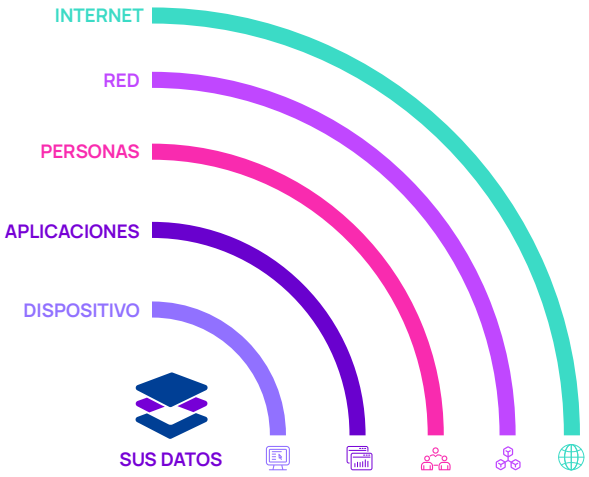
La seguridad por capas para departamentos de TI de N-able N-central

Solo N-able puede ofrecer un enfoque multicapa de seguridad, que proporciona un nivel de protección inigualable y la máxima sencillez. Todo ello integrado en un único panel. Además de sus funciones excepcionales, N-able aporta su experiencia en el sector, programas de formación y asistencia a empresas de primera clase que llevan la seguridad al siguiente nivel.



N-able aporta un increíble conjunto de nueve características de seguridad esenciales para hacer frente a todas las capas de la red, así como siete elementos de éxito para mejorar su negocio, su equipo y sus habilidades.

Características de seguridad esenciales

- Administración de parches
- Detección y respuesta en endpoints (EDR)
- Análisis de vulnerabilidades
- Seguridad del correo electrónico basada en la nube
- Administrador de seguridad y cifrado de disco
- Antivirus administrado
- Administración de contraseñas
- Copia de seguridad
- Supervisión
- Seguridad web

Características de éxito

- Expertos del sector
- Éxito de clientes
- Soporte técnico de primera clase ininterrumpido
- Formación detallada
- Automation Cookbook
- Una comunidad activa
- Canales de comentarios sobre productos

Los datos son su recurso más importante y el elemento al que quieren acceder la mayoría de los cibercriminales. Al implementar la tecnología de seguridad en cada capa, puede crear varias líneas de defensa para proteger sus datos. Los atacantes intentan acceder a los datos por diferentes motivos. Puede que quieran destruirlos, cifrarlos o devolverlos a cambio de un rescate, o bien robarlos y revenderlos en la Dark Web. En cualquier caso, los datos son el objetivo.

Una estrategia multicapa de seguridad permite detener los ataques en el nivel más externo y alejado de los datos. Por ejemplo, mediante el bloqueo de un correo electrónico malicioso, se evita que un posible ataque de ransomware llegue a acceder a la red. Parar un ataque en este punto resulta más seguro que bloquearlo a nivel de dispositivo, donde ya puede haber comenzado a cifrar archivos.

A continuación, se ofrece una descripción general de las características de seguridad por capas de N-able, que protege los datos en diferentes niveles.

Detección y respuesta en endpoints (EDR)

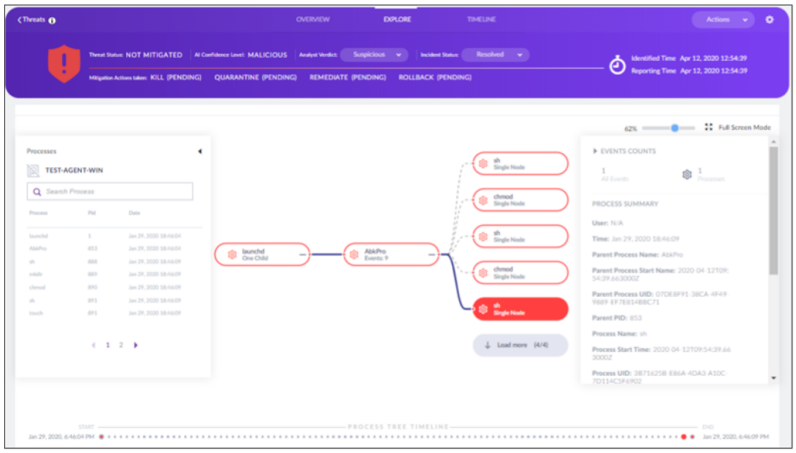
N-able™ Endpoint Detection and Response (EDR) ofrece a los técnicos de primera línea la capacidad de detectar los malwares más recientes (ransomware incluido), investigar las amenazas y corregir cualquier daño causado. Esto incluye la restauración de los endpoints a estados funcionales y finalizar la respuesta a un incidente de amenaza en minutos (y no horas).

EDR es un software de administración de amenazas que usa la tecnología SentinelOne. Al combinar N-central con la protección de endpoints de SentinelOne, la EDR permite a los dispositivos Windows defenderse y repararse de forma autónoma al detener procesos, establecer cuarentenas, realizar correcciones y revertir eventos para proteger los dispositivos.

La EDR usa comportamientos de procesos para supervisar varios procesos y reconocer los ataques a medida que se producen para responder a la máxima velocidad. Este enfoque es diferente al de la detección basada en firmas que utilizan las soluciones antivirus tradicionales, que supervisan los procesos a medida que se ejecutan en lugar de anticiparse a los problemas.

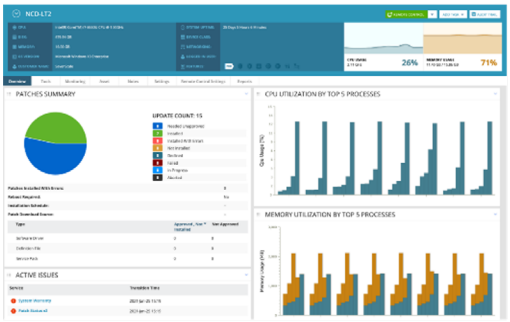
La EDR proporciona datos forenses que permiten mitigar las amenazas con rapidez, ejecutar acciones de aislamiento de la red y ofrecer protección frente a las amenazas recientemente detectadas.

Las nuevas características clave integradas en N-central incluyen la posibilidad de implementar agentes de EDR, la configuración de perfiles y la supervisión de dispositivos desde el panel.



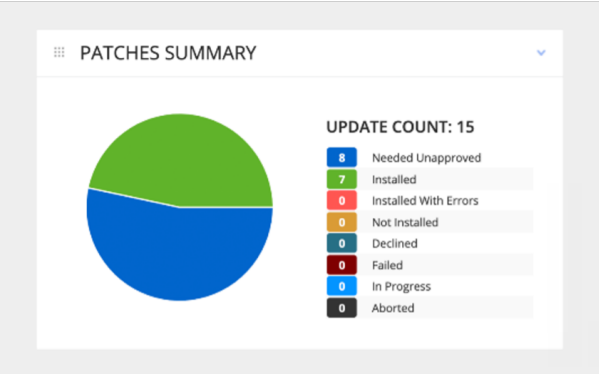
Administración de parches

La administración de parches ofrece a los administradores un control individualizado sobre cuándo, cómo y qué parches se despliegan en la red, los dispositivos o los grupos. La administración de parches a través de N-central® también permite proteger varios sistemas operativos y aplicaciones de terceros a la vez.



La administración de parches de N-able™ N-central ofrece a los administradores las herramientas que necesitan, entre las que se incluyen:

- Designar un concentrador de sitios (opcional)
- Habilitar y aplicar las políticas de administración de parches
- Políticas de administración de parches personalizadas
- Consulta de información detallada sobre el parche (incluyendo informes)
- Administración de parches en uno o varios dispositivos
- Reprocesamiento de los parches no aplicados
- Acciones de aprobación de parches
- Desinstalación de parches de Microsoft
- Programación de parches
- Aplicaciones compatibles
- Nueva ejecución manual de la comprobación del estado del parche
- Creación de un ciclo de vida de aprobación de parches y flujos de trabajo para su identificación

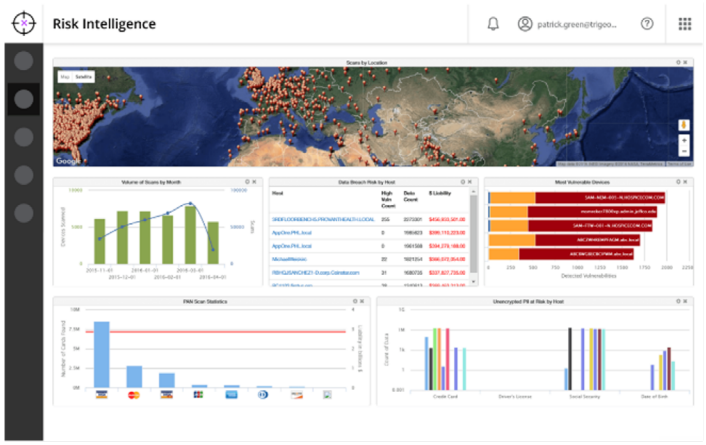


Esto no solo permite disponer de las mejoras de productividad necesarias para gestionar de forma efectiva la seguridad de las aplicaciones, sino que además ofrece herramientas de fácil uso para procesos de seguridad sofisticados sin que sea necesaria una formación especializada en este ámbito, lo que permite liberar recursos que pueden emplearse en la actividad principal de la empresa.

Análisis de vulnerabilidades e inteligencia de riesgos

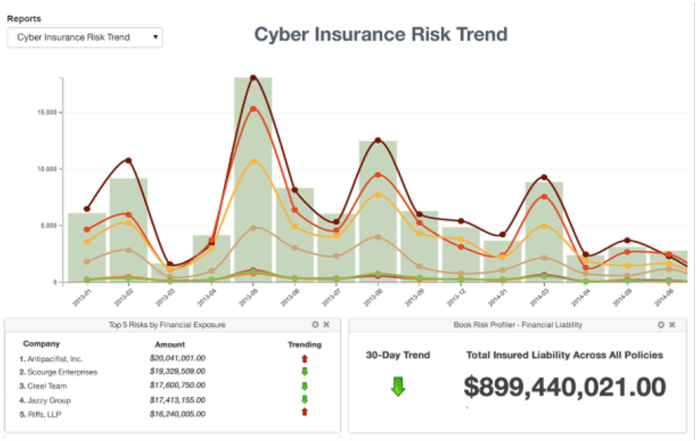
Diseñado para identificar posibles elementos mal configurados o puertos abiertos en la red, así como para ofrecer un historial de informes, estos elementos permiten de forma conjunta que los departamentos de TI puedan mostrar el progreso en materia de seguridad a lo largo del tiempo.

Aunque la plataforma N-central incluye redes de dispositivos, elaboración de informes rápida y detección y corrección de parches, las evaluaciones sobre cumplimiento y riesgos verdaderos son salvaguardas clave y adicionales que permiten cumplir los requisitos en materia de cumplimiento normativo.



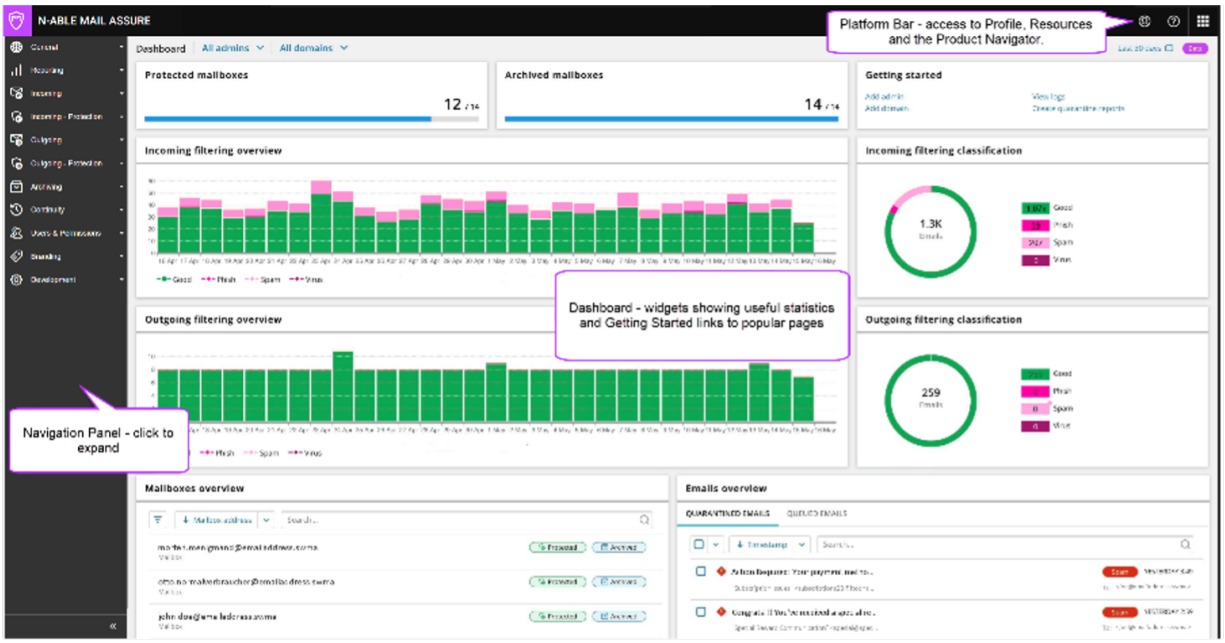
N-able™ Risk Intelligence localiza datos confidenciales y en riesgo dentro de sus estaciones de trabajo y redes administradas, y muestra a cuánto puede ascender el importe de una pérdida de datos, ofreciendo:

- Análisis profundo de vulnerabilidades
- Informes personalizables que detallan el impacto financiero de los riesgos
- Identificación de accesos de usuarios inadecuados
- PCI, DSS, PAN y análisis PII
- Descubrimiento de datos en riesgo
- Informes de tendencias de riesgos para mostrar las mejoras



El informe detallado sobre puertos de red muestra los puertos TCP/IP activos en el sistema, lo que indica que un servicio está a la escucha de una comunicación externa por parte de un equipo remoto. El informe detallado permite visualizar las amenazas con facilidad y en tiempo real.

Seguridad del correo electrónico basada en la nube



El correo electrónico sigue siendo importante. Incluso con una capa principal de seguridad, como sucede en Microsoft 365™, Mail Assure ofrece control añadido y un nivel adicional de protección diseñado frente al correo no deseado, los virus, el malware, el phishing, el ransomware y otras amenazas asociadas al correo electrónico, al mismo tiempo que protege los datos gracias al archivado basado en la nube.

La solución N-able™ Mail Assure ofrece diferentes características de seguridad del correo electrónico que protegen la capa más expuesta de la red:

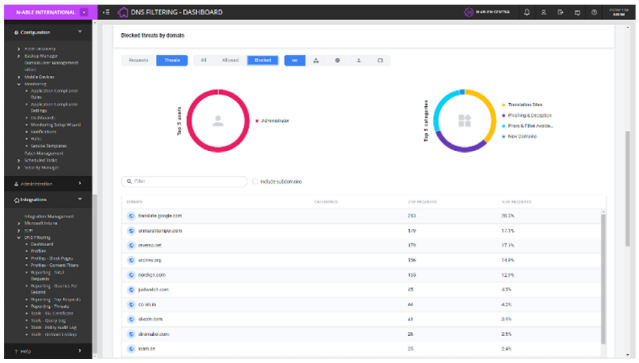
- Seguridad del correo electrónico de entrada y salida
- Protección inteligente y motor de filtrado que evita las amenazas conocidas y emergentes
- Configuración sencilla que le permite añadir dominios y modificar registros MX con facilidad
- Interfaz web para administradores y usuarios finales
- Administración de cuarentenas que ofrece a los usuarios la capacidad de examinar, liberar, eliminar, bloquear o aprobar contenido
- Detección automática de buzones de correo mediante SMTP o sincronización a través de LDAP
- Estadísticas avanzadas sobre filtrado
- Administración del bloqueo de extensiones y adjuntos
- Cifrado del tráfico SSL/TLS
- Implementación de host inteligente para el filtrado del correo electrónico de salida
- Firmas DKIM para los correos de salida, lo que contribuye a garantizar la autenticidad del remitente
- Continuidad del correo 24 horas al día, 7 días a la semana
- Acceso web a los correos electrónicos archivados y en cuarentena
- Posibilidad de envío y recepción del correo electrónico directamente desde el panel de Mail Assure

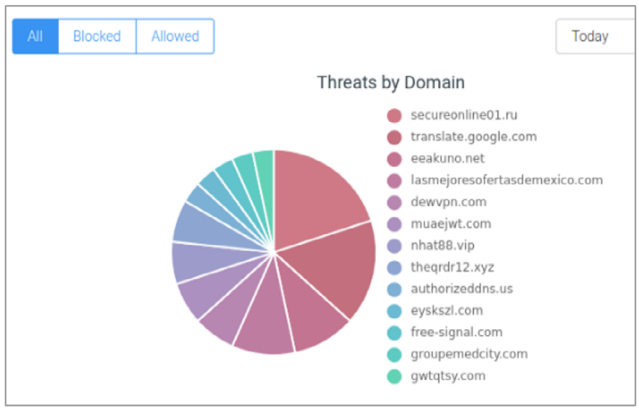
Seguridad web

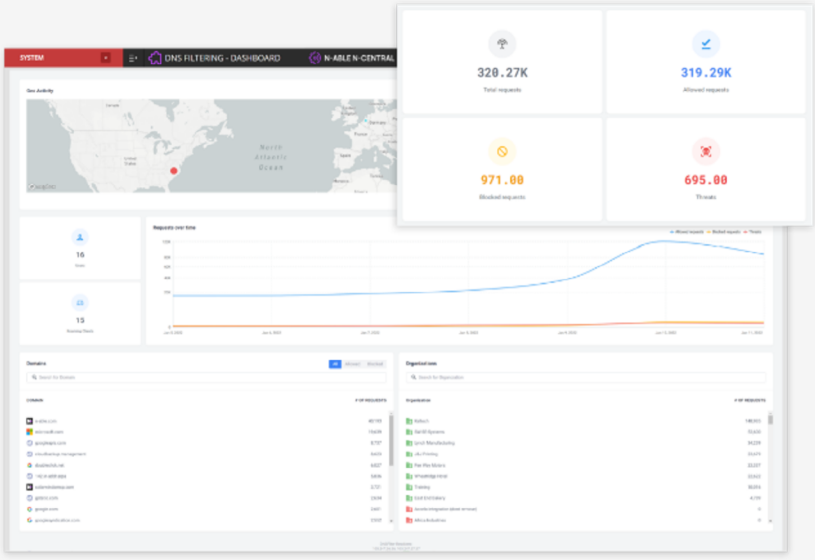
La seguridad web es esencial para garantizar la seguridad de cualquier empresa, sobre todo con la evolución de la fuerza de trabajo móvil. Las bases de datos web y el filtrado basado en DNS mantienen a las empresas, el personal y sus datos a salvo, tanto dentro como fuera de la red.

Cada día se crean miles de sitios web peligrosos. La publicidad maliciosa, el phishing y otras amenazas de seguridad pueden burlar el filtrado de contenido heredado. N-able™ DNS Filtering le ofrece una protección más sólida, mayor visibilidad sobre la red y capacidad de elaboración de informes basados en los usuarios a través del panel de N-central®.

Además, el producto N-able usa protección frente a amenazas inteligente para detectar y bloquear los sitios web maliciosos en tiempo real antes de que puedan afectar a sus clientes y usuarios. Protéjalos, en línea y fuera de la red, con la solución DNS Filtering. Está completamente basado en la nube, lo que permite una escalabilidad ágil y una mayor tranquilidad.

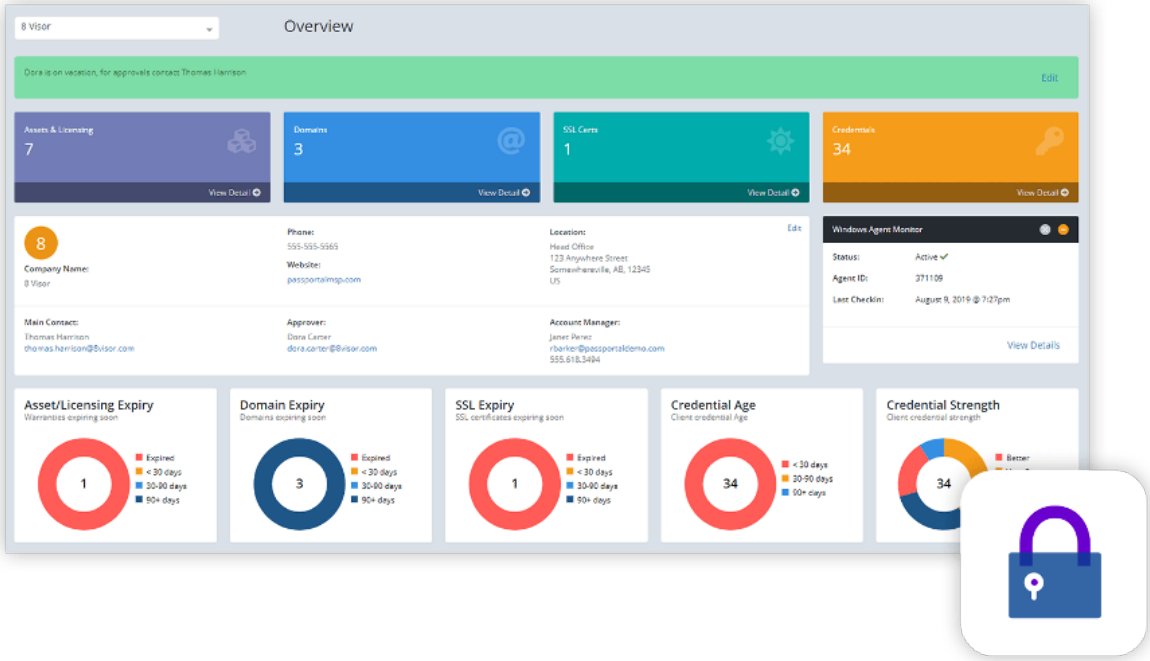




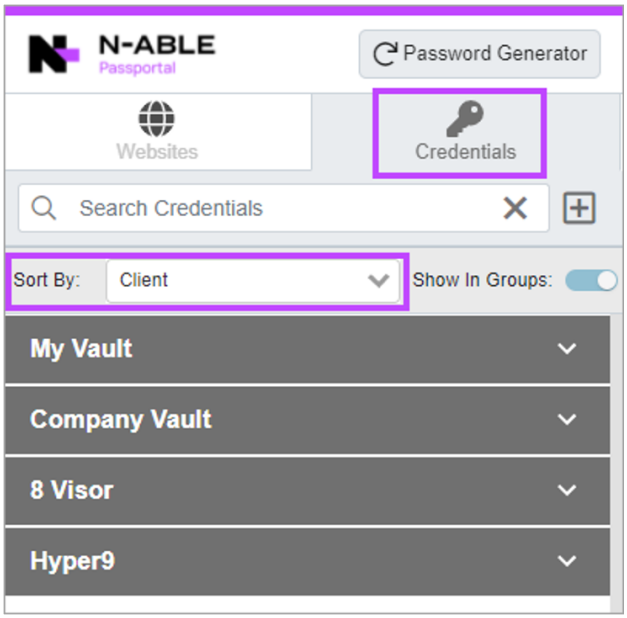


- Evite el acceso a los contenidos no deseados y maliciosos
- Bloquee los ataques de phishing, los virus, los ataques de día cero y otras ciberamenazas
- Identificación inteligente de dominios maliciosos, con una velocidad hasta 80 horas más rápida que muchas otras soluciones
- Red de difusión por proximidad fiable y altamente redundante: 50 centros de datos
- Informes completos por ubicación o usuario
- Visualice la actividad de red, el tráfico de red y la seguridad
- Exponga las debilidades en materia de seguridad mediante los registros de actividad DNS
- Cree directivas por grupo, dispositivo o red
- Redirija a los usuarios a una página bloqueada personalizada
- Bloquee amenazas de phishing no clasificadas previamente con tácticas antiphishing basadas en imágenes
- Mitigue las amenazas asociadas a botnets, el criptominado malicioso y el malware mediante el incremento de hilos de amenazas

Administración de contraseñas

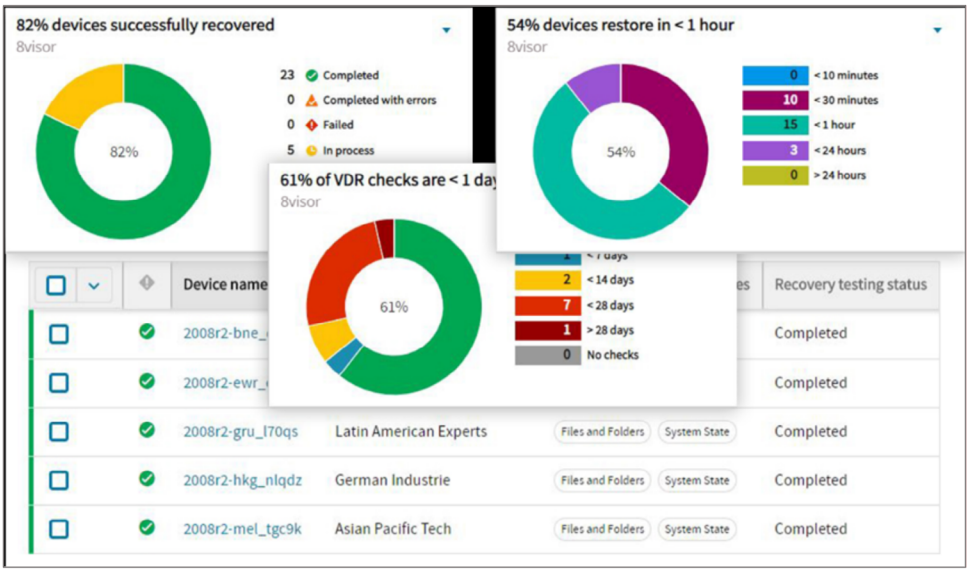


La administración de contraseñas permite a los directores de TI implementar reglas para generar contraseñas sólidas, eliminar la reutilización y automatizar la rotación de contraseñas y el mantenimiento de rutina. Cifre, almacene, administre y recupere credenciales de forma rápida y segura, al mismo tiempo que minimiza los riesgos asociados a las contraseñas.



N-able™ Passportal es una plataforma basada en la nube que ofrece administración de documentación y contraseñas sencilla y segura, adaptada a sus operaciones. Passportal usa protección de contraseñas automatizada que permite que el almacenamiento, la administración y la recuperación de las contraseñas y de los conocimientos del departamento sea un proceso rápido y sencillo desde prácticamente cualquier dispositivo conectado. Gracias a la inyección de credenciales que facilita una conectividad rápida, ágil y segura con los dispositivos, redes y aplicaciones de los usuarios, Passportal se ha diseñado para agilizar las operaciones del día a día de los técnicos. Por último, le permite adoptar y demostrar con facilidad los flujos de trabajo recomendados en materia de administración de contraseñas.

Copia de seguridad



Las empresas no solo requieren la arquitectura híbrida, segura y rápida necesaria para las soluciones para copias de seguridad modernas, sino también capacidades de almacenamiento múltiple y restauración que permitan la reducción de las posibilidades de que un ataque de ransomware tenga éxito a prácticamente cero.

Con N-able Backup, dispondrá de diferentes opciones de recuperación que le permitirán sacar partido a la recuperación rápida a nivel de archivo y carpeta, así como de sistema completo, gracias a la restauración completa o la recuperación de catástrofes virtual. Cree un servidor en suspensión con nuestra opción de recuperación continua y recupere a la velocidad que ofrece la LAN a través de la opción Local Speed Vault si lo necesita. Por último, pruebe y verifique la capacidad de recuperación de la copia de seguridad mediante un programa automatizado gracias al testeo de la recuperación.

N-able Backup incluye las siguientes características asociadas a nuestros centros de datos de primera clase disponibles en todo el mundo:

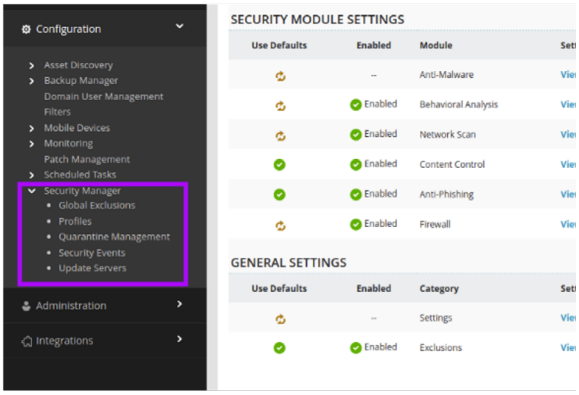
- Soporte técnico y copia de seguridad de Microsoft 365
- Sin requisitos de hardware
- Despliegue de copias de seguridad automatizadas (incluyendo perfiles)
- Cifrado AES de 265 bits
- Claves privadas personalizadas
- Centros de datos con certificación ISO
- Configuración de acceso en función del puesto
- Tecnología True Delta con seguimiento de los cambios a nivel de byte
- Deduplicación y compresión
- Optimización WAN

País	HIPAA	ISO27001	ISO9001	NIST 800-53	PCI DSS	SOC TIPO II	SOC 2 TIPO II
Alemania		x	x		x	x	x
Australia		x			x	x	x
Bélgica		x					
Brasil		x	x		x	x	x
Canadá	x	x		x	x	x	x
Dinamarca		x			x	x	x
EE. UU.	x	x		x	x	x	x
España		x	x		x		
Francia		x	x		x	x	x
Italia		x	x		x	x	x
Noruega		x	x				
Países Bajos		x	x		x	x	x
Portugal		x	x		x	x	x
Reino Unido		x	x		x	x	x
Sudáfrica			x				
Suecia		x	x				
Suiza		x	x		x	x	x

**Existen otras certificaciones específicas para cada ubicación. La tabla anterior incluye las más solicitadas.

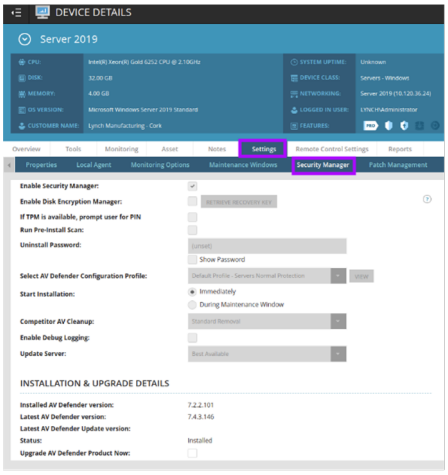
Administrador de seguridad con gestión de cifrado de disco

Para cumplir las necesidades de protección a nivel de dispositivo, hemos desarrollado una solución de administración de seguridad que se despliega y puede administrarse directamente desde el panel N-central. En el caso de las empresas que aún no requieran la EDR, esta solución puede adaptarse a sus necesidades específicas, con la opción de permitir interacciones con el usuario final como la ejecución de análisis y la actualización de las definiciones de amenazas. Asimismo, puede habilitar el cifrado de disco a nivel de volumen para que sus datos cuenten con un nivel adicional de protección.



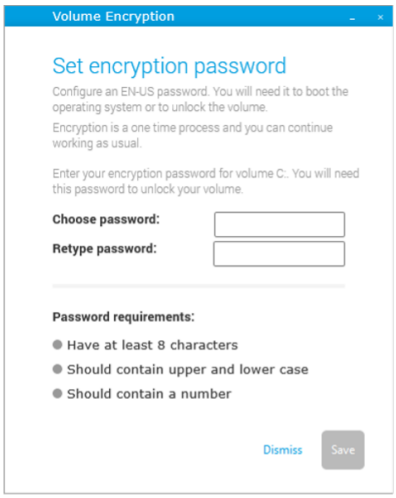
El cifrado de disco protege los datos frente al robo o la pérdida accidental al provocar que la información de los discos duros sea ilegible para los usuarios no autorizados. El cifrado de disco es la opción ideal para los entornos en los que los datos son un activo esencial o en los que se aplican normativas como el RGPD o la norma PCI DSS y en los que existe el riesgo de pérdida de datos.

Las políticas de protección de N-able controlan cada aspecto del administrador de seguridad. Esto incluye análisis programados, acciones de corrección tras la detección de amenazas e interacciones con el usuario final. Hemos incluido políticas predeterminadas para que pueda empezar a trabajar, así como la posibilidad de crear políticas personalizadas que cubran sus requisitos específicos.



Nuestro motor y nuestras políticas corren a cargo de Bitdefender, un líder del sector de la seguridad cuyas políticas están presentes en las instalaciones tanto de Windows como de Mac. Asimismo, se aplica automáticamente la configuración del administrador de seguridad compatible con el sistema operativo del equipo.

El cifrado de disco de N-able saca partido a la tecnología nativa BitLocker, por lo que puede aprovechar los cifrados existentes de los que ya disponga y beneficiarse de nuestro sistema de claves de recuperación fácil de gestionar. Nuestro administrador de cifrado ofrece varias opciones de seguridad (módulo de plataforma de confianza, contraseñas, etc.), lo que permite una personalización muy sencilla.

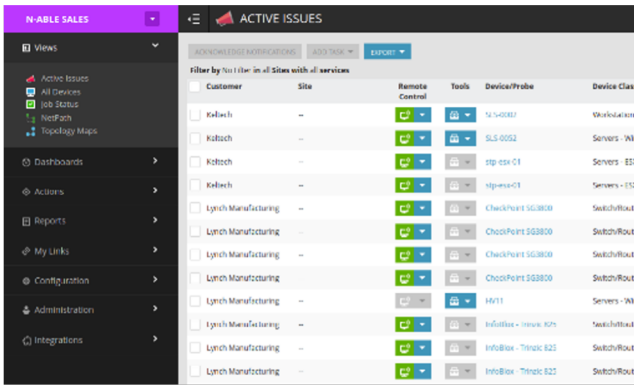


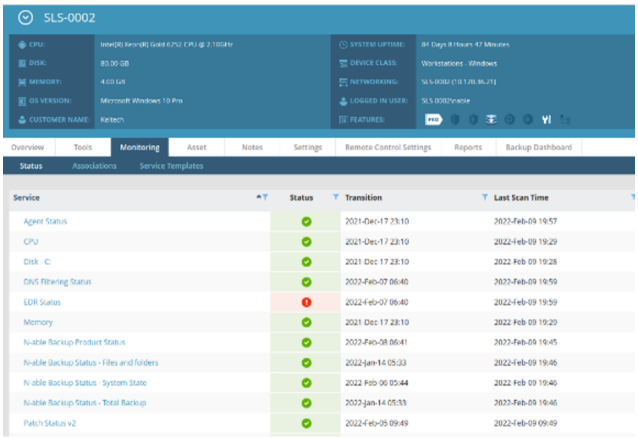
Supervisión de dispositivos

La supervisión ofrece a los técnicos de primera línea, los directores de TI y los especialistas en seguridad la información en tiempo real y las tendencias históricas para predecir y detectar las amenazas y ataques antes de que tengan la posibilidad de desplegarse. La supervisión permite visibilizar los posibles ataques y envía alertas instantáneas sobre tendencias anormales, algo que sirve como indicadores tempranos esenciales.

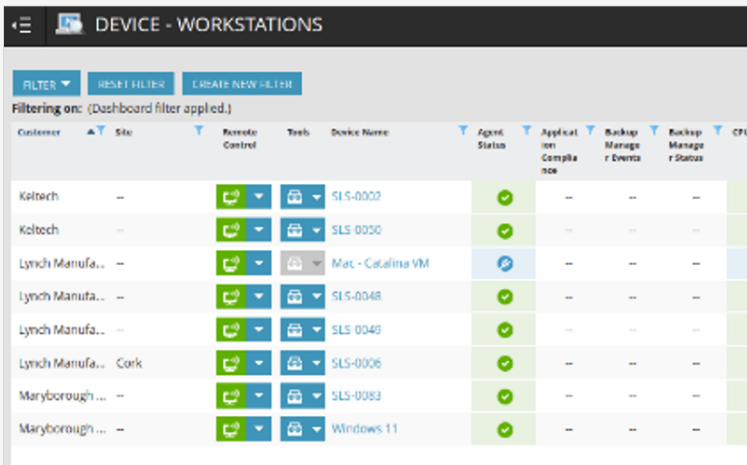
Los agentes de supervisión son software especializado que permiten mantener las estaciones de trabajo, los servidores y las redes actualizadas mediante un análisis continuo sin interrupciones. Alertan al equipo de soporte de TI sobre posibles problemas y contribuyen a mantener el software malicioso lejos de los sistemas supervisados. Estos agentes contribuyen a la seguridad y la fiabilidad, al mismo tiempo que realizan un seguimiento de las redes.

La supervisión de dispositivos de N-able le ofrece la máxima visibilidad para gestionar su seguridad correctamente. Le permite mantener sus redes protegidas, llevar a cabo mantenimiento proactivo y adelantarse a posibles amenazas.





- Reciba alertas sobre posibles incidencias
- Aplique parches y actualice software en sus dispositivos
- Programe tareas como la actualización y la ejecución del antivirus o realice copias de seguridad a diario
- Automatice el mantenimiento rutinario
- Compatibilidad con Windows, Mac y Linux
- Supervisión y administración de red avanzadas para servidores y estaciones de trabajo en diferentes ubicaciones del cliente
- Alertas sobre incidencias como estado de los discos, antivirus no actualizados y estado de servicios
- Perfiles de configuración que le permiten desplegar los agentes de forma conjunta o en grupos
- Protección de las conexiones y cifrado de las transferencias de datos mediante HTTPS
- Supervisión del rendimiento de la red
- Detección, importación y supervisión de los dispositivos de red esenciales mediante el uso de SNMP, lo que incluye cortafuegos, routers, impresoras y conmutadores
- Supervisión de dispositivos móviles
- Supervisión de máquinas virtuales



Elementos de la seguridad por capas

DETECCIÓN Y RESPUESTA EN ENDPOINTS (EDR)

Ofrece a los técnicos de primera línea la capacidad de detectar las amenazas de malware más recientes (ransomware incluido) y de investigar y reparar los daños causados. Esto incluye la restauración de los endpoints a estados funcionales y finalizar la respuesta a un incidente de amenaza en minutos (y no horas).

ADMINISTRACIÓN DE PARCHES

La administración de parches ofrece a los administradores un control individualizado sobre cuándo, cómo y qué parches se despliegan en la red, los dispositivos o los grupos. La administración de parches a través de N-central también permite proteger varios sistemas operativos y aplicaciones de terceros a la vez.

ANÁLISIS DE VULNERABILIDADES

Diseñado para identificar posibles elementos mal configurados o puertos abiertos en la red, así como para ofrecer un historial de informes. Estos elementos permiten de forma conjunta que los departamentos de TI puedan mostrar el progreso en materia de seguridad a lo largo del tiempo.

SEGURIDAD DEL CORREO ELECTRÓNICO BASADA EN LA NUBE

El correo electrónico sigue siendo importante. Incluso con una capa principal de seguridad, como sucede en Microsoft 365™, Mail Assure ofrece control añadido y un nivel adicional de protección diseñado frente al correo no deseado, los virus, el malware, el phishing, el ransomware y otras amenazas asociadas al correo electrónico, al mismo tiempo que protege los datos gracias al archivado basado en la nube.

SEGURIDAD WEB

La seguridad web es esencial para garantizar la seguridad de cualquier empresa, sobre todo con la evolución de la fuerza de trabajo móvil. Las bases de datos web y el filtrado basado en DNS mantienen a las empresas, el personal y sus datos a salvo, tanto dentro como fuera de la red.

ADMINISTRACIÓN DE CONTRASEÑAS

La administración de contraseñas permite a los directores de TI implementar reglas para generar contraseñas sólidas, eliminar la reutilización y automatizar la rotación de contraseñas y el mantenimiento de rutina. Cifre, almacene, administre y recupere credenciales de forma rápida y segura, al mismo tiempo que minimiza los riesgos asociados a las contraseñas.

COPIA DE SEGURIDAD

Las empresas no solo requieren la arquitectura híbrida, segura y rápida necesaria para las soluciones para copias de seguridad modernas, sino también capacidades de almacenamiento múltiple y restauración que permitan la reducción de las posibilidades de que un ataque de ransomware tenga éxito a prácticamente cero.

ADMINISTRADOR DE SEGURIDAD CON GESTIÓN DE CIFRADO DE DISCO

Para cumplir las necesidades de protección a nivel de dispositivo, hemos desarrollado una solución de antivirus administrado que se despliega y que puede administrarse directamente desde el panel. Asimismo, puede habilitar el cifrado de disco a nivel de volumen para que sus datos cuenten con un nivel adicional de protección.

SUPERVISIÓN DE DISPOSITIVOS

La supervisión ofrece a los técnicos de primera línea, los directores de TI y los especialistas en seguridad la información en tiempo real y las tendencias históricas para predecir y detectar las amenazas y ataques antes de que tengan la posibilidad de desplegarse. La supervisión permite visibilizar los posibles ataques y envía alertas instantáneas sobre tendencias anormales, algo que sirve como indicadores tempranos esenciales.