

Caso de éxito:

Gestión de Seguridad Global Facilitada para Proveedor de Servicios de TI Líder



Computer Sciences
Corporation

Perfil del cliente

MSSP global para Compañía de
Entretenimiento Global.

Industria

Entretenimiento.

Entorno de TI

200.000 endpoints en 70 países,
con "cada sabor" de sistema
operativo.

Desafíos

- Falta de visibilidad entre endpoints debido a múltiples entornos de seguridad con múltiples soluciones puntuales.
- Proteger una empresa vasta geográficamente y a múltiples clientes.
- Falta de gestión de seguridad centralizada.

Soluciones de McAfee

- Software McAfee VirusScan Enterprise
- Software McAfee VirusScan for Storage
- McAfee Host Intrusion Prevention for Servers
- Software McAfee ePolicy Orchestrator

Resultados

- Gestión, generación de informes y despliegue más fáciles gracias a un control centralizado.
- Visibilidad en tiempo real de todos los endpoints en el mundo.
- Detección más rápida de incidentes y corrección de amenazas.
- Ahorro de tiempo por una administración más eficiente y más efectiva.

Un ingeniero de seguridad de la información y su equipo defienden a este proveedor de servicios globales de TI y sus muchos clientes mucho más fácilmente y de forma más eficiente, gracias a la gestión centralizada del software McAfee® ePolicy Orchestrator® (McAfee ePO™) y la plataforma unificada de Intel® Security.

Como ingeniero de seguridad de la información de Computer Sciences Corporation (CSC), uno de los principales proveedores de servicios de TI, Christopher Sacharok gestiona la seguridad cotidiana de endpoint para las organizaciones de los clientes, y también soluciona los problemas de seguridad de otros equipos de consultores de CSC. Debido a que las brechas de datos importantes se han convertido en titulares nacionales, Sacharok ha observado que los clientes de CSC, desde grandes agencias del gobierno federal hasta pequeñas empresas, dedican cada vez más recursos a la seguridad.

"Lo bueno que han generado estas brechas públicas es que la seguridad se está volviendo una prioridad principal, como siempre debería ser", dijo Sacharok. "En CSC, nuestra primera prioridad es proporcionar un entorno seguro que proteja los datos, garantice la continuidad de los negocios, y cumpla con todas las regulaciones necesarias. Asegura que las operaciones de nuestros clientes se ejecuten tan eficientemente y efectivamente como sea posible viene después, pero la seguridad es lo primero".

Las Soluciones Puntuales Representan una Carga de Gestión

"Uno de los mayores desafíos que veo en la mayoría de los entornos de TI es el hacer que las soluciones de seguridad hablen unas con otras", afirmó Sacharok. "Operaciones de Seguridad tiene que gastar mucha energía intentando hacer que los datos de distintos productos de software y hardware propios y de terceros vayan a un lugar central donde se puedan gestionar de forma eficiente. También es extremadamente difícil gestionar y proteger los activos o estar en conformidad con PCI y otras regulaciones".

Con soluciones de varios proveedores protegiendo sus propios endpoints, CSC solía tener el mismo problema. Sin gestión central,

no había manera de ver el estado de la seguridad en todos sus 200.000 endpoints repartidos en 70 ubicaciones y cuatro continentes. El demostrar la conformidad con las reglamentaciones, que iban desde PCI e HIPAA hasta Sarbanes-Oxley, era difícil y requería mucho tiempo. También es beneficioso tener una consola única para ver productos de protección de endpoint similares para diferentes sistemas operativos. Una ventaja añadida es que los productos individuales que informan al software McAfee ePO son mejores que las protecciones estándares de SO.

Solución: Unified Security Platform with Central Management

Después de investigar las opciones de protección de endpoint, CSC recurrió a las soluciones de Intel Security para obtener una plataforma unificada de seguridad con gestión centralizada fácil de usar. CSC implementó el software McAfee VirusScan® Enterprise para proteger sus 200.000 endpoints en todo el mundo contra malware y spyware, y McAfee VirusScan for Storage para extender la protección hacia 18 dispositivos de almacenamiento conectados a la red. Además, la empresa desplegó McAfee Host Intrusion Prevention for Servers para proteger proactivamente cerca de 5.600 servidores contra ataques conocidos y nuevos de día cero, y McAfee Vulnerability Manager para detectar inmediatamente las vulnerabilidades del sistema.

Sin embargo, lo que distingue a estos productos, es la consola de gestión central del software McAfee ePO que viene incluido con cada uno de ellos y les permite ser gestionados desde una única pantalla común. "El software McAfee ePO sobresale en comparación con otras soluciones", dijo Sacharok, quien ha visto su cuota

"El software McAfee ePO sobresale en comparación con otras soluciones. Es una única tienda para nuestra protección de endpoint. Puedo ver todo lo que necesito para ver todos nuestros productos McAfee desde una consola única. Sus paneles fáciles de utilizar y funcionalidad incorporada hacen que todo - visibilidad, informes, despliegue, actualización, mantenimiento, toma de decisiones - sea mucho más fácil".

- Christopher Sacharok, Ingeniero de Seguridad de la Información de Computer Sciences Corporation

de Prueba de Conceptos para una amplia gama de productos de seguridad. "Es una única tienda para nuestra protección de endpoint. Puedo ver todo lo que necesito para ver todos nuestros productos McAfee desde una consola única. Sus paneles fáciles de utilizar y funcionalidad incorporada hacen que todo - visibilidad, informes, despliegue, actualización, mantenimiento, toma de decisiones - sea mucho más fácil".

Cómo Hace el Software McAfee ePO para que las Operaciones de Seguridad sean Más Fáciles y Eficientes

Además de Sacharok, otros siete integrantes de su equipo y dos administradores de seguridad en otros equipos de CSC confían en el software McAfee ePO para obtener una vista centralizada del estado de la seguridad a lo largo de todos los 200.000 Endpoints corporativos y de clientes. También dependen de él para elaborar informes - informes programados periódicamente para fines de conformidad y de consultas sobre la marcha. Sacharok y los otros se refieren a menudo a un número de informes listos para usar, incluyendo las principales amenazas para la organización interna, 10 principales equipos con detección de malware, y un listado de todos los nuevos incidentes de seguridad.

En promedio, la compañía observa 200 eventos únicos de amenazas cada 24 horas y 4.100 cada mes. "Para las operaciones diarias, los paneles intuitivos de McAfee ePO son simplemente lo mejor", afirmó Sacharok. "Puedo ver al instante si algún evento necesita mi atención y profundizar en los detalles. El software McAfee ePO me hace más eficiente y alivia muchos dolores de cabeza".

El equipo de Sacharok también utiliza el software McAfee ePO para analizar periódicamente, para detectar vulnerabilidades de seguridad, obtener las actualizaciones de software, y solucionar problemas o realizar actividades de corrección. Cuando otros equipos de seguridad de la información de CSC - el equipo de firewall, el equipo de gateway de correo electrónico, etc. - necesitan solucionar problemas de protección de endpoint, llaman al equipo de Sacharok. "Si tenemos que escribir una nueva regla de exclusión o actualizar DATs o HIPs, por ejemplo, o cada vez que ocurre un incidente de seguridad en la en la red inmediatamente somos capaces de detectar dónde y qué es lo que está ocurriendo en tiempo real y tomar las

medidas correctivas", dijo.

Ahorro de tiempo desde un Nivel Alto de Herramientas Integradas de Granularidad

Sacharok también menciona que la capacidad dentro del software McAfee ePO de utilizar un árbol de sistema y ordenar dinámicamente a un nivel muy granular es extremadamente útil. Él puede ver la información de estado de endpoint por continente, ciudad, edificio, o incluso piso, así que es fácil localizar exactamente donde corregir si es necesaria una intervención física. "Usted no puede ver ese el nivel de granularidad de gestión en muchas otras herramientas de seguridad", señaló Sacharok. "Sin duda brinda a Intel Security la ventaja".

Las herramientas de corrección integradas en el software McAfee ePO también facilitan operaciones de seguridad más eficientes. Por ejemplo, con el software, Sacharok puede transferir un endpoint directamente de una organización interna hacia una diferente, y aplicarle las políticas de dicha organización interna, o ejecutar un análisis de antivirus de alta prioridad. "Ser capaz de realizar muchos actos de remediación de forma remota mediante el software McAfee ePO también alivia la necesidad de disponer de un técnico de deskside y el subsiguiente grado de separación entre mi equipo y el usuario final", añadió Sacharok. "Menos tiempo en persona ahorra a Operaciones de Seguridad una gran cantidad de tiempo y recursos".

Un Fuerte Soporte y una Estrategia para el Futuro

Además de la tecnología de Intel Security, Sacharok y otros en CSC dependen del Intel Security Platinum Support. "Hemos quedado muy satisfechos con el nivel de soporte que recibimos", señaló Sacharok. "Cada vez que tenemos una pregunta, verificamos la base de conocimientos de soporte, y en raras ocasiones en que necesitemos hablar con alguien, la resolución siempre es muy rápida".

Caso de éxito

Justo como el software McAfee ePO destaca en la mente de Sacharok, también lo hace Intel Security en la compañía. "Cuando usted está buscando proveedores de seguridad, la estrategia está por encima de todo", explicó Sacharok. "El proveedor necesita obviamente tener un producto rentable que funcione bien, pero al final del día, el proveedor también debe tener una estrategia para brindar mejor que nadie, seguridad a su entorno. Intel Security tiene con mucho la más amplia visión y estrategia de seguridad de cualquier proveedor que he visto".

Sacharok se refiere a la estrategia de Intel Security de una arquitectura de seguridad abierta e interconectada, que simplifica el ciclo de vida de defensa contra amenazas para ayudar a las organizaciones a resolver más amenazas, más rápido y con menos gente. "En el futuro próximo, incrementar la integración de nuestras distintas soluciones sin duda, será fundamental para hacernos una compañía de seguridad más integral", dijo Sacharok. "Espero que Intel Security tenga un papel clave en este proceso".

