CASO PRÁCTICO

La revisión de la protección de endpoints contribuye a la innovación y fortalece el estado de seguridad

Una innovadora empresa mundial de transformación de procesos empresariales transforma sus propios procesos de seguridad con la ayuda de McAfee

Sutherland Global Services

Perfil del cliente
Empresa multinacional de transformación de procesos empresariales

Sector
Tecnología y servicios empresariales

Entorno de TI
Aproximadamente 50 000 endpoints en 16 países de seis continentes

Sutherland Global Services ayuda a más de 100 empresas del índice *Fortune 1000* en 16 países a redefinir y reconstruir los procesos empresariales para la era digital mediante análisis de datos y otras tecnologías, diseñar capacidades mentales, y conocimiento específico del sector. La empresa, con sede en Pittsford, Nueva York, invirtió en la transformación de su propia seguridad para endpoints, consiguiendo mejorar drásticamente su estado de seguridad global, además de ahorrar tiempo y dinero. Además, aprovechando el marco Open Data Exchange Layer (OpenDXL), la empresa está creando una defensa unificada en la que los distintos sistemas de seguridad trabajan de manera conjunta para respaldarse y fortalecerse entre sí.

Síganos

Protección contra la interrupción de la actividad y las fugas de datos

"Cada minuto que un sistema está fuera de servicio cuando un usuario de la empresa lo necesita nos cuesta mucho dinero", afirma Prashanth M J, responsable global de infraestructuras tecnológicas de Sutherland Global Services. "La interrupción de la actividad y las fugas de datos son un riesgo importante contra el que queremos protegernos. Trabajamos permanentemente para garantizar que disponemos de los controles para minimizar estos riesgos y permitirnos continuar ofreciendo soluciones y servicios personalizados a nuestros clientes".

Con aproximadamente 50 000 nodos que proteger, incluidos 1000 servidores, más de 80 centros de datos/distribución, y una red troncal digital distribuida por 16 países y seis continentes, minimizar los riesgos de seguridad es una tarea monumental que requiere muchas soluciones de seguridad. Conseguir que los distintos sistemas y controles se comuniquen entre sí y compartan inteligencia sobre seguridad para mantener protegida toda la empresa es parte de la batalla permanente del equipo de infraestructura tecnológica.

Imperativo: partners estratégicos que apoyan la innovación

Con una empresa de semejante envergadura, Sutherland Global Services depende de la ayuda de partners estratégicos como McAfee. "Hemos desarrollado un alto nivel de confianza con McAfee porque siempre ha cumplido a la hora de satisfacer los requisitos empresariales, incluida la necesidad de innovación continua", explica Prashanth.

"La innovación es lo que mantiene a nuestra empresa viva y prosperando".

"Nuestros servicios innovan en la intersección entre empresa y tecnología, transformado procesos para hacer realidad el objetivo de nuestros clientes", añade Prashanth. "McAfee lanza continuamente soluciones que responden a los requisitos de nuestra empresa, por ejemplo, nos ayuda a cerrar la brecha entre la detección y las medidas correctoras, o a avanzar en nuestra transformación digital".

Creación de defensas unificadas aprovechando OpenDXL

Prashanth también alaba a McAfee por desarrollar OpenDXL, una iniciativa de la industria tecnológica para crear sistemas adaptables de soluciones interconectadas que se comunican y comparten información para tomar decisiones sobre seguridad precisas y en tiempo real. Gracias al uso de OpenDXL, Sutherland Global Services trabaja actualmente para integrar la solución de información de seguridad y administración de eventos (SIEM) no de McAfee de la empresa con su protección para endpoints de McAfee. La integración con el gateway web y el firewall de la empresa también está en la hoja de ruta OpenDXL de Sutherland.

"Veo un enorme potencial en OpenDXL", señala Prashanth. "Tenemos muchos productos de seguridad de distintos proveedores, todos operando en sus propios silos. Para crear una defensa unificada contra ciberataques, es muy importante que la inteligencia de un sistema pueda ser utilizada por otro".

Desafíos

- Proporcionar disponibilidad 24/7 a los usuarios de la empresa en todo el mundo
- Integrar las soluciones de seguridad para una ciberdefensa unificada
- Cumplir eficazmente las normativas, en particular en el caso de los sectores de la atención sanitaria y los servicios financieros

Soluciones de McAfee

- McAfee® Advanced Threat Defense
- McAfee® DLP Endpoint
- McAfee® Endpoint Encryption
- McAfee® Endpoint Security
- McAfee® Endpoint Threat Defense and Response
- McAfee® ePolicy Orchestrator®
- McAfee® File Integrity Monitoring
- Servicios profesionales de McAfee®
- McAfee® Threat Intelligence Exchange

La consolidación de la protección de endpoints disminuye los costos y aumenta el potencial de generación de ingresos

Para proteger sus endpoints en todo el mundo, Sutherland Global Services depende enormemente de la consola de administración central de McAfee ePolicy Orchestrator (McAfee ePO™). Gracias al software McAfee ePO, los administradores gestionan y supervisan múltiples productos y soluciones de McAfee —antivirus, prevención de la pérdida de datos en host, prevención de intrusiones en host, cifrado de endpoints, supervisión de la integridad de archivos, etc. —desde un solo panel.

"McAfee ePO [software] nos proporciona la ventaja para gestionar nuestra empresa sin problemas", afirma Prashanth. "Además, es tan fácil de utilizar que no tengo que emplear costosos ingenieros de seguridad de nivel 2 o 3".

En los últimos dos años, como parte de una actualización y transformación completas de su protección de endpoints, la empresa consolidó siete servidores del software McAfee ePO dispersos en uno solo. Hoy, la protección de todos y cada uno de los aproximadamente 50 000 endpoints se gestiona a través de una consola de McAfee ePO central dentro del centro de operaciones de seguridad de la empresa.

"Cuando retiramos del servicio activo los otros seis servidores de McAfee ePO [software], obtuvimos un ahorro inmediato", recuerda Prashanth.

"Además de reducir los costos de hardware y software, se desplomaron el consumo eléctrico del centro de datos y el tiempo dedicado al mantenimiento y administración. También hemos añadido una nueva función sin tener que incorporar personal y hemos liberado al personal para que dedique tiempo a actividades de mayor valor añadido.

"Por otra parte, la revisión de la protección de endpoints aumentó la disponibilidad de los sistemas en toda la empresa", añade Prashanth. "Una mayor disponibilidad aumentó nuestro potencial de generar ingresos adicionales".

La generación de informes de cumplimiento de forma más rápida y sencilla ayuda a elevar los niveles de cumplimiento por encima del 95 %

La consolidación en una consola central generó un enorme ahorro de tiempo en el área de cumplimiento, en particular en los sectores de la atención sanitaria y servicios financieros. "Con una consola central, la generación de informes de cumplimiento de normativas es ahora muchas veces más eficaz", afirma Prashanth. "Podemos proporcionar de forma rápida y sencilla paneles que están personalizados y contextualizados para los responsables de seguridad de las distintas zonas geográficas, clientes o sectores. Como consecuencias, es mucho más fácil generar los informes necesarios, y nuestro nivel de cumplimiento ha aumentado hasta niveles superiores al 95 %.

Resultados

- Reducción de la carga administrativa y los gastos en hardware y software
- Mayor disponibilidad de los sistemas
- Mayor potencial de aumentar la generación de ingresos
- Simplificación de la administración de la protección de endpoints, liberando administradores en todo el mundo
- Defensa multicapa más robusta contra el malware, incluidas las amenazas de tipo zero-day
- Informes de cumplimiento muchos más eficaces en todo el mundo
- Aumento de los niveles de cumplimiento por encima del 95 %
- Mayor rapidez para detectar y responder a amenazas

La protección multicapa y las amenazas compartidas fortalece la defensa frente a las amenazas de tipo zero-day

La migración a McAfee Endpoint Security desde McAfee® VirusScan® Enterprise fue otro elemento fundamental de la renovación de la protección de endpoints de la empresa. "Sabíamos que era el momento de disponer de antimalware robusto de próxima generación con capas adicionales de protección y, afortunadamente, McAfee tenía lo que necesitábamos", explica Prashanth. "Estábamos especialmente interesados en utilizar la Contención dinámica de aplicaciones para poner en cuarentena los archivos desconocidos y la funcionalidad de aprendizaje automático Real Protect para analizar los archivos personales de forma inmediata".

La empresa también migró a McAfee Endpoint Security para aprovechar McAfee Threat Intelligence Exchange, que almacena inteligencia sobre amenazas global y local actualizada continuamente y la comparte bidireccionalmente a través de Data Exchange Layer (DXL) a todos los sistemas conectados con DXL. McAfee Endpoint Security se conecta a DXL de manera predefinida. "Por lo tanto, cuando uno de los endpoints encuentra un archivo malicioso, o un centro de investigación mundial encuentra una nueva amenaza de tipo zero-day, en lugar de tener que esperar a que estén disponibles las firmas y que las distribuya un administrador, todos nuestros endpoints reciben automáticamente la información inmediatamente", explica Prashanth.

Sutherland Global Services contrató los servicios profesionales de McAfee para ayudar a llevar a cabo una migración fluida y escalonada a McAfee Endpoint Security, que tuviera cero impacto en la disponibilidad de los sistemas para los usuarios empresariales en todo el planeta. La migración de todos los endpoints a McAfee Endpoint Security incluía el módulo Advanced Threat Protection de la solución, que contiene las tecnologías Contención dinámica de aplicaciones y Real Protect. La empresa también desplegó la estructura DXL y McAfee Threat Intelligence Exchange a través de su red.

Aceleración de la respuesta a incidentes

Como parte de su transformación de la protección de endpoints, Sutherland Global Services también implementó un appliance McAfee Advanced Threat Defense para el análisis en entorno aislado dinámico y estático. "McAfee Advanced Threat Defense nos ayuda en dos aspectos importantes", señala Prashanth. "En primer lugar, cuando nuestros endpoints encuentran un archivo desconocido y lo ponen en cuarentena, el archivo se envía directamente al appliance de McAfee para su análisis en profundidad. Una vez analizado, el resultado se comparte, a través de [McAfee Threat Intelligence Exchange] en toda la empresa. De esta forma, hemos capturado un buen número de archivos maliciosos y protegido de manera proactiva todos nuestros endpoints".

"Nuestros servicios innovan en la intersección entre empresa y tecnología, transformado procesos para hacer realidad el objetivo de nuestros clientes". "McAfee lanza continuamente soluciones que responden a los requisitos de nuestra empresa, por ejemplo, nos ayuda a cerrar la brecha entre la detección y las medidas correctoras, o a avanzar en nuestra transformación digital".

—Prashanth M J, vicepresidente sénior, responsable global de infraestructuras tecnológicas, Sutherland Global Services

"En segundo lugar, McAfee Advanced Threat Defense acelera nuestro proceso de investigación de indicadores de peligro", continúa Prashanth. "En el pasado, por cada indicador de peligro desconocido, teníamos que enviar una muestra hash al equipo de soporte de McAfee y esperar a recibir la información sobre si era malicioso. Con McAfee Advanced Threat Defense, ahora podemos analizar los indicadores de peligro nosotros mismos y determinar más rápidamente la medida que conviene adoptar".

Además, la empresa está en el proceso de añadir McAfee Endpoint Threat Defense and Response para impulsar su capacidad de cazar amenazas de forma proactiva. "Queremos ser más ofensivos, no solo defensivos", añade Prashanth. "Espero que McAfee Endpoint Threat Defense and Response sea una de las herramientas más importantes de nuestro arsenal para proteger frente a amenazas durmientes que podrían estar en nuestro entorno esperando a activadores... Todo se reduce a acelerar la respuesta. Las medidas adecuadas son inútiles si no se responde con suficiente rapidez".

Para estar preparados para el futuro, hacen falta más que productos

"Nuestra alianza con McAfee ha sido extremadamente fructífera, y me ha ayudado a tener la seguridad de que nuestros sistemas están protegidos y listos para el futuro", afirma Doug Gilbert, director de tecnología (CIO) de Sutherland Global Services. "La elección de uno u otro partner no depende tanto de un producto o productos, sino de todo el ecosistema. Con McAfee, contamos con personas que se unen a nosotros, no solo para vender productos, sino también para ayudarnos a diseñarlos, desplegarlos, mantenerlos y optimizarlos".

En el futuro, cuando Sutherland Global Services aumente su migración a la nube y continúe con su transformación digital en marcha, McAfee continuará jugando un papel fundamental. Prashanth menciona los nuevos productos de McAfee® MVISION como otro ejemplo de innovación que sin duda ayudará a la empresa: "El panorama de amenazas es tan complicado que es necesario trabajar de forma conjunta. McAfee nos proporciona tecnología [adecuada]. Nosotros aportamos el dominio del negocio [conocimiento]. 'Together is Power' es la forma adecuada de avanzar".

"Nuestra alianza con McAfee ha sido extremadamente fructífera, y me ha ayudado a tener la seguridad de que nuestros sistemas están protegidos. La elección de uno u otro partner no depende tanto de un producto o productos, sino de todo el ecosistema. Con McAfee, contamos con personas que se unen a nosotros, no solo para vender productos, sino también para ayudarnos a diseñarlos, desplegarlos, mantenerlos y optimizarlos".

—Doug Gilbert, director de tecnología, Sutherland Global Services

McAfee
Together is power.

Av. Paseo de la Reforma No.342 Piso 25
Colonia Juárez, México DF
C.P. 06600
+52-55-50890250
www.mcafee.com/mx