SMART PROTECTION

No Hardware Adicional

Bajo Costo

Basado en DNS

Admón Centralizada

Informes

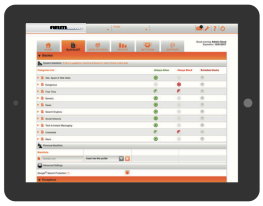
Todos los Dispositivos

SmartProtection

Es una tecnología de mitigación de malware y filtrado de Internet basada en la nube para pequeñas y medianas empresas, instituciones educativas, el gobierno y cualquier otra persona. ARM SmartProtection no requiere hardware o software adicional y se integra fácilmente con dispositivos de acceso de terceros. ARM puede activarse en solo 15 minutos ofreciendo un filtrado y monitoreo confiable y sin complicaciones.

Cualquier Momento, Cualquier Lugar

SmartProtection es un servicio en la nube. Esto significa que la tecnología de filtrado no está instalada en dispositivos locales, está alojada en un sitio remoto y seguro en muchos sitios alrededor del mundo.



Sobre ARM SmartProtection

ARM SmartProtection se ejecuta en granjas de servidores distribuidos geográficamente para proporcionar una alta disponibilidad de servicio y baja latencia. El filtrado es basado en tecnología DNS que tiene un impacto imperceptible en el la experiencia de usuario en la navegación a Internet

ARM WebFilter identifica automáticamente las categorías de contenido a las que acceden los usuarios y facilita la definición de reglas de filtrado. Se pueden crear reglas para monitorear o bloquear la actividad, y se mantiene un registro de actividad durante 6 meses. Las reglas de filtrado se pueden establecer por hora del día y día de la semana y se pueden variar para diferentes comunidades de usuarios. ARM SmartProtection también puede bloquear automáticamente los intentos de acceder a sitios de malware conocidos, sitios de ransomware o sitios en cualquier país que se considere asociado con una amenaza específica.

Características Clave

Funcionalidad	Comentario
Control de Contenido	54 categories de contenido 0.1% de falsos positivos
Personalización de Listas Negras	Provee una alternativa adicional para conseguir la mitigación deseada
Listas Blancas	SI
Control de Aplicaciones	Control de aplicaciones así como dominions e IPs
Safe Search (búsqueda segura)	Google, BING, Youtube
Geo Blocking	Excluye países altamente riesgosos o construye un walled garden de países seguros hacia donde navegar.
Control de Amenazas	Ransomware, Troyanos, Botnets, Gusanos, etc
Acciones	Bloqueo, monitoreo, log, control horario (ver siguiente)
Control Horario	Las políticas de control horario pueden ser aplicadas para hora especifica del día, día de la semana para cada categoría.

Funcionalidad	Comentario
Latencia de paquete de datos	0ms
Latencia de paquete DNS	Tipicamente 10-50ms
Compatibilidad con routers comerciales y open source	SI
Sporte para instalaciones con IP privada	Si, utilizando dyndns v2
Disponibilidad del servicio Cloud	99.9%, excluye la conexión local (infraestructura de cliente)
Despligue de Hardware adicional ¿?	NO
Despliegue de Software adicional¿?	NO (requiere cliente para dispositivos móviles)
Tiempo de implementación	Tipicamente 15 minutos
Modelo de Precios	Precio por numero de usuarios concurrentes. Total de usuarios ilimitado.
Temporalidad de Licencias	1 y 3 años