Um guia para proteger plataformas em nuvem

Principais conceitos

1 De preferência, um fornecedor de nuvem deve estar apto a integrar o sistema de gerenciamento de identidade de sua empresa em sua plataforma—e, em qualquer caso, fornecer uma solução de gerenciamento de identidade confiável que possa ser usada conforme a necessidade.

2 Para estabelecer a confiança, verifique se uma plataforma em nuvem oferece firewalls, grupos de segurança e opções bem-integrados para microssegmentação, com base na carga de trabalho e nos hosts de cálculo confiáveis.

3 Exija que os fornecedores de nuvem ofereçam soluções BYOK que permitam que sua organização gerencie as chaves exclusivamente em todo o armazenamento de dados e em todos os serviços.

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

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

Repense na segurança para aplicativos na nuvem

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

As organizações que fazem a transição para um modelo de nuvem nativa ou que planejam realizar implementações de aplicativo em nuvem híbrida devem complementar a segurança de rede tradicional baseada em perímetro com tecnologias que protejam as cargas de trabalho na nuvem. As empresas devem confiar no provedor de serviços em nuvem, pois ele protegerá sua pilha em toda a infraestrutura. Estabelecer a confiança na segurança da plataforma se tornou fundamental para a escolha de um fornecedor.

Motivadores de segurança da nuvem

A proteção dos dados e a conformidade regulatória estão entre os principais motivadores da segurança da nuvem—e eles também são inibidores da adoção de nuvem. A abordagem dessas questões abrange todos os aspectos do desenvolvimento e das operações. Com aplicativos em nuvem nativa, os dados podem ser difundidos entre armazenamentos de objetos, serviços de dados e nuvens, o que cria diversas frentes para possíveis ataques. E os ataques não estão vindo apenas de gangues cibernéticas sofisticadas e de origens externas. De acordo com uma pesquisa de opinião recente, 53% dos entrevistados confirmaram ataques internos nos últimos 12 meses. [1]

Cinco fundamentos da segurança de nuvem

À medida que as organizações tratam da necessidade de uma segurança especializada ao usar plataformas em nuvem, elas precisam e esperam que seus fornecedores se tornem parceiros de tecnologia confiáveis. Na verdade, uma organização deve avaliar os fornecedores de nuvem com base nesses cinco aspectos da segurança, pois eles estão relacionados aos próprios requisitos específicos da organização:

1. **Gestão de identidade e acesso:** autenticação, controles de identidade e acesso
2. **Segurança de rede:** proteção, isolamento e segmentação
3. **Proteção de dados:** criptografia de dados e gerenciamento de chave
4. **Segurança de aplicativos e DevSecOps:** incluindo teste de segurança e segurança de contêiner
5. **Visibilidade e inteligência:** monitoramento e análise de logs, fluxos e eventos para obter padrões

Verifique a identidade e gerencie o acesso da plataforma em nuvem

Qualquer interação com uma plataforma em nuvem começa com a verificação de identidade, estabelecendo quem ou o que está fazendo a interação—um administrador, um usuário ou até mesmo um serviço.

Na economia da API, os serviços assumem suas próprias identidades, portanto, a capacidade de fazer uma chamada API de maneira precisa e segura para um serviço com base nessa identidade é essencial para executar apps de nuvem nativa com êxito.

Procure fornecedores que ofereçam uma maneira consistente de autenticar uma identidade para acesso à API e chamadas de serviço. Também é necessária uma maneira de identificar e autenticar usuários finais que acessam aplicativos hospedados na nuvem.

Como exemplo, o IBM® Cloud usa ID de App como uma maneira de desenvolvedores integrarem a autenticação em seus apps móveis e da web.

A autenticação eficiente evita que usuários não autorizados acessem sistemas de nuvem. Já que a gestão de identidade e acesso (IAM) da plataforma é tão fundamental, as organizações que possuem um sistema existente devem esperar que os fornecedores de nuvem integrem o sistema de gestão de identidadede suas empresas. Isso geralmente é suportado por meio da tecnologia de federação de identidade, que vincula o ID e os atributos de uma pessoa em diversos sistemas.

Por que autenticar chamadas de serviço?

Em arquiteturas com base em microsserviços, as APIs permitem que os aplicativos se comuniquem e compartilhem dados. Quando um aplicativo é executado, ele usa APIs para chamar serviços, conforme necessário, para a conclusão de diversas operações. Por exemplo, seu aplicativo pode chamar um serviço de armazenamento de objetos para obter dados. Como parte do cumprimento do pedido, o próprio serviço de armazenamento de objetos pode, então, chamar um serviço de gerenciamento de chave para obter as chaves de criptografia necessárias para decriptografar os dados. E, como parte da entrega da experiência do usuário, um aplicativo pode usar APIs para acessar informações de identidade do usuário, postar conteúdo entre apps (como postar conteúdo de um aplicativo no Twitter) e determinar a localização de um usuário para fornecer informações específicas do local. **Todos esses pontos de integração representam desafios de segurança.**

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

Peça que os fornecedores de nuvem em potencial provem que suas arquiteturas e sistemas de IAM abrangem todas as bases. Na IBM Cloud, por exemplo, a gestão de identidade e acesso é baseadaem diversos recursos-chave (Figura 1):

Identidade

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

Gerenciamento de acesso

- Conforme os usuários e serviços tentam acessar os recursos, um sistema IAM determina se o acesso e as ações são permitidos ou negados
- Os serviços definem as ações, os recursos e as funções
- Os administradores definem as políticas que designam as funções e permissões dos usuários em diversos recursos
- A proteção se estende às APIs, às funções de nuvem e aos recursos de backend hospedados na nuvem

À medida que você avaliar a segurança de um fornecedor de nuvem, procure por listas de controle de acesso, juntamente com nomes de recursoscomuns que permitam limitar os usuários não apenas a determinados recursos, mas também a determinadas operações nesses recursos. Esses recursos permitem que seus dados estejam protegidos contra acesso externo e interno não autorizado.

Estender seu próprio fornecedor de identidade da empresa (IdP da Empresa) para a nuvem é particularmente útil quando você constrói um aplicativo em nuvem nativa por cima de um aplicativo corporativo existente que usa o IdP da empresa. Seus usuários podem efetuar login facilmente nos aplicativos em nuvem nativa e subjacentes sem precisar usar diversos sistemas ou IDs. Reduzir a complexidade é sempre um objetivo valioso.

Principal conceito

De preferência, um fornecedorde nuvem deve estar apto a integraro sistema de gerenciamento de identidade de sua empresa em sua plataforma—e, em qualquer caso, fornecer uma solução de gerenciamento de identidade confiável para uso, conforme a necessidade.

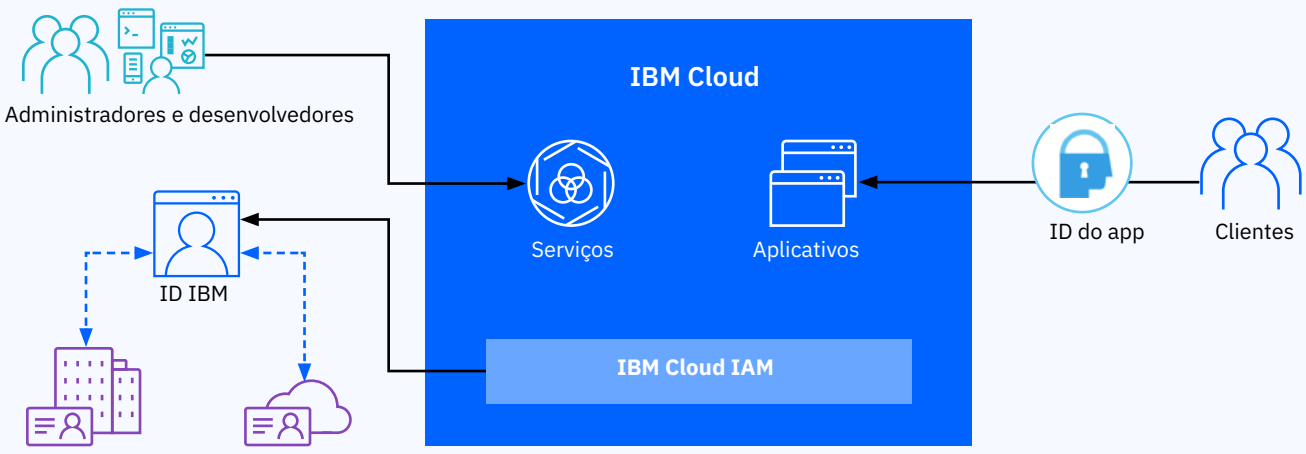

Figura 1. Separação dos elementos de cluster gerenciados pelo fornecedor e gerenciados pelo cliente.

Redefina o isolamento e a proteção da rede

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

Os fornecedores de nuvem oferecem tecnologias de proteção—que vão desde firewalls de aplicativo da web até redes privadas virtuais e mitigação de negação de serviço—como serviços para segurança de rede definida por software e encargos por uso. Considere as seguintes tecnologias como segurança de rede essencial na era da computação em nuvem.

Grupos e firewalls de segurança

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

Muitos clientes requerem o 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 essa necessidade. Os firewalls são projetados para evitar que tráfego indesejado atinja os servidores e para reduzir a superfície de ataque. Exija que os fornecedores de nuvem ofereçam firewalls virtuais e de hardware que permitam configurar regras baseadas em permissão para toda a rede ou sub-redes.

As VPNs, obviamente, fornecem conexões seguras de nuvem para seus recursos on premises. Elas são um item obrigatório se você está executando um ambiente de nuvem híbrida.

Microssegmentação

O desenvolvimento de aplicativos nativamente em nuvem como um conjunto de pequenos serviços fornece a vantagem de segurança de poder isolá-los usando segmentos de rede. Procure uma plataforma em nuvem que implemente a microssegmentação por meio da automação da configuração e do fornecimento de rede. **Os aplicativos conteinerizados arquitetados no modelo de microsserviços estão rapidamente se tornando padrão no suporte de ajustes de escala no isolamento da carga de trabalho.**

Principal conceito

Para estabelecer a confiança, verifique se uma plataforma em nuvem oferece firewalls, grupos de segurança e opções bem-integrados para microssegmentação, com base na carga de trabalho e nos hosts de cálculo confiáveis.

Proteja os dados com criptografia e gerenciamento de chave

Proteger os dados com confiança é fundamental para a segurança em qualquer negócio digital—especialmente aqueles em segmentos de mercado altamente regulamentados como serviços financeiros e assistência médica.
Os dados associados aos aplicativos em nuvem nativa podem ser difundidos entre armazenamentos de objetos, serviços de dados e nuvens. Aplicativos 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 têm razão em se preocupar com operadores de nuvem ou outros usuários não autorizados acessando seus dados sem seu conhecimento e em exigir total visibilidade no acesso aos dados. **O controle de acesso aos dados com criptografia e também o controle de 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 garantia de que as chaves raízes nunca sairão dos limites do sistema de gerenciamento de chave e permite auditar todas as atividades do ciclo de vida de gerenciamento de chave (Figura 2).

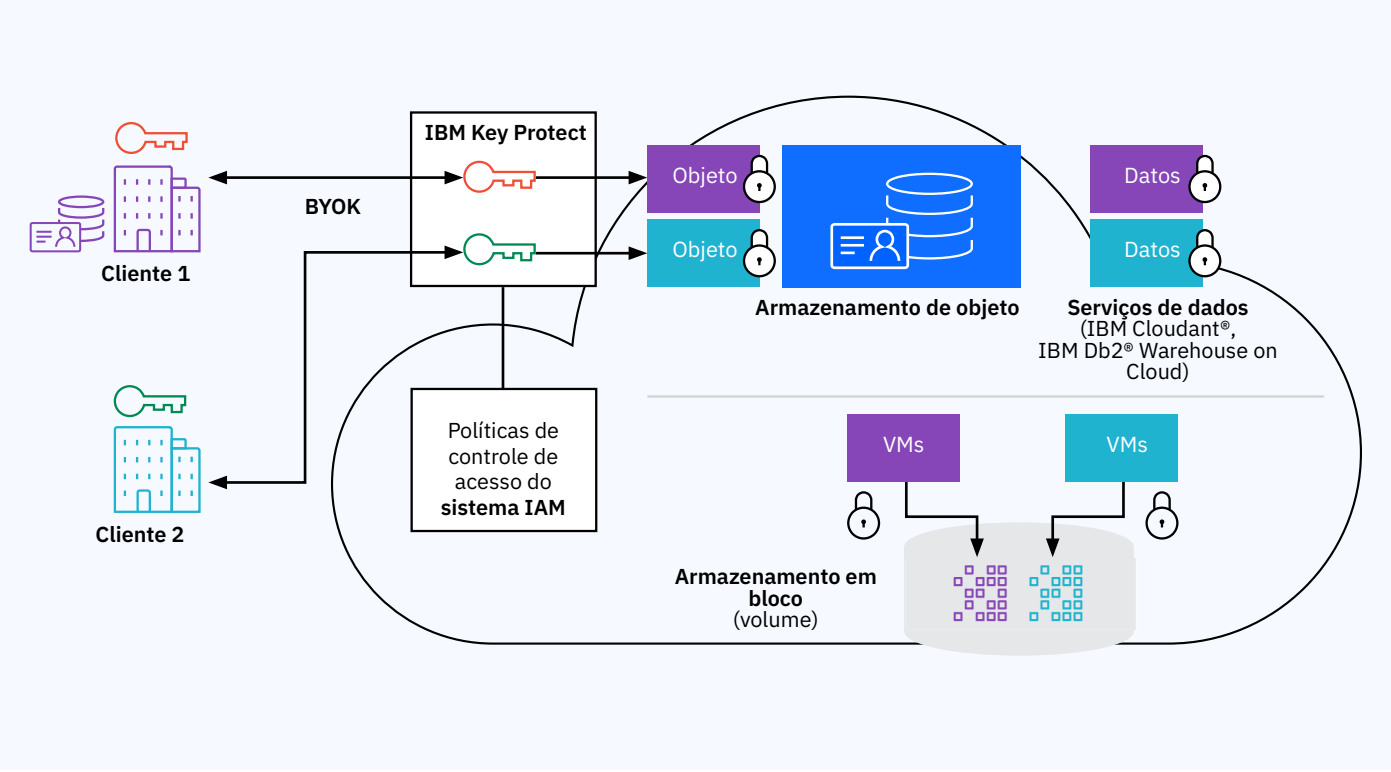

Figura 2. Arquitetura de uma solução BYOK.

Hosts de cálculo confiáveis

No que se refere ao hardware: ninguém deseja implementar dados e aplicativos valiosos em um host não confiável. Os fornecedores de plataforma em nuvem que oferecem hardware com protocolos de medição, verificação e ativação fornecem hosts altamente seguros para aplicativos implementados no sistema de orquestração de contêiner.

O Intel Trusted Execution Technology (Intel TXT) e o Trusted Platform Module (TPM) são exemplos de tecnologias no nível do host que ativam a confiança para plataformas em nuvem. O Intel TXT defende contra ataques baseados em software com o intuito de roubar informações confidenciais corrompendo o sistema ou o 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 armazenados e em transferência

A criptografia integrada com BYOK permite manter o controle de seus dados, sejam eles on premises ou na nuvem. Ela é uma excelente maneira de controlar o acesso aos dados nas implementações de aplicativo em nuvem nativa. Nessa abordagem, o sistema de gerenciamento de chave do cliente gera uma chave on premises e a transmite para o serviço de gerenciamento de chaves do fornecedor. Essa abordagem engloba 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 TLS/SSL também permite demonstrar conformidade, segurança e controle sem requerer controle administrativo no criptossistema ou na infraestrutura. A capacidade de gerenciar certificados SSL é um requisito para a confiança em uma plataforma em nuvem.

Atendendo às necessidades de auditoria e de conformidade

Fornecer suas próprias chaves de criptografia e mantê-las na nuvem — sem acesso ao provedor de serviços — fornece a visibilidade e o controle das informações requeridas para as auditorias de conformidade da CISO.

Principal conceito

Exija que os fornecedores de nuvem ofereçam soluções BYOK que permitam que sua organização gerencie as chaves em todo o armazenamento de dados e em todos os serviços.

Automatize a segurança para DevOps

À medida que as equipes de DevOps constroem serviços de nuvem nativa e trabalham com tecnologias de contêiner, elas precisam de uma maneira de integrar as verificações de segurança dentro de um pipeline cada vez mais automatizado. Pois, da mesma forma que sites como o Docker Hub promovem troca aberta, os desenvolvedores podem economizar facilmente tempo de preparação da imagem simplesmente fazendo download do que eles precisam. Mas comessa 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 possibilita 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 (tais como “não implementar imagens quepossuem vulnerabilidades” ou “avise-me antes de implementar essas imagens na produção”) como parte da segurança de pipeline de DevOps.

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

Principal conceito

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

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

- **Configurações de violação da política:** com o CV, administradores podem configurar políticas de implementação de imagem com base 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 adivinharam facilmente as senhas.
- **Melhores práticas:** o CV atualmente verifica 26 regras com base no ISO 27000, inclusive configurações, como idade mínima da senha e comprimento mínimo
- **Detecção de configuração errônea de segurança:** o CV sinaliza cada problema de configuração errônea, fornece uma descrição dele e recomenda um curso de ação para corrigi-lo.
- **Integração com o IBM X-Force®:** o CV realiza o pull na inteligência de segurança em cinco origens de terceiros e usa critérios como vetor do ataque, complexidade e disponibilidade de uma correção conhecida para classificar cada vulnerabilidade. O sistema de classificação (crítico, alto, moderado ou baixo) ajuda administradores a entender rapidamente a severidade das vulnerabilidades e a priorizar a correção.

Quando se trata da resolução de problemas, o CV não interrompe a execução de imagens para correção. Em vez disso, a IBM corrige a imagem "de ouro" no registro e implementa uma nova imagem no contêiner. Essa abordagem possibilita que todas as instanciações futuras dessa imagem tenham a mesma correção em vigor. As VMs ainda podem ser manipuladas tradicionalmente, usando um serviço de segurança de endpoint para correção de VMs e correção de vulnerabilidades de segurança do Linux.

Referência ao Kubernetes

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

Pergunte se o fornecedor da plataforma em nuvem suporta Calico e Istio com seu sistema Kubernetes. Calico e Istio são dois componentes importantes do Kubernetes, que ajudam na segurança do aplicativo e da carga de trabalho. O Calico ajuda a simplificar o gerenciamento de endereços IP designados às cargas de trabalho em um nó de cálculo e listas de controle de acesso de programas em cada nó de cálculo para impingir as políticas de segurança.

Usando definições de política estabelecidas e impingidas por meio de rótulos de configuração, o Istio fornece controle de comunicação baseado em certificado entre microsserviços dentro de um pod ou cluster do Kubernetes.

Crie um sistema de segurança imune por meio do monitoramento inteligente

Ao mover para a nuvem, as CISOs geralmente se preocupam com a baixa visibilidade e com a perda de controle. Tendo em vista que a nuvem inteira da organização poderia ficar inativa se uma chave específica fosse excluída ou se uma mudança na configuração direcionar inadvertidamente uma conexão para recursos on premises ou com o centro de operações de segurança (SOC) de uma empresa, por que os engenheiros de operações não deveriam exigir total visibilidade das cargas de trabalho, APIs e microsserviços baseados em nuvem, ou seja, de tudo?

Trilhas de acesso e logs de auditoria

Todo o acesso de usuário e administrativo, seja pelo fornecedor de nuvem ou por sua organização, deve ser registrado automaticamente. Um controlador de atividade de nuvem integrado pode criar uma trilha de todo o acesso à plataforma e aos serviços, inclusive acesso de API, web e dispositivo móvel. Sua organização deve estar apta a consumir esses logs e integrá-los no SOC de sua empresa.

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) on premises (Figura 3). Alguns provedores de serviços de nuvem também oferecem monitoramento de segurança com gerenciamento e relatório de incidentes, análise de alertas de segurança em tempo real e uma visualização integrada em implementações híbridas. O IBM QRadar®, por exemplo, é uma solução de SIEM abrangente que oferece um conjunto de soluções de inteligência de segurança que podem crescer com as necessidades de uma organização. Seus recursos de aprendizado de máquina treinam sobre padrões de ameaça de maneira a construir um sistema de segurança imune preditivo.

Segurança gerenciada com conhecimento

Se sua organização não possui conhecimento de segurança significativo, explore fornecedores que possam gerenciar a segurança para você. Alguns fornecedores podem monitorar seus incidentes de segurança, aplicar a inteligência de ameaça a partirde diversas indústrias e correlacionar essas informações para executar ações. Pergunte se eles também podem entregar um único painel de controle que integra serviços de segurança internos e gerenciados.

Principal conceito

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

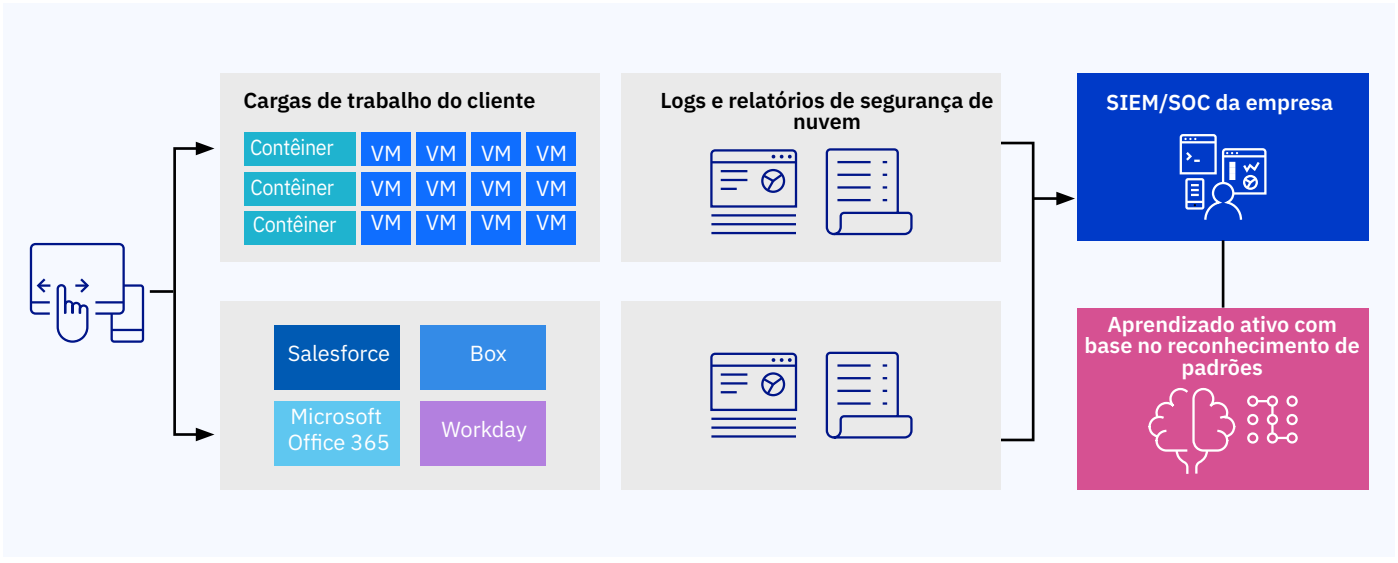

Figura 3. Integrando a visibilidade da nuvem em um SIEM/SOC corporativo.

Segurança que possibilita o sucesso dos negócios

Com a computação em nuvem se tornando uma parte cada vez maior e mais importante na execução de um negócio digital, literalmente paga-se para procurar um fornecedor de nuvem que ofereça o conjunto ideal de recursos e controles para proteger seus dados, aplicativos e a infraestrutura em nuvem da qual os aplicativos voltados para o cliente dependem. Exija 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 do aplicativo e visibilidade e inteligência. O objetivo é se preocupar menos com tecnologia e focar mais no core do seu negócio.

Uma nuvem bem protegida fornece vantagens significativas de negócios e TI, inclusive:

- **Tempo de maturação reduzido:** como a segurança já está instalada e configurada, as equipes podem provisionar recursos facilmente, modelar rapidamente as experiências do usuário, avaliar os resultados e iterar conforme necessário.
- **Custos de capital reduzidos:** o uso de serviços de segurança na nuvem pode eliminar diversos custos iniciais, inclusive servidores, licenças de software e dispositivos.
- **Cargas administrativas reduzidas:** ao estabelecer e manter com sucesso a confiança na plataforma de nuvem, o fornecedor com as melhores ofertas de segurança assume a maior carga de administração, reduzindo seus custos em relatórios e em manutenção de recursos.

Para obter mais informações

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

Fique conectado

Blog da IBM Cloud

Siga-nos

@IBMcloud
Facebook

Entre em contato

LinkedIn
YouTube

IBM Corporation
1 New Orchard Road
Armonk, NY 10504-1722

Produzido nos Estados Unidos da América em janeiro de 2018

[1]Relatório de Ameaça Interna 2018, publicado em novembro de 2017, http://crowdresearchpartners.com/portfolio/insider-threat-report