

Arbor Cloud DDoS Protection Service para empresas

Verdadera protección global contra DDoS a demanda

PRINCIPALES CARACTERÍSTICAS Y BENEFICIOS

Protección global contra DDoS

Una única solución que ofrece protección global contra DDoS independientemente del portador, respaldada por productos de protección contra DDoS con inteligencia de seguridad de categoría internacional y liderazgo en la industria.

Más de 1 Tbps de protección en cloud

Filtra ataques DDoS de gran volumen al usar más de 1 Tbps de capacidad de depuración de tráfico basado en cloud. Soporte para mitigación IPv4 e IPv6 en cloud.

Protección inteligente y en capas

Integra la protección APS en las instalaciones y Arbor Cloud en cloud por medio de la tecnología exclusiva Cloud Signaling™ de Arbor.

Con tecnología de Inteligencia de amenazas global

Las soluciones de protección contra DDoS en las instalaciones y de Arbor Cloud cuentan automáticamente con la inteligencia de amenazas globales más reciente del Security Engineering and Response Team (ASERT) de Arbor.

Servicio gestionado APS (mAPS)

Confíe en la experiencia líder en la industria de Arbor Networks para administrar y optimizar su protección APS en las instalaciones contra DDoS.

La tendencia de los ataques DDoS no es muy favorable para las empresas. Los ataques volumétricos están creciendo. La popularidad creciente de los ataques de amplificación/reflejo aumenta el nivel de complejidad. En la actualidad, los ataques DDoS modernos emplean una combinación de vectores que incluyen ataques volumétricos, de agotamiento de estados de TCP y de ataques a nivel de aplicaciones. La Protección Arbor CloudSM contra DDoS para empresas (Arbor Cloud) brinda servicios de depuración basados en cloud, fuertemente integrados con defensa de mitigación contra DDoS en las instalaciones. Este método con varias capas para la protección contra DDoS es algo que ninguna empresa puede dejar de tener para mitigar la actual gama de las amenazas de DDoS.

Protección en capas contra ataques DDoS en la actualidad

Como parte de un método pensado en capas para la protección contra DDoS, Arbor Cloud proporciona protección en cloud contra ataques DDoS avanzados y de gran volumen sin interrumpir el acceso a sus aplicaciones y servicios. El servicio de depuración a demanda de Arbor Cloud, controlado por expertos en seguridad contra DDoS de Arbor, lo defiende de los ataques DDoS volumétricos que son demasiado grandes como para poder mitigarlos en las instalaciones.

El componente de Arbor Cloud que se encuentra en las instalaciones, controlado por APS de Arbor Networks®, brinda visibilidad del tráfico que ingresa a su red, y provee detección y mitigación de ataques DDoS siempre activas. Ofrece una completa transparencia en las operaciones, lo que incluye ofrecer una visión dentro de los huéspedes bloqueados e incluso dentro de los paquetes, lo cual provee la flexibilidad que las empresas necesitan para modificar las contramedidas de ataque y los umbrales. A diferencia de otras soluciones dispares contra DDoS, el dispositivo APS presente en las instalaciones puede "hacer una señal de Cloud" a Arbor Cloud para que se prepare y comience a depurar el tráfico cuando los volúmenes alcanzan un umbral específico de ancho de banda. Cloud Signaling reduce de forma significativa el tiempo para mitigar los ataques y así asegura que usted esté protegido incluso si consume todo el ancho de banda.

Por medio de la protección en capas, Arbor brinda una solución de protección contra DDoS integral y líder en la industria para su negocio.

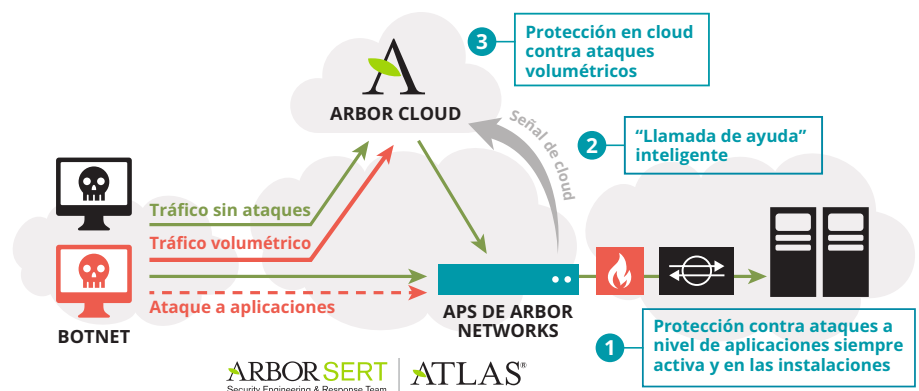


Figura 1

La combinación totalmente integrada de 1) APS en las instalaciones para protección contra ataques a nivel de aplicaciones siempre activa y en línea; 2) la Cloud Signaling inteligente que le indica a 3) Arbor Cloud para que detenga los ataques más grandes, todo continuamente equipado con la inteligencia de amenazas global de ATLAS/ASERT, ofrece la solución de protección contra DDoS más completa de la industria.

ARBOR SECURITY ENGINEERING & RESPONSE TEAM (ASERT)

ASERT es un equipo de categoría internacional integrado por investigadores de seguridad, con acceso a más de 120 Tbps de tráfico de Internet global en tiempo real para análisis. ASERT usa una sofisticada combinación de recopilación de datos de ataques, información de los socios y herramientas de análisis para encontrar y analizar amenazas de Internet incipientes, así como para crear defensas específicas a fin de protegerlo de los ataques más sofisticados y avanzados.

ASERT les brinda a los clientes inteligencia global por medio de Resúmenes de Amenazas semanales que están disponibles en el portal de Arbor Cloud. La siguiente información puede verse en el portal:

- Mapa de amenazas globales
- Resúmenes de amenazas (Arbor Cloud) —datos sobre informes posteriores a incidentes— contextualizados y específicos del cliente
- Fuentes principales de amenazas
- Índice de amenazas
- Principales ataques de Internet



The Security Division of NETSCOUT

Sede corporativa

76 Blanchard Road
Burlington, MA 01803 EE. UU.
Llamada gratuita en los
EE. UU.: +1 866 212 7267
Tel.: +1 781 362 4300

www.arbornetworks.com

Ventas en Latinoamérica

Brasil
Tel.: +55.11.4380.8035
brasil@arbor.net

México, Caribe y América Central
Tel.: +52.55.4624.4842
mxcca@arbor.net

América Latina del Norte
Tel.: +57.1.508.7099
nola@arbor.net

América Latina del Sur
Tel.: +54.11.5218.4007
sola@arbor.net

©2016 Arbor Networks, Inc. Todos los derechos reservados. Arbor Networks, Arbor Networks logo, ArbOS, Cloud Signaling, Arbor Cloud, ATLAS y Arbor Networks son marcas registradas de Arbor Networks, Inc. Todas las demás marcas pueden ser marcas comerciales de sus respectivos propietarios.

DS/ACENTERPRISE/ES/1016-LETTER

Depuración de tráfico eficiente, a demanda y basada en cloud

Cuando hay un ataque, la velocidad y la agilidad son fundamentales para la continuidad del negocio. En el caso de un ataque volumétrico, APS en las instalaciones sirve como la primera línea de defensa que detecta la aproximación del ataque hacia su capacidad de ancho de banda, y que le indica a Arbor Cloud para que se haga cargo. Arbor Cloud cambia la ruta del tráfico entrante hacia uno de los cuatro centros de depuración globales de Arbor para realizar una mitigación basada en cloud. Juntos, los centros de depuración tienen más de 1 Tbps de capacidad de mitigación de DDoS a su disposición. Cuando esto ocurre, el Centro de Operaciones de Seguridad (SOC) de Arbor Cloud, que está en funcionamiento constante, trabaja a la par de sus equipos de seguridad/TI para bloquear rápidamente el tráfico de DDoS malicioso al tiempo que hace que todo el tráfico legítimo regrese al data center.

Arbor Cloud provee capacidad global de depuración IPv4 e IPv6, y puede controlar los ataques más grandes y complejos que amenazan la disponibilidad de recursos y activos esenciales.

Especificaciones de Arbor Cloud

CENTRO DE OPERACIONES DE SEGURIDAD DE ARBOR CLOUD

América del Norte (Sterling, VA)

UBICACIONES DE LOS CENTROS DE DEPURACIÓN BASADOS EN CLOUD	OPCIONES DEL PAQUETE
Depuración en cloud combinada > 1 Tbps: • Costa Este (Ashburn, VA) • Costa Oeste (San Jose, CA) • Europa Central (Amsterdam, NL) • Asia (Singapur)	• Precio basado en tráfico limpio • Mitigación = lapso de 72 horas de uso • Sin tarifa de configuración para provisión estándar • Todos los precios son mensuales, a menos que se indique lo contrario

OPCIONES DE PROVISIÓN DEL SERVICIO

- **Arbor Cloud Connect:** brinda soporte en espera para mitigación en cloud en caso de un ataque
- **Arbor Cloud Essentials:** brinda soporte en tiempo real para mitigación hasta 12 veces por año
- **Arbor Cloud Essentials+:** soporte ilimitado en tiempo real para mitigación en cloud

PAQUETE DE SERVICIO FLEXIBLE

Opciones basadas en tráfico limpio:	Incluye:
• 100 Mbps • 500 Mbps • 1 Gbps • 2 Gbps • 4 Gbps • 8 Gbps • 10 Gbps	• 12 mitigaciones por año • BGP: protección 1/24 con 1 ubicación de regreso (GRE) • DNS: 5 nombres de host protegidos • Alerta y monitoreo de Cloud Signaling • Informes de amenazas ASERT, análisis y advertencias de ataques • Nivel 1, 2 y 3 de servicios de soporte continuo • SLA "hora de mitigar" de Arbor

PAQUETE DE SERVICIO DE RETENCIÓN

Opciones basadas en tráfico limpio:	Incluye:
• 100 Mbps • 500 Mbps • 1 Gbps	• Tarifa de suscripción mensual baja • Incluye 1 mitigación por año (las mitigaciones adicionales se cobran) • BGP: protección 1/24 con 1 ubicación de regreso (GRE) • DNS: 5 nombres de host protegidos • Alerta y monitoreo de Cloud Signaling • Informes de amenazas ASERT, análisis y advertencias de ataques • Nivel 1, 2 y 3 de servicios de soporte continuo • SLA "hora de mitigar" de Arbor

LAS OPCIONES ADICIONALES INCLUYEN

Opciones DNS:	Opciones BGP:
• Host adicional • Certificado SSL (por certificado) • Cambio/configuración de emergencia (única vez)	• Extremo adicional de túnel GRE • Protección 24/adicional • Conexión directa a uno o más centros de depuración de Arbor Cloud