efficient iP™

@GIS GLOBAL INVESTMENT SOLUTIONS S.A.C.

Datasheet

# DNS Guardian

## Protege los Datos y Garantiza la Continuidad de los Servicios de DNS

## Principales Ventajas:

- Detección, protección y características de corrección de la caché, recursiva y de autorizaciones de DNS
- Inspección de la transacción de DNS en tiempo real para analítica avanzada de DNS
- Detección de amenazas de comportamiento para una toma de decisiones precisa
- Filtrado de dominio granular por usuario para mejorar el control de acceso a las aplicaciones
- Contramedidas de seguridad adaptables para una inigualable continuidad del servicio
- Gestión centralizada de políticas de seguridad DNS en toda la red
- Estadísticas avanzadas de DNS para informes más inteligentes
- Integración con Cisco Umbrella para proteger las apps, red on/off de datos y usuarios

El servicio DNS es un componente de red de misión crítica, un hecho que no ha pasado desapercibido para los hackers. En los últimos años, se ha observado un alto ritmo de ataques a los servidores DNS (resaltado en la encuesta sobre amenazas DNS de EfficientIP 2020). La naturaleza de las amenazas de DNS está evolucionando rápidamente, y los ataques se han vuelto muy sofisticados, basados en modelos de asalto distribuidos, con vectores múltiples, y de varias etapas. Las soluciones de seguridad DNS tradicionales han demostrado ser insuficientes. Peor aún, suponen el alto riesgo de crear falsos positivos. Como resultado, es necesario un nuevo enfoque de seguridad para evitar interrupciones en la red y posibles robos de datos que podrían repercutir significativamente en los negocios.

Gracias a sus innovadores avances tecnológicos, DNS Guardian de EfficientIP es la primera solución de seguridad DNS que permite una inspección completa de transacciones DNS y una analítica avanzada para la detección de comportamientos de amenazas en tiempo real. Sus contramedidas inteligentes patentadas proporcionan una seguridad adaptable para proteger la confidencialidad de los datos y garantizar una continuidad de los servicios DNS inigualable, incluso ante los ataques más insidiosos.

## Un marco de seguridad reforzado

DNS Guardian se beneficia de una innovación arquitectónica que separa la caché de DNS de la función recursiva y funciones de autorización para fortalecer y mejorar notablemente la seguridad del servicio global. Sometida al ataque, cada función está protegida por separado respecto a sus propias propiedades, evitando efectos secundarios y garantizando la disponibilidad del servicio. Las contramedidas patentadas de DNS Guardian pueden ser adaptadas en función de las necesidades específicas de cada función y de cada ataque detectado, consiguiendo una protección inigualable.

## Tecnología de inspección de transacción DNS

DNS Guardian es la primera y única solución en el mercado que ofrece una inspección de transacciones DNS (DTI) completa, en tiempo real y sin ninguna repercusión en el rendimiento. DNS Guardian examina, en el corazón mismo del protocolo, el conjunto de secuencias de intercambios de consultas para cada transacción DNS:

- Fragmentos, consultas y su carga, y respuestas relacionadas
- Duración y tamaño de transacción

La innovación de la inspección de transacciones DNS Guardian permite un completo entendimiento del contexto del cliente, superando las limitaciones de los sistemas de seguridad basados en firmas que sólo ofrece una visibilidad limitada del tráfico periférico. Esto es clave para lograr una verdadera analítica DNS y una capacidad de detección de amenazas de comportamiento.

## Identificación de usuario avanzada

DNS Guardian analiza en profundidad el comportamiento del cliente para aplicar las contramedidas adecuadas cuando sea necesario. La identificación estándar del cliente se basa en la dirección IP de origen de la solicitud DNS, pero las topologías complejas requieren que el cliente sea identificable a partir de otros parámetros. DNS Guardian puede utilizar el DNS integrado como fuente de identificación, en lugar de la dirección IP. Esto permite contar con controles como el control parental, CG-NAT en redes de telecomunicaciones, y solicitudes DNS en cascada de otro remitente.

## Proxy DNS transparente

Hay situaciones en que se requiere interceptar peticiones DNS dirigidas a determinados servidores de Internet, con el fin de proporcionar servicios adicionales, como filtrado, contabilidad o interceptación del tráfico. DNS Guardian puede configurarse para tener en cuenta dicho tráfico, actuando como proxy DNS transparente. Cualquier petición de DNS que llegue a DNS Guardian será analizada con las funciones de seguridad estándar, y remitida al destino original: la respuesta será enviada al cliente en cuanto se reciba. Esta solución es ideal para filtrado RPZ global o análisis en profundidad del comportamiento del tráfico del cliente para filtrar o poner en cuarentena los IPs malignos.

## Gestión centralizada de políticas de seguridad

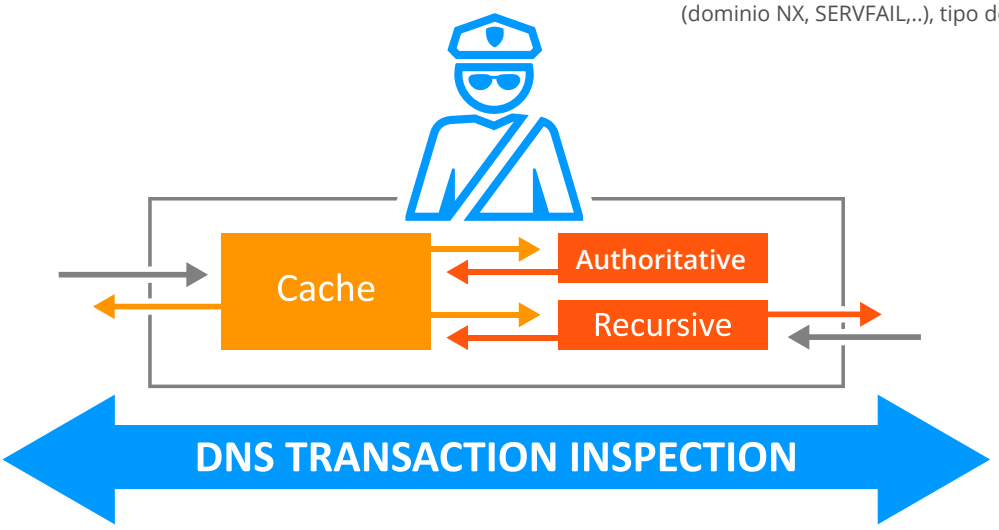
Las políticas de seguridad global que se aplicarán en mùltiples DNS Guardian pueden configurarse desde una interfaz gráfica de usuario central. Estas políticas reforzarán la configuración de la detección de amenazas de comportamiento y mitigación en toda la red, para una gestión unificada de los mecanismos de seguridad que aprovechan y protegen los componentes DNS. Esta capacidad de manipular simultáneamente un grupo de servidores reduce los costes de administración y permite un ajuste fino de los umbrales.

## Analítica avanzada DNS de detección de amenazas de comportamiento

**Visibilidad en profundidad del tráfico DNS**

La capacidad de inspección transaccional de DNS Guardian asegura una visibilidad profunda y una comprensión precisa del tráfico DNS a lo largo del tiempo. Recoge, agrupa y almacena en tiempo real las estadísticas más avanzadas sobre una base global y para cada cliente:

- Proporción de pruebas/errores en caché, consultas mal formuladas, fragmentación, tiempos de recursividad, distribución de código de retorno, latencia
- Consumo de ancho de banda de DNS
- Lista principal: clientes, dominios solicitados, código de retorno (dominio NX, SERVFAIL,..), tipo de consulta




*Innovador Marco de Seguridad DNS Guardian*

**Análisis de amenazas de múltiples factores para una detección de ataques inigualable**

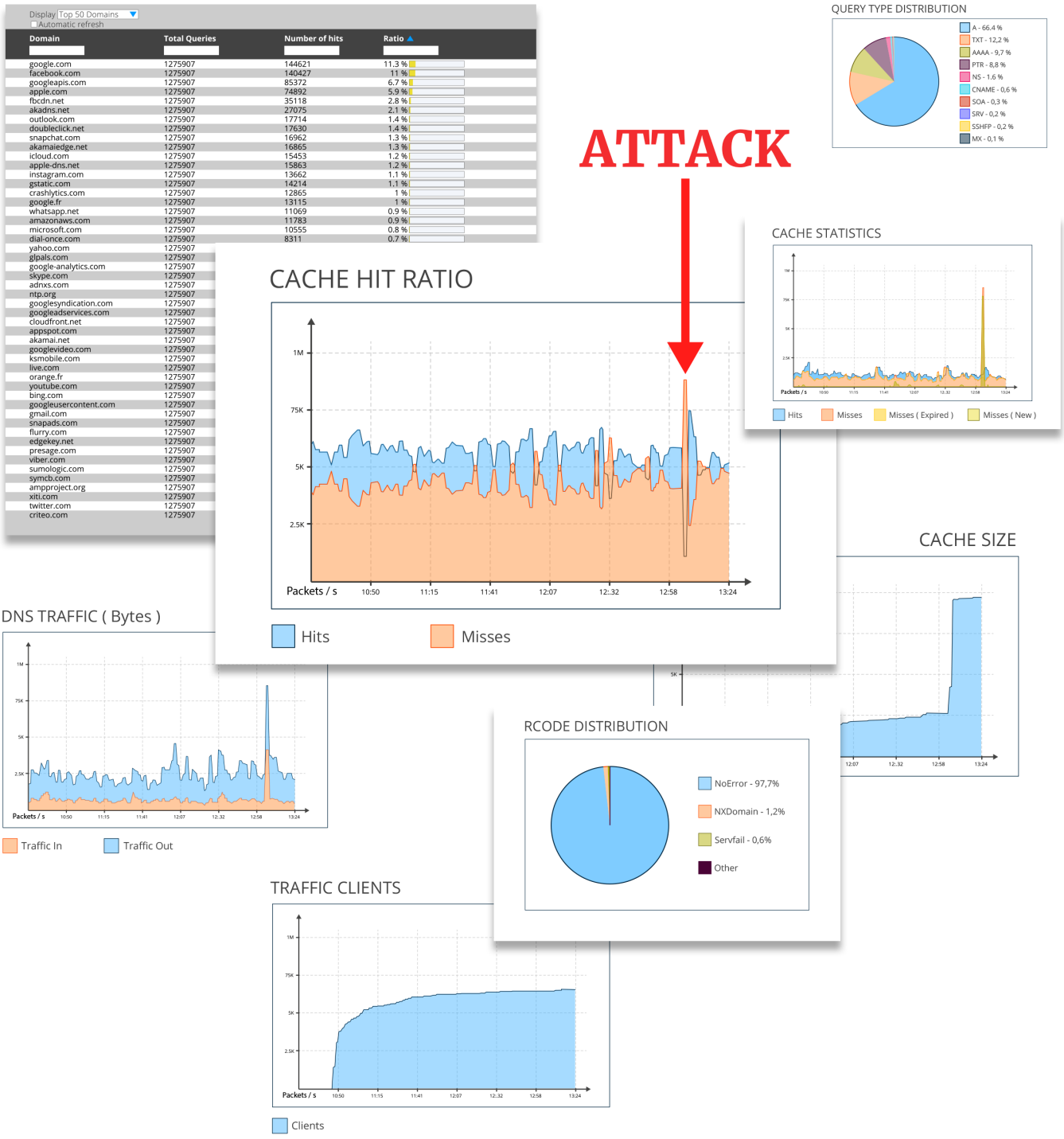
Esta visibilidad exclusiva, junto con la visibilidad en tiempo real de múltiples factores de análisis del tráfico (que considera las tendencias del tráfico global, los comportamientos de los clientes y las funciones DNS), asegura un rendimiento inigualable de detección de amenazas de comportamiento basado en la más avanzada capacidad de análisis de seguridad DNS.

Resalta la visibilidad de las amenazas más allá de patrones de ataques conocidos y de los mecanismos de listas negras que quedan obsoletas rápidamente, consiguiendo la identificación de los ataques a dominios más avanzados, tales como Tunneling, Phantom o Sloth.

**DNS Guardian protege contra cualquiera de los siguientes ataques:**

Consultas no válidas: análisis de las consultas DNS, y eliminación de aquellas que no cumplan con la normativa RFC(s), antes de que lleguen al motor DNS recursivo

- Ataques NXDOMAIN: análisis de la proporción de respuestas nxdomain por dirección IP de origen. Esto permite una detección y mitigación más eficaz que cualquier otro enfoque basado en patrones de expresiones normales que rebajan el rendimiento del motor de DNS
- Ataques a dominios con subdominios aleatorios / dominio fantasma: análisis de la proporción de respuestas nxdomain y Servfail por dirección IP de origen. Esto permite una detección y mitigación más eficaz que cualquier otro enfoque basado en patrones de expresiones normales que rebajan el rendimiento del motor de DNS
- Ataques de dominio Sloth: análisis del tiempo que pasa esperando las respuestas DNS desde cualquier servidor de nombre de dominio ante las consultas de los clientes. Esto permite la rápida identificación y aislamiento de cualquier generación de consultas de clientes dirigidas a cualquier nombre de dominio del servidor diseñado específicamente para desacelerar el motor recursivo con respuestas lentas
- Ataques túnel de DNS: análisis de consultas y tamaño DNS sin caché. Esto permite una eficiente prevención y detección de efecto túnel, mucho mejor que cualquier detección basada en un patrón de base de datos de referencia conocida, posiblemente desactualizada.
- Ataques de envenenamiento de caché: implementación del soporte para cookies y consultas DNS EDNS, y puerto de aleatorización de origen en combinación con 16 bits únicos criptográficamente seguros para reducir drásticamente la probabilidad de éxito del recorrido de los ataques a DNS. Sin embargo, sólo el apoyo de DNSSEC garantiza la validez de las respuestas proporcionadas por zonas firmadas
- Ataques reflectantes distribuidos: análisis de consultas por dirección IP de origen de la limitación de velocidad de la tasa de consultas (Nota: La solución más efectiva para prevenir un ataque de ese tipo sigue siendo evitar la suplantación de IP dentro de una red). Esto permite la prevención de la utilización de su infraestructura como vector reflectante de cualquier ataque
- Inundaciones de DNS: el análisis del rendimiento de tráfico DNS global permite el aislamiento de clientes sospechosos o la activación del modo de rescate, asegurando la disponibilidad de caché DNS bajo condiciones extremas de ataque




*EfficientIP DNS Guardian Threat Monitoring*

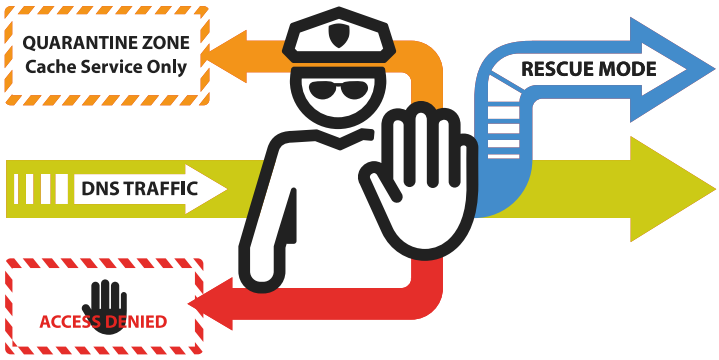
## Contramedidas inteligentes para seguridad adaptable

La analítica avanzada de DNS Guardian proporciona una comprensión sin precedentes de amenazas de DNS, ofreciendo la oportunidad de activar la contramedida correcta en el momento oportuno en función de cada tipo de ataque. La solución exclusiva de seguridad adaptable de EfficientIP ofrece contramedidas inteligentes que protegen la continuidad de los servicios de DNS y la confidencialidad de los datos:

- Bloquear direcciones IP de origen ante los ataques
- Limitar la velocidad del tráfico DNS por IP de origen
- Cuarentena para las IPs de origen sospechosas de ataques (patentado)
- Activación del modo de rescate: asegure la continuidad del servicio, incluso si el ataque es de origen no identificable (patentado)

El modo de cuarentena aísla las direcciones IP que tengan comportamientos maliciosos, de modo que tienen acceso ilimitado únicamente a los datos de la caché, mientras que sus solicitudes recursivas están bloqueadas. Esto protege al servidor de los ataques, y reduce el riesgo de bloquear a los clientes legítimos.

Sin embargo, bajo condiciones extremas, cuando no es identificable el origen del ataque (normalmente en el caso de ataques por goteo lento o muy distribuidos), DNS Guardian detecta el riesgo de agotamiento de la capacidad del servidor y activa el modo de rescate patentado. Esta contramedida exclusiva asegura que las respuestas DNS en caché permanecen 100% a disposición de los clientes, incluso cuando no sea posible una actualización de validez de los datos que garantice la accesibilidad del 100% para la mayoría de las aplicaciones críticas de la empresa y de los servicios.




*DNS Guardian Actions*

## Fallo de los servidores DNS de flujo ascendente

Cuando falla el sistema DNS global o se vuelve inaccesible debido a algún fallo en el eje troncal de internet, puede que el motor DNS recursivo no sea capaz de atender las consultas de un cliente al DNS recursivo. Como resultado, los clientes terminan desconectados de todos los servicios, mientras que, en realidad, todavía podrían estar accesibles, en marcha y funcionando. La inteligencia de DNS Guardian evita que se produzcan situaciones de este tipo. Cuando se recibe una consulta a un dominio presente en la memoria caché pero caducado, DNS Guardian ignora el fracaso procedente del motor recursivo local y responde al cliente con la respuesta almacenada en la caché con un valor  TTL (30 segundos). La ventaja es la continuidad mejorada de servicio durante algún breve fallo externo, muy parecido al modo de rescate.

## Mejora del control de acceso a las aplicaciones

La seguridad es un punto clave en la gestión del tráfico DNS. La solución Guardian instala un cortafuegos DNS que filtra las solicitudes de los clientes en función de una lista de dominios que deben ser rechazados o autorizados según la política global (enfoque de lista blanca o lista negra). El cortafuegos puede tener diferentes objetivos, desde proteger dispositivos y clientes contra aplicaciones maliciosas hasta autorizar solo las aplicaciones seleccionadas bien conocidas e identificadas en dispositivos específicos como IoT, dispositivos compartidos o equipos industriales.

Además de la función de cortafuegos, que se centra principalmente en el destino del tráfico de la aplicación, DNS Guardian se caracteriza por su enfoque orientado al cliente con la solución Client Query Filtering (CQF), que ayuda a reducir el riesgo de exposición al ofrecer una barrera de seguridad que controla el acceso a la aplicación en el punto más inicial del flujo. Con CQF es posible aplicar algunas listas de filtrado más granulares en el cortafuegos a un grupo de clientes o dispositivos. Al unir listas de clientes y listas de dominios para autorizar o denegar, se amplía significativamente el número de casos de uso. La naturaleza dinámica de las listas utilizadas en CQF admite escenarios automatizados donde se pueden agregar y eliminar clientes sobre la marcha, así como los dominios enumerados en el cortafuegos DNS. Estas actualizaciones dinámicas suponen directamente una mayor seguridad de la red. En este sentido aporta un enfoque de seguridad global en el ecosistema con más puntos de control entre el cliente y su aplicación al combinar el DNS con otras soluciones habituales de cortafuegos y filtrado de IP.

## Mejora de la experiencia de usuario

### Rendimiento de la caché inigualable

DNS Guardian implementa un sistema de caché DNS que aumenta significativamente el rendimiento de la búsqueda en caché. Combinado con los dispositivos Blast SOLIDServer™, Guardian es capaz de alcanzar hasta 17 millones de consultas por segundo.

### Compartir caché de multidifusión

La propiedad de compartir caché de DNS Guardian mejora el rendimiento de la plataforma DNS completa, reduciendo la cantidad de consultas recursivas enviada a los servidores autorizadores y reduciendo la latencia del servicio DNS. Se basa en un mecanismo de multidifusión IP para optimizar el uso de la red. Combinado con el modo de rescate y el conjunto de los mecanismos de seguridad ofrecidos por Guardian, permite el despliegue de plataformas muy seguras de distribución en colaboración de DNS recursivo, reforzando la seguridad de la infraestructura global.

### Caché persistente (reinicio y restauración)

DNS Guardian permite realizar la copia de seguridad de la caché. Los datos de caché existentes se pueden utilizar para reiniciar, permitiendo una inmediata recuperación del rendimiento de DNS. Elimina la necesidad de que el motor de DNS realice consultas recursivas hasta que se reconstruya su caché, lo que podría llevar a un exceso de carga y repercutiría enormemente en el rendimiento del servicio.

### Cifrado de tráfico DNS local

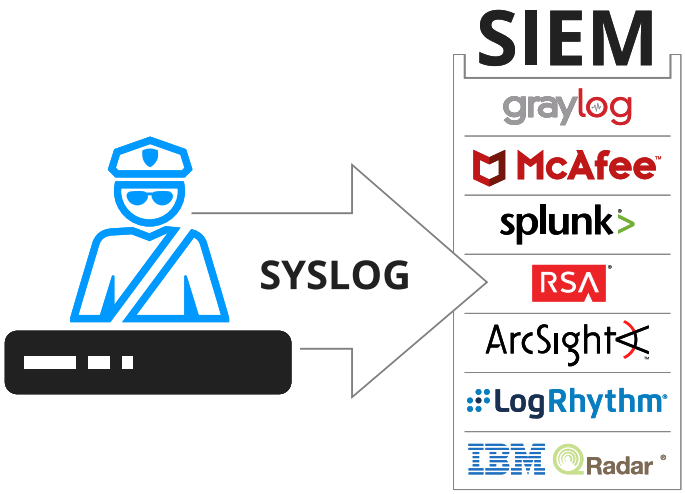
DNS Guardian protege el tráfico del usuario mediante cifrado, al activar DoT (DNS en TLS). Este método de acceso se suma al DNS estándar en UDP y DNS en TCP que trasladan el tráfico sin cifrar. Al utilizar DNS en TLS, el tráfico se cifra y el acceso se puede proteger mediante certificados digitales para evitar que puedan ser espiadas las solicitudes DNS del cliente.  Además de DoT, también acepta el protocolo de tunelización DNS sobre HTTPS (DoH) para proporcionar al cliente la seguridad del navegador con un estándar de facto.

## Centralización de registro de alto rendimiento

El DNS es un servicio de red fundamental y una valiosa fuente de datos que pueden utilizar los defensores de la red. La monitorización de DNS tiene que ser parte de la estrategia de seguridad y es clave para mantener el seguimiento de la actividad DNS con fines periciales. Esto podría permitir la detección y la comprensión de la actividad sospechosa como propagación de malware, suplantación, campañas o cualquier ataque que pudiera haber puesto en peligro un sistema de información en el pasado sin ser notado.

DNS Guardian ofrece un sistema exclusivo de registro de alto rendimiento que no tiene impacto alguno en el rendimiento del software de DNS. El registro asíncrono asegura la continuidad de una visibilidad detallada del historial de transacciones, incluso durante ataques volumétricos, superando la limitación de los servicios DNS tradicionales. Sustenta el formato Syslog estándar para cumplir con los sistemas de gestión de registro existentes. Las implementaciones típicas pueden aprovechar los dispositivos de terceros como Splunk, Graylog, ELK, o cualquier SIEM para recopilar y analizar esta enorme cantidad de datos archivados para generar informes de análisis de tráfico avanzados.

DNS Guardian es parte de la solución de seguridad exclusiva 360° de EfficientIP diseñada para proteger las infraestructuras DNS públicas y privadas, tanto contra amenazas internas como externas de DNS, independientemente del tipo de ataque.




*High Performance Logging Technology*

efficient iP™

REV: C-200210



**Americas**
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

**Europe**
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

**Latam**
GIS-SAC
Av Santiago de Surco
2875, Of 602, Lima - Perú
+51 1 2710852
contacto@gis-sac.com