Comparativo de las soluciones y funcionalidades de Heimdal Security

TABLA DE CONTENIDO

¿Qué soluciones ofrece Heimdal Security?

1. Seguridad de endpoints (Endpoint Security)
2. Gestión de vulnerabilidades (Vulnerability Management)
3. Gestión de accesos privilegiados (Privileged Access Management)
4. Detección y respuesta ante amenazas (Threat Detection & Response)
5. Administración unificada de endpoints (Unified Endpoint Management)

Comparativo de las soluciones de Heimdal Security

¿Qué solución de Heimdal debería adquirir mi empresa?

¿Se pueden combinar diferentes soluciones de Heimdal?

Conclusión

Heimdal Security ofrece una plataforma de ciberseguridad que reúne diferentes herramientas para proteger los equipos, gestionar vulnerabilidades, controlar los accesos privilegiados y detectar posibles amenazas. Sus soluciones pueden implementarse de acuerdo con las necesidades de cada organización y combinarse para construir una estrategia de seguridad más completa.

En este artículo presentamos las principales soluciones de Heimdal Security disponibles en nuestro portafolio, sus funcionalidades y los escenarios en los que pueden resultar útiles para una empresa.

¿Qué soluciones ofrece Heimdal Security?

1. Seguridad de endpoints (Endpoint Security)

Esta categoría reúne soluciones orientadas a proteger los dispositivos de los usuarios frente a amenazas digitales, conexiones maliciosas y ataques que puedan comprometer la información de la

organización.

DNS Security – Endpoint

[Enlace pendiente: DNS Security – Endpoint]

Proporciona protección mediante el filtrado de solicitudes DNS directamente en los dispositivos. Permite bloquear conexiones hacia dominios asociados con actividades maliciosas, incluso cuando los equipos se encuentran fuera de la red corporativa.

¿Para quién es recomendable?

Empresas con empleados que trabajan de forma remota, equipos móviles o dispositivos que necesitan mantener una capa de protección independientemente de su ubicación.

Next-Gen Antivirus & Firewall

[Enlace pendiente: Next-Gen Antivirus & Firewall]

Combina capacidades de antivirus de nueva generación y firewall para proteger los endpoints frente a malware y otras amenazas. Su administración centralizada permite gestionar la protección de los dispositivos desde una consola.

¿Para quién es recomendable?

Organizaciones que necesitan una solución de protección para sus computadores y servidores, con administración centralizada de las políticas de seguridad.

Ransomware Encryption Protection (REP)

[Enlace pendiente: Ransomware Encryption Protection]

Está orientada a detectar y detener procesos de cifrado malicioso asociados con ataques de ransomware. Complementa las herramientas de protección de endpoints al enfocarse en una de las amenazas que puede generar mayores impactos en la disponibilidad de la información.

¿Para quién es recomendable?

Empresas que desean reforzar su protección frente al ransomware y reducir el riesgo de que un ataque cifre sus archivos y afecte sus operaciones.

2. Gestión de vulnerabilidades (Vulnerability Management)

Estas soluciones ayudan a mantener los sistemas y aplicaciones actualizados, gestionar los activos de software y reducir los riesgos derivados de vulnerabilidades conocidas.

Patch & Asset Management

[Enlace pendiente: Patch & Asset Management]

Facilita la gestión centralizada de actualizaciones para sistemas operativos y aplicaciones de terceros. También permite obtener visibilidad sobre los activos de software presentes en los dispositivos administrados.

¿Para quién es recomendable?

Organizaciones que necesitan mantener sus equipos actualizados, reducir la exposición a vulnerabilidades conocidas y tener mayor control sobre el software instalado.

Infinity Management

[Enlace pendiente: Infinity Management]

Permite gestionar el despliegue y la administración de aplicaciones y paquetes de software dentro de los dispositivos de la organización.

¿Para quién es recomendable?

Empresas que necesitan centralizar determinadas tareas de distribución y administración de software en sus equipos.

3. Gestión de accesos privilegiados (Privileged Access Management)

Las soluciones de esta categoría permiten controlar cómo se utilizan los privilegios administrativos y gestionar el acceso a recursos y aplicaciones que requieren permisos especiales.

Privilege Elevation & Delegation Management (PEDM)

[Enlace pendiente: Privilege Elevation & Delegation Management]

Permite administrar la elevación de privilegios y delegar permisos específicos sin necesidad de conceder derechos de administrador permanentes a los usuarios. Esto ayuda a limitar los privilegios y mantener un mayor control sobre las acciones que requieren permisos elevados.

¿Para quién es recomendable?

Empresas que desean reducir el número de usuarios con permisos de administrador local y aplicar el principio de mínimo privilegio en sus equipos.

Privileged Account & Session Management (PASM)

[Enlace pendiente: Privileged Account & Session Management]

Está orientada a la administración y supervisión de cuentas y sesiones privilegiadas. Ayuda a establecer controles sobre el acceso a recursos críticos y a mejorar la trazabilidad de las actividades realizadas con privilegios elevados.

¿Para quién es recomendable?

Organizaciones que necesitan reforzar el control sobre las cuentas administrativas y supervisar el acceso a sistemas o recursos sensibles.

Application Control

[Enlace pendiente: Application Control]

Permite establecer políticas para controlar qué aplicaciones pueden ejecutarse en los dispositivos administrados. De esta manera, las organizaciones pueden limitar la ejecución de software no autorizado o que represente un riesgo para la seguridad.

¿Para quién es recomendable?

Empresas que necesitan restringir la ejecución de aplicaciones, controlar el software utilizado por sus colaboradores y reducir la superficie de ataque.

4. Detección y respuesta ante amenazas (Threat Detection & Response)

Esta categoría reúne herramientas para identificar actividades sospechosas, investigar incidentes y responder a amenazas que puedan afectar los endpoints y otros componentes del entorno de seguridad.

Threat-hunting & Action Center (TAC)

[Enlace pendiente: Threat-hunting & Action Center]

Proporciona capacidades para investigar eventos de seguridad, analizar posibles amenazas y facilitar acciones de respuesta desde el entorno de administración de Heimdal.

¿Para quién es recomendable?

Organizaciones que necesitan mejorar la visibilidad de los eventos de seguridad y contar con herramientas para investigar actividades potencialmente maliciosas.

Endpoint Detection & Response (EDR)

[Enlace pendiente: Endpoint Detection & Response]

Permite detectar, investigar y responder a amenazas que afectan los endpoints. Complementa las herramientas tradicionales de protección al ofrecer mayor visibilidad sobre las actividades que ocurren en los dispositivos.

¿Para quién es recomendable?

Empresas que necesitan capacidades adicionales para identificar comportamientos sospechosos, investigar incidentes y responder ante amenazas en sus equipos.

Extended Detection & Response (XDR)

[Enlace pendiente: Extended Detection & Response]

Amplía las capacidades de detección y respuesta mediante la correlación de señales y eventos provenientes de diferentes componentes de seguridad. Esto permite obtener una visión más amplia de posibles incidentes y facilitar su investigación.

¿Para quién es recomendable?

Organizaciones que buscan centralizar el análisis de eventos de seguridad y correlacionar información de diferentes soluciones para mejorar la detección de amenazas.

5. Administración unificada de endpoints (Unified Endpoint Management)

Esta categoría agrupa herramientas para administrar determinados aspectos de los dispositivos desde una plataforma centralizada, facilitando tareas de soporte, configuración y control.

Remote Desktop

[Enlace pendiente: Remote Desktop]

Ofrece capacidades de acceso y soporte remoto para facilitar la asistencia técnica y la administración de dispositivos sin necesidad de estar físicamente frente a ellos.

¿Para quién es recomendable?

Empresas cuyos equipos de TI necesitan brindar soporte remoto a los usuarios y administrar dispositivos distribuidos en diferentes ubicaciones.

BitLocker Management

[Enlace pendiente: BitLocker Management]

Facilita la administración centralizada de BitLocker, la tecnología de cifrado de unidades integrada en Windows, para gestionar aspectos relacionados con la protección de los datos almacenados en los dispositivos.

¿Para quién es recomendable?

Organizaciones que utilizan equipos Windows y necesitan administrar de forma centralizada el cifrado de sus unidades.

USB Control

[Enlace pendiente: USB Control]

Permite establecer controles sobre el uso de dispositivos USB conectados a los equipos, ayudando a gestionar el acceso a medios extraíbles y reducir riesgos asociados con la transferencia de información.

¿Para quién es recomendable?

Empresas que necesitan controlar el uso de memorias USB y otros dispositivos extraíbles para reforzar sus políticas de seguridad de la información.

Scripting

[Enlace pendiente: Scripting]

Permite ejecutar scripts y automatizar determinadas tareas de administración y mantenimiento en los dispositivos gestionados.

¿Para quién es recomendable?

Equipos de TI que buscan simplificar tareas repetitivas, ejecutar acciones de mantenimiento y administrar dispositivos de manera más eficiente.

Comparativo de las soluciones de Heimdal Security

La siguiente tabla resume el propósito principal de cada solución para facilitar su identificación y comparación.

Categoría	Solución	Funcionalidad principal
Seguridad de endpoints	DNS Security – Endpoint	Filtrado DNS y bloqueo de dominios maliciosos en los dispositivos.
Seguridad de endpoints	Next-Gen Antivirus & Firewall	Protección antivirus de nueva generación y firewall.
Seguridad de endpoints	Ransomware Encryption Protection (REP)	Detección y detención de procesos de cifrado malicioso.
Gestión de vulnerabilidades	Patch & Asset Management	Gestión de actualizaciones e inventario de software.
Gestión de vulnerabilidades	Infinity Management	Administración y despliegue de software.
Accesos privilegiados	PEDM	Control y delegación de privilegios administrativos.
Accesos privilegiados	PASM	Administración y supervisión de cuentas y sesiones privilegiadas.
Accesos privilegiados	Application Control	Control de las aplicaciones que pueden ejecutarse.
Detección y respuesta	Threat-hunting & Action Center (TAC)	Investigación de eventos y acciones frente a amenazas.
Detección y respuesta	EDR	Detección, investigación y respuesta en endpoints.
Detección y respuesta	XDR	Correlación de eventos de seguridad de diferentes componentes.
Administración de endpoints	Remote Desktop	Acceso y soporte remoto de dispositivos.
Administración de endpoints	BitLocker Management	Administración del cifrado de unidades en Windows.
Administración de endpoints	USB Control	Control de dispositivos USB y medios extraíbles.

Categoría	Solución	Funcionalidad principal
Administración de endpoints	Scripting	Ejecución de scripts y automatización de tareas.

¿Qué solución de Heimdal debería adquirir mi empresa?

La elección depende de los riesgos que la organización desea atender, la infraestructura tecnológica que utiliza y el nivel de control que necesita implementar. Estos son algunos escenarios que pueden ayudar a identificar la solución más adecuada:

Si necesita reemplazar o reforzar su antivirus actual:

Next-Gen Antivirus & Firewall es una alternativa para proteger los dispositivos frente a amenazas. Puede complementarse con Ransomware Encryption Protection para reforzar la protección frente a procesos de cifrado malicioso.

Si tiene empleados que trabajan desde diferentes ubicaciones:

DNS Security – Endpoint permite aplicar protección DNS directamente en los dispositivos, incluso cuando no están conectados a la red corporativa.

Si necesita mantener actualizados sus equipos y aplicaciones:

Patch & Asset Management ayuda a centralizar la gestión de actualizaciones y obtener visibilidad sobre el software instalado.

Si desea reducir los permisos de administrador en los equipos:

Privilege Elevation & Delegation Management (PEDM) permite controlar la elevación de privilegios y evitar que los usuarios necesiten mantener permisos administrativos permanentes.

Si necesita controlar qué aplicaciones pueden utilizar sus colaboradores:

Application Control permite establecer políticas de ejecución de aplicaciones y restringir software no autorizado.

Si requiere mayor capacidad para detectar e investigar incidentes:

EDR permite detectar, investigar y responder ante amenazas en los endpoints. XDR amplía el análisis mediante la correlación de eventos de diferentes componentes de seguridad.

Si su equipo de TI necesita administrar dispositivos de forma centralizada:

Remote Desktop, BitLocker Management, USB Control y Scripting ofrecen capacidades para facilitar el soporte, la administración y el control de los dispositivos.

¿Se pueden combinar diferentes soluciones de Heimdal?

Sí. Las soluciones pueden complementar sus capacidades para atender diferentes necesidades de seguridad y administración. Algunos ejemplos son:

- **Protección de endpoints:** combinar Next-Gen Antivirus & Firewall con Ransomware Encryption Protection para contar con protección frente a diferentes tipos de amenazas.
- **Protección de dispositivos remotos:** utilizar DNS Security – Endpoint junto con las herramientas de protección de endpoints.
- **Gestión y seguridad de dispositivos:** combinar Patch & Asset Management, Next-Gen Antivirus & Firewall y PEDM para atender la actualización, protección y administración de privilegios.
- **Control de accesos y aplicaciones:** combinar PEDM, PASM y Application Control para reforzar el control sobre los privilegios y la ejecución de software.
- **Detección y respuesta:** utilizar EDR y XDR, de acuerdo con las necesidades de visibilidad, investigación y correlación de eventos de la organización.
- **Administración de endpoints:** complementar las herramientas de seguridad con Remote Desktop, BitLocker Management, USB Control y Scripting para facilitar la gestión de los dispositivos.

La disponibilidad de estas combinaciones, así como las funcionalidades incluidas, depende de las licencias y condiciones comerciales aplicables. Por ello, es importante validar el alcance de cada solución antes de definir una adquisición.

Conclusión

Heimdal Security ofrece diferentes herramientas para abordar necesidades de protección de endpoints, gestión de vulnerabilidades, control de accesos privilegiados, detección de amenazas y administración de dispositivos.

No todas las empresas necesitan implementar todas estas soluciones. Lo más conveniente es identificar primero los riesgos y necesidades de la organización, evaluar las capacidades requeridas y seleccionar las herramientas que aporten mayor valor a su estrategia de seguridad.

En SOGYO podemos ayudarte a identificar las soluciones de Heimdal Security más adecuadas para tu organización y orientarte sobre las alternativas de licenciamiento disponibles.