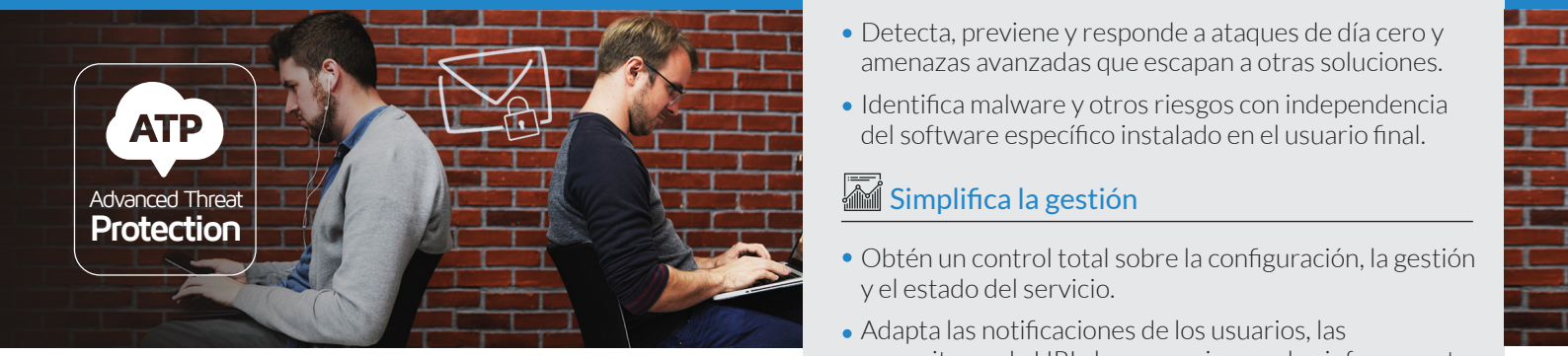
SPAMINA
Securing Digital Communications

ADVANCED THREAT PROTECTION

Detén las amenazas de malware de día cero, fraude al CEO, ransomware y otros riesgos antes de que lleguen a los usuarios



MALWARE Y RANSOMWARE

AMENAZAS BEC

VIRUS

VULNERABILIDADES DÍA CERO

Spamina Advanced Threat Protection (ATP) es una solución cloud para la detección, prevención y respuesta al malware día cero, ransomware, fraude al CEO, Business Email Compromise (BEC), suplantación de identidad personalizada, virus y otros ataques avanzados a través de correo electrónico.

Con su tecnología de sandboxing de última generación, Spamina ATP analiza dinámicamente archivos y URLs para descubrir, poner en cuarentena e identificar archivos adjuntos y enlaces maliciosos, incluso aquellos que utilizan las técnicas de evasión más sofisticadas.

Con Spamina ATP, desplegarás una potente defensa contra amenazas avanzadas que intentan a los usuarios y tus sistemas.

BENEFICIOS

Defiéndete del principal vector de ataque

- Analiza los emails, archivos adjuntos sospechosos, contenido y URLs maliciosas, antes de que se entreguen a los usuarios.
- Detecta, previene y responde a ataques de día cero y amenazas avanzadas que escapan a otras soluciones.
- Identifica malware y otros riesgos con independencia del software específico instalado en el usuario final.

Simplifica la gestión

- Obtén un control total sobre la configuración, la gestión y el estado del servicio.
- Adapta las notificaciones de los usuarios, las reescrituras de URL, las excepciones y los informes a tus necesidades.
- Logra una visibilidad completa de los registros de correo electrónico y los resultados del análisis.

Facilita el cumplimiento normativo

- Protege tus activos bloqueando las amenazas que buscan infiltrarse en tu infraestructura para perpetrar ataques avanzados multi-etapa.
- Facilita las auditorías y el cumplimiento normativo con informes y análisis detallados.
- Mantén un registro de todos los correos electrónicos analizados.

Aumenta la protección del usuario

- Alerta a los usuarios y bloquea automáticamente el acceso a sitios maliciosos.
- Prevén infecciones analizando los elementos sospechosos antes de que se entreguen.
- Detén el fraude del CEO y la suplantación de emails.
- Notifica a los usuarios cuando se analizan elementos para concienciarles y prevenirles ante posibles amenazas.

Análisis dinámico

Nuestra tecnología de análisis dinámico ofrece una visibilidad y análisis en profundidad para identificar y detener las amenazas que provienen de archivos adjuntos, anomalías en los encabezados, similitud de dominios y enlaces maliciosos. Spamina ATP detiene incluso amenazas que intentan evadir la detección o deshabilitar las capacidades de sandboxing.

Información y análisis detallado

Visualiza la actividad de las amenazas de forma detallada con informes inmediatos del estado de protección. Comprueba el volumen de correos electrónicos procesados, el porcentaje de malware, dominios o usuarios clasificados por tipología de malware, el estado del sandbox y todos los datos relevantes que necesitas.

Flexibilidad de implementación y gestión

Despliega la opción Dry-Run-Mode para medir la efectividad del sandboxing antes de una implementación más completa sin interrumpir los flujos de trabajo existentes. Adapta las defensas contra amenazas avanzadas a las necesidades de departamentos específicos. Desactiva el análisis de URLs para empleados en entornos controlados y habilita la notificación del usuario para respaldar campañas de concienciación.

Desarrollo europeo

Entendemos las necesidades de información y requisitos de los diferentes territorios. Nuestros centros de datos operan en áreas donde tu información privada está protegida por las más estrictas normativas en materia de privacidad y seguridad del mundo.

VALIDA LOS ARCHIVOS ADJUNTOS CON ANÁLISIS DINÁMICO

Los archivos adjuntos de correo electrónico se analizan mediante el sandboxing para garantizar que están a salvo de malware de día cero, ransomware y virus, antes de enviarlos a las bandejas de entrada de los usuarios. Spamina ATP analiza ejecutables, documentos, archivos, scripts y archivos multimedia.

Durante el ciclo completo del entorno de ejecución, Spamina ATP tiene visibilidad de los archivos a nivel de kernel para tener conocimiento de las interacciones entre el archivo sospechoso y el sistema operativo del servidor host. El sandbox de Spamina induce al malware a actuar para que se revelen su presencia e intenciones.

DEFIÉNDETE DE SUPLANTADORES DE IDENTIDAD

Algunas amenazas se basan en técnicas de ingeniería social para engañar a los usuarios a fin de que revelen datos confidenciales. Las amenazas de Business Email Compromise, fraude del CEO o estafas a través de correos de directivos suplantan la identidad del ejecutivo de la empresa y solicitan datos de nóminas, transferencias de fondos o pagos de facturas a los empleados. Spamina ATP escanea todos los correos entrantes e inspecciona los encabezados, datos de dominio y contenido para identificar los intentos de suplantación y bloquearlos.

ACTÍVALO SIN INTERFERIR EN EL FLUJO DE TRABAJO

Nuestra exclusiva opción "Dry Run Mode" te permite implementar Spamina ATP para un grupo de usuarios mientras preservas el flujo de trabajo. En este entorno limitado, tu equipo de seguridad puede evaluar la eficacia del sandboxing del correo electrónico, el tiempo de respuesta y otras capacidades. Durante este tipo de ejecución, se envía una copia del mensaje a la bandeja de entrada del destinatario y a Spamina ATP. Si se encuentra contenido malicioso, el mensaje queda marcado en cuarentena, permanentemente bloqueado o para revisión.

PROTÉGETE DE WEBS INFECTADAS

Spamina ATP URL sandboxing identifica ataques dirigidos a la navegación vulnerable a través de elementos maliciosos de Flash, JavaScript y ActiveX. Impide que los sistemas se infecten cuando los usuarios hacen clic en enlaces maliciosos que intentan instalar malware o están conectados a servidores C&C (Command & Control). Cuando un usuario hace clic en los enlaces, se analiza para detectar cualquier comportamiento sospechoso. Si es malicioso, Spamina ATP alerta al usuario y bloquea el acceso al sitio. La reescritura de enlaces es opcional y puede activarse por completo o por empresa, dominio o usuario.

MANTÉN INFORMADOS A LOS USUARIOS

Spamina ATP te permite elegir si notificar a los usuarios cuando se analizan correos electrónicos o URLs. Si activas la notificación al usuario, recibirán un mensaje de cortesía en el que se comunica que se está analizando un correo electrónico.

PRUEBA SPAMINA ADVANCED THREAT PROTECTION
spamina.com/es/evaluacion-gratuita

Acerca de Spamina

Spamina ofrece soluciones de comunicación empresariales innovadoras en las áreas de prevención de amenazas, gobernanza de datos y colaboración segura. Nuestros servicios en la nube proveen un entorno seguro de comunicación que garantiza a nuestros clientes continuidad del negocio, escalabilidad y optimización de costes. Las soluciones de Spamina están implantadas en más de 50 países y son distribuidas a través de una red de partners autorizados. Con sede central en Madrid (España), la compañía, que distribuye productos y servicios en más de 50 países, cuenta con oficinas en Madrid y Barcelona , Milán, Bogotá , México DF, Lima y Buenos Aires .

SPAMINA
Securing Digital Communications

www.micronet.com
+34 91 761 23 70

SIMPLIFICA LA GESTIÓN Y LA RESPUESTA A AMENAZAS

Spamina ATP está integrado en la consola de administración en la nube, lo que te permite controlar la configuración y el estado del servicio, y dar una respuesta fácil a las necesidades de auditoría y cumplimiento normativo. Los registros de correo electrónico guardan la actividad de todos los elementos analizados por el sandbox y si se reescribieron las URLs. Descarga los análisis del sandbox con un clic y define tu respuesta ante amenazas.

ACELERA LA IDENTIFICACIÓN DE MALWARE

Spamina ATP incluye un antivirus avanzado de primer nivel basado en firmas que identifica y detiene el malware oculto en los archivos adjuntos de emails. Identifica las familias de malware conocidas y sus mutaciones, así como las amenazas que cambian rápidamente. La monitorización y el análisis del comportamiento permiten una detección inmediata de las amenazas. Para minimizar los falsos positivos, el motor antivirus cuenta con listas actualizadas de ejecutables libres de malware.

APOYA LAS INICIATIVAS DE CUMPLIMIENTO NORMATIVO

Spamina ATP cumple con los requisitos esenciales de gobernanza de datos en cuanto a disponibilidad, seguridad, usabilidad e integridad de datos. Spamina ATP facilita las auditorías de seguridad y el cumplimiento de actividades regulatorias y de normativas como RGPD, PCI DSS, HIPAA, FINRA, PIPED y otras normativas locales. Las normativas de protección de datos requieren que las organizaciones mantengan un registro de todos los datos que incluyen información privada, y las organizaciones deben mantener actualizadas sus políticas, inventarios de mensajería y procedimientos. Spamina lo hace sencillo.

AMPLÍA LOS BENEFICIOS

Spamina ATP es una modalidad premium para los clientes de Spamina Cloud Email Firewall y Parla Secure Cloud Email. Puedes suscribirte a Spamina ATP para todos los dominios y usuarios o para dominios y usuarios individuales. Además, la integración de plataforma de Spamina permite la protección integral de correo electrónico y mensajería instantánea, la prevención de fugas de información, el cifrado, el archivado y la prevención de amenazas desde una única consola.