Plan de éxito del servicio de análisis de malware

MAXIMICE EL VALOR DE SU SUSCRIPCIÓN AL SERVICIO DE ANÁLISIS DE MALWARE DE APPGATE

Introducción

El servicio de análisis de malware de Appgate es una herramienta confidencial y poderosa que puede mitigar el riesgo de amenazas basadas en malware, proporcionando un valor significativo a cualquier organización. Sin embargo, para obtener los máximos beneficios, es importante comprender cómo usar de manera efectiva su conjunto de características y hallazgos.

Con ese fin, este plan de éxito es un plan integral para ayudarlo a optimizar su inversión en ciberseguridad. Nuestro enfoque confidencial y personalizado ofrece servicios personalizados, conocimiento experto e información procesable para fortalecer su postura de seguridad, mitigar las amenazas cibernéticas y ayudarlo a alcanzar sus objetivos.

Para fortalecer sus defensas, los hallazgos de los informes de Análisis Rápido o Análisis Profundo del Servicio de Análisis de Malware deben integrarse completamente en sus métodos de protección de ciberseguridad. Eso significa incorporar los hallazgos en los flujos de trabajo diarios de sus analistas de seguridad. Todos los informes generados son estrictamente confidenciales y accesibles solo para Appgate y el personal autorizado de su organización. Para garantizar esto, Appgate requiere que los usuarios tengan direcciones de correo electrónico aprobadas asociadas con su organización.

Además, para obtener información continua sobre los ataques, su equipo debe enviar las muestras de malware que encuentren, a menos que puedan rastrearlas hasta el malware analizado anteriormente.

Suscripción

El servicio de análisis de malware de Appgate proporciona paquetes de suscripción flexibles diseñados para satisfacer las necesidades específicas de su organización. Las suscripciones incluyen Escaneo rápido, Análisis profundo y una combinación de ambos.

- Las opciones de escaneo rápido están disponibles en paquetes de 50 y 100.
- Las opciones de análisis profundo están disponibles en paquetes de 20 y 40 días.
- Las opciones combinadas de análisis rápido y profundo están disponibles en paquetes combinados de 10 y 3 y 50 y 10, respectivamente.

Los análisis tienen un plazo de 12 meses, a excepción del paquete combinado de Análisis Rápido y Profundo (10 y 3), que es de 60 días. Para la mayoría de las organizaciones, recomendamos encarecidamente una combinación de análisis rápido y profundo para aprovechar al máximo el servicio en términos de velocidad tiempo de respuesta y niveles más profundos de examen a través de un compromiso con el equipo de análisis de malware de Appgate.

Comienzo

Appgate trabajará con su punto de contacto principal designado para establecer el acceso al Servicio de Análisis de Malware. Appgate también solicitará un punto de contacto secundario, que puede actuar como respaldo. Ambos contactos se registrarán como clientes de Appgate. Dada la sensibilidad del servicio, informe a Appgate de cualquier cambio en las necesidades de acceso del usuario, incluido el aprovisionamiento o la revocación del acceso.

Una vez activadas las cuentas, los usuarios autorizados pueden enviar muestras de malware para su análisis y luego ver los informes históricos de su organización, almacenados en el panel del sistema. Cualquier restricción deseada en estas solicitudes debe ser administrada por su organización.

Inicio de sesión

Para iniciar sesión, los usuarios recibirán un correo electrónico de mas.no-reply@appgate.com con un enlace al sitio web e instrucciones. Los usuarios deben hacer clic en el enlace proporcionado en el correo electrónico y se les pedirá que ingresen su dirección de correo electrónico, creen una contraseña y configuren un segundo factor de autenticación. Esta capa adicional de seguridad garantizará que solo los usuarios autorizados puedan acceder a la información confidencial de su organización.

SU HOJA DE RUTA PARA RESILIENCIA DE LA CIBERSEGURIDAD

- **Acelere los resultados:** Los gerentes de éxito experimentados lo ayudan a ejecutar planes centrados en los resultados e identificar formas de fortalecer su postura de ciberseguridad con el servicio de análisis de malware de Appgate.
- **Habilite su SOC:** integre el servicio en los flujos de trabajo de operaciones de seguridad existentes para mejorar las capacidades de detección y respuesta a amenazas.
- **Investigación de malware:** Mejore su estrategia de defensa contra malware equipando a su equipo del Centro de Operaciones de Seguridad (SOC) con experiencia avanzada en análisis de malware y técnicas útiles.
- **Maximice su retorno de la inversión:** Obtenga una orientación sin precedentes sobre la gestión de amenazas de malware y la ejecución de programas para disfrutar plenamente de los beneficios del servicio de análisis de malware de Appgate.

Uso del servicio

Para obtener los mejores beneficios, los hallazgos del informe del Servicio de análisis de malware deben integrarse en el proceso analítico existente de su equipo.

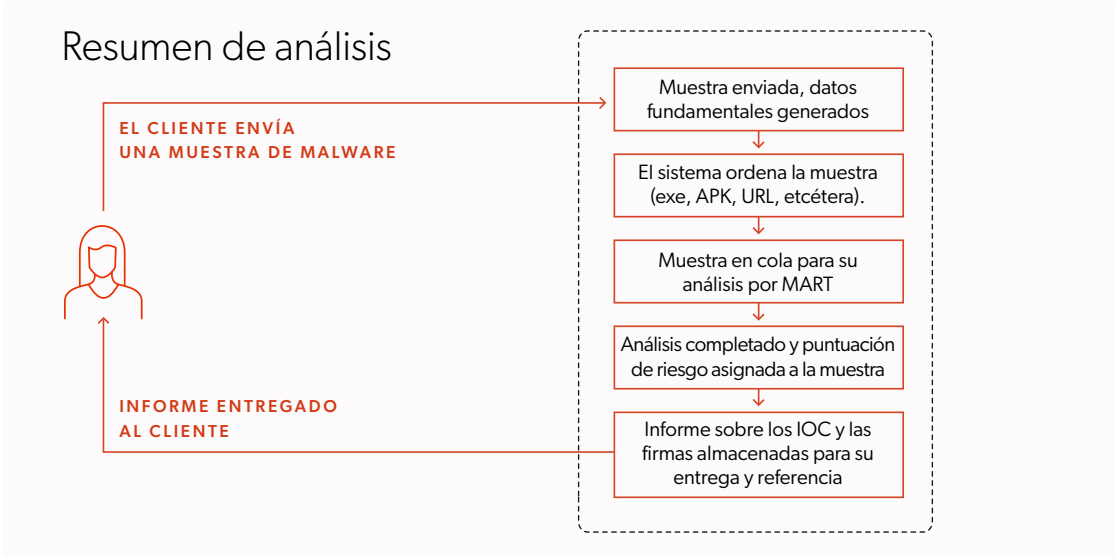
Cuando un miembro del equipo encuentra una muestra de malware sospechosa, debe seguir los procedimientos establecidos para identificarla y aislarla. Dependiendo de los protocolos de su organización, esto puede implicar escalar el problema a una capa analítica superior para su validación antes de enviar la muestra para su análisis.

Solicitud de una revisión

Dependiendo de su suscripción, el miembro del equipo debe iniciar sesión en el servicio y seleccionar Análisis rápido para comenzar a analizar el malware sospechoso. Este enfoque mantiene los costos bajos y entrega el informe y los indicadores de compromiso (IOC) asociados rápidamente.

Para enviar la muestra para el análisis rápido:

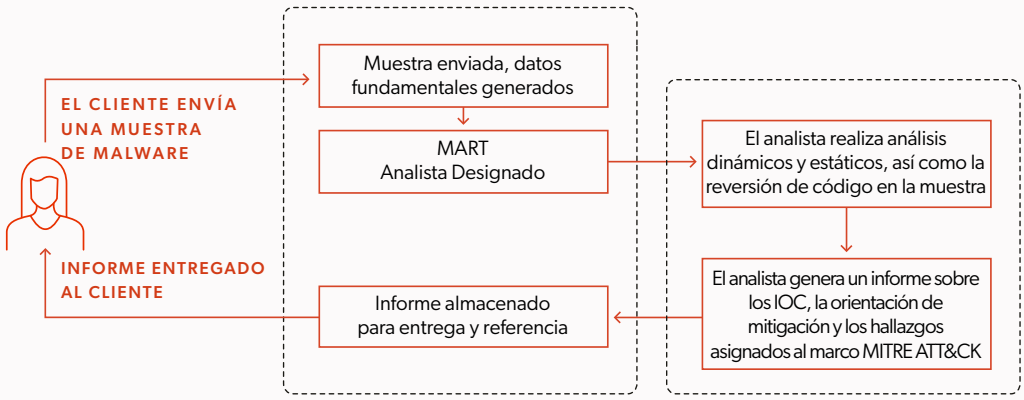
- Use la interfaz de Malware Analysis Service para enviar la muestra en un formato de archivo, hash o dirección URL.
- El servicio de análisis de malware analiza automáticamente los envíos de muestras de malware a través de una serie de procesos, herramientas y sistemas automatizados.
- Los análisis incluyen análisis estáticos y dinámicos, identificación basada en reglas y firmas, inteligencia de amenazas e informes IOC, detección de etiquetas dirigidas y más.
- Los informes de análisis rápido para la mayoría de las muestras de malware están disponibles en 30 minutos e incluyen detalles específicos sobre nombres de archivo, hashes, marcas de tiempo, tipos de archivos, servidores de comando y control (C2), cadenas útiles, imágenes y más.
- Puede iniciar sesión en el servicio para recuperar el informe o recibir el informe directamente por correo electrónico; El informe se entregará al correo electrónico de la persona que presenta la solicitud.
- El informe también se mantendrá en la lista de informes de su organización, para que usted y otros usuarios de su organización puedan revisar los informes en la interfaz.



Si necesita más información de la que se proporciona en Análisis rápido o está limitado a una suscripción solo a Análisis profundo, envíe el ejemplo a Análisis profundo. Como alternativa, considere la posibilidad de actualizar su suscripción para incluir Análisis profundo si actualmente solo tiene la opción Análisis rápido. El informe de análisis profundo siempre se enviará por correo electrónico al remitente y se almacenará en el repositorio de su organización. Para enviar la muestra para un análisis profundo:

- Use la interfaz del servicio de análisis de malware para proporcionar detalles específicos sobre el ejemplo y, a continuación, seleccione Análisis profundo.
- Nuestro equipo de análisis e investigación de malware aplicará ingeniería inversa al malware para descubrir detalles de ataque específicos del cliente.
- El equipo analiza meticulosamente la comunicación con los servidores C2 e identifica las funciones del malware, como la inyección de procesos, las inyecciones web y el cifrado. Un informe detallado de análisis profundo proporciona información completa, incluido el comportamiento de las amenazas y las tácticas, técnicas y procedimientos (TTP).
- Los informes de análisis profundos suelen entregarse en uno a tres días, pero pueden ser más largos dependiendo de la complejidad de la muestra presentada.
- El informe se enviará por correo electrónico directamente a la persona que presenta la solicitud.
- El informe también se guardará en la lista de informes de su organización para futuras referencias suyas y de otras personas dentro de su organización.

Descripción general del análisis profundo



Aprovechamiento de los resultados

Una vez que se complete el análisis y se entreguen los resultados, puede usar IOC para fortalecer su barrera de protección agregando reglas de detección/bloqueo según sea necesario. Además, si se confirma o se sospecha de un riesgo, aproveche los indicadores y las firmas para buscar malware de forma proactiva en su entorno.

Valor de seguimiento

Le recomendamos que evalúe los propios IOC, para verificar que le permiten detectar y mitigar amenazas; algunos COI son mucho más valiosos que otros. Nota: El valor del Servicio de análisis de malware radica en su confidencialidad, lo que garantiza que el malware descubierto no se divulgue a terceros. A medida que integra indicadores, puede ajustar su uso e identificar aquellos con el valor más alto y aquellos con el valor más bajo. Esta información debe incorporarse a sus capacidades de búsqueda y protección de amenazas.

Realice un seguimiento de los detalles específicos de sus esfuerzos para asegurarse de que los informes agreguen valor y que pueda demostrar su éxito a la empresa. Supervise el impacto de sus esfuerzos de búsqueda y cómo los informes amplían el alcance de sus herramientas de seguridad. Compartir estas historias de éxito fomentará una cultura de ciberseguridad más sólida en toda su organización y construirá una reputación de éxito.

Informes de uso

Appgate proporcionará informes mensuales (o informes bajo demanda a pedido) que detallan el uso del servicio de análisis de malware por parte de su organización. Estos informes le ayudarán a realizar un seguimiento del uso y a tomar decisiones informadas sobre cuándo renovar el servicio. Appgate le proporcionará un informe adicional cuando se encuentre dentro de los cinco informes automatizados o dentro de un mes de llegar al final de su contrato.

Interactúa con tu gerente de éxito del cliente

Los Gerentes de Éxito del Cliente de Appgate se asocian con usted para maximizar el valor de sus informes y proporcionar comentarios valiosos a Appgate. A medida que implementa el servicio, los registros semanales pueden facilitar una integración perfecta. Luego, las comprobaciones trimestrales garantizarán que aproveche al máximo los análisis proporcionados.

Proporcionar comentarios sobre el servicio de análisis de malware

¡Queremos saber de ti! Póngase en contacto con su Gerente de Éxito del Cliente o envíe información directa sobre nuestro Servicio de Análisis de Malware enviando comentarios a mas.support@appgate.com. Trabajamos constantemente para aumentar su valor mediante la adición de funciones que lo ayudarán a reforzar su resiliencia de ciberseguridad y profundizar su comprensión de las posibles vulnerabilidades.

Acerca de Appgate

Appgate protege los activos y aplicaciones más valiosos de una organización. Appgate es líder del mercado en acceso a la red Zero Trust (ZTNA) y protección contra el fraude en línea. Los productos de Appgate incluyen Appgate SDP para Universal ZTNA y 360 Fraud Protection. Los servicios de Appgate incluyen análisis de asesoramiento de amenazas y ZTNA implementación. Appgate protege a empresas y agencias gubernamentales de todo el mundo. Más información en appgate.com.

appgate