Heimdal®

Red de seguridad

- Red de seguridad DNS
- Protección contra ransomware en la nube

Endpoint Security

- Seguridad de DNS - Endpoint
- Next-Gen Antivirus, Firewall & MDM
- Protección de cifrado contra Ransomware

Gestión de Vulnerabilidad

- Gestión de parches y activos
- Infinity Management

Gestión de Acceso Privilegiado

- Gestión de Delegación y Elevación de Privilegios
- Control de aplicaciones

Seguridad y Colaboración de Correos Electrónicos

- Seguridad de Email
- Seguridad de Email ante Fraudes

Threat Hunting

- Cazador de Amenazas & Centro de Acciones

Gestión de Endpoints Unificados

- Escritorio Remoto
- Administrador de BitLocker

Proteger Superficies Digitales

Defensa en Profundidad

KAYROS
SOLUCIONES INFORMATICAS S.A.S.

Heimdal®

Red de seguridad DNS

Mejore su red con una capa perfecta de protección de IA que le permitirá cazar, prevenir, detectar y responder a cualquier amenaza, independientemente de lo avanzada que sea.
Heimdal DNS Security Network le permite ser dueño de su BYOD con confianza y proteger todos los dispositivos de sus usuarios, todo bajo un mismo techo unificado y accesible.

Protección contra ransomware en la nube

Nuestra solución patentada de cifrado antiransomware es un producto revolucionario 100% libre de firmas que protege sus dispositivos contra intentos de cifrado maliciosos iniciados durante ataques de ransomware. Proteja sus endpoints y su red incluso contra los intentos de cifrado de ransomware más avanzados, en tiempo real, todo el tiempo.

KAYROS
SOLUCIONES INFORMATICAS S.A.S.

Heimdal®

Endpoint Security

- **Seguridad de DNS - Endpoint**
- Next-Gen Antivirus, Firewall & MDM
- Protección de cifrado contra **Ransomware**

Seguridad de DNS - Endpoint

Es responsable de filtrar todos los paquetes de red según el origen y el destino de la solicitud de DNS. Reemplaza los valores de DNS establecidos manualmente o DHCP con direcciones IP del rango de direcciones IP del host del cliente, por lo que les dice a las computadoras que resuelvan las solicitudes de DNS por sí mismas.

Los valores de DNS originales de la configuración de la tarjeta de red no se pierden, pero se guardan en GUID en el Registro de Windows y se utilizan cuando se realizan solicitudes de DNS hacia recursos internos (servidores de impresión, servidores de archivos locales o cualquier cosa que tenga asignada una dirección IP privada) o recursos externos.

Next-Gen Antivirus, Firewall & MDM

Es el lado de protección reactiva de nuestro conjunto de productos. La solución antivirus de próxima generación reacciona a los archivos infectados que se encuentran en el sistema. Next-Gen Antivirus combina las técnicas conocidas por los antivirus tradicionales y Next-Gen Antivirus para detectar y remediar virus, APT, fraude financiero, ransomware y fugas de datos. Complementa el módulo de producto Threat Prevention - Endpoint para ofrecer una protección integral. Ofrece una interfaz de administración centralizada en todos los dispositivos para facilitar la administración de clientes corporativos. Es flexible y fácil de usar y ofrece una amplia variedad de perfiles de escaneo para adaptarse a sus necesidades corporativas.

KAYROS
SOLUCIONES INFORMATICAS S.A.S.

Heimdal®

Endpoint Security

- **Seguridad de DNS - Endpoint**
- Next-Gen Antivirus, Firewall & MDM
- Protección de cifrado contra **Ransomware**

Protección de cifrado contra Ransomware

Ransomware Encryption Protection es una solución revolucionaria 100 % libre de firmas que protege sus dispositivos contra intentos de cifrado maliciosos iniciados durante ataques de ransomware. Ransomware Encryption Protection amplía la funcionalidad de los antivirus tradicionales, convirtiéndose en una solución capaz de prevenir y proteger tus endpoints frente a cualquier tipo de ataque de ransomware.

¿Cómo Funciona La Protección Contra El Cifrado De Ransomware?

Ransomware Encryption Protection opera con análisis de comportamiento (activa detecciones basadas en reglas que imitan el comportamiento del ransomware) y procesa eventos del kernelpara lecturas de E/S, escrituras, enumeración de directorios y ejecución de archivos. Los patrones se comparan con los eventos recopilados después de estudiar los mismos patrones que está creando el ransomware real. El motor permitirá que se cifren aproximadamente 3 archivos de tamaño promedio (según el tamaño de los archivos y la velocidad del ransomware, se pueden cifrar más archivos. Por ejemplo, el ransomware podría cifrar fácilmente más de 3 archivos de 20 KB) hasta que emita el veredicto de que el proceso es sospechoso. Una vez marcado, los detalles sobre el proceso sospechoso se recopilan y se envían a los servidores de HEIMDAL. Estos detalles incluyen los argumentos de la línea de comandos del proceso, las conexiones de red (dirección IP y puerto), el recuento de operaciones de lectura/escritura en el momento de la detección y también el árbol de procesos desde el proceso sospechoso con seguimiento hasta el proceso raíz.Perspectivas de Heimdal .

El servicio se encarga de escanear permanentemente los procesos activos y mapear cada acción del proceso, así como buscar patrones de encriptación en los procesos en ejecución. El servicio Heimdal Insights se ejecutará solo si el módulo está habilitado en la Política de grupo. Si REP está deshabilitado en la Política de grupo, el servicio Heimdal Insights estará presente pero no se ejecutará.

KAYROS
SOLUCIONES INFORMATICAS S.A.S.

Heimdal®

Gestión de Vulnerabilidad

Gestión de parches y activos

Infinity Management

Gestión de parches y activos

Nuestra solución de administración de parches de terceros automatiza las actualizaciones de las aplicaciones de terceros según sus políticas configuradas. Implementa los parches de manera silenciosa, sin reinicios ni interrupciones para los usuarios, tan pronto como los proveedores los lanzan.

HEIMDAL entrega actualizaciones probadas y cifradas a través de HTTPS a sus dispositivos, optimizando la distribución con una red P2P local. Puede personalizar las políticas de implementación en grupos de Active Directory para adaptarse a sus necesidades y desplegarlas de manera fácil y sencilla.

Infinity Management

Es una herramienta que puede ofrecer la posibilidad de implementar de forma silenciosa Aplicaciones de terceros que no están incluidas en la lista de Aplicaciones de terceros gestionadas por HEIMDAL Security. Cualquier aplicación que admita comandos de instalación silenciosa (/I; /qn; /s; /update , etc.) puede implementarse mediante el módulo Infinity Management. Con esta herramienta, puede implementar aplicaciones que tengan las siguientes extensiones de archivo: .msi, .exe, .msp o .zip.

KAYROS
SOLUCIONES INFORMATICAS S.A.S.

Heimdal®

Privileged Access Management

- **Gestión de Delegación y Elevación de Privilegios**
- **Control de Aplicaciones**

Gestión de Delegación y Elevación de Privilegios

La administración de acceso privilegiado es una herramienta PAM que se puede usar para brindarles a los usuarios la capacidad de instalar el software que necesitan durante un período de tiempo que seleccione mediante la sesión del administrador o la opción Ejecutar con PAM para la elevación de un solo archivo. Los derechos otorgados se pueden revocar en cualquier momento y las acciones se registran para una pista de auditoría completa.

Esta es la función que permite a un usuario final solicitar privilegios de administrador sobre su máquina enviando una solicitud al Administrador del Panel HEIMDAL, quien puede rechazar o aceptar su solicitud. La duración de la sesión es limitada y todas sus acciones se registran en el Panel HEIMDAL.

Control de Aplicaciones

Le permite acelerar el flujo de aprobación o denegación de su aplicación para archivos con reglas predeterminadas y crear o modificar flujos para usuarios individuales o grupos de AD. Puede manejar cómo debe ejecutarse un proceso (puede obtener una elevación automática desde el módulo de administración de acceso privilegiado , si está configurado) o un proceso secundario (puede permitir o bloquear todos los procesos generados por el proceso que coincide con la regla).

Application Control es un producto/servicio bajo HEIMDAL Agent que controla los procesos que pueden ejecutarse o no en una computadora. Cuando se permite que los procesos se ejecuten, se les puede permitir que se ejecuten con un rol de administrador y se les puede permitir que generen procesos secundarios. Application Control es administrado por el servicio Heimdal ProcessLock que captura cada proceso que se inicia y verifica si se permite su ejecución o no.

KAYROS
SOLUCIONES INFORMATICAS S.A.S.

Heimdal®

Email & Collaboration Security

Seguridad de Email

Seguridad de Email ante Fraudes

Seguridad de Email

Nuestro Email Security utiliza motores de filtrado y detección de spam líderes en el mercado que van más allá de las simples definiciones de spam. Previene de manera proactiva incluso las vulnerabilidades de correo electrónico más sofisticadas que buscan dañar a su organización al pasar por alto los filtros de correo no deseado y las soluciones antivirus habituales.

Las funciones de Email Security incluye protección antispam, protección contra botnets, filtrado avanzado de malware, protección contra el secuestro de DNS, protección contra phishing, seguimiento de amenazas y registro de auditoría completo, detección de fugas de números de seguridad social

Seguridad de Email ante Fraudes

El servicio de Prevención de Fraude por Correo Electrónico escanea y previene el fraude en los correos electrónicos, comparando las comunicaciones entrantes y salientes con firmas registradas previamente. Detecta cambios en los mensajes y evita ataques BEC.

El servicio se inicia con la instalación del Agente HEIMDAL o mediante la verificación de la Política de grupo. Intercepta y valida los correos electrónicos en las carpetas de Bandeja de entrada y Enviados, con respuestas en 10 minutos y resultados finales en 24 horas. Los correos infectados se mueven a la carpeta "Heimdal - EFP".

KAYROS
SOLUCIONES INFORMATICAS S.A.S.

Heimdal®

Threat Hunting

Cazador de Amenazas & Centro de Acciones

Cazador de Amenazas & Centro de Acciones

Aproveche el poder de Unity en una sola plataforma.

KAYROS
SOLUCIONES INFORMATICAS S.A.S.

Heimdal®

Gestión de Endpoints Unificados

- Escritorio Remoto
- Administrador de BitLocker

Escritorio Remoto

Remote Desktop es una aplicación de escritorio remoto segura y confiable que le permite brindar soporte a sus clientes o acceder a computadoras desatendidas. Es asequible y simplemente funciona. Puede configurar la computadora de su oficina para el teletrabajo en menos de un minuto y puede acceder de forma segura a la computadora de su oficina desde su hogar o mientras está en movimiento. La tecnología de pantalla compartida le permite trabajar de manera eficiente de forma remota en cualquier momento, desde cualquier parte del mundo.

Administrador de BitLocker

Proximamente

KAYROS
SOLUCIONES INFORMATICAS S.A.S.