CASE STUDY

El sistema judicial de Chile se beneficia a través de la automatización y una mejor protección

La nueva tecnología de seguridad de los puntos finales de McAfee ayuda al sistema judicial chileno a combatir el ransomware, a aumentar la visibilidad, y a optimizar la gestión

Poder Judicial of Chile

Perfil del cliente
El Poder Judicial de Chile es una de las tres ramas del gobierno de la nación e incluye a la Corte Suprema, a 17 Cortes de Apelaciones, y a 465 tribunales de primera instancia.

Industria
Gobierno

Entorno de TI
Múltiples ubicaciones en todo Chile, con aproximadamente 6550 nodos de puntos finales que usan Microsoft Windows XP, Windows 7, y Windows 10

El Poder Judicial de Chile actualizó sus soluciones McAfee existentes, incluida la consola de gestión y la seguridad de puntos finales, con el objetivo de garantizar una detección más robusta y rápida y de prevenir los ataques de ransomware, para hacer más con menos recursos, y para obtener visibilidad de las amenazas y la postura de seguridad de los puntos finales.

Connect With Us

Matías Luengo es el administrador de sistemas que supervisa los equipos de TI y seguridad del Poder Judicial, que incluye un total de siete técnicos cuyo principal objetivo es administrar los requerimientos del usuario, asegurarse de que los sistemas estén operativos, y supervisar la consola de gestión McAfee® ePolicy Orchestrator® (McAfee ePO™). Implementando estrictos requisitos de seguridad autoimpuestos, los miembros del equipo tienen por práctica ejecutar periódicamente los controles de seguridad en las aplicaciones que usan los empleados y en los archivos de datos, a fin de asegurarse de que estén libres de infecciones que podrían comprometer las operaciones en red.

Los ataques de ransomware motivan la necesidad de actualizar a McAfee Endpoint Security

Recientemente, el organismo gubernamental se vio afectado por el ransomware WannaCry, que infectó a cientos de miles de puntos finales de Windows en organizaciones comerciales y gubernamentales en más de 100 países por todo el mundo. WannaCry se propaga rápidamente de un dispositivo a otro y bloquea archivos con un cifrado para que no sea posible acceder a ellos. Los responsables del ataque exigen un pago para desbloquear los archivos y amenazan con eliminarlos si no se paga el rescate.

Para el Poder Judicial, este fue un hecho de inseguridad grave que podría haber resultado en el cierre de determinadas operaciones a nivel interno y en la reducción de la disponibilidad de los servicios de los sistemas del tribunal que cada día usan miles de ciudadanos chilenos.

Luengo y su equipo actuaron rápidamente para impedir la amenaza a datos sensibles hospedados en los puntos finales de la organización,y dedicaron mucho tiempo y esfuerzo a bloquear manualmente el ataque para evitar que se propagara. Además, crearon y aplicaron nuevas políticas, algo que también se hizo manualmente. En aquel momento, el equipo usaba una versión antigua de la consola de gestión McAfee ePO, v. 5.3 y McAfee® VirusScan® Enterprise, v. 8.8.

Este hecho provocó que Luengo buscara mayores eficiencias a través de la automatización. Decidió actualizar las defensas de los puntos finales del Poder Judicial al software McAfee ePO, v. 5.9 y McAfee Endpoint Security, v. 10.5. En alianza con los ingenieros de ventas y técnicos de McAfee, Luengo y su equipo migraron McAfee Endpoint Security a 6550 nodos basados en Microsoft Windows en todo la organización, en menos de una semana.

Detección de incidentes más rápida y respuesta más efectiva a través de la automatización

Actualmente, el Poder Judicial ejecuta muchas de las defensas colaborativas incluidas en la solución—por ejemplo, defensa adaptativa avanzada contra amenazas, control web, firewall, y Data Exchange Layer (DXL). Esta poderosa combinación de tecnologías automatiza acciones y brinda conocimientos más sólidos y

Desafíos

- Proteger los puntos finales de los usuarios contra ataques de ransomware
- Mejorar la visibilidad de amenazas en toda la infraestructura informática
- Reducir los procesos manuales de creación y cumplimiento de políticas, los cuales requieren mucho tiempo
- Garantizar una experiencia del usuario segura para los empleados y los ciudadanos que utilizan los servicios del sistema judicial
- Simplificar y centralizar la gestión de la seguridad

Soluciones de McAfee

- McAfee Endpoint Security
- McAfee ePolicy Orchestrator software

profundos de las amenazas. Todo esto le permite al Poder Judicial contener amenazas de día cero como el ransomware, salvar al paciente cero, y prevenir infecciones en la red. DXL hace posible que múltiples tecnologías compartan inteligencia sobre amenazas y les permite a Luengo y a su equipo obtener inteligencia para detectar dónde se están produciendo las infecciones, para que puedan actuar rápidamente.

Luengo es quien está al mando del software McAfee ePO. Esta herramienta singular de gestión centralizada le permite controlar, investigar, y responder a las amenazas. La versión actualizada ha simplificado enormemente la administración de la seguridad y proporciona visibilidad completa de los puntos finales en toda la infraestructura del Poder Judicial. Luengo valora especialmente el panel fácil de usar con su interfaz gráfica. Ahora puede ver las "10 principales" amenazas responsables de las violaciones de seguridad más frecuentes y puede generar informes mensuales de gestión fácilmente. Hasta ahora, con base en las métricas que obtuvo de la consola de McAfee ePO, descubrió que McAfee Endpoint Security ha bloqueado o eliminado 232.000 amenazas en el Poder Judicial.

"Desde que hicimos la actualización a McAfee Endpoint Security, ya no tenemos que dedicar tiempo a bloquear las amenazas manualmente. Las nuevas herramientas detectan amenazas avanzadas y las bloquean automáticamente, y, en algunos casos, las eliminan completamente," destaca Luengo.

La transformación en la seguridad impacta positivamente en la TI y en los usuarios finales

Luengo también destacó que las nuevas herramientas McAfee también tuvieron otras ventajas. Antes de la implementación, el equipo de seguridad tenía problemas de conectividad, pero ahora, según explica Luengo, "Todo funciona sin inconvenientes." Además, la automatización ha reducido considerablemente la carga de trabajo sobre su personal, permitiéndoles que dediquen más tiempo a proyectos más estratégicos.

"Estas nuevas herramientas más ágiles tienen eficiencias que nos benefician a todos. Hemos reducido el tiempo que se dedica a configuración e implementación. Además, la detección de amenazas es más sencilla, rápida, y eficiente, gracias a las funciones de automatización incorporadas en McAfee Endpoint Security," explica Luengo.

Por otra parte, Luengo hace referencia a cómo el factor humano contribuye a la proliferación del malware. En el pasado, los usuarios sistemáticamente conectaban memorias USB infectadas con troyanos o virus a sus computadores, y esas amenazas, por lo general, no eran detectadas. Si bien los usuarios no han modificado esta conducta, con la ayuda de McAfee Endpoint Security y el cumplimiento de nuevas directivas a través del software McAfee ePO, el malware que introducen las memorias USB ya no es un problema.

Resultados

- Seguridad de puntos finales totalmente integrada con protección contra los devastadores ataques de ransomware
- Bloqueo automatizado de amenazas antes de que causen algún daño
- Gestión, información, y cumplimiento de directivas de seguridad simplificados e integrales
- Visibilidad con respecto a la postura de seguridad de los puntos finales a lo largo de todo el entorno
- Menor consumo de recursos informáticos y menos intervención manual
- Experiencia del usuario transparente, que optimiza la productividad y minimiza las interrupciones

Desde el punto de vista del usuario final, Luengo opina que la solución funciona de manera rápida y transparente. "Antes teníamos que comunicarnos con el usuario para hacer actualizaciones y entrar en forma remota a sus sistemas. Eso ya no es necesario—todo se hace en forma interna. Los usuarios pueden continuar siendo productivos y trabajar sin interrupciones," dice Luengo.

Implementación de funciones avanzadas en el futuro

Luengo y su equipo esperan con interés las funciones avanzadas integradas en McAfee Endpoint Security. Ya iniciaron una prueba de concepto (PoC) tanto para Dynamic Application Containment (DAC) como para Real Protect. DAC se basa en la automatización para contener amenazas de día cero cuando se detectan comportamientos maliciosos y evita que infecten los puntos finales. Real Protect usa el aprendizaje automático para clasificar las amenazas y aplica ese conocimiento para incrementar la eficacia de los procesos de detección y reparación. Actualmente, también están ejecutando una PoC para la integración de DXL y McAfee Threat Intelligence, que proporcionará inteligencia de la reputación de seguridad de los archivos y su contenido. DXL, una estructura de comunicación bidireccional, permite compartir esta inteligencia con otros componentes de seguridad y les permite detectar amenazas y evitar que se propaguen.

McAfee simplemente funciona

Luengo ha mantenido una larga relación con McAfee porque, como él mismo explica, "McAfee siempre encuentra las amenazas. ¿Por qué cambiar por otra herramienta?" Incluso llegó a realizar pruebas comparativas con un producto de la competencia y descubrió que, cuando se producía un incidente grave, McAfee era mucho más eficaz.

Luengo no tiene dudas de recomendarles a sus colegas en otros organismos gubernamentales una actualización a McAfee Endpoint Security, y de hecho, ya ha hablado con un colega en el Registro Civil de Chile acerca de sus múltiples beneficios.

"Estas nuevas herramientas más ágiles tienen eficiencias que nos benefician a todos. Hemos reducido la cantidad de tiempo destinado a configuración e implementación. Asimismo, la detección de amenazas es más sencilla, rápida, y eficiente, gracias a las funciones de automatización incorporadas en McAfee Endpoint Security."

—Matías Luengo, administrador de sistemas, Poder Judicial (Chile)

McAfee
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com