IBM **Cloud**

Proteção da plataforma do contêiner

Criação de uma cadeia de confiança

IBM

O desafio de DevOps: inovação segura com velocidade

O suporte aos objetivos de negócios em mercados altamente competitivos exige que os executivos de desenvolvimento de aplicativos e as equipes deles ofereçam experiências de alta qualidade aos clientes em todos os tipos de dispositivo em um ritmo acelerado. Como resultado, as equipes de DevOps usam cada vez mais plataformas em nuvem baseadas em contêiner com métodos de colaboração ágeis e uma cadeia de ferramentas para maximizar a automação no processo de criação e iteração de aplicativos nativos em nuvem como microserviços independentes, mas interoperáveis.

Embora a configuração e a manutenção de uma excelente segurança pareçam adicionar atrito ao avançar para um cenário de DevOps baseado em nuvem, a segurança definitivamente não pode ser ignorada. A maioria das plataformas de nuvem usa o Docker para contêineres, por exemplo, e os contêineres são executados em um kernel Linux compartilhado, herdando os desafios de segurança dele. Transferido de uma troca de comunidade, o software de contêineres não autorizado e não detectado que obtém uma escalada privilegiada no kernel do Linux de um host pode começar a exfiltrar dados ou se ramificar para causar danos por meio de ataques de negação de serviço (DoS). Os contêineres também podem interferir em outros contêineres porque todos compartilham acesso a recursos como canais, bibliotecas e binários.

Com a maior adoção do modelo BYOD (traga seu próprio dispositivo), muitas organizações também perderam o controle dos endpoints corporativos, enfraquecendo o perímetro tradicional da empresa. Agora, a segurança deve ir para onde a carga de trabalho se desloca ao passar pelo data center e pela nuvem.

Enquanto a cadeia de ataque (invadir, trancar, expandir, reunir, exfiltrar) permanece a mesma, a engenhosidade dos invasores não tem fim. Manchetes frequentes sobre violações catastróficas refletem que o quadro geral da segurança continua a mudar:

- Os invasores perceberam que o crime cibernético realmente compensa, resultando em um aumento de ameaças persistentes avançadas e outros malwares que se transformam rapidamente.
- Nações se tornaram mais sofisticadas em suas capacidades de guerra cibernética. Em muitos países, os invasores usaram recursos estatais para desenvolver ferramentas sofisticadas com as quais fazem muito mais dinheiro do que em seus trabalhos diários.

Os desafios básicos para proteger uma plataforma de nuvem certamente podem fazer um agente de segurança perder o sono. Um objetivo da CISO é definir a estrutura de segurança e os requisitos da organização para minimizar os riscos e satisfazer a conformidade com os regulamentos. As implementações devem ser auditáveis.

Esses requisitos podem colocar a CISO em desacordo com o executivo de AppDev, que precisa de uma solução de segurança que forneça automação sempre que possível e integre-se com flexibilidade aos processos e aos pipelines de DevOps (se não puder ser totalmente invisível).

Como uma plataforma de nuvem pode atender com eficiência e eficácia as necessidades importantes, porém contrastantes, das principais partes interessadas?

Criação de uma cadeia de confiança

A solução é criar uma cadeia de confiança baseada em hardware que verifique a integridade de todos os componentes relevantes na plataforma de nuvem. **Uma verdadeira cadeia de confiança começaria no firmware do chip host e se desenvolveria pelo mecanismo de contêiner e sistema de orquestração, protegendo todos os dados críticos e as cargas de trabalho durante o ciclo de vida de um aplicativo.** O resultado seria um sistema de contêineres altamente automatizado e confiável.

O hardware é a base ideal porque está enraizado no silício, dificultando a alteração pelos hackers. A cadeia de confiança seria construída com base nessa raiz usando o modelo de segurança de mensuração e verificação, com cada componente mensurando, verificando e iniciando o próximo nível. Esse processo se estenderia ao mecanismo do contêiner, criando um limite de confiança, com mensurações armazenadas em um módulo de plataforma confiável (TPM) no host. Um software de certificação em um servidor diferente compararia as mensurações atuais com valores bons conhecidos. O orquestrador de contêineres se comunicaria com o servidor de certificação para verificar a integridade dos hosts de trabalho e eventuais imagens de contêiner implantadas neles.

Dica importante

Certifique-se de que a plataforma na nuvem aceite um limite de confiança gerenciado por política, o que é essencial para automatizar a segurança.

A Figura 1 representa uma cadeia de confiança, baseada em hardware, que estaria envolvida ao adicionar um novo funcionário a um cluster do Kubernetes. Os números na ilustração correspondem aos passos 1 a 6 descritos aqui. A verificação de uma mensuração no host de inicialização requer comparação com um item conhecido armazenado em um servidor de certificado separado.

1. No host de trabalho, o hardware do TPM autentica o firmware do sistema, mensurando e verificando o BIOS, inclusive as ROMs opcionais. Ele então inicializa o BIOS.
2. O BIOS mensura, verifica e inicializa o sistema operacional (SO).
3. O SO mensura, verifica e inicializa o tempo de execução do contêiner Docker, os plugins do Docker e todos os principais componentes que fazem parte de uma base de computação confiável (TCB).
4. Com um plugin do Cloud Integrity Technology (CIT), o mestre do Kubernetes verifica o host de trabalho pelo servidor de certificação. A certificação também pode envolver a verificação de informações de localização geográfica/limite para o cluster do Kubernetes, como o bloqueio do uso de um funcionário que não seja adequadamente geolocalizado.
5. O mestre do Kubernetes configura o host válido certificado como parte do cluster existente, que inclui a atribuição de contêineres a ele.
6. O mecanismo do Docker no host de trabalho, comunicando-se por meio de uma conexão criptografada com o servidor de certificação, verificaria a integridade das imagens do contêiner e as compararia com a política de segurança.

Por ser orientada por políticas de segurança, toda a plataforma do contêiner executa automaticamente e só hospeda hosts e contêineres em bom estado.

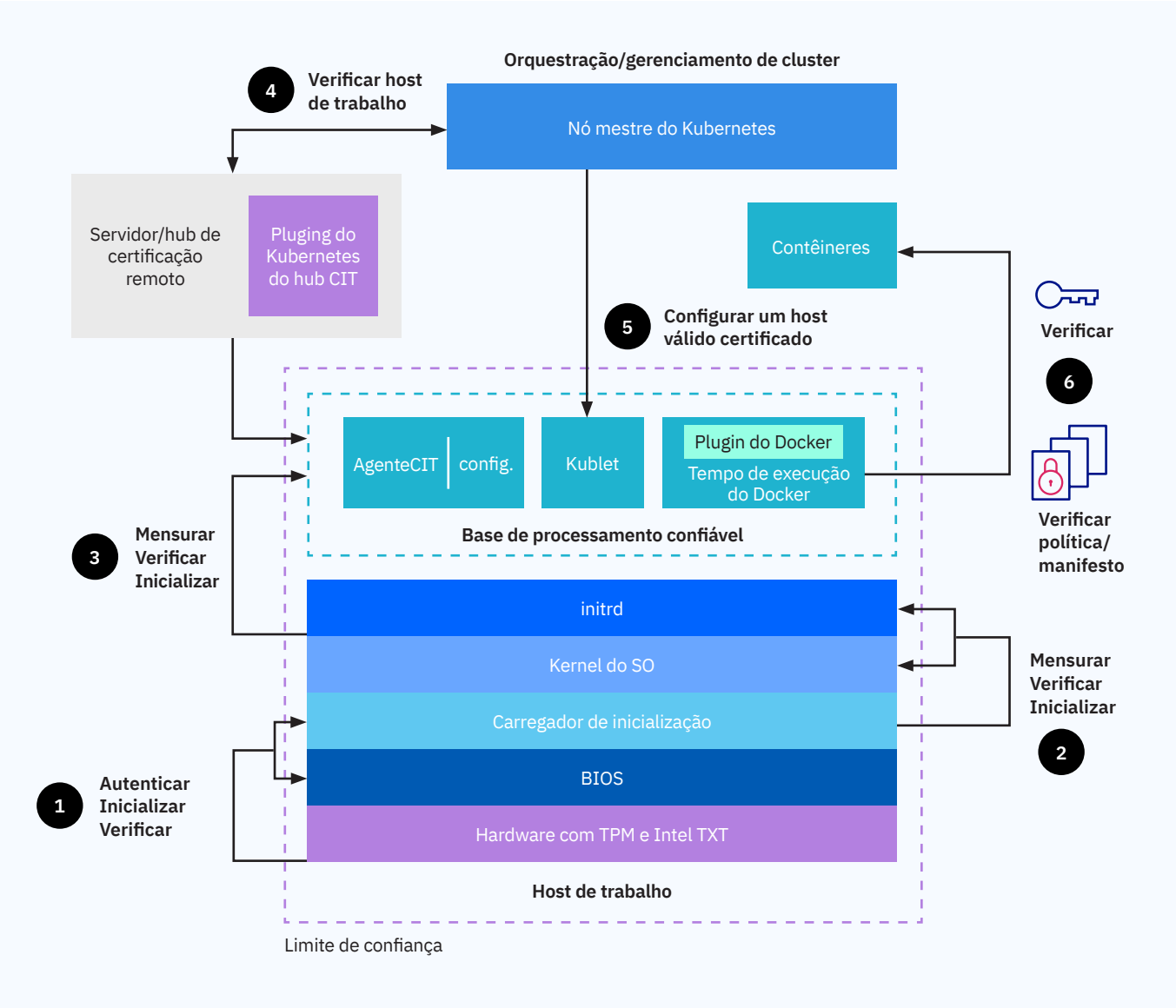


Figura 1. Uma arquitetura de referência que permite uma cadeia de confiança para contêineres que emprega o modelo de segurança de mensuração e verificação como a base que se estende ao nível de orquestração do Kubernetes. Veja na página 3 as descrições completas dos 6 passos.

Viabilização de contêineres confiáveis

Sistemas de contêineres como o Docker têm metodologias integradas para criar microperímetros em torno de elementos separados do sistema que ajudam a proteger a comunicação entre eles.

Para avaliar se os aplicativos em contêiner serão suficientemente protegidos, pergunte ao fornecedor da plataforma em nuvem sobre estes aspectos da implementação do Docker:

As imagens de software são mantidas em um registro privado? As plataformas de nuvem baseadas no Docker Registry V2 podem atribuir a cada organização um registro de imagem privada protegido, no qual as imagens são armazenadas e compartilhadas apenas por usuários e grupos especificados. Adicionar imagens ao registro privado envolve autorizar os usuários a criar ou copiar imagens locais ou a importar uma imagem diretamente de um repositório público, como o Docker Hub.

A implementação do Docker permite a criptografia das imagens dele?
A criptografia protege contra adulterações com as imagens no registro.

Os daemons do Docker que são executados nos hosts de processamento são configurados sem acesso direto do usuário? Eles são configurados apenas pelo provedor de serviços?
A resposta para as duas perguntas deve ser sim. O acesso direto ao host por outros clientes poderia comprometer a segurança dos seus contêineres.

Todos os sockets do daemon do Docker estão protegidos por certificados TLS (Transport Layer Security)?
O TLS combina as vantagens da criptografia de chave pública, da validação externa de terceiros e da criptografia por sessão.

Todos os contêineres Docker privilegiados são permitidos?
A não permissão de contêineres privilegiados permite que os contêineres de outros clientes provedores de serviços não tenham acesso a discos rígidos no host de computação que possam conter seus dados e aplicativos.

Do limite de confiança do nó para a nuvem confiável

Como o nó de processamento se torna o foco no estabelecimento da cadeia de confiança, e como cada nó tem o próprio limite de confiança, todos os membros de um cluster e pod do Kubernetes começam a proteger a carga de trabalho geral antes que ocorra qualquer processamento e transferência de dados.

Espere que os provedores de nuvem descrevam e demonstrem as tecnologias de confiança deles. Por exemplo, o Intel Trusted Execution Technology (Intel TXT), qualquer TPM que esteja em conformidade com as especificações 1.2 ou 2.0 e o Intel CIT são tecnologias estabelecidas que um provedor pode usar para criar uma nuvem confiável.

- **O Intel TXT** defende contra ataques baseados em software que visam roubar informações confidenciais corrompendo o sistema ou o código BIOS, ou ainda modificando a configuração da plataforma.
- **O TPM** é um dispositivo de segurança baseado em hardware que armazena as mensurações usadas no processo de segurança de mensuração e verificação. Ele ajuda a garantir que o sistema esteja livre de violações antes de liberar o controle do sistema para o próximo nível de software.
- **O Intel CIT** se baseia na raiz da confiança para fornecer informações de certificação orientadas por políticas, de modo que as cargas de trabalho sejam executadas em hardware verificado com conformidade em ambientes de nuvem pública e privada.

A certificação remota é uma etapa importante no processo de confiança, estendendo-se além do limite de confiança do host até o nível de orquestração do contêiner. Um orquestrador como o Kubernetes deve ser capaz de verificar a integridade de um nó de processamento antes de implantar contêineres nele.

Para fornecer certificação remota, os fornecedores de nuvem podem usar as tecnologias CIT, que adicionam uma etapa de verificação adicional sempre que um nó de processamento em nuvem é atribuído ao ambiente do contêiner. O Intel CIT, por exemplo, trabalha lado a lado com o Intel TXT para ajudar a garantir que o nó ainda esteja livre de violação e confiável antes de ser aceito em um cluster de contêiner. O Intel CIT também oferece uma extensão que facilita a habilitação de políticas de segurança para as equipes de DevOps, sem exigir que o desenvolvedor de aplicativos lide com as políticas.

Dica importante

Estender o limite de confiança no nível do nó requer uma solução de criptografia comprovada.

Máxima segurança na separação de recursos

O orquestrador do Kubernetes também ajuda a proteger um cluster, permitindo a separação de recursos gerenciados pelo provedor de serviços de elementos privados na conta de uma organização (Figura 2):

- O nó mestre dedicado do Kubernetes e o registro de imagem privada com acesso controlado a imagens podem ser executados na rede gerenciada.
- Os nós de trabalho do Kubernetes, com pods de carga de trabalho em contêiner, podem ser implantados na conta de infraestrutura da organização em redes dedicadas controladas pela organização, não pelo provedor.

Essa abordagem dá às equipes de DevOps um alto nível de controle e fornece o isolamento que os CISOs desejam. A comunicação entre os nós mestre e de trabalho ocorreria por meio de uma conexão de rede criptografada, com o Kubernetes fornecendo a criptografia e as chaves. Um controlador de entrada geraria automaticamente certificados TLS para acessar os pods do Kubernetes. Usando os controles de acesso baseados em função do Kubernetes, organizações podem definir restrições refinadas sobre os recursos dentro de clusters.

Automação orientada por políticas

O Kubernetes permite que as equipes de DevOps dividam as funções do sistema em elementos atômicos muito pequenos, cada um dos quais pode ser vinculado à arquitetura de base confiável para ajudar a garantir que cada elemento permita acesso e comunicação de acordo com a política. À medida que as equipes constroem arquiteturas complexas de microserviços, a automação orientada por políticas pode controlar o acesso e o roteamento, facilitando a expansão e a escala de contratos para aplicativos individuais e os componentes deles.

Calico e Istio são dois componentes importantes do ecossistema do Kubernetes que ajudam na segurança de aplicativos e cargas de trabalho. O Calico simplifica o gerenciamento de endereços IP atribuídos às cargas de trabalho em um nó de processamento e programa listas de controle de acesso em cada nó de computação para impor políticas de segurança. Por meio de políticas definidas e aplicadas com rótulos, o Istio fornece controle de comunicação baseado em certificado entre microserviços dentro de um pod ou cluster do Kubernetes.

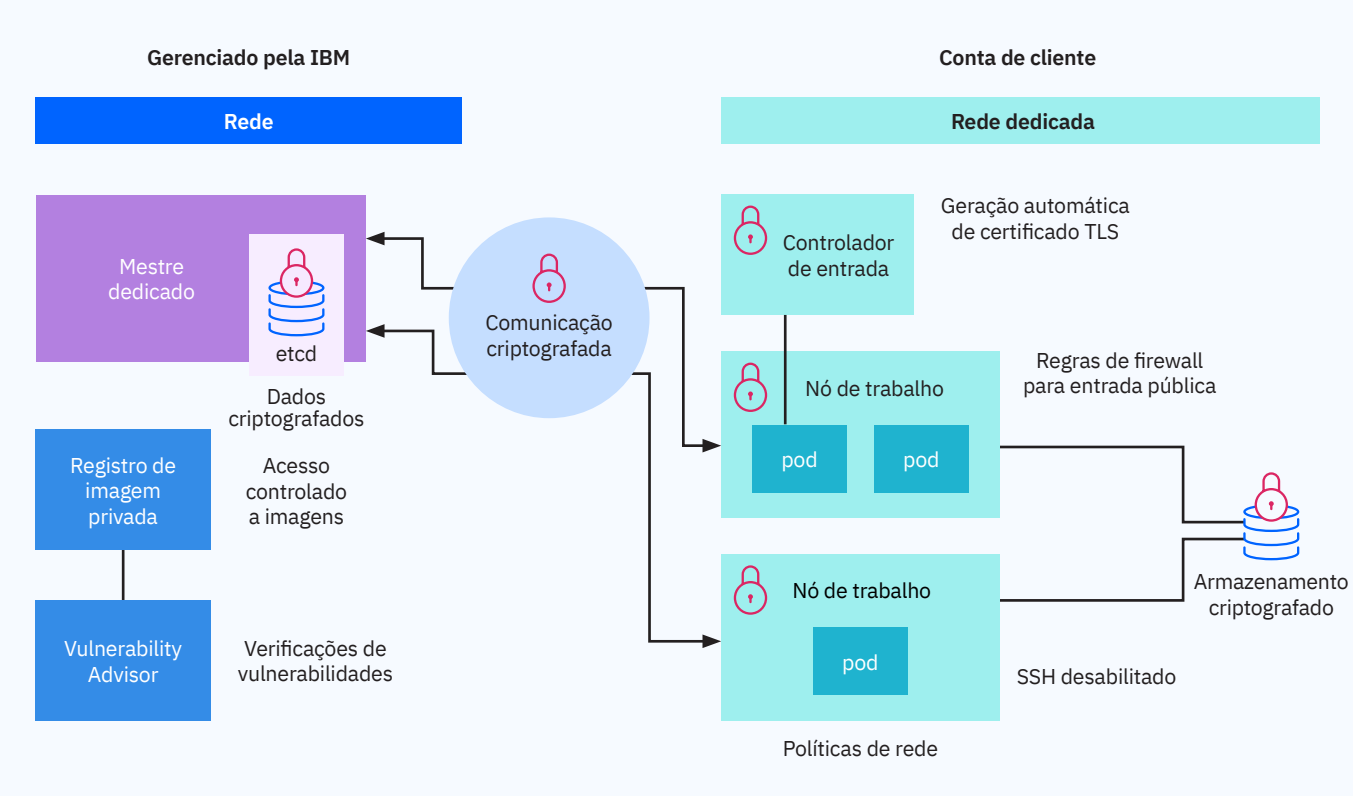


Figura 2. Separação de elementos de cluster gerenciados pelo provedor e gerenciados pelo cliente.

Ampliação os benefícios de uma cadeia de confiança

Uma cadeia de confiança totalmente implementada com certificação e criptografia remotas vinculadas a políticas de segurança permite esses recursos importantes para gerenciar contêineres, aplicativos e cargas de trabalho:

- **Transparência e escalabilidade:** com a automação possibilitada pela cadeia de confiança, as equipes de DevOps ficam livres para trabalhar com bastante rapidez. Elas só precisam gerenciar as políticas de segurança com as quais o sistema de contêineres confiáveis avalia as mensurações dele. Com a configuração apropriada em vigor, a orquestração dimensiona de forma mais ou menos automática os recursos de aplicativos com base no tráfego em tempo real.
- **Verificação da política de carga de trabalho geográfica:** a orquestração de contêineres inteligentes limita a movimentação para apenas locais aprovados.
- **Garantia de integridade do contêiner:** quando os contêineres são movidos, eles são verificados para garantir que não houve adulteração durante o processo. O contêiner movido é verificado para garantir que seja o mesmo criado originalmente.
- **Segurança para dados sensíveis:** contêineres criptografados só podem ser descriptografados em servidores aprovados em locais específicos.
- **Controles e relatórios de conformidade simplificados:** uma trilha de auditoria de metadados fornece visibilidade e evidência auditável de que cargas de trabalho críticas de contêineres são executadas em servidores confiáveis.

Dica importante

Enquanto sua equipe avalia as plataformas de nuvem, peça aos fornecedores para explicar como a confiança é estabelecida e mantida para o alcance da tecnologia que hospedará os aplicativos. Essa é a base da qual os negócios da sua organização dependem para envolver os clientes e proteger dados importantes.

Caso em questão: aliviando as preocupações com o GDPR

Suponha que você tenha clientes na Europa e esteja preocupado com possíveis grandes responsabilidades que virão quando o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia entrar em vigor. Como os requisitos de soberania e outras regulamentações significam que determinados tipos de dados não podem sair do país de origem, é necessário o seguinte:

- Garantia total de que, quando você quiser que a sua carga de trabalho esteja em um determinado lugar, ela não possa ir e não irá para outro lugar.
- Chaves de criptografia para sua carga de trabalho que são gerenciadas de forma que os dados não possam ser descriptografados em nenhum lugar, exceto onde você colocou sua carga de trabalho.

Depois de estabelecer uma cadeia de confiança baseada em hardware, é possível vincular todos os elementos essenciais para manter a integridade, gerenciar suas chaves e garantir a localidade das suas cargas de trabalho. E você pode viabilizar essa confiança por meio de políticas, dimensionando a segurança junto com as implantações de aplicativos.

Verificação de contêineres estáticos e ativos

Começar a usar contêineres do Docker é fácil: os desenvolvedores podem baixar qualquer imagem de contêiner disponível publicamente no Docker Hub, por exemplo, evitando ou reduzindo significativamente o tempo necessário para preparar partes de uma pilha de imagens. O problema não é saber ao certo o que está nessa imagem antes de implantá-la. Uma prática necessária, portanto, é verificar cada imagem antes de liberá-la no pipeline de DevOps. As plataformas de nuvem devem fornecer uma maneira eficiente de fazer isso.

O IBM® Cloud Container Service, por exemplo, oferece um sistema Vulnerability Advisor (VA) para verificar contêineres estáticos e ativos (Figura 3). O VA inspeciona todas as camadas de cada imagem no registro privado de um cliente na nuvem para ajudar a detectar vulnerabilidades ou malwares antes da implantação da imagem. No entanto, como a simples verificação de imagens do registro pode deixar passar problemas como a imagem estática e os contêineres implantados, o VA também verifica a existência de anomalias nos contêineres em execução. Além disso, ele fornece recomendações na forma de alertas em camadas.

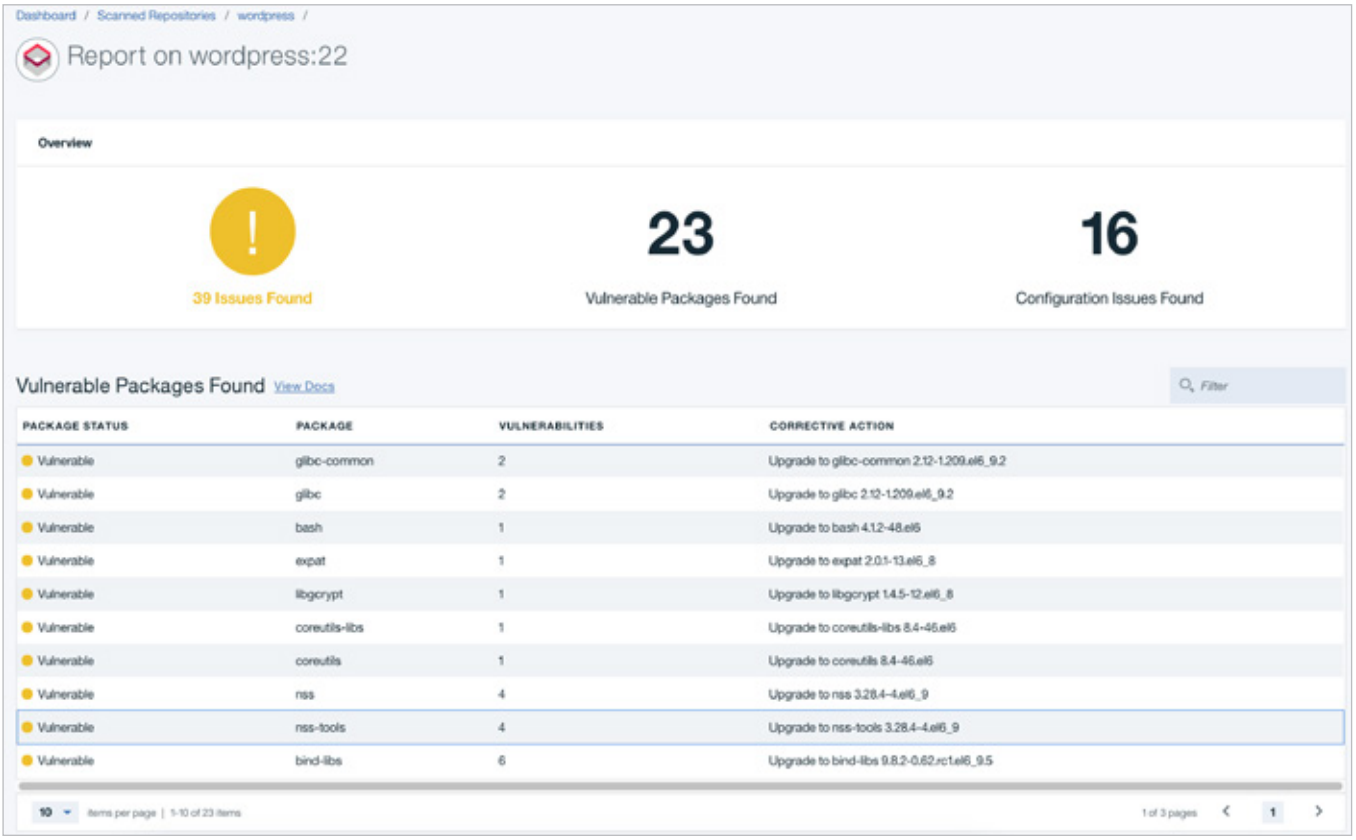


Figura 3. O VA se integra com o X-Force para avaliar vulnerabilidades com base no vetor de ataque, na complexidade e na disponibilidade de uma correção conhecida.

Tecnologias de isolamento de nuvens

Implicada por tecnologias baseadas em chip, a implementação de uma cadeia de confiança exige a capacidade de implantar em hosts dedicados que dão suporte ao acesso VPN. Todos os contêineres devem ser executados como processos independentes e isolados em um host de processamento e devem ter acesso restrito aos recursos dele.

Usando kernels de host de processamento otimizados, um provedor de nuvem deve ser capaz de limitar automaticamente o número total de threads e processos que são executados em um host de processamento. Essa otimização beneficia você garantindo que o host não seja sobrecarregado, o que pode afetar o desempenho do seu aplicativo.

Um provedor de serviços também deve monitorar continuamente os hosts de processamento para controlar e corrigir fork bombs e outros ataques DoS no nível do processo. Os controles de segurança que controlam o acesso a pastas, arquivos, domínios de rede e permissões para criar e alterar dados devem começar no nível do kernel do Linux.

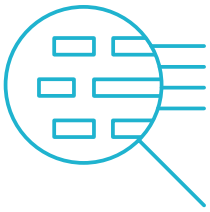
Visibilidade da segurança da nuvem

Os engenheiros de operações estão acostumados a analisar recursos locais e, com justificativa, esperar o mesmo insight nas cargas de trabalho em contêineres baseadas em nuvem. Para fornecer essa visibilidade, os fornecedores de nuvem devem registrar automaticamente todos os acessos de usuários e administrativos, seja pela organização ou pelo fornecedor. Um rastreador de atividade de nuvem integrado pode criar uma trilha de todo o acesso à plataforma e aos serviços, dando às organizações do cliente acesso a registros em logs relevantes.

Verifique se você tem a opção de integrar todos os registros em log e eventos no seu centro de operações de segurança (SOC) e no sistema de informações de segurança e gerenciamento de eventos (SIEM). Alguns provedores de serviços em nuvem oferecem serviços adicionais, como monitoramento de segurança com relatórios e gerenciamento de incidentes, análise em tempo real de alertas de segurança e uma visão integrada de implantações híbridas.

O IBM QRadar®, por exemplo, é uma solução SIEM abrangente que fornece um conjunto de recursos de inteligência de segurança que podem crescer com as necessidades de uma organização. Ele tem recursos de aprendizado de máquina que treinam os padrões de ameaças de uma maneira que cria um sistema imunológico de segurança inteligente.

Conheça o Vulnerability Advisor



Entre os recursos do IBM Vulnerability Advisor estão:

- **Configurações de violação de política:** com o VA, os administradores podem definir políticas de implementação de imagem com base em 3 tipos de situação de falha de imagem: pacotes instalados com vulnerabilidades conhecidas, logins remotos habilitados e logins remotos habilitados com alguns usuários que facilmente adivinharam senhas.
- **Práticas recomendadas:** o VA atualmente verifica 26 regras baseadas no ISO 27000. Entre as verificações estão configurações como idade mínima da senha, tamanho mínimo da senha e logins remotos habilitados.
- **Detecção de configuração incorreta de segurança:** o VA sinaliza cada problema de configuração incorreta, fornecendo uma descrição e recomendando um curso de ação para remediá-lo.
- **Integração com o IBM X-Force®:** o VA obtém informações de segurança de 5 fontes de terceiros e usa critérios como vetor de ataque, complexidade e disponibilidade de uma correção conhecida para avaliar cada vulnerabilidade. O sistema de classificação (crítico, alto, moderado ou baixo) ajuda os administradores a entender rapidamente a gravidade das vulnerabilidades e priorizar a correção.

Segurança de ponta a ponta a serviço das necessidades da empresa

A tecnologia de contêiner atende às equipes de desenvolvimento de aplicativos otimizando e aumentando a velocidade do trabalho colaborativo em ambientes de nuvem. Mas, para fornecer esses benefícios, uma plataforma de nuvem deve atender aos requisitos de segurança do CISO sem introduzir atrito excessivo. Portanto, para alcançar as metas da empresa, as equipes de DevOps precisam implementar as políticas de CISO por meio de segurança automatizada.

Uma cadeia de confiança enraizada no hardware é uma base eficaz para esse objetivo. Ela deve incluir tecnologias para garantir contêineres confiáveis e impor políticas de segurança que controlem a implantação de contêineres. A arquitetura da cadeia de confiança foi projetada para atender à necessidade urgente de segurança e inovação rápida:

- Os agentes de segurança podem formular políticas de segurança que são aplicadas automaticamente a todos os contêineres criados ou movidos.
- Cada etapa da sequência é automatizada, permitindo que as equipes de DevOps criem e implementem aplicativos rapidamente sem parar para adicionar componentes de segurança.

Essa arquitetura protege dados e aplicativos do nível do hardware até a camada de orquestração de contêineres das plataformas de nuvem, ajudando as organizações a cumprir regras de conformidade como o GDPR da União Europeia, o Programa Federal de Gerenciamento de Risco e Autorização dos EUA (FedRAMP) e a Lei de Portabilidade e Responsabilidade em Seguros de Saúde dos EUA (HIPAA). As organizações definem exatamente as políticas necessárias para o próprio setor e asseguram os elementos de garantia.

Visão da IBM

Inovar na cadeia de confiança é um foco importante para a IBM e os parceiros dela. A IBM e a Intel têm uma longa parceria dedicada ao desenvolvimento de soluções de segurança de cadeia de confiança, e agora estão aplicando seus conhecimentos em ofertas baseadas em contêineres. Os objetivos: Ajudar as organizações a implantar contêineres de maneira segura, porém ágil, que permita a flexibilidade de desenvolvimento e arquiteturas de microserviços de ponta que os inovadores de hoje exigem e merecem.

O IBM Cloud capacita as equipes com ferramentas de software livre prontamente disponíveis para automatizar a implantação e o gerenciamento. E se os clientes quiserem implantar cargas de trabalho em diversas nuvens, a plataforma de nuvem deverá permitir que eles usem as mesmas ferramentas de maneira consistente em todo o ambiente de diversas nuvens. O futuro da segurança de contêineres é aberto, ágil, automatizado sempre que possível, e é forte e inteligentemente defensivo.

O futuro da segurança de contêineres é aberto, ágil, automatizado sempre que possível, e é forte e inteligentemente defensivo.

Para mais informações

Para saber mais sobre como criar uma cadeia de confiança para a segurança do contêiner, acesse **ibm.com**/cloud/container-service

Está interessado em segurança e DevOps? Participe do nosso canal Slack e compare notas com os desenvolvedores na equipe do produto IBM Cloud Container Service.

Fique conectado

IBM Cloud Container Service
Blog do IBM Cloud

Siga-nos

@IBMcloud
Facebook

Conecte-se conosco

LinkedIn
YouTube

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

Produzido nos Estados Unidos da América, fevereiro de 2018