WHITE PAPER: ABRIL 2021

Proteção de cargas de trabalho na nuvem

Como proteger cargas de trabalho em nuvens híbridas

vmware®

Sumário

Resumo executivo

A nuvem híbrida é o ponto central da transformação digital. Atualmente, mais de 90% das empresas relatam usar uma estratégia multi-cloud, na qual a maior parte delas combina o uso de nuvens públicas e privadas.[1] A boa notícia é que essa abordagem oferece a flexibilidade e o dimensionamento necessários para dar suporte à rápida inovação. A desvantagem é que ela costuma trazer mais complexidade e risco, o que torna a segurança um componente essencial em nuvens privadas e públicas.

À medida que as equipes corporativas implantam e gerenciam cargas de trabalho essenciais em ambientes multi-cloud, a visibilidade da postura de segurança de cargas de trabalho e o controle da superfície de ataque são essenciais para proteger os dados e manter as operações.

Muitas equipes distintas na empresa, incluindo as de operações de TI e SecOps, são as principais partes interessadas no desempenho, na disponibilidade e na segurança das cargas de trabalho na nuvem. Manter os membros da equipe alinhados em vez de fragmentados também é fundamental para o sucesso.

Este white paper aborda os principais desafios que as equipes corporativas têm encontrado na proteção de cargas de trabalho na nuvem e como superá-los usando a abordagem de segurança intrínseca da VMware, que conta com o VMware Carbon Black Cloud™, o VMware vSphere® e o VMware NSX®. Este documento também inclui uma discussão sobre como a nuvem obriga a refletir sobre o risco, de forma a reunir as partes interessadas das várias equipes em vez de mantê-las separadas na divisão digital. Além disso, fornece uma lista de verificação para avaliar a plataforma de proteção de cargas de trabalho na nuvem para ajudar as organizações a examinar requisitos importantes ao considerar as soluções.

Desafios de segurança com nuvens privadas, públicas e híbridas

A implantação e o gerenciamento de cargas de trabalho e apps em nuvens privadas, públicas e híbridas é uma tarefa conjunta. O que antes considerávamos a TI tradicional foi substituído por um esforço coletivo. As equipes de operações de TI, DevOps e SecOps agora se reúnem para fornecer e proteger apps e serviços na nuvem.

1. Flexera. “Flexera 2020 State of the Cloud Report”, abril de 2020.

Conforme mostrado na Tabela 1, não desenvolver uma coordenação entre as equipes para os aspectos únicos das cargas de trabalho na nuvem pode levar ao aumento dos riscos.

	OPERAÇÕES DE NUVEM HÍBRIDA	DESAFIOS DE SEGURANÇA	OPERAÇÕES DE TI TRADICIONAIS	LACUNAS NA SEGURANÇA DE TI TRADICIONAL
Arquitetura de design	Serviços interconectados	• Nenhuma visibilidade de como as cargas de trabalho se comunicam e se conectam • Redes planas não segmentadas aumentam o risco	Monolítica e isolada	• O antivírus tradicional não foi criado para um contexto de carga de trabalho na nuvem • O monitoramento centrado no data center não tem uma noção básica de qual é o comportamento normal da rede
Modelo operacional	Propriedade e gerenciamento distribuídos	• As operações de TI são responsáveis pela postura, pelo gerenciamento e pela disponibilidade das cargas de trabalho, mas não conseguem identificar vulnerabilidades nelas • A tecnologia e os silos de processos contribuem para configurações inadequadas ou inseguras, além de outros erros humanos	Centralizado	• A adição de produtos de segurança pontuais exige a instalação de agentes adicionais, o que reduz o desempenho do sistema e dificulta as operações • A falta de visibilidade unificada das cargas de trabalho e entre cargas de trabalho e as nuvens complica a coordenação entre equipes
Dimensionamento	Altamente dinâmico e automático	• A falta de controle de alterações resulta em configurações inadequadas, como armazenamento de dados inseguro, permissões excessivas, definição predeterminada de credenciais e configuração e desabilitação de controles de segurança • A incapacidade de padronizar políticas de segurança de carga de trabalho em nuvens privadas e públicas aumenta o risco	Manual e estático	• A verificação tradicional não foi projetada para detectar configurações inadequadas comuns da nuvem (a principal causa das violações de dados com base em nuvem)[2] • A implantação de soluções pontuais de segurança para cada ambiente de nuvem distinto complica o gerenciamento da governança e da política em escala

TABELA 1: Os desafios de segurança com cargas de trabalho de nuvem híbrida se originam do não reconhecimento das principais diferenças entre a computação em nuvem e a TI tradicional.

2. Cloud Security Alliance "Top Threats to Cloud Computing: Egregious Eleven Deep Dive." Setembro de 2020.

As equipes de operações de TI, DevOps e SecOps, todas compartilham a responsabilidade de manter a segurança e a disponibilidade das cargas de trabalho essenciais na nuvem.

Três etapas para redefinir o risco

A melhor maneira de aproveitar ao máximo a transformação digital é aceitar o quanto ela representa uma mudança de paradigma. Os modelos de gerenciamento de risco antigos não se aplicam mais quando a mudança é uma constante e há muitas pessoas envolvidas.

Ao proteger cargas de trabalho na nuvem, as equipes corporativas precisam:

1. Aumentar a visibilidade – identificar riscos desconhecidos ou não detectados em cargas de trabalho
2. Agilizar a recuperação – acelerar a recuperação do risco desenvolvendo resiliência nas cargas de trabalho na nuvem
3. Simplificar a segurança – unificar a redução dos riscos em cargas de trabalho, endpoints e contêineres

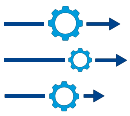
Etapa 1: Aumentar a visibilidade – identificar riscos desconhecidos ou não detectados em cargas de trabalho

- **Por que isso é um desafio?** Você não pode gerenciar riscos que desconhece. Infelizmente, a maioria dos administradores de máquina virtual (VM, pela sigla em inglês) não tem visibilidade de como os apps e as cargas de trabalho em execução são potencialmente vulneráveis a ataques. Embora um invasor só precise identificar e aproveitar-se de uma única vulnerabilidade para obter acesso não autorizado, os responsáveis pela proteção precisam conhecer todas as formas pelas quais ela pode ser explorada para que possam fechar essas lacunas. Além disso, depois que as vulnerabilidades são identificadas, obter o consenso entre as equipes de operações de TI e SecOps sobre quais vulnerabilidades têm prioridade maior para correção, por que e quando, nem sempre é uma tarefa simples.
- **Exemplo**: José é engenheiro de confiabilidade de site (SRE, pela sigla em inglês) de uma grande empresa do setor de assistência médica. Ele é responsável pelo gerenciamento da infraestrutura em nuvem privada, que inclui servidores, cargas de trabalho e apps que processam dados sigilosos de assistência médica. José sabe que precisa identificar e mitigar qualquer vulnerabilidade que possa afetar a conformidade ou expor os dados dos pacientes. Apesar disso, o desempenho, a disponibilidade e o tempo de atividade são as principais prioridades de José e dos outros SREs em sua equipe. Afinal, o cuidado dos pacientes é essencial.

  Atualmente, José espera que Sara, uma analista de segurança, informe quando uma verificação agendada detectar uma vulnerabilidade de alta gravidade que exija mitigação. Muitas vezes, eles discordam sobre o melhor procedimento, porque cada um utiliza um conjunto de ferramentas diferente. Sem um sistema comum de registro, chegar ao consenso sobre esses problemas críticos continua sendo uma tarefa difícil. Quais vulnerabilidades têm a maior prioridade? Esses controles de compensação são suficientes? Qual é o alvo dos invasores e como estão agindo? E assim sucessivamente.
- **O que é necessário: Detecção de risco em todo o domínio**: Detecte todos os riscos da carga de trabalho na nuvem, de todos os ângulos e vetores de ataque, e use um sistema comum de registro para gerenciá-los. Se não for possível implementar um patch em virtude do risco de tempo de inatividade, obtenha consenso sobre um controle compensatório ou configure uma lista de espera para detectar quando a vulnerabilidade será enfrentada.

Etapa 2: Agilizar a recuperação – acelerar a recuperação do risco desenvolvendo resiliência nas cargas de trabalho na nuvem

- **Por que isso é um desafio**: Para a maioria das empresas, as violações de dados se tornaram não uma questão de "se", mas de "quando". Durante uma violação, conhecer o alcance ou o raio de explosão da exposição é essencial para evitar ataques similares no futuro. Além disso, essas informações são fundamentais para uma recuperação rápida e completa. O desafio é uma questão de prioridades que competem entre si. A prioridade das equipes de DevOps e operações de TI é restaurar os serviços o mais rápido possível, mesmo que isso signifique destruir evidências forenses e elementos que a equipe de SecOps precisa para identificar e averiguar a origem e o escopo completo do ataque.
- **Exemplo**: A recuperação de um ataque de ransomware em seu ambiente de nuvem pode ser dispendiosa, complicada e trabalhosa. Esses surtos podem migrar de cargas de trabalho para os servidores que as hospedam e os endpoints usados por funcionários para acessar as cargas de trabalho. O objetivo é reduzir a superfície de ataque do ransomware ao desativar os estágios iniciais do ataque (execução de código na própria carga de trabalho) antes que o conjunto de ferramentas seja totalmente implantado, ou que as conexões de comando e controle (C2) sejam configuradas para extrair ou criptografar os dados para o ataque.



- **O que é necessário: Resiliência ao risco**: Recuperar os serviços com rapidez, após uma violação ou ataque de malware, e manter os dados necessários para realizar investigações forenses é possível na nuvem, desde que você tenha a plataforma de segurança de carga de trabalho adequada. Na verdade, eliminar essa divisão é um aspecto fundamental da construção da resiliência a riscos em suas cargas de trabalho na nuvem. O gerenciamento da segurança de carga de trabalho e endpoint na mesma plataforma permite que as equipes identifiquem os riscos nesses pontos de controle e busquem uma estratégia de recuperação mais resiliente.

Etapa 3: Simplificar a segurança – unificar a redução dos riscos em cargas de trabalho, endpoints e contêineres

- **Por que isso é um desafio:** O gerenciamento do risco em cargas de trabalho na nuvem que usam soluções pontuais tradicionais leva a processos de fluxo de informações que adicionam despesas indiretas operacionais e riscos compostos. O uso de diferentes ferramentas de segurança baseadas no provedor de nuvem pública, sistema operacional host ou tipo de nuvem (privada versus pública) deixa fora do alcance, em termos práticos, uma estratégia consistente de redução de riscos. Afinal, quando não há uma fonte única de informações confiáveis sobre segurança, as equipes não conseguem chegar a um acordo sobre como impedir surtos de malware, localizar e corrigir configurações inadequadas ou conter ameaças ágeis.
- **Exemplo:** Para otimizar a resiliência operacional, algumas equipes de operações de TI escolhem usar vários provedores de nuvem ou combinar seu uso da infraestrutura de nuvem privada e pública. Sem uma política de segurança verdadeiramente independente capaz de transcender esses ambientes, as equipes ficam com um conjunto fragmentado de controles ou presas a um único provedor de serviços de nuvem ou arquitetura de nuvem (privada ou pública).
- **O que é necessário: Segurança unificada:** O objetivo é implantar a segurança unificada projetada para nuvem e aplicada uniformemente, independentemente de onde a carga de trabalho esteja localizada (nuvem pública versus privada). O uso de um único gerenciamento de ciclo de vida entre nuvens, cargas de trabalho e contêineres permite uma política de segurança e estratégia de redução de risco consistentes e amplas. Por exemplo, o uso de uma plataforma única para gerenciamento de vulnerabilidade, auditoria e correção, e Endpoint Detection and Response (EDR) simplifica a segurança da carga de trabalho e possibilita a colaboração entre equipes de operações de TI, SecOps e DevOps.

Segurança intrínseca para cargas de trabalho na nuvem

Conforme mostrado neste documento, o uso de tecnologias distintas para gerenciar cargas de trabalho na nuvem complica o risco e simplesmente não é dimensionável. Ao mesmo tempo, é essencial capacitar todas as equipes, desde a equipe de operações de TI até DevOps e SecOps, para que usem seu console escolhido. Isso não significa que a migração para a nuvem exige a adoção de um processo inteiramente novo, nova UI ou um console de gerenciamento. Afinal, essas equipes já têm muitas responsabilidades.

Com a abordagem de segurança intrínseca da VMware, o monitoramento profundo e a análise comportamental são implementados em cada ponto de controle (nuvem, carga de trabalho, endpoint, rede e identidade) e, em seguida, unificados para obter a conscientização do contexto completo. Como uma câmera de vídeo que registra cada movimento em todos os pontos de controle, a segurança intrínseca possibilita a conscientização detalhada do contexto. Como não há necessidade de formar a telemetria a partir de pontos de controle distintos, as equipes podem rastrear ameaças com rapidez, desde o ponto de entrada e a cada etapa.

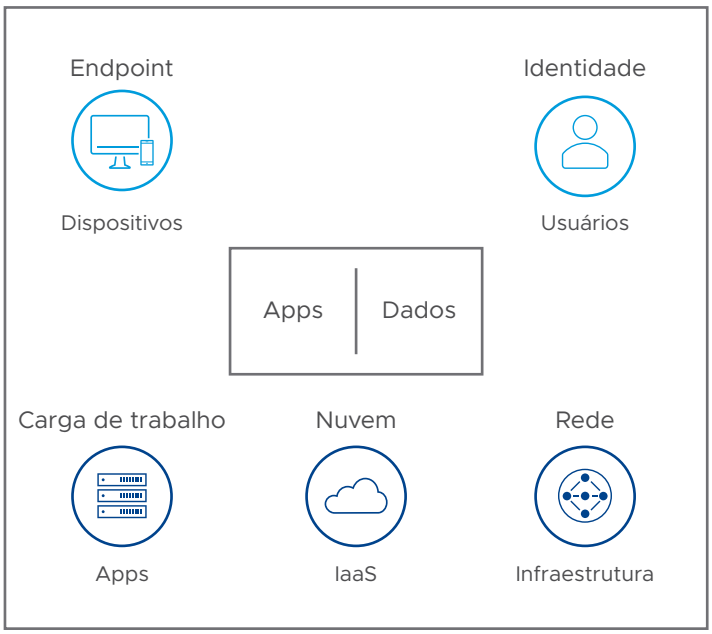


FIGURA 1: Os cinco pontos de controle da segurança intrínseca.

Proteção dimensionável de cargas de trabalho na nuvem

O VMware Carbon Black Cloud oferece toda a funcionalidade da proteção dimensionável de cargas de trabalho na nuvem e se integra nativamente ao vSphere e ao NSX. Graças a essa forte integração, os administradores do vSphere e do NSX podem acessar todos os dados relevantes sobre ameaças de seus respectivos domínios e no mesmo console otimizado para suas próprias funções.

Além de oferecer conscientização contextual completa na nuvem e entre nuvens, cargas de trabalho, endpoints, redes e identidades, o VMware Carbon Black Cloud disponibiliza o sistema comum de registro para equipes de operações de TI, DevOps e SecOps para evitar, detectar e corrigir ameaças que afetam suas cargas de trabalho e apps essenciais.

Os componentes básicos da segurança intrínseca são:

- VMware Carbon Black Cloud
- VMware vSphere
- VMware NSX

VMware Carbon Black Cloud

O VMware Carbon Black Cloud é uma plataforma de proteção de cargas de trabalho nativa da nuvem que combina o fortalecimento inteligente do sistema e a prevenção comportamental necessários para combater novas ameaças, usando gerenciamento de ciclo de vida único e um console intuitivo.

VMware vSphere

O vSphere é a plataforma de virtualização da camada de processamento e foi rearquitetado com *Kubernetes* nativo para permitir que os clientes modernizem as cargas de trabalho que estão em execução no vSphere.

VMware NSX Advanced Threat Prevention™

Com tecnologia de aprendizado de máquina, o VMware NSX Service-defined Firewall™ oferece análise do tráfego de rede, detecção e prevenção de intrusões e análise avançada de malwares com funções abrangentes de detecção e resposta de rede.

Proteção de cargas de trabalho na nuvem da VMware: como funciona

A abordagem de segurança intrínseca da VMware permite que as empresas protejam as cargas de trabalho na nuvem utilizando a infraestrutura existente para identificar riscos, evitar explorações e exposições de forma proativa e detectar e responder a novas ameaças.

O processo em três etapas funciona da seguinte maneira, com o suporte de controles essenciais de segurança.

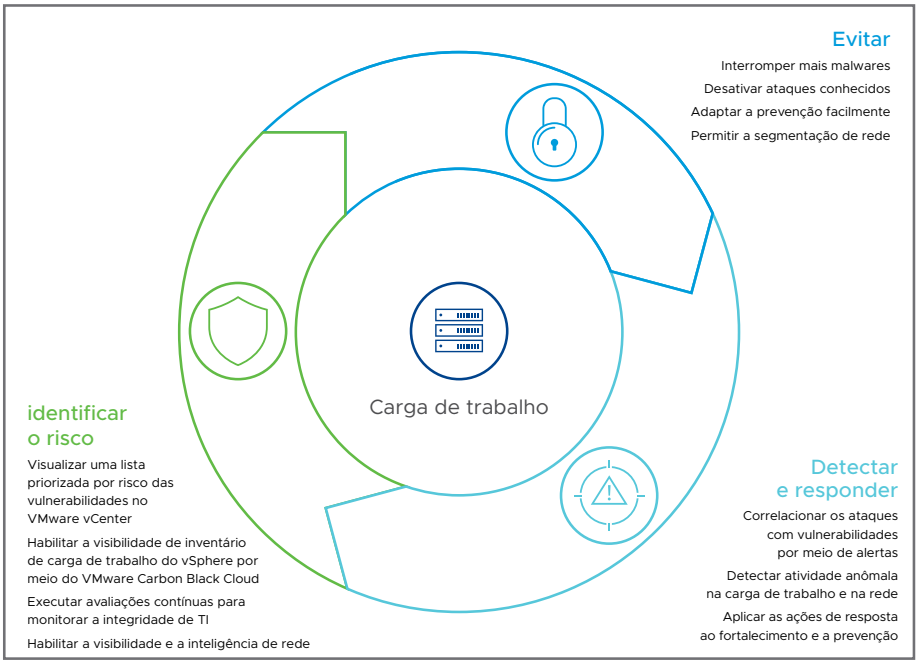


FIGURA 2: A segurança intrínseca para cargas de trabalho na nuvem oferece proteção abrangente para cargas de trabalho do vSphere.

Etapa 1: Identifique o risco

- **Verificação de integridade do estado inicial:** O VMware Carbon Black Cloud conduz uma verificação de integridade do estado inicial para ratificar que o sistema em que você está instalando a carga de trabalho está limpo e em conformidade e é apropriado para o tipo de carga de trabalho. Ele também vai coletar e analisar os níveis de patch do sistema operacional, avaliar vulnerabilidades e configurações inadequadas e determinar se mais fortalecimento é necessário.
- **Visibilidade contínua do estado do sistema:** O VMware Carbon Black Cloud identifica o desvio de configuração, a presença de aplicativos desconhecidos ou não autorizados, vulnerabilidades e outras atividades dinâmicas que aumentam a superfície de ataque do ambiente. Por exemplo, ele:
  - Acompanha a existência de mudanças que indiquem atividades mal-intencionadas (como limpeza de senhas e alterações na configuração de BitLocker)
  - Audita e corrige a fim de consultar 1.500 elementos para cada carga de trabalho e endpoint em nuvens privadas e públicas
  - Fortalece administradores para que executem consultas SQL personalizadas e estejam em alerta quanto a atividades ou comportamentos específicos mal-intencionados
- **Visibilidade contínua das vulnerabilidades e da atividade da rede:** O VMware Carbon Black Cloud possibilita que os administradores do vSphere visualizem as vulnerabilidades de carga de trabalho priorizadas por risco no VMware vCenter® e executem regularmente avaliações de vulnerabilidade sem verificação em cargas de trabalho. O NSX fornece um firewall distribuído incorporado, para que as equipes de operações de TI possam acompanhar a comunicação de cargas de trabalho em nuvens privadas e públicas, determinar quais cargas de trabalho fazem parte de um app e determinar como segmentar as cargas de trabalho não relacionadas.

Etapa 2: Evite o aumento dos riscos

- **Evitar explorações da carga de trabalho:** O VMware Carbon Black Cloud disponibiliza um antivírus de próxima geração (NGAV, pela sigla em inglês) para proteção que transcende os indicadores pontuais para malware, ransomware, dia zero, variantes rápidas, arquivos suspeitos e processos potencialmente indesejados (PUPs, pela sigla em inglês) específicos das cargas de trabalho em nuvens privadas e públicas. A plataforma da VMware combina armadilhas para ransomware, análise dinâmica e aprendizado de máquina para fornecer análise contínua que impede a execução de arquivos suspeitos.
- **Evitar ataques sem programa malicioso:** Além de bloquear ataques de malware, o VMware Carbon Black Cloud protege contra os últimos ataques persistentes usando táticas de malware fileless (sem arquivo), baseados em memória e living-off-the-land (LotL). Esses ataques danosos usam o software existente e os apps na lista de elementos permitidos (por exemplo, PowerShell) e protocolos autorizados para desenvolver atividades mal-intencionadas. Ao contrário das abordagens legadas que se baseiam em ameaças conhecidas, a plataforma da VMware pode identificar novas variantes e explorações de dia zero combinando comportamentos conectados.
- **Impedir ataques baseados na rede:** O NSX Service-defined Firewall protege as cargas de trabalho ao mitigar o movimento lateral e bloquear explorações de entrada de aplicativos e serviços vulneráveis. Com esse nível de visibilidade, é possível compreender como ataques de LotL se movem pela rede, identificar indicadores de comprometimento (IOCs, pela sigla em inglês) e suspender essas conexões de rede para isolar cargas de trabalho dos invasores.
- **Personalizar a prevenção:** Cada ambiente tem restrições operacionais diferentes e que frequentemente concorrem entre si. A VMware oferece aos nossos clientes a capacidade de equilibrar a segurança e os riscos operacionais com detalhamento preciso. Com o mecanismo de políticas da VMware, é possível escolher como mitigar ameaças com base no tipo específico de carga de trabalho, sua função, criticalidade e adjacência com outras cargas de trabalho essenciais. Por exemplo, para isolar uma carga de trabalho essencial, um sysadmin pode impedir que o PowerShell extraia a memória de outro processo ou invoque um aplicativo não confiável.

Etapa 3: Detecte e responda a riscos contínuos

- **Saber quando e onde começar uma investigação (aumente o nível dos detalhes):** Use a detecção automatizada de ameaças pronta para uso da VMware por meio da inteligência de detecção de ameaças atualizada do VMware Threat Analysis Unit™ para identificar sistemas afetados e isolá-los para correção. As APIs da VMware permitem que você integre seus próprios feeds e listas de observações de terceiros e forneça mais informações colaborativas de compartilhamento de ameaças no robusto User Exchange da VMware.
- **Ver o escopo completo e o período do ataque (reduza o zoom):** A plataforma da VMware permitem que os investigadores voltem no tempo para compreender como um ataque se desenrolou, quais sistemas foram afetados e como o ataque progrediu ao longo do tempo. Como a VMware captura todos os dados (por exemplo, atividade de processo detalhada, interação de processo com processo, relacionamento pais-filhos do processo etc.), a criação de uma linha de tempo detalhada sem pontos cegos, muito depois da ocorrência, possibilita a resposta a incidentes e que equipes forenses cheguem à verdade.
- **Fluxo de trabalho rápido de detecção para prevenção:** Em três etapas simples, o VMware Carbon Black Cloud permite que você converta a detecção de ameaças em uma política de prevenção padronizada em todas as suas cargas de trabalho. Primeiro, aplique políticas automatizadas com base em detecções anteriores personalizadas para suas cargas de trabalho. Em seguida, visualize instantaneamente os efeitos subsequentes da política de prevenção antes que ela seja implementada. Por fim, com um único clique, implemente a política atualizada em cargas de trabalho de qualquer ambiente.

A proteção de cargas de trabalho na nuvem contra uma ampla variedade de ameaças exige uma abordagem com muitos elementos, com visibilidade detalhada e unificada de todos os aspectos do ambiente de computação. As equipes de operações de TI, DevOps e SecOps precisam compartilhar a responsabilidade pela proteção das cargas de trabalho essenciais na nuvem. As empresas que tentam usar abordagens tradicionais para proteger nuvens híbridas enfrentam muitos desafios, incluindo a falta de visibilidade de como as cargas de trabalho se conectam, processos fragmentados e configurações inadequadas. Conforme discutido neste documento, aumentar a visibilidade, acelerar a recuperação e simplificar a segurança são três estratégias-chave que as equipes corporativas precisam colocar em prática para mitigar os riscos.

A VMware está em uma posição única para proteger cargas de trabalho em nuvens híbridas. Especificamente, as soluções VMware capacitam equipes a identificar de forma precisa os riscos emergentes a cargas de trabalho, evitar o aumento desses riscos e conter surtos rapidamente sem interromper as operações. Embora outros produtos de segurança de endpoints e cargas de trabalho coletem apenas um conjunto de dados relacionados a malfeitores conhecidos, o VMware Carbon Black Cloud coleta continuamente dados abrangentes de cargas de trabalho, endpoints e redes e analisa os padrões de comportamento dos invasores para interromper ataques de forma proativa antes do impacto. Esse nível de visibilidade operacional aumentada simplifica a segurança e acelera a recuperação do sistema.

Embora haja no mercado muitos fornecedores de proteção de cargas de trabalho na nuvem, nem todas as soluções são iguais. As empresas precisam considerar requisitos fundamentais, como a arquitetura de design, modelos operacionais e o dimensionamento, e fazer as perguntas certas para determinar com que eficácia a plataforma corresponde às necessidades. Use a lista de verificação na Tabela 2 ao considerar plataformas de proteção de carga de trabalho na nuvem. Com 100 pontos para alocar, atribua pontos a cada pergunta chave no que se refere à sua organização. O valor total da coluna de valor ponderado deve ser igual a 100. Ao preencher essa lista de verificação, você terá uma noção melhor de suas prioridades e considerações principais.

Lista de verificação de avaliação da plataforma de proteção de cargas de trabalho na nuvem

	REQUISITO PRINCIPAL	PRINCIPAIS PERGUNTAS	VALOR PONDERADO
Arquitetura de design	Descreva como a plataforma de proteção de cargas de trabalho na nuvem acompanha as comunicações e conexões entre as cargas de trabalho.	Ela pode consolidar os dados de telemetria entre nuvens, cargas de trabalho, redes e endpoints?	
		Ela oferece suporte a cada aplicativo, independentemente do sistema operacional, da configuração e da nuvem, ou é dependente de algum desses itens?	
		Ela consegue reconhecer o que constitui comportamento normal em uma carga de trabalho ou entre cargas de trabalho?	
		Quais modelos comportamentais ela implanta para detectar ataques de malware e sem programa malicioso (fileless) nas cargas de trabalho e entre elas?	
Modelo operacional	Descreva como a plataforma de proteção de carga de trabalho na nuvem oferece suporte ao alinhamento e à coordenação sem conflitos entre equipes de operações de TI, DevOps e SecOps para reduzir o risco, simplificar a conformidade e aumentar a resiliência.	Quantos agentes são necessários para instalação em cada carga de trabalho, contêiner e sistema operacional?	
		As equipes de operações de TI, DevOps e SecOps podem aproveitar o mesmo conjunto de dados ao acompanhar e responder a incidentes?	
		A quais estruturas de governança a sua plataforma oferece suporte (por exemplo, NIST 800-53)?	
		Como funcionaria um típico fluxo de trabalho entre equipes de operações de TI, DevOps e SecOps uma vez que uma ameaça, vulnerabilidade ou configuração inadequada fosse identificada?	
Dimensionamento	Descreva como a plataforma de proteção de carga de trabalho na nuvem oferece suporte a programas de controle de mudanças seguros e rápidos para aumentar a padronização da política de segurança e reduzir o risco de configurações inadequadas e outros erros humanos em escala.	Qual é o consumo médio de CPU de cada agente de proteção de carga de trabalho na nuvem?	
		É possível consolidar várias funções de segurança, como EDR, antivírus de última geração e gerenciamento de vulnerabilidade, em um único agente e console de gerenciamento?	
		A plataforma de proteção de carga de trabalho na nuvem pode promover uma política de segurança consistente e padronizada, bem como preparar relatórios sobre ela em ambientes de nuvem privada, pública e híbrida?	
		Como ela conduz a verificação de vulnerabilidade regular sem afetar a disponibilidade e o desempenho?	

TABELA 2: Lista de verificação de avaliação da proteção de cargas de trabalho na nuvem.

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