MELHORES PRÁTICAS

PROTEGER OS DADOS DENTRO DE APLICATIVOS DE SAAS

Reduzir a superfície de ataque e prevenir ameaças conhecidas

Por diversas razões, incluindo escalabilidade, disponibilidade e custo, a mudança para dados e aplicativos baseados em nuvem está cada vez mais rápida e incontrolável.

A incorporação de SaaS aos dados corporativos

Na última década, surgiu um novo paradigma sobre aplicativos publicamente disponíveis e baseados na Internet que resultou em uma grande mudança de aplicativos comerciais implantados internamente para aplicativos baseados em nuvem. A primeira grande manifestação dessa mudança foi a adoção de aplicativos Software as a Service (Software como um serviço – SaaS) desenvolvidos, vendidos e mantidos por fornecedores, como Salesforce.com, NetSuite, Microsoft, Box e Dropbox.

Contudo, como o ambiente SaaS comum é invisível para os administradores de rede, as ferramentas de segurança empresariais desenvolvidas para proteger centros de dados internos, servidores e estações de trabalho não podem proteger de forma eficaz os aplicativos SaaS ou impedir o vazamento de dados.

O modelo SaaS possibilita que usuários não sofisticados tecnicamente adquiram e usem aplicativos sem tomar as medidas adequadas para proteger os dados empresariais. O uso de aplicativos SaaS não autorizados, pelo menos pelo departamento de TI, (os chamados de “shadow IT”) pode criar o risco de um grande vazamento de dados e não conformidade regulatória, seja por acidente ou por intenção maliciosa. Mesmo se os usuários de SaaS tiverem consciência da necessidade de segurança, sua capacidade de proteger os dados depende das ferramentas oferecidas pelo fornecedor, que podem não ser suficientes para esta tarefa.

Como resultado, os aplicativos SaaS representam um vetor de ameaça atraente, uma vez que eles abrem brechas na visibilidade da segurança e têm potencial de transmissão de ameaças diretamente para a rede-alvo.

Aperture, o serviço de segurança de SaaS da Palo Alto Networks®, oferece uma segurança adicional à plataforma de segurança de última geração da Palo Alto Networks, fornecendo informações importantes sobre exposição de dados e ameaças nos aplicativos SaaS autorizados. O Aperture soluciona o problema da segurança de aplicativos SaaS ao se conectar diretamente aos aplicativos SaaS e fornecer aos administradores uma classificação de dados, visibilidade sobre direitos de compartilhamento e acesso e a detecção de ameaças. O Aperture é integrado ao ambiente de análise de malware baseado em nuvem do WildFire™ para proteger dados da empresa que estejam dentro dos aplicativos SaaS contra a ameaça de ataques externos e subsequente vazamento de dados ou não conformidade regulatória.

Quer você tenha acabado de implantar os produtos da Palo Alto Networks ou os utilize há anos, certifique-se de que esteja maximizando todo seu valor ao rever as melhores práticas para proteger dados dentro de aplicativos SaaS.

Tal como acontece com qualquer tecnologia, geralmente há uma abordagem gradual para uma implantação completa, que consiste em fases de implantação cuidadosamente planejadas destinadas a tornar a transição o mais suave possível, com o mínimo de impacto para os seus usuários finais. Com essa abordagem em mente, recomendamos uma abordagem gradual para implantar o Aperture. O objetivo da sua implantação de segurança de SaaS deve ser o de ter no final um conjunto robusto de políticas para identificar aplicativos SaaS autorizados, não autorizados e tolerados, além de proteger os dados que eles armazenam.

FASE 1: VISIBILIDADE E AVALIAÇÃO DE RISCOS

Dica: use o "SaaS Application Usage Report" (relatório de uso de aplicativos SaaS) na guia Monitor na interface de usuário do NGFW da Palo Alto Networks para identificar os aplicativos SaaS atualmente em uso.

Em primeiro lugar, tome medidas para identificar os aplicativos SaaS que estão em uso atualmente, autorizados ou não autorizados. Comunique-se com as unidades de negócios e líderes de tecnologia em toda a organização para determinar quais aplicativos SaaS eles aprovaram para seus usuários. Todos os aplicativos SaaS que você descobrir que não estejam explicitamente autorizados pelos líderes de negócios devem ser considerados não autorizados. Entre esses, descubra quais você está disposto a tolerar ao analisar os riscos que oferecem para a organização.

Para cada aplicativo autorizado que tenha sido identificado, acesse os recursos de segurança disponibilizados pelo fornecedor e identifique qualquer falha de segurança que possa ser motivo de preocupação. Por exemplo:

- Quem pode acessar o aplicativo e seus dados, por exemplo, como e se o aplicativo permite o compartilhamento com usuários que estejam fora da organização
- Como a autenticação é aplicada e se o aplicativo suporta autenticação de dois fatores
- Quão sensíveis são os dados armazenados nos aplicativos, por exemplo, se são classificados como PII, PCI ou qualquer outro padrão de conformidade
- Recursos de criptografia de arquivos e como as chaves são gerenciadas
- Tipos de arquivos suportados pelo aplicativo e seus potenciais usos para a entrega de ameaças

O resultado dessa análise ajudará você a definir quais recursos e políticas de segurança devem ser implantadas no Aperture e no NGFW e em qual sequência.

Dica: ao ativar o User-ID no seu NGFW, é possível identificar os usuários que estão acessando aplicativos SaaS não autorizados e então tomar medidas para migrá-los para aplicativos SaaS autorizados.

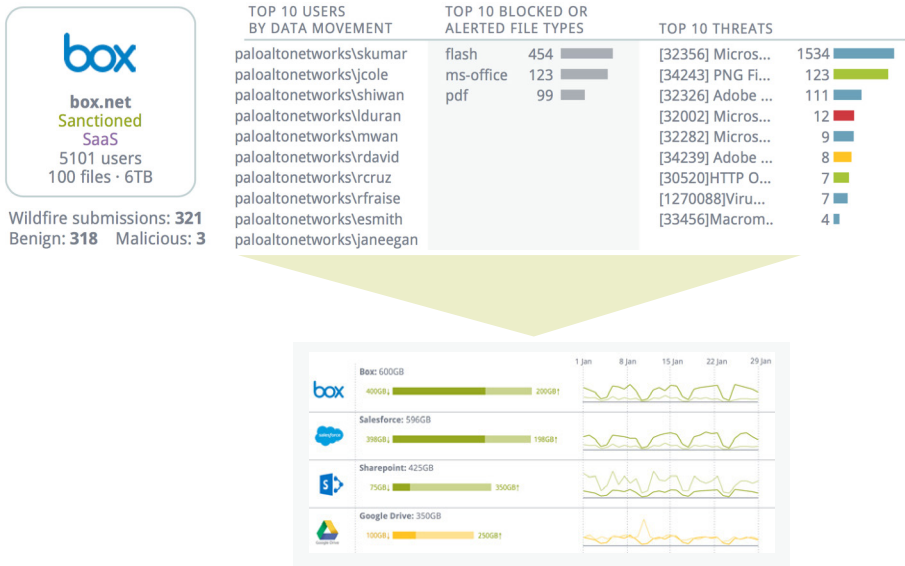

Figura 1: O relatório de uso de aplicativos SaaS fornece valiosas informações sobre os aplicativos SaaS, incluindo quais aplicativos estão sendo usados, o número de sessões e a quantidade de dados movimentados por cada usuário e o detalhamento dos tipos de arquivos e malwares detectados

Dica: classifique os aplicativos SaaS autorizados como tais na interface de usuário do NGFW para ter mais detalhes nos relatórios de uso.

Guia do administrador:

- Acessar o serviço Aperture
- Gerenciar os administradores do Aperture
- Aplicativos SaaS suportados
- Gerar o relatório de uso de aplicativos SaaS
- Avaliar riscos

Dica: é possível configurar várias contas de administrador do Aperture e exigir que os administradores façam login usando subredes ou endereços IP específicos.

Dica: Como o serviço Aperture utiliza a lista de domínios internos para determinar o nível de exposição de um ativo durante o processo de varredura, você deve criar sua lista de domínios internos para o app antes de começar a varredura nos aplicativos SaaS suportados.

Dica: personalize a identificação de conteúdo do Aperture para sua organização ao carregar exemplos de documentos normalmente carregados para seus aplicativos SaaS autorizados, como documentos legais, código-fonte, ordens de compra etc. O Aperture pode extrair metadata e/ou conteúdo textual de mais de 100 formatos de arquivos.

Dica: uma regra pode estar no estado "ativada" ou "desativada". Certifique-se de ativar novas regras de política após incluí-las se quiser que elas estejam ativas durante as varreduras subsequentes.

FASE 2: CRIAR UMA POLÍTICA DE APLICATIVOS SAAS AUTORIZADOS

Como o Aperture é um aplicativo SaaS puro, ele não requer a instalação de nenhum hardware ou software residente no seu sistema. Basta fazer login na sua conta de administrador do Aperture usando as credenciais fornecidas pela Palo Alto Networks e alterar sua senha de administrador.

Conecte os aplicativos SaaS suportados ao Aperture ao autenticar os aplicativos usando uma conta administrativa. Após a autenticação, o serviço Aperture recebe um token do aplicativo de nuvem, que ele utiliza para estabelecer e manter uma conexão segura. O serviço Aperture então se conecta diretamente à interface de programação de aplicativo (API) do aplicativo especificado, o que permite que ele faça uma varredura em todos os dados históricos que residem nele, monitore dados alterados ou novos e identifique violações das políticas e seus riscos associados.

Como tanto usuários internos como externos podem ter acesso ao aplicativo SaaS, configure níveis de confiança no Aperture para o aplicativo SaaS ao identificar domínios internos de e-mail, os quais o Aperture utiliza para diferenciar os colaboradores que são usuários internos dos externos. Você também pode marcar domínios ou usuários externos como confiáveis ou não confiáveis, o que afeta a política global subjacente que o serviço Aperture utiliza quando faz varredura nos ativos.

Analise a lista de colaboradores externos em busca de endereços de e-mail pessoais. Eles podem ser de funcionários ou parceiros de negócios, contudo, se e quando essas pessoas não estiverem mais afiliadas à empresa, elas ainda terão acesso aos ativos da empresa compartilhados com seus endereços de e-mail pessoais.

O Aperture define quatro níveis de exposição:

- **Pública** – acessível para qualquer pessoa na Internet
- **Externa** – compartilhada com indivíduos, grupos ou empresas fora da sua organização
- **Empresa** – explicitamente compartilhado com indivíduos ou grupos dentro da sua organização
- **Interna** – não explicitamente compartilhada (mas, baseada no aplicativo específico, outras pessoas na sua organização podem ter acesso ao documento através de um link, por exemplo)

Se uma varredura revelar que o nível de exposição de um ativo foi excedido, isso gerará um alerta.

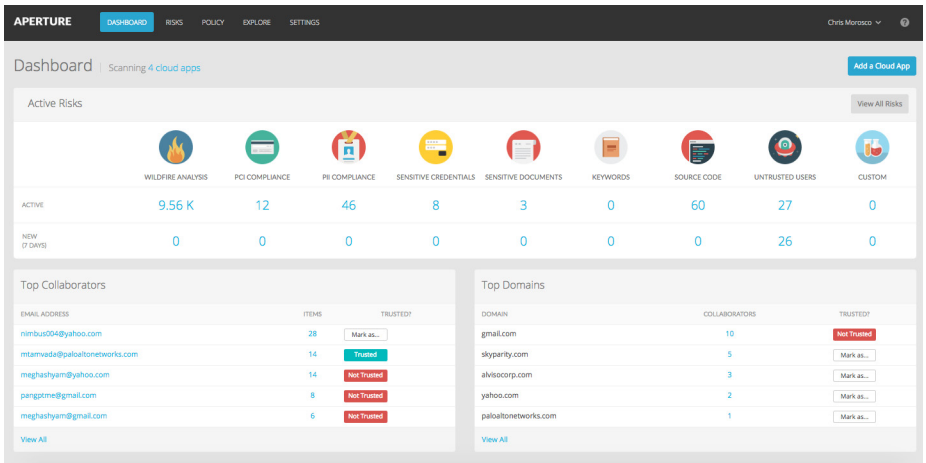

Figura 2: A interface de usuário do Aperture fornece visibilidade sobre uma potencial exposição de dados, não conformidade regulatória e ameaças ocultas nos aplicativos SaaS autorizados

O Aperture contém políticas que são ativadas por padrão, incluindo:

- Conformidade com PCI (setor das operadoras de cartões)
- Conformidade com PII (informações pessoalmente identificáveis)
- Credenciais confidenciais
- Documentos confidenciais
- Usuários não confiáveis – identifica arquivos que foram compartilhados com usuários na lista de usuários não confiáveis ou de domínios não confiáveis

Dica: é possível configurar modelos de e-mail para usar para alertas comumente encontrados. Eles serão enviados para os usuários que violarem sua política de aplicativos SaaS ativada.

- Análise do WildFire – faz uma varredura nos arquivos para detectar arquivos executáveis portáteis (PE) maliciosos e ameaças conhecidas com base no hash de arquivo

Você também pode criar políticas personalizadas que usem palavras-chave ou expressões regulares para identificar violações de políticas. O Aperture também inclui uma política para identificar código-fonte.

Guia do administrador:

- Proteger aplicativos em nuvem
- Avaliar e remediar riscos
- Definir seus domínios internos
- Configurar o alias de e-mail para enviar notificações

FASE 3: VIOLAÇÕES DE POLÍTICAS E AÇÃO

Dica: se um ativo violar a regra de política da análise do WildFire, isso significa que o WildFire identificou um malware no ativo. Você pode visualizar o relatório do WildFire para saber mais sobre o comportamento malicioso que o WildFire detectou e rastrear a fonte do malware na sua rede.

O Aperture inclui a aplicação de políticas retroativas. Quando você inclui um novo aplicativo SaaS, o Aperture faz uma varredura nele e colhe informações detalhadas sobre todos os usuários, metadata e conteúdos de arquivos. Durante essa varredura inicial, o Aperture identifica e classifica os riscos e as exposições por nível de gravidade para todos os ativos em todos os apps SaaS suportados. Você pode visualizar a lista de classificação de riscos no painel do Aperture.

Quando uma varredura gera um alerta, as seguintes ações estarão disponíveis para você, dependendo do tipo de alerta:

- Realocar um ativo para outra pasta.
- Eliminar alguns ou todos os compartilhamentos do ativo – por exemplo, remover o compartilhamento público e deixar apenas o compartilhamento para toda a empresa.
- Eliminar o acesso de um colaborador para aquele ativo ou todos os ativos.
- Atribuir a outro administrador que esteja mais familiarizado com o conteúdo e seu uso adequado para o acompanhamento.
- Enviar um e-mail de notificação de risco para um usuário para alertar e instruir sobre as políticas de uso aceitáveis.
- Ignorar o alerta após determinar que nem o conteúdo do ativo nem a forma como ele é compartilhado coloca em risco a organização.
- Usar o WildFire para rastrear ameaças.

Dica: ao excluir uma categoria de incidente, todos os riscos marcados com essa categoria são automaticamente marcados como não categorizados.

Após a varredura inicial ser concluída, o Aperture continuará automaticamente a fazer varreduras no aplicativo SaaS quase em tempo real para detectar futuras violações de políticas.

Com o tempo, à medida que ganha mais experiência com o Aperture, você pode decidir se quer incluir uma nova regra de política ou fazer o ajuste fino em uma regra de política existente.

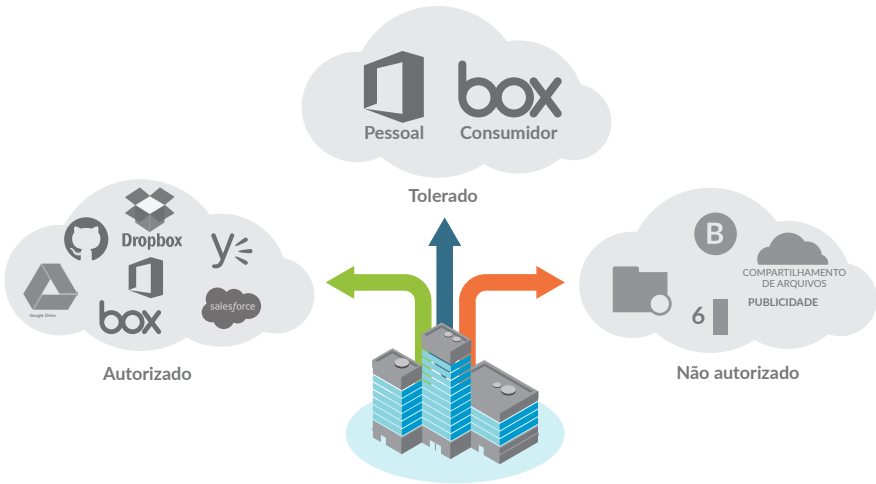

Figura 3: Os aplicativos SaaS separados em três grupos: apps autorizados gerenciados de forma granular através do Aperture, aplicativos tolerados controlados através do NGFW e aplicativos não autorizados monitorados ou bloqueados através do NGFW

Também é possível atribuir uma categoria de incidente a um risco, o que torna fácil filtrar e visualizar riscos por categoria, agilizando sua capacidade de detectar e responder a tipos específicos de riscos. As categorias padrão incluem: teste, pessoal, justificado por negócios, ignorado, análise, incidente, falso positivo e não analisado. Você pode personalizar essa lista para incluir ou excluir uma categoria de risco.

O Aperture funciona em conjunto com o NGFW como parte da plataforma de segurança de última geração para mitigar os riscos para a sua organização de aplicativos SaaS não autorizados. Uma ampla biblioteca do App-ID no NGFW fornece uma classificação instantânea e controles específicos para aplicativos SaaS não autorizados que você escolher tolerar, fornecendo a você a capacidade de controlar o acesso de forma granular.

Lembre-se de que você ainda tem recursos no NGFW que permitem controlar o nível de interação que os seus usuários possuem nos aplicativos em uso. Limite o acesso a aplicativos SaaS tolerados no NGFW ao permitir que apenas alguns grupos de usuários os acessem ou proibir que determinados tipos de arquivo sejam carregados, baixados ou compartilhados. Bloqueie totalmente os aplicativos SaaS não autorizados no NGFW para toda a empresa ou para grupos de usuários.

Guia do administrador:

- Gerenciar política do Aperture
- Política de segurança (PAN-OS®)
- Uso de etiquetas para agrupar e diferenciar visualmente objetos
- Ajuste fino de política

Nosso compromisso de fornecer suporte aos nossos clientes

A Palo Alto Networks está empenhada em garantir uma implantação bem-sucedida e fornecer um suporte abrangente através de nossa organização de Atendimento ao Cliente Global. Compreendemos perfeitamente que o fracasso não é uma opção. Nossas ofertas de suporte e programas de treinamentos foram concebidos para mitigar qualquer preocupação com a implantação que você possa ter.

- Serviços de garantia das soluções da Palo Alto Networks
- Planos de suporte ao cliente da Palo Alto Networks
- Serviços de consultoria da Palo Alto Networks
- Serviços educacionais da Palo Alto Networks

Junte-se à Comunidade AO VIVO da Palo Alto Networks para ter acesso a discussões de usuários, tutoriais e artigos da base de dados de conhecimento.

- Guia do administrador do Aperture
- Guia do administrador do PAN-OS, versão 7.1

fuel
PALO ALTO NETWORKS
USER GROUP

Junte-se à comunidade do Grupo de usuários do Fuel da Palo Alto Networks para se conectar com profissionais que pensam como você ao redor do mundo e que estão prontos para discutir suas melhores práticas duramente conquistadas e trocar informações. Você também pode ter acesso exclusivo a especialistas no assunto para responderem suas perguntas mais desafiadoras relacionadas à segurança através de eventos online, como webinars e sessões de perguntas e respostas, e eventos presenciais.

paloalto NETWORKS®

4401 Great America Parkway
Santa Clara, CA 95054

Principal: +1.408.753.4000
Vendas: +1.866.320.4788
Suporte: +1.866.898.9087

www.paloaltonetworks.com

© 2016 Palo Alto Networks, Inc. Palo Alto Networks é uma marca registrada da Palo Alto Networks. Uma relação de nossas marcas registradas pode ser encontrada em http://www.paloaltonetworks.com/company/trademarks.html. Todas as outras marcas mencionadas aqui podem ser marcas comerciais de suas respectivas empresas. pan-best-practices-securing-datawithin-saas-applications-wp-053116