SOPHOS

Segurança na nuvem pública: setes práticas recomendadas

Documento técnico Sophos Junho de 2019

Conteúdo

Segurança na nuvem pública: setes práticas recomendadas

O que significa sucesso para você quando o assunto é proteger aplicativos na nuvem pública?

Passar um ano longe das manchetes por causa de uma violação de dados? Ou ser capaz de entender a área de cobertura da estrutura de nuvem da sua organização de modo a poder protegê-la com precisão? Talvez seja garantir o andamento das auditorias de conformidade sem atropelos? Ou melhorar a colaboração nas correções de segurança e conformidade entre as equipes confinadas de desenvolvimento e conformidade?

O que quer que você queira, este guia irá ajudá-lo. Ele explora os sete passos mais importantes para proteger a nuvem pública, oferecendo orientações práticas que toda organização pode seguir. Inclui também os resultados das pesquisas em ameaça realizadas pelo SophosLabs sobre a frequência com que os criminosos virtuais visam às instâncias baseadas na nuvem, além de expor como o Sophos Cloud Optix permite às organizações cuidar dos desafios em segurança e visibilidade.

Rodar novas instâncias em Amazon Web Services (AWS), Microsoft Azure ou Google Cloud Platform (GCP) é fácil, o difícil é as equipes de operação, segurança, desenvolvimento e conformidade monitorar as mudanças em dados, cargas de trabalho e arquitetura nesses ambientes para manter tudo protegido.

Enquanto os provedores de nuvem pública são responsáveis pela segurança da nuvem (as centrais de dados físicas e a separação virtual dos dados e ambientes do cliente), a responsabilidade pela segurança de cargas de trabalho e dados que você coloca na nuvem é totalmente sua. Da mesma forma que você precisa proteger os dados armazenados em suas redes locais, você precisa proteger o seu ambiente na nuvem. Os equívocos em relação à distribuição de responsabilidades são notórios, e as lacunas de segurança resultantes disso transformaram as cargas de trabalho na nuvem na nova mina de ouro dos hackers mais astutos.

Os desafios mais árduos em segurança da nuvem

Dada a simplicidade e o baixo custo da nuvem pública, não surpreende nada que mais e mais organizações estejam se voltando para o Amazon Web Services, Microsoft Azure e Google Cloud Platform. Com elas, você pode colocar novas instâncias em operação em minutos e redistribuir recursos quando necessário enquanto paga apenas pelo que usa, além de evitar os custos iniciais com hardware.

Enquanto a nuvem pública soluciona muitos dos tradicionais desafios de TI, ela também cria novos problemas. O segredo para ter uma segurança virtual eficaz na nuvem é melhorar a sua postura de segurança geral, garantindo que a sua arquitetura esteja segura e configurada corretamente e que você tenha a visibilidade necessária da sua arquitetura e, muito importante, de quem a está acessando.

Ainda que pareça simples, a realidade não é bem assim.

O rápido aumento no uso da nuvem resultou na distribuição de dados desbalanceada, com cargas de trabalho espalhadas por instâncias ou, em alguns casos, plataformas díspares. Em média, as organizações já executam aplicativos em duas nuvens públicas enquanto se emaranham em outras 1,8 nuvens públicas [1]. Essa abordagem multinuvem constitui um desafio de visibilidade para as equipes de TI que precisam pular de plataforma para plataforma para ter uma visão completa de suas áreas de operações na nuvem.

A falta de visibilidade das cargas de trabalho na nuvem pública leva a riscos de segurança e conformidade:

Exposição aumentada

Maior agilidade e melhor tempo de colocação no mercado para produtos e serviços são grandes motivadores para uma organização mudar para a nuvem pública. Isso, em geral, requer a agilidade e receptividade de uma abordagem de DevOps. Para muitos, essa nova abordagem de desenvolvimento e lançamento de um produto envolve vários desenvolvedores trabalhando em diferentes plataformas e, com frequência, em diferentes fusos horários.

Monitorar as cargas de trabalho não era um problema tão grande quando os ciclos de desenvolvimento duravam meses, por vezes anos – mas isso acabou. Você precisa se manter atualizado com as várias versões que, por vezes, são lançadas no mesmo dia. Manter o controle ininterrupto das rápidas mudanças na arquitetura, atualizações na configuração e configurações de grupo de segurança é quase impossível. Tudo isso se acumula em uma receita desastrosa de aumento de exposição a ameaças virtuais, onde as vulnerabilidades podem ser facilmente exploradas.

Ameaças a dados, propriedade intelectual e serviços

As organizações apreciam os benefícios da automação que a nuvem pública oferece tanto quanto os criminosos virtuais. Hoje, os invasores escrutinam cada vez mais os ambientes na nuvem para se aproveitar das APIs nativas do provedor e automatizar implementações em novas instâncias, se instalar em bancos de dados, alterar configurações de segurança e bloquear a entrada de usuários legítimos.

Para quantificar o problema, recentemente o SophosLabs configurou ambientes em 10 das centrais de dados AWS mais populares no mundo. A pesquisa revelou que:

- Em um período de duas horas, todos os 10 sofreram tentativas de login [2]
- Cada dispositivo passou por uma média de 13 tentativas de login por minuto, cerca de 757 por hora

Esses resultados estarrecedores destacam a frequência com que os criminosos virtuais visam às instâncias baseadas na nuvem utilizando-se de sofisticadas técnicas automatizadas. O desafio para as equipes de segurança está em identificar e se proteger contra possíveis vulnerabilidades antes dos invasores e identificar comportamentos incomuns (do invasor) em tempo real para impedir o ataque que se aproxima.

Manutenção das normas de conformidade

Não importa onde a sua infraestrutura e dados sejam mantidos, é preciso demonstrar conformidade com as regulamentações relevantes, incluindo CIS, HIPPA, GDPR e PCI, ou correr o risco de ficar fora das normas regulatórias.

O desafio na nuvem é que os ambientes mudam por dia, por hora, por minuto. Ainda que as verificações de conformidade semanais ou mensais tenham funcionado até então para as redes locais, elas não funcionam tão bem para a nuvem pública. A necessidade de análise contínua de conformidade pode exaurir as forças das equipes que estão gerenciando os ambientes na nuvem manualmente ou com ferramentas nativas. Além disso, uma vez que a questão de conformidade seja identificada, a natureza fractal da segurança, desenvolvimento, operações e conformidade na maioria das organizações é frequentemente pressionada a tratar da situação de modo pontual.

Sete passos para a segurança na nuvem pública

Passo 1: Conheça as suas responsabilidades

Pode parecer óbvio, mas a segurança é tratada um pouco diferente na nuvem. Os provedores de nuvem pública, como Amazon Web Services, Microsoft Azure e Google Cloud Platform, operam sob um modelo de responsabilidade compartilhada, ou seja, eles asseguram a proteção da nuvem enquanto a responsabilidade pela segurança de tudo o que você coloca na nuvem é sua.

Aspectos como proteção física na central de dados, separação virtual dos dados do cliente e ambientes – isso tudo é administrado pelos provedores da nuvem pública.

Você pode até obter algumas regras básicas sobre os tipos de firewall indicados para reger o acesso ao seu ambiente, mas se essas regras não forem configuradas adequadamente – por exemplo, se você deixar a porta de entrada aberta para o mundo –, aí o problema é todo seu. Portanto, conheça as suas responsabilidades com a segurança.

A Fig. 1 dá uma visão geral dessas responsabilidades compartilhadas – ou, se preferir, assista ao vídeo aqui.

Modelo de responsabilidade compartilhada de segurança	No local	Public Cloud	Por quê?
Usuários	■	■	Impor autenticação, definir restrições de acesso e monitorar o uso de credenciais.
Dados	■	■	Bloquear a perda de dados, definir e impor quem pode acessar o quê, enquanto assegura o cumprimento das normas de conformidade.
Aplicativos	■	■	Prevenir o comprometimento do aplicativo através de políticas, patches e segurança.
Controle de redes	■	◪	Monitorar e impor permissões de acesso à rede.
Infraestrutura de host	■	◪	Gerenciar e proteger sistemas operacionais, soluções de armazenamento e sistemas relacionados para evitar bugs sem correção e escalonamento de privilégios.
Segurança física	■	■	Restringir o acesso físico a sistemas e redundância de design para prevenir um ponto único de falha.

■ Cliente ■ Provedor da plataforma

Fig. 1. Visualização resumida da Sophos do modelo de responsabilidade compartilhada. Para obter a versão específica de cada provedor de nuvem, visite sophos.com/public-cloud.

Passo 2: Planeje um serviço multi-cloud

Multinuvem não é mais vista como uma boa estratégia de trabalho. Agora, ela é vista como uma estratégia de trabalho indispensável. Há diferentes motivos para você querer usar várias nuvens, como disponibilidade, agilidade melhorada ou funcionalidade. Ao planejar a sua estratégia de segurança, parta do princípio de que você irá trabalhar com várias nuvens – se não agora, em algum momento no futuro. Dessa forma, você estará coberto para o que vier.

Pense sobre como você irá gerenciar segurança, monitoramento e conformidade entre vários provedores de diferentes nuvens em sistemas e painéis independentes. Quanto mais fácil for a sua experiência de gerenciamento mais fácil será diminuir o tempo de resposta a incidentes, aumentar a detecção de ameaças e reduzir os problemas de auditoria de conformidade. Sem mencionar a retenção dos valiosos membros da equipe.

Busque soluções sem agente que permitam monitorar ambientes de vários provedores de nuvem em um único painel SaaS, reduzindo a quantidade necessária de ferramentas, tempo e pessoas para gerenciar a segurança em várias contas na nuvem em diferentes regiões.

Passo 3: Veja tudo

Se você não pode ver, não pode proteger. É por isso que um dos principais obstáculos para se ter a postura de segurança certa é conseguir ter visibilidade acurada da sua infraestrutura.

Aproveite as ferramentas que oferecem visualização em tempo real da topologia da rede e do fluxo do tráfego com um inventário totalmente detalhado, incluindo hosts, redes, contas de usuários, serviços de armazenamento, contêineres e funções que operam sem servidor.

Para ter uma visibilidade melhorada, busque ferramentas que sejam capazes de identificar possíveis vulnerabilidades dentro da sua arquitetura de modo que você possa prevenir um possível ponto de invasão. As áreas de riscos potenciais incluem:

- Bancos de dados com portas abertas à internet pública que permitiriam que os invasores os acessassem
- Serviços de armazenamento público Amazon S3 (Simple Storage Service)
- Comportamentos suspeitos no login do usuário e chamadas de API – tais como logins múltiplos na mesma conta ao mesmo tempo ou o login de um usuário em diferentes partes do mundo no mesmo dia

Passo 4: Integre a conformidade aos processos diários

Mover cargas de trabalho para a nuvem introduz o desafio de atender a regulamentações de conformidade em toda uma rede mais distribuída, geralmente envolvendo o desenvolvimento regular de versões. Para assegurar a conformidade, você precisa criar relatórios de inventário precisos e diagramas de rede da sua cobertura de nuvem e assegurar que a sua lista de tópicos de conformidade seja atendida em um ambiente dinâmico.

Quando se trata de cumprir prazos de auditoria, frequentemente as organizações se ajeitam temporariamente desviando recursos de projetos de negócios rentáveis para suprir a necessidade imediata. Essa não é uma solução de longo prazo sustentável e, como os instantâneos diários ficam obsoletos em um estalar de dedos, essa situação não oferece a conformidade continuada necessária para o monitoramento de normas como ISO 27001, HIPAA e GDPR.

Busque soluções que permitam elevar os seus padrões de conformidade sem aumentar o número de funcionários, disponibilizando instantâneos em tempo real da sua topologia de rede e detectando automaticamente alterações em seus ambientes de rede em tempo real. Também seria do seu interesse ter a opção de personalizar a política para atender a necessidades específicas do seu setor ou do mercado vertical.

Logicamente que a geração de relatórios é apenas um aspecto da conformidade. Você também precisa tratar das falhas de conformidade. O desafio é que, em geral, é difícil ter as pessoas certas em operações, desenvolvimento e conformidade trabalhando em conjunto devido à falta de canais de colaboração eficientes.

Para que o processo de tratamento de falhas de conformidade seja descomplicado, encontre

soluções que se integrem com as suas soluções de tíquetes existentes, incluindo informações de alerta que podem ser usadas para criar, atribuir e rastrear tíquetes de problemas para resolução, assegurando que tarefas importantes não sejam perdidas, mesmo durante um lançamento.

Passo 5: Automatize os seus controles de segurança

A habilidade de automatizar processos é um dos grandes prazeres do pessoal de DevOps. Já que as suas equipes gostam de automatizar a implantação de modelos de infraestrutura e scripts, economizando horas para o pessoal de desenvolvimento, você deveria considerar atentamente quais controles de segurança poderia automatizar.

Na estrutura de trabalho colaborativa do DevOps, a segurança é uma responsabilidade compartilhada e integrada de ponta a ponta. Essa visão criou o termo "DevSecOps", que enfatiza a necessidade de criar uma fundação sólida de segurança para as iniciativas de desenvolvimento e operações do DevOps.

A necessidade de segurança automatizada fica clara quando pensamos nos crimes cibernéticos, que mais e mais se aproveitam da automação em seus ataques – por exemplo, usando credenciais de usuários roubadas para automatizar o provisionamento de instâncias para atividades como criptojacking, alteração de configurações da conta ou revogação de usuários legítimos para evitar a detecção. De fato, o escrutínio dos ambientes de nuvem em busca de vulnerabilidades em senhas, configurações de grupos de segurança e códigos se tornou uma trivialidade.

Os dois motivos principais de os ataques a ambientes de nuvem pública darem certo são que a configuração da arquitetura não está segura e que a resposta à ameaça não acompanhou o ritmo dos invasores. A automação dos controles de segurança é fator-chave para tratar desses problemas.

Para garantir a segurança dos seus ambientes de nuvem pública, procure uma solução que possa:

- **Corrigir automaticamente as vulnerabilidades e recursos de acesso do usuário**, com entrada de qualquer origem ou de qualquer porta
- **Identificar eventos suspeitos de login e chamadas de API no painel** que sugiram que credenciais de usuários roubadas ou compartilhadas estão sendo usadas por um invasor
- **Informar sobre anomalias no tráfego de saída** para alertar a organização sobre atividades como criptojacking ou exfiltração de dados
- **Revelar cargas de trabalho de aplicações ocultas** do comportamento da instância do computador host para destacar pontos obscuros de exposição (como bancos de dados)

Passo 6: Proteja TODOS os ambientes (inclusive Dev e QA)

Ainda que as violações de dados em nuvem pública que fazem manchete geralmente atinjam o ambiente de produção na nuvem da organização (aquele que os seus clientes utilizam), os invasores não isentarão os seus ambientes de desenvolvimento e qualidade para tomar o seu poder computacional e operar ataques de criptojacking.

Você precisa de uma solução que possa proteger todos os seus ambientes (produção, desenvolvimento e garantia de qualidade) tanto de modo reativo quanto proativo. A solução deve ser capaz de ingerir e digerir os seus logs de atividade (por exemplo, logs de VPC Flow e logs de CloudTrail) para identificar questões que já tenham ocorrido, como quando uma porta indesejada é aberta no firewall. Ao mesmo tempo, a solução deve ser capaz de fazer a varredura proativa de modelos de Infraestrutura como Código (IaC) dos seus repositórios, como o GitHub, e se integrar com as suas ferramentas em pipeline CI/CD, como o Jenkins. Isso assegura que as vulnerabilidades introduzidas no código sejam detectadas bem antes de sua distribuição a seus servidores – evitando uma nova manchete desagradável nos noticiários.

Passo 7: Aplique seu aprendizado em segurança local

Isso pode soar estranho em um guia para nuvens públicas, mas a segurança no local é o resultado de décadas de experiências e pesquisas. Quando se trata de proteger os seus servidores na nuvem contra infecções e perda de dados, pense naquilo que você já faz para a sua infraestrutura convencional e adapte para a nuvem:

- Firewall de última geração: Bloqueie a entrada de ameaças em seus servidores baseados na nuvem colocando um WAF, firewall de aplicativos da web, no gateway da sua nuvem. Pense também em incluir IPS (para ajudar com conformidades) e controle de conteúdo de saída (para proteger servidores/VDI).
- Proteção de servidor: Aplique uma proteção de segurança virtual eficiente a seus servidores baseados na nuvem, exatamente como faria com os seus servidores físicos.
- Proteção de endpoint: Ainda que a sua rede esteja na nuvem, os seus laptops e outros dispositivos estão em terra, e tudo o que é preciso é um e-mail de phishing ou um spyware para roubar as credenciais de seus usuários de contas na nuvem. Garanta que a segurança de endpoints e e-mails esteja atualizada em seus dispositivos para prevenir o acesso não autorizado às contas na nuvem.

Apresentamos o Sophos Cloud Optix:

Veja tudo, proteja tudo

A visibilidade é a fundação sobre a qual todas as atividades e políticas de segurança da nuvem pública são criadas. O Sophos Cloud Optix simplifica o monitoramento de múltiplos ambientes de provedores de nuvem, incluindo contas do Amazon Web Services (AWS), assinaturas do Microsoft Azure, projetos do Google Cloud Platform (GCP), cluster do Kubernetes e repositórios de códigos de desenvolvimento. Essa visibilidade superior recheada de camadas de controles e alertas de políticas de conformidade e DevSecOps permite que as equipes assumam o controle e criem as suas próprias estratégias de segurança na nuvem com confiança.

Definido como um serviço sem agente baseado em SaaS integrado com APIs nativas de provedores de nuvem pública, o Cloud Optix monta automaticamente uma imagem geral da arquitetura, incluindo um inventário completo e uma visualização em tempo real da topologia da rede, com hosts, redes, contas de usuários, serviços de armazenamento, contêineres e funções que operam sem servidor.

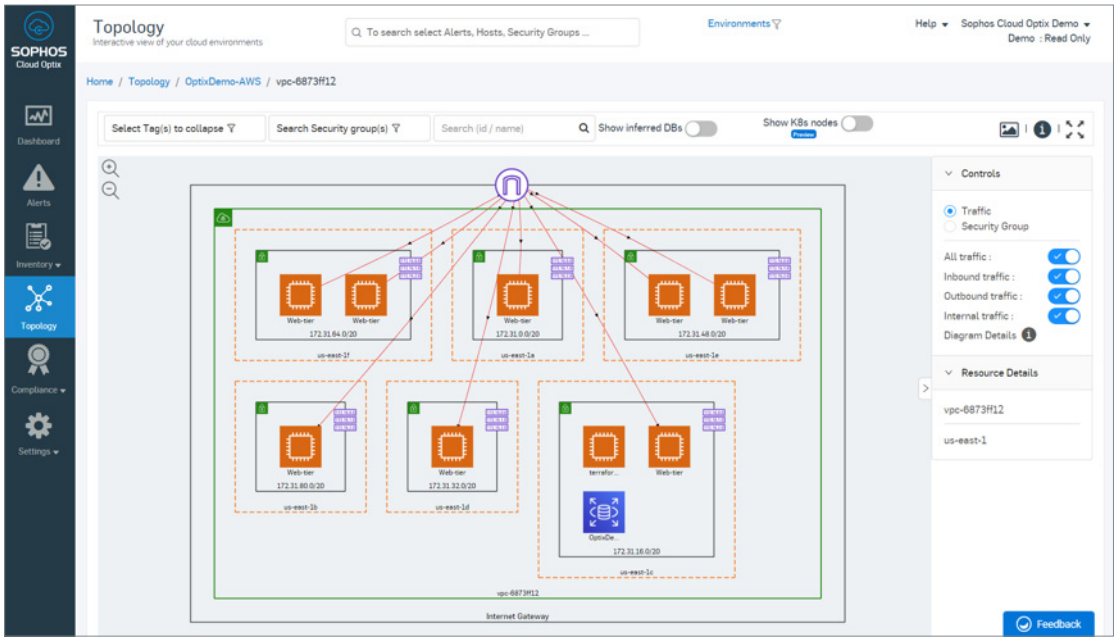

Fig. 2. Visualização da topologia da rede do Sophos Cloud Optix que mostra o tráfego de entrada, saída e interno em um ambiente AWS.

Mais que apenas simples verificações de configuração

O Cloud Optix utiliza a inteligência artificial de Machine Learning para encontrar anomalias e vulnerabilidades de segurança em toda a sua plataforma – monitorando o tráfego na rede, configurações de recursos, eventos de login de usuários e chamadas de API, status de conformidade, repositórios de infraestrutura como código (IaC) e mais, isso tudo com sistemas de proteção para remediar automaticamente alterações acidentais ou maliciosas na configuração da rede.

Para acompanhar, alertas contextuais identificam a causa raiz das questões de segurança e conformidade, permitindo que você se concentre nas áreas mais críticas que precisam de atualizações de segurança, seguindo uma descrição do problema, etapas de remediação e recursos afetados.

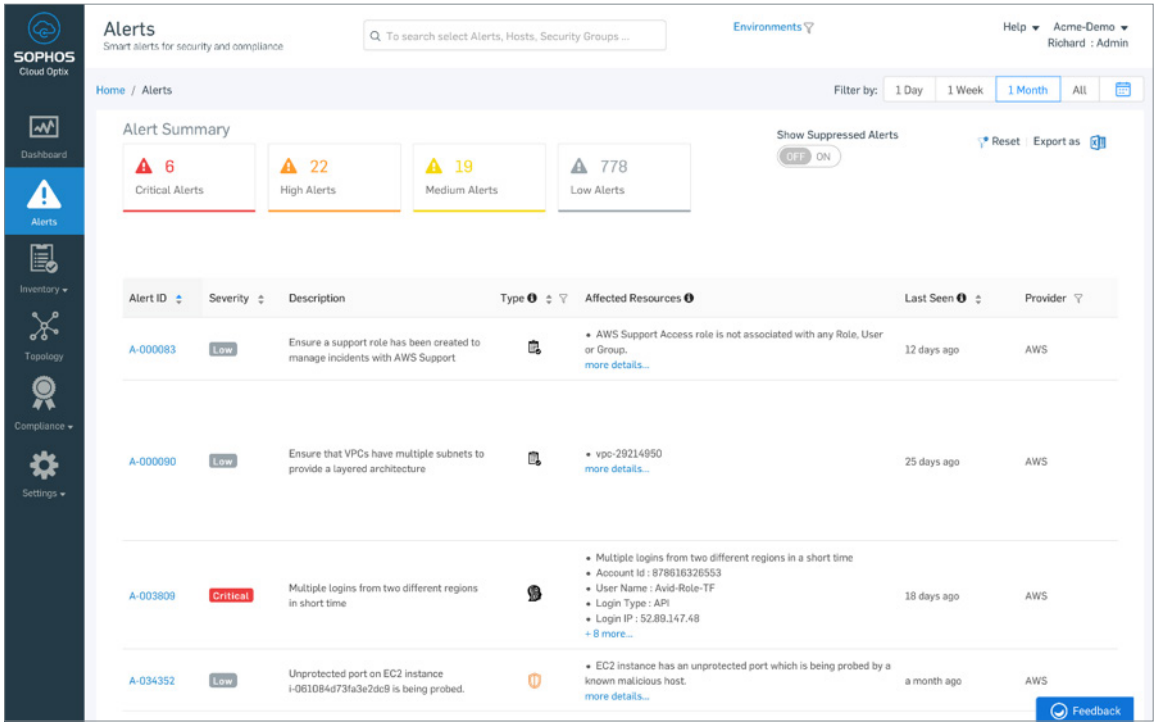

Fig. 3. Resumo de alertas do Sophos Cloud Optix que mostra um alerta crítico de múltiplos logins a uma conta partindo de diferentes regiões simultaneamente.

Monitore e responda do seu jeito

O Cloud Optix oferece API Rest e integração com Splunk, PagerDuty e Amazon GuardDuty para oferecer informações de alerta em tempo real sempre que preciso. Graças às integrações incorporadas com Jira e ServiceNow, as informações de alerta também podem ser usadas para criar tíquetes de problemas que podem ser rastreados até a sua resolução, assegurando que tarefas importantes não sejam perdidas, mesmo durante um lançamento.

Com tudo compactado no painel de modo a oferecer uma vista rápida de relatórios por demanda, você vai economizar horas ou mesmo dias de gerenciamento da postura de segurança na nuvem – além de ajudar a dar os sete passos mais importantes rumo a proteção da nuvem pública.

Saiba mais

O Sophos Cloud Optix é a solução ideal para as organizações que já usam ou que estão mudando para a nuvem pública. Ao combinar o poder da IA com a automação, ele dá à sua organização a visibilidade constante que é necessária para detectar, responder e prevenir vulnerabilidades de conformidade e segurança que, do contrário, poderiam deixar a sua organização exposta.

Para saber mais sobre a solução Sophos Cloud Optix e dar início a uma avaliação de 30 dias sem compromisso em seus ambientes de nuvem, ou se quiser ver uma demonstração on-line já, visite www.sophos.com/cloud-optix.

Conclusão

Mudar de cargas de trabalho convencionais para cargas baseadas na nuvem promove grandes oportunidades para as organizações de todos os tamanhos. Porém, a segurança da nuvem pública é imperativa para proteger sua infraestrutura e sua organização contra ataques virtuais. Seguindo os setes passos descritos neste guia você pode maximizar a segurança nas suas nuvens públicas e, assim, simplificar a geração de relatórios de gerenciamento e conformidade.

Modelo de responsabilidade compartilhada: Como a Sophos pode ajudar

	No local	Public Cloud	Por quê?	Assistência da Sophos
Usuários	■	■	Impor autenticação, definir restrições de acesso e monitorar o uso de credenciais.	O XG Firewall e o Sophos UTM impõem a autenticação de entrada e saída com SSO e 2FA e oferece relatórios detalhados de acesso. O Sophos Cloud Optix monitora o uso compartilhado ou não autorizado de credenciais de contas.
Dados	■	■	Bloquear a perda de dados, definir e impor quem pode acessar o quê, enquanto assegura o cumprimento das normas de conformidade.	O Sophos Cloud Optix oferece monitoramento de automação de conformidade, governança e segurança na nuvem enquanto o Sophos Safeguard, DLP e Sophos Mobile auxiliam na segurança dos dados e determinam as permissões de acesso.
Aplicativos	■	■	Prevenir o comprometimento do aplicativo através de políticas, patches e segurança.	O IPS do XG Firewall e Sophos UTM e o HIPS e Bloqueio do Sophos Server Protection protegem contra ataques a aplicativos e contra a exposição não intencional de aplicativos.
Controle de redes	■	◪	Monitorar e impor permissões de acesso à rede.	A interface descomplicada do XG Firewall e Sophos UTM, a poderosa inspeção de pacote e a Segurança Sincronizada (somente XG) ajudam a proteger e gerenciar o acesso à rede e impor privilégios de rede.
Infraestrutura de host	■	◪	Gerenciar e proteger sistemas operacionais, soluções de armazenamento e sistemas relacionados para evitar bugs sem correção e escalonamento de privilégios.	O Sophos Intercept X protege contra ameaças de dia zero observando técnicas de exploit. O Bloqueio do Sophos Server Protection impõe restrições de tempo de execução e o Sophos XG Sandstorm interrompe a proliferação de códigos desconhecidos.
Segurança física	■	■	Restringir o acesso físico a sistemas e redundância de design para prevenir um ponto único de falha.	O XG Firewall e o Sophos UTM têm opções de implantação de Alta Disponibilidade para equipamentos físicos e plataformas na nuvem.

■ Cliente ■ Provedor da plataforma

Fig. 4. Como a Sophos ajuda com o modelo de responsabilidade compartilhada de nuvem pública

"O Sophos Cloud Optix dá à nossa equipe a visibilidade inteligente de nossos ambientes AWS e o status de conformidade de configuração que precisamos em tempo real, na ponta dos dedos. Com isso temos um nível de monitoramento e alerta que anteriormente era impossível obter. O Sophos Cloud Optix promove uma visão holística das atividades de infraestrutura, permitindo que nos concentremos em proteções mais abrangentes."

Ryan Stinson
Gerente de engenharia de segurança
HubSpot Inc.

1 RightScale 2019 State of the Cloud Report from Flexera

2 Fonte de dados de ataques automatizados: Exposed: Cyberattacks on Cloud Honeypots, Matt Boddy, Sophos, abril de 2019

Faça um test drive do Sophos Cloud Optix

www.sophos.com/cloud-optix

Vendas na América Latina
E-mail: latamsales@sophos.com

Vendas no Brasil
E-mail: Brasil@sophos.com

19-06-19 WP-PTBR (RP)

SOPHOS