requisitos de cumplimiento de normativas y regulaciones, como HIPAA, GDPR y PCI-DSS, para garantizar la seguridad y privacidad de los datos del usuario.

Backups y restauración | Vembu BDR Suite

Protección de datos empresariales simplificada

Vembu BDR Suite es una solución integral de backup y recuperación de datos que protege la información crítica de las empresas. Permite realizar copias de seguridad programadas y restaurar datos rápidamente, garantizando su disponibilidad ante fallos, errores humanos o desastres. También ofrece replicación remota de datos y se integra con otros sistemas de gestión de TI para mejorar la eficiencia. Con monitoreo y alertas en tiempo real, asegura que los datos estén siempre protegidos y accesibles.

➢ Protección de máquinas virtuales

Mediante el uso de Vembu BDR Suite, es posible crear copias de seguridad de manera regular de las máquinas virtuales en entornos de virtualización, asegurando la protección de la información crítica y su disponibilidad en caso de un fallo del sistema o una interrupción del servicio.

➢ Copia de seguridad de servidores físicos

BDR Suite facilita la realización de copias de seguridad programadas de los servidores físicos, protegiendo la información crítica y asegurando su disponibilidad en caso de un fallo del sistema o una interrupción del servicio.

➢ Recuperación ante desastres

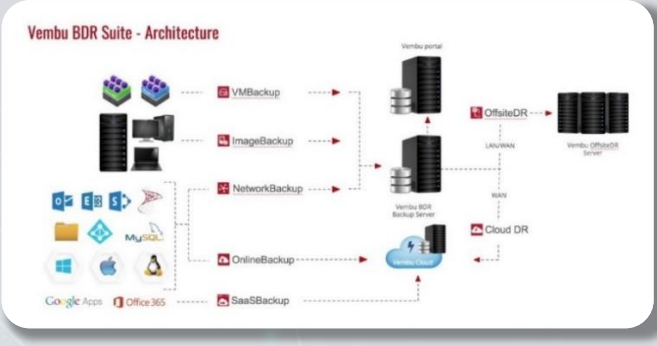
La solución BDR Suite permite recuperar los datos rápidamente a su estado anterior al desastre, ya sea por causas naturales, errores humanos o ciberataques, minimizando el tiempo de inactividad y garantizando la continuidad del negocio.

➢ Migración de datos

BDR Suite simplifica la transferencia de datos de un entorno a otro, permitiendo la migración de datos de un servidor antiguo a uno nuevo o de una plataforma de virtualización a otra.

➢ Copia de seguridad en la nube

BDR Suite ofrece la posibilidad de realizar copias de seguridad en la nube, lo que permite proteger la información crítica ante desastres naturales o ciberataques.



➢ Backup de bases de datos

BDR Suite permite la realización de copias de seguridad de bases de datos, incluyendo Microsoft SQL Server, Oracle y MySQL, garantizando la protección de los datos críticos.

➢ Copia de seguridad de dispositivos móviles

Con BDR Suite es posible realizar copias de seguridad de los datos de dispositivos móviles, protegiendo la información crítica y garantizando su disponibilidad en caso de pérdida o robo.

➢ Supervisión y alertas en tiempo real

La solución BDR Suite ofrece supervisión y alertas en tiempo real, lo que permite a los administradores de TI monitorear el estado de los sistemas y recibir notificaciones en caso de un problema.

➢ Restauración granular

BDR Suite ofrece la posibilidad de restaurar datos de manera regular, lo que significa que es posible recuperar un solo archivo o una sola carpeta en lugar de restaurar todo el sistema, lo que ahorra tiempo y recursos.

➢ Replicación de datos

La solución de BDR Suite facilita la replicación de datos entre ubicaciones geográficas remotas, lo que garantiza la disponibilidad de los datos en caso de una falla en el sitio principal.

Movilidad | Workspace One UEM

Workspace ONE UEM

Protección de datos empresariales simplificada

Workspace Unified Endpoint Management (UEM) es una plataforma basada en la nube de VMware para gestionar de forma centralizada y segura todos los dispositivos de una empresa, incluyendo móviles, portátiles, de escritorio y IoT. Permite implementar políticas de seguridad, distribuir aplicaciones, actualizar firmware y proteger los endpoints contra amenazas. Además, ofrece una experiencia unificada y personalizada para mejorar la productividad y satisfacción de los empleados, reduciendo costos y mejorando la seguridad.

➢ Gestión de contenido y dispositivos

Workspace UEM permite a las empresas gestionar + controlar el acceso y la distribución de contenido empresarial garantizando seguridad y eficiencia en el acceso a dicha información y configurar de forma centralizada los dispositivos de los empleados, incluyendo la configuración de políticas de seguridad, la distribución de aplicaciones y la eliminación remota de datos en caso de pérdida o robo.

➢ Seguridad de Endpoints

Workspace UEM ofrece características de seguridad avanzadas para proteger los endpoints, incluyendo el cifrado de datos, la gestión de contraseñas, la autenticación multifactor y la protección contra malware.

➢ Distribución de aplicaciones

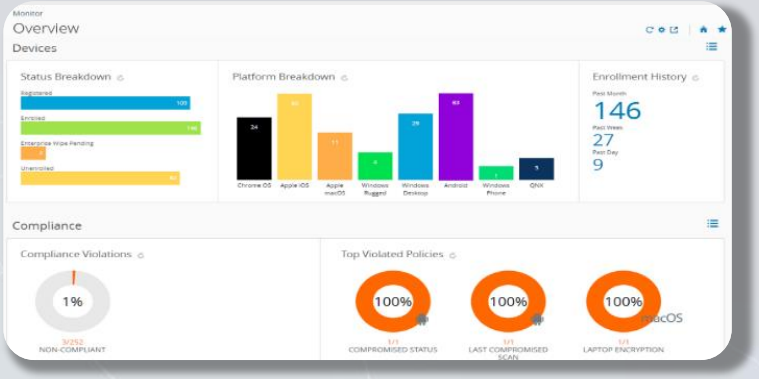
Con Workspace UEM, las empresas pueden distribuir aplicaciones empresariales a los dispositivos de los
empleados de forma segura y sin intervención del usuario, lo que garantiza que los empleados tengan acceso a las aplicaciones que necesitan para realizar su trabajo.

➢ Gestión de identidades

Workspace UEM permite a las empresas gestionar las identidades y los accesos de los empleados a los recursos empresariales, lo que ayuda a prevenir el acceso no autorizado a los datos y aplicaciones empresariales.

➢ Integración de servicios en la nube

Workspace UEM se integra con servicios en la nube como Office 365 y Salesforce, lo que permite a los empleados acceder a estos servicios de forma segura desde sus dispositivos.



➢ Gestión de parches

Workspace UEM permite a los equipos de TI aplicar y controlar de forma centralizada los parches y actualizaciones de software en los dispositivos endpoints de la organización, lo que garantiza que los endpoints se mantengan actualizados y protegidos contra las últimas vulnerabilidades.

➢ Gestión de políticas

Workspace UEM permite a las empresas configurar y aplicar políticas de gestión de endpoints, incluyendo políticas de seguridad y de cumplimiento, lo que ayuda a garantizar que los endpoints se utilicen de manera segura y en cumplimiento de las políticas empresariales.

➢ Análisis de datos y generación de informes

Workspace UEM permite a las empresas recopilar y analizar datos sobre el uso de los endpoints, lo que ayuda a identificar tendencias, problemas y oportunidades de mejora en la gestión de endpoints, y a generar informes para la toma de decisiones empresariales.

➢ Personalización de la experiencia del usuario

Workspace UEM permite a las empresas personalizar la experiencia del usuario en los endpoints, lo que incluye configurar y distribuir aplicaciones empresariales, fondos de pantalla, configuraciones de teclado, entre otras personalizaciones.

Movilidad | SOTI MOBICONTROL

Empodere su empresa móvil

SOTI MobiControl es una plataforma de gestión de movilidad empresarial que permite a las organizaciones administrar y asegurar dispositivos móviles y aplicaciones. Ofrece funciones de gestión de dispositivos móviles (MDM) y gestión de aplicaciones móviles (MAM), controlando la seguridad, el acceso y el uso de los dispositivos y datos. Además, permite personalizar políticas de seguridad, optimizar el rendimiento de los dispositivos y realizar actualizaciones remotas, mejorando la eficiencia y solución de problemas técnicos.

➢ Administración de dispositivos móviles y de IoT

SOTI MobiControl permite a los administradores de TI controlar y administrar una amplia gama de dispositivos móviles y de IoT, incluyendo teléfonos móviles, tabletas, dispositivos de punto de venta (POS), sensores y otros dispositivos conectados.

➢ Seguridad avanzada

SOTI MobiControl cuenta con una amplia variedad de características de seguridad, incluyendo la encriptación de datos, el bloqueo remoto y la eliminación de datos, la autenticación de dos factores, la gestión de contraseñas y el control de acceso a la red.

➢ Gestión de aplicaciones y de contenido

La plataforma de SOTI MobiControl proporciona herramientas avanzadas para gestionar aplicaciones y contenido en dispositivos móviles. Permite a los administradores de TI instalar, actualizar y desinstalar aplicaciones de forma remota, además de establecer políticas y restricciones. También facilita la gestión del contenido almacenado en los dispositivos, asegurando la protección de los datos empresariales y el cumplimiento de las políticas de seguridad.

➢ Control de aplicaciones

Los administradores de TI pueden usar SOTI MobiControl para controlar y gestionar las aplicaciones que se instalan en los dispositivos móviles de la empresa. Esto puede incluir la posibilidad de bloquear o permitir la instalación de ciertas aplicaciones, así como la capacidad de supervisar y actualizar las aplicaciones existentes.

➢ Análisis y generación de informes

SOTI MobiControl ofrece una amplia gama de herramientas de análisis y generación de informes, que permiten a los administradores de TI obtener información valiosa sobre el uso y el estado de los dispositivos móviles y de IoT. Esto les ayuda a tomar decisiones informadas y proactivas en cuanto a la gestión de sus dispositivos móviles.

➢ Integración con otras soluciones empresariales

La plataforma se integra con una amplia gama de soluciones empresariales, como Microsoft Intune, VMware Workspace ONE, Cisco Meraki y BlackBerry Dynamics. Esto permite a las empresas y organizaciones crear un ecosistema completo y eficaz de gestión de dispositivos móviles y de IoT.

➢ Escalabilidad y flexibilidad

La plataforma es altamente escalable y se adapta a las necesidades de las empresas, permitiéndoles controlar y administrar cualquier cantidad de dispositivos móviles y de IoT desde una sola plataforma centralizada. Además, ofrece flexibilidad en cuanto a la personalización y la configuración de las características y herramientas de la plataforma.

➢ Automatización

La plataforma de SOTI MobiControl cuenta con una serie de herramientas de automatización que permiten a los administradores de Ti automatizar tareas y procesos para ahorrar tiempo y mejorar la eficiencia. Por ejemplo, se pueden establecer políticas y acciones automatizadas para la gestión de dispositivos y aplicaciones.

➢ Facilidad de uso

SOTI MobiControl cuenta con una interfaz de usuario intuitiva y fácil de usar, que permite a los administradores de TI gestionar y controlar dispositivos móviles y de IoT de manera rápida y eficiente. Además, ofrece una serie de herramientas de soporte y formación para ayudar a los usuarios a aprovechar al máximo la plataforma.

Movilidad | Ivanti Endpoint Manager

Controla tus dispositivos móviles de principio a fin con Ivanti Endpoint Manager Mobile

Ivanti Endpoint Manager Mobile es una solución MDM que permite gestionar y asegurar dispositivos móviles desde una plataforma centralizada. Ofrece herramientas para la gestión de dispositivos, protección de datos, control de gastos y soporte remoto. Los administradores pueden establecer políticas de seguridad, configurar dispositivos, automatizar procesos y acceder a informes. Ayuda a proteger datos empresariales, garantizar el cumplimiento de políticas de seguridad y reducir costos, mejorando la eficiencia del soporte técnico.

➢ Administración de dispositivos móviles

Ivanti Endpoint Manager Mobile permite a los administradores de TI gestionar dispositivos móviles, incluidos los personales, desde una sola consola. Pueden controlar políticas de seguridad, actualizaciones de software y configuraciones para mantener los dispositivos seguros y actualizados.

➢ Protección de datos

Ivanti Endpoint Manager Mobile ayuda a proteger los datos confidenciales en dispositivos móviles mediante políticas de seguridad como cifrado, autenticación de usuarios y borrado remoto. También permite monitorear el uso de datos y aplicaciones para detectar actividades sospechosas.

➢ Gestión de aplicaciones

Ivanti Endpoint Manager Mobile permite a los administradores de TI distribuir y gestionar aplicaciones en dispositivos móviles. Pueden agregar o eliminar aplicaciones y actualizarlas según sea necesario, lo que les permite mantener a los usuarios finales actualizados con las últimas versiones de las aplicaciones empresariales.

➢ Control de gastos

Ivanti Endpoint Manager Mobile ayuda a las empresas a controlar los costos de dispositivos móviles al monitorear el uso de datos y llamadas, optimizando planes de datos y voz. También permite controlar el uso de roaming para evitar costos excesivos en el extranjero.

➢ Cumplimiento de las políticas de seguridad

Ivanti Endpoint Manager Mobile permite a los administradores de TI establecer y hacer cumplir políticas de seguridad para los dispositivos móviles, incluidas las contraseñas de seguridad, las restricciones de uso de la cámara y los límites en la instalación de aplicaciones no autorizadas. Esto ayuda a garantizar que los dispositivos móviles sean seguros y cumplan con los requisitos de cumplimiento.

➢ Implementación de las políticas de acceso

Ivanti Endpoint Manager Mobile permite a los administradores de TI establecer políticas de acceso a los recursos empresariales, como aplicaciones y datos, para los usuarios móviles. Esto les permite asegurarse de que solo los usuarios autorizados puedan acceder a la información confidencial y reducir el riesgo de filtración de datos.

➢ Automatización de procesos

Ivanti Endpoint Manager Mobile permite a los administradores de TI automatizar procesos comunes, como la distribución de actualizaciones de software y parches de seguridad. Esto ayuda a reducir la carga de trabajo de los equipos de TI y a garantizar que los dispositivos móviles estén actualizados con las últimas versiones de software y parches de seguridad.

➢ Informes y análisis

Ivanti Endpoint Manager Mobile proporciona informes y análisis detallados sobre el uso de dispositivos móviles en la organización, lo que incluye el uso de datos, el uso de aplicaciones y el cumplimiento de políticas de seguridad. Esto ayuda a los administradores de TI a tomar decisiones informadas sobre la gestión de dispositivos móviles y garantiza que la organización esté en cumplimiento de las políticas de seguridad.

Movilidad | Ivanti Neurons for MDM

Mejores experiencias, mejores resultados

Ivanti Neurons for MDM es una plataforma que permite gestionar y asegurar dispositivos móviles, cumpliendo con las políticas de la empresa. Facilita la inscripción, configuración y gestión de dispositivos, así como el despliegue de aplicaciones. Asegura la seguridad mediante políticas como la complejidad de contraseñas y cifrado, y permite borrar dispositivos de forma remota y generar informes de cumplimiento. Ayuda a las organizaciones a administrar dispositivos de manera eficiente y segura.

➢ Gestión unificada de endpoints

Ivanti Neurons proporciona una solución de gestión unificada de endpoints (dispositivos, aplicaciones y usuarios) que permite a los administradores de TI controlar y proteger una amplia variedad de endpoints desde una sola consola. Esto incluye dispositivos móviles, endpoints de escritorio, servidores y dispositivos IoT.

➢ Automatización

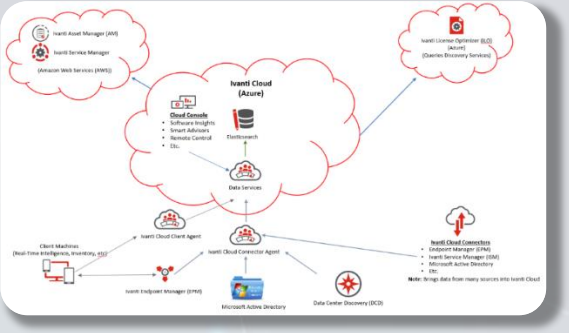
La plataforma utiliza la inteligencia artificial (IA) para automatizar tareas y procesos en la gestión de endpoints. Esto incluye la identificación y resolución proactiva de problemas, la aplicación de parches y actualizaciones de software, y la implementación de políticas de seguridad.

➢ Seguridad avanzada

Ivanti Neurons ofrece una amplia gama de herramientas de seguridad avanzada, incluyendo el cifrado de datos, el control de acceso y la protección contra amenazas de seguridad. La plataforma utiliza la IA para identificar y remediar automáticamente los riesgos de seguridad.

➢ Análisis avanzado de datos

La plataforma recopila y analiza datos de endpoints, usuarios y aplicaciones, lo que permite a los administradores de TI obtener información valiosa sobre el rendimiento y la seguridad de los sistemas. Ivanti Neurons utiliza la IA para identificar patrones y tendencias en los datos, lo que ayuda a los administradores de TI a tomar decisiones informadas sobre la gestión de endpoints.



➢ Experiencia de usuario mejorada

La plataforma de Ivanti Neurons se enfoca en mejorar la experiencia del usuario final al proporcionar una gestión y soporte más rápido y eficiente de los endpoints. Ivanti Neurons utiliza la IA para identificar y solucionar problemas antes de que afecten a los usuarios finales, lo que ayuda a reducir los tiempos de inactividad y aumenta la satisfacción del usuario.

➢ Integración con otros sistemas

Ivanti Neurons se integra con otros sistemas y herramientas empresariales, lo que permite a los administradores de TI aprovechar al máximo sus inversiones existentes. La plataforma es compatible con una amplia gama de soluciones de seguridad, gestión de servicios de TI (ITSM) y automatización de procesos empresariales (BPA).

➢ Automatización de procesos de negocio

Ivanti Neurons puede automatizar procesos empresariales y de TI mediante el uso de flujos de trabajo y bots de software que pueden interactuar con otros sistemas y plataformas empresariales.

➢ Análisis predictivo

Ivanti Neurons utiliza el análisis predictivo para identificar posibles problemas y amenazas antes de que ocurran. Esto ayuda a los administradores de TI a tomar medidas preventivas para evitar problemas y reducir el tiempo de inactividad.

Movilidad | MaaS360

IBM **MaaS360**

Movilidad simplificada, seguridad maximizada

MaaS360 es una plataforma MDM en la nube que permite gestionar y proteger dispositivos móviles, aplicaciones y contenidos desde una consola centralizada. Los administradores pueden configurar políticas de seguridad, implementar actualizaciones, monitorear el uso de datos y controlar el acceso a la red corporativa. Ofrece herramientas MAM para asegurar el uso de aplicaciones aprobadas y funciones de análisis e informes sobre el rendimiento y la seguridad. Con MaaS360, las empresas protegen sus dispositivos y datos mientras mantienen la productividad.

➢ Administración de dispositivos móviles

MaaS360 se utiliza ampliamente para la gestión de dispositivos móviles en entornos empresariales. Los administradores de TI pueden utilizar la plataforma para inscribir, configurar y monitorizar dispositivos móviles y garantizar que estén actualizados con las últimas políticas de seguridad.

➢ Administración de aplicaciones móviles

MaaS360 también se utiliza para administrar las aplicaciones móviles en dispositivos empresariales. Los administradores pueden controlar el acceso a las aplicaciones, aprobar o denegar la instalación de aplicaciones y enviar actualizaciones de aplicaciones a los dispositivos.

➢ Seguridad de los datos móviles

Las empresas pueden utilizar MaaS360 para garantizar que los datos móviles estén protegidos en todo momento. La plataforma ofrece controles de seguridad avanzados, como la encriptación de datos, la autenticación de usuarios y la eliminación remota de datos, en caso de pérdida o robo del dispositivo.

➢ Administración de la red móvil

Administre y asegure la red móvil de una empresa. Los administradores pueden controlar el acceso a la red y aplicar políticas de seguridad en tiempo real para proteger la red contra amenazas de seguridad.

➢ Análisis y generación de informes

MaaS360 también proporciona capacidades de análisis y generación de informes, lo que permite a los administradores de TI obtener información detallada sobre el uso de dispositivos móviles y aplicaciones en la empresa. Los informes pueden ayudar a los administradores a identificar tendencias y problemas de seguridad potenciales y tomar medidas proactivas para abordarlos.

➢ Cumplimiento normativo

MaaS360 es una herramienta valiosa para ayudar a las empresas a cumplir con las normas y regulaciones relacionadas con la protección de datos, como HIPAA, GDPR, SOX y PCI-DSS. Los administradores pueden utilizar la plataforma para garantizar que los dispositivos y datos móviles estén protegidos según los requisitos de cumplimiento.

➢ Administración de dispositivos IoT

MaaS360 también se puede utilizar para administrar dispositivos IoT (Internet de las cosas) en entornos empresariales. Los administradores pueden configurar y supervisar los dispositivos IoT para asegurarse de que estén actualizados y protegidos contra amenazas de seguridad.

➢ Administración de dispositivos personales

Con el aumento de la tendencia BYOD (Bring Your Own Device), MaaS360 también se puede utilizar para gestionar dispositivos personales de los empleados que se utilizan para fines de trabajo. Los administradores pueden asegurar que los datos corporativos estén protegidos en los dispositivos personales de los empleados, al tiempo que respetan la privacidad y los derechos de propiedad de los mismos.

Movilidad | Samsung Knox

SAMSUNG Knox

Movilidad simplificada, seguridad maximizada

Samsung Knox es una plataforma de seguridad móvil que protege datos personales y empresariales en dispositivos Samsung. Ofrece un entorno seguro para aplicaciones empresariales y personales, y se usa en sectores como salud, finanzas, gobierno y defensa. Permite a los empleados usar dispositivos personales sin comprometer la seguridad empresarial y ofrece herramientas de control parental y restricciones de acceso. Es una solución completa que garantiza la seguridad y privacidad de los datos en diversos entornos.

- **Seguridad empresarial**
Samsung Knox proporciona seguridad para los dispositivos móviles que se utilizan en el entorno empresarial. Los empleados pueden acceder a datos confidenciales de la empresa de manera segura sin preocuparse por posibles violaciones de seguridad.

- **Protección de datos personales**
Samsung Knox protege los datos personales almacenados en el dispositivo contra posibles ataques de hackers y otros ciberdelincuentes. Los usuarios pueden estar seguros de que sus datos personales están seguros y protegidos.

- **Aplicaciones seguras**
Samsung Knox proporciona un entorno seguro para las aplicaciones empresariales y personales. Las aplicaciones están protegidas contra posibles ataques de malware y virus, lo que ayuda a garantizar que los usuarios puedan utilizar sus aplicaciones de manera segura.

- **Control parental**
Samsung Knox también puede utilizarse como una herramienta de control parental para ayudar a proteger a los niños de contenido inapropiado en Internet. Los padres pueden utilizar la plataforma para establecer límites de tiempo y restringir el acceso a determinados sitios web y aplicaciones.

- **Protección de pagos móviles**
Samsung Knox puede utilizarse para proteger los pagos móviles y las transacciones financieras realizadas a través del dispositivo. Los usuarios pueden estar seguros de que sus datos financieros están seguros y protegidos contra posibles ataques.

- **Teletrabajo**
Con la pandemia de COVID-19, el teletrabajo se ha vuelto cada vez más común. Samsung Knox ayuda a garantizar la seguridad de los dispositivos utilizados para trabajar desde casa, evitando que los datos empresariales confidenciales sean vulnerables a posibles ataques.

- **BYOD (Bring Your Own Device)**
El uso de dispositivos personales en el entorno empresarial se ha vuelto cada vez más común. Con Samsung Knox, los empleados pueden utilizar sus propios dispositivos sin comprometer la seguridad de los datos empresariales.

- **Sector financiero**
En el sector financiero, la seguridad de los datos es esencial. Samsung Knox puede utilizarse para proteger los datos financieros y personales de los clientes contra posibles ataques de ciberdelincuentes.

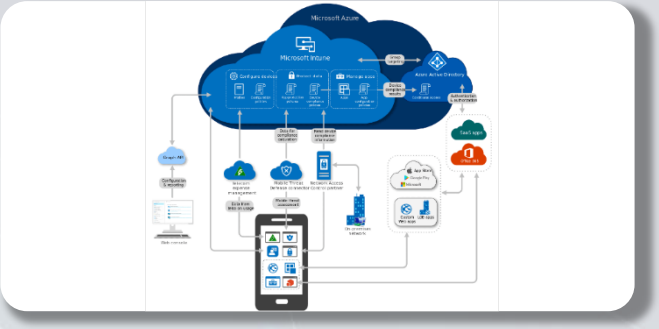
- **Salud**
En el sector de la salud, la seguridad de los datos del paciente es fundamental. Samsung Knox puede utilizarse para proteger los datos médicos y personales de los pacientes, garantizando que sean seguros y confidenciales.

- **Gobierno y defensa**
En el sector gubernamental y de defensa, la seguridad de los datos confidenciales es crítica. Samsung Knox puede utilizarse para proteger los datos gubernamentales y militares contra posibles ataques de ciberdelincuentes y otras amenazas.

Movilidad | Microsoft Intune

Administre todo: dispositivos, aplicaciones, datos…

Microsoft Intune es una plataforma de administración de dispositivos móviles y de escritorio en la nube que permite a las empresas proteger y gestionar dispositivos y datos. Ofrece funciones como la administración de dispositivos, protección de datos, políticas de seguridad y gestión de aplicaciones. También permite la administración en entornos de nube híbrida y protege el correo electrónico empresarial. Intune es escalable y ayuda a mejorar la eficiencia y seguridad en diversas plataformas, siendo una solución valiosa para las empresas.



Administración de dispositivos móviles (MDM)
Intune permite a los administradores de TI controlar y administrar dispositivos móviles en toda la organización. Los usuarios pueden acceder a aplicaciones y datos de trabajo en sus dispositivos personales de forma segura, sin comprometer la seguridad de los datos corporativos.

Administración de aplicaciones
Intune permite a los administradores de TI distribuir, configurar y actualizar aplicaciones en dispositivos móviles y de escritorio. Los usuarios pueden acceder a las aplicaciones necesarias para realizar su trabajo, lo que aumenta la productividad y la eficiencia.

Protección de datos
Intune ayuda a proteger los datos de la empresa en dispositivos móviles y de escritorio, ya sea mediante el cifrado de datos, la restricción de acceso a ciertas aplicaciones o mediante la eliminación remota de datos si un dispositivo se pierde o es robado.

Administración de actualizaciones
Intune permite a los administradores de TI administrar y controlar las actualizaciones de software en dispositivos móviles y de escritorio, lo que ayuda a mantener los dispositivos seguros y actualizados.

Configuración de políticas de seguridad
Configure políticas de seguridad para dispositivos móviles y de escritorio. Esto incluye el establecimiento de contraseñas complejas, la implementación de medidas de autenticación de dos factores y la configuración de políticas de acceso a la red.

Administración de perfiles
Intune permite a los administradores de TI crear y aplicar perfiles de configuración para dispositivos móviles y de escritorio. Esto incluye la configuración de la conexión a la red, la configuración de correo electrónico y la configuración de la política de seguridad.

Administración de dispositivos en la nube híbrida
Intune también puede administrar dispositivos que se ejecutan en entornos de nube híbrida, lo que significa que se pueden administrar dispositivos tanto en la nube como en la infraestructura local.

Protección de correo electrónico
Intune también puede ayudar a proteger el correo electrónico empresarial de la organización mediante la configuración de políticas de seguridad para el correo electrónico, como la detección de malware y la prevención de pérdida de datos.

Administración de dispositivos Windows 10
Intune permite a los administradores de TI administrar dispositivos Windows 10 en toda la organización. Esto incluye la configuración de políticas de seguridad y la implementación de actualizaciones de software.

Administración de dispositivos macOS
Intune también permite la administración de dispositivos macOS en la organización. Esto incluye la configuración de políticas de seguridad y la implementación de actualizaciones de software.