

# Plataforma Hillstone de Seguridad en Auditoría

HSA-10P / HSA-10 / HSA-5 / HSA-3 / vHSA



Los ISPs, universidades, grandes empresas, agencias gubernamentales y grandes centros de datos generan millones de eventos todos los días. Ellos requieren almacenamiento de registros de alto rendimiento y resultados de consulta casi instantáneos para analizar una explosión de datos generados por los actuales Firewalls de Próxima Generación. La Plataforma de Auditoría en Seguridad de Hillstone (HSA) transforma los datos de registro en inteligencia de seguridad con búsquedas en fracciones de segundo que proporcionan una visión instantánea de miles de millones de registros. La Plataforma de Auditoría en Seguridad de Hillstone reúne y compara NAT's, Amenazas, URL's y Registros de sesión y proporciona capacidades de búsqueda granulares que proporcionan visibilidad en tiempo real sobre el tráfico de red.

## Detalles del Producto

### Visibilidad en la Red

Los archivos de registros permiten visibilidad de las actividades en la red y ayudan a cumplir con las normativas. Pero correr consultas sobre millones de registros puede tardar horas con los sistemas tradicionales de gestión de registros. No obstante, sin una gestión eficaz de los registros, las empresas se privan de la inteligencia proporcionada por sus propios entornos y se exponen a desenfundados eventos de seguridad. La Plataforma de Seguridad en Auditoría de Hillstone proporciona potentes consultas, que son fáciles de utilizar y que proporcionan rápidamente una visión instantánea de millones de registros.

### Procesamiento de Registros de Alto Rendimiento

Las grandes empresas pueden generar hasta 100 gigabytes de datos de registros al día. Poder escalar a estas velocidades de datos es un aspecto importante para iniciar la sesión de retención. La Plataforma de Seguridad en Auditoría de

Hillstone apoya el syslog estándar, así como un protocolo binario de muy alto rendimiento que puede recibir hasta 100.000 eventos por segundo de tráfico NAT. Puede escalar dinámicamente el almacenamiento para satisfacer los requisitos de retención y cumplimiento a través del balanceo de carga distribuida o mediante el envío de registros específicos a servidores específicos.

### Consultas de Gran Alcance

La Plataforma de Seguridad en Auditoría de Hillstone permite a los usuarios fácilmente crear y guardar las consultas que se ejecutan por demanda o de forma programada. Se puede buscar por IP de origen, por IP destino, por URL, por IP pública y por tiempo. Además, los registros de NAT de Hillstone pueden cambiar una dirección IP pública a una dirección IP o puerto privado y nombre de usuario. Esto proporciona importantes detalles forenses en entornos que utilizan NAT y necesitan visibilidad en la red privada.

## Características Principales

### Control de Dispositivos

- Monitoreo de los KPI para dispositivos
- Análisis de la relación del tipo de almacenamiento de registros
- Análisis de tendencias por dispositivo y de tipos de registros
- Monitoreo de dispositivos de envío
- Seguimiento personalizado
- Estado de salud de disco duro y monitoreo de estado RAID

### Administración de registros

- NAT, Sesión, URL, correo electrónico, mensajería instantánea y fuera de línea y registros de amenazas de prevención
- Puede importar y analizar Syslogs de dispositivos de terceros
- Búsquedas combinando múltiples estados
- Adición de Registros

- Soporta la transmisión de registros por SSL
- Guarda parámetros de búsqueda
- Búsquedas en trasfondo
- Consultas distribuidas para múltiples dispositivos
- Servidores NFS extensibles para almacenamiento de registros

### Gestión de Informes

- Vienen incluidas múltiples plantillas para informes
- Informes personalizables
- HTML, PDF e informes en formato MS Word

### Administración del Sistema

- Configuraciones confiables de los dispositivos
- Importación/exportación de registros
- Reenvío de registros
- Configuración de búsquedas distribuidas
- Gestión basada en roles como: administrador, operador y auditor
- Configuración de la zona horaria de ahorro de luz diurna

## Especificaciones del producto

Especificación	HSA-10P	HSA-10	HSA-5	HSA-3
Desempeño	NAT: 100,000 EPS Syslog: 10,000 EPS	NAT: 100,000 EPS Syslog: 10,000 EPS	NAT: 50,000 EPS Syslog: 5,000 EPS	NAT: 30,000 EPS Syslog: 3,000 EPS
Almacenamiento	NAT log: 180 days for 10G link	NAT Log: 180 days for 5G link	NAT Log: 180 days for 3G link	NAT Log: 180 days for 1.5G link
HDD	16TB	8 TB	4 TB	2 TB
Puertos I/O fijos	2 x GE	2 x GE	2 x GE	2 x GE
Niveles RAID	RAID 5	RAID 5	RAID 0	RAID 0
F. Alimentación	Single/Dual	Single/Dual	Single	Single
Factor Forma	2U	2U	1U	1U

Especificación	vHSA-2
vCPU	Minimum 4 Core
Memory	Minimum 4G
Disk	Minimum 200G
Log Storage	NAT log: 180 Days for 1G link
Performance	NAT: 20,000 EPS, Syslog: 20,000 EPS
Hypervisor Support	VMware EXSi 5.1/5.5/6.0, VMware Workstation 12 or later version, KVM