



CASO DE ESTUDIO GESTIÓN Y ASESORAMIENTO INMOBILIARIO

Anticipa acepta el reto de la Cyberseguridad

INDUSTRIA

Gestión y
asesoramiento inmobiliario

ENTORNO

- 630 endpoints protegidos por CylancePROTECT®

OBJETIVOS

- Implantar una solución eficaz contra las nuevas amenazas de malware zero-day
- Desplazar la tecnología anti-virus tradicional implantada en la compañía
- Asegurar los endpoints que contienen información confidencial de datos personales

SOLUCIÓN

- Desplegar CylancePROTECT para proteger los endpoints contra amenazas de ransomware con un alto grado de prevención
- Proceso de implantación sin impacto en la actividad de los usuarios

La empresa

Anticipa es una empresa de servicios de gestión y asesoramiento inmobiliario, especializado en ofrecer soluciones integrales para la gestión tanto de préstamos como de activos inmobiliarios, con más de 20 años de experiencia en el sector. Su misión es ofrecer soluciones personalizadas e innovadoras que se ajusten a las necesidades de sus clientes. Como servicer inmobiliario, Anticipa ofrece una gestión global especializada, avalada por un equipo humano con gran experiencia en el sector, unos recursos tecnológicos centrados en la eficiencia, y presencia en todo el territorio nacional.

El problema

Anticipa ya disponía de un antivirus de firmas tradicional, tanto en servidores como en las máquinas de usuario. Debido a la importancia de proteger la información, altamente confidencial de la compañía, era necesario disponer de una solución liviana con un porcentaje de detección de prácticamente el 100% de las amenazas actuales, incrementando el porcentaje de detección actual.

Desde Anticipa se necesitaba una solución eficaz contra las nuevas amenazas de malware surgidas en los últimos años, especialmente las amenazas por ransomware. A través de la motivación por encontrar una herramienta con un alto porcentaje de detección de las nuevas amenazas surgidas, se analizaron diversas tecnologías, entre ellas Cylance.

“Desde Anticipa, recomendamos Cylance por su alto grado de protección frente a nuevas amenazas y por la transparencia que ofrece frente al usuario.”



Actualmente, Cylance es la solución de seguridad en todos los endpoints de Anticipa, conviviendo únicamente con otra solución antivirus de firmas tradicional en los endpoints que ya se habían implementado en la infraestructura de la compañía, hasta fin de licencia.



El proceso

La implementación de Cylance se realizó con el objetivo de obtener una protección contra malware más robusta que la que se disponía por entonces. Por tanto, se decidió que Cylance conviviera con la otra solución antivirus de firmas por entonces implantada, sin esperar a finalizar las licencias.

A la hora de elegir Cylance como la solución de protección principal, se realizó un trabajo previo de pruebas y estudio, donde destacaron beneficios clave que ofrecía su tecnología. Uno de ellos es el alto grado de detección frente a nuevas amenazas, debido a su método de predicción mediante algoritmo matemático y sin la necesidad de firmas; lo que permite prevenir la ejecución de malware sin necesidad de conexión a internet y sin depender de actualizaciones permanentes. Otro de los grandes beneficios que ofrece es el bajo consumo de recursos de las máquinas donde se implanta, llegando a ser éste prácticamente imperceptible. La consola de administración es muy intuitiva, sencilla y limpia permitiendo clasificar y consultar las amenazas fácilmente.

Debido a que Cylance tiene un método de prevención innovador y eficaz, se decidió incorporarlo como primera medida de seguridad frente al malware.

La migración a Cylance fue muy sencilla y rápida. El despliegue a las estaciones de trabajo de los usuarios se realizó de manera centralizada, sin que estos sufrieran ninguna interrupción de su actividad. Además, se realizaron pruebas comparativas donde Cylance obtuvo un alto grado de satisfacción, en general. En estas pruebas, se ejecutaron cientos de muestras

de malware, algunas de ellas modificadas manualmente para hacerlas más difíciles de detectar, con el objetivo de analizar los porcentajes de detección de cada uno de los diversos productos comparados. También se tuvo en consideración el consumo de CPU de cada una de las soluciones analizadas, donde Cylance también obtuvo unos resultados muy satisfactorios.

Los resultados

Actualmente, Cylance es la principal herramienta de protección frente a malware en Anticipa, relegando a otras soluciones a complementar servicios secundarios únicamente. También se ha postergado la implantación de otras soluciones en otros puntos de la infraestructura como, por ejemplo, el malware distribuido por correo electrónico, ya que Cylance mitiga en gran parte el riesgo por malware en los dispositivos finales y servidores.

Durante este tiempo, se han detectado múltiples ficheros infectados con malware del tipo ransomware, siendo todos ellos detenidos y puestos en cuarentena por Cylance antes de su ejecución. Por otra parte, Cylance no requiere una gran carga de trabajo para su gestión por parte de los técnicos de seguridad que lo controlan, sin perder por ello efectividad.

Además, el mantenimiento de la herramienta es prácticamente nulo debido a su sistema de prevención, por lo que no requiere actualizaciones constantes. Cabe destacar que, desde que se implantó Cylance, existe una gran tranquilidad ante las nuevas amenazas surgidas y la gran cantidad de malware existente.

La migración no tuvo ningún impacto en los usuarios finales, ni durante ni después. La solución no consume recursos ni es intrusiva para los usuarios.

Cylance es una solución que funciona de manera totalmente transparente, sin avisar de actualizaciones o ventanas emergentes continuas; lo que ayuda al usuario y pasa totalmente desapercibida sin perder eficacia.

“Desde que Cylance se encuentra implantado, no se ha experimentado ningún incidente crítico en Anticipa.”