Aryan

VALUE ADDED SOLUTIONS

SEGURIDAD

CATÁLOGO
DE SOLUCIONES

soporte.preventa@aryan.es | 91 657 48 48 | www.aryan.es

ÍNDICE

Seguridad Perimetral

4

UTM - WatchGuard Total Security Suite

6

APT Blocker

8

VPN SSL (VPN Branch Office)

9

QVPN QNAP (Browser Station)

Seguridad Perimetral | UTM - Total Security Suite

Porque elegir los UTM de Watchguard.

Es una plataforma de seguridad de red que se centra en brindar el mejor nivel de seguridad de clase empresarial, independientemente del tamaño de la organización. Gracias a sus equipos Unifined Threat Management (UTM) diseñados desde cero enfocados en la facilidad de implementación, uso y administración continua.

Los equipos UTM de WatchGuard, disponen de una protección multicapa, capaz de correlacionar eventos entre ellas, para brindar a la empresa del nivel más sólido de seguridad. Además, disponen de una serie de servicios de seguridad diferenciadores respecto a la competencia, basados en soluciones “Endpoint Detection Response” y “Machine Learning” capaz de detectar y parar cualquier malware avanzado “Zero Day”.

¿Qué incluye los UTM de Watchguard?

APT Blocker - Sandbox Cloud
APT Blocker Sandbox de nueva generación para detectar y detener los ataques de ransomware, amenazas de día cero y otro malware avanzado diseñado para evadir las defensas de seguridad de red tradicionales.

Lastline impulsa a APT Blocker. Ofrece la mejor plataforma de protección contra malware de su clase que brinda soporte al servicio de seguridad APT Blocker de WatchGuard, detecta y detiene amenazas avanzadas persistentes, vulnerabilidades de día cero y malware avanzado.

Data Loss Prevention (DLP)
Prevención de pérdida de datos
Evite violaciones de datos y haga cumplir el cumplimiento escaneando texto y archivos para detectar información confidencial que intenta salir de su red.

DNSWatch – Resolución DNS Limpia
Reduzca las infecciones de malware detectando y bloqueando solicitudes DNS maliciosas, redirigiendo a los usuarios a una página segura

Access Portal – Portal publicación aplicaciones SSL
Access Portal proporciona una ubicación central para el acceso a aplicaciones alojadas en la nube y el acceso seguro sin cliente a recursos internos con RDP y SSH.
Access Portal admite implementaciones de inicio de sesión única (SSO) para acceso centralizado a aplicaciones alojadas en la nube y recursos internos mediante RDP y SSH. La compatibilidad con SAML brinda integración conveniente con proveedores de SSO y AuthPoint (u otros proveedores de MFA) y están disponibles todas las opciones de autenticación admitidas por Firebox, incluidas Active Directory, Radius, Firebox-DB.

IntelligentAV – Antivirus basado en Inteligencia artificial & Machine Learning
IntelligentAV es una solución antimalware sin firma que se basa en la inteligencia artificial para automatizar el descubrimiento de malware.
WatchGuardIntelligentAV está incorporado en la Plataforma AI Cylance, y presenta un poderoso motor de machine learning para mejorar la defensa contra el malware de día cero de evolución continua.

Cylance fue la primera compañía que aplicó inteligencia artificial, ciencia algorítmica y machine learning a la ciberseguridad para prevenir las amenazas de seguridad más avanzadas del mundo. Incorporado en un innovador proceso de análisis predictivo, la Plataforma AI Cylance sirve como base de innovadores productos de seguridad impulsados por IA para enfrentar ángulos de ataque críticos.

ThreatDetection and Response
Detección de amenazas y respuesta
Las amenazas de malware continúan centrándose en las empresas distribuidas y en las pequeñas y medianas empresas, y no parece que esto vaya a cambiar. Pero, con pocos recursos y un presupuesto limitado, ¿cómo pueden estas organizaciones ganar la batalla contra los ataques avanzados? Detección y Respuesta ante Amenazas de WatchGuard utiliza varios métodos de detección para detener amenazas conocidas y desconocidas. Mediante la correlación y la priorización de los datos de eventos de red, de endpoint y de inteligencia sobre amenazas, los usuarios pueden responder con confianza a los ataques más graves antes de que se produzca un daño.

Seguridad Perimetral | UTM - Total Security Suite

Modelo	T20/T20-W	T40/T40-W	T80	M290	M390	M590	M690
Usuarios	5	20	50	75	250	500	850
Rendimiento Firewall	1,7 Gbps	3,4 Gbps	4,7 Gbps	5,8 Gbps	18 Gbps	20 Gbps	29,7 Gbps
Rendimiento UTM	154 Mbps	300 Mbps	631 Mbps	1.180 Mbps	2,4 Gbps	3,3 Gbps	4,6 Gbps
Rendimiento VPN	450 Mbps	880 Mbps	1,4 Gbps	2,4 Gbps	5,2 Gbps	4.6 Gbps	5.2 Gbps
Conex. concurrentes	100.000	200.000	200.000	3.500.000	4.500.000	6.000.000	15.000.000
VPN Tunnels / Mobile VPN	10/10	30/30	60/60	75/75	250/250	500/500	1.000/1.000
Interfaces	5x 1 Gb,	5[a] x 1 Gb, 1 x PoE+ 1 serie / 2 USB	8x 1 Gb, 2x PoE+ 1 serie / 2 USB, 1x bahía exp.SFP+	8x1Gb 2xSFP+ fiber	8x1Gb 2xSFP+ fiber	8x1Gb 2xSFP+ fiber	8x1Gb 2xSFP+ fiber
Formato	Desktop	Desktop	Desktop	Rack	Rack	Rack	Rack

Consulta ofertas con tu comercial

Desenmascare amenazas ocultas antes de que ataquen.

Las organizaciones de todos los tamaños se han visto infestadas de ataques sofisticados que evaden las defensas mediante firmas tradicionales, lo que resulta en la pérdida de información, millones de dólares y daño permanente a su reputación. APT Blocker de WatchGuard le pone fin a estas rápidas y persistentes amenazas mediante el uso de un espacio aislado en la nube de última generación que simula un hardware físico y expone al malware diseñado para evadir defensas de seguridad de red tradicionales.

Caracterísiticas principales

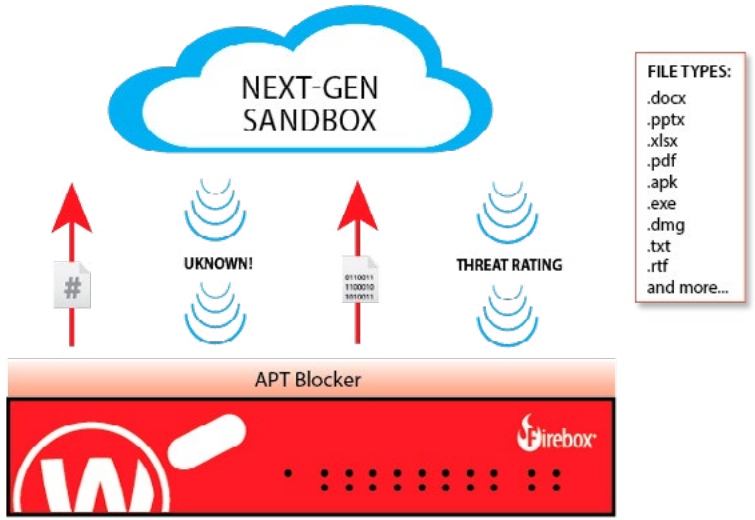
- Proporciona protección avanzada contra ransomware, amenazas de tipo zero-day y malware cambiante.
- Se implementa en segundos como parte de una solución de seguridad integrada.
- Analiza a fondo un amplio rango de ejecutables y documentos, incluidos los archivos de oficina.
- Ofrece respuesta instantánea a amenazas con alertas automáticas.
- Se integra a la perfección con WatchGuard Dimension para obtener visibilidad total.

  Tiempo de análisis promedio de menos de dos minutos.

Cómo funciona

APT Blocker de WatchGuard trabaja en tándem con Gateway AntiVirus de WatchGuard para lograr la solución suprema para la detección y prevención de malware avanzado. Si el archivo pasa el análisis de Gateway AntiVirus*, se envía una porción del archivo al espacio aislado en la nube de APT Blocker para determinar si es una amenaza conocida. Si no se reconoce la porción, APT Blocker solicita al Firebox que envíe el archivo completo, que se ejecuta en un entorno que simula un hardware físico para realizarle un análisis integral contra amenazas. Luego, si el archivo es sospechoso, se alerta a los administradores con un índice de amenaza.

**APT Blocker requiere suscripción a Gateway AntiVirus de WatchGuard*



Combata las amenazas en evolución

A medida que las amenazas continúan evolucionando y se vuelen más complejas, no existe una sola tecnología que pueda ofrecer una protección completa contra amenazas por sí sola. Es por eso que en WatchGuard, adoptamos un enfoque en capas para la seguridad de red, manteniéndonos constantemente adelantados al panorama de amenazas en evolución con un conjunto de potentes servicios de seguridad. Las defensas basadas en firmas todavía son fundamentales como primera línea de defensa, ya que eliminan las amenazas conocidas en la gateway. Sin embargo, todavía necesita protección contra los ataques desconocidos que puedan pasar por las primeras capas de seguridad. Allí es donde entra APT Blocker al ofrecer su próximo nivel en detección y prevención de malware avanzado.

La emulación de sistema total simula el hardware físico

El malware moderno, incluidas las amenazas persistentes avanzadas, ransomware, y ataques de día cero, está diseñado para reconocer y evadir las defensas tradicionales. La emulación de sistema total de APT Blocker, la cual simula el hardware físico que incluye la CPU y la memoria, proporciona el nivel más completo de protección contra el malware avanzado.

Prevención, detección y resolución

WatchGuard APT Blocker se centra en el análisis de comportamiento para determinar si un archivo es malintencionado, mediante la identificación y el envío de los archivos sospechosos a una sandbox basada en la nube en la que se emula, se ejecuta y se analiza el código para determinar su potencial de amenaza. Si se determina que el archivo sospechoso es malintencionado, APT Blocker rápidamente actúa para garantizar que su red y activos digitales permanezcan seguros.

Facilidad de uso

WatchGuard APT Blocker no solo ofrece protección integral contra el malware avanzado, sino que lo hace con una interfaz de usuario simple e intuitiva. Desde la consola de administración, puede acceder a los controles fáciles de usar para permitir, anular, bloquear o poner en cuarentena archivos por nivel de gravedad, así como también establecer notificaciones personalizadas para cuando APT Blocker detecte una amenaza.

Visibilidad sin precedentes

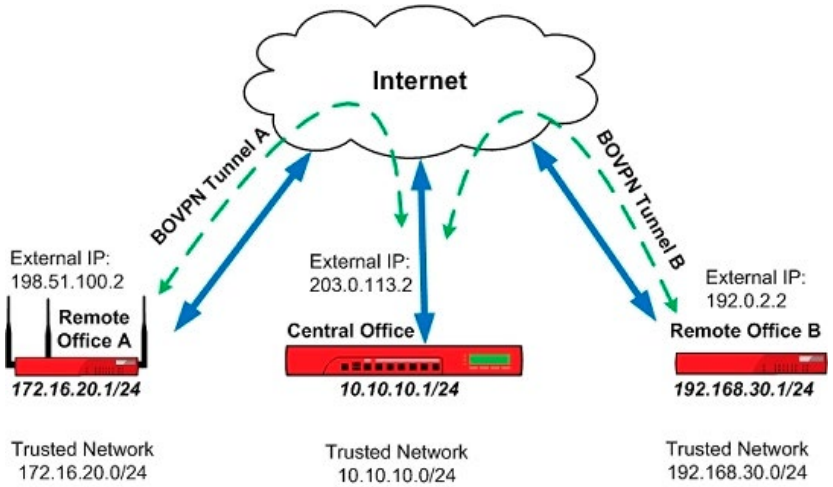
Obtenga visibilidad completa de las amenazas avanzadas que intentan atacar su red, incluidos los protocolos utilizados, las identificaciones de las amenazas, el origen del remitente y los tipos específicos de actividades malintencionadas que se habrían producido si APT Blocker no hubiera actuado.

Agent-less, trabaja sin necesidad de software adicionales.

- Activación servicio
- Autenticación usuarios
- Políticas de acceso.

Solución multi-puesto, permite trabajar con varios dispositivos simultáneamente.

Despliegue en minutos gracias a la funcionalidad WatchGuard RapidDeploy



Browser Station

Acceso seguro y cómodo a redes privadas

Con myQNAPcloud Link puede acceder, compartir, descargar y gestionar archivos almacenados en un NAS basado en HQ a través de Internet. El NAS de QNAP también admite servicios VPN para los empleados que tienen que acceder de forma remota al NAS y a los recursos en una red privada desde Internet. QNAP Browser Station dispone de navegadores virtuales en el NAS de QNAP, para que pueda acceder fácilmente a los recursos de LAN desde dispositivos remotos con seguridad y privacidad en línea.

Caracterísiticas principales

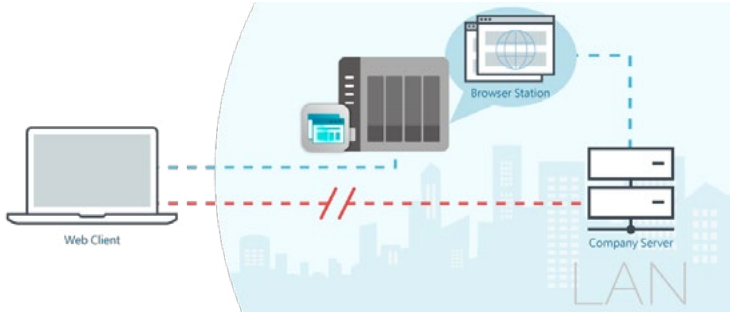
Acceso remoto codificado y tráfico de Internet.

Elimina las restricciones geográficas y desbloquea las páginas web.

Descarga archivos directamente al NAS.

Acceso cifrado y desbloqueo de páginas web

Cuando viaja o trabaja desde una oficina remota/doméstica, debe acceder de forma remota a los servidores privados de su empresa que requieren autenticación. Los navegadores virtuales proporcionados por Browser Station le ayudan a acceder fácilmente a los recursos de LAN desde dispositivos remotos sin necesidad de un proxy o VPN, y se beneficia de la seguridad y la privacidad online.



Descargar archivos directamente al NAS

Puede especificar una carpeta compartida NAS para descargar archivos (incluidos archivos adjuntos de correo electrónico y sitios web) cuando utilice los navegadores virtuales en la Browser Station.

Nota: Browser Station no es compatible con la transmisión de audio o video.

Intuitiva Interfaz de gestión

La sencilla interfaz de gestión le permite abrir varios navegadores en una única interfaz y también administrar fácilmente todos los navegadores mediante la visualización de su información en tiempo real, incluidos los usuarios, la utilización del sistema NAS, el tiempo creado, los registros, etc.

Nota: Actualmente Browser Station solo es compatible con Google Chrome™.

Seguridad del EndPoint

EndPoint Security

Complementos de Seguridad EndPoint

Comunicación Privada

Seguridad del EndPoint | Introducción de Soluciones

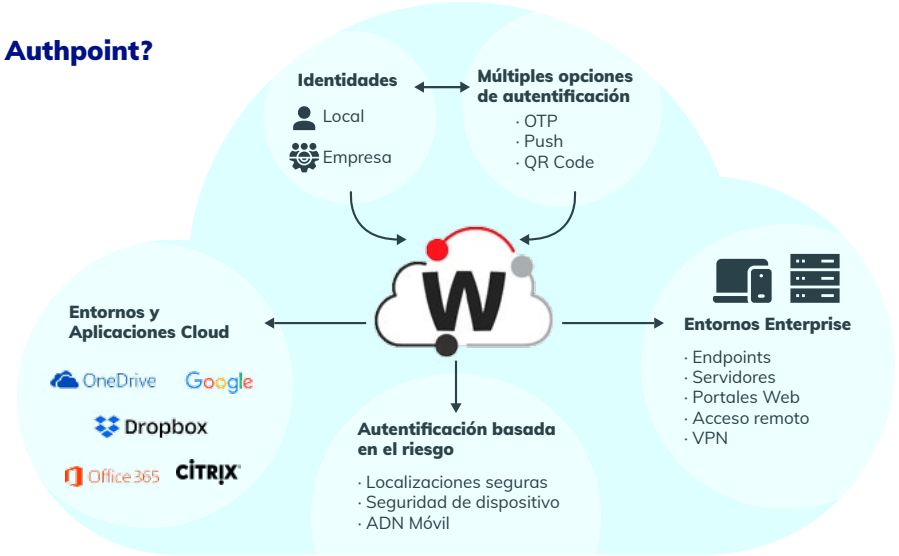
¿Por qué WatchGuard como solución de seguridad?

- Simplicidad, despliega, configura y administra de forma aágil y centralizada.
- Innovación, desarrollo constante de nuevas capas de seguridad incorporadas a sus equipos.
- Agilidad, el rendimiento de sus soluciones está muy equilibrado y balanceado cuando se trata de aunar servicio en una única máquina o servicio.
- Visibilidad, conviertes esas grandes fuentes de información en una interfaz fácil de utilizar con unos dashboard e informes adaptables a cualquier perfil empresarial.
- Apoyo directo, cuenta con un equipo de soporte que satisfacera las necesidades tanto técnicas como comerciales, garantizando la mejor atención a clientes y socios.
- Soluciones diferenciadoras. Características de estas soluciones.

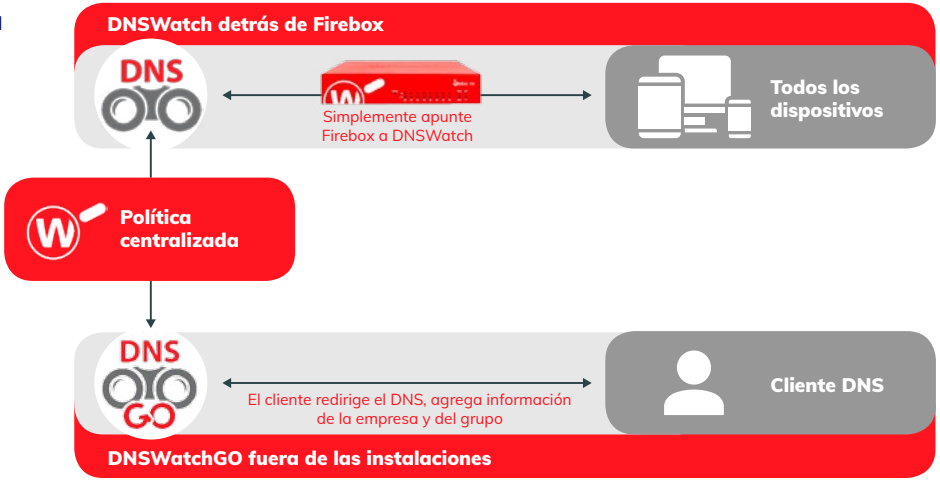
WatchGuard Passport Pack

Authpoint
+
DNSWatchGO

¿Cómo funciona Authpoint?



¿Cómo funciona DNSWatch & DNSWatchGO?

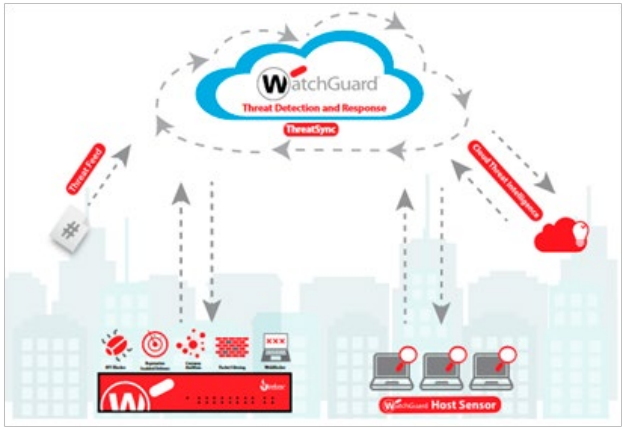


Seguridad del EndPoint | WatchGuard Thread Detection and Response

Entendiendo los Comportamientos del Malware.

Estos son algunos de los pasos favoritos del malware:

- ■ Esconde un destino que hospeda malware en una macro de Microsoft para descargar y ejecutar el malware
- □ Se genera y elimina a sí mismo para evadir las tecnologías de detección
- ■ Intenta obtener privilegios de administrador evadiendo controles que existen para gestionar la autorización y el control de acceso del usuario en él núcleo del sistema operativo
- □ Modifica archivos o procesos introduciendo componentes maliciosos
- ■ Elimina archivos originales del sistema y los reemplaza con copias maliciosas del mismo nombre y tipo de archivo



Detección con TDR

Para encontrar amenazas avanzadas de malware, el servicio de seguridad más reciente de WatchGuard, Detección y Respuesta ante Amenazas (TDR), aprovecha diversas formas de detección, a través del Sensor de Host de WatchGuard

Firmas: las firmas son una línea de defensa crucial en la lucha contra el malware. Siempre es bueno contar con un arsenal de amenazas conocidas.

Heurística: TDR utiliza reglas o algoritmos para buscar comandos que pudieran indicar intenciones maliciosas. Cuenta con hasta 17 métodos de heurística, mediante el Sensor de Host de WatchGuard.

Análisis de Comportamientos: Nuestro módulo de Prevención de Ransomware de Host realiza un seguimiento de los comportamientos que generalmente se relacionan con ataques de ransomware, para realmente prevenir estos ataques antes de que se realice el cifrado de archivos.

Detección de Redes: La visibilidad de los patrones de tráfico bloqueados o inusuales, las visitas a sitios web maliciosos o riesgosos y la detección de botnets y otras amenazas son fundamentales para proteger su organización.

El Poder de la Correlación

Recopilar datos de una variedad de fuentes es la decisión inteligente en seguridad.
A través de la correlación, se toma toda la información que estas soluciones de seguridad producen, se la relaciona e interpreta.
Disminuya la cantidad de tiempo necesario para detectar y solucionar amenazas.

Circulo Completo con ThreatSync

TreatSync no solo brinda visibilidad sobre los eventos queocurren en la red y en los puntos finales, sino que, al brindaruna valorización y clasificación integrales de las amenazas los equipos de seguridad saben qué amenazas son lasmás importantes y cuáles requieren atención inmediata.La priorización de amenazas permite a las organizaciones disminuir el tiempo de detección y corrección, así como la cantidad de recursos dedicados que se requieren para eliminar amenazas.

Automatización de Respuestas con TDR.

La TDR de WatchGuard permite a los usuarios establecer políticas fácilmente, para habilitar la automatización según las necesidades de la organización. Mediante la aplicación de estas políticas se pueden destruir procesos maliciosos, poner un archivo infectado en cuarentena y eliminar el valor de claves del registro de dudosa procedencia. Todo sin la intervención humana, convirtiendo al sistema en una potente solución equipada con capacidades de resiliencia, es decir, procesos automatizados de corrección y respuesta ante amenazas.

TDR está disponible en todos los UTM WatchGuard que se adquieran con un licenciamiento Total Security Suite. A continuación, se muestra una tabla comparativa de licencias por modelos.

Firefox Model	Included Host Sensors
T20	5
T40	20
T80	50
M290	75
M390	150
M590 / M690 / M4800 / M5800	250
M440 / M570 / 670 / M4600 / M5600	250
Firebox Cloud / FireboxV S	50
Firebox Cloud / FireboxV M	150
Firebox Cloud / FireboxV L	250
Firebox Cloud / FireboxV XL	250

WatchGuard Passport
MFA Authpoint

Porque elegir los Autenticación Multifactor de Watchguard.

La autenticación multifactor (MFA) AuthPoint le brinda la seguridad que necesita para proteger los activos, las cuentas y la información crítica de su empresa, permitiendo que su empresa trabaje de forma segura y sin preocupaciones.

Porque es tan segura la solución de MFA de WatchGuard:

Autenticación basada en contexto, aporta información referente a usuario que está haciendo la solicitud, a que recurso se intenta acceder, desde donde y la hora y fecha.
Token virtuales anti-clonación, el token está compuesto por tres factores, una internal unique key, internal Clock y finalmente el ADN del móvil. La suma de ellos hace una llave única que dificultad las capacidades para ser clonada.

Caracterísiticas principales

- **Implementación y administración basada en la nube, rápido y simple.**
  Administre la plataforma en cualquier lugar, en cualquier momento a través de una plataforma de administración fácil de usar.
- **Autenticación fácil de usar directamente desde su teléfono móvil.**
  No es necesario transportar tokens; puede autenticarse usando una simple aplicación móvil en su teléfono.
- **Ecosistema completo de aplicaciones para integración.**
  Asegure sus accesos VPN, acceso al login de los equipos corporativos, acceso aplicaciones on-premise o cloud.

AuthPoint (Coste por usuario)

Duración de licencia	1 año		
Part Number	WGATH571	WGATH581	WGATH591
Usuarios	5-250	251-1.000	+1.000

Consulta ofertas con tu comercial

AuthPoint (Coste por usuario)

Duración de licencia	3 años		
Part Number	WGATH573	WGATH583	WGATH593
Usuarios	5-250	251-1.000	+1.000

Consulta ofertas con tu comercial

Seguridad del EndPoint | WatchGuard Passport DNS WatchGO

Porque elegir las soluciones de movilidad de Watchguard.

Protección a nivel de DNS para usuarios en cualquier lugar.
Tanto si trabaja desde una oficina o en el hogar, En la actualidad, tres cuartos de los empleados de todo el mundo trabajan de forma remota al menos un día a la semana. Como resultado, una parte cada vez mayor de su negocio se lleva a cabo fuera de la red y fuera de sus herramientas de seguridad tradicionales. DNSWatchGO de WatchGuard proporciona protección a nivel de DNS y filtrado de contenido que mantiene su empresa a salvo de la suplantación de identidad, el ransomware y otros ataques, incluso cuando su usuario está fuera de la red, sin requerir una VPN.

Caracterísiticas principales

- Detección a nivel de DNS, que proporciona una capa de seguridad adicional para bloquear las conexiones.
- Protege automáticamente a los usuarios finales de ataques de suplantación de identidad.
- Filtrado de contenido que limita el acceso web, basado en categorías web.
- No se requiere VPN.
- Seguridad ligera y siempre activa, basada en software.

DNSWatchGO (Coste por usuario)

Duración de licencia	1 año		
Part Number	WGDNS951	WGDNS961	WGDNS971
Usuarios	5-250	251-1.000	+1.000

Consulta ofertas con tu comercial

DNSWatchGO (Coste por usuario)

Duración de licencia	3 años		
Part Number	WGDNS953	WGDNS963	WGDNS973
Usuarios	5-250	251-1.000	+1.000

Consulta ofertas con tu comercial

Seguridad del EndPoint | WatchGuard Passport

Proteja a los empleados remotos

WatchGuard Passport brinda a sus empleados la seguridad en la nube que necesitan para trabajar sin inconvenientes desde la oficina, la casa o en cualquier lugar. Cada servicio del paquete de Passport proporciona protección permanente y siempre activa que se mueve con sus usuarios.

Caracterísiticas principales

- **Protección de nivel DNS para usuarios en cualquier lugar.**
  Mantenga a sus usuarios a salvo de suplantaciones de identidad, ransomware y otros ataques sin requerir una VPN.
- **Autenticación fácil de usar directamente desde su teléfono móvil.**
  No es necesario transportar tokens; puede autenticarse usando una simple aplicación móvil en su teléfono.

Pack Passport (Coste por usuario)

Duración de licencia	1 año		
Part Number	WGPSP861	WGPSP871	WGPSP881
Usuarios	5-250	251-1.000	+1.000

Consulta ofertas con tu comercial

Pack Passport (Coste por usuario)

Duración de licencia	3 años		
Part Number	WGPSP863	WGPSP873	WGPSP883
Usuarios	5-250	251-1.000	+1.000

Consulta ofertas con tu comercial

Seguridad del EndPoint | Suite WatchGuard

	WatchGuard Email Protection	EndPoint Protection Plus	Adaptive Defense	Adaptive Defense 360
Gestión centralizada desde una única consola en la nube	●	●	●	●
Único agente ligero en el endpoint		●	●	●
Protección de aplicaciones maliciosas (malware, phishing, ransomware, troyanos,...)	●	●	●	●
Protección phishing, malware y amenazas avanzadas en correo	●	Exchange		Exchange
Protección antispam en correo	●	Exchange		Exchange
Aplicación de políticas de configuración y tareas en tiempo real		●	●	●
Dashboard, informes y alertas en tiempo real	●			
Detección de exploits desconocidos por comportamiento de los procesos			●	●
Monitorización de actividad en Windows, macOS y Linux			●	●
macOS y Linux	Perimetral	●	●	●

Seguridad del EndPoint | Suite WatchGuard Email Protection

Seguridad y filtrado del correo electrónico desde la nube

Una protección deficiente de la seguridad del correo electrónico puede provocar latencia, tiempo de inactividad del servidor de correo electrónico, indisponibilidad de la red, pérdida de productividad e interrupción de las actividades comerciales. Las campañas masivas de marketing por correo electrónico pueden comprometer la reputación de una empresa.

Protección multicapa para el correo de tu empresa contra todo tipo malware y spam.

Email Protection ofrece protección inmediata y efectiva contra los virus y el spam, gracias a los escaneos online que se realizan en los servidores de WatchGuard Security.

Su tecnología de escaneo avanzado en la nube no necesita infraestructuras adicionales para empezar a operar.

Caracterísiticas principales

- **No requiere infraestructura de cliente. Todas las operaciones se realizan en la nube.**
- **Ofrece protección inmediata y eficaz contra virus y spam, a través de análisis en línea realizados en los servidores de WatchGuard Security.**
- **Email Protection es increíblemente sencillo de usar. La configuración del servicio y su consola Web aseguran una operatividad completa desde el principio.**

Beneficios

- Protección sólida La protección del correo electrónico aprovecha el poder de la inteligencia colectiva para brindar protección proactiva en tiempo real desde la nube, lo que garantiza los niveles más altos de detección de malware y amenazas conocidos y desconocidos en el tráfico de correo electrónico entrante y saliente.
- Costos y consumo de recursos mínimos. Disponible como una nube. servicio basado, no requiere inversión en infraestructura ni personal especializado. Utiliza tecnologías específicas para reducir el uso de recursos y ancho de banda sin una inversión inicial.
- Fácil de usar y mantener La seguridad se puede administrar en cualquier momento y en cualquier lugar desde la consola web. La instalación es sencilla y las actualizaciones son automáticas y transparentes para los usuarios.
- Disponibilidad del servicio 24x7. Brinda a los usuarios acceso seguro e ininterrumpido al correo electrónico a través del correo web, independientemente de su dispositivo y ubicación. Garantiza la entrega de correo electrónico en caso de problemas con el servidor de correo y ofrece respaldo de correo electrónico.
- Monitoreo permanente y en profundidad: el tablero proporciona a los administradores una vista dinámica del estado del sistema y la actividad de filtrado para varios períodos de tiempo. Sus informes automatizados muestran resúmenes detallados de la actividad de la red y permiten a los administradores filtrar información a pedido.

Seguridad del EndPoint | Suite WatchGuard EndPoint Protection Plus (Antivirus)

Proteja a los empleados remotos

WatchGuard Endpoint Protection Plus es una solución completa de seguridad avanzada para equipos, portátiles y servidores que gestiona de manera centralizada, la seguridad de los endpoints que se encuentrentanto dentro como fuera de la red corporativa.

Este servicio ofrece un conjunto de tecnologías EPP contra el malware, ransomware y amenazas que aprovechan vulnerabilidades desconocidas (zero-day), sin necesidad de instalar o mantener nuevos recursos hardware en la infraestructura de la organización.

Además, su agente es ligero y no impacta en el rendimiento de los endpoints, siendo accesible a través de una única consola web. Esto simplifica la administración de la seguridad de los endpoints y proporciona eficacia operativa.

Caracterísiticas principales

- **Seguridad centralizada de los EndPoints**
- **Protección contra malware y ransomware**
- **Desinfección avanzada**
- **Monitorización y filtrado web**
- **Control centralizado de dispositivos**
- **Filtrado de contenidos, spam y virus**
- **Instalación rápida y flexible**
- **Certificación ISO27001 y SAS 70 con disponibilidad 24x7**

Beneficios

Seguridad Multiplataforma

- Seguridad contra amenazas desconocidas: detección y bloqueo de malware, troyanos, phishing y ransomware.
- Seguridad en todos los vectores de ataque: navegación, correo, sistemas de ficheros y control de los dispositivos conectados a los endpoints.
- Análisis y Desinfección de equipos automática. Análisis de comportamientos: detección de malware conocido y desconocido.
- Seguridad en sistemas Windows, Linux, macOS, Android y entornos virtuales (VMware, Virtual PC, MS Hyper-V, Citrix). Así como entornos de virtualización (VDI), tanto persistentes como no persistentes.

Mayor Productividad

- WatchGuard Endpoint Protection Plus implementa una protección anti-spam para servidores Exchange para optimizar el tiempo de trabajo de los usuarios y aumentar la seguridad de los equipos de la red.
- Monitoriza y filtra el tráfico web evitando que los empleados tengan comportamientos improductivos o sufran amenazas de seguridad tales como bots y phishing.
- No requiere infraestructura específica o mantenimiento, el departamento de IT podrá dedicarse a tareas más productivas.

Simplifica la gestión

- Fácil de mantener: no requiere infraestructura específica para alojar la solución; el departamento de IT podrá dedicarse a tareas más productivas.
- Fácil de proteger a usuarios remotos: cada equipo protegido con WatchGuard Endpoint Protection Plus se comunica con la nube; los usuarios desplazados y delegaciones remotas se protegen de forma natural, sin instalaciones.
- Fácil de desplegar: múltiples métodos de despliegue y con desinstaladores automáticos de las soluciones de la competencia, lo que facilita una rápida migración desde soluciones de terceros

Seguridad del EndPoint | Suite WatchGuard Adaptive Defense 360 (AV + EDR)

¿En qué consiste WatchGuard Adaptive Defense 360?

WatchGuard Adaptive Defense es una suite de ciberseguridad que integra soluciones Endpoint Protection y Endpoint Detection and Response (EDR), con los servicios de clasificación del 100% de los procesos, y basado en un único y ligero agente.

La combinación de estas soluciones y servicios proporcionan una visibilidad detallada de toda la actividad en todos los endpoints, un control absoluto de los procesos en ejecución, y la reducción de la superficie de ataque.

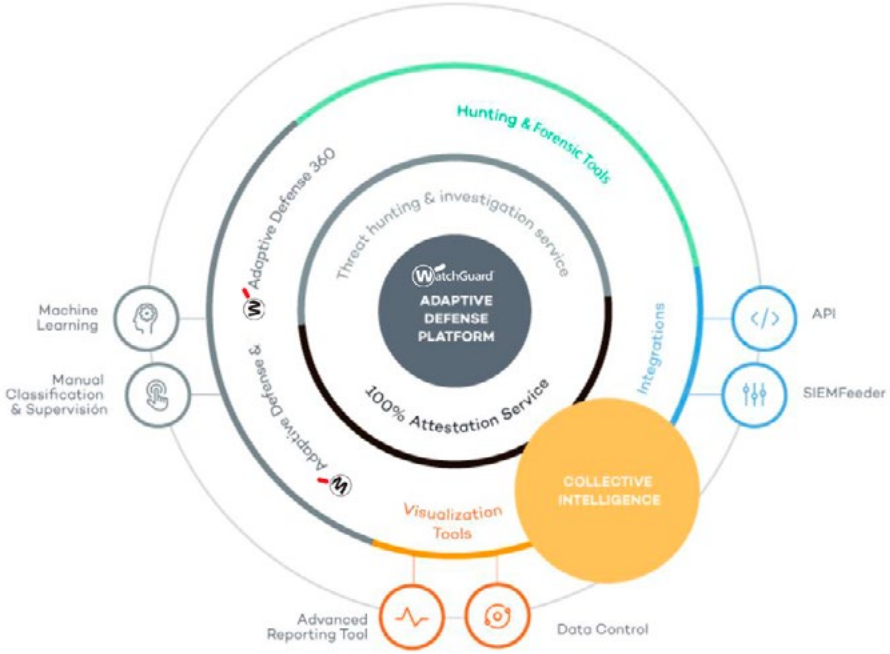
EndPoint Protection Platform
Ciberseguridad avanzada contra el malware, con capacidad de prevención, detección y remediación.

Endpoint Detection and Response
Monitoriza, registra y categoriza el 100% de los procesos activos en todos los endpoints de la red corporativa.

Servicio de Clasificación del 100%
Certifica la confiabilidad de todos los procesos activos y permite una respuesta continua e inmediata contra hackers e insiders.

Caracterísiticas principales

- **Prevención, Detección y Respuesta.**
  Para ataques con y sin malware, en un solo agente.
- **Visibilidad en Tiempo Real e Histórica.**
  Información detallada de toda la actividad de los endpoints.
- **Clasificación del 100% de los procesos.**
  El 99,98% a través de Machine Learning y el 0,02% por los analistas expertos de Panda.
- **Análisis de comportamientos**
  Análisis heurístico y detección de IoAs (Indicadores de Ataque).



Seguridad del EndPoint | With Secure EndPoint Security

W / T H secure

¿En qué consiste Protection Service for Business (PSB)?

Servicio de protección F-Secure para empresas, Protege todos sus endpoints gracias a su protección multi-capas e incluye herramientas como la administración de parches.

F-Secure ProtectionServicefor Business (PSB)
PSB incluye características de seguridad avanzadas, que brindan más visibilidad, control y capacidad de administración para empresas con mayores requisitos de seguridad, protegiendo todos sus dispositivos contra todas las amenazas, como ransomware y robo de datos.

F-Secure Protection Service for Business

	PSB Partner Managed Computer		
Duración de licencia	1 año		
Part Number	FCXCSN1NVXAQQ	FCXCSN1NVXBQQ	FCXCSN1NVXCQQ
Usuarios	1-24	25-99	100-499

Consulta ofertas con tu comercial

Seguridad del EndPoint | With Secure EndPoint Security

W / T H secure

Proteja su negocio y sus datos contra ataques avanzados

Rapid Detection & Response le ayuda a preparar a su organización para ataques cibernéticos avanzados, antes y después de que ocurran. El servicio de RDR está diseñado para detectar al más hábilde los atacantes, utilizando procedimientos, técnicas y tácticas de malware o no-malware. Le permite responder a las amenazas con rapidez.

La información más valiosa se encuentra en el endpoint.Controle constantemente su red y detecte ciberataques que se dirigen a lo que más le importa a su negocio.

Caracterísiticas principales

- Visibilidad total en todo el entorno de TI.
- Identificar amenazas avanzadas automáticamenteBloquea brechas de seguridad.
- Visualiza ataques en un contexto más amplio.
- Detección eficaz frente a cualquier tipo de ataque.

F-Secure Rapid Detection & Response

	F-Secure RDR, Partner Managed RDR Computer		
Duración de licencia	1 año		
Part Number	FCEASN1NVXAQQ	FCEASN1NVXBQQ	FCEASN1NVXCQQ
Usuarios	1-24	25-99	100-499

Consulta ofertas con tu comercial

Seguridad del EndPoint | Complementos Suite WatchGuard

WatchGuard ofrece la posibilidad de añadir complementos de seguridad a la protección de Endpoint para reducir el perímetro de ataque frente a vulnerabilidades de aplicaciones o programas sin actualizar, evitar el robo de información y la protección del correo electrónico.

	WG Full Encryption	WG Patch Management
Gestión centralizada desde una única consola en la nube	●	●
Único agente ligero en el endpoint	●	●
Protección de aplicaciones maliciosas (malware, phishing, ransomware, troyanos,...)		
Protección phishing, malware y amenazas avanzadas en correo		
Protección antispam en correo		
Aplicación de políticas de configuración y tareas en tiempo real	●	●
Dashboard, informes y alertas en tiempo real	●	●
Gestión de parches de sistemas operativos Windows y aplicaciones de terceros		●
Cifrado/Descifrado completos de discos mediante BitLocker	●	
Backup de correo entrante		
Validación estricta de emisores de correo		

WatchGuard Patch Management

WatchGuard Patch Management es una solución de gestión de vulnerabilidades y sus correspondientes actualizaciones y parches, tanto de los sistemas operativos como de cientos de aplicaciones.

Fortalece las capacidades de prevención, contención y remediación de las amenazas y de reducción de la superficie de ataque en servidores y estaciones Windows.

Proporciona visibilidad de la salud de los endpoints en tiempo real en cuanto a vulnerabilidades, parches o actualizaciones pendientes y software no soportado (EoL). Descubre, planifica, instala y monitoriza.

WatchGuard Full Encryption

WatchGuard Full Encryption, es un módulo adicional a las soluciones de protección endpoint y seguridad avanzada adaptativa de WatchGuard Security, que gestiona de forma centralizada el cifrado completo de discos.

WatchGuard Full Encryption utiliza Windows BitLocker, una tecnología estable y avalada por Microsoft, para cifrar y descifrar los discos sin impactar a los usuarios, con el valor añadido de permitir a la organización la gestión centralizada y el control de las claves de recuperación almacenadas en la plataforma cloud de gestión de WatchGuard Security: Aether.

WatchGuard Data Control

Los robos masivos de datos se han convertido en un problema demasiado frecuente: El acceso incontrolado a la información de carácter personal (PII) y sensible (IP) almacenada por las empresas es una amenaza cotidiana que puede traducirse en importantes pérdidas económicas y daños a su reputación.

WatchGuard Data Control ayuda a las organizaciones a cumplir con las normativas de protección de datos, descubriendo y protegiendo la información de carácter personal almacenada en sus equipos y servidores tanto en tiempo real como durante todo su ciclo de vida.

Advanced Reporting Tool

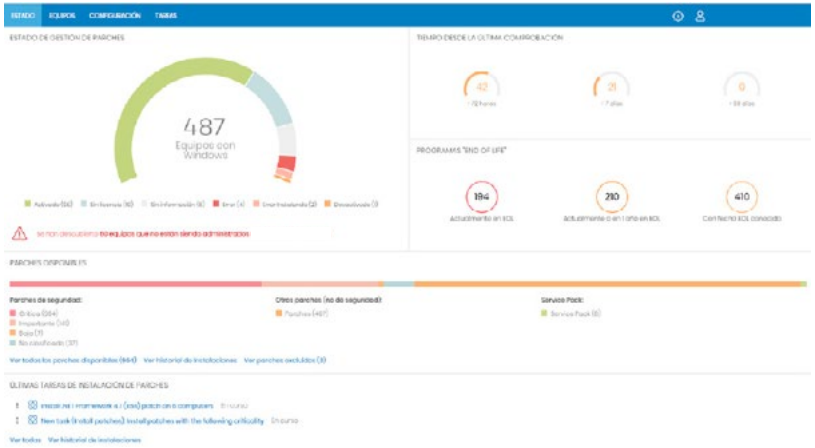
WatchGuard Advanced Reporting Tool correlaciona información, generando inteligencia de seguridad de forma automática y ofreciendo herramientas que permiten tanto localizar ataques y comportamientos extraños, como descubrir el uso incorrecto de los equipos y la red corporativa

WatchGuard Patch Mangement
Simplifica la gestión de vulnerabilidades en tu empresa

WatchGuard Patch Management es una solución de gestión de vulnerabilidades y sus correspondientes actualizaciones y parches, tanto de los sistemas operativos como de cientos de aplicaciones.

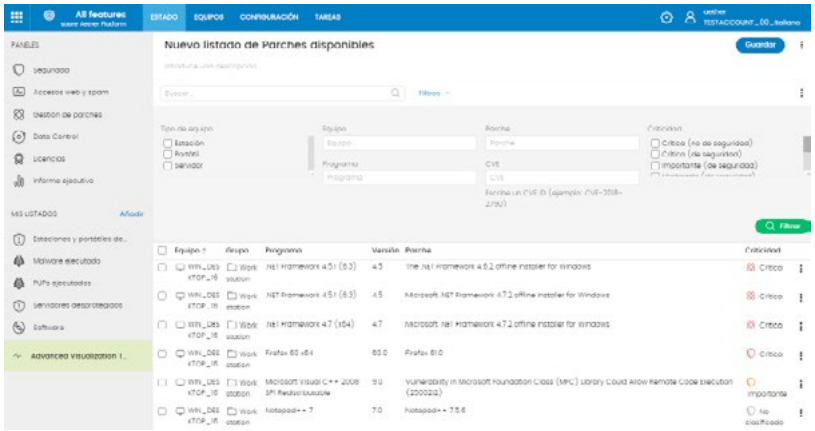
Fortalece las capacidades de prevención, contención y remediación de las amenazas y de reducción de la superficie de ataque en servidores y estaciones Windows.

Proporciona visibilidad de la salud de los endpoints en tiempo real en cuanto a vulnerabilidades, parches o actualizaciones pendientes y software no soportado (EoL). Descubre, planifica, instala y monitoriza.



Caracterísiticas principales

- Audita, monitoriza y prioriza las actualizaciones.
- Previene incidentes, reduce la superficie de ataque por vulnerabilidades.
- Contiene y mitiga ataques, parcheando inmediatamente uno o varios endpoints.
- Reduce costes operativos.
- Cumple con el principio de responsabilidad activa.



WatchGuard Full Encryption
La primera línea de defensa para proteger los datos de una manera simple y efectiva

WatchGuard Full Encryption utiliza Windows BitLocker, una tecnología estable y avalada por Microsoft, para cifrar y descifrar los discos sin impactar a los usuarios, con el valor añadido de permitir a la organización la gestión centralizada y el control de las claves de recuperación almacenadas en la plataforma cloud de gestión de WatchGuard Security: Aether.

Caracterísiticas principales

- **Previene el robo, pérdida y acceso no autorizado.**
  Mientras los discos están cifrados, protege los datoscontra el robo, pérdida accidental y hackers internos. El cifrado, descifrado, y acceso a la información es inmediato, automático y transparente para el usuario.Para evitar cualquier inconveniente, las claves de recuperación se almacenan y recuperan de forma seguradesde la plataforma cloud y su consola web.

- **Sin despliegues ni instalaciones.**
  WatchGuard Full Encryption gestiona centralizadamente Bitlocker, una tecnología de Windows probada y ampliamente difundida.BitLocker está listo para ser utilizado en casi todos los dispositivos Windows, la Plataforma Aether, con su consola web centralizada, es el único punto de gestión.No hace falta desplegar e instalar otro agente, todas las soluciones basadas en la Aether comparten el mismo agente ligero.

- **Cumplimiento de regulaciones, informes y gestión centralizada**
  WatchGuard Full Encryption simplifica y ayuda a tu organización a cumplir con las regulaciones de protección de datos, a supervisar y a forzar la activación de BitLocker en los dispositivos Windows. Todas las soluciones basadas en Aether cuentan con dashboards intuitivos, informes de detalle y auditorías de cambios. Además, la administración basada en roles permite implementar niveles de autorización separados y establecer políticas para grupos y dispositivos desde una única consola web centralizada.

WatchGuard Data Control
Supervisa los datos sensibles en el endpoint

Este módulo ha sido diseñado para ayudarte a cumplir con las regulaciones de protección de datos (GDPR), y para proteger y dar visibilidad sobre los datos de carácter personal y sensible de tu organización tanto en tiempo real como durante todo su ciclo de vida, cuando estos residen en los servidores y puestos de trabajo.

WatchGuard Data Control descubre, audita y monitoriza los datos de carácter personal y sensible desestructurados en los endpoints: desde el dato en reposo, hasta las operaciones sobre ellos y su tránsito.

Evita los accesos incontrolados a los datos sensibles de tu empresa y te ayuda a cumplir con el nuevo reglamento de protección de datos GDPR.

Beneficios principales

- **Descubre y audita.**
  Identifica los ficheros con datos de carácter personal (PII) de tu empresa y registra cualquier tipo de acceso a ellos.
- **Monitoriza y detecta.**
  Alerta en tiempo real, sobre fuga, uso o tráfico sospechosos o no autorizados.
- **Simplifica la gestión.**
  No requiere ningún despliegue adicional y su activación es inmediata y desatendida.
- **Control de los Datos.**
  Demuestra a los responsables, al DPO y a los autorizados que tu empresa tiene un control exhaustivo de los PII ubicados en sus equipos.

Funcionalidades

Data Discovery
Crea un inventario indexado de todos los ficheros donde se han encontrado datos personales desestructurados, con el número de ocurrencias por cada tipo mediante una clasificación automática de los mismos (data at rest).
La clasificación combina diferentes técnicas y algoritmos de machine learning que optimizan los resultados tanto para minimizar falsos positivos, como para disminuir el consumo de recursos en los dispositivos.

Data Search
Realiza búsquedas libres personalizadas para identificar ficheros con cualquier tipo de información personal.
Ofrece un listado de todos los ficheros donde se encuentra dicha información y permite su exportación para un sencillo manejo.

Data Monitoring:
Se monitorizan las diferentes operaciones sobre los ficheros desestructurados manteniendo actualizado el inventario de ficheros con datos personales (data in use). Cuando estos ficheros van a ser copiados o movidos desde el dispositivo, se registra la operación de exfiltración sobre los clientes de correo, navegadores, FTP, etc (data in motion).

Data Visualization:
El resultado del descubrimiento y la monitorización continua se sincroniza constantemente en la Plataforma de Adaptive Defense y su módulo de Advanced Visualization Tool. En él se dispone de herramientas de explotación de los eventos sobre los datos personales en reposo, uso y tránsito, tanto en tiempo real como retrospectivo, a lo largo de su ciclo de vida en los dispositivos.

Advanced Reporting Tool
Convierte los datos en conclusiones de Seguridad y Gestión IT

Este módulo agrega toda la información obtenida, la correlaciona y la representa gráficamente en tiempo real para ofrecer visibilidad granular de todos los eventos que suceden en la red corporativa.

Los paneles de control de WatchGuard Advanced Reporting Tool incluyen indicadores clave, búsquedas y alertas prestablecidas en base a:

· Incidentes de ciberseguridad.
· Acceso a información crítica.
· Consumo de recursos de red y uso de aplicaciones.

Características principales

- **Control de amenazas.**
  Determina el origen de las amenazas y activa las medidas de seguridad necesarias para prevenir futuros ataques.
- **Gestión de acceso.**
  Implementa políticas de acceso para restringir el acceso a la información crítica.
- **Monitoriza y detecta.**
  El uso inapropiado de los recursos corporativos que pueden tener impacto en tu negocio o en el desempeño de los trabajadores.
- **Corregir los comportamientos.**
  De aquellos empleados que no se ajustan a las políticas de uso establecidas.

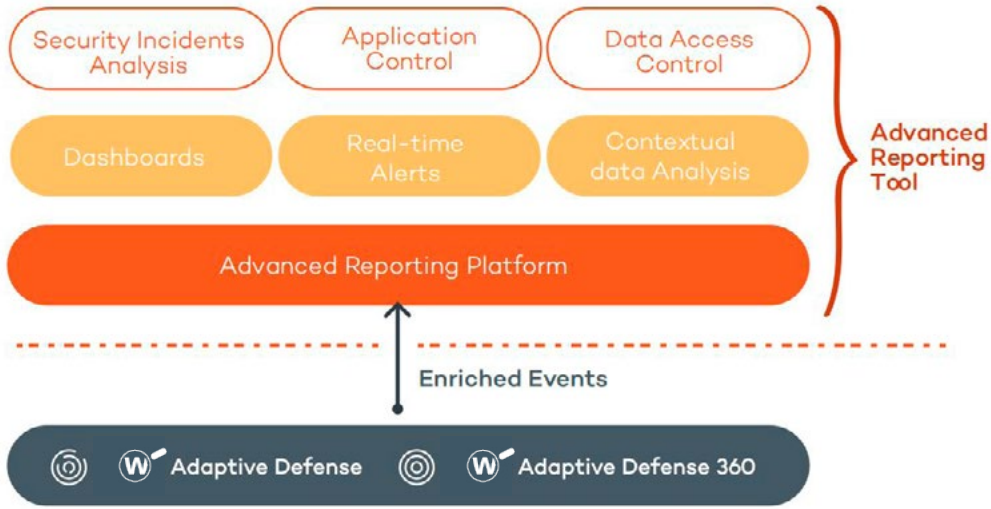
El aumento del volumen de información de seguridad manejado impide a los departamentos de IT fijarse en los detalles importantes.

Esta información es utilizada para detectar problemas e infracciones de seguridad provocados tanto por elementos externos como por los Insiders de la compañía.
Los departamentos de IT se encuentran desbordados: el alto volumen de información gestionada y la entrada en escena del malware de nueva generación, hacen que muchos detalles pasen inadvertidos o no sean registrados en absoluto, comprometiendo la seguridad de todo el sistema.

La solución: WatchGuard Adaptive Defense 360 + Advanced Reporting Tool.

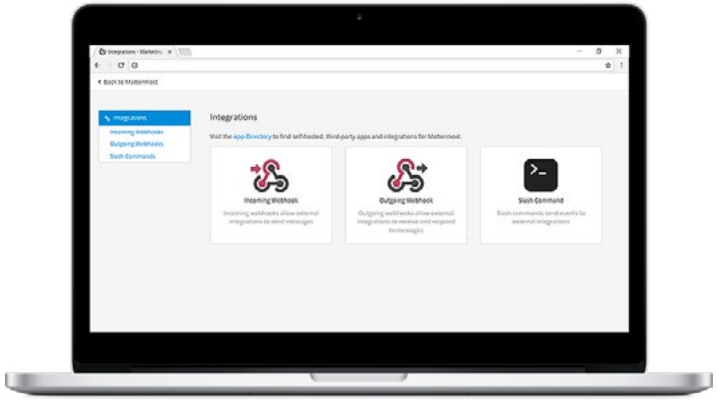
Advanced Reporting Platform automatiza el almacenamiento y correlación de la información generada por la ejecución de procesos y su contexto, extraída por **WatchGuard Adaptive Defense 360 en el endpoint.**

Advanced Reporting Tool permite encontrar, explorar y analizar conclusiones operativas de IT & Seguridad sin necesitar infraestructura, instalaciones, mantenimientos o procesamiento de logs.



Separe sus mensajes personales de sus mensajes de trabajo

Mattermost es una plataforma de mensajería instantánea segura y colaborativa que ahora está disponible para QNAP NAS. Mattermost es una herramienta de colaboración ágil que proporciona a los miembros de un equipo tanto un chat público como un privado, transferencia de archivos y más funciones de productividad. Gracias a la integración con QNAP NAS, disfrutará de una disponibilidad permanente, una fiabilidad superior y una enorme capacidad de almacenamiento. Con Mattermost, su QNAP NAS será el portal de sus necesidades de comunicación y colaboración.



Al utilizar una plataforma de comunicación alojada en su QNAP NAS, la dirección IP de su empresa, los patrones de uso y las conversaciones se guardarán de forma local y no se transmitirán al exterior, lo que garantiza una mayor confidencialidad.

El enfoque de alojamiento en un servidor propio de Mattermost proporciona el nivel de control, privacidad y cumplimiento legal que necesitan las empresas.

QNAP NAS ofrece una enorme capacidad de almacenamiento y una escalabilidad flexible para responder a las necesidades de las empresas.

Mattermost permite a los miembros de un equipo comunicarse con texto e intercambiar archivos de forma clara y eficaz. Dada la alta capacidad de almacenamiento de QNAP NAS, los registros se pueden conservar durante más tiempo.

La compatibilidad con webhooks permite a los usuarios integrar fácilmente aplicaciones externas en el servidor, lo que facilita la automatización y la integración.

Mattermost proporciona diversas formas de comunicarse, entre las que se incluye la posibilidad de que los miembros del equipo puedan estar conectados desde cualquier lugar utilizando sus dispositivos móviles.

Wi-Fi Seguro

WatchGuard Secure Cloud Wi-Fi

Wi-Fi Seguro | Secure Cloud Wi-Fi

Porque crear entornos Wi-Fi seguros con WatchGuard.

Las empresas siempre han estado preocupadas por la seguridad inalámbrica pero nunca se les presentó una solución que pudieran pagar, o una que pudieran hacer funcionar. WatchGuard pudo poner todo eso en una solución de fácil implementación que realmente funciona".

Su entorno inalámbrico confiable (TWE) comienza con Cloud-ManagedWi-Fi seguro

Un entorno inalámbrico confiable (TWE) se tiene que basar en una estructura en el cual se desarrolla una red completa de Wi-Fi que cuente con las siguientes características, que searápida, fácil de administrar y, sobre todo, segura. Los negocios enfrentan la responsabilidad de desarrollar entornos inalámbricos confiables (TWE) para proteger a sus empleados y clientes. WatchGuard es la única empresa que proporciona la tecnología y las soluciones que usted puede usar para desarrollar un entorno inalámbrico confiable (TWE), cumpliendo con cada uno de los tres pilares fundamentales del desempeño líder del mercado, la administración escalable y la seguridad integral y verificada.

■ Gestión escalable en la nube& Aplicación web móvil

El entorno de WatchGuardWi-Fi Cloud ofrece administración centralizada y puede brindar a su negocio desde uno hasta una cantidad ilimitada de puntos de acceso en múltiples ubicaciones, sin una infraestructura de controladores.
WatchGuard GO es una aplicación web móvil que le permite configurar rápida y fácilmente redes inalámbricas desde cualquier teléfono inteligente o tableta, independientemente de dónde se encuentre.

□ Protección patentada de seguridad WIPS

Una violación a la seguridad inalámbrica puede significar para su empresa mucho tiempo, problemas y gastos. Nuestro patentado Wireless IntrusionPreventionSystem (WIPS) ayuda a garantizar que usted tenga la protección que necesita. WIPS defiende su espacio aéreo las 24 horas, los 7 días de la semana, contra dispositivos no autorizados, ataques «man-in-the-middle», ataques de negación de servicio, puntos de acceso (AP) no autorizados y mucho más, todo con casi cero falsos positivos.

No necesita quitar y reemplazar. Solo agregue WIPS.

Cada punto de acceso WatchGuard tiene la flexibilidad de operar tanto como punto de acceso y como sensor de seguridad WIPS dedicado. Esto significa que, cuando se implementan como sensores WIPS dedicados, los dispositivos trabajan con sus puntos de acceso existentes (Cisco, Aruba, Ruckus, Ubiquiti, etc.) y agregan protección de seguridad inalámbrica empresarial a su red. En este caso, en vez de ofrecer tráfico Wi-Fi seguro a los usuarios, ofrecemos protección de seguridad WIPS sin precedentes que está dedicada 100% a explorar el aire y proteger su empresa de amenazas inalámbricas.

■ Solución de problemas y visibilidad de red inteligente

Los profesionales de TI han sufrido la carencia de capacidad de resolución de problemas y de visibilidad remota a la salud de su red. La aplicación Discover dentro de Wi-Fi Cloud cambia las reglas de juego y se adapta para cautivar a los administradores de red con la serie más completa de funciones de visibilidad Wi-Fi, solución de problemas y estado de red, lo que ahorra tiempo y dinero.

Wi-Fi Seguro | Secure Cloud Wi-Fi

¿Por qué WatchGuard Wificloud como solución WLAN?

WatchGuard Secure Wi-Fi tu entornos inalambricos seguros y confiables, para aquellos preocupados por su seguridad.

Despliegua un entorno inalambrico de confianza de forma rápida, fácil de administrar y lo más importante muy seguro. Crea entornos inalambricos confiables para garantizar la protección de sus empleados y evita los peligros que rodean a las redes inalambricas por su exposición al entorno. Los puntos de acceso de WatchGuard actuan como sensores WIPS tanto en una red con puntos de acceso de WatchGuard como de otros fabricantes, proveyendo a estos de forma automatica de un escudo de seguridad capaz de identificar las seis categorias de amenazas conocidas. Restringen el acceso de agentes externos a la red empresarial y a su vez garantizan que los dispositivos corporativos puedan operar en otras redes de dudosa procedencia.

Pide tu soporte personalizado

Modelo	AP130	AP330	AP430CR	AP432
Entorno	INDOOR	INDOOR	OUTDOOR	INDOOR
Velocidad de Wi-Fi	1.200 Mbps (5Ghz), 574 Mbps (2.4 Ghz)	1.200 Mbps (5Ghz), 574 Mbps (2.4 Ghz)	2.300 Mbps (5Ghz), 574 Mbps (2.4 Ghz)	2.400 Gbps (5Ghz), 1.148 Mbps (2.4 Ghz)
Interfaz	2x GbE, 1x PoE	2x GbE, 1x PoE	3x GbE, 1x PoE, 1x LAN	2x GbE, 1x PoE
Alimentación	802.3at (PoE+)	802.3 at (PoE+)	802.3at (PoE+)	802.3at (PoE+)

Consulta ofertas con tu comercial

*Incluye suscripción de un año a Secure Wi-Fi, licencia Cloud, soporte básico y WIPS.

Visibilidad

33

Visibilidad de Red
WatchGuard Dimension
(WatchMode)

34

Visibilidad Wi-Fi
WatchGuard WIPS

36

Visibilidad del EndPoint
F-Secure Radar

Visibilidad | Red - WatchGuard WatchMode

Porque elegir las soluciones de movilidad de Watchguard.

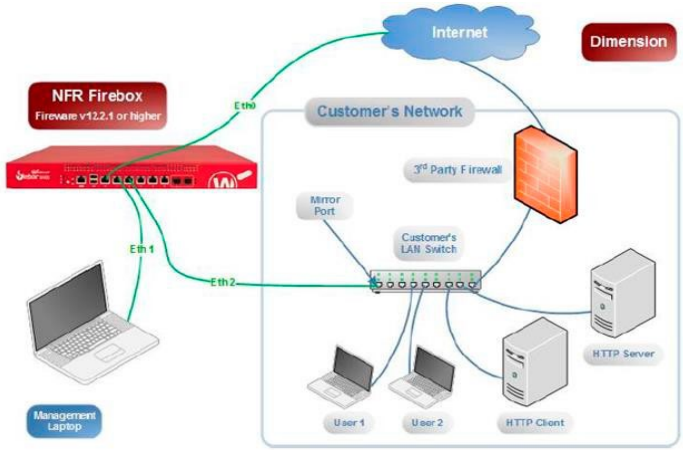
WatchMode es una herramienta que puede usar para mostrar a sus clientes el valor indispensable que un WatchGuardFirebox puede agregar a su solución de seguridad de red. Cuando se configura en WatchMode (modo auditoría), el Firebox recopila información sobre la actividad de la red y envía mensajes de registro a un WatchGuardDimension Server, para visibilidad e informes.
Para usar WatchMode, es necesario habilitar la opción WatchMode en Firebox e instale Firebox en el clientered detrás de un dispositivo de terceros (un conmutador o switch) que cuente con la capacidad de configurar un puerto espejo.
Los Firebox recibe en el puerto especjo el tráfico de red enviado por el dispositivo de terceros que actua como gateway de la red y generando a su vez el registro de los mensajes con información sobre la actividad de la red. Después de que Firebox envía los mensajes de registro a un WatchGuardDimension Server, puede generar informes para demostrar cómo WatchGuardFirebox puede proporcionar una seguridad superior, así como una visibilidad detallada e incomparable de la actividad en su red.

¿Qué necesito?

- Firebox M270 o superior en formato NFR.
- Switch capa 2 con capacidad de “Port Mirror”.
- Máquina virtual WatchGuardDimension(Free) en un equipo local o remoto.

¿Cómo funciona?

El firebox recopila información sin impacto sobre la red y envía mensajes de log a un servidor. Dimensión para visibilidad e informes.



Visibilidad | WiFi - WatchGuard Wips

¿En qué consiste WatchGuard Wips?

WIPS es un término de la industria del Wi-Fi que habla de la prevención de amenazas de Wi-Fi, y en WatchGuard lo han llevado al siguiente nivel. El sistema WIPS de WatchGuardno se parece a ninguna otra solución de seguridad de Wi-Fi que compita en el mercado. La tecnología patentada de WatchGuard asegura la protección de Wi-Fi real, precisa y automatizada que su empresa necesita.

Cloud-ManagedWi-Fi seguro de WatchGuard es la ÚNICA solución para detecta y previene automáticamente las seis categorías conocidas de amenazas de Wi-Fi simultáneamente.

Lamentablemente, es probable que su solución Wi-Fi existente no pueda bloquear ninguna de las amenazas mencionadas, y menos aún proteger a su empresa de que se presenten TODAS al mismo tiempo.

WatchGuard tiene la respuesta:
No necesita quitar y reemplazar. Solo agregue WIPS.

Cuando se implementan como sensores WIPS dedicados, los dispositivos trabajan con sus puntos de acceso existentes (Cisco, Aruba, Ruckus, Ubiquiti, etc.)

¿Cómo funciona?

- Los APsWatchGuard como “sensores WIPS dedicados” instalados junto 3 a 4 puntos de acceso de la competencia, aseguran a las comunicaciones inalámbricas y dan visibilidad de infracciones de seguridad en el medio aéreo.

¿Qué necesito?

- Watchguard AP125 o superior por cada 3 o 4 ya instalados.
- Licenciamiento Wificloud en modalidad Secure Wifi o Total Wifi.

1. **Punto de acceso no autorizado**
Permite que los atacantes eludan la seguridad del perímetro.

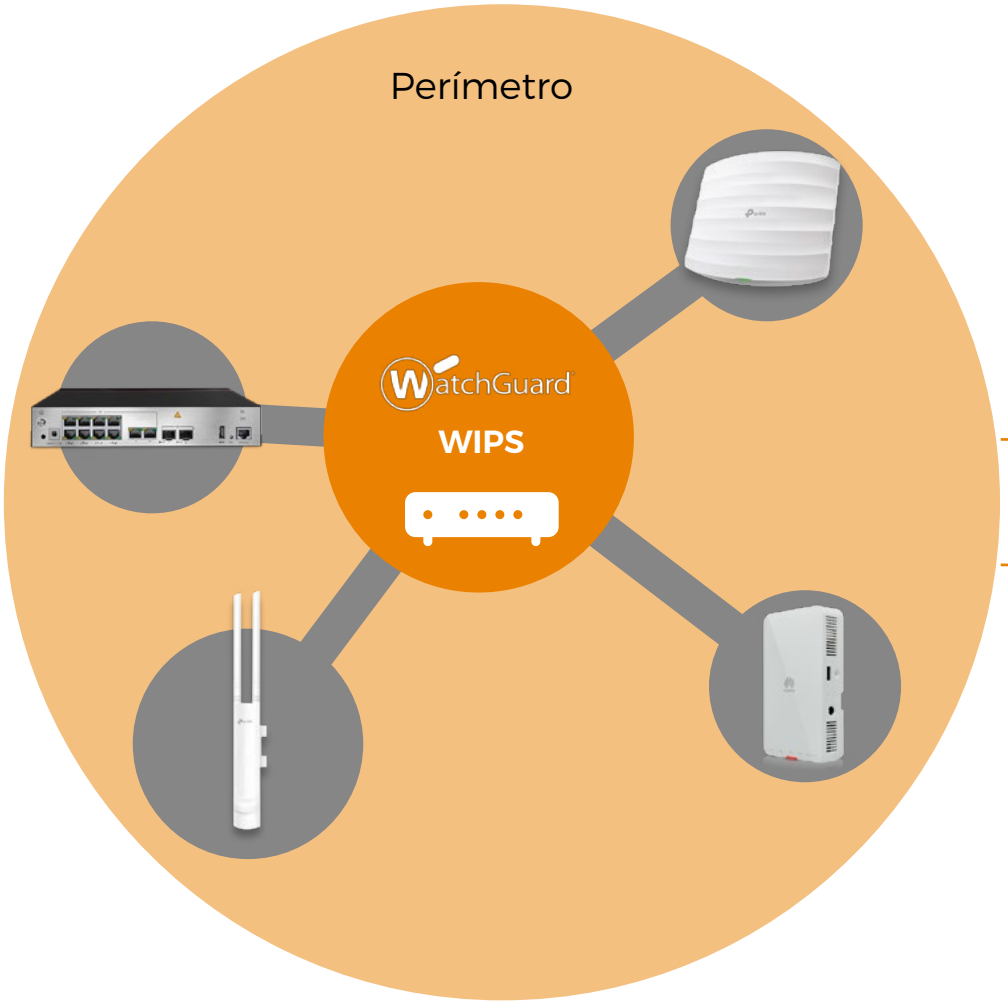
2. **Cliente no autorizado**
Esparce cargas de malware en la red luego de conectarse a PA malintencionados.

3. **Punto de acceso vecino o Mala asociación de cliente**
Pone en peligro de infección por conectarse a otras SSID mientras está en el alcance del PA autorizado.

4. **Red ad hoc**
Utiliza conexiones punto a punto para evadir controles de seguridad y pone en riesgo la exposición a malware.

5. **Punto de acceso de "Gemelo malvado/eviltwin"**
Atrae a usuarios a conectarse a él para espiar el tráfico, robar datos e infectar sistemas.

6. **Punto de Acceso Mal Configurado**
Abre redes para atacar como resultado de errores de configuración.



DESCUBRE CON **WATCHGUARD** LA MANERA DE TENER UNA **DEFENSA PERIMETRAL**

Obtenga seguridad Wi-Fi adicional
sin necesidad de reemplazar sus puntos de acceso existentes.

SUPERVISA HASTA 4 PUNTOS DE ACCESO DE CUALQUIER FABRICANTE

Compatible con:

- Firewalls
- Switches
- APs
- Routers

Administrar las vulnerabilidades críticas para el negocio

F-Secure Radar es una plataforma de escaneo que identifica dónde son vulnerables los activos de su organización, lo que le permite minimizar su superficie de ataque para reducir el riesgo.

Combina la detección y el inventario de herramientas de TI, la identificación y la gestión de amenazas tanto internas como externas.
Informa sobre los riesgos y el cumplimiento de las normas actuales y futuras ((como el cumplimiento con la Industria de las tarjetas de pago y del Reglamento General de Protección de Datos, RGPD.

Con Radar de F-Secure, su equipo de seguridad de TI mapea la superficie de ataque de su organización junto con:

- Todas las vulnerabilidades conocidas, desconocidas y potenciales que son críticas para el negocio
- Los controles en todo el software, el hardware, el firmware y las redes
- La TI en la sombra, los sistemas externos mal configurados, los sitios web de malware, los servidores vinculados a los sitios web
- La entropía de la seguridad de los socios y los contratistas
- El phishing y las violaciones de marca

Análisis y gestión de vulnerabilidades en una única solución. EXPLORE MÁS ALLÁ DE SU RED

- DESCUBRA LAS HERRAMIENTAS DE RED
- ANALICE LOS SISTEMAS Y LAS APLICACIONES
- GESTIONE LAS VULNERABILIDADES
- EVALÚE Y VERIFIQUE
- INFORMES SOBRE RIESGOS

F-Secure Radar

	F-Secure Radar Cloud License (competitive upgrade and new)		
Duración de licencia	1 año		
Part Number	FCKCSN1NVXBQQ	FCKCSN1NVXCQQ	FCKCSN1NVXDQQ
Usuarios	25-99	100-499	500-999

Consulta ofertas con tu comercial

Backup

Entorno Híbrido

Entorno Virtualizado

Entorno Cloud

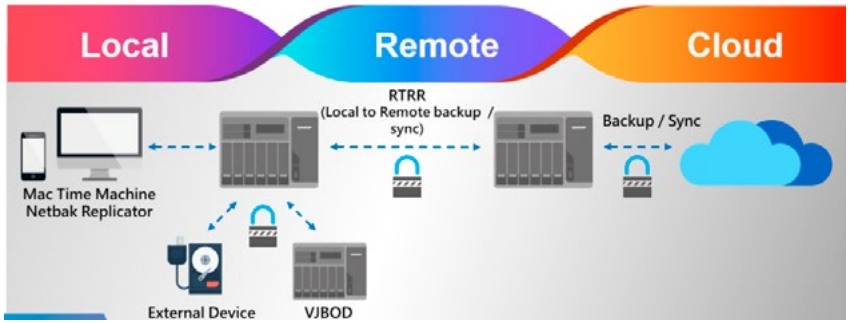
UDP

Snapshots & QSYNC

HBS 3. Copia de seguridad de múltiples nubes, deduplicación de datos, restauración instantánea y sincronización flexible

HBS 3 consolida las funciones de copia de seguridad, restauración y sincronización en una única aplicación de QTS para que transfiera fácilmente sus datos a espacios de almacenamiento local, remoto o en la nube a modo de almacenamiento completo de datos y plan de recuperación ante desastres. Con la tecnología QuDedup que deduplica los datos en el origen, la eficiencia de la copia de seguridad multiversión en el almacenamiento de destino se mejora considerablemente, a la vez que también optimiza el uso del almacenamiento.

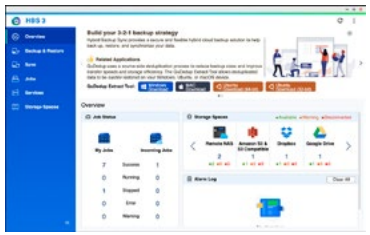
Solución con nube híbrida



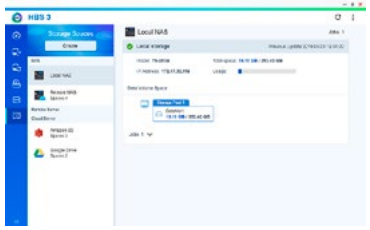
- Se tiene la ventaja de la nube privada y la nube híbrida al mismo tiempo.
- Copia de seguridad 3 – 2 – 1, tres copias, dos lugares mínimo y uno en la nube.
- Soporta la mayoría de destinos de almacenamiento. (File Storage, object storage, QNAP NAS, VJBOD, RSYNC SERVER, CIFS/SMB, FTP SERVER.

Interfaz fácil de usar que permite optimizar los procesos

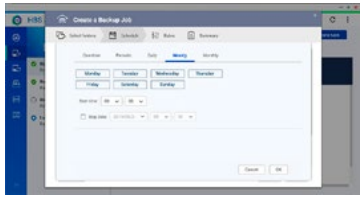
HBS 3 ofrece una interfaz fácil de usar que permite ver fácilmente el estado de las tareas y los horarios Puede configurar fácilmente tareas de copia de seguridad/restauración y de sincronización, así como gestionar espacios de almacenamiento.



Visión general de instantáneas
Gestione sus instantáneas con una interfaz profesional y más detallada. Todas las versiones de las instantáneas y la hora de la última instantánea se registran con precisión.



Réplica de instantáneas
Visualice las tareas de copia de seguridad de instantáneas de un volumen/LUN, incluido el destino, la programación, la última hora de finalización/siguiente hora de inicio y la información sobre el progreso.



Almacenamiento de instantáneas
Almacene instantáneas de forma centralizada desde otro NAS.

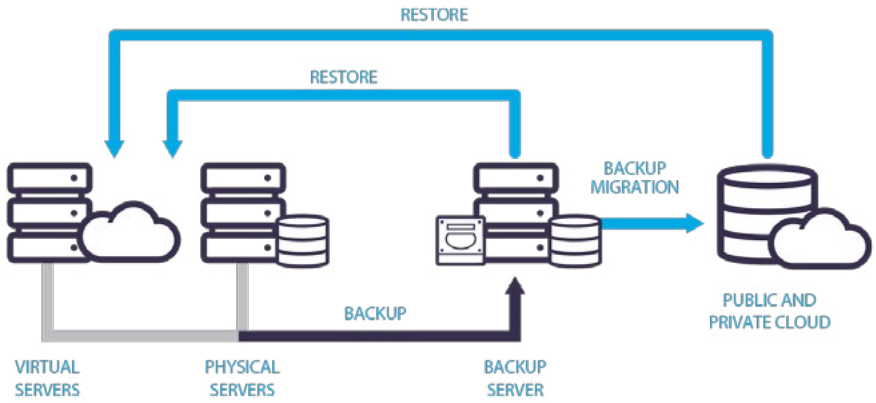
Backup | Entorno Híbrido - Arcserve Backup

arcserve®

Proteja su almacenamiento de gran capacidad con el software de copia de seguridad en cinta más potente del mundo

Arcserve hace la copia de seguridad en cinta de forma diferente con tecnologías únicas que mejoran las economías de la protección de datos al permitir períodos de retención más largos, reducir el almacenamiento e integrar una potente deduplicación en su entorno de copia de seguridad existente.

Almacene los datos críticos en casi cualquier dispositivo de cinta, desde una única unidad de cinta hasta enormes bibliotecas de cintas. Gestione más datos en más ubicaciones. Reduzca el tiempo dedicado a la gestión de las copias de seguridad, independientemente de lo sencilla o compleja que sea su infraestructura.



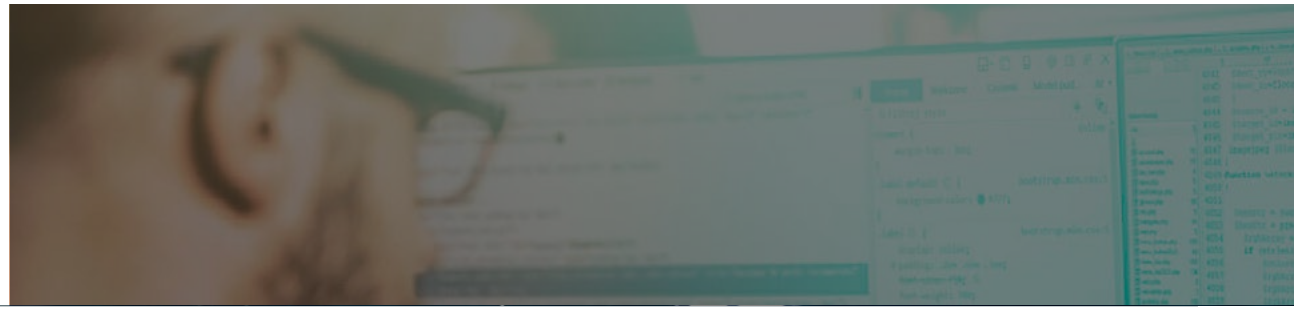
Características principales

- Deje de perder tiempo rebuscando entre los datos con la gestión centralizada y los informes del gestor de recursos de almacenamiento (SRM). Supervise el estado de todas las actividades de copia de seguridad, encuentre los nodos que más tardan, localice los datos respaldados y haga un seguimiento de los volúmenes y discos.
- Incorpore funciones sofisticadas a sus plataformas VMware, Microsoft Hyper-V y Citrix XenServer. Simplifique la gestión del sistema con una visión de todo su entorno y mitigue el riesgo de pérdida de datos en los servidores virtualizados.
- Aumente la fiabilidad con las funciones de restauración inteligente. Redirija los trabajos de restauración a otros soportes que contengan los mismos datos sin ninguna intervención manual.
- Restaurar rápidamente objetos de aplicación individuales de Active Directory, Microsoft Exchange, Microsoft SQL Server y Microsoft SharePoint.
- Ofrezca copias de seguridad y restauraciones más rápidas y eficientes con los transportadores de datos UNIX y Linux para las copias de seguridad basadas en SAN.
- Cumplir con los requisitos específicos de la aplicación con la copia de seguridad en disco, la copia de seguridad en cinta, la copia de seguridad de disco a disco a cinta (D2D2T), la copia de seguridad de disco a disco a la nube (D2D2C), la biblioteca virtual de cintas (VTL), la compatibilidad con las instantáneas de hardware, la multiplexación y el flujo múltiple.

¿Cómo funciona?

El software Arcserve Backup es una solución integral de gestión del almacenamiento para entornos distribuidos y multiplataforma que puede realizar copias de seguridad y restaurar datos de todos los equipos de la red, incluidos los que ejecutan Windows, UNIX y Linux. Ofrece un control y una visibilidad completos desde una consola de gestión, tanto si se trata de entornos empresariales a pequeña escala como a gran escala en diferentes plataformas y organizaciones.

Una vez instalado, podrá crear, gestionar y supervisar los trabajos de Arcserve Backup desde una ubicación central. Los trabajos se envían en el servidor primario y pueden ejecutarse localmente en el propio servidor primario o de forma remota en cualquiera de los servidores miembros asociados. Realice operaciones de trabajo como copias de seguridad, restauraciones, fusiones, escaneos, migraciones, copias, comparaciones, etc. para todos los servidores desde el servidor primario. Supervise el estado de los trabajos desde la cola central de trabajos.



Backup | Entorno Híbrido - Arcserve Continuous Availability

Protección continua de datos para servidores de archivos y aplicaciones empresariales, con alta disponibilidad de todo el sistema para empresas que operan 24/7

Arcserve Continuous Availability garantiza la continuidad del negocio con tecnologías probadas que tienen un propósito común: mantener su negocio en funcionamiento. Cumpla con confianza los acuerdos de nivel de servicio (SLA) más estrictos mediante la replicación continua de datos a nivel de sistema de archivos/carpetas y aplicaciones, y sistemas físicos/virtuales completos, con conmutación por error automática.

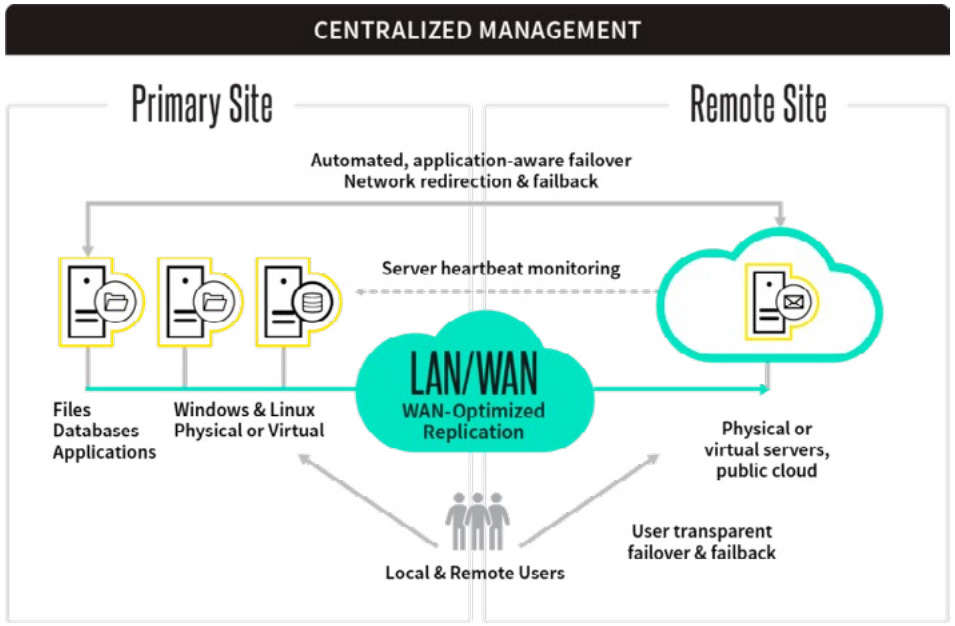
Arcserve Continuous Availability simplifica el despliegue de una sólida estrategia de alta disponibilidad al eliminar la necesidad de una colección de costosas herramientas de replicación centradas en aplicaciones y sistemas específicos. Diseñado para funcionar en hardware y entornos distintos, evita el tiempo de inactividad en toda su infraestructura con alta disponibilidad y protección de datos continua para aplicaciones y sistemas Windows y Linux en las instalaciones, en remoto y en la nube.

Características principales

- Mantener réplicas actualizadas de sistemas de misión crítica; sistemas Windows a XenServer, VMware, Hyper-V, Amazon EC2 o Microsoft Azure; sistemas Linux a VMware, Hyper-V, KVM, Amazon EC2 o Microsoft Azure.
- Mantenga las aplicaciones disponibles y accesibles mediante la replicación en tiempo real en servidores físicos, VMware, Hyper-V, Amazon EC2 o Microsoft Azure.
- Gestione la replicación de datos para Exchange, SQL, IIS, SharePoint, Oracle, Hyper-V y aplicaciones personalizadas en un solo programa.
- Retroceder las aplicaciones a un punto en el tiempo antes de una caída del sistema, corrupción de datos o evento de ransomware.
- Transferencia de datos con cifrado AES-128, AES-256 o de nivel personalizado entre ubicaciones locales y remotas sin necesidad de una VPN.

¿Cómo funciona?

El software Arcserve Continuous Availability sincroniza los datos de sus sistemas Windows y Linux con un segundo sistema físico o virtual que usted aprovisiona localmente, en una ubicación remota o en la nube. Una vez sincronizados, los cambios a nivel de bytes se replican continuamente desde su sistema de producción al sistema de réplica, proporcionando una protección constante para mantener los datos y la información precisos, con los sistemas en funcionamiento.



Backup | Entorno Virtualizado - Hiper Data Protector

¿En qué consiste Hiper Data Protector?

Se trata de un dispositivo de copia de seguridad VMware® y Hyper-V sin licencia

Con un único NAS de QNAP y sin necesidad de pagar cuotas de licencia, podrá hacer copia de seguridad de entornos VMware® e Hyper-V ilimitados. Hyper Data Protector le ofrece un plan de recuperación de desastres rentable y fiable, lo que garantiza un funcionamiento permanente de sus servicios.

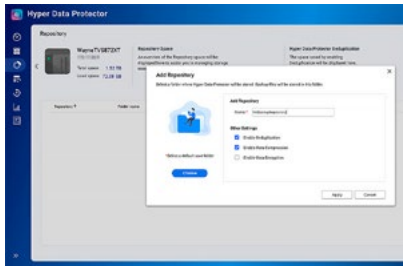
Ya no necesita un hardware y un software independientes para la copia de seguridad de máquinas virtuales (VM). Con el NAS de QNAP e Hyper Data Protector, podrá crear una tarea de copia de seguridad sin agente para hacer copias de seguridad ilimitadas de máquinas virtuales VMware® vSphere y Microsoft® Hyper-V. Hyper Data Protector incluye funciones de copia de seguridad incremental, deduplicación global, programación de la copia de seguridad y compresión de recuperación para ahorrar tiempo de copia de seguridad, tiempo de almacenamiento y recuperación. Sin necesidad de licencias ni gastos adicionales, Hyper Data Protector es ideal para crear un plan de recuperación asequible y fiable.

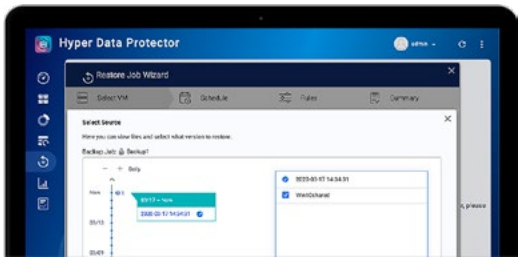
Características principales

- **Menor TCO.**
  Copia de seguridad de máquinas virtuales sin licencia y con un solo NAS, lo que reduce el coste total de propiedad.
- **Ahorre tiempo de copia de seguridad y almacenamiento.**
  Incluye funciones de copia de seguridad incremental en el origen y deduplicación global, lo que ahorra tiempo y almacenamiento.
- **Reduzca el tiempo de recuperación**
  Admite funciones de cifrado y compresión de la recuperación, lo que hace que las tareas de recuperación resulten más rápidas y más seguras.

Sencilla copia de seguridad de máquinas virtuales con retención de múltiples versiones

Simplemente añada su VMware® y Hyper-V al inventario de Hyper Data Protector y luego siga los pasos del Asistente para tareas de copia de seguridad con el fin de crear sus propias tareas de copia de seguridad. Puede hacer copia de seguridad de todas las máquinas virtuales del Hipervisor o bien hacer copia de seguridad de determinadas copias de seguridad individuales. Hyper Data Protector admite la retención de múltiples versiones para un máximo de 1000 versiones.





Cuatro razones por las que debería usar Hyper Data Protector en el NAS de QNAP

- Copia de seguridad de máquinas virtuales sin licencia con un único NAS: sin software ni hardware adicional, sin necesidad de licencia.
- El NAS de QNAP incluye protección mediante instantáneas, protección de RAID y reparación y limpieza de RAID para una mayor protección de los datos.
- El espacio de almacenamiento del NAS se puede ampliar para responder a las crecientes necesidades de las empresas.
- Y lo más importante, el NAS de QNAP es algo más que un dispositivo de copia de seguridad de máquinas virtuales. Puede instalar una amplia gama de aplicaciones desde el App Center para sacar el máximo partido a su NAS.

Backup | Entorno Virtualizado
Soluciones de Arcserve Secured by Sophos

arcserve®

Protección de datos y cibernética integrada para información en local, en la nube y basada en SaaS.

Es hora de defenderse con la única solución que permite neutralizar los ataques cibernéticos, como el ransomware, sin la complejidad de las aisladas estrategias de protección de datos y seguridad cibernética.

¿El resultado? Un enfoque proactivo y multicapa orientado al ransomware y los datos que le permitirá alcanzar la resiliencia informática con mayor rapidez.

Características principales

- Proteger sus copias de seguridad con Sophos Intercept X Advanced, una tecnología de vanguardia en seguridad cibernética que aplica una red neuronal de deep learning para detectar malware conocido y desconocido sin depender de firmas.
- Responder rápidamente a las amenazas y eliminarlas, gracias a CyptoGuard y WipeGuard, que usan análisis de comportamientos para bloquear ataques de ransomware y de MBR nunca vistos.
- Implantar copias de seguridad inmutables, con protección de datos heterogénea y basada en imágenes que protege la información en local, en la nube y basada en SaaS frente a amenazas externas, grandes desastres, errores humanos u otras interrupciones no planificadas.
- Si lo requiere, active de manera segura copias de sistemas físicos y virtuales dentro o fuera del sitio, o en nubes privadas y públicas. Las amenazas se neutralizan y se elimina la probabilidad de pérdida de datos y tiempo de inactividad.

Protección de servidores en local

Protección de cargas de trabajo en la nube

Seguridad para los datos basados en SaaS

Orquestación y migración no disruptiva de datos, aplicaciones y cargas de trabajo a la nube y a cualquier otra infraestructura

Arcserve Live Migration fue diseñado para eliminar las interrupciones durante su transformación en la nube. Mueva fácilmente los datos, las aplicaciones y las cargas de trabajo a la nube o al destino de su elección mientras mantiene su negocio totalmente en funcionamiento. Elimine la complejidad orquestando la transición al destino de destino. Gestione todo el proceso de migración a la nube desde una consola central.

Características principales

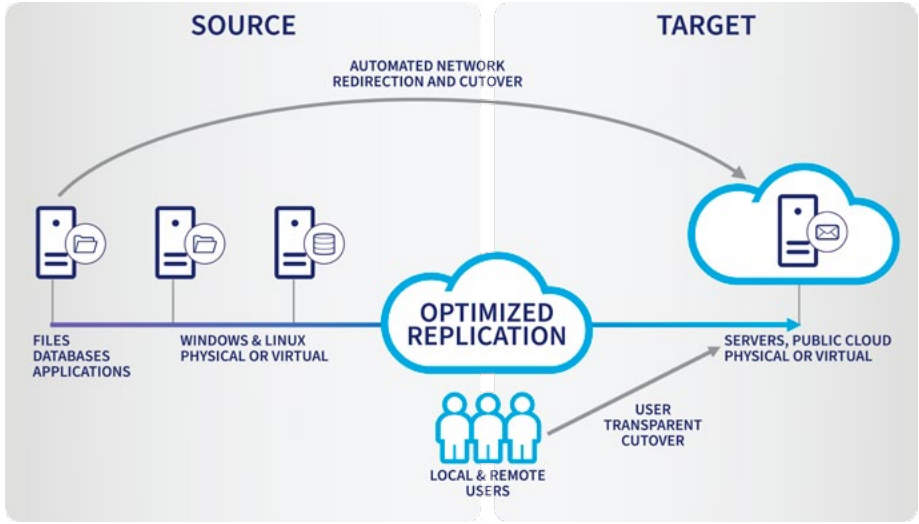
- Migrar sin interrumpir el negocio con una replicación asíncrona en tiempo real que mueve los datos, las aplicaciones y las cargas de trabajo de las instalaciones a la nube, de la nube a la nube, de la nube a las instalaciones y de las instalaciones a las instalaciones.
- Elimine los pasos manuales que suelen ser necesarios durante el proceso de migración con la redirección automática de la red.
- Consiga una mayor flexibilidad con la replicación encriptada en varios entornos que admite la replicación de virtual a virtual, de físico a virtual y de físico a físico.
- Probar la migración antes de la transición sin afectar a la producción.

¿Cómo funciona?

Arcserve Live Migration sincroniza automáticamente los archivos, las bases de datos y las aplicaciones de los sistemas Windows y Linux con un segundo entorno físico o virtual situado en las instalaciones, en una ubicación remota o en la nube. Una vez sincronizados, los cambios se replican en tiempo real para garantizar que el origen y el destino estén sincronizados antes de la migración.

El cifrado permite transferir datos de forma segura entre los sistemas locales y las ubicaciones remotas sin necesidad de una VPN, y la redirección de red automatizada hace que el proceso de cambio sea perfecto, con un botón de corte para garantizar la disponibilidad del nuevo entorno de producción.

Todo el proceso de migración se gestiona desde una consola central con pruebas de integridad integradas y no disruptivas que pueden automatizarse por completo o realizarse de forma programada o según sea necesario.



Backup | Entorno Virtualizado - Arcserve ShadowXafe

arcserve®

Solución de copia de seguridad y recuperación de última generación con protección sin agente y con agente para entornos altamente virtualizados

ShadowXafe® ofrece una completa protección de datos de última generación, la mejor copia de seguridad y recuperación de datos del sector y escalabilidad empresarial, todo ello con una experiencia perfecta. ShadowXafe es fácil de implementar y gestionar, y garantiza una protección de datos segura, menos tiempo de inactividad de las aplicaciones y una mayor productividad.

Características principales

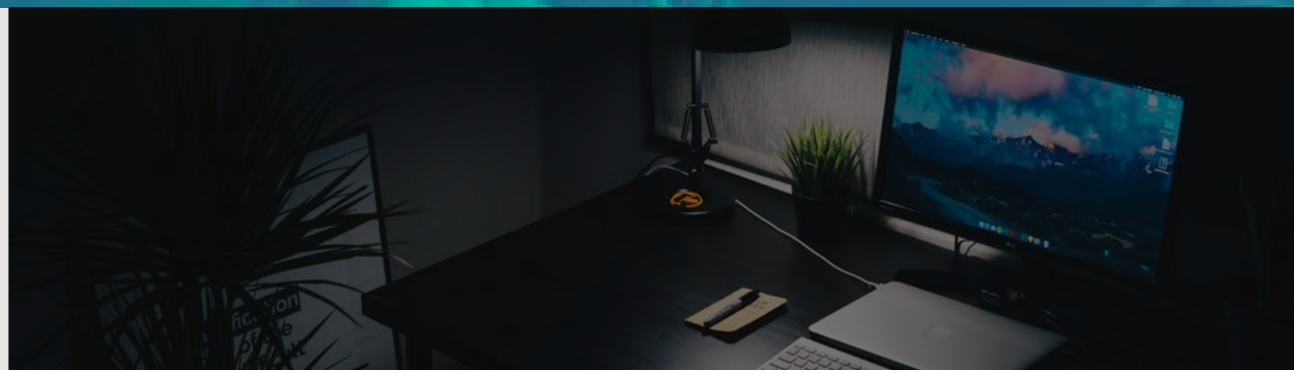
- **Copias de seguridad y recuperación de desastres fiables**
  La re-verificación automatizada y avanzada de las imágenes de copia de seguridad junto con la verificación en vuelo garantizan imágenes de copia de seguridad fiables.
- **Recuperación instantánea**
  Arranque rápidamente las imágenes de copia de seguridad como máquinas virtuales utilizando la tecnología patentada VirtualBoot, y recupere archivos y carpetas en segundos y sistemas completos en minutos.
- **Recuperación flexible**
  Recupere en entornos virtuales o de hardware diferentes, incluso realizando una restauración de metal desnudo.
- **Simplicidad de gestión**
  Un único flujo de trabajo de gestión para el ciclo de vida de la protección de datos y la recuperación ante desastres
- **Recuperación de desastres como servicio**
  La estrecha integración con los servicios en la nube ofrece una completa recuperación y protección ante desastres en una nube creada a tal efecto, con la capacidad de ejecutar una conmutación por error con un solo clic.

Backup | Entorno Virtualizado - Arcserve ShadowProtect

arcserve®

Las copias de seguridad continuas basadas en imágenes permiten una recuperación de desastres rápida, sencilla y fiable en entornos pequeños

Al igual que las catástrofes, los entornos de TI son cualquier cosa menos estándar. Por eso las empresas necesitan una única solución multiplataforma que proteja un entorno mixto e híbrido. El software de copia de seguridad y recuperación ante desastres ShadowProtect® garantiza que los sistemas y datos empresariales on-prem estén totalmente protegidos y siempre disponibles.



Características principales

- Protección de sistemas multiplataforma
  Proteja los sistemas Windows y Linux, ya sean físicos o virtuales, con una única solución de software de copia de seguridad.

- Almacenamiento agnóstico
  ShadowProtect es compatible con casi cualquier tipo de almacenamiento basado en disco, incluido OneXafe. Utilice la combinación de almacenamiento de producción y de copia de seguridad que mejor se adapte a sus necesidades, ahora o en el futuro.

- Amplia compatibilidad con hipervisores
  Utilice nuestra solución con VMware ESX/ESXi, Microsoft Hyper-V, Red Hat Enterprise Virtualization y muchos otros hipervisores.

- Programación
  Realice copias de seguridad con regularidad, incluso mientras la gente trabaja (ni siquiera se darán cuenta), y nunca se arriesgará a perder más de unos minutos de datos, ofreciendo excelentes RPO.

- Replicación
  Disponer de copias de seguridad remotas le da flexibilidad y opciones durante un desastre. Replique las copias de seguridad en cualquier lugar: un dispositivo local, un servidor remoto, una instalación de coubicación, una nube de terceros, una nube privada o la nube de Arcserve.

¿Por qué deberías disponer de un Backup para Office 365?

Office 365 es una herramienta muy eficaz que además se adapta a cualquier situación y momento que requieras.

Y a pesar de ser segura contra amenazas esta no está totalmente protegida ante las mismas. Una brecha o pérdida de su información podría tardar meses en ser localizada poniendo bajo compromiso la privacidad de tu empresa.

Cientos de profesionales de TI en todo el mundo que migraron a Office 365, describen estas seis vulnerabilidades:

Office 365

Borrado de datos accidental
Office 365 no dispone de un Backup de los archivos y datos en One Drive de un usuario si este es eliminado. Esta pérdida de información replicaría en todos los demás integrantes de la red.

Amenazas de seguridad externas
Las amenazas externas pueden colarse a través de correos electrónicos y archivos adjuntos dentro de tu empresa. Una copia periódica de tus datos te ayudará a recuperar archivos de forma sencilla y rápida que podrían haberse infectado.

Requerimientos legales
En ocasiones necesitas recuperar archivos o correos electrónicos por métodos legales. El Backup en Office 365 te permitirá evitar potenciales disputas legales o multas.

Políticas de retención
El ritmo frenético de las empresas actuales hace que las políticas estén en constante cambio y evolución. Esto incluye las de retención. Office 365 ofrece políticas limitadas de retención que solo podrían ser de ayuda en situaciones muy ocasionales y no ofrecen una solución de respaldo integral.

Amenazas de seguridad internas
Un empleado podría intencional o involutariamente eliminar o manipular archivos críticos de la compañía. Una solución en Backup te permitirá tener estos archivos siempre a salvo.

Migraciones y correo electrónico híbrido
A veces por incompatibilidades o la gran cantidad de tiempo que se puede invertir en una migración de datos esta puede resultar solo parcial. Con el Backup en Office 365 podrás tener almacenados los datos allá donde lo precises.

Backup | Entorno Cloud - BOXAFE

¿En qué consiste?

La tendencia global del Software como servicio (SaaS, Software-as-a-Service) ha provocado un aumento continuado del gasto y la adopción de SaaS por parte de las empresas. A pesar de las comodidades del SaaS, sigue siendo una solución vulnerable a la pérdida de datos y las limitaciones de la recuperación de datos. Cuando se producen incidentes, el error humano puede provocar una enorme pérdida de datos, pero con la completa solución de copia de seguridad de G Suite Google™ y Microsoft 365® de QNAP Boxafe para empresas, puede tener una mayor tranquilidad.

¿Le preocupa que se produzca una pérdida de datos?

Los datos pueden tener un valor incalculable. Aunque los proveedores de la nube garanticen la protección de los datos, seguirá enfrentándose a las siguientes situaciones:

- Error humano y fallos que provocan el borrado de datos accidental.
- Destrucción de datos intencionada que provoca grandes pérdidas para las empresas.
- Aparte de los accidentes, las empresas deben realizar una conservación de los datos a largo plazo y aceptar el cumplimiento de una protección de los datos.

Boxafe protege los datos de la nube de las empresas

Con Boxafe, no tendrá que preocuparse por la pérdida de datos. Puede hacer una copia de seguridad archivos, correos electrónicos, calendarios y contactos de G Suite de Google™ y Microsoft 365® en el NAS de QNAP, lo que aporta múltiples beneficios:

Copia de seguridad de la nube con el NAS local
Haga una copia de seguridad de los datos de la nube en un NAS de QNAP local, lo cual puede proteger fácilmente los datos de su empresa.

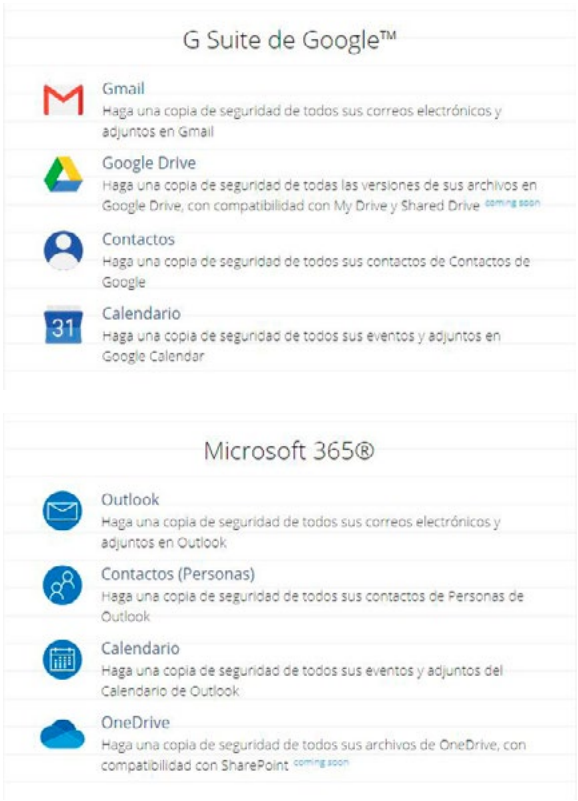
Seguridad
El NAS privado de alta seguridad evita que los datos sean vistos por terceros.

Centralización de los datos
Utilice Boxafe para hacer una copia de seguridad y administrar múltiples datos de G Suite y Microsoft 365®.

Fiabilidad
La programación de una copia de seguridad de múltiples versiones reduce el riesgo de pérdida de datos.

Boxafe: completa solución de copia de seguridad para empresas

Haga una copia de seguridad de los correos electrónicos, las unidades de la nube, los contactos y los calendarios de G Suite de Google™ y Microsoft 365® en un NAS local.



Copia de seguridad en un paso

Lo único que necesita es una configuración en un paso para hacer una copia de seguridad de cientos de miles de archivos de diferentes empleados. Boxafe ahorra tiempo y energía fácilmente.

Interfaz sencilla
La interfaz simple y fácil de usar, le permite ver rápidamente el estado de protección de Boxafe, el consumo de datos y proporciona un informe de tareas recientes en formato de calendario.

Administración flexible de la copia de seguridad
La copia de seguridad programada de múltiples versiones de Boxafe permite proteger todos los datos y reducir eficazmente el riesgo de una pérdida de datos.

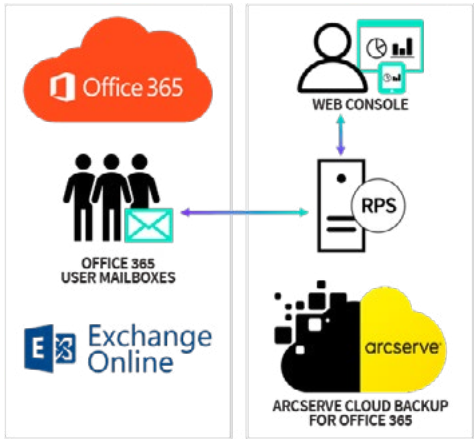
Vista previa de los datos
Puede previsualizar todos los datos de la copia de seguridad para evitar seleccionar los elementos equivocados.

Backup | Entorno Cloud
Arcserve Cloud backup para Office 365

arcserve®

Copia de seguridad de nube a nube con ciberseguridad de Sophos para datos en Microsoft Office 365

Arcserve Cloud Backup para Office 365 le da el control al garantizar que los datos se respalden de forma segura fuera del sitio en la nube, al mismo tiempo que los protege de los ataques cibernéticos con las tecnologías probadas de prevención de amenazas y antiransomware de Sophos.



Características principales

- Hacer copias de seguridad fácilmente mediante una simple configuración para elaborar sus estrategias de backup para buzones de Exchange Online y para sus datos de OneDrive y SharePoint Online.
- Restaurar datos de Office 365 Exchange Online y SharePoint trasladando fácilmente los datos nuevamente al servidor de Office 365 si se ha borrado la información, en forma accidental o no.
- Reforzar la seguridad y el cumplimiento con cifrado AES y control de accesos basado en roles.
- Neutralizar el malware, el ransomware y los exploits de manera efectiva, gracias a la integración total con Sophos Intercept X Advanced, la premiada solución de protección de endpoints a través de la inteligencia artificial (IA).
- Exportar datos de OneDrive migrándolos rápidamente desde Cloud Backup for Office 365 a un servidor de Office 365.
- Ahorrar hasta un 50 % del tiempo utilizando solo una IU para todas las tareas de seguridad y protección de datos de Office 365 y de otras cargas físicas, virtuales y en la nube.

¿Cómo funciona?

Arcserve Cloud Backup for Office 365 repica automáticamente sus buzones y datos de Office 365 directamente a Arcserve Cloud. La seguridad cibernética de Sophos Intercept X Advanced le protege de cualquier amenaza, incluyendo el ransomware y el malware, con una red neuronal de Deep Learning y la protección contra amenazas comunes basada en firmas.

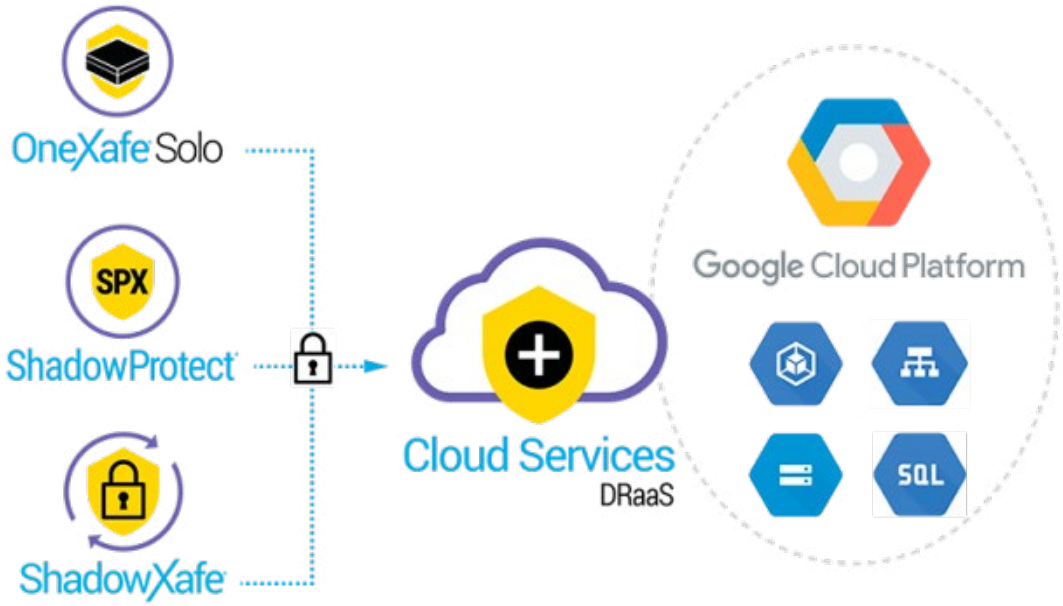
Usted administra todo el proceso desde una consola web intuitiva y específica de cuáles datos datos de Office 365 hay que realizar backup.

Backup | Entorno Cloud
Arcserve Services (DRaaS)

arcserve®

Nube de recuperación ante desastres como servicio (DRaaS) especialmente diseñada para la protección de las cargas de trabajo locales y la continuidad del negocio.

Cuando se combina con las soluciones de respaldo y recuperación de Arcserve, los servicios en la nube (DRaaS) garantizan una continuidad comercial completa y confiable. Está diseñado desde cero para agilizar la gestión de copias de seguridad y recuperación de datos, y para volver a poner en línea los sistemas críticos con rapidez y facilidad. Puede replicar imágenes de copia de seguridad de OneXafe®, ShadowXafe™, OneXafe Solo o ShadowProtect® en nuestros servicios en la nube (DRaaS), lo que le brinda las herramientas que necesita para mantener su negocio en funcionamiento sin importar lo que suceda.



Características principales

- Seguridad y Disponibilidad
  Sepa que los datos están seguros y siempre disponibles dentro de nuestra nube distribuida, escalable y tolerante a fallas creada específicamente para la recuperación ante desastres.
- Personalización
  Personalice el almacenamiento en la nube para que se ajuste a sus necesidades, ya sea que su entorno de TI sea pequeño y sencillo o grande y complejo. Elija el nivel de servicio según sus necesidades. Disfrute de costos bajos, control sobre la configuración de la nube y precios mensuales predecibles.
- Control y Flexibilidad
  Administre y controle de forma centralizada todas sus cuentas de Arcserve Cloud Services™, así como la conmutación por error en caso de desastre sin la intervención de terceros.
- Opciones avanzadas de recuperación de red
  Póngase en marcha después de un desastre con funciones de red avanzadas (disponibles con Cloud Premium) que le permiten ejecutar su red en nuestra nube tal como lo haría en el sitio.
- Conmutación por error con un clic
  Use la política de máquina virtual (disponible con Cloud Premium) para configurar la secuencia, el orden y el tiempo para cada sistema de misión crítica, y poder presionar solo un botón para probar o iniciar procesos de conmutación por error en todo el sitio.

Backup | Entorno Cloud
Cloud Hybrid

arcserve®

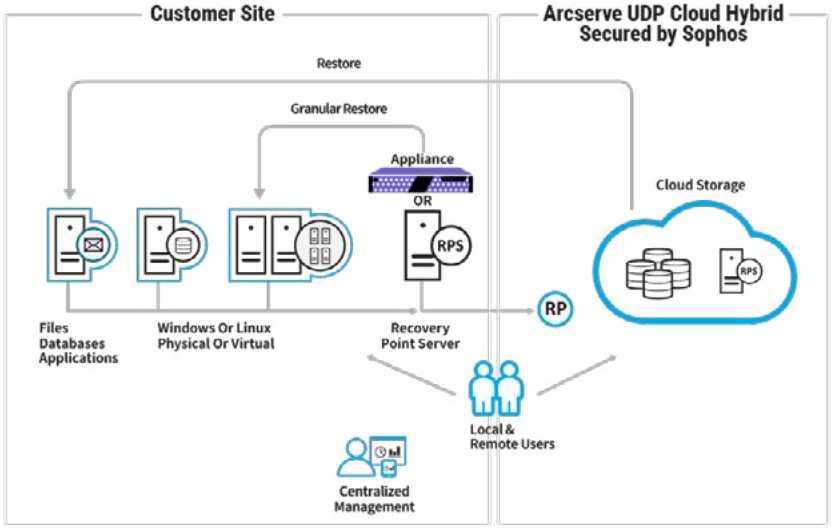
Copia de seguridad en la nube, ciberseguridad y extensión de recuperación ante desastres totalmente integradas para el software y los dispositivos de protección de datos

Arcserve Cloud Hybrid Secured by Sophos cumple con los requisitos de TI modernos al permitirle crear una estrategia cohesiva de seguridad, protección y retención de datos.

Implemente rápidamente copias de seguridad basadas en la nube y DR en nubes públicas y privadas, y protección del sistema de aprendizaje profundo para proteger las copias de seguridad de los ataques cibernéticos. Adáptese a los requisitos comerciales que cambian rápidamente mientras cumple con los estrictos RTO y RPO.

Características principales

- Admite máquinas en la nube, físicas y virtuales que ejecutan aplicaciones basadas en Windows y Linux
- Neutralice eficazmente el malware, los exploits y el ransomware con Sophos Intercept X Advanced, la galardonada protección para endpoints con inteligencia artificial totalmente integrada.
- Mantenga su empresa en funcionamiento con el modo de espera virtual remoto para conmutación por error y conmutación por recuperación de aplicaciones de emergencia, y conmutación por error desencadenada manualmente a recursos remotos
- Aumente su agilidad con copia de seguridad en la nube externa rentable y DR como alternativa a los discos o cintas locales
- Restaure archivos, carpetas y cargas de trabajo fácilmente cuando sea necesario
- Obtenga visibilidad completa desde una consola de usuario para realizar un seguimiento del uso de la nube, programar copias de seguridad y administrar la conmutación por error y la recuperación



¿Cómo funciona?

Usado junto con el software y los dispositivos de Arcserve UDP, Arcserve UDP Cloud Hybrid Secured by Sophos replica automáticamente sus datos o copias de seguridad desde un servidor de punto de recuperación (RPS) de Arcserve UDP local a un RPS correspondiente en la nube.

La ciberseguridad integrada de Sophos Intercept X Advanced protege las cargas de trabajo en la nube de cualquier amenaza con una red neuronal de aprendizaje profundo para malware conocido y desconocido, y protección basada en firmas contra amenazas comunes.

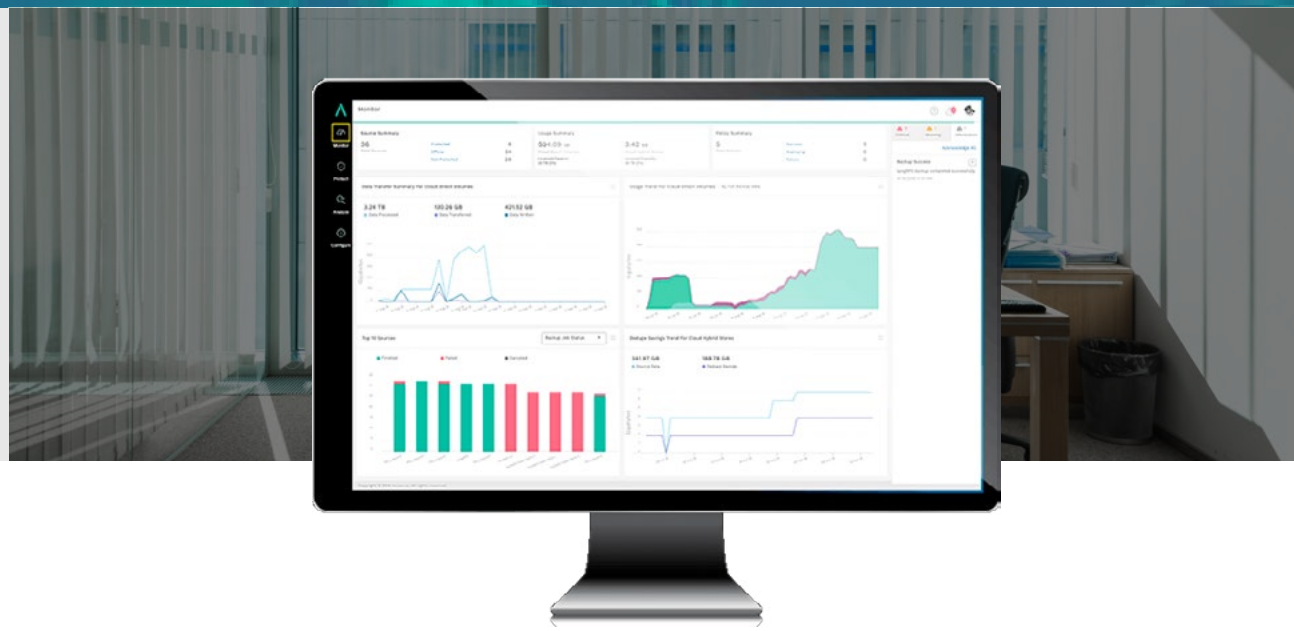
Gestiona todo el proceso de copia de seguridad desde la consola de UDP, especificando el origen, el destino y las políticas de retención de la copia de seguridad.

Backup | Entorno Cloud
Cloud de continuidad de la actividad de Arcserve

arcserve®

La interfaz de administración unificada basada en la web para Arcserve proporciona una experiencia de usuario perfecta desde la cual proteger todo el negocio

Arcserve Business Continuity Cloud desenreda el nudo de la TI del siglo XXI. Esta solución completa de continuidad del negocio y recuperación ante desastres alojada en la nube combina potentes tecnologías de respaldo, alta disponibilidad y archivado de correo electrónico para eliminar el tiempo de inactividad y la pérdida de datos en cualquier ubicación, desde sus aplicaciones y sistemas, en sus instalaciones y en sus nubes
Aumente su productividad y recupere hasta un 50 por ciento más de tiempo.
Elimine las brechas en su estrategia de continuidad comercial con una solución.
Proteja cada byte desde una consola de administración.



Características principales

- Evite el tiempo de inactividad y la pérdida de datos de infraestructuras de TI complejas y multigeneracionales con la única solución integrada de protección de datos de continuidad empresarial nativa de la nube, basada en la nube y lista para la nube.
- Pruebe y valide automáticamente su capacidad de recuperación y proporcione informes granulares a las partes interesadas clave en la protección de datos.
- Restaure inmediatamente el acceso a sistemas y aplicaciones críticos después de una interrupción o un desastre, incluidos los ataques de ransomware.
- Respalde el cumplimiento regulatorio y corporativo al simplificar el descubrimiento legal y las auditorías.
- Restaure SLA y respalde sus objetivos de tiempo y punto de recuperación (RTO/RPO), de segundos a horas.
- Mueva de forma segura grandes volúmenes de datos hacia y desde la nube sin agotar el ancho de banda.
- Escale fácilmente y pague a medida que crece sin agregar herramientas adicionales o interfaces de administración.

¿Cómo funciona?

Arcserve Business Continuity Cloud le brinda acceso a la gama más completa de tecnologías disponibles para satisfacer las necesidades de TI actuales y futuras. ¿Migrar cargas de trabajo a una nube pública o privada? Te tenemos cubierto. ¿Necesita protección de hipervisor avanzada? Está justo aquí. ¿Requiere soporte de RTO y RPO de menos de un minuto? Nosotros también apoyamos eso.

A diferencia de las herramientas puntuales que pueden proteger algunos de sus sistemas y aplicaciones, pero no todos, Arcserve ofrece tecnologías compatibles con todas las plataformas de TI, desde UNIX y x86 hasta nubes públicas y privadas. Se accede a potentes tecnologías a través de una única consola de administración basada en web, lo que le brinda una experiencia de usuario perfecta para proteger todo su negocio. No más alternar entre pantallas o administrar múltiples productos con diferentes SLA.

Reduzca su costo total de propiedad (TCO) y recupere hasta un 50 % más de tiempo administrando todos los procesos de protección de datos desde un solo lugar. Con la continuidad del negocio y la recuperación ante desastres, todo lo que necesita está aquí.

Backup | UDP - Arcserve UDP

arcserve®

Una plataforma con todas las capacidades de protección de datos que necesites, y nada que la complejidad.

El software Arcserve UDP ofrece una solución de protección de datos y ransomware todo en uno para neutralizar los ataques de ransomware, restaurar los datos y realizar una recuperación de desastres (DR) eficaz.

Protegido por la ciberseguridad Sophos Intercept X Advanced, Arcserve UDP combina de forma única la protección de servidores con aprendizaje profundo, el almacenamiento inmutable y la continuidad empresarial escalable in situ y fuera de las instalaciones para un enfoque multicapa que ofrece una resistencia informática completa para sus infraestructuras virtuales, físicas y en la nube.

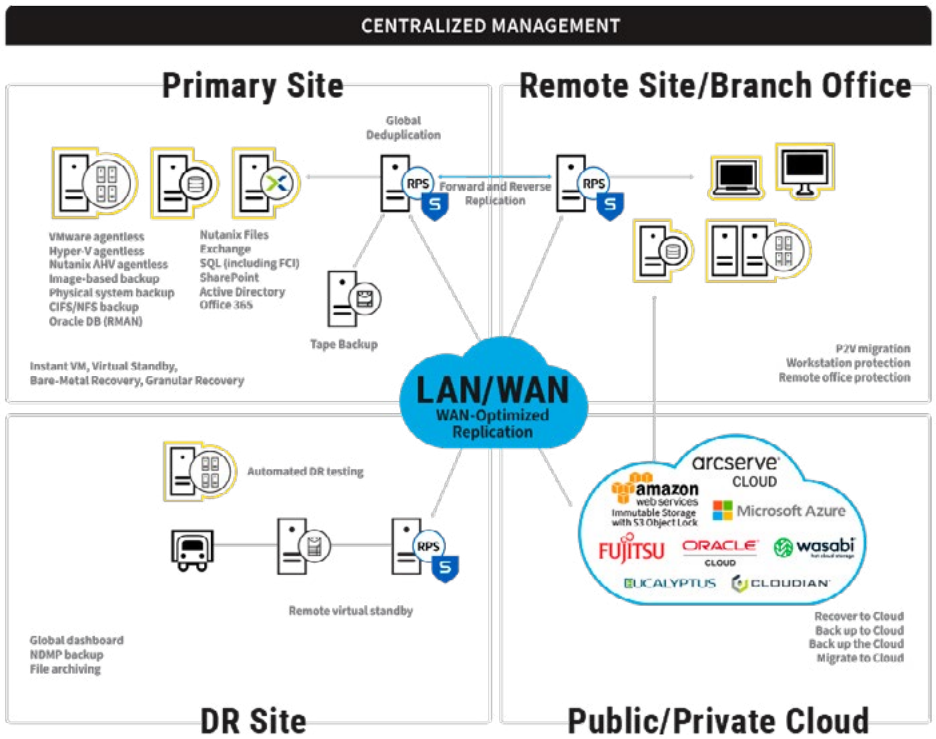
Características principales

- Proteja contra la pérdida de datos y la prolongación del tiempo de inactividad en las cargas de trabajo basadas en la nube, locales, virtuales, hiperconvergentes y SaaS, utilizando sólo una interfaz de gestión centralizada unificada.
- Reduzca el tiempo de inactividad de días a minutos, y valide los objetivos de tiempo y puntos de recuperación (RTOs/RPOs) y los acuerdos de nivel de servicio (SLAs) con pruebas automatizadas e informes granulares.
- Acelere la obtención de valor sin necesidad de una amplia formación ni de costosos servicios profesionales. Implante en minutos y recupere hasta un 50% más de tiempo.
- Evite los ataques de ransomware en infraestructuras críticas de recuperación de desastres con Sophos Intercept X Advanced for Server disponible. Asegure la inmutabilidad de las copias de seguridad de datos con la compatibilidad con Amazon AWS S3 Object Lock.
- Restauración más rápida gracias a la recuperación instantánea de máquinas virtuales y de metal desnudo (BMR), a la reserva virtual local y remota, a la copia de seguridad coherente con las aplicaciones y a la restauración granular, a la compatibilidad con instantáneas de hardware y a las extensiones que ofrecen alta disponibilidad y compatibilidad con cintas.

¿Cómo funciona?

Arcserve UDP 8.0 Secured by Sophos proporciona una TI libre de ransomware, permitiéndole proteger los datos críticos de los ciberataques; detectar y revertir el cifrado del ransomware; responder con un "no" a las demandas de rescate; y recuperar todos sus sistemas y datos de forma segura.

Escale fácilmente las topologías híbridas de continuidad de negocio, localmente o a larga distancia con múltiples sitios, incluyendo proveedores de servicios y de la nube. La instalación se realiza en unos pocos clics. Cree almacenes de datos en el servidor del punto de recuperación, añada los nodos que desea proteger, un destino de almacenamiento y un plan. Realice trabajos como la copia de seguridad, la espera virtual y la replicación.



Backup | UDP - Arcserve UDP Hybrid Secured by Sophos

arcserve®

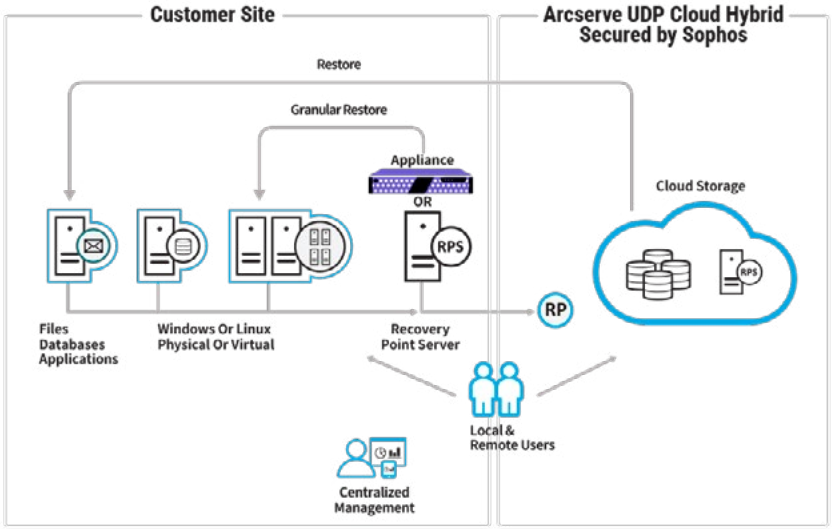
Copia de seguridad en la nube, ciberseguridad y extensión de recuperación ante desastres totalmente integradas para el software y los dispositivos de protección de datos

Arcserve Cloud Hybrid Secured by Sophos cumple con los requisitos de TI modernos al permitirle crear una estrategia cohesiva de seguridad, protección y retención de datos.

Implemente rápidamente copias de seguridad basadas en la nube y DR en nubes públicas y privadas, y protección del sistema de aprendizaje profundo para proteger las copias de seguridad de los ataques cibernéticos. Adáptese a los requisitos comerciales que cambian rápidamente mientras cumple con los estrictos RTO y RPO.

Características principales

- Admite máquinas en la nube, físicas y virtuales que ejecutan aplicaciones basadas en Windows y Linux
- Neutralice eficazmente el malware, los exploits y el ransomware con Sophos Intercept X Advanced, la galardonada protección para endpoints con inteligencia artificial totalmente integrada.
- Mantenga su empresa en funcionamiento con el modo de espera virtual remoto para conmutación por error y conmutación por recuperación de aplicaciones de emergencia, y conmutación por error desencadenada manualmente a recursos remotos
- Aumente su agilidad con copia de seguridad en la nube externa rentable y DR como alternativa a los discos o cintas locales
- Restaure archivos, carpetas y cargas de trabajo fácilmente cuando sea necesario
- Obtenga visibilidad completa desde una consola de usuario para realizar un seguimiento del uso de la nube, programar copias de seguridad y administrar la conmutación por error y la recuperación



¿Cómo funciona?

Usado junto con el software y los dispositivos de Arcserve UDP, Arcserve UDP Cloud Hybrid Secured by Sophos replica automáticamente sus datos o copias de seguridad desde un servidor de punto de recuperación (RPS) de Arcserve UDP local a un RPS correspondiente en la nube.

La ciberseguridad integrada de Sophos Intercept X Advanced protege las cargas de trabajo en la nube de cualquier amenaza con una red neuronal de aprendizaje profundo para malware conocido y desconocido, y protección basada en firmas contra amenazas comunes.

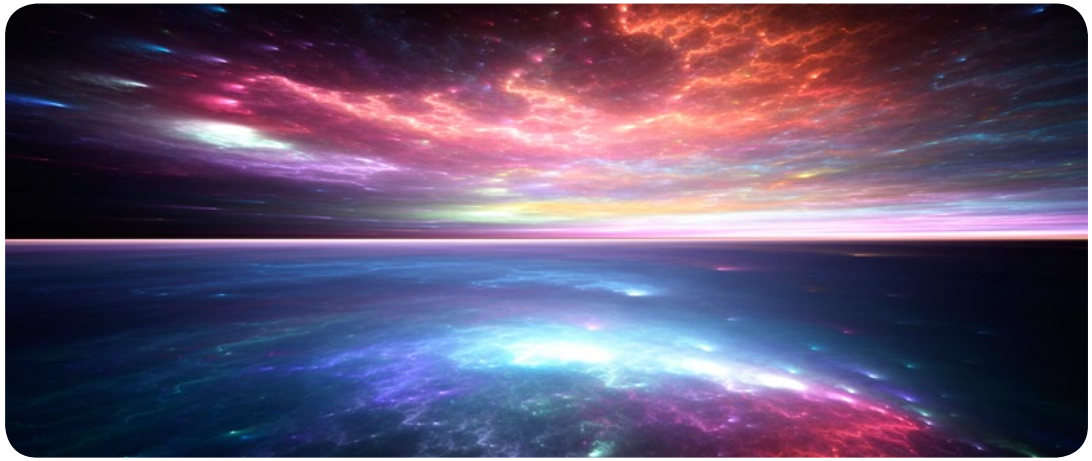
Gestiona todo el proceso de copia de seguridad desde la consola de UDP, especificando el origen, el destino y las políticas de retención de la copia de seguridad.

Backup | UDP - Arcserve UDP Cloud Direct

Copia de seguridad nativa en la nube y recuperación ante desastres sin necesidad de hardware local

Arcserve Cloud Direct ofrece una tercera y mejor opción. Administre fácilmente la copia de seguridad y la recuperación ante desastres y restaure los acuerdos de nivel de servicio (SLA) desde una interfaz de usuario hermosamente simple basada en la web. Proteja cualquier sistema y aplicación de la pérdida de datos y vuelva al negocio más rápido.

Específicamente diseñado para que las empresas funcionen sin problemas, el servicio en la nube de Arcserve proporciona una configuración sencilla y una gestión sencilla, enriquecido con velocidades de copia de seguridad líderes en la industria y una capacidad de recuperación del 100 %. Los entornos de TI grandes y distribuidos no son rival para la potencia, la escalabilidad y la flexibilidad que ofrece Arcserve Cloud Direct.



Características principales

- Configure y gestione todas las implementaciones de copia de seguridad con unos pocos clics y escale infinitamente sin necesidad de subsistemas de almacenamiento o dispositivos de mayor capacidad.
- Asegúrese de que nada se pase por alto accidentalmente capturando todos los datos en sus servidores con copias de seguridad de imágenes. Si está en el servidor, está en la imagen del servidor.
- Minimice el consumo de recursos del sistema con detección avanzada de cambios y transporte multihilo
- Transfiera automáticamente grandes conjuntos de datos de forma segura fuera del sitio con poca o ninguna necesidad de supervisión humana regular
- Elimine el impacto del ransomware con escaneos continuos de vulnerabilidades de terceros, cifrado SSL y otros controles técnicos. Retroceda en el tiempo a múltiples puntos de recuperación y restaure sin errores en minutos

¿Cómo funciona?

Arcserve Cloud Direct instala un agente ligero en sus servidores locales y replica los datos en su formato de archivo nativo para crear una copia de seguridad completa de la imagen del servidor, incluidos el sistema operativo, los archivos, los directorios y las aplicaciones. Los datos se transfieren directamente a través de Internet a Arcserve Cloud, sin necesidad de un dispositivo o una unidad de ensayo local. Después de una copia de seguridad completa inicial, solo se envían los datos modificados.

Sus datos y múltiples inquilinos se administran fácilmente en cualquier momento y en cualquier lugar con una visibilidad completa de la actividad a través de una consola de administración de autoservicio centralizada. Cuando sea necesario restaurar los datos, simplemente elija entre múltiples puntos de recuperación de imágenes del servidor para recuperar un servidor en Arcserve Cloud como una máquina virtual.

Aproveche el punto a sitio para conectarse de forma segura al entorno recuperado en Arcserve Cloud.

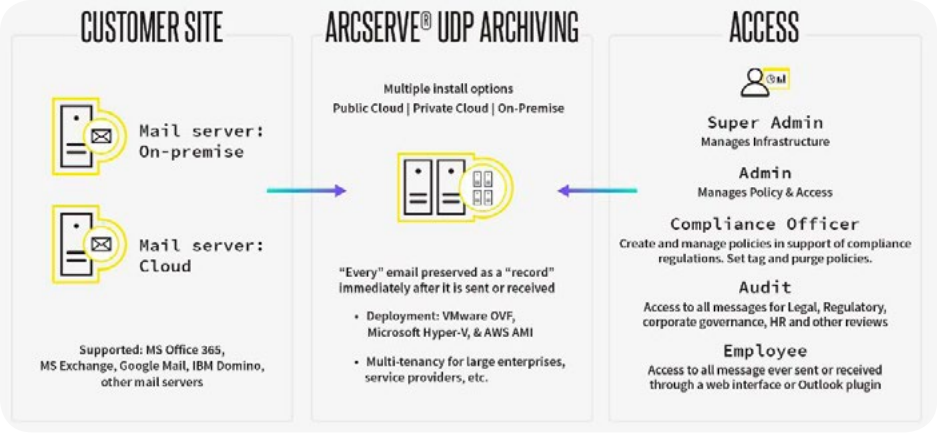
Backup | UDP - Archivo en el cloud de UDP de Arcserve

arcserve®

Conserva tus registros de correos electrónicos locales o en el cloud reduciendo gastos y ganando tiempo.

El Archivo de UDP de Arcserve hace posible la gestión moderna del archivado de correos electrónicos equipándote con las capacidades necesarias para cumplir con los requisitos legales mientras se evitan los costes y el engorro de las soluciones de archivo de toda la vida.

Optimiza el almacenamiento y aumenta el rendimiento guardando correos electrónicos archivados en el cloud segura de Arcserve: un lugar independiente del sistema de correo primario. Olvídate de acumular empleados protegiendo buzones de correos ilimitados y pagando únicamente por el almacenamiento que utilices. Una única solución para el control de la administración de correos electrónicos: no se necesitan hardware ni almacenamiento locales.



Características principales

- Captura y conserva correos electrónicos de manera automática como registros corporativos cifrados e inalterables desde el momento en que se envían y reciben.
- Simplifica la gestión del ciclo de vida eliminando automáticamente registros de correos electrónicos cuando hayan expirado los períodos de retención.
- Acceder a capacidades específicas para adecuarse al cumplimiento del reglamento general de protección de datos (RGPD) de la Unión Europea (UE).
- Busca, recupera y exporta correos electrónicos de forma rápida y precisa en interés de descubrimientos legales y auditorías de conformidad.
- Aplica retenciones legales fácilmente y consigue que no se destruyan los correos electrónicos con información sensible para eliminarlos de manera justificable.

¿Cómo funciona?

El Archivo en el cloud de UDP de Arcserve no necesita ser instalado. Como servicio basado en SaaS y disponible en el cloud seguro de Arcserve, su configuración es sencilla y ofrece la transferencia rápida de correos electrónicos actuales e históricos habilitados por una integración basada en API con tu Exchange u Office 365 Exchange Online locales.

Aplica políticas corporativas eligiendo los mensajes que se conservarán o excluirán (según el remitente, el receptor o la palabra clave), fija programas de conservación y aplica retenciones por razones legales y políticas de eliminación.

El control del acceso seguro se determina por función: Los superadministrador y administradores gestionan las políticas pero no pueden ver los correos electrónicos, en cambio, los auditores pueden verlos y los empleados solo pueden hacerlo a través de sus cuentas de Outlook, web o móviles.

Los administradores y los usuarios autorizados pueden realizar búsquedas pormenorizadas en todos los datos de los correos, exportar datos de búsqueda y aplicar solicitudes de retenciones por razones legales. Es posible extraer datos del archivo y cargarlos de nuevo en el sistema de correo primario para evitar pérdidas y borrados de datos.

Backup | UDP - Archivo de UDP de Arcserve

arcserve®

Protege tus registros vitales de correos y simplifica el cumplimiento a nivel local, en el cloud público o privado.

El Archivo de UDP de Arcserve se ha diseñado para facilitar la gestión moderna del archivado de correos electrónicos equipándote con las capacidades necesarias para cumplir con los requisitos legales y normativos mientras se evitan los costes y el engorro de las soluciones de archivado de toda la vida.

Optimiza el almacenamiento y aumenta el rendimiento de plataformas guardando correos electrónicos archivados en un lugar independiente del sistema de correo principal. Olvídate de acumular empleados protegiendo buzones de correos ilimitados y pagando únicamente por el almacenamiento que utilices. Simplifícate la vida con una única solución para el control de la administración de correos electrónicos.

Características principales

- Captura y conserva correos electrónicos de manera automática como registros corporativos cifrados e inalterables desde el momento en que se envían y reciben.
- Busca, recupera y exporta correos electrónicos de forma rápida y precisa en interés de descubrimientos legales y auditorías de conformidad.
- Simplifica la gestión del ciclo de vida eliminando automáticamente registros de correos electrónicos cuando hayan expirado los períodos de retención.
- Aplica retenciones legales fácilmente y consigue que no se destruyan los correos electrónicos con información sensible para eliminarlos de manera justificable.
- Acceder a capacidades específicas para adecuarse al cumplimiento del reglamento general de protección de datos (RGPD) de la Unión Europea (UE).

¿Cómo funciona?

El Archivo de UDP de Arcserve, diseñado para arquitecturas de una o múltiples empresas, permite la gestión moderna del archivado de correos electrónicos en numerosas divisiones, localizaciones o usuarios finales con plataformas locales o en el cloud como Microsoft Exchange, IBM Domino, Microsoft Office 365 y Google Gmail. No instala ningún software en el servidor del correo electrónico, sino que ejecuta una aplicación virtual ofrecida como VMware OVF, Microsoft Hyper-V y Amazon Web Services AMI.

Puede introducirse a nivel local o en el cloud público o privado, y emplea un almacenamiento de instancia única (SIS) para reducir el almacenamiento de archivo. Los mensajes con el mismo ID de mensaje se guardan una sola vez.

En el caso de Office 365, se reciben correos electrónicos de diario desde Exchange Online y se cifran y guardan en el almacén de datos del Archivo de UDP de Arcserve.

Las políticas corporativas se aplican eligiendo los mensajes que se conservarán o excluirán (según el remitente, el receptor o la palabra clave), fijando programas de conservación y aplicando retenciones por razones legales y políticas de eliminación.

El control del acceso seguro se determina por función: Los superadministrador y administradores gestionan las políticas, pero no pueden ver los correos electrónicos, en cambio, los auditores pueden verlos, y los empleados solo pueden hacerlo a través de sus cuentas de Outlook, web o móviles.

Los administradores y los usuarios autorizados pueden realizar búsquedas pormenorizadas en todos los datos de los correos, exportar datos de búsqueda y aplicar solicitudes de retenciones por razones legales. Es posible extraer datos del archivo y cargarlos de nuevo en el sistema de correo primario para evitar pérdidas y borrados de datos.

Backup | Snapshots

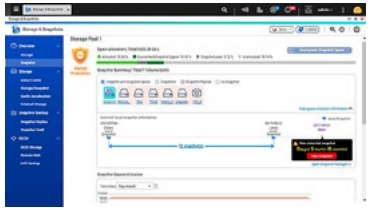
Instantáneas: una función estándar para todos los NAS de QNAP

Las instantáneas basadas en bloques de QNAP ofrecen una solución rápida y fácil de copia de seguridad y recuperación de los datos para protegerlos de cualquier pérdida accidental o posible ataque de malware. La restauración de todos los datos en un volumen que utilice instantáneas es hasta 10 veces más rápido que restaurar los datos copiándolos de una fuente de copia de seguridad. La protección mediante instantáneas está disponible tanto para NAS de QNAP basados en x86 como basados en ARM con al menos 1 GB de RAM.

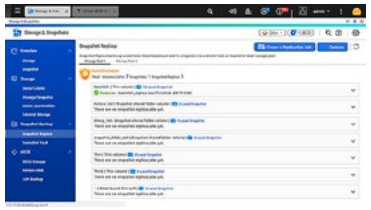
Características principales

- **Rápido.**
  Las instantáneas basadas en ext4 son más rápidas y más estables en el rendimiento de acceso a archivos.
- **Basado en bloques**
  El ransomware, a nivel de archivo, no puede acceder ni modificar nada si el volumen se ve afectado.
- **Copias de seguridad incrementales**
  Ahorra espacio de almacenamiento, ancho de banda y tiempo para realizar copias de seguridad y restaurar datos.
- **Restauración en un solo clic**
  La recuperación de datos mediante instantáneas solo tarda unos minutos.

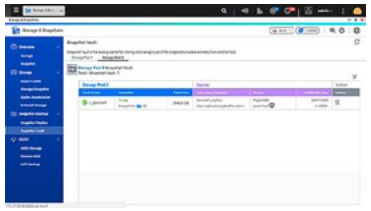
Potente Administrador de Almacenamiento e Instantáneas



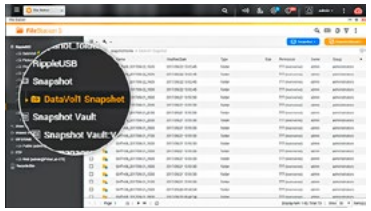
Visión general de instantáneas
Gestione sus instantáneas con una interfaz profesional y más detallada. Todas las versiones de las instantáneas y la hora de la última instantánea se registran con precisión.



Réplica de instantáneas
Visualice las tareas de copia de seguridad de instantáneas de un volumen/LUN, incluido el destino, la programación, la última hora de finalización/siguiente hora de inicio y la información sobre el progreso.



Almacenamiento de instantáneas
Almacene instantáneas de forma centralizada desde otro NAS.



Examinar el contenido de instantáneas
Examine todas las versiones de instantáneas e identifique los distintos contenidos utilizando el Directorio de instantáneas, File Station.

Sincronización de archivos entre dispositivos para optimizar el trabajo en equipo

Qsync permite una eficiente sincronización de archivos entre un NAS de QNAP y los dispositivos vinculados tales como ordenadores, portátiles y dispositivos móviles. Los usuarios profesionales pueden acceder a los archivos más recientes de la carpeta compartida en cualquier momento desde una amplia gama de dispositivos, lo que mejora en gran medida el trabajo en equipo y la colaboración. Los usuarios personales pueden acceder fácilmente a sus archivos multimedia desde dispositivos móviles para disfrutar de una experiencia multimedia completa y compartirla fácilmente con familiares y amigos.

Uso tanto en el entorno profesional como personal

Carpeta compartida de grupo para optimizar la eficacia del trabajo en equipo

Sincronización de archivos entre dispositivos para entretenimiento móvil multimedia

Principales ventajas

No hay gastos extras o limitaciones de espacio
Qsync es una parte integral de un NAS de QNAP y no requiere ninguna cuota extra o costes de suscripción. El espacio de almacenamiento está limitado sólo por la capacidad total del NAS.

Control total sobre sus datos
Ya que Qsync está en su NAS de QNAP, no tiene que enviarlo a través de terceros durante la sincronización de archivos. De esta manera usted mantiene el control de cómo se utiliza y se transmite su información.

Sincronización con todos sus dispositivos

Control de versiones. Todas las revisiones de archivos se guardan como una copia para su futura recuperación

Ahorra espacio en su dispositivo
Qsync le permite eliminar archivos de un dispositivo sin que ello afecte a las copias almacenadas en otros que están vinculados con el NAS. Sin embargo, cuando alguien actualiza los archivos borrados en otro dispositivo, aún puede descargarlos desde la carpeta Qsync.

Compartir carpetas de equipo con diferentes grupos de personas
Puede crear subcarpetas dentro de la carpeta Qsync, y compartir cada una de ellas con diferentes grupos de usuarios del NAS como un centro de intercambio de archivos. Todas las personas incluidas en la misma sub-carpeta están siempre al día con la última versión de los archivos.

Sincronizar carpetas compartidas

Aplicar la configuración a todos los dispositivos

Compartir archivos rápidamente con enlaces de descarga

Borrar a distancia la carpeta Qsync en caso de pérdida o robo

MSPs

MSPs | Soluciones para MSPs

Asóciese con WatchGuard – Simplemente es Más Fácil

Todo lo que hacemos comienza por hacer que el proceso sea fácil para nuestros socios y clientes y está respaldado por nuestros galardonados productos, servicios y Programa de Socios WatchGuardONE.

Características principales

- **Más Fácil de Vender**
  Una plataforma, un SKU y toda la seguridad. Nuestra plataforma Firebox proporciona un conjunto de eficaces servicios de seguridad de red y endpoints, junto con la inteligencia de correlación de máximo rendimiento del sector. Incluye opciones de precios flexibles, distribuidos y a petición.

- **Más Fácil de Implementar**
  Implemente y configure de modo remoto múltiples dispositivos Firebox®, sin necesidad de intervención y con asistencia mínima en el lugar usando RapidDeploy de WatchGuard.

- **Más Fácil de Administrar**
  WatchGuard System Manager, WatchGuard Dimension y la Nube Wifi de WatchGuard ofrecen controles intuitivos, generación de informes detallados y visibilidad completa de la red y seguridad de wifi de sus clientes.

- **Más Fácil para Hacer Negocios**
  Nuestro galardonado programa WatchGuardONE pone el poder en sus manos, ya que le ofrece todos los recursos técnicos, de ventas y de marketing que necesita, como también descuentos, rebajas y soporte las 24 horas del día.

- **Canales al 100 %; 100 % del Tiempo**
  WatchGuard siempre ha sido una organización enfocada en canales al 100 % y siempre lo será. Como su socio en términos de rentabilidad, le brindamos todo lo que necesita para una asociación exitosa.RapidDeploy2

Un Programa Flexible

El Programa de Socios de MSSP de WatchGuard, una clasificación dentro del más amplio y galardonado Programa de Socios de Canal WatchGuardONE, ofrece la flexibilidad y el soporte necesarios para crear un flujo de ingresos recurrente y predecible.

Opciones Flexibles de Pago

Comience de inmediato con pagos recurrentes y predecibles que eliminan los costos iniciales de un contrato anual. Además de nuestras opciones estándar de precios, puede usar puntos prepagos de MSSP de WatchGuard para asignar rápidamente servicios de seguridad a los dispositivos de seguridad de sus clientes.

Seguridad a Petición

Habilite o deshabilite servicios de seguridad al instante para cumplir con las necesidades cambiantes de sus clientes. Los puntos de MSSP no se vencen y se pueden distribuir en múltiples equipos y servicios, ya sea para uno o más clientes.

Recurso Integral

Acceda al Portal de Socios de WatchGuard para administrar las suscripciones a servicios de sus clientes, mantenerse actualizado con las noticias más recientes, descargar materiales personalizables de marketing, ver documentación técnica de autoayuda y mucho más.

Soporte Especializado

WatchGuard ofrece formación exhaustiva y soporte técnico las 24 horas del día, de modo que pueda convertirse en un especialista en seguridad. También ofrecemos facilidad de acceso a dispositivos no aptos para reventa (NFR). Adquirir conocimiento práctico de nuestros productos mediante la experiencia práctica y real es la mejor manera de conocer y adoptar las ventajas de WatchGuard.

MSPs | Soluciones para MSPs

Partners MSSP de WatchGuard.

Los clientes necesitan más que solo la instalación del hardware, el soporte técnico y la prevención de amenazas. Ya sean infraestructuras físicas o virtuales, o la cobertura de seguridad a través de redes, endpoints y entornos de Wi-Fi, los clientes necesitan seguridad total y tranquilidad con los servicios de seguridad proactivos y reactivos. Con WatchGuard, los proveedores de servicios de seguridad administrada (MSSP - Managed security service Providers) cuentan con un programa flexible, un portafolio de productos diversos y sólidos, y un ecosistema de integraciones tecnológicas que les permite a los MSSP mantenerse a la vanguardia en un mercado cada vez más creciente y competitivo.

Nuestra seguridad, entregada a su manera.

WatchGuard proporciona una cartera completa de soluciones de seguridad que habilita servicios de seguridad proactivos y reactivos con una administración simplificada, protección inteligente y visibilidad accionable.

Administración Simplificada

WatchGuard optimiza la administración de seguridad y maximiza la eficiencia con herramientas listas y fáciles de usar que satisfacen las necesidades empresariales críticas de los MSSP, como administración centralizada, arquitectura multiempresa y automatización en toda la red, los extremos y Wi-Fi.

- **Implemente seguridad rápida y fácilmente.**
- **Mantenimiento simplificado para todos los clientes.**
- **Mantenga actualizada la seguridad de sus clientes.**

Protección Inteligente

WatchGuard ofrece el portafolio más completo de servicios de seguridad, desde prevención de intrusiones tradicionales, Gateway Antivirus, control de aplicaciones, prevención de correo no deseado y filtrado de direcciones URL, hasta servicios más avanzados de protección contra malware de evolución, ransomware y brecha de datos. Además, WatchGuard ofrece capacidades de respuesta y corrección respaldadas por servicios de inteligencia ante amenazas internas y externas.

- **Prevenga amenazas malintencionadas**
- **Rápidamente detecte amenazas antes de que se produzca el daño**
- **Responda automáticamente a amenazas**

Visibilidad Accionable

WatchGuard brinda a los MSSP herramientas de visibilidad de datos y generación de informes que exclusivamente identifican y eliminan amenazas, problemas y tendencias de todos los clientes. Supervise, informe y solucione problemas fácil y rápidamente utilizando conocimientos aplicables en tiempo real, garantizando la seguridad, el rendimiento y el cumplimiento a sus clientes.

- **Supervisión accionable en tiempo real**
- **Libere a su equipo de informes que requieren mucho trabajo**
- **Resuelva los problemas de sus clientes de manera eficiente**

¿Cómo te ayuda Aryan?

Uno de nuestros principales objetivos añadir valor a cada una de las necesidades de nuestros partners. Desde la preventa, pasando por la formación, implementación y terminando por la postventa.

Watchguard - Puesta en marcha Firewall UTM
Aryan ofrece 2 pack de puesta marcha para implementación de equipos firewall UTM de Watchguard. Una pack "Básico" y otro "Avanzado". Con el objetivo de explotar todas las funcionalidades que ofrece la solución y obtener el máximo nivel de integridad para la infraestructura. En aquellas configuraciones que incluyan equipos ya instalados del mismo fabricante, se requiere que dichos equipos tengan los servicios de mantenimiento en vigor.

Servicios oficina segura en casa y visibilidad 360
Debido a la gran demanda que estamos teniendo de soluciones de movilidad mediante sistemas que permiten VPN, hemos diseñado y puesto a su disposición de nuestros partner, una serie de paquetes de servicios profesionales enfocados a cubrir y solucionar los problemas que se plantean debido a la situación de epidemia actual.

Watchguard - Puesta en marcha AuthPoint
Aryan ofrece a sus partner un servicio de implementación de una solución para garantizar la seguridad de acceso a los sistemas y redes, introduciendo un factor de doble autenticación de la mano de unos de nuestros fabricantes de seguridad Watchguard. El servicio permite securizar el login de nuestra sistemas operativos, como nuestras conexiones VPN, como cualquier tipo de dispositivo o aplicación que sea compatible con el protocolo de autenticación RADIUS.

Watchguard - Puesta en marcha TDR
Aryan ofrece a sus partner un servicio de despliegue para extender la seguridad de nuestros entornos desde el perimetro hacia los eslavones más debiles, los endpoint de cliente, los cuales son el factor de riesgo más importante que debemos potenciar a nivel de seguridad.

Instalación Bitdefender GravityZone
Con la instalación del fabricante Bitdefender, Aryan ofrece 2 packs de puesta en marcha, pack Básico y pack Avanzado.

Soporte Técnico - Bolsa de horas
Aryan pone a disposición de sus cliente un servicio de técnico enfocado a todas aquellas actividades que requieran de una cualificación y asistencia técnica para el desarrollo de instalaciones, despliegue de nuevas funcionalidades y resolución de incidencias.

Con ellas, tendrás a un acceso preferente a nuestro servicio técnico y garantizamos unas condiciones de servicio rápido y de calidad.

Consultoría
Servicio de asesoramiento profesional que ayuda a las organizaciones a alcanzar los objetivos y consecución de sus requisitos. En una llamada previa analizamos los requisitos expuestos, asesorando la mejor metodología para que nuestro cliente alcance sus objetivos otorgándole un valor diferencial.

Llave en mano
Servicio con el que nos involucramos desde las fases iniciales del proyecto, selección de la solución, diseño, planificación, implementación y mejora continua. Este tipo de servicios, incluyen integraciones a alto nivel e involucración en proyectos de gran complejidad para su negocio, consiguiendo la excelencia profesional en todos los aspectos.

Paquete de servicios - Workbox
Servicios empaquetados que se pueden desplegar en modalidad remota o in-situ y están diseñados para ayudar tanto a la implementación como a la formación de las soluciones más populares de nuestro catálogo. Este tipo de servicio se basa en la formación y configuración estándar sobre las soluciones contratadas.

Formación a medida
Servicio de formación a medida adaptado a las necesidades de nuestros clientes. Aporta un excelente punto de partida y se imparte de forma interactiva junto con el cliente.

Desde el departamento financiero ofrecemos un plan personalizado de financiación a nuestros clientes donde evaluamos además de las capacidades financieras de la compañía aquellas variables no computables, como son la operativa habitual, la antigüedad, el histórico de gestiones... entendemos que no limitándonos a una única variable conseguimos ofrecer a nuestros clientes una financiación más flexible. No dude en ponerse en contacto con nuestro Dpto. de Servicios Financieros

Solicitud de Renting

Si cliente desea una solución aplazada para sus operaciones, Aryan ofrece la posibilidad de realizar un estudio de renting: nuestro cliente sólo deberá enviarnos su oferta económica y en un plazo inferior a 24 horas podremos enviarles una cotización personalizada de acuerdo a sus necesidades.

Respuesta de cotización en un **plazo de 24** horas máximo.

Aryan te financia: Análisis interno e **individualizado** de todas las solicitudes

Proyectos superiores a 100K€ oferta a medida de las necesidades.

Pago mensual consulta nuestras opciones de pago mensual (perfecto para modelos de pago por uso)

Solicita ahora tu oferta de financiación

Pedidos Especiales

Aryan, en búsqueda de un mejor servicio, ofrece a sus clientes para operaciones de volumen un estudio individualizado dando diferentes alternativas de pago tales como pagos aplazados, cesiones de cobro, con el fin de facilitar sus gestiones y liberando parte de su tensión financiera.

Soluciones
Si necesitas ampliar la forma de pago para un pedido concreto, no dudes en contactar con nuestro Dpto de Servicios Financieros, seguro que encuentran la forma de ayudarte. ¡Estamos abiertos a tus propuestas!

Servicios Logísticos

Gracias a nuestro centro logístico de más de 5000m2 podemos ofrecer a todos nuetros clientes una gran variedad de soluciones logísticas para adaptarse a sus necesidades.

Usuario Final | **Pedidos Urgentes** | **Aviso Expedición** | **Seguro Mercancia**

Entregas directas a usuarios finales

Aryan le ofrece el servicio de envío directamente al usuario final. Damos la opción de albarán sin valor comercial.

Entrega Inmediata

En Aryan realizamos las entregas de material en 24 horas a cualquier punto de la Península Ibérica, desde nuestro Centro Logístico de Camarma de Esteruelas (Madrid). Cualquier pedido confirmado antes de las 17:00 h. se entregará en 24 horas, excepto Andorra, Ceuta, Melilla e Islas que el plazo será de 48 horas (ver anexo plazos de entrega).

Transporte General

Los envíos se realizarán a portes pagados y con las agencias de transporte contratadas por Aryan. Los portes se le incluirán en la factura a precios muy competitivos. Los envíos a portes pagados incluyen el seguro de la mercancía a todo riesgo (ver anexo seguro de mercancías).

Transporte Canarias

Los envíos a las Islas Canarias se pueden solicitar a través de dos agencia de transportes: DHL o Central Canarias; y serán a portes pagados incluidos en la factura con servicio puerta a puerta. En las tarifas esta incluido: recogida en nuestro almacén, transporte a las islas, despacho de exportación, entrega en casa del cliente y seguro a todo riesgo. El coste del despacho de aduana importanción y los impuestos IGIC son a cargo del cliente dando la opción de pagar Aryan y cargando como coste adicional en factura, dando la opción de incluir la factura de cliente en caso que vaya a cliente fina.

Servicio Aréreo
· Entrega 24 horas Islas Baleares (Central Canarias)
· Entrega 49 a 72 horas Islas Baleares (DHL)
· Entrega 48 a 72 horas Las Palmas y Tenerife. (Central Canarias)
· Entrega 72 a 96 horas al resto de las islas. (central Canarias)

Servicio Marítimo
Hay una única salida semanal, siendo el viernes. Los envíos se recogen el viernes antes de las 18:00 horas

· Días de tránsito Las Palmas: de 5 a 6 días naturales
· Días de tránsito Tenerife: de 7 a 13 días naturales
· Días de tránsito resto de islas: de 9 a 10 días naturales

Condiciones Generales

Es necesario enviar la Solicitud para la devolución del material, marcando la casilla de material averiado.

El nº de DOA tiene una validez de 15 días, transcurrido ese plazo se anulará. Debes enviar la mercancia con portes pagados. Aryan Comunicaciones le sustituirá el producto sin cargo alguno.

La devolución de cualquier producto debe tener su correspondiente número de DOA.

Recibirá su número de DOA en un plazo máximo de 24h o si se solicita a través de la web lo recibirá de inmediato (formulario).

El producto debe ir correctamente embalado, no escriba ni precinte la caja original del fabricante.

Todos los productos se testean, si no están defectuosos se devuelven a portes debidos.