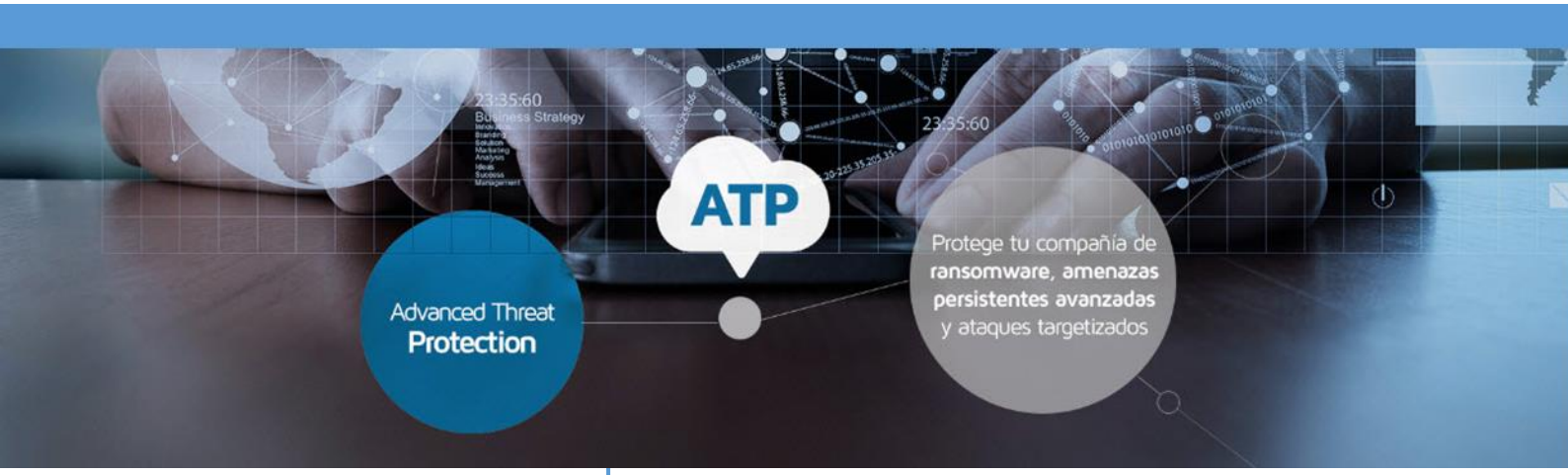

El **Proceso de Digitalización** de las compañías, está concienciando a los comités de dirección de la importancia de monitorizar el flujo de la información para **detectar y bloquear los ciberataques** en tiempo real.

Sin embargo, tan sólo el 51% de las grandes empresas*, tienen contratados servicios de seguridad avanzadas que les permita actuar proactivamente, evitando el acceso a la información y el robo de datos.

"La misión de Spamina es ir por delante de los hackers"

La mayoría de las organizaciones confían en técnicas de prevención estándar como son las soluciones antivirus, firewall y prevención de intrusiones. Sin embargo, estas herramientas son insuficientes, y los casos de filtraciones de datos muestran que **la detección en tiempo real debe mejorarse con la implementación de soluciones de protección avanzadas (ATPs)**. El principal beneficio de utilizar estas técnicas, es la habilidad de prevenir, detectar y responder a los nuevos y sofisticados ataques.

(*) 2017 Global State of Information Security Survey – CSO from IDC

SPAMINA
Securing Digital Communications

Advanced Threat Protection

Detección Proactiva y Eficaz de los Ciberataques

ATP
Advanced Threat Protection

La solución **Advanced Threat Protection** de Spamina (ATP) es una poderosa herramienta para **detectar, analizar y bloquear amenazas avanzadas en tiempo real.** La solución ATP, añade una capa una capa adicional de protección al correo electrónico por encima de los servicios antimalware y antispam.

La solución ATP de Spamina incorpora una combinación de tecnologías innovadoras:

- **Tecnología Sandboxing 2.0** para el análisis de ficheros y de URLs: La tecnología Sandboxing ofrece un mecanismo de seguridad para ejecutar programas/ficheros en un entorno controlado. La versión 2.0 ofrece mayor visibilidad de los estados internos del malware, mejorando la identificación de su comportamiento interno en tiempo real.
- **Advanced Premium Antivirus Engine (APAV)**: Un motor antivirus basado en firmas que permite detectar todos los patrones de malware conocidos.

Beneficios de la solución ATP:

- **Protección proactiva** de la información de la empresa.
- **Detección de malware** en el Sandbox de Spamina.
- **Control** de incidencias y ataques dirigidos.
- **Gestión desde una única consola** de administración.
- **Subscripción granular** para toda o parte de la empresa.
- **Integrable** con cualquier servidor de correo.

Cómo funciona la solución ATP de SPAMINA

El análisis por técnicas de Sandboxing se utiliza frecuentemente para comprobar en tiempo real emails o programas que no han sido verificados y puedan contener un virus, códigos o enlaces maliciosos, evitando así que estos afecten al dispositivo del usuario final.

La solución ATP de Spamina está desarrollada sobre **la segunda generación de tecnología sandboxing**, que aprovecha las facilidades ofrecidas por el **Complete run-time Environment Instrumentation** (CEI, Instrumentación detallada del entorno de ejecución) para realizar verificaciones exhaustivas de todos los objetos sometidos a análisis y sus partes.

Análisis de ficheros basado en sandboxing

La solución ATP de Spamina proporciona un **análisis dinámico de los ficheros adjuntos de los correos previo a su entrega a los usuarios finales**, asegurando que los ficheros se encuentran libres de virus, ransomware y cualquier malware hora cero.

La solución de ATP, realiza una detección efectiva de intentos de interferir con el sandbox o eludir el rastreo del programa analizado; y manipula e interactúa con el objeto analizado, y con su entorno, para provocar reacciones por parte del primero que pongan en evidencia su objetivo.

Análisis de código latente que permite identificar malware escondido en un programa, pendiente de ser activado. Este análisis permite detectar el código incluso si ha sido programado para activarse más adelante.

Tipo de ficheros analizados por el servicio sandbox ATP de Spamina:

- Ejecutables
- Documentos
- Archivos
- Scripts
- Multimedia

Análisis de URLs basado en sandboxing

La tecnología de sandboxing identifica ataques dirigidos a navegadores vulnerables. Típicamente, las campañas de malware y los ataques dirigidos, envían una URL en el cuerpo del correo, incitando al receptor a pinchar en él, momento en el que instala el malware en el dispositivo de la víctima, o se realizan acciones que permitan dejarlo vulnerable y explotarlo más adelante.

El análisis de URLs de Spamina reescribe los enlaces incluidos en el email para que en caso de que el destinatario pinche en alguno de ellos, cada uno sea verificado al momento. La URL es revisada en el sandbox y si se detecta algún comportamiento sospechoso, el usuario recibe una alerta y el acceso es bloqueado.

El director de TI puede definir las excepciones, es decir los dominios de confianza que pueden estar exentos de ser reescritos.

Tipo de URLs analizadas por el servicio sandbox ATP de Spamina:

- Flash
- JavaScript
- ActiveX