



DIGITAL THREAT PROTECTION

Proteja su marca contra phishing y amenazas externas

Los ataques online que suplantan la identidad de compañías, marcas y empleados son cada vez más frecuentes. Estos ataques ponen en riesgo la información sensible de los clientes y afectan la confianza y lealtad en una organización, lo cual resulta en pérdidas financieras.

Appgate ayuda a las compañías a desarrollar una estrategia proactiva de protección contra amenazas digitales externas. Nuestro enfoque único descubre y elimina amenazas sin importar el tamaño de su población de usuarios, reduciendo drásticamente las ganancias criminales mientras disuade futuros ataques. Así, las compañías pueden enfocarse en el futuro, no en el miedo al fraude.

Digital Threat Protection Interrumpe y Disuade Ataques

Continuamente analiza y monitorea una amplia gama de canales, como email, web y redes sociales, con integración personalizada de reportes DMARC y fuentes externas de información.

Detección e inteligencia únicas en su tipo

Ágilmente detecta y confirma evidencia de phishing y otros ataques mediante algoritmos de clasificación patentados basados en machine learning.

Veloz desactivación de ataques

Rápidamente elimina amenazas identificadas antes de que sus clientes o empleados se enteren de su existencia

Conveniente adopción

El servicio brinda una fácil instalación sin necesidad de un dispendioso proceso de integración o inversión de recursos adicionales.

Detenga el fraude vía email

Bloqueo de afectación de correos corporativos, fraudes vía email y dominios falsos antes de que sus empleados y clientes se vean afectados.

BENEFICIOS:

Detección e informes únicos para alertar a las organizaciones sobre qué usuarios se vieron comprometidos por un ataque.

Encuentra y confirma rápidamente evidencia de phishing y otros ataques a escala utilizando clasificaciones patentadas de aprendizaje automático.

Elimina las amenazas identificadas ante de que los clientes o los empleados se dan cuenta de ellos.

Un servicio llave en mano significa una configuración simple, no se requiere integración y una inversión mínima de recursos.

LOS DATOS

97%

de los usuarios a nivel mundial no pueden identificar emails de phishing.¹

Los negocios pierden **USD \$5.3 MIL**

MILLONES debido a emails comprometidos.²

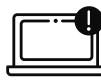
A la mayoría de compañías Fortune 500 les tomó **146 DÍAS** para detectar ciberataques.³





Detección temprana de phishing

Total cobertura de la web, las redes sociales y el canal de email para detectar ataques de phishing, incluso antes de que sean lanzados.



Monitoreo de dominios y perfiles sociales usados para suplantación

Ánalisis de redes sociales y registro de dominios para identificar perfiles falsos, menciones maliciosas de marca y dominios similares que busquen suplantar compañías legítimas y comprometer la información de los clientes.



Escaneo de la Dark Web en busca de tarjetas robadas/ comprometidas

Nuestra solución de monitoreo de amenazas penetra la restringida zona de la Dark Web y detecta tarjetas crédito/ débito comprometidas para mitigar proactivamente el impacto de las brechas.



Aprendizaje Automático Impulsado por la Inteligencia Humana

Aproveche el aprendizaje automático para anticipar patrones de URL de phishing, configuración automática a medida que evolucionan las estrategias de los atacantes y sitios de phishing en la lista negra al instante. Nuestro equipo de agentes obtiene rápidamente los sitios que alojan ataques y los derriba.



Protección contra aplicaciones móviles falsas

Detección y eliminación de aplicaciones no autorizadas que imitan marcas legítimas en las tiendas de terceros. Esto reduce el riesgo de que sus clientes inadvertidamente descarguen aplicaciones impostoras.



Protección contra el fraude vía email

La afectación de emails corporativos y el phishing dirigido a los consumidores están en su nivel más alto. Obtenga visibilidad de quién envía emails entre empresas e implemente una política que bloquee mensajes enviados desde fuentes no autorizadas.



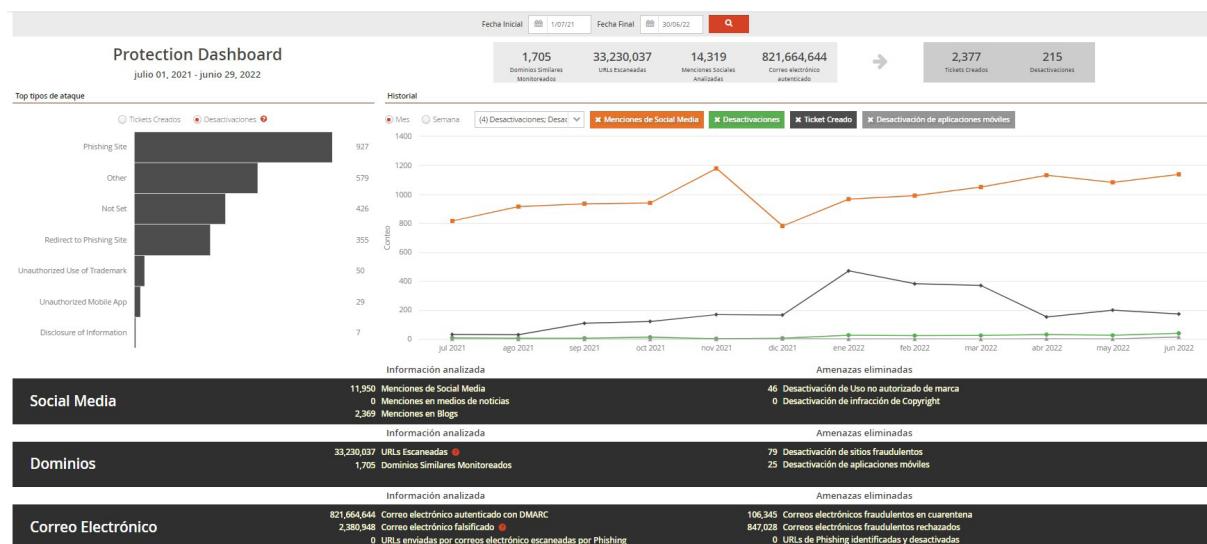
Completos reportes

El portal en la nube ofrece visión en tiempo real de los componentes de la estrategia de protección contra amenazas digitales de una compañía. La consola muestra datos sobre amenazas clasificados por fuente, categoría y estado de eliminación. Los usuarios pueden definir alertas, crear gran variedad de reportes personalizados en formato físico u online y solicitar eliminaciones. Los datos pueden ser fácilmente integrados con otros sistemas mediante API REST.



24/7/365 Appgate SOC

Nuestro equipo de agentes examina continuamente nuestro vasto depósito de fuentes de datos de amenazas para posibles ataques, se comunican con los ISP para eliminar el contenido malicioso de la web y documenta su trabajo paso a paso en el portal de clientes de Appgate



Sobre Appgate

Appgate es la empresa de acceso seguro. Potenciamos la forma en que las personas trabajan y se conectan proporcionando soluciones diseñadas específicamente sobre los principios de seguridad Zero Trust. Este enfoque de seguridad definido por las personas permite conexiones rápidas, simples y seguras desde cualquier dispositivo y ubicación a las cargas de trabajo en cualquier infraestructura de TI en entornos híbridos, locales y en la nube. Obtenga más información en appgate.com

1 <http://securityaffairs.co/wordpress/36922/cyber-crime/study-phishing-emails-response.html>

2 <https://www.ic3.gov/media/2017/170504.aspx>

3 <http://www.securityweek.com/breach-detection-time-improves-destructive-attacks-rise-fireeye>