appgate

# DETECT SAFE BROWSING

## Transacciones seguras en cualquier dispositivo

**Identificar y eliminar archivos maliciosos ya no es suficiente para detener el malware financiero; la gran mayoría de los dispositivos ya están infectados, y todos los días llegan nuevas amenazas.**

Detect Safe Browsing adopta un enfoque de seguridad diferente. Al interrumpir la recopilación de credenciales y la comunicación externa que utiliza el malware para hacerse cargo de las cuentas y retirar los ataques, garantiza que incluso los dispositivos comprometidos puedan continuar realizando transacciones seguras.

### Detecta y detiene las infecciones de malware

Alerta a los equipos de seguridad sobre infecciones de malware al analizar todos los procesos que se ejecutan en los dispositivos y los protege contra ataques de malware al bloquear las conexiones a los servidores de comando y control. Utiliza tecnología avanzada de identificación clientless para reconocer instantáneamente las inyecciones de códigos maliciosos en las páginas transaccionales de su sitio web.

### Utiliza inteligencia de amenazas en tiempo real

Nuestro equipo del Centro de Operaciones de Seguridad 24-7 analiza la inteligencia que recopila Detect Safe Browsing de más de 270 millones de terminales y cientos de organizaciones globales, para adaptar la protección a cada interacción individual con el cliente.

### Previene la causa raíz del fraude al encontrar amenazas activas

Detiene las amenazas lo antes posible en el ciclo de vida del fraude y detecta con precisión lo que no se puede prevenir. De esta forma, los clientes pueden actuar frente a las amenazas más peligrosas antes de verse afectados por ellas. La función Clientless Malware Snapshot toma una captura de pantalla instantánea de cualquier página inyectada con malware para reducir el tiempo dedicado a las investigaciones y acelerar la respuesta.

### Mejora la experiencia del cliente mediante la reducción Interrupciones innecesarias

Reduce los desafíos de autenticación redundante, la verificación de transacciones y otras interrupciones que afectan negativamente la experiencia del cliente, brindando una solución de remediación proactiva para cuentas comprometidas.

### Descubre y detiene los ataques de phishing

Nuestra exclusiva solución de monitoreo de amenazas penetra en la zona remota del delito cibernético conocida como la web oscura, en busca de datos de tarjetas de crédito/débito comprometidos para mitigar de manera proactiva el impacto después de que se produzca una violación de la seguridad.

### Protege los datos confidenciales del usuario final

Identifica el envenenamiento de DNS que indica que se está produciendo un ataque pharming y bloquea la redirección a sitios web fraudulentos. Cifra las pulsaciones de teclas del teclado al navegador para que no puedan ser interceptadas.

### Defensa contra ataques Smishing en dispositivos Android

Proteja a sus usuarios finales de ser víctimas de una estafa de phishing dirigida a ellos a través de mensajes de texto SMS, un ataque conocido como Smishing. El SDK móvil de DSB analiza los mensajes de texto SMS en los teléfonos inteligentes de los usuarios finales en busca de enlaces en los que se pueda hacer clic, en busca de URL de phishing conocidas y URL que podrían ser nuevos ataques de phishing, al mismo tiempo que mantiene la privacidad del usuario final. Todas las URL detectadas se pueden revisar en el Portal de clientes de DSB, donde la institución puede confirmarlas como phishing o categorizarlas como confiables.

### Reduce el impacto operativo de las investigaciones de fraude

Calibre la tolerancia al riesgo en todos los canales mientras reduce el volumen de alertas y los falsos positivos, de modo que los esfuerzos contra el fraude puedan dirigirse de manera más eficiente a donde más se necesitan. La función innovadora y única del controlador de riesgos móvil restringe el acceso y la funcionalidad en función de factores tales como si un teléfono tiene jailbreak, está rooteado, infectado, conectado a Wi-Fi público y mucho más.



## DETECT SAFE BROWSING MOBILE

Protege tanto las aplicaciónes bancarias como la navegación móvil mediante la detección de malware y otros riesgos móviles.

Visibilidad completa

Implementación sencilla

MitM dirigido, superposición, pharming y protección contra ataques de aplicaciones reempaquetadas

Evaluación de riesgos de dispositivos y autenticación basada en riesgos

## DETECT SAFE BROWSING CLIENTLESS

Clientless detecta el malware que intenta manipular portales y sesiones en línea.

Malware dirigido, MitB, zero-day, MitM, and phishing attack detection

Identifica la inyección de código HTML en las páginas

Malware snaptchat como evidencia procesable

Detección de credenciales comprometidas

### Acerca de 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