ABOX

Catálogo de seguridad 2024

Índice

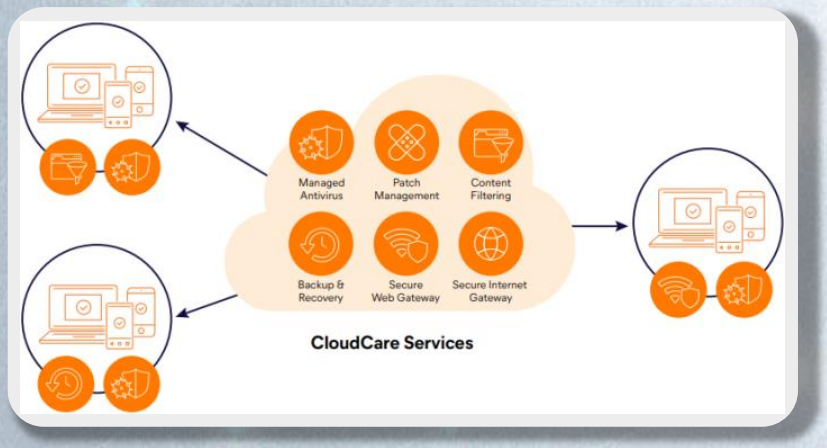
Antivirus | Avast CloudCare 3
Antivirus MTD | Zimperium 4
Antivirus MTD | Lookout 5
Antivirus MTD | Harmony Mobile Security 6
Firewall | Clavister Netwall – NGFW 7
Firewall | Clavister Netwall – NGFW 8
Firewall | Clavister Netwall – NGFW 9
Firewall | Clavister Netwall - NGFW 10
Firewall | Clavister Netwall - NGFW 11
Firewall | Clavister Netwall - Virtual 12
Monitorización | Fastvue 13
Monitorización | WebSpy 14
Monitorización | Promodag 15
Filtrado de contenidos | ModusCloud 16
Filtrado de contenidos | ContentKeeper 17
Filtrado de contenidos | MailCleaner 18
Filtrado de contenidos | Hornet Security 19
Gestión de identidades | HelloID 20
Gestión de identidades | MobilityGuard 21
Gestión de identidades | PhenixID 22
Gestión de identidades | SSRPM 23
Backups y restauración | Veeam 24
Backups y restauración | Vembu BDR Suite 25
Movilidad | Workspace One UEM 26
Movilidad | SOTI MOBICONTROL 27
Movilidad | Ivanti Endpoint Manager 28
Movilidad | Ivanti Neurons for MDM 29
Movilidad | MaaS360 30
Movilidad | Samsung Knox 31
Movilidad | Microsoft Intune 32

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 ofrece protección para las empresas de cualquier tamaño. La plataforma de Avast CloudCare es fácil de usar y proporciona una amplia gama de características, incluyendo antivirus, protección de correo electrónico, seguridad de red y mucho más. Con su sistema de administración centralizada, Avast CloudCare permite a los administradores de IT gestionar y monitorear la seguridad de la red desde cualquier lugar y en cualquier momento.

La solución antivirus de Avast CloudCare utiliza tecnología de vanguardia para garantizar la detección y eliminación de virus, malware y otras amenazas informáticas. La protección de correo electrónico de Avast CloudCare utiliza un filtro antispam para mantener los correos electrónicos no deseados fuera de la bandeja de entrada, y una protección antiphishing para prevenir la suplantación de identidad. La seguridad de red de Avast CloudCare incluye cortafuegos y detección de intrusiones para proteger la red de la empresa 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

Proteja sus endpoint móviles

Zimperium Mobile Threat Defense (MTD), anteriormente conocida como zIPS, es una aplicación que prioriza la privacidad y proporciona seguridad móvil integral para empresas. Está diseñado para proteger dispositivos de propiedad corporativa y/o BYO (bring-your-own/traiga el suyo) de amenazas persistentes avanzadas en cuatro categorías: dispositivos, redes, phishing y ataques a aplicaciones.

La detección basada en aprendizaje automático de Zimperium proporciona prevención contra las últimas amenazas móviles, incluido el malware de día cero. Zimperium se compromete a ofrecer las mejores soluciones de seguridad móvil para proteger a los clientes del creciente volumen y gravedad de las amenazas móviles. Como parte de ese compromiso, se contrató a AV-TEST GmbH para una evaluación de su solución Mobile Threat Defense, zIPS. Esta evaluación encuentra que Zimperium detecta más del 99 % del malware y las aplicaciones maliciosas (Fuente: https://get.zimperium.com/av-test-evaluation/)

Por último, Zimperium brinda cobertura de seguridad completa en Android, iOS y ChromeOS, ya sea desde una tablet como un smartphone.

➢ 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 al brindarles configuraciones de usuario 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 también proporciona análisis forense móvil crítico necesario para que los equipos de seguridad evalúen y respondan a incidentes de seguridad, reduciendo el tiempo medio de reparación. A través de integraciones con los principales sistemas MDM/EMM/UEM, SIEM, SOAR y XDR, los equipos de respuesta a incidentes finalmente tienen visibilidad de las amenazas y riesgos móviles. Los análisis forenses de Zimperum MTD evitan que un dispositivo comprometido se convierta en un brote. Al recopilar datos forenses sobre el dispositivo, las conexiones de red y las aplicaciones maliciosas, los equipos de operaciones de seguridad pueden revisar dichos análisis y minimizar los riesgos.

➢ Implementación Zero Touch

Implemente y active Zimperium MTD en los terminales móviles Endpoint de sus empleados y contratistas sin la necesidad de complicados 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

En un momento en el que las ciber amenazas están en auge y con el aumento de la flexibilidad para trabajar en cualquier lugar (incluso conectado desde el móvil), es una misión crítica proteger los dispositivos de tu empresa y de tus empleados a todos los niveles con las soluciones MTD.
Lookout Mobile Threat Defense es una aplicación que se instala en los dispositivos móviles (disponible para iOS, Android y Chrome OS) y que los protege contra todo tipo de amenazas, 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.
- Adecuado para empresas de todos los tamaños: SOHO a corporaciones multinacionales.
- Despliegue sin fricciones, experiencia simple de usuario.
- 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:

- 85% de los ataques de phishing en dispositivos móviles ocurren fuera del correo electrónico.
- 91% de los ciberataques empresariales comienzan con un correo electrónico de spear phishing.

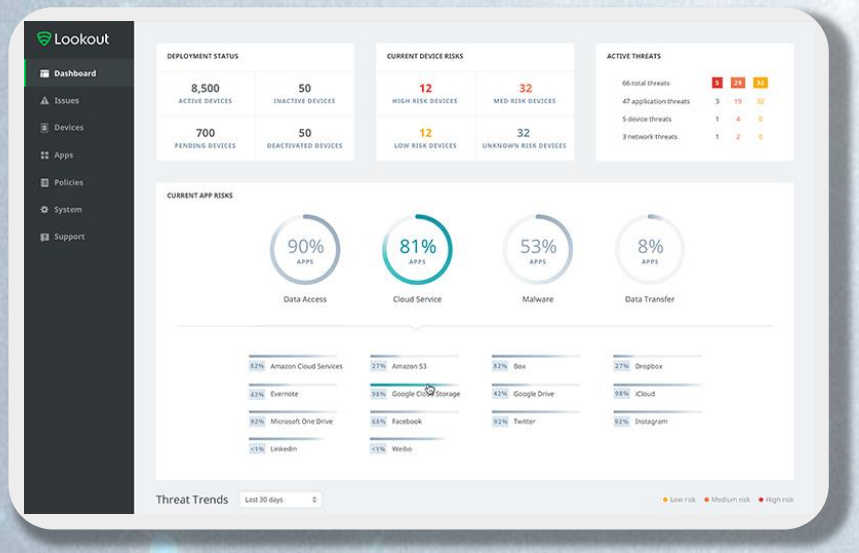
Lookout detecta y bloquea la navegación del usuario a un sitio de phishing en todos los puntos de entrada manteniendo seguros el dispositivo, el usuario y la organización, todo esto sin acceder a los datos del usuario ni enrutar el tráfico a la nube para su inspección.

Detección de malware:

- Lookout vio un aumento del 120% en las amenazas de aplicaciones móviles de 2021 a 2022
- 41% de los usuarios de Lookout reciben una alerta sobre un evento de amenaza móvil dentro de los primeros 90 días.

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 (Mobile Device Manager)" 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

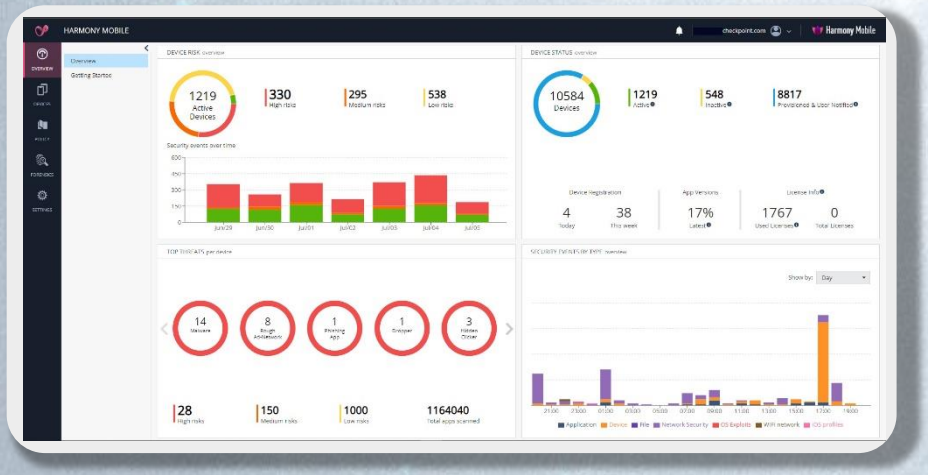
Protege contra amenazas provenientes de la manipulación no autorizada del dispositivo, modificación del sistema operativo, (Jailbreak o rooting) para evadir controles de seguridad o instalar aplicaciones no permitidas o maliciosas (software espía).

Antivirus MTD | Harmony Mobile Security

Seguridad móvil: robusta, ágil y transparente

La seguridad móvil es una de las principales preocupaciones de todas las empresas hoy en día, y por una buena razón. Como es normal, sus trabajadores remotos acceden cada vez más a los datos corporativos desde sus dispositivos móviles, y eso significa que está más expuesto que nunca a filtraciones de datos.

Harmony Mobile es la solución de defensa contra amenazas móviles líder en el mercado. Mantiene tus datos corporativos seguro al proteger los dispositivos móviles de los empleados en todos los vectores de ataque: aplicaciones, archivos, redes y sistemas operativos.
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 compañía líder en seguridad cibernética que ofrece una amplia gama de soluciones de seguridad, incluyendo Next-Generation Firewalls (NGFW) Los NGFW de Clavister proporcionan una seguridad de red avanzada y completa que incluye la inspección profunda de paquetes, la prevención de intrusiones, el filtrado de contenido, la protección contra malware y mucho más. Además, los NGFW de Clavister utilizan tecnologías avanzadas, como el aprendizaje automático y la inteligencia artificial, para garantizar una detección y prevención proactivas de amenazas.

Los NGFW de Clavister son altamente personalizables y escalables, lo que permite a las empresas adaptar su seguridad de red a sus necesidades específicas. Además, Clavister ofrece una plataforma de gestión centralizada que permite a las empresas monitorear y administrar de manera eficiente su seguridad de red.

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.

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.

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.

Firewall | Clavister Netwall - NGFW

Clavister NetWall 100 Series

La arquitectura de la serie 100 de Clavister NetWall está diseñada para brindar una mayor visibilidad, protección y rendimiento de la red, lo que ayuda a los gerentes de TI y administradores de sistemas a abordar algunos de los mayores desafíos que enfrentan las redes hoy en día. Estos NGFW abordan las crecientes violaciones y protegen contra las amenazas emergentes con el líder en la industria Secure SD-WAN en una aplicación sencilla, asequible y flexible de implementar.

Características Técnicas	Netwall 110	Netwall 140
Rendimiento del firewall	1 Gbps	4 Gbps
Rendimiento de VPN	42.000 Conexion/es	42.000 Conexión/es
Sesiones concurrentes	128.000	256.000
Sesiones VPN conrurrentes (IPsec)	50	100
VLANs	128	128
Virtual Routers	10	10
Interfaces	4 x 1GbE (RJ45)	4 x 1GbE (RJ45)

Aspectos destacados

- Provisionamiento sin contacto - para una implementación simple y rentable.
- Conjunto de características de NGFW completamente habilitado.
- SSL VPN para soportar trabajo remoto seguro con clientes Windows, macOS e iOS incluidos.
- Fácil de implementar nuevos firewalls usando plantillas de configuración personalizadas con herramientas de gestión centralizadas.
- Incluido con herramientas de análisis en la nube para proporcionar solución de problemas en tiempo real y paneles de vista general.
- Puntuación de ciberseguridad única para análisis de seguridad simplificados y prácticos.
- Application Visibility & Control con alta granularidad y soporte para más de 3000 aplicaciones únicas.
- Integración de Sistema de Detección/Protección de Intrusión con actualizaciones en tiempo real.
- Protección contra botnets y denegación de servicio (DoS) mediante fuentes de reputación de IP actualizadas continuamente.

	Basics	Essentials	Enhanced
Soporte técnico (24/7)	●	●	●
Reemplazo de hardware	●	●	●
Gestión Centralizada	●	●	●
Actualizaciones de software	●	●	●
Clavister OneConnect		●	●
Geobloqueo		●	●
Alta disponibilidad		●	●
Visibilidad y control de aplicaciones		●	●
Inteligencia de dispositivos		●	●
Escaneo Antivirus			●
Prevención de intrusiones			●
Reputación de IP			●
Filtrado de contenidos Web			●
Protección DoS			●
Bloqueo de Botnet			●

Firewall | Clavister Netwall - NGFW

Clavister NetWall 300 Series

La arquitectura de la serie 300 de Clavister NetWall está diseñada para brindar una mayor visibilidad, protección y rendimiento de la red, lo que ayuda a los gerentes de TI y administradores de sistemas a abordar algunos de los mayores desafíos que enfrentan las redes hoy en día. Estos NGFW abordan los crecientes riesgos y protegen contra las amenazas emergentes con el líder en la industria Secure SDWAN en una aplicación sencilla, asequible y flexible de implementar.

Aspectos destacados

- Provisionamiento sin contacto - para una implementación simple y rentable.
- Conjunto de características de NGFW completamente habilitado.
- SSL VPN para soportar trabajo remoto seguro con clientes Windows, macOS e iOS incluidos.
- Fácil de implementar nuevos firewalls usando plantillas de configuración personalizadas con herramientas de gestión centralizadas.
- Incluido con herramientas de análisis en la nube para proporcionar solución de problemas en tiempo real y paneles de vista general.
- Puntuación de ciberseguridad única para análisis de seguridad simplificados y prácticos.
- Application Visibility & Control con alta granularidad y soporte para más de 3000 aplicaciones únicas.
- Integración de Sistema de Detección/Protección de Intrusión con actualizaciones en tiempo real.
- Protección contra botnets y denegación de servicio (DoS) mediante fuentes de reputación de IP actualizadas continuamente.

Características Técnicas	Netwall 310	Netwall 340
Rendimiento del firewall	4 Gbps	8 Gbps
Rendimiento de VPN	1000 Mbps	2000 Mbps
Sesiones concurrentes	500.000	1.000.000
Sesiones VPN conrurrentes (IPsec)	500	1000
VLANs	256	512
Virtual Routers	20	50
Interfaces	6 x 1GbE (Rj45), 2 x 1GbE (SFP)	6 x 1GbE (Rj45), 2 x 1GbE (SFP)

	Basics	Essentials	Enhanced
Soporte técnico (24/7)	●	●	●
Reemplazo de hardware	●	●	●
Gestión Centralizada	●	●	●
Actualizaciones de software	●	●	●
Clavister OneConnect		●	●
Geobloqueo		●	●
Alta disponibilidad		●	●
Visibilidad y control de aplicaciones		●	●
Inteligencia de dispositivos		●	●
Escaneo Antivirus			●
Prevención de intrusiones			●
Reputación de IP			●
Filtrado de contenidos Web			●
Protección DoS			●
Bloqueo de Botnet			●

Firewall | Clavister Netwall - NGFW

Clavister NetWall 500 Series

La arquitectura de la serie 500 de Clavister NetWall está diseñada para brindar una mayor visibilidad, protección y rendimiento de la red, lo que ayuda a los gerentes de TI y administradores de sistemas a abordar algunos de los mayores desafíos que enfrentan las redes hoy en día. Estos NGFW abordan lo crecientes riesgos y protegen contra las amenazas emergentes con el líder en la industria Secure SDWAN en una aplicación sencilla, asequible y flexible de implementar.

Características Técnicas	Netwall 510	Netwall 550
Rendimiento del firewall	8 Gbps	14 Gbps
Rendimiento de VPN	2 Gbps	4 Gbps
Sesiones concurrentes	1.000.000	2.000.000
Sesiones VPN conrurrentes (IPsec)	500	1000
VLANs	256	512
Virtual Routers	20	50
Interfaces	6 x 1GbE (Rj45), 2 x 10 GbE (SFP)	6 x 1GbE (Rj45), 2 x 10 GbE (SFP)

Aspectos destacados

- Provisionamiento sin contacto - para una implementación simple y rentable.
- Conjunto de características de NGFW completamente habilitado.
- SSL VPN para soportar trabajo remoto seguro con clientes Windows, macOS e iOS incluidos.
- Fácil de implementar nuevos firewalls usando plantillas de configuración personalizadas con herramientas de gestión centralizadas.
- Incluido con herramientas de análisis en la nube para proporcionar solución de problemas en tiempo real y paneles de vista general.
- Puntuación de ciberseguridad única para análisis de seguridad simplificados y prácticos.
- Application Visibility & Control con alta granularidad y soporte para más de 3000 aplicaciones únicas.
- Integración de Sistema de Detección/Protección de Intrusión con actualizaciones en tiempo real.
- Protección contra botnets y denegación de servicio (DoS) mediante fuentes de reputación de IP actualizadas continuamente.

	Basics	Essentials	Enhanced
Soporte técnico (24/7)	●	●	●
Reemplazo de hardware	●	●	●
Gestión Centralizada	●	●	●
Actualizaciones de software	●	●	●
Clavister OneConnect		●	●
Geobloqueo		●	●
Alta disponibilidad		●	●
Visibilidad y control de aplicaciones		●	●
Inteligencia de dispositivos		●	●
Escaneo Antivirus			●
Prevención de intrusiones			●
Reputación de IP			●
Filtrado de contenidos Web			●
Protección DoS			●
Bloqueo de Botnet			●

Firewall | Clavister Netwall - NGFW

Clavister NetWall 6000 Series

Clavister NetWall 6000 es una serie de firewalls de última generación (NGFW) que ofrecen alto rendimiento, escalabilidad y flexibilidad de implementación, una combinación perfecta cuando busca proteger centros de datos, proveedores de servicios y grandes empresas. La serie NetWall 6000 viene con características seguras de SD-WAN para cubrir redes distribuidas y híbridas y es capaz de servir una amplia variedad de casos de uso contra amenazas cibernéticas avanzadas. También incluye Clavister OneConnect SSL VPN para apoyar el trabajo remoto seguro con clientes de Windows, Android, macOS e iOS.

Aspectos destacados

- Fácil de implementar y con flexibilidad SD-WAN, para hubs o puntos remotos.
- Conjunto completo de características de Firewall de última generación.
- SSL VPN para soportar trabajo remoto seguro con clientes Windows, macOS e iOS incluidos.
- Rendimiento sobresaliente con hasta 50 Gbps de rendimiento de firewall y hasta 15 Gbps de rendimiento de SDWAN.
- Sencillo de implementar nuevos firewalls utilizando plantillas de configuración personalizadas con herramienta de gestión centralizada.
- Incluido con herramientas de análisis en la nube para proporcionar solución de problemas en tiempo real y paneles de control general.
- Puntuación de Ciberseguridad Única para análisis de seguridad simplificados y accionables.
- Visibilidad y control de aplicaciones con alta granularidad y soporte para más de 3000 aplicaciones únicas.
- Sistema integrado de Detección/Protección de Intrusos con actualizaciones en tiempo real.
- Protección de botnets y ataques de denegación de servicio (DoS) a través de feeds de reputación de IP actualizados continuamente.

Características Técnicas	Netwall 6200	Netwall 6600
Rendimiento del firewall	20 Gbps	50 Gbps
Rendimiento de VPN	1Gbps/5 Gbps	1 Gbps/15 Gbps
Sesiones concurrentes	5.000.000	8.000.000
Sesiones VPN conrurrentes (IPsec)	2500	5000
VLANs	4096	4096
Virtual Routers	250	500
Interfaces	8x 1 GbE (RJ45), 2x 10 GbE (SFP+)	8x 1 GbE (RJ45), 2x 10 GbE (SFP+)

	Essentials	Enhanced	Premium*
Funciones básicas del cortafuegos	●	●	●
Control de aplicaciones	●	●	●
Clavister InCenter Cloud	●	●	●
Inteligencia de dispositivos	●	●	●
Antivirus		●	●
Filtrado de contenidos Web		●	●
Reputación de IP		●	●
Clavister OneConnect		●	●
Características de SD-WAN		●	●
Licencia/Servicio de NetEye			●
(NetEye VM gratis, hardware a coste)			●

Firewall | Clavister Netwall - Virtual

Clavister NetWall Virtual Models

La arquitectura de la serie Clavister NetWall Virtual está diseñada para proporcionar una mayor visibilidad, protección y rendimiento de red mejorado para ayudar a los gerentes de TI y administradores del sistema a enfrentar algunos de los mayores desafíos que enfrentan las redes hoy en día. Estos NGFW virtuales abordan el creciente número de violaciones de seguridad y protegen contra amenazas emergentes con una de las principales soluciones de Secure SD-WAN, todo en un dispositivo virtual de fácil implementación, accesible y flexible.

Aspectos destacados

- Fácil de implementar y flexible como uCPE basado en las ramificaciones de SD-WAN.
- Provisionamiento fácil usando cloud-init.
- VPN SSL para admitir trabajo remoto seguro con clientes Windows, macOS e iOS incluidos.
- Fácil de implementar nuevos firewalls utilizando plantillas de configuración personalizadas con herramientas de gestión centralizada.
- Incluido con herramientas de análisis en la nube para proporcionar solución de problemas en tiempo real y paneles de resumen.
- Puntuación de Ciberseguridad Única para análisis de seguridad simplificados y accionables.
- Sistema integrado de Detección/Protección de Intrusos con actualizaciones en tiempo real.
- Protección de botnets y ataques de denegación de servicio (DoS) a través de continuas actualizaciones de feeds de reputación de IP.
- Admite hipervisores como KVM, VMware, Hyper-V.

	NetWall 100V	NetWall 500V	NetWall 1000V	NetWall 2000V	NetWall 4000V	NetWall 6000V	NetWall 12000V
Rendimiento* de Firewall	100 Mbps	500 Mbps	1 Gbps	2 Gbps	4 Gbps	6 Gbps	12 Gbps
Rendimiento* de VPN	100 Mbps	500 Mbps	1 Gbps	2 Gbps	4 Gbps	6 Gbps	12 Gbps
Conexiones concurrentes	16.000	64.000	128.000	256.000	512.000	1M	1M
Túneles VPN concurrentes (Ipsec)	50	250	500	500	1.000	1.500	1.500
Interfaces de Ethernet	Hasta 10						
Interfaces virtuales (IEEE 802.1q/802.1ad)	1024						
Routers Virtuales	25	25	50	50	100	100	125
Soporte de alta disponibilidad	Sí						
Memoria RAM mínima recomendada	512 MB	512 MB	512 MB	1 GB	2 GB	4 GB	4 GB
Almacenamiento disponible recomendado	1 GB						
Número de vCPUs**	1 GB						
Clavister OS	Clavister cOS Core						
Aceleración Crypto Intel AES-NI	Sí						
Soporte de Intel DPDK y SR-IOV	Sí						
Hypervisors soportados	VMWare vSphere, KVM (ARM & Intel), Microsoft Hyper-V						

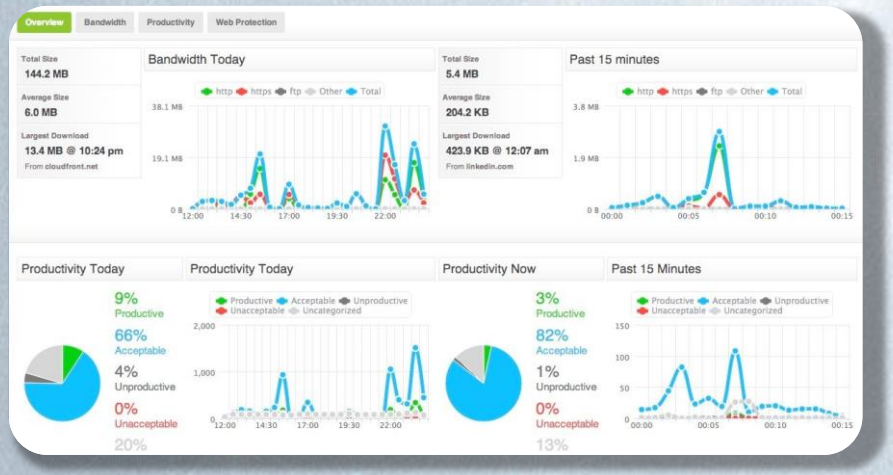
	Basics	Essentials	Enhanced	Premium
Soporte Técnico 24/7	●	●	●	●
Gestión Centralizada	●	●	●	●
Actualizaciones de Software	●	●	●	●
Clavister OneConnect	●	●	●	●
Geobloqueo		●	●	●
Alta Disponibilidad		●	●	●
Visibilidad y control de aplicaciones		●	●	●
Inteligencia del dispositivo		●	●	●
Escáner Antivirus			●	●
Prevención de intrusiones			●	●
Reputación IP			●	●
Filtrado de contenidos Web			●	●
Protección DoS			●	●
Bloqueo de Botnets			●	●
Inspección SSL				●

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 controlar y monitorear el uso de internet de su organización. La solución ofrece informes detallados y en tiempo real sobre el tráfico de internet, lo que permite a los administradores identificar problemas de seguridad, optimizar el uso de ancho de banda y mejorar la productividad de los empleados.

Fastvue es compatible con varios dispositivos de seguridad web y firewall, incluidos los de la marca Sophos, Barracuda, Fortinet y Cisco Meraki. La solución es fácil de implementar y personalizar, con opciones para crear informes y alertas personalizadas según las necesidades de la organización. Fastvue ofrece un excelente servicio al cliente y un soporte técnico de alta calidad para garantizar la satisfacción de sus clientes.



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 también puede ser útil para la investigación de incidentes de seguridad y la resolución de problemas. Los administradores pueden utilizar la herramienta para buscar registros de tráfico web específicos 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

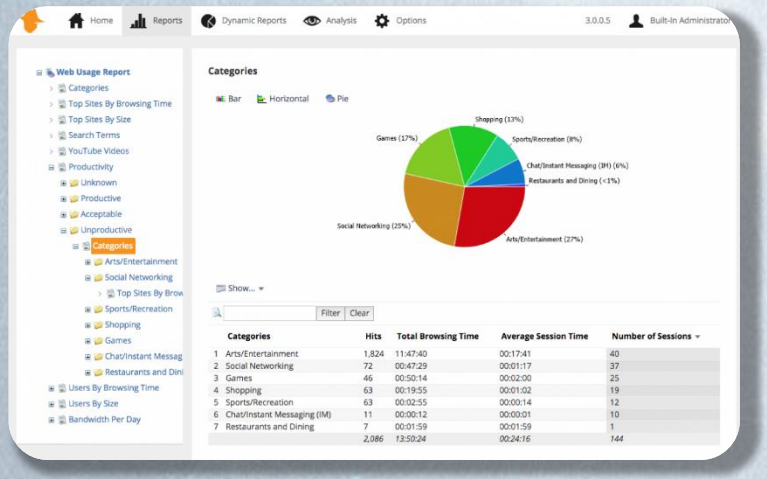
Gestione el uso del ancho de banda y optimizar el rendimiento de la red. Los administradores pueden ver informes detallados sobre el uso del ancho de banda y tomar medidas para equilibrar el tráfico de la red y evitar cuellos de botella.

Monitorización | WebSpy

Controla tu red, protege tu negocio con WebSpy

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

WebSpy es altamente personalizable y escalable, lo que permite a las empresas adaptar la herramienta a sus necesidades específicas. Además, WebSpy es compatible con una amplia gama de dispositivos de red y plataformas, lo que lo hace fácilmente integrable en cualquier infraestructura de red existente. En resumen, WebSpy es una herramienta de análisis de tráfico de Internet integral y eficaz que ayuda a las empresas a mantener su seguridad en línea y a administrar su uso de Internet de manera efectiva.



➢ 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.

paloalto NETWORKS · FORTINET · cisco · McAfee by Intel · Barracuda · WatchGuard · SOPHOS · Exchange · Symantec

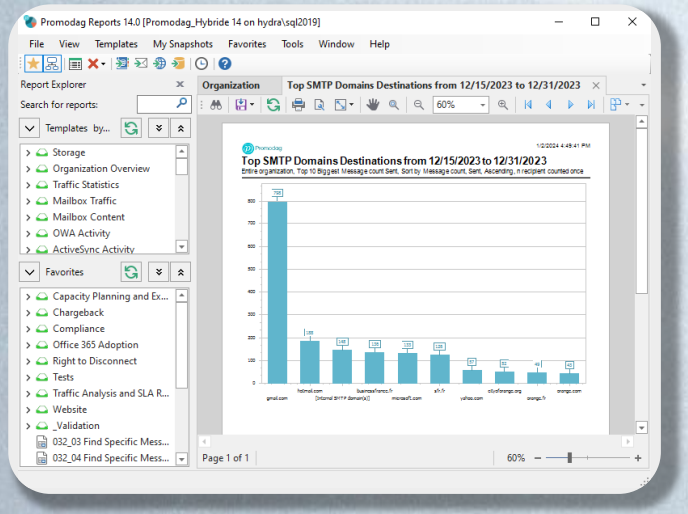
Monitorización | Promodag

Informes de Exchange para Office 365 y Exchange On-premises

Promodag Reports for Exchange es una herramienta versátil que cubre todas sus necesidades de informes de Exchange, compatible tanto con el sistema de mensajería Exchange Online (Office 365) o híbrido como On-premise. Simplifique y automatice los procesos de auditoría de correo electrónico, asegúrese de que cumplan con las reglas comerciales y optimice el rendimiento de su sistema de correo electrónico.

La herramienta proporciona una descripción general del sistema y le ayuda a cumplir con sus obligaciones legales, como el RGPD, pero también a optimizar el uso de sus recursos. Por último, puede generar indicadores que pueden utilizarse como parte de la gestión diaria, especialmente la del contenido del buzón.

Promodag Reports ha sido la herramienta de informes preferida por la comunidad de administradores de Exchange Server durante más de 20 años. Úselo para auditar las mejores prácticas y especialmente la aplicación GDRP, o para prepararse para una migración a otra versión de Exchange Server u Office 365. Aproveche sus características únicas para analizar su tráfico y el contenido de la base de datos en diferentes niveles.



➢ 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

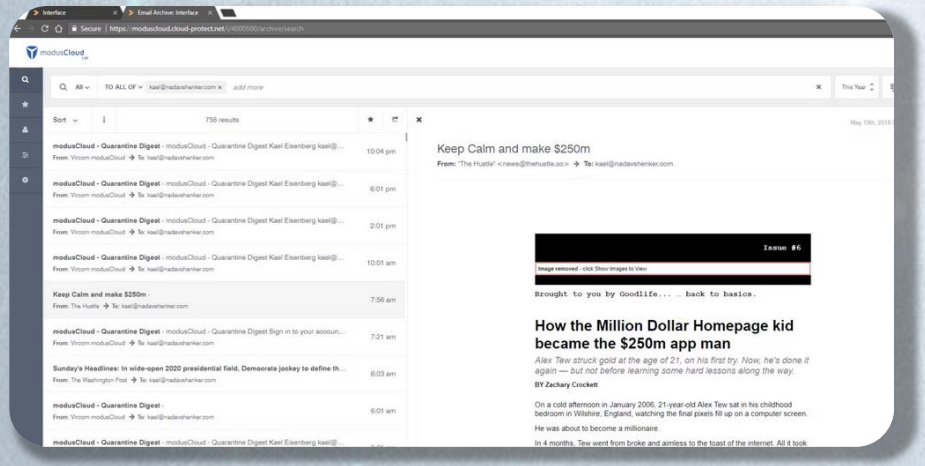
Utilice informes de facturación para facturar a departamentos o sucursales internos en función del volumen de correo electrónico que envían o reciben, el tamaño de sus buzones de correo o ambos.

Filtrado de contenidos | ModusCloud

Seguridad en la nube para proteger su negocio

ModusCloud es una plataforma de seguridad en la nube que ofrece una amplia gama de soluciones para proteger la red de la empresa contra los riesgos de seguridad en línea. La plataforma incluye protección contra spam, virus y filtrado de contenido web, gestión de correo electrónico, cumplimiento normativo, prevención de pérdida de datos, autenticación multifactor, filtrado de correo electrónico entrante y saliente, seguimiento y análisis de amenazas, y protección de endpoints. Además, ModusCloud ofrece informes detallados y análisis de amenazas, así como alertas en tiempo real para ayudar a los administradores a responder rápidamente a las amenazas.

La plataforma es fácil de implementar y usar, y se integra con otras soluciones de seguridad de la empresa. En conjunto, ModusCloud es una solución integral de seguridad en la nube diseñada para cumplir con los requisitos de seguridad y privacidad de datos y ofrecer flexibilidad y escalabilidad para adaptarse a las necesidades de la empresa.



➢ Protección contra spam

ModusCloud utiliza tecnologías avanzadas de detección de spam para bloquear correos electrónicos no deseados, phishing y correos electrónicos maliciosos antes de que lleguen a la bandeja de entrada del usuario. Esto ayuda a proteger la red de la empresa y a prevenir ataques cibernéticos.

➢ Protección contra virus

El motor integrado de ModusCloud está diseñado para proteger la red de la empresa contra virus y malware. El motor antivirus es capaz de detectar y bloquear amenazas avanzadas y desconocidas, lo que ayuda a prevenir ataques cibernéticos y a proteger la información confidencial.

➢ Gestión de correo electrónico

ModusCloud proporciona una interfaz de administración centralizada que permite a los administradores de TI gestionar y controlar el correo electrónico de la empresa. Los administradores pueden configurar reglas de filtrado, supervisar el tráfico de correo electrónico y crear informes detallados.

➢ Seguimiento y análisis de amenazas

Realice informes detallados y análisis de amenazas que ayudan a los administradores de TI a identificar patrones de actividad y detectar amenazas avanzadas. La plataforma también proporciona alertas en tiempo real para ayudar a los administradores a responder rápidamente a las amenazas.

➢ Prevención de pérdida de datos (DLP)

ModusCloud ofrece una solución de DLP para detectar y prevenir la filtración de información confidencial. Los administradores de TI pueden definir políticas para identificar y bloquear el envío de información confidencial, como números de tarjetas de crédito o información de identificación personal.

➢ Autenticación multifactor (MFA)

ModusCloud ofrece una solución de MFA para aumentar la seguridad del inicio de sesión de usuario. Los usuarios deben proporcionar una contraseña y una segunda forma de autenticación, como un código enviado por mensaje de texto o una aplicación de autenticación móvil, para acceder a sus cuentas.

➢ Filtrado de correo electrónico entrante y saliente

Configure políticas de filtrado para el correo electrónico entrante y saliente con ModusCloud. Los administradores pueden bloquear el correo electrónico saliente que contiene información confidencial y el correo electrónico entrante que contiene malware o phishing.

➢ Protección de endpoints

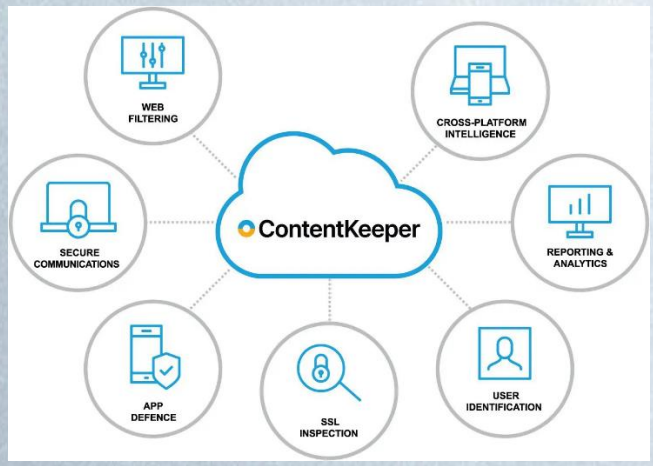
Con ModusCloud dispone de una solución de protección de endpoints que incluye la detección y prevención de malware, la prevención de exploits y la monitorización de comportamiento. La solución de protección de endpoints también incluye funciones de administración remota y control de aplicaciones.

Filtrado de contenidos | ContentKeeper

Seguridad, control y confianza

Content Keeper es una solución de seguridad y filtrado de contenido web para empresas, organizaciones y escuelas. Su objetivo es proteger a los usuarios y la red de los peligros en línea, como sitios web maliciosos, virus, malware, phishing y ataques de hackers. Content Keeper ofrece una solución integral que permite a los administradores personalizar las políticas de filtrado y seguridad para adaptarse a las necesidades de su organización.

Con Content Keeper, los administradores pueden monitorear y registrar el uso de Internet para garantizar el cumplimiento de las políticas de uso aceptable y evitar el acceso a sitios web no autorizados o inapropiados. Además Content Keeper puede ayudar a reducir el riesgo de responsabilidad de la organización y cumplir con las regulaciones de privacidad de datos. En resumen, Content Keeper es una solución esencial para garantizar la seguridad en línea y proteger a la organización contra las 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.

- **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.

- **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.

- **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.

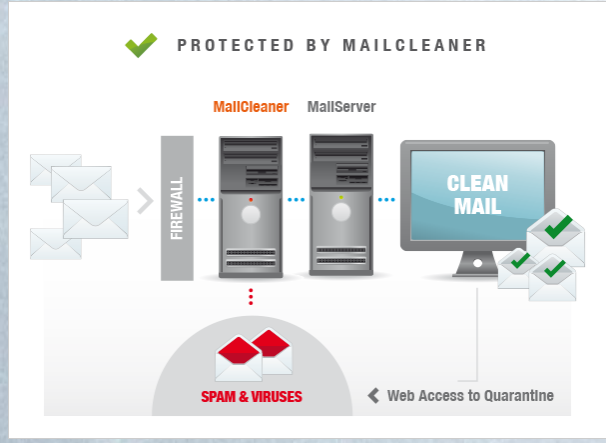
- **Cumplimiento de las regulaciones de privacidad de datos**
Content Keeper puede utilizarse para garantizar que los empleados no accedan a sitios web o descarguen archivos que violen las regulaciones de privacidad de datos. Esto es especialmente importante en organizaciones que manejan información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

Filtrado de contenidos | MailCleaner

¡Mantén tu bandeja de entrada limpia y organizada con Mail Cleaner!

Mail Cleaner es una herramienta que te ayuda a limpiar y organizar tu bandeja de entrada de correo electrónico. Con Mail Cleaner, puedes eliminar correos no deseados o spam, clasificar correos electrónicos por prioridad, eliminar correos electrónicos duplicados, administrar tus suscripciones y organizar correos electrónicos por temas en carpetas específicas.

También puedes personalizar tu bandeja de entrada y enviar respuestas automáticas cuando estás fuera de la oficina. Con su interfaz fácil de usar, Mail Cleaner te permite ahorrar tiempo al reducir la cantidad de correos electrónicos que debes revisar y ayudarte a encontrar rápidamente los correos electrónicos importantes. Además, la herramienta es completamente segura y protege tu privacidad y la de tus datos personales. Si buscas una forma eficiente y rápida de administrar tus correos electrónicos, Mail Cleaner es una excelente opción.



Eliminación de correos electrónicos no deseados

Mail Cleaner 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, lo que te ayudará a 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. Mail Cleaner puede ayudarte a eliminar estos correos electrónicos para que puedas mantener tu bandeja de entrada limpia y ordenada.

Identificación de correos electrónicos importantes

Mail Cleaner 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, Mail Cleaner puede ayudarte a administrar estas suscripciones. Puedes utilizar la función de eliminación masiva de Mail Cleaner 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. Mail Cleaner 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. Mail Cleaner 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

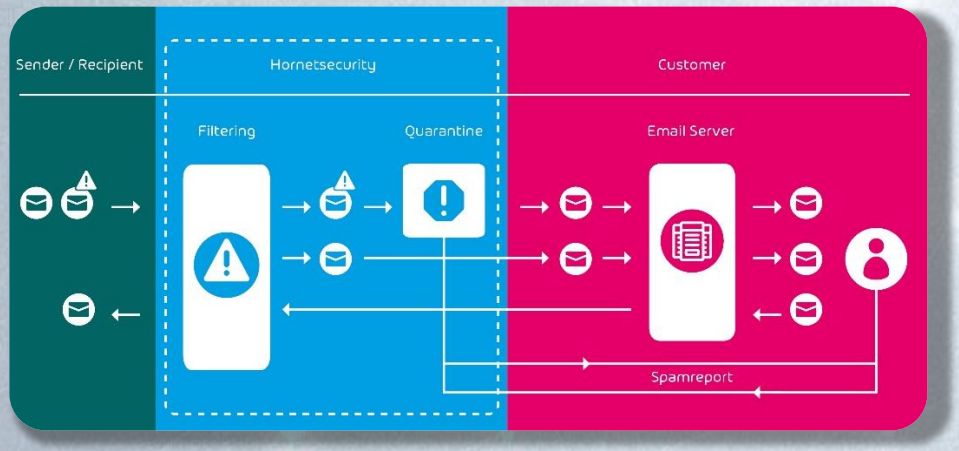
Si tienes una gran cantidad de correos electrónicos en tu bandeja de entrada, puede ser difícil encontrar los que sean importantes. Mail Cleaner puede ayudarte a reducir el tamaño de tu bandeja de entrada al eliminar correos electrónicos no importantes o antiguos, lo que te permitirá centrarte en aquellos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

Filtrado de contenidos | Hornet Security

Potenciando tu mundo seguro

Hornet Security Spam and Malware es una solución de seguridad informática que se enfoca en proteger a las empresas de las amenazas del spam y el malware. Utilizando tecnologías avanzadas, Hornet Security Spam and Malware filtra el correo no deseado y detecta y bloquea malware en correos electrónicos y archivos adjuntos. La solución también ayuda a prevenir el phishing al detectar correos electrónicos sospechosos y evitar que los usuarios hagan clic en enlaces maliciosos o proporcionen información confidencial.

Además de su capacidad para detectar y bloquear amenazas, Hornet Security Spam and Malware ofrece una consola de administración centralizada para una supervisión y gestión más efectivas. También se puede configurar para filtrar contenido inapropiado o ofensivo en los correos electrónicos y para cumplir con políticas y regulaciones de seguridad. Los informes y análisis detallados proporcionados por la solución también ayudan a los administradores de TI a identificar patrones de amenazas y mejorar la seguridad de la empresa.



Protección contra el correo no deseado
Hornet Security Spam and Malware utiliza tecnologías avanzadas para filtrar el correo no deseado y evitar que llegue a la bandeja de entrada de los usuarios. Esto ayuda a reducir la cantidad de tiempo que los empleados tienen que pasar revisando el correo no deseado y minimiza la posibilidad de que abran correos electrónicos maliciosos.

Detección de malware
Hornet Security Spam and Malware también utiliza tecnologías avanzadas para detectar malware en los correos electrónicos y en los archivos adjuntos. Esto ayuda a prevenir la propagación de virus y otros tipos de malware a través de la red de la empresa.

Prevención de phishing
El phishing es una técnica común utilizada por los ciberdelincuentes para obtener información confidencial de los usuarios. Hornet Security Spam and Malware utiliza tecnologías avanzadas para detectar correos electrónicos sospechosos y evitar que los usuarios hagan clic en enlaces maliciosos o proporcionen información confidencial.

Supervisión y gestión centralizada
Hornet Security Spam and Malware proporciona una consola de administración centralizada que permite a los administradores de TI supervisar y gestionar la solución de seguridad en toda la empresa. Esto hace que sea más fácil para los administradores identificar y responder rápidamente a posibles amenazas.

Protección contra ransomware
Hornet Security Spam and Malware puede detectar y bloquear correos electrónicos maliciosos que contienen ransomware, una forma de malware que puede cifrar los archivos del sistema de un usuario y exigir un rescate para su liberación. La detección temprana de ransomware ayuda a minimizar el impacto en la empresa y evita la pérdida de datos.

Filtro de contenido
Hornet Security Spam and Malware puede ser utilizado para filtrar contenido ofensivo o inapropiado en los correos electrónicos que se envían y reciben en la empresa. Esto ayuda a garantizar que los empleados no sean expuestos a contenido inapropiado y ayuda a mantener la cultura laboral y la reputación de la empresa.

Cumplimiento de políticas
Hornet Security Spam and Malware puede ser configurado para aplicar políticas de seguridad en los correos electrónicos que se envían y reciben en la empresa. Por ejemplo, se pueden configurar políticas de retención de correos electrónicos para cumplir con las regulaciones y las políticas de la empresa.

Análisis y reportes
Hornet Security Spam and Malware proporciona informes y análisis detallados sobre las amenazas detectadas, la eficacia del filtro y otras métricas importantes. Estos informes pueden ayudar a los administradores de TI a identificar patrones de amenazas y tomar medidas para mejorar la seguridad de la empresa.

Gestión de identidades | HelloID

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

HelloID Provisioning es una solución de automatización de la gestión de identidades y accesos que permite a los administradores de TI gestionar de forma centralizada y automatizada los procesos de incorporación, cambio y baja de usuarios y el acceso a recursos empresariales. La solución facilita la integración de diferentes sistemas, tanto locales como en la nube, para garantizar la sincronización y la consistencia de los datos de los usuarios y los recursos.

Con HelloID Provisioning, los administradores pueden establecer flujos de trabajo personalizados para automatizar los procesos de gestión de identidades y accesos, lo que reduce significativamente el tiempo y los costos asociados con la administración manual. La solución también incluye características avanzadas de auditoría y generación de informes que permiten a los administradores de TI supervisar el uso de la solución y garantizar el cumplimiento de las 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.

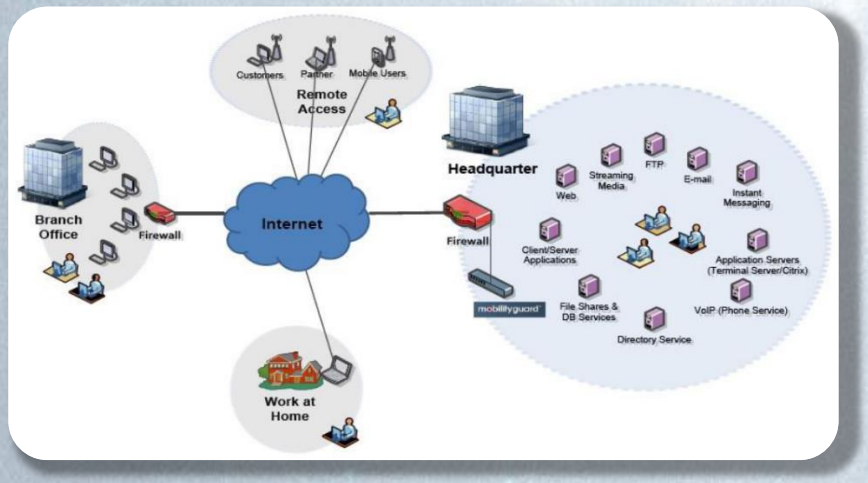
Gestión de identidades | MobilityGuard

mobilityguard®
Unified Access Management

Acceda con confianza, proteja con MobilityGuard

MobilityGuard es una solución de seguridad y acceso en la nube que proporciona una experiencia de usuario segura y sin interrupciones para dispositivos móviles y aplicaciones en la nube. Ofrece autenticación multifactor, políticas de seguridad de dispositivos, control de acceso basado en roles, análisis de riesgos y prevención de amenazas, y gestión centralizada para garantizar que solo los dispositivos y usuarios autorizados tengan acceso a los datos y aplicaciones.

MobilityGuard se integra con una variedad de soluciones de autenticación y puede adaptarse a las necesidades específicas de cada organización. Con MobilityGuard, los administradores pueden establecer políticas de seguridad personalizadas y monitorear el acceso de los usuarios desde una única consola, lo que simplifica la administración de la seguridad de la red. En resumen, MobilityGuard proporciona una solución integral para proteger contra amenazas a la seguridad de la red y brinda una experiencia de usuario segura y sin interrupciones.



➢ 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.

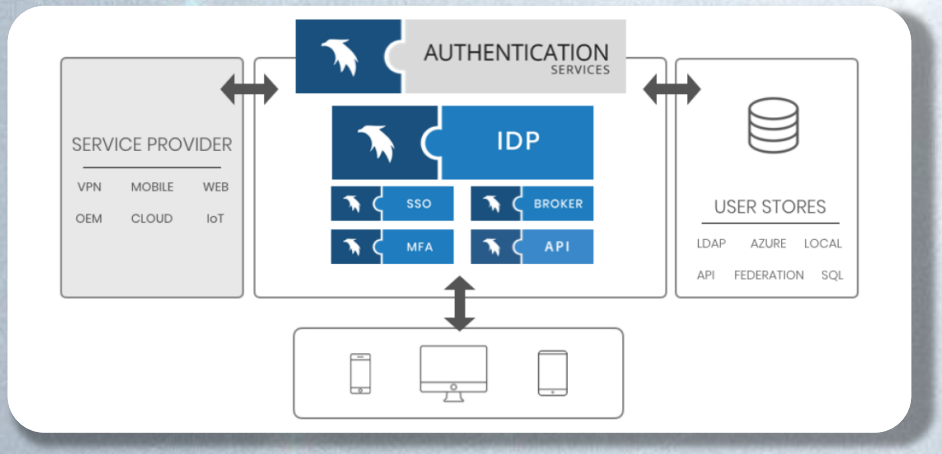
➢ Auditoría y seguimiento de accesos

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

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

PhenixID es una solución de gestión de identidad y acceso (IAM) que proporciona una plataforma completa y escalable para administrar los usuarios, recursos y privilegios en una organización. Ofrece una amplia gama de funcionalidades, como autenticación y autorización de usuarios, gestión de contraseñas, gestión de identidades y grupos, federación de identidades, gestión de accesos y seguridad de la información. Además, PhoenixID cumple con los requisitos normativos de privacidad de datos, como la gestión de consentimiento y la protección de datos personales. La plataforma es altamente personalizable y escalable, lo que permite a las organizaciones adaptar la solución a sus necesidades específicas y manejar grandes volúmenes de usuarios y recursos. En resumen, PhoenixID es una solución completa y robusta de IAM que puede ayudar a las organizaciones a mejorar su seguridad, cumplimiento normativo y gestión de identidades y accesos.



- **Autenticación de usuario**
PhenixID se utiliza para autenticar a los usuarios y permitirles acceder a recursos específicos basados en sus permisos.

- **Gestión de identidades**
PhenixID se utiliza para administrar las identidades de los usuarios, incluida la creación, modificación y eliminación de cuentas de usuario.

- **Autorización de usuario**
PhenixID se utiliza para autorizar a los usuarios a acceder a recursos específicos basados en su función y permisos.

- **Gestión de contraseñas**
PhenixID se utiliza para administrar las contraseñas de los usuarios, incluyendo la configuración de políticas de contraseñas y el restablecimiento de contraseñas olvidadas.

- **Gestión de acceso**
PhenixID se utiliza para administrar el acceso de los usuarios a recursos específicos, incluida la definición de reglas de acceso y la auditoría de accesos.

- **Gestión de privilegios**
PhoenixID se utiliza para la gestión de privilegios de usuario, lo que significa que los usuarios tienen acceso solo a los recursos necesarios para realizar su trabajo.

- **Gestión de grupos**
PhoenixID se utiliza para administrar grupos de usuarios, incluyendo la creación, modificación y eliminación de grupos de usuarios y la asignación de usuarios a grupos específicos.

- **Federación de identidades**
PhenixID se utiliza para permitir que los usuarios accedan a recursos en otros sistemas utilizando sus credenciales de PhoenixID.

- **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 se utiliza para proporcionar SSO, lo que significa que los usuarios pueden acceder a múltiples aplicaciones y servicios con una sola autenticación.

- **Cumplimiento normativo**
PhenixID se utiliza para cumplir con los requisitos normativos, como el Reglamento General de Protección de Datos (RGPD) y la Ley de Protección de Datos Personales.

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

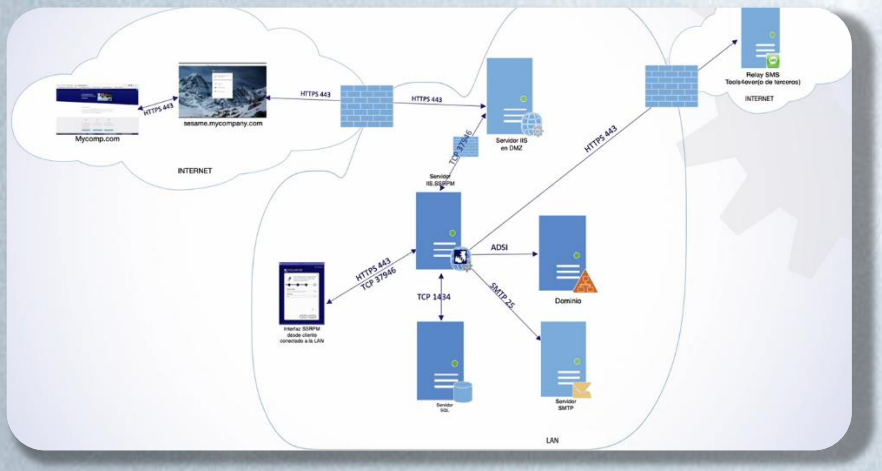
Gestión de identidades | SSRPM

SSRPM
Passwords Made Easy

Empodera a tus usuarios, protege tu organización

Self-Service Password Reset Manager (SSRPM) es una solución de gestión de contraseñas que permite a los usuarios restablecer sus propias contraseñas de forma segura y sencilla, sin la necesidad de ayuda del personal de TI. La solución está diseñada para mejorar la seguridad de la empresa al reducir la probabilidad de que se produzcan infracciones de seguridad debido a contraseñas débiles o comprometidas. SSRPM utiliza tecnologías de autenticación y validación para asegurar que los usuarios sean quienes dicen ser antes de permitirles restablecer sus contraseñas.

Los usuarios pueden restablecer sus contraseñas a través de una variedad de métodos, incluyendo preguntas de seguridad personalizadas, correo electrónico, SMS y autenticación multifactor. La solución también incluye características avanzadas de auditoría y generación de informes que permiten a los administradores de TI supervisar el uso de la solución y garantizar el cumplimiento de las políticas de seguridad.



➢ Reducción de la carga del servicio de asistencia técnica

Con SSRPM, los usuarios pueden restablecer sus contraseñas ellos mismos sin tener que ponerse en contacto con el servicio de asistencia técnica, lo que reduce la carga de trabajo del personal de TI.

➢ Incremento de la seguridad

SSRPM puede ayudar a aumentar la seguridad de una organización al exigir que los usuarios sigan procedimientos de seguridad y autenticación rigurosos para restablecer sus contraseñas.

➢ Cumplimiento de las normativas

Muchas normativas exigen que las organizaciones tengan un proceso de restablecimiento de contraseñas seguro y eficaz en su lugar. SSRPM puede ayudar a las organizaciones a cumplir con estos requisitos.

➢ Ahorro de tiempo y costos

El software permite que los usuarios restablezcan sus contraseñas de forma autónoma, se puede ahorrar tiempo y costos al evitar la necesidad de que el personal de TI intervenga en el proceso de restablecimiento de contraseñas.

➢ Mejora de la experiencia del usuario

Se mejora la experiencia del usuario al evitar la necesidad de esperar en la cola del servicio de asistencia técnica y, en consecuencia, mejora la satisfacción del usuario.

➢ Restablecimiento de contraseñas olvidadas

SSRPM es ideal para los usuarios que olvidan sus contraseñas y necesitan restablecerlas rápidamente.

➢ Aumento de la productividad

SSRPM permite a los usuarios restablecer sus contraseñas sin tener que interrumpir su trabajo y esperar a que el servicio de asistencia técnica les ayude, lo que puede aumentar la productividad en la empresa.

➢ Reducción del riesgo de seguridad

SSRPM puede ayudar a reducir el riesgo de seguridad al evitar que los usuarios escriban sus contraseñas en papel o las almacenen en lugares inseguros, lo que podría comprometer la seguridad de la empresa.

➢ Restablecimiento de contraseñas expiradas

SSRPM también puede ayudar a los usuarios a restablecer sus contraseñas expiradas en el momento en que lo necesiten.

➢ Protección contra ataques de phishing

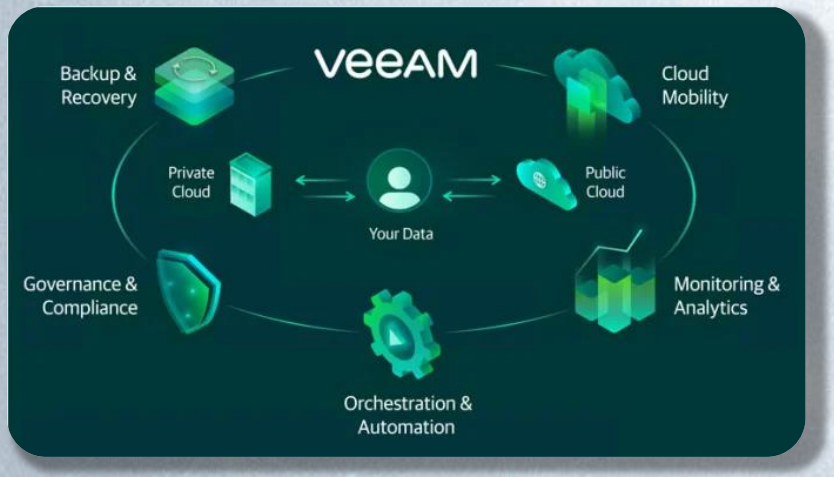
SSRPM puede ayudar a proteger a los usuarios contra los ataques de phishing, ya que los usuarios pueden restablecer sus contraseñas de forma autónoma sin tener que proporcionar información personal a terceros.

Backups y restauración | Veeam

Siempre activo. Siempre confiable.

Veeam Backup es una solución líder en el mercado para la protección de datos en entornos virtuales, físicos y en la nube. Ofrece una plataforma unificada y escalable para copias de seguridad, replicación y recuperación de datos, con una gestión centralizada des de una única consola.

La solución proporciona copias de seguridad en tiempo real de los datos críticos y la recuperación de datos en minutos, minimizando el tiempo de inactividad y la pérdida de datos. Con características como la recuperación granular de archivos, la replicación en tiempo real y la integración con proveedores de almacenamiento en la nube, Veeam Backup es una solución completa y flexible para la protección de datos. Además, su facilidad de uso y eficiencia hacen de Veeam Backup una excelente opción para empresas de cualquier tamaño que buscan una solución confiable y eficaz para la protección de sus datos críticos.



- **Protección de entornos virtuales**
Veeam Backup es una solución líder en la protección de datos de entornos virtuales, como VMware, Hyper-V y Nutanix AHV. Los usuarios pueden realizar copias de seguridad en tiempo real de máquinas virtuales y recuperarlas en minutos en caso de una falla del sistema.

- **Copia de seguridad de datos físicos**
Veeam Backup también es compatible con entornos físicos, lo que permite a los usuarios realizar copias de seguridad de servidores, estaciones de trabajo y dispositivos de almacenamiento conectados.

- **Protección de datos en la nube**
Veeam Backup se integra con proveedores de almacenamiento en la nube, como AWS, Azure y Google Cloud, para proteger los datos almacenados en la nube.

- **Copia de seguridad de endpoints**
Veeam Backup ofrece una solución de protección de datos para endpoints, lo que permite a los usuarios realizar copias de seguridad y recuperar datos críticos en dispositivos móviles y laptops.

- **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.

- **Copia de seguridad de bases de datos**
Veeam Backup es compatible con una amplia variedad de bases de datos, incluidos Microsoft SQL Server, Oracle y MySQL, lo que permite a los usuarios realizar copias de seguridad y recuperar datos críticos en caso de una falla del sistema.

- **Copia de seguridad de aplicaciones**
Veeam Backup es compatible con una amplia variedad de aplicaciones, como Microsoft Exchange, SharePoint y Active Directory, lo que permite a los usuarios realizar copias de seguridad y recuperar datos críticos en caso de una falla del sistema.

- **Copia de seguridad de almacenamiento de objetos**
Veeam Backup es compatible con el almacenamiento de objetos, como Amazon S3, Microsoft Azure Blob Storage y IBM Cloud Object Storage, lo que permite a los usuarios realizar copias de seguridad y recuperar datos críticos almacenados en el almacenamiento de objetos.

- **Recuperación ante desastres**
Veeam Backup permite la replicación en tiempo real de datos críticos a un sitio de recuperación en caso de una falla del sistema o desastre natural.

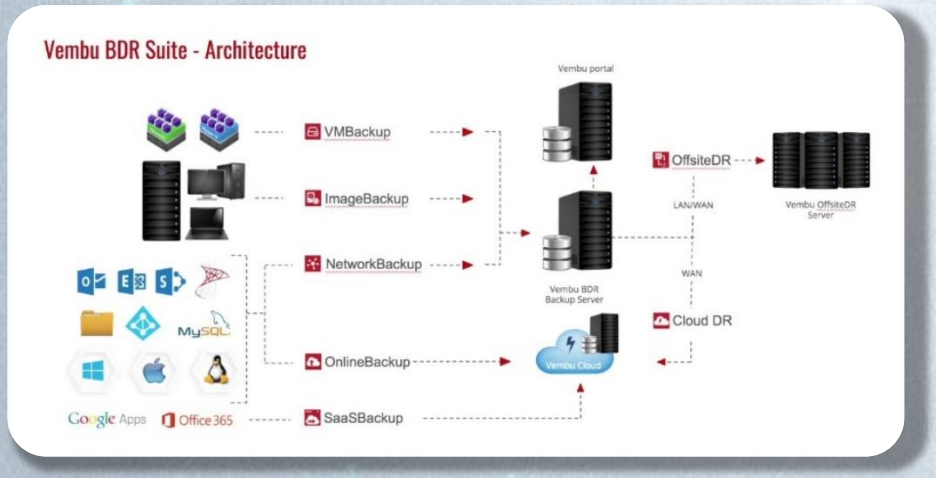
- **Migración de datos**
Veeam Backup también se utiliza para migrar datos de un entorno a otro, como la migración de máquinas virtuales de un host a otro o la migración de datos de un proveedor de almacenamiento en la nube a otro.

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 ofrece una protección efectiva de los datos críticos de una empresa. Con esta herramienta es posible realizar copias de seguridad programadas y restaurar los datos de manera rápida y eficiente, lo que garantiza su disponibilidad en caso de fallos del sistema, errores humanos o desastres naturales. Además, BDR Suite permite la replicación de los datos en ubicaciones remotas, asegurando su disponibilidad en caso de problemas en el sitio principal.

Esta solución también ofrece la integración con otros sistemas de gestión de TI, lo que permite una mayor eficiencia en la administración de sistemas y una mejor visibilidad de los datos críticos. Con la supervisión y alertas en tiempo real, los administradores de TI pueden monitorear el estado de los sistemas y recibir notificaciones en caso de problemas. Con BDR Suite, los datos de la empresa están siempre protegidos y disponibles.



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

Protección de datos empresariales simplificada

Workspace Unified Endpoint Management (UEM) es una plataforma de gestión de endpoints unificada y basada en la nube de VMware que permite a las empresas gestionar de forma centralizada y segura todos sus dispositivos, incluyendo dispositivos móviles, ordenadores portátiles, de escritorio y IoT, desde una sola consola.

Con Workspace UEM, las empresas pueden implementar políticas de seguridad y cumplimiento, distribuir aplicaciones y actualizar el firmware de forma remota, permitir a los empleados trabajar desde cualquier dispositivo y en cualquier lugar de forma segura, y proteger los endpoints contra amenazas de seguridad.

Además, Workspace UEM proporciona una experiencia de usuario unificada y personalizada para los empleados, lo que mejora la productividad y la satisfacción del usuario final. Con esta solución, las empresas pueden reducir costos, aumentar la eficiencia y mejorar la seguridad de sus endpoints.

➢ Gestión de dispositivos
Workspace UEM permite a las empresas gestionar 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.

➢ Gestión de contenido
Workspace UEM permite a las empresas gestionar y controlar el acceso y la distribución de contenido empresarial, lo que garantiza que los empleados tengan acceso a la información relevante de manera segura y eficiente.

➢ 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 integral de gestión de movilidad empresarial diseñada para ayudar a las organizaciones a administrar y asegurar sus dispositivos móviles y aplicaciones. Esta plataforma ofrece una amplia gama de funciones de gestión de dispositivos móviles (MDM) y gestión de aplicaciones móviles (MAM) que permiten a las empresas controlar la seguridad, el acceso y el uso de sus dispositivos móviles y datos.

Con SOTI, las empresas pueden monitorear y controlar la seguridad de sus dispositivos móviles y datos, así como administrar el ciclo de vida de las aplicaciones móviles. La plataforma también permite a las empresas personalizar las políticas de seguridad y acceso para satisfacer las necesidades específicas de su organización.

Además, SOTI MobiControl también ayuda a las empresas a optimizar el rendimiento y la eficiencia de sus dispositivos móviles mediante la configuración de políticas de uso de dispositivos, la realización de actualizaciones remotas y la solución rápida 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

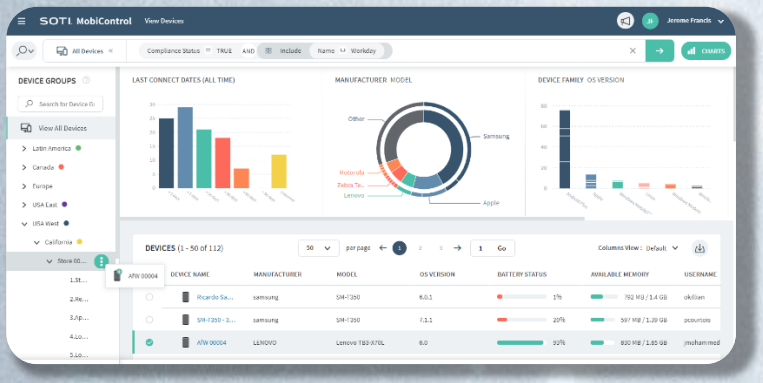
La plataforma ofrece una amplia gama de herramientas avanzadas de gestión de aplicaciones, que permiten a los administradores de TI instalar, actualizar y desinstalar aplicaciones de manera remota, y establecer políticas y restricciones en las aplicaciones instaladas en los dispositivos móviles.

Gestión de contenido

SOTI MobiControl también ofrece herramientas avanzadas de gestión de contenido, que permiten a los administradores de TI controlar y administrar el contenido que se almacena en los dispositivos móviles de los usuarios, lo que les permite garantizar la seguridad de los datos empresariales y cumplir con las políticas de cumplimiento.

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

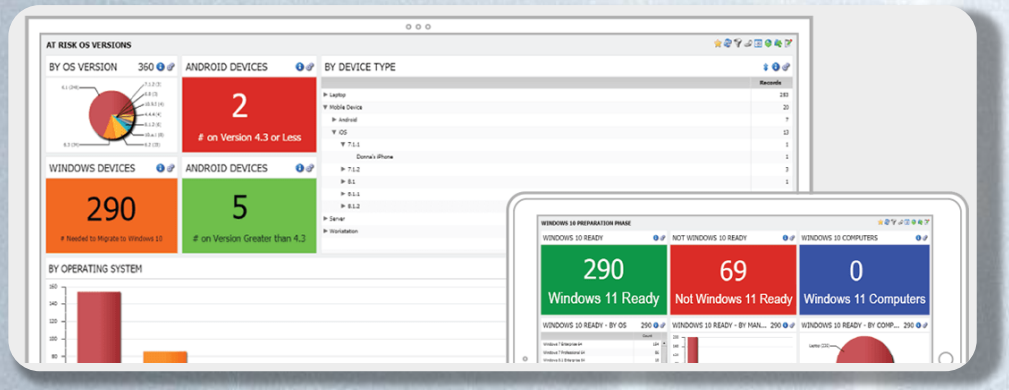
SOTI MobiControl cuenta con una interfaz de usuario intuitiva y fácil de usar, que permite a los administradores de TI gestionar y controlar dispositivos móviles y de IoT de manera rápida y eficiente. Además, ofrece una serie de herramientas de soporte y formación para ayudar a los usuarios a aprovechar 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 de gestión de dispositivos móviles (MDM) que permite a las empresas gestionar y asegurar dispositivos móviles desde una plataforma centralizada. La solución proporciona herramientas para la gestión de dispositivos, protección de datos, gestión de aplicaciones, control de gastos y soporte técnico remoto.

Los administradores de TI pueden establecer políticas de seguridad y acceso, configurar dispositivos móviles, automatizar procesos y acceder a informes detallados y análisis sobre el uso de dispositivos móviles. La solución ayuda a las empresas a proteger los datos empresariales, garantizar el cumplimiento de políticas de seguridad, reducir los costos asociados con el uso de dispositivos móviles y aumentar la eficiencia del soporte técnico. Ivanti Endpoint Manager Mobile es una solución integral que ofrece una gestión completa de dispositivos móviles y ayuda a las empresas a mantener el control sobre sus activos móviles.



Administración de dispositivos móviles

Ivanti Endpoint Manager Mobile permite a los administradores de TI supervisar y administrar dispositivos móviles, incluidos los dispositivos personales de los empleados, desde una sola consola de administración. Los administradores pueden controlar las políticas de seguridad, las actualizaciones de software y las configuraciones de los dispositivos, lo que les permite mantener los dispositivos móviles seguros y actualizados.

Protección de datos

Ivanti Endpoint Manager Mobile ayuda a las empresas a proteger los datos confidenciales en dispositivos móviles. Los administradores pueden establecer políticas de seguridad para proteger los datos empresariales, como el cifrado de datos, la autenticación de usuarios y el borrado remoto de datos. También pueden monitorear el uso de datos y aplicaciones para detectar cualquier actividad sospechosa.

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 asociados con el uso de dispositivos móviles. Los administradores pueden monitorear el uso de datos y llamadas para identificar patrones de uso y optimizar los planes de datos y voz según sea necesario. También pueden controlar el uso de roaming para evitar costos excesivos asociados con el uso de datos 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

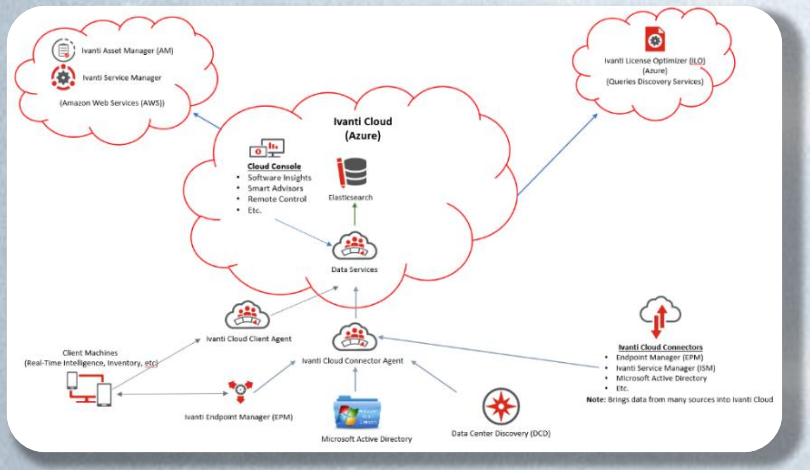
Ivanti Endpoint Manager Mobile proporciona informes y análisis detallados sobre el uso de dispositivos móviles en la organización, lo que incluye el uso de datos, el uso de aplicaciones y el cumplimiento de políticas de seguridad. Esto ayuda a los administradores de TI a tomar decisiones informadas sobre 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 de administración de dispositivos móviles que permite a las organizaciones gestionar y asegurar sus dispositivos móviles, cumpliendo con las políticas de la empresa y garantizando la seguridad de la información empresarial.

La plataforma permite la inscripción, configuración y gestión de dispositivos, así como la administración y despliegue de aplicaciones. También ayuda a asegurar que los dispositivos sean seguros al hacer cumplir políticas de seguridad, como la complejidad de contraseñas y el cifrado de dispositivos. Ivanti Neurons for MDM también ofrece la capacidad de borrar dispositivos de forma remota y generar informes de cumplimiento. En general, la plataforma ayuda a las organizaciones a administrar y asegurar sus dispositivos móviles de manera eficiente, mientras que los empleados tienen acceso a las herramientas necesarias para realizar su trabajo.



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 de gestión de dispositivos móviles (MDM) basada en la nube que permite a las empresas proteger y administrar sus dispositivos móviles, aplicaciones y contenidos desde una única consola centralizada. Con MaaS360, los administradores de TI pueden configurar políticas de seguridad, implementar actualizaciones y parches, monitorear el uso de datos y aplicaciones, y controlar el acceso a la red corporativa en dispositivos móviles. Además, la plataforma ofrece herramientas de gestión de aplicaciones móviles (MAM) para ayudar a las empresas a garantizar que solo se utilicen aplicaciones aprobadas y seguras.

MaaS360 también ofrece funciones de análisis y generación de informes para que los administradores puedan obtener información sobre el rendimiento y la seguridad de los dispositivos móviles. Con MaaS360, las empresas pueden asegurarse de que sus dispositivos móviles y datos estén protegidos mientras mantienen una productividad óptima en el entorno de trabajo móvil actual.

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

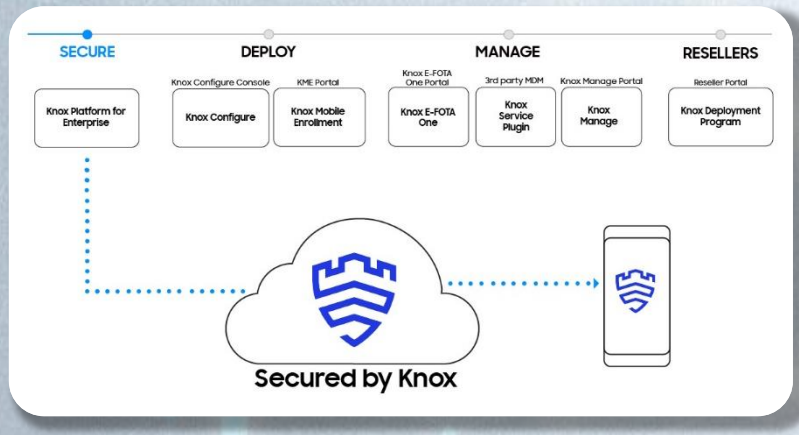
Con el aumento de la tendencia BYOD (Bring Your Own Device), MaaS360 también se puede utilizar para gestionar dispositivos personales de los empleados que se utilizan para fines de trabajo. Los administradores pueden asegurar que los datos corporativos estén protegidos en los dispositivos personales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

Movilidad | Samsung Knox

Movilidad simplificada, seguridad maximizada

Samsung Knox es una plataforma de seguridad móvil diseñada para proteger los datos personales y empresariales en dispositivos Samsung. Ofrece un entorno seguro para las aplicaciones empresariales y personales y se utiliza en una amplia variedad de casos de uso, como seguridad empresarial, protección de datos personales, control parental, protección de pagos móviles y teletrabajo, entre otros. También se utiliza en sectores críticos como la salud, finanzas, gobierno y defensa. Permite a los empleados utilizar sus dispositivos personales sin comprometer la seguridad de los datos empresariales y ofrece herramientas de control parental, establecimiento de límites de tiempo y restricción de acceso a sitios web y aplicaciones.

En general, Samsung Knox es una solución de seguridad móvil completa y versátil que garantiza la seguridad y privacidad de los datos personales y empresariales en una amplia variedad de entornos y situaciones.



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.

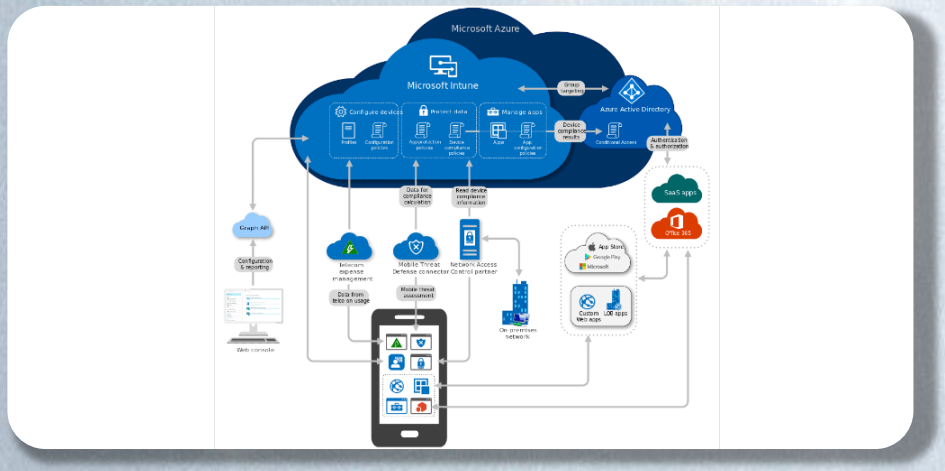
Gobierno y defensa
En el sector gubernamental y de defensa, la seguridad de los datos confidenciales es crítica. Samsung Knox puede utilizarse para proteger los datos gubernamentales y militares contra posibles ataques de ciberdelincuentes y otras amenazas.

Movilidad | Microsoft Intune

Administre todo: dispositivos, aplicaciones, datos...

Microsoft Intune es una plataforma de administración de dispositivos móviles y de escritorio basada en la nube que brinda a las empresas la capacidad de administrar y proteger sus dispositivos y datos. La plataforma incluye una amplia variedad de funciones, como la administración de dispositivos, la protección de datos, la configuración de políticas de seguridad y la administración de aplicaciones. Además, Intune puede administrar dispositivos en entornos de nube híbrida, lo que permite a las empresas extender la administración de dispositivos más allá de la infraestructura local.

La plataforma también ofrece la protección del correo electrónico empresarial y la administración de dispositivos Windows 10 y macOS. Intune es una solución completa y escalable que puede ayudar a las empresas a mejorar la eficiencia y la productividad mientras mantienen un alto nivel de seguridad en diferentes plataformas. Al permitir la administración y protección de dispositivos móviles y de escritorio, Intune se ha convertido en una solución valiosa para las empresas que buscan administrar y proteger sus datos y dispositivos.



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.