Um guia para proteger plataformas de nuvem

Índice

3 Repense sobre a segurança para as aplicações baseadas em nuvem
4 Verifique a identidade e gerencie o acesso em uma plataforma de nuvem
6 Redefina o isolamento e a proteção da rede
7 Proteja dados com criptografia e gerenciamento de chaves
9 Automatize a segurança para DevOps
11 Crie um sistema imune de segurança por meio da monitoração inteligente
12 Segurança que promove o sucesso dos negócios

Principais conclusões

1 De modo ideal, um provedor de nuvem deve ser capaz de integrar o sistema de gerenciamento de identidade de sua empresa com sua plataforma e, em qualquer caso, fornecer uma solução de gerenciamento de identidade confiável para você usar conforme necessário.

2 Como parte do estabelecimento da confiança, verifique se uma plataforma de nuvem oferece firewalls bem integrados, grupos de segurança e opções para microssegmentação baseados em carga de trabalho e hosts de computação confiáveis.

3 Espere que provedores de nuvem ofereçam soluções BYOK que permitam que sua organização gerencie chaves exclusivamente em todo o armazenamento de dados e serviços.

4 A melhor prática de segurança para contêineres é varrê-los em busca de vulnerabilidades antes da implementação e quando eles estão em execução.

5 A segurança da plataforma de nuvem deve controlar efetivamente o acesso, operar no nível de cargas de trabalho, controlar a atividade em detalhes e integrar-se com sistemas locais.

Repense sobre a segurança para as aplicações baseadas em nuvem

À medida que mais organizações migram para um modelo nativo de nuvem para desenvolver apps e gerenciar cargas de trabalho, as plataformas de computação em nuvem estão limitando rapidamente a eficácia do modelo de segurança baseado em perímetro tradicional. Embora ainda necessária, a segurança de perímetro é, por si só, insuficiente. Como os dados e aplicações na nuvem estão fora dos antigos limites da empresa, eles devem ser protegidos de novas maneiras.

As organizações que mudam para um modelo nativo da nuvem ou que planejam implementações de aplicação de nuvem híbrida devem suplementar a segurança de rede tradicional baseada em perímetro com tecnologias que protegem cargas de trabalho baseadas em nuvem. As empresas devem confiar no modo como um provedor de serviços de nuvem protege suas pilhas desde a infraestrutura. Estabelecer confiança na segurança da plataforma se tornou fundamental na escolha de um provedor.

Condutores de segurança de nuvem

A proteção de dados e a conformidade regulamentar estão entre os principais condutores de segurança de nuvem, e são também os inibidores da adoção da nuvem. A abordagem dessas questões se estende a todos os aspectos do desenvolvimento e das operações. Com aplicações nativas da nuvem, os dados podem ser propagados entre armazenamentos de objetos, serviços de dados e nuvens, o que cria várias frontes para potenciais ataques. E os ataques não vêm apenas de sofisticadas gangues cibernéticas e fontes externas, de acordo com uma pesquisa recente, 53% dos entrevistados confirmaram ataques internos nos últimos 12 meses.[1]

Cinco fundamentos da segurança de nuvem

À medida que as organizações atendem às necessidades de segurança especializadas de uso das plataformas de nuvem, elas precisam e esperam que seus provedores se tornem parceiros de tecnologia confiáveis. De fato, uma organização deve avaliar provedores de nuvem com base nesses cinco aspectos de segurança, uma vez que eles se relacionam aos próprios requisitos específicos da organização:

1. **Identity and Access Management (IAM):** autenticação, identidade e controles de acesso
2. **Segurança de rede:** proteção, isolamento e segmentação
3. **Proteção de dados:** criptografia de dados e gerenciamento de chaves
4. **Segurança da aplicação e DevSecOps:** incluindo teste de segurança e segurança de contêiner
5. **Visibilidade e inteligência:** monitoramento e análise de logs, fluxos e eventos em busca de padrões

Verifique a identidade e gerencie o acesso em uma plataforma de nuvem

Qualquer interação com uma plataforma de nuvem começa com a verificação da identidade, o estabelecimento de quem ou o que está fazendo a interação: um administrador, um usuário ou até mesmo um serviço. Na API Economy, os serviços utilizam suas próprias identidades, portanto, a capacidade de fazer uma chamada de API com precisão e segurança para um serviço com base nessa identidade é essencial para executar aplicações nativas da nuvem com sucesso.

Procure provedores que ofereçam uma maneira consistente de autenticar uma identidade para acesso à API e chamadas de serviço. Também é preciso uma maneira de identificar e autenticar usuários finais que acessam aplicações hospedadas na nuvem. Como um exemplo, a IBM Cloud usa o ID do app como uma maneira para a equipe de desenvolvedores integrar a autenticação em seus apps móveis e da web.

Uma autenticação forte impede que usuários não autorizados acessem sistemas em nuvem. Como o Identity and Access Management (IAM) da plataforma é tão fundamental, as organizações que têm um sistema existente esperam que provedores de nuvem integrem o sistema de gerenciamento de identidade de suas empresas. Isso geralmente é suportado por meio da tecnologia de federação de identidade que vincula o ID e os atributos de um indivíduo entre vários sistemas.

Por que autenticar as chamadas de serviço?

Em arquiteturas baseadas em microsserviços, as APIs permitem que as aplicações se comuniquem e compartilhem dados. Quando uma aplicação é executada, ela usa APIs para chamar serviços conforme necessário para concluir várias operações. Por exemplo, sua aplicação pode chamar um serviço de armazenamento de objetos para obter dados. Como parte do cumprimento da solicitação, o próprio serviço de armazenamento de objetos pode, então, chamar um serviço de armazenamento de chaves para obter as chaves de criptografia necessárias para decriptografar os dados. E, como parte da oferta de sua experiência de usuário, uma aplicação pode usar APIs para acessar informações de identidade do usuário, postar conteúdo entre apps (como postar conteúdo de um app no Twitter) e determinar a localização de um usuário para fornecer informações específicas do local. **Todos esses pontos de integração implicam desafios de segurança.**

Os provedores de nuvem devem ter uma maneira consistente para autenticar a identidade de um usuário ou um serviço que precisa acessar uma API ou, até mesmo, um serviço. Obviamente, como parte da autenticação, todas as sessões de solicitação de acesso e transações devem ser registradas para propósitos de auditoria. **As APIs e os serviços muito provavelmente contêm uma propriedade intelectual valiosa, e você não quer que qualquer pessoa os use.**

Peça aos potenciais provedores de nuvem para provar que sua arquitetura e sistemas de IAM cobrem todas as bases. Na IBM Cloud, por exemplo, o Identity and Access Management (IAM) é baseado nos vários recursos-chave (Figura 1):

Identidade

- Cada usuário tem um identificador exclusivo
- Os serviços e aplicações são identificados por seus IDs de serviço
- Os recursos são identificados e tratados pelo nome do recurso de nuvem (CRN)
- Para os usuários e serviços são emitidos tokens autenticados com suas identidades

Gerenciamento de acesso

- À medida que usuários e serviços tentam acessar recursos, um sistema IAM determina se o acesso e as ações são permitidos ou negados
- Os serviços definem ações, recursos e funções
- Os administradores definem políticas que designam funções e permissões de usuários em vários recursos
- A proteção se estende às APIs, funções de nuvem e recursos de back-end hospedados na nuvem

Conforme você avaliar a segurança de um provedor de nuvem, procure listas de controle de acesso juntamente com nomes de recursos comuns que permitam limitar usuários não apenas para determinados recursos, mas também para determinadas operações nesses recursos. Essas capacidades ajudam a assegurar que seus dados sejam protegidos contra acesso externo e interno não autorizado.

Estender seu próprio Enterprise Identity Provider (Enterprise IdP) para a nuvem é particularmente útil quando você desenvolve uma aplicação nativa da nuvem por cima de uma aplicação corporativa existente que usa o Enterprise IdP. Seus usuários podem efetuar login facilmente em ambas as aplicações, nativa da nuvem e subjacente, sem precisar usar vários sistemas ou IDs. Reduzir a complexidade é sempre um objetivo valioso.

Principal conclusão

De modo ideal, um provedor de nuvem deve poder integrar o sistema de gerenciamento de identidade de sua empresa com sua plataforma e, em qualquer caso, fornecer uma solução de gerenciamento de identidade confiável para você usar, conforme necessário.

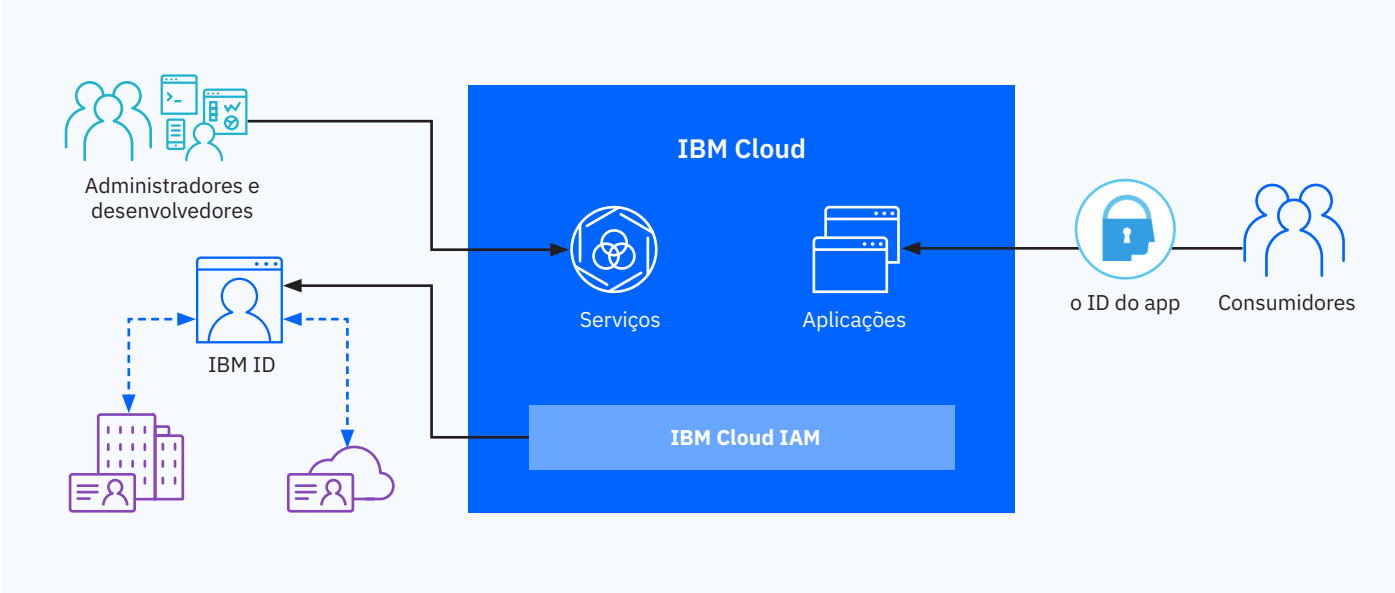


Figura 1. Separação dos elementos de cluster gerenciados pelo fornecedor e gerenciados pelo cliente.

Redefina o isolamento e a proteção da rede

Muitos provedores de nuvem usam segmentação de rede para limitar o acesso a dispositivos e servidores na mesma rede. Além disso, fornecedores criam redes virtuais isoladas por cima da infraestrutura física e limitam automaticamente os usuários ou serviços a uma rede isolada específica. Essas e outras tecnologias básicas de segurança de rede são fundamentais para estabelecer a confiança em uma plataforma de nuvem.

Os provedores de nuvem oferecem tecnologias de proteção, desde firewalls de aplicação da web até redes privadas virtuais e diminuição na negação de serviço, como serviços para segurança de rede definida por software e encargos por uso. Considere as seguintes tecnologias como segurança de rede crucial na era da computação em nuvem.

Grupos de segurança e firewalls

Clientes de nuvem geralmente inserem firewalls de rede para proteção de perímetro (acesso de rede no nível da sub-rede/nuvem privada virtual) e criam grupos de segurança de rede para o acesso no nível da instância. Os grupos de segurança são uma prioridade na linha de defesa para designar o acesso aos recursos de nuvem. É possível usar esses grupos para incluir facilmente a segurança de rede no nível da instância para gerenciar o tráfego de entrada e saída em ambas as redes, pública e privada.

Muitos clientes requerem controle de perímetro para proteger a rede e as sub-redes do perímetro e os firewalls virtuais são uma maneira facilmente implementável para atender a esta necessidade. Os firewalls foram desenvolvidos para evitar que um tráfego indesejado atinja servidores e para reduzir a superfície de ataque. Espera-se que os provedores de nuvem ofereçam firewalls virtuais e de hardware que permitam configurar regras baseadas em permissão para toda a rede ou sub-redes.

As VPNs, é claro, fornecem conexões seguras da nuvem de volta para os seus recursos no local. Elas são um item essencial se você está executando um ambiente de nuvem híbrida.

Microssegmentação

O desenvolvimento de aplicações nativas da nuvem, como um conjunto de pequenos serviços, fornece a vantagem de segurança capaz de isolá-las usando segmentos de rede. Procure uma plataforma de nuvem que implemente a microssegmentação por meio da automação da configuração de rede e do provisionamento de rede. **Aplicações conteinerizadas arquitetadas sobre o modelo de microsserviços estão se tornando rapidamente a norma para suportar o isolamento de carga de trabalho que se amplia.**

Principal conclusão

Como parte do estabelecimento da confiança, verifique se uma plataforma de nuvem oferece firewalls bem integrados, grupos de segurança e opções para microssegmentação baseados em carga de trabalho e hosts de computação confiáveis.

Proteja dados com criptografia e gerenciamento de chaves

A proteção confiável de dados é o fundamento de segurança para qualquer negócio digital, especialmente aqueles em setores altamente regulados como serviços financeiros e assistência médica.

Os dados associados as aplicações nativas da nuvem podem ser propagados entre armazenamentos de objetos, serviços de dados e nuvens. As aplicações tradicionais podem ter seu próprio banco de dados, sua própria VM e dados sensíveis localizados em arquivos. Nesses casos, a criptografia de dados sensíveis em repouso e em movimento se torna crítica.

As empresas estão certas em se preocupar com operadores de nuvem ou outros usuários não autorizados acessando seus dados sem seu conhecimento e em esperar visibilidade completa quanto ao acesso aos dados. **Controlar o acesso aos dados com criptografia e, também, controlar o acesso às chaves de criptografia estão se tornando proteções esperadas.** Como resultado, um modelo bring-your-own-keys (BYOK) agora é um requisito de segurança de nuvem. Ele permite gerenciar as chaves de criptografia em um local central, fornece a garantia de que as chaves raízes nunca sairão dos limites do sistema de gerenciamento de chaves e permite auditar todas as atividades de ciclo de vida de gerenciamento de chaves (Figura 2).

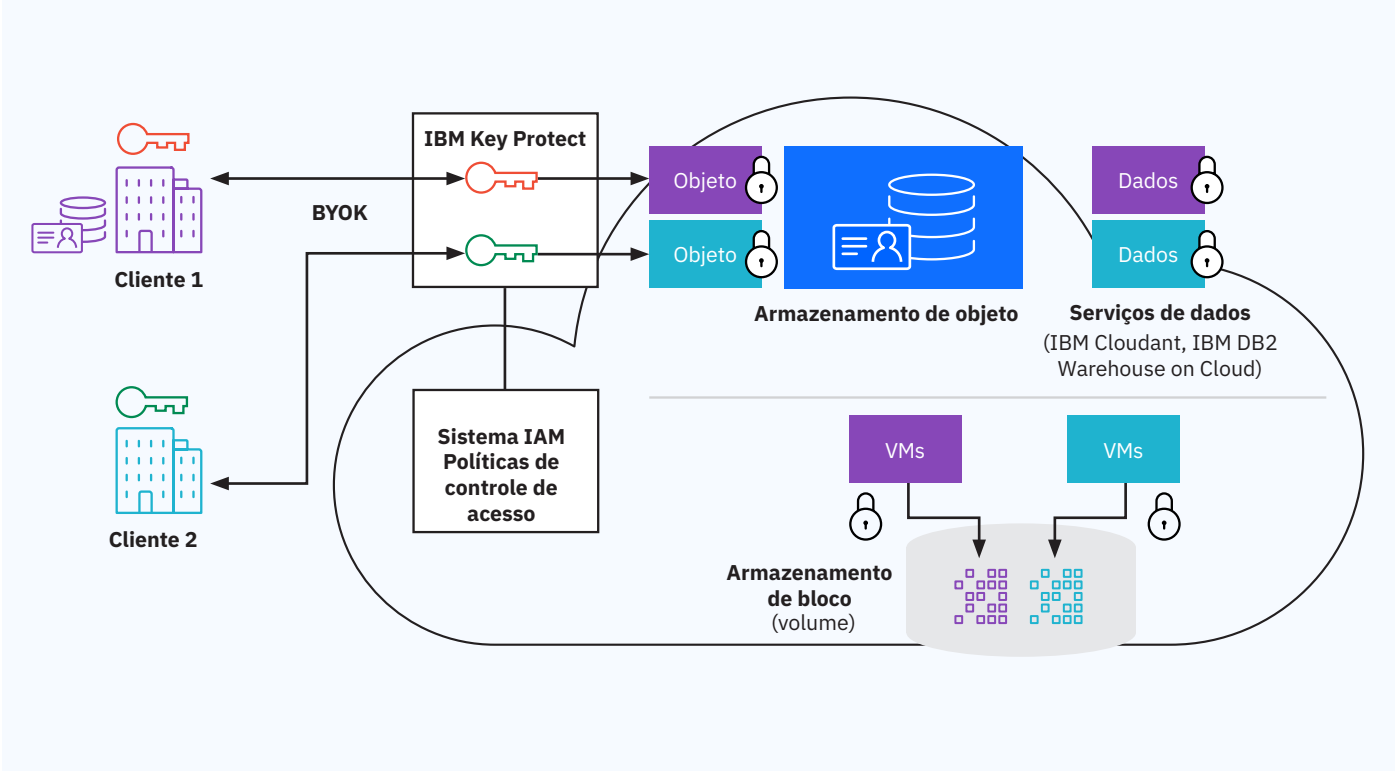
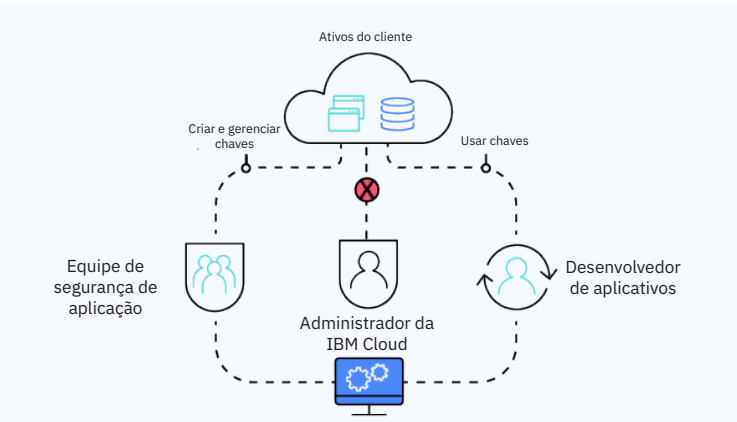


Figura 2. Arquitetura de uma solução BYOK.

Keep your own key (KYOK)

Para implementar a segurança de dados que permanece 100% privada dentro da nuvem pública, a IBM oferece exclusivamente uma solução que permite que você seja unicamente responsável por sua chave de criptografia. Como o único serviço no setor desenvolvido com hardware certificado com FIPS 140-2 Nível 4, o IBM Cloud Hyper Protect Crypto Services fornece um gerenciamento de chaves e um módulo de segurança de hardware (HSM) de nuvem.



Hosts de computação confiáveis

Tudo se resume ao hardware: ninguém deseja implementar dados e aplicações valiosas em um host não confiável. Os fornecedores de plataforma de nuvem que oferecem hardware com protocolos de medição-verificação-ativação oferecem hosts altamente seguros para aplicações implementadas dentro do sistema de orquestração de contêiner.

Intel Trusted Execution Technology (Intel TXT) e Trusted Platform Module (TPM) são exemplos de tecnologias no nível do host que permitem a confiança nas plataformas de nuvem. O Intel TXT defende contra-ataques baseados em software voltados ao roubo de informações sensíveis, corrompendo o sistema ou código BIOS ou modificando a configuração da plataforma. O Intel TPM é um dispositivo de segurança baseado em hardware que ajuda a proteger o processo de inicialização do sistema assegurando que ele esteja livre de violações antes de liberar o controle do sistema para o sistema operacional.

Proteção de dados em repouso e em trânsito

A criptografia integrada com BYOK permite manter o controle de seus dados, sejam eles baseados localmente ou na nuvem. Ela é uma excelente maneira de controlar o acesso aos dados em implementações de aplicação nativa da nuvem. Nessa abordagem, o sistema de gerenciamento de chaves do cliente gera uma chave no local e a transmite para o serviço de gerenciamento de chaves do fornecedor. Essa abordagem abrange a criptografia de dados em repouso entre tipos de armazenamento como bloco, objeto e serviços de dados.

Para dados em trânsito, a comunicação e a transferência seguras ocorrem por meio de Transport Layer Security/Secure Sockets Layer (TLS/SSL). A criptografia de TLS/SSL também permite demonstrar conformidade, segurança e governança sem precisar de controle administrativo sobre o criptossistema ou a infraestrutura. A capacidade de gerenciar certificados SSL é um requisito para confiança em uma plataforma de nuvem.

Atendendo às necessidades de auditoria e conformidade

Fornecer suas próprias chaves de criptografia e mantê-las na nuvem, sem acesso de provedor de serviços, dá a você a visibilidade e o controle das informações necessárias para auditorias de conformidade CISO.

Principal conclusão

Espere que provedores de nuvem ofereçam soluções BYOK que permitam que sua organização gerencie chaves em todo o armazenamento de dados e serviços.

Automatize a segurança para DevOps

À medida que as equipes DevOps criam serviços nativos da nuvem e trabalham com tecnologias de contêiner, elas precisam de uma maneira de integrar verificações de segurança dentro de um pipeline cada vez mais automatizado. Por conta de sites como o Docker Hub que promovem troca aberta, a equipe de desenvolvedores pode economizar facilmente o tempo de preparação da imagem simplesmente fazendo o download do que precisam. Mas com essa flexibilidade vem a necessidade de inspecionar rotineiramente todas as imagens de contêiner colocadas em um registro antes que elas sejam implementadas.

Um sistema de varredura automatizado ajuda a assegurar a confiança procurando potenciais vulnerabilidades em suas imagens antes que você comece a executá-las. Pergunte aos fornecedores de plataforma se eles permitem que sua organização crie políticas (como “não implementar imagens que têm vulnerabilidades” ou “avise-me antes de implementar essas imagens na produção”) como parte da segurança de pipeline DevOps.

O IBM Cloud Container Service, por exemplo, oferece um sistema Vulnerability Advisor (VA) para fornecer varredura de contêiner estática e em tempo real. O VA inspeciona todas as camadas de cada imagem no registro privado do cliente de nuvem para detectar vulnerabilidades ou malware antes da implementação da imagem. Como a simples varredura de imagens de registro pode deixar passar problemas como o desvio da imagem estática para contêineres implementados, o VA também varre contêineres em execução em busca de anomalias. Ele também fornece recomendações na forma de alertas em camadas.

Principal conclusão

A melhor prática de segurança para contêineres é varrê-los em busca de vulnerabilidades antes da implementação e quando eles estão em execução.

Outros recursos de VA que ajudam a automatizar a segurança no pipeline DevOps incluem:

- **Configurações de violação de política:** com o VA, os administradores podem configurar políticas de implementação de imagem baseadas em três tipos de situações de falha de imagem: pacotes instalados com vulnerabilidades conhecidas, logins remotos ativados e logins remotos ativados com alguns usuários que possuem senhas fáceis de adivinhar.
- **Melhores práticas:** atualmente, o VA verifica 26 regras baseadas em ISO 27000, incluindo configurações como a idade e o comprimento mínimos da senha.
- **Detecção de erro de configuração de segurança:** o VA sinaliza cada problema de erro de configuração, fornece uma descrição dele e recomenda um curso de ação para remediá-lo.
- **Integração com o IBM X-Force:** o VA extrai inteligência de segurança de cinco fontes de terceiros e usa critérios como vetor de ataque, complexidade e disponibilidade de uma correção conhecida para classificar cada vulnerabilidade. O sistema de classificação (crítico, alto, moderado ou baixo) ajuda os administradores a entender rapidamente a severidade das vulnerabilidades e a priorizar a correção.

Quando se trata de correção, o VA não interrompe a execução de imagens para a correção. Em vez disso, a IBM corrige a imagem “de ouro” no registro e implementa uma nova imagem no contêiner. Essa abordagem ajuda a assegurar que todas as futuras instanciações dessa imagem tenham a mesma correção em vigor. As VMs ainda podem ser manipuladas tradicionalmente, usando um serviço de segurança de terminal para corrigir as VMs e as vulnerabilidades de segurança do Linux.

Discussão do Kubernetes

Se suas equipes DevOps trabalham com o popular software de orquestração de contêiner Kubernetes, assegure-se que elas possam continuar usando suas ferramentas preferenciais. Além disso, avalie com que facilidade uma plataforma provisiona novos clusters Kubernetes e gerencia os existentes.

Pergunte se um fornecedor de plataforma de nuvem suporta Calico e Istio com seu sistema Kubernetes. Calico e Istio são dois componentes importantes do Kubernetes que ajudam na segurança da aplicação e da carga de trabalho. Calico ajuda a simplificar o gerenciamento de endereços IP designados às cargas de trabalho em um nó de cálculo e os programas acessam listas de controle em cada nó de cálculo para impor políticas de segurança. Usando definições de política configuradas e aplicadas por meio de rótulos de configuração, o Istio fornece controle de comunicação baseado em certificado entre microsserviços dentro de um pod ou cluster Kubernetes.

Crie um sistema imune de segurança por meio da monitoração inteligente

Ao mover para a nuvem, os CISOs geralmente se preocupam com a baixa visibilidade e com a perda de controle. Já que a nuvem inteira da organização pode ficar indisponível se uma chave específica for excluída ou uma mudança na configuração corta inadvertidamente uma conexão de volta para os recursos no local ou a um centro de operações de segurança (SOC) da empresa, por que profissionais de engenharia de operações não deveriam esperar total visibilidade quanto a cargas de trabalho, APIs e microsserviços baseados em nuvem?

Trilhas de acesso e logs de auditoria

Todo o acesso de usuário e administrativo, seja pelo provedor de nuvem ou por sua organização, deve ser registrado automaticamente. Um rastreador de atividade de nuvem integrado pode criar uma trilha de todo o acesso à plataforma e aos serviços, incluindo API, web e acesso a partir de dispositivos móveis. Sua organização deve estar apta a consumir esses logs e integrá-los em seu SOC corporativo.

Inteligência de segurança da empresa

Certifique-se de ter a opção de integrar todos os logs e eventos em seu sistema Security Information and Event Management (SIEM) localmente (Figura 3). Alguns fornecedores de serviço de nuvem também oferecem monitoração de segurança com gerenciamento de incidentes e relatório, análise em tempo real de alertas de segurança e uma visualização integrada entre implementações híbridas.

O IBM QRadar, por exemplo, é uma solução de SIEM abrangente que oferece um conjunto de soluções de inteligência de segurança que pode crescer com as necessidades de uma organização. Suas capacidades de aprendizado de máquina são treinadas com base em padrões de ameaça de uma maneira que constrói um sistema imune de segurança preditiva.

Segurança gerenciada com conhecimento

Se sua organização não tem um conhecimento de segurança significativo, explore provedores que possam gerenciar a segurança para você. Alguns provedores podem monitorar seus incidentes de segurança, aplicar inteligência de ameaça de uma variedade de setores e correlacionar essas informações para tomar uma ação. Pergunte se eles também podem fornecer um único painel de vidro que integre serviços de segurança internos e gerenciados.

Principal conclusão

A segurança da plataforma de nuvem deve controlar efetivamente o acesso, operar no nível de cargas de trabalho, controlar a atividade em detalhes e integrar-se com sistemas no local.

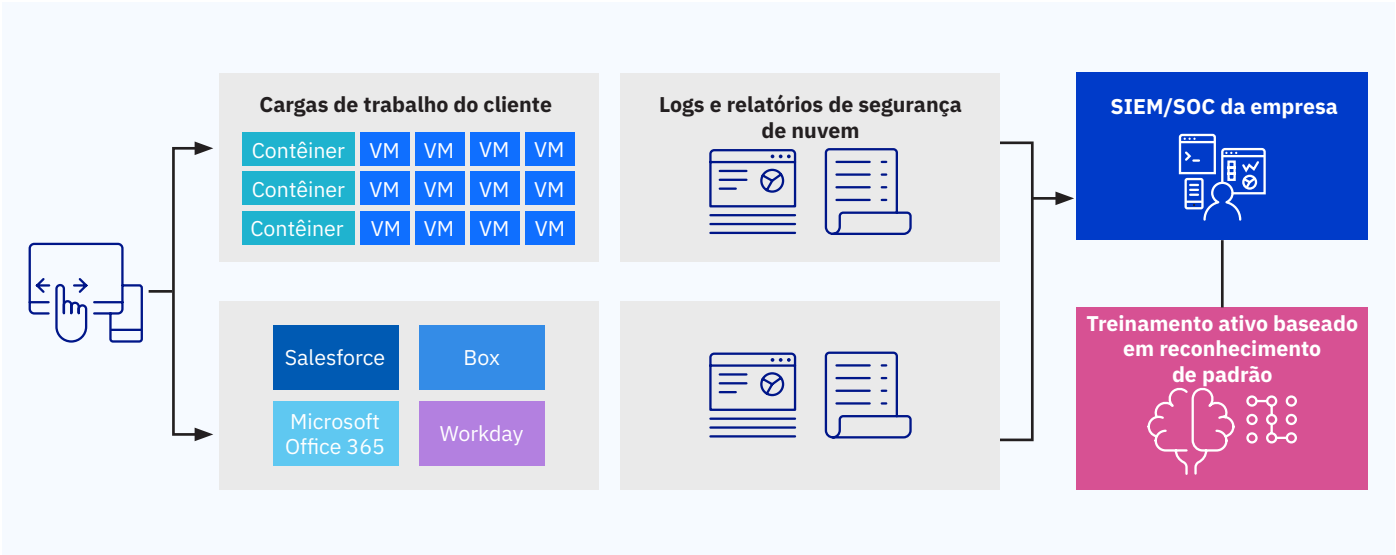


Figura 3. Integrando a visibilidade de nuvem em um SIEM/SOC da empresa.

Segurança que promove o sucesso dos negócios

Com a tecnologia de nuvem se tornando uma parte maior e mais importante da realização de um negócio digital, ela literalmente paga para procurar um provedor de nuvem que ofereça o conjunto ideal de capacidades e controles para proteger seus dados, aplicações e a infraestrutura em nuvem da qual as aplicações voltadas para cliente dependem. Espera-se que a solução de segurança de plataforma cubra as cinco principais áreas de foco da segurança de nuvem: identidade e acesso; segurança de rede; proteção de dados; segurança de aplicação e visibilidade e inteligência. O objetivo é se preocupar menos com a tecnologia e focar mais em seu negócio principal.

Uma nuvem bem protegida oferece vantagens de negócios e de TI significativas, incluindo:

- **Retorno mais rápido:** como a segurança já está instalada e configurada, as equipes podem provisionar facilmente recursos e criar rapidamente protótipos de experiências de usuário, avaliar resultados e iterar conforme necessário.
- **Custo de capital reduzido:** o uso de serviços de segurança na nuvem pode eliminar vários custos iniciais, incluindo servidores, licenças de software e dispositivos.
- **Carga administrativa reduzida:** ao estabelecer e manter com sucesso a confiança na plataforma de nuvem, o provedor com as ofertas de segurança certas assume a maior carga de administração, reduzindo seus custos de relatório e de manutenção de recursos.

Verifique o Gartner Peer Insights para ver por que a IBM Cloud:

Recebeu as avaliações mais altas para integração corporativa (4,6 de 5 estrelas)

E foi classificada com a maior pontuação geral entre os provedores líderes de nuvem (4,7 de 5 estrelas)

...baseado em **90 avaliações durante os últimos 12 meses, a partir de 1º de junho de 2020.**

https://www.gartner.com/reviews/market/public-cloud-iaas/vendor/ibm/product/ibm-cloud

As avaliações da Gartner Peer Insights constituem em opiniões subjetivas de usuários finais individuais baseadas em suas próprias experiências e não representam os pontos de vista da Gartner ou de suas afiliadas.

Para obter mais informações

Para saber mais sobre as cinco principais áreas de segurança de nuvem e as tecnologias e os serviços relacionados da IBM, visite: ibm.com/cloud/security

Fique conectado

Blog IBM Cloud

Siga-nos

@IBMcloud
Facebook

Conecte-se a nós

LinkedIn
YouTube

IBM Brasil Ltda
Rua Tutóia, 1157
CEP 04007-900
São Paulo – SP
Brasil

A página inicial da IBM pode ser localizada em:
ibm.com

[1] Insider Threat Report 2018, publicado em novembro de 2017, http://crowdresearchpartners.com/portfolio/insider-threat-report