Hoja de datos del producto

RSA® Data Loss Prevention Endpoint

Prevención completa de la pérdida de datos para información confidencial que se encuentra en computadoras de escritorio y portátiles

En resumen

- Comprenda su perfil de riesgo al detectar y analizar información confidencial en computadoras de escritorio y portátiles
- Alcance altos niveles de precisión y exactitud en la identificación de datos confidenciales
- Controle las acciones que se realizan con la información confidencial en tiempo real
- Aproveche la administración centralizada de políticas a fin de simplificar la implementación y el mantenimiento continuo

Descripción general

Las terminales, como las computadoras portátiles y de escritorio, han revolucionado la manera de hacer negocios, y la mayor parte de las actividades diarias del negocio se llevan a cabo en estas estaciones de trabajo. Sin embargo, estas terminales son una fuente fundamental para la pérdida de información. Las estadísticas muestran que más del 50% de las pérdidas de información confidencial se originan en estas terminales. Para complicar esta situación aún más, el tipo y la cantidad de información confidencial en estas terminales cambia a diario y las organizaciones no han establecido procesos para hacer un seguimiento de esta información.

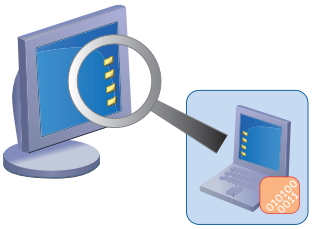
RSA Data Loss Prevention (DLP) Endpoint, una parte de RSA DLP Suite, es una solución integral para la prevención de pérdida de datos para la información que se encuentra en las computadoras portátiles y de escritorio. Viene en dos módulos: Detección y Ejecución. El módulo Detección halla la información confidencial por medio del análisis del contenido de los archivos en la unidad de disco duro local. El módulo Ejecución monitorea las acciones, como imprimir y copiar, en las computadoras de los usuarios y bloquea o registra las acciones que violan una política de seguridad. Esto permite una prevención proactiva de la pérdida de información confidencial.

Los más altos niveles de precisión

Todo archivo confidencial identificado que viole una política constituye una amenaza de seguridad que requiere consideración y rectificación. Las soluciones convencionales que carecen de altos niveles de precisión identifican gran cantidad de archivos no confidenciales como confidenciales (por ejemplo, confunden un número de quince dígitos al azar con un número de tarjeta de crédito), lo cual deriva en información falsa acerca del perfil de seguridad y de los niveles de amenaza. Esto no solamente aumenta el costo total de la propiedad, sino que además disminuye la credibilidad de la solución con el tiempo e impide la productividad del usuario al controlar las actividades efectuadas en los archivos no confidenciales. Las falsas alarmas fuerzan a las organizaciones a dedicar ciclos a riesgos que no existen, lo que deriva en el mal uso de la seguridad y los recursos de TI de gran valor.

RSA DLP Endpoint es de una exactitud excepcional en la identificación de datos reglamentarios confidenciales, como información de identificación personal (PII) y datos de la industria de tarjetas de pago (PCI), y datos no reglamentarios, como los datos de operaciones, estrategias y propiedad intelectual. La gran precisión se logra por medio de la implementación de algoritmos sofisticados de detección que analizan los patrones, las palabras clave y su ubicación

RSA®
The Security Division of EMC



RSA DLP Endpoint
Módulo Detección

- Detecta información confidencial
- Se implementa de manera temporal o permanente
- Genera informes y pistas de auditoría

contextual dentro de un archivo. Las organizaciones pueden usar las plantillas de detección de datos previamente integradas (para los datos relacionados con PCI, PII, HIPAA, GLBA, SOX, entre otros) o crear sus propias reglas a fin de lograr altos niveles de precisión en la detección y el monitoreo de información confidencial y en la prevención de la pérdida de datos.

Administración centralizada y escalabilidad

Las organizaciones empresariales que cuentan con decenas de miles de computadoras de escritorio y portátiles exigen una metodología escalable y eficaz para detectar y monitorear los datos confidenciales, e implementar y administrar la solución. RSA DLP Endpoint, que cuenta con una arquitectura de administración unificada de políticas y de un único agente, permite la fácil implementación y la administración de la solución, independientemente de la ubicación geográfica de las estaciones de trabajo. Desde una ubicación centralizada, los administradores pueden configurar las plantillas de detección de datos y ejecutar controles en todas las estaciones de trabajo de la empresa, y así reducen el tiempo de introducción y el costo total de la propiedad.

Los agentes que se pueden configurar por completo se pueden implementar de modo temporal, en el que el agente se desinstala por sí mismo después de analizar el sistema, o de modo permanente, en el que el agente reside en la computadora portátil para realizar futuras búsquedas. La tecnología de agentes distribuidos le permite al módulo Ejecución monitorear activamente las computadoras portátiles y bloquear las acciones no autorizadas que se realizan con la información confidencial, incluso cuando la computadora portátil está desconectada de la red.

Descubra, monitoree y controle la información confidencial

RSA DLP Endpoint se diferencia de las soluciones de protección convencionales para las computadoras de escritorio, ya que es capaz no solamente de detectar información confidencial, sino también de ejecutar controles sobre la información. Al utilizar el módulo Ejecución, las organizaciones pueden introducir controles detallados en el momento de usarlos, a fin de garantizar el bloqueo de una actividad específica en vez de bloquear el acceso en su totalidad. Para garantizar el cumplimiento confiable de las políticas, realiza un seguimiento de todas las acciones que atentan contra la información confidencial y bloquea aquellas que la política no permite.

El módulo Detección se puede usar para comprender el perfil de riesgo de la información confidencial que se encuentra en las computadoras portátiles. Analiza todos los archivos de la computadora, incluso la carpeta Archivos temporales de Internet, la Papelera de reciclaje y Mis documentos, a fin de detectar y analizar información confidencial.

Implementar acciones: permitir o bloquear

RSA DLP Endpoint

- Detecta toda la información confidencial
- Monitorea las acciones en tiempo real
- Bloquea las acciones que realizan los usuarios con la información confidencial
- Aplica políticas eDRM (mediante Microsoft RMS)

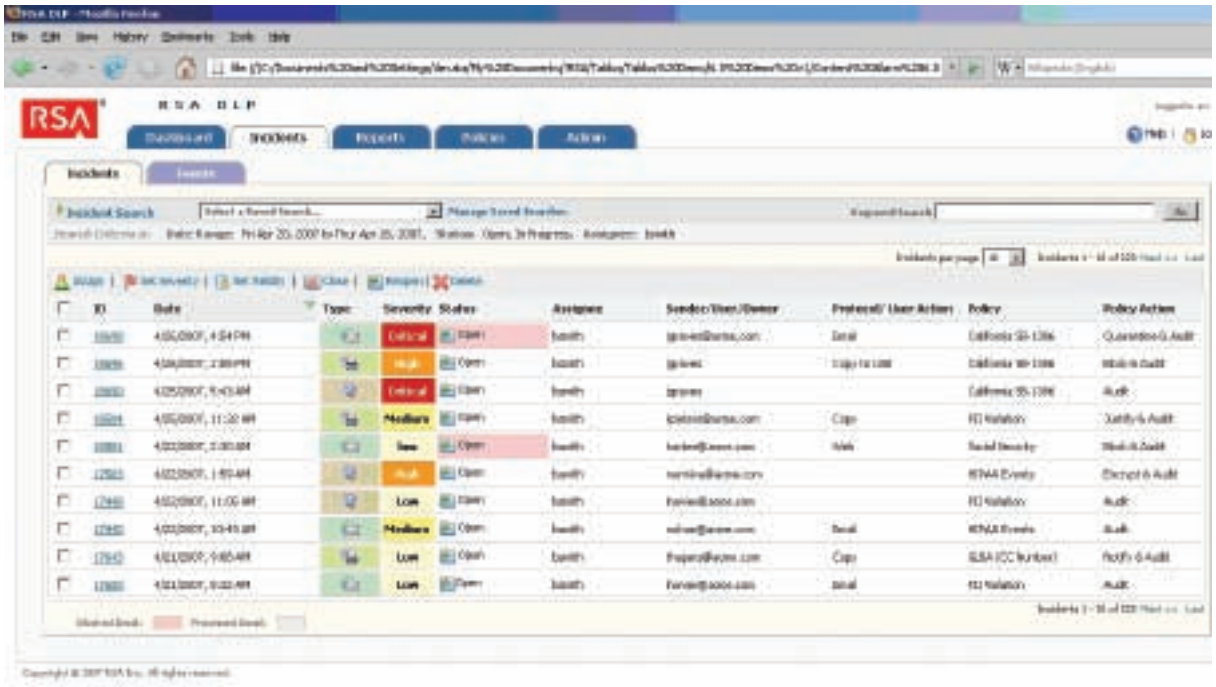
Además de bloquear, se pueden crear acciones de políticas, ya sea para informar a los usuarios que las acciones que están llevando a cabo violan una política empresarial, o para pedirles a los usuarios que justifiquen sus acciones (copiar, imprimir). Los mensajes de justificación de los usuarios se registran para una revisión posterior.

La encuesta realizada a casi 500 profesionales de TI reveló que el 81 por ciento de las empresas perdieron máquinas que contenían información confidencial el año pasado. Quizá, lo que da más temor es la razón por la que se pierde tanta información confidencial: las empresas simplemente desconocen que está ahí.

Computerworld

Administración y reporting de incidentes empresariales

Una vez que se detecta información confidencial o se bloquea una acción del usuario, RSA Data Loss Prevention Endpoint comienza un proceso sobre el flujo de trabajo para el seguimiento de los incidentes a fin de registrar y monitorear los datos en riesgo. Lleva a cabo una pista de auditoría de incidentes y puede alertar a un grupo predefinido de partes interesadas por medio de correo electrónico o contenido Web en formato RSS.



Descripción	Sistemas soportados	Beneficios
Sistema operativo en computadoras portátiles y PCs	– Las computadoras portátiles y de escritorio con Windows® 2000 SP4 o superior (nota: soporte limitado Enforce para Vista)	– Brinda soporte a los sistemas operativos conocidos de computadoras de escritorio empresariales
Información reglamentaria soportada	– Industria de pagos con tarjeta (PCI) – Información de identificación personal (PII) – Ley de Portabilidad y Responsabilidad de Seguro Médico (HIPAA) – Ley Gramm-Leach-Bliley (GLBA) – Sarbanes-Oxley (SOX) – CA SB 1386 – Aproximadamente otras 50 reglamentaciones	– Ayuda a cumplir con las reglamentaciones – Modera el riesgo de multas legales – Mejora la confianza del cliente – Ayuda a impedir los costos asociados con las violaciones de datos
Información no reglamentaria soportada	– Propiedad intelectual, como código fuente, blueprints, entre otros – Información sobre las operaciones y las estrategias del negocio, como datos sobre las adquisiciones, los precios, el análisis competitivo y las fusiones	– Ayuda a impedir las demandas colectivas – Modera el riesgo de perder ventajas competitivas – Ayuda a impedir la pérdida de ingresos – Protege el valor de la marca – Protege la propiedad intelectual empresarial

Prevención integral de la pérdida de datos

RSA Data Loss Prevention Suite (los módulos Network, Datacenter y Endpoint) comprende una solución integral de prevención de pérdida de datos que permite descubrir, monitorear y proteger la información confidencial ante cualquier pérdida o uso indebido, ya sea que se encuentre en un data center, en la red o afuera en la terminal.

Acerca de RSA

RSA, la División de Seguridad de EMC, es el principal proveedor de soluciones de seguridad para aceleración del negocio y ayuda a las más importantes organizaciones del mundo a alcanzar el éxito resolviendo los más complejos y delicados desafíos de seguridad. El enfoque de seguridad centrado en la información que ofrece RSA protege la integridad y la confidencialidad de la información durante todo su ciclo de vida, sin importar adónde se transfiera, quién acceda a ella o cómo se use.

RSA ofrece soluciones líderes en la industria de verificación de identidad y control de acceso, encriptación y administración de claves, administración del cumplimiento de normas e información de seguridad, y protección contra fraudes. Estas soluciones brindan confianza a millones de identidades de usuarios, a las transacciones que realizan y a los datos que se generan. Para obtener más información, visite argentina.rsa.com y argentina.emc.com.

RSA®
The Security Division of EMC

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

RSA, RSA Security y el logotipo de RSA son marcas registradas o marcas comerciales de RSA Security Inc. en Estados Unidos y en otros países. Microsoft, Vista y Windows son marcas comerciales o marcas registradas de Microsoft Corporation en los Estados Unidos y otros países. EMC es una marca comercial de EMC Corporation. Todas las otras marcas comerciales que aparecen aquí son propiedad de sus respectivos dueños.

DLPEP DS 1208