Data Sheet do produto

RSA® Data Loss Prevention Datacenter

Detecte dados confidenciais localizados em data centers e atenue o risco de modo proativo

Resumo geral

- Compreenda o perfil de risco por meio da detecção e análise de dados confidenciais em compartilhamentos de arquivos, SAN/NAS, arquivos de bancos de dados e outros repositórios de dados
- Obtenha altos níveis de precisão e velocidade na identificação de dados confidenciais
- Gerencie dados confidenciais por meio de ações como mover, mover para quarentena, excluir e eDRM
- Aproveite o gerenciamento centralizado de políticas para simplificar a implantação e o gerenciamento contínuo

Visão geral

O volume de dados digitais armazenados em data centers empresariais está praticamente duplicando a cada ano, sendo que a maior parte deles está na forma de dados não estruturados — arquivos contidos em compartilhamentos de arquivos e repositórios. Alguns desses arquivos podem conter números do seguro social de clientes ou dados de cartões de crédito que são administrados por normas, uma vez que alguns deles podem conter propriedade intelectual e planos de produtos que são de suma importância às operações de negócios. Isso é muito importante para que as empresas compreendam onde residem esses dados confidenciais, de modo que possam gerenciá-los de forma apropriada. Todavia, detectar esses dados confidenciais no data center permaneceu um desafio, principalmente devido ao volume de dados a serem analisados e à falta de ferramentas automatizadas e precisas para classificação.

O RSA® Data Loss Prevention (DLP) Datacenter, parte integrante do RSA DLP Suite, é uma solução abrangente de prevenção de perda de dados para informações que residam em compartilhamentos de arquivo, caixas de armazenamento (SAN/NAS), sites de SharePoint® e outros repositórios de dados. Ele examina fontes de dados com velocidade e precisão incomparáveis, o que produz um perfil de risco completo dos dados no data center.

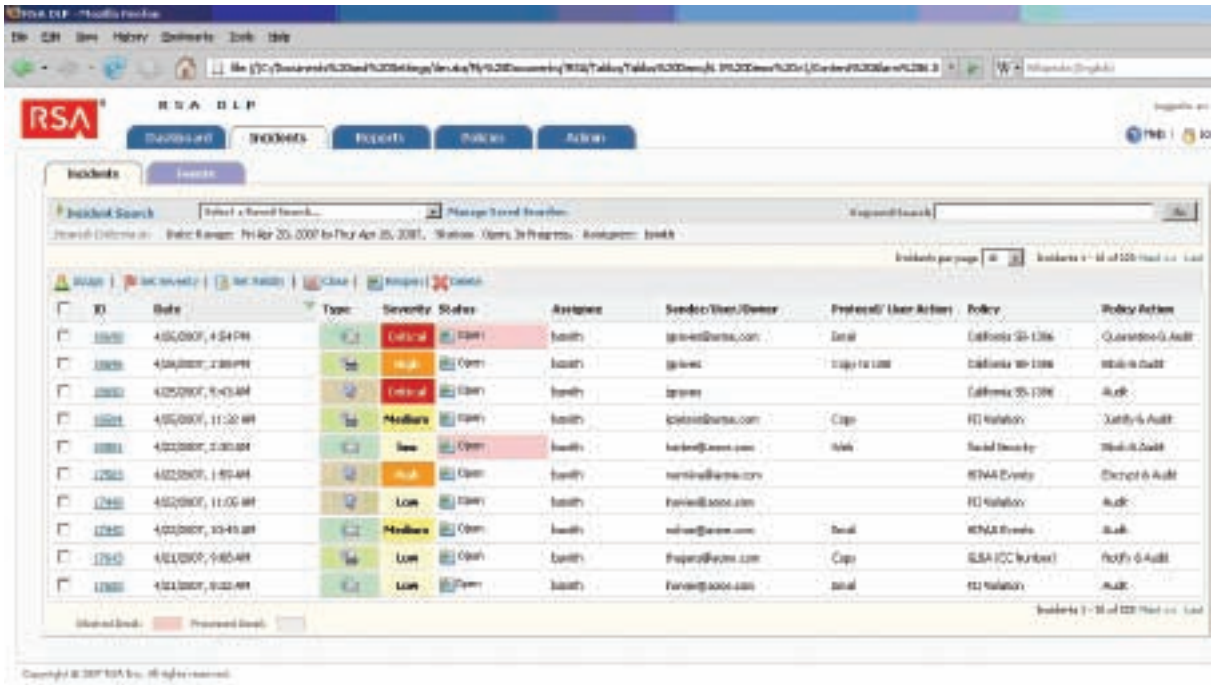
Detecte e gerencie dados confidenciais

O RSA DLP Datacenter apresenta uma arquitetura revolucionária que traz o software para os dados, ao invés de trazer os dados para o software. Ao contrário das tecnologias comuns de detecção, nas quais os dados de diversos locais são movidos para um local central para fins de análise, o RSA DLP Datacenter verifica e analisa os dados próximos ao local onde se encontram. Sua exclusiva arquitetura incorporada baseada em grade, juntamente com recursos de verificação baseados em agentes temporários, permite que empresas efetuem a verificação de todos os dados confidenciais armazenados em compartilhamentos de arquivos, bancos de dados, sites de SharePoint® e outros repositórios sem gerar nenhum tráfego significativo de rede. Isso permite que as empresas examinem milhares de servidores de arquivo de forma simultânea e reduzam de meses para horas o tempo de verificação. O RSA DLP Datacenter apresenta mais de 120 políticas incorporadas que permitem às empresas detectar dados confidenciais desde o primeiro momento com a maior precisão.

RSA®
The Security Division of EMC

Gerenciamento e emissão de relatórios de incidentes corporativos

Assim que os dados confidenciais são detectados, o RSA DLP Datacenter dá início a um processo de fluxo de trabalho de rastreamento de incidentes para registrar e monitorar os dados em risco. Ele mantém uma trilha de auditoria dos incidentes e pode alertar um conjunto predefinido de interessados por meio de e-mail ou feeds RSS. Os responsáveis pela conformidade também podem tomar atitudes como mover, colocar em quarentena ou aplicar políticas eDRM (utilizando Microsoft RMS) em arquivos confidenciais conforme as políticas corporativas.



Altos níveis de precisão

Cada arquivo confidencial identificado como violação de política precisa ser tratado como uma ameaça à segurança, depois corrigido. As soluções convencionais sem altos níveis de precisão identificam números significativos de arquivos não confidenciais como arquivos confidenciais (por exemplo, confundir um número aleatório de quinze dígitos com um número de cartão de crédito), o que resulta em falsos positivos. Estas informações imprecisas de perfil de risco não apenas aumentam o custo total da propriedade como também diminuem a credibilidade da solução com o passar do tempo. Esses alarmes falsos forçam as empresas a gastar ciclos para corrigir riscos que não existem, o que resulta no uso desnecessário de recursos valiosos de segurança e de TI.

"Processamento em grade e análise incremental foram essenciais para a Microsoft, considerando o volume de dados que armazenamos. Além disso, o RSA DLP Datacenter (anteriormente Content Sentinel) gera arquivos combinados com uma taxa de precisão de no mínimo 98%."

Olav Opeda
Programa de segurança, Microsoft

O RSA Data Loss Prevention Datacenter alcança um nível excepcionalmente alto de precisão na identificação de dados confidenciais como PII (Personally Identifiable Information, informações de identificação pessoal), dados de PCI (Payment Card Industry, setor de cartões de pagamento) e dados de negócios confidenciais. Altos níveis de precisão são alcançados por meio da implantação de algoritmos sofisticados de detecção que seguem regras exatas para identificar dados confidenciais. Essas regras de precisão ajudam os algoritmos não apenas a analisar palavras-chave e padrões, mas também a examinar a disposição contextual das palavras-chave dentro de um arquivo. As empresas podem permitir modelos de detecção de dados predefinidos (para dados relacionados a PCI, PII, HIPAA, GLBA, SOX, códigos-fonte etc.) ou gerar suas próprias regras para alcançar altos níveis de precisão na detecção de dados confidenciais evitando a perda de dados.

Dimensionamento e gerenciamento centralizado

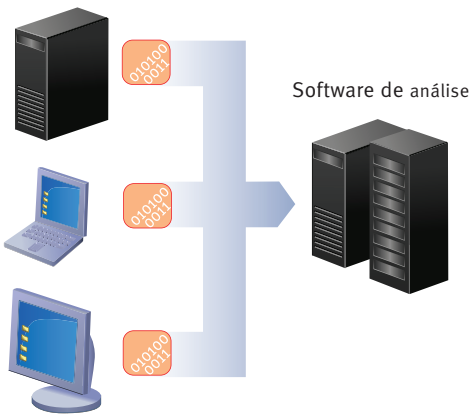
As corporações que têm milhares de servidores e repositórios de arquivos precisam de uma metodologia eficiente e dimensionável não apenas para detectar e analisar dados confidenciais, mas para assumir atitudes de segurança, como excluir e colocar em quarentena. O RSA DLP Datacenter, parte integrante do RSA Data Loss Prevention Suite, com uma arquitetura unificada de gerenciamento de política, possibilita fácil implantação e gerenciamento independentemente do local dos dados. A partir de um local centralizado, os administradores podem configurar os modelos de detecção de dados e impor políticas em todas as fontes de dados na empresa, o que facilita para as empresas a implementação e manutenção da solução. Para examinar grandes volumes de dados de forma eficaz, o RSA DLP apresentou o Grid Scanning (exame em grade), um recurso que aproveita a tecnologia de processamento paralelo utilizando servidores padrão prontos para utilizar configurados como um cluster. Esta abordagem exclusiva reduz o custo total de propriedade (novos produtos de hardware etc.), além de aumentar em pelo menos dez vezes a velocidade das verificações.

"Segundo o que encontrei em uma avaliação anterior do RSA DLP Datacenter (Tablus Content Sentinel) , a detecção de conteúdo da empresa é precisa. As lâminas predefinidas de conteúdo especializado geraram muito poucos falsos positivos. Após registrar minhas listas personalizadas de clientes e o código-fonte, o RSA Datacenter 3.0 encontrou todas as ocorrências de dados confidenciais."

"Detecte rapidamente conteúdo confidencial"
InfoWorld

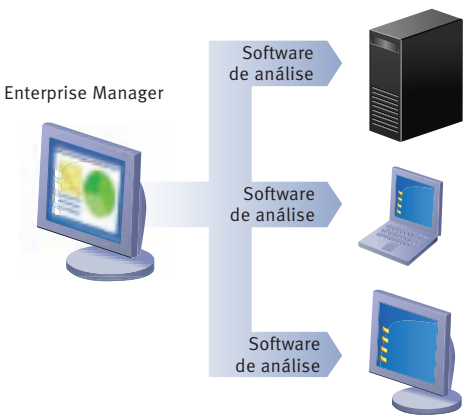
Examine e analise dados confidenciais onde estão localizados

Detecte e analise dados confidenciais com grande desempenho utilizando uma revolucionária arquitetura distribuída de verificação no local.



Enfoque tradicional de verificação de ponto único

Mover todos os dados para o software de análise.



Enfoque distribuído do RSA DLP Datacenter

Enviar o software de análise para os dados.

Recursos e benefícios do RSA DLP Datacenter

Descrição	Sistemas compatíveis	Benefícios
Destinos de detecção	– Compartilhamentos de arquivo do Windows®, AIX®, HP-UX® e Solaris® – SharePoint®, Documentum® e outros repositórios – Armazenamento em NAS/SAN	– Suporte para diversas fontes de dados empresariais
Dados normativos aceitos	– PCI (Payment Card Industry, setor de cartões de pagamento) – PII (Personally Identifiable Information, informações de identificação pessoal) – HIPAA (Health Insurance Portability and Accountability Act, lei de responsabilidade e mobilidade de seguros de saúde) – Lei de Gramm-Leach-Bliley (GLBA) – Sarbanes-Oxley (SOX) – CA SB 1386 – Cerca de 50 outras normas	– Ajudar a cumprir com as normas – Reduzir o risco de multas legais – Manter a confiança do cliente – Ajudar a impedir despesas relacionadas a violações de dados
Dados não normativos aceitos	– Propriedade intelectual, como código-fonte, projetos etc. – Estratégia de negócios e dados operacionais, como informações de demarcação de preços, análise da concorrência, fusões e aquisição	– Ajudar a impedir ações judiciais coletivas – Reduzir o risco de perder a vantagem sobre a concorrência – Ajudar a impedir a perda de receita – Proteger o valor da marca – Proteger a propriedade intelectual

Ampla prevenção contra perda de dados

O RSA DLP Suite (módulos de rede, data center e ponto de extremidade) inclui uma solução abrangente de prevenção de perda de dados que detecta, monitora e protege dados confidenciais contra perda ou má utilização, estejam em um data center, na rede ou nos pontos de extremidade.

Sobre a RSA

RSA, a divisão de segurança da EMC, é a melhor fornecedora de soluções de segurança para a aceleração de negócios, ajudando as mais importantes empresas do mundo a alcançar a solução para seus desafios de segurança mais complexos e delicados. A abordagem de segurança centrada em informações da RSA protege a integridade e a confidencialidade das informações em todo o seu ciclo de vida — não importando para onde são transferidas, quem as acessa ou como são utilizadas.

A RSA oferece soluções líderes do setor quanto à segurança de identidade e controle de acesso, gerenciamento de chaves e criptografia, gerenciamento de informações de segurança e conformidade e proteção contra fraude. Essas soluções levam confiança às identidades de milhões de usuários, às transações executadas por eles e aos dados gerados. Para obter mais informações, visite www.RSA.com e www.EMC2.com.br.

RSA®
The Security Division of EMC

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

RSA, RSA Security e o logo da RSA são marcas registradas ou marcas comerciais da RSA Security Inc. nos Estados Unidos e/ou em outros países. Microsoft, Windows e SharePoint são marcas registradas ou marcas comerciais da Microsoft Corporation nos Estados Unidos e/ou em outros países. EMC é marca registrada da EMC Corporation. Todas as outras marcas comerciais mencionadas neste documento pertencem a seus respectivos proprietários.

DLPCTR DS 1208