Como compartilhar a carga de trabalho de segurança

Como operacionalizar e simplificar para equipes de segurança e administradores de TI

vmware®

Sumário

Introdução

As equipes de segurança precisam das operações de TI para proteger as cargas de trabalho

Tanto os administradores de TI quanto as equipes de segurança cumprem seus papéis para manter a segurança dos sistemas, mas o fazem em um isolamento relativo entre si. No entanto, a transição dos aplicativos e das cargas de trabalho para os ambientes de nuvem está forçando uma mudança no modo como essas funções são executadas.

As equipes de segurança em uma organização costumam ser compostas por grupos de política e auditoria, além de equipes de procura de ameaças e equipes de resposta a incidentes. O ônus diário de segurança e conformidade recai sobre os recursos e as equipes de operação de TI que não são necessariamente voltadas para segurança. Na verdade, de acordo com um relatório da Forrester Consulting Spotlight, apenas 33% das organizações já unificaram as equipes de TI e segurança, e 47% acreditam que essa unificação será o padrão nos próximos três a cinco anos.[1] Este é o melhor momento para adotar uma nova abordagem que facilita a coesão entre essas duas equipes.

Este white paper abrange as principais estruturas que permitem às equipes de TI e segurança reduzir proativamente a superfície de ataque e fortalecer os recursos. Quando adotadas, essas estruturas eliminam as brechas entre as equipes, simplificam operações e compartilham a carga de trabalho de segurança.

ESTRUTURA PRINCIPAL	DESCRIÇÃO
Minimize as despesas indiretas de agentes	Eliminar a necessidade de instalar agentes em cargas de trabalho reduz a proliferação de agentes de segurança, as instalações e reinicializações e as despesas indiretas operacionais. Isso simplifica o fornecimento de segurança como serviço para a TI.
Compartilhe a visão sobre as vulnerabilidades	Uma visão unificada dos dados de segurança garante compreensão e comunicação claras sobre as vulnerabilidades detectadas.
Automatize a priorização de riscos	Ambas as equipes precisam definir seu foco, não só para minimizar o excesso de alertas e a sobrecarga dos recursos, mas também para otimizar as defesas. É imprescindível ter um sistema centrado no contexto, capaz de priorizar vulnerabilidades automaticamente e sem parcialidade.
Otimize os processos de carga de trabalho	Com a visibilidade compartilhada e a priorização de riscos, as equipes de TI e segurança desfrutam de uma experiência sem atrito por meio de automação e operacionalização consistentes da segurança, como parte da higiene da TI.

TABELA 1: Quatro estruturas principais para reduzir a superfície de ataque e fortalecer os recursos.

1. Realizado pela Forrester Consulting, solicitado pela VMware. "Security As A Team Sport: A Spotlight On The Growing Role Of IT In Security Tasks." Maio de 2020.

O desafio

Cargas de trabalho causam desentendimentos sobre a vulnerabilidade

As cargas de trabalho estão se tornando cada vez mais distribuídas, à medida que os nossos ambientes se tornam mais amplos e complexos. A maioria dos aplicativos com base em nuvem são essenciais aos negócios, mas vulneráveis a comprometimentos quando há problemas na carga de trabalho (app, dados ou sistema operacional). Obviamente, desligar o servidor da empresa durante um incidente não é a solução. As operações de TI e segurança são secundárias em relação à produtividade da empresa. Isso significa que proteger e monitorar cada parte da carga de trabalho é parte adicional (e essencial) da segurança dos seus negócios.

Quem é responsável por proteger cargas de trabalho?
Quando as cargas de trabalho se encontravam em servidores de rack estático em data centers locais, era fácil atribuir a responsabilidade de protegê-las. Hoje em dia, cargas de trabalho podem existir em servidores físicos, em servidores virtuais, na nuvem pública ou até mesmo sem servidor. Além disso, as cargas de trabalho podem coexistir em todos esses ambientes, o que dificulta o monitoramento e o gerenciamento delas. A segurança, os administradores de TI, os administradores da nuvem, os administradores do VMware vCenter®, os engenheiros de confiabilidade do site (SREs, pela sigla em inglês), os DevOps e os desenvolvedores exercem um papel no ciclo de vida da carga de trabalho. Por vezes, eles podem repercutir nas cargas de trabalho de forma a alcançar objetivos em comum, mas esses objetivos também podem ter efeitos contrários.

Os administradores de TI são capazes de proteger as cargas de trabalho com eficiência. No entanto, eles não são capazes de identificar a maioria das vulnerabilidades da carga de trabalho e certamente não têm o contexto para priorizar o impacto. E, como os administradores de TI não costumam ter controle sobre o ambiente da nuvem, as funções e responsabilidades se tornam incompreensíveis. As equipes de segurança podem ter algumas das informações necessárias para identificar vulnerabilidades, mas talvez não tenham o contexto ou a priorização clara dos riscos para gerenciar as correções de forma efetiva.

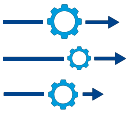
Em outras palavras, a segurança da carga de trabalho pode não estar sendo devidamente gerenciada por todos.

É possível dividir essa responsabilidade?
Como consequência, tanto as equipes de segurança quanto os administradores de TI precisam atuar na segurança das cargas de trabalho. Para evitar a troca de acusações, no entanto, essas equipes precisam estar unificadas com os processos, as informações e as ferramentas específicas para cargas de trabalho.

Com uma metodologia e um entendimento compartilhado para automatizar a descoberta e a priorização de correções de vulnerabilidade, torna-se muito mais fácil para os administradores de TI compartilhar a responsabilidade de fortalecer e reduzir as superfícies de ataque. Na verdade, a segurança da carga de trabalho pode ser operacionalizada para eliminar a tensão e a troca de acusações entre essas duas equipes essenciais. São necessárias apenas quatro etapas para tornar isso uma realidade.

DADOS ESSENCIAIS PARA COMPARTILHAR ENTRE EQUIPES DE SEGURANÇA E ADMINISTRADORES DE TI

- Indicadores de comprometimento (IOCs)
- Táticas, técnicas e procedimentos (TTPs)
- Visibilidade dos ataques bloqueados e detectados
- Eventos comuns que ocorrem no sistema
- Avaliação de mais de dois mil estados de configuração de carga de trabalho
- Inventário de cargas de trabalho e seu estado de proteção
- Contexto de vulnerabilidades sem varredura com pontuações de risco e links para o Banco de dados nacional de vulnerabilidades
- Rastreamento e tendências cronológicas de higiene de TI



Quatro etapas para operacionalizar e simplificar a segurança das cargas de trabalho

Etapa 1: Minimize as despesas indiretas de agentes

A proliferação de agentes de segurança agregados causa muitos problemas para administradores de TI e equipes de segurança. Os desafios mais comuns são:

- Diferentes fontes de informação de segurança que levam à comunicação insatisfatória
- Carga de manutenção e chance de erros maiores
- Mais custos de armazenamento para dados coletados

Para eliminar esses problemas, consolide a TI e as pilhas de segurança ao substituir várias soluções pontuais por uma abordagem de segurança integral, capaz de coletar dados entre ambientes de nuvem e locais.

Escolha um agente integrado

A solução ideal é utilizar um único agente na camada de virtualização integrada à sua infraestrutura existente. Isso permite registrar os eventos necessários para visibilidade total em todos os ambientes. Um único agente proporciona monitoramento de segurança com uma área de cobertura a mais próxima possível de zero.

Grandes benefícios de um único agente

Consolidar soluções de segurança em um único agente (uma fonte de dados única e abrangente) traz grandes benefícios para melhorar a segurança das cargas de trabalho:

- Facilita o gerenciamento de agentes de operacionalização para a TI
- Permite o compartilhamento de dados e a integração de fluxos de trabalhos entre equipes
- Fornece informações voltadas para o contexto, tornando as saídas mais acionáveis
- Remove verificações de vulnerabilidades periódicas, o que melhora o desempenho e acelera o tempo de resposta para ataques
- Reduz os custos de armazenamento e o trabalho de manutenção

Etapa 2: Compartilhe a visão sobre as vulnerabilidades

O grupo responsável pela aplicação de patches é raramente o mesmo grupo responsável pelo impacto das vulnerabilidades. Os dados tradicionais de verificação se tornam dessincronizados rapidamente, e os sistemas de emissão de tíquetes são lentos. Isso resulta em diferentes interpretações das correções necessárias.

Os administradores de TI e a equipe de segurança usam fontes de dados diferentes, mas devem contribuir com processos de segurança mais abrangentes. Isso leva a expectativas incompatíveis e resultados de higiene insatisfatórios.

Uma visão unificada de dados de segurança garante comunicação e entendimento claros das vulnerabilidades detectadas e o nível de risco associado.

Uma visão unificada reduz fiscos de forma efetiva

A consolidação para um único agente na Etapa 1 produz dados de segurança que podem ser facilmente compartilhados entre administradores de TI e equipes de segurança. Teoricamente, essas informações devem ser apresentadas nas ferramentas que essas equipes usam diariamente, tais como ferramentas de virtualização (por exemplo, VMware vSphere® e vCenter).

Ter os mesmos dados e saídas de avaliação entre equipes melhora a comunicação e colaboração. O mais importante é ter dados de vulnerabilidade atuais e sempre disponíveis, em vez de uma verificação em ponto no tempo. Isso garantirá que as equipes estejam sempre em sincronia. Um inventário compartilhado de vulnerabilidades de cargas de trabalho priorizadas por risco garantirá que os recursos sejam direcionados para solucionar os problemas mais críticos.

Etapa 3: Automatize a priorização de riscos

Utilizar um agente único e ter visibilidade compartilhada dos dados de segurança são ótimas etapas para gerenciar a segurança das cargas de trabalho. No entanto, somente o acesso a vulnerabilidades conhecidas não significa que há uma noção compartilhada de onde centrar os recursos.

A próxima etapa lógica é padronizar a avaliação de riscos. Considere uma solução de segurança que lida automaticamente com a avaliação e a priorização de riscos.

Dados com prioridade de riscos nas ferramentas atuais para resultados acionáveis
Uma avaliação de riscos baseada unicamente no sistema comum de pontuação de vulnerabilidades não é o suficiente. Os dados contextuais selecionados de conjuntos de dados de ameaças personalizados (incluindo feeds de exploração e inteligência de detecção de ameaças e mais de 7 bilhões de vulnerabilidades gerenciadas) permitirá que as organizações apliquem o modelo preditivo para prever novas vulnerabilidades e priorizar atividades de correção com base no nível de gravidade.

Teoricamente, os administradores de TI devem ter uma visão da maioria das explorações e vulnerabilidades de alto risco em seu console do vCenter. Dessa forma, o fortalecimento de cargas de trabalho é facilmente incorporado às atividades diárias de higiene.

Além disso, os administradores de TI precisam de informações de auditoria sobre o estado atual do sistema para que possam colaborar com as equipes de segurança na correção de ameaças. Ter uma visão compartilhada dessas informações permitirá que essas equipes trabalhem em conjunto para aplicar patches por prioridade ou tomar outras medidas, como desativar sistemas vulneráveis.

Uma visão compartilhada das ameaças e vulnerabilidades atuais com riscos associados garante mais clareza na priorização e no foco das tarefas, o que leva a mais rapidez na resolução de ameaças existentes e melhor proteção contra eventuais ataques.

Etapa 4: Otimize os processos de carga de trabalho

Tradicionalmente, as verificações de vulnerabilidade são atividades mensais ou trimestrais. No entanto, esses exercícios pontuais não são o suficiente. Com a expansão contínua das cargas de trabalho em ambientes multi-cloud, essas verificações não fornecem informações tão abrangentes ou pontuais, pois precisam mitigar os riscos de segurança críticos.

Com a visibilidade compartilhada e a priorização de riscos, a próxima etapa para as equipes de TI e segurança é integrar a segurança da carga de trabalho à higiene da TI.

Operacionalização de segurança da carga de trabalho
A operacionalização de segurança da carga de trabalho exige que os administradores de TI reduzam continuamente as superfícies de ataque, como parte das práticas de higiene padrão da TI. Os administradores de TI precisam acessar avaliações de milhares de estados de configuração em suas cargas de trabalho, bem como as informações e orientações para corrigir as vulnerabilidades descobertas.

O gerenciamento de TI deve ter acesso a uma visão compartilhada das tendências cronológicas de higiene da TI. Isso incentivará discussões da equipe sobre o gerenciamento de vulnerabilidades e desempenho das medidas. Os gerentes de TI devem usar essas informações para garantir que as prioridades sejam seguidas e os recursos sejam alocados adequadamente para fortalecer as cargas de trabalho de forma contínua.

O que vem em seguida?

O alinhamento da TI com a segurança das cargas de trabalho reduz ataques

As equipes de segurança e os administradores de TI podem trabalhar em conjunto para melhorar a segurança das cargas de trabalho. E, com as funções de segurança adequadas, essa colaboração pode ser tranquila e facilmente operacionalizada no dia a dia. Para aproveitar essa oportunidade, as equipes devem:

- Usar uma solução integrada com um único agente
- Ter uma visão unificada dos dados de segurança integrados em suas ferramentas de trabalho atuais
- Ter o contexto necessário e o monitoramento contínuo para vulnerabilidades com priorização de riscos automatizada
- Ter o suporte da liderança, a fim de garantir a operacionalização do fortalecimento das cargas de trabalho

Três fatores para melhorar a segurança das cargas de trabalho

1. Reúna os responsáveis das áreas de segurança e TI para discutir um possível trabalho em conjunto a fim de reduzir ataques.
2. Identifique as lacunas atuais na visibilidade e coleta de dados para melhor priorizar as vulnerabilidades e fortalecer as cargas de trabalho.
3. Analise soluções que ofereçam o contexto e a visibilidade compartilhada necessários para que os administradores de TI e as equipes de segurança sejam bem-sucedidos.

Tratar da segurança de cargas de trabalho gera grandes dividendos

- Abrangência e visibilidade em todas as cargas de trabalho
- Simplificação da pilha de segurança de TI
- Capacidade para reagir mais rapidamente a problemas com detecção antecipada
- Recursos mais fortalecidos
- Melhor prevenção contra malwares, bem como softwares e processos indesejados
- Eliminação completa de não malwares
- Ativação da segurança para o futuro: ambientes e cargas de trabalho modernas

Saiba mais

Leia este datasheet e sabia como o VMware Carbon Black Cloud™ fortalece a TI e a segurança para melhorar as cargas de trabalho em conjunto.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel.: +1-877-486-9273 Fax: +1-650-427-5001 www.vmware.com
Rua Surubim, 504 4º andar CEP 04571-050 Cidade Monções – São Paulo – SP Tel.: (11) 5509-7200 www.vmware.com/br

Item nº: 764618aq-wp-shrng-wkld-sec-a4_BR_BR 3/21