

Microsoft

RSA® Data Loss Prevention Suite ayuda a un líder en tecnología a detectar información confidencial

Aceleración

El producto RSA Data Loss Prevention (DLP) Datacenter ayuda a Microsoft a acelerar el cumplimiento de los requisitos regulativos y obtener conocimiento acerca de las tendencias de la información, sin interrumpir las operaciones del negocio y los recursos de TI. RSA DLP Datacenter le brindó a Microsoft el performance, la escalabilidad y la precisión necesarios para detectar y remediar la información confidencial en miles de espacios compartidos y sitios Microsoft SharePoint®.

EN RESUMEN

Desafío para el negocio

- Seguir el cumplimiento de regulaciones Sarbanes-Oxley e industria de pagos con Tarjeta (PCI)
- Asegurar la propiedad intelectual, como el código fuente, los planes estratégicos y la información operacional

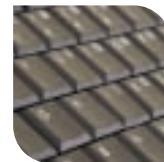
Solución:

- RSA® Data Loss Prevention Datacenter (antes Tablus Content Sentinel), gracias a su arquitectura distribuida y capacidades de análisis, permite analizar toda la información almacenada en el grupo completo de espacios compartidos y sitios SharePoint.

Resultados

- El rápido análisis de 12TB de información del file system y 120.000 sitios SharePoint hicieron posible la continua detección de contenido
- Dado que la tasa de falsos positivos es inferior al 1%, saben que los incidentes registrados son genuinos

Para una corporación internacional como Microsoft, el mayor desafío que enfrenta al impedir las violaciones de datos y cumplir con las regulaciones sobre privacidad no es un problema técnico de protección de datos, ya que la empresa cuenta entre su personal a varios de los líderes mundiales de TI. El problema es, en realidad, la dispersión del contenido. “Antes que nada, sabíamos que teníamos que ubicar nuestra información confidencial y medir el cumplimiento



de las políticas que ya regían en el lugar”, explica Olav Opedal, administrador del programa de seguridad de Microsoft. “El problema era que contábamos con aproximadamente 30.000 espacios compartidos que contenían casi 12 terabytes de información y más de 120.000 sitios SharePoint que necesitaban ser analizados y escaneados. ¿Cómo se logra hacerlo a corto plazo y sin causar una gran interrupción a las operaciones del negocio y los recursos de TI? Este era el propósito detrás de nuestro proyecto Information Classification and Data Handling”.

DESAFÍO PARA EL NEGOCIO

Como procesador de nivel 1 de tarjetas de crédito, Microsoft claramente tuvo que abordar el estándar de seguridad de datos (DSS) de la industria de pagos con tarjeta (PCI) como parte de su iniciativa de seguridad de

contenido. El estándar de PCI exige que las empresas acepten tarjetas de pago para aplicar fuertes controles, a fin de restringir el acceso a la información de cuenta del titular y tomar medidas para proteger la información almacenada.

Asimismo, al igual que todas las empresas que cotizan públicamente acciones, Microsoft está sujeta a Sarbanes-Oxley y a sus reglas estrictas sobre la información de la seguridad financiera. Con estas dos reglamentaciones, el desafío del cumplimiento de normas de Microsoft estaba claramente definido. No obstante, en cuanto a las políticas de seguridad de la información, Microsoft también tuvo que considerar la propiedad intelectual, que amplió considerablemente el alcance de su proyecto Information Classification and Data Handling.

“El código fuente, los planes estratégicos, la información operacional y otros tipos de información confidencial del negocio son todos tipos de propiedad intelectual que necesitamos proteger”, sostiene Opedal. “Por supuesto que algunos tipos de información son más confidenciales que otros: los datos del cliente, el código fuente, la información financiera corporativa eran, claramente, los más importantes para nosotros. Este es el motivo por el que, en vez de tratar de proteger nuestra información según la reglamentación específica, seguimos el enfoque de clasificación de toda la información en nuestro espacio de TI administrado en una de tres categorías: Alto impacto del negocio, Impacto moderado del negocio o Bajo impacto del negocio”.





Dado que los conceptos básicos de la estrategia pasaron a ser el centro de atención, el nuevo interrogante de Microsoft era: ¿cómo comprender mejor los riesgos que presentan las prácticas de gestión de datos y el almacenamiento de la información? Opedal y su equipo entendieron que tenían que conocer no solamente los archivos específicos, sino las tendencias generales de la información.

“Creamos un modelo de riesgo”, explica Opedal, “cuyo propósito era cuantificar el nivel de riesgo de nuestra información. Decidimos comenzar con HBI, que comprende toda la propiedad intelectual más importante y la información regulada según PCI y SOX y, a continuación, continuar con otras áreas. Para ejecutar nuestra estrategia HBI, necesitábamos una manera de analizar todo espacio administrado donde se pudiera almacenar la información confidencial, a fin de constatar su naturaleza. Este fue un desafío de detección de contenido. Allí fue donde RSA DLP Datacenter entró en acción.”

SOLUCIÓN

Los parámetros que Microsoft desarrolló para su proyecto Information Classification and Data Handling fijaron el criterio estricto para juzgar las soluciones de detección de contenido. Al contar con grandes cargas de trabajo y miles de ubicaciones para analizar, se consideraron principalmente la escalabilidad empresarial, el performance y la precisión. La administración y las operaciones también estuvieron como prioridad en la lista.

Los ejecutivos de Microsoft necesitaban saber que podían manejar los incidentes y las amenazas de seguridad de manera rápida y segura, y documentar los esfuerzos de corrección a fin de realizar seguimientos de auditoría según PCI y SOX. “La identificación de contenido no es uno de esos problemas que se resuelven usando gran cantidad de hardware a fin de obtener el tipo de performance requerido”, comenta Opedal. “La precisión incomparable y las características exclusivas de RSA DLP Datacenter, como el creciente procesamiento, hicieron que fuera la única opción viable para la detección de todo nuestro contenido confidencial”.

Microsoft implementó RSA DLP Datacenter, que adopta un enfoque revolucionario para la detección de contenido, gracias a su arquitectura distribuida y capacidades de análisis, y que permite analizar toda la información almacenada en el grupo completo de espacios compartidos y sitios SharePoint. Esta es una capacidad vital en las organizaciones que, como Microsoft, tienen una gran cantidad de información almacenada.

Para aumentar el performance del proceso de análisis, Opedal optó por usar la capacidad del producto Grid Processing, que le permitió especificar un grupo de servidores en cada ubicación a fin de procesar el análisis. Se hace provisioning de los servidores automáticamente, los cuales equilibran la carga del trabajo de análisis de contenido de la misma manera, a fin de obtener un procesamiento más acelerado. Microsoft también aprovecha la creciente tecnología de análisis de patentes pendientes para el análisis en curso. Esto les permite escanear y analizar nuevos archivos y directorios que se modificaron o se transfirieron, o a los cuales se les cambió el nombre regularmente.

“Realmente necesitamos el performance, la escalabilidad y las capacidades de detección de contenido de alta precisión que solamente RSA DLP Datacenter podría brindar”, dice Opedal. “El

procesamiento de red y el análisis incremental fueron esenciales para Microsoft, debido al volumen de datos que almacenamos. Asimismo, RSA DLP Datacenter genera archivos compatibles con una tasa de precisión de 98% o superior de modo consistente”.

La precisión líder en la industria de RSA DLP Datacenter incorpora el performance, la precisión y las técnicas de análisis de contenido más avanzadas.

RESULTADOS

Como resultado, Opedal y su equipo analizaron 12TB de información del file system y 120.000 sitios SharePoint en nueve días, y mantuvieron los más altos niveles de precisión. El creciente análisis continuo únicamente de la información nueva, que se modificó o se transfirió, o a la cual se le cambió el nombre, y que se encuentra en los mismos 120.000 sitios SharePoint tarda menos del 5% del tiempo que llevó el análisis original; por lo tanto, la continua detección de contenido se hizo realidad.

Además, gracias a RSA DLP Datacenter, Microsoft mantiene los costos de las operaciones de seguridad de la información lo más bajo posible. Al planificar el proyecto de detección de la información, el equipo estableció que un solo encargado del cumplimiento de las normas o asesor de seguridad podía tratar 250 incidentes por día. “La tasa de falsos positivos es inferior al 1%, de modo que sabemos que los incidentes que nuestro personal encargado del cumplimiento de normas tiene que examinar son genuinos”, explica Opedal. “Si no contáramos con RSA DLP Datacenter, hubiésemos tenido que tomar y capacitar más personal y hacer frente a un costo total de propiedad mucho más alto”.

RSA DLP Datacenter nos proporcionó una mejor comprensión de la ubicación de nuestra información del negocio de alto impacto y nos permite protegernos de la proliferación de información, lo cual es de suma importancia para todos nosotros aquí, en Microsoft.



“La identificación de contenido no es uno de esos problemas que se resuelven usando gran cantidad de hardware a fin de obtener el tipo de performance requerido. La precisión incomparable y las características exclusivas de RSA® Data Loss Prevention Datacenter hicieron que fuera la única opción viable para la detección de todo nuestro contenido confidencial”.

Olav Opedal, Security Program Manager, Microsoft



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

RSA, el logotipo de RSA y SecurID son marcas registradas o marcas comerciales de RSA Security Inc. en Estados Unidos y en otros países. EMC es una marca registrada de EMC Corporation. Las otras marcas comerciales que aparecen en este documento son propiedad de sus respectivos dueños. ©2009 RSA Security Inc. Todos los derechos reservados.

MICRO_CP_1208