**Introdução**

Neste módulo, você aprenderá sobre algumas das ferramentas de segurança que podem ajudar a manter a infraestrutura e os dados seguros ao trabalhar na nuvem.

Segurança é uma palavra pequena com um conceito significativo. Há muitos fatores que você deve considerar para proteger os aplicativos e os dados. Como o Azure ajuda você a proteger cargas de trabalho executadas na nuvem e no datacenter local?

## **Conheça a Tailwind Traders**

A [Tailwind Traders](https://www.tailwindtraders.com/" \t "az-portal) é um varejista fictício de materiais para reforma e construção. A empresa opera lojas de varejo de ferragens em todo o mundo e online. Os diferenciais da Tailwind Traders são os preços competitivos, as entregas rápidas e a ampla gama de itens. Eles estão examinando as tecnologias de nuvem para aprimorar as operações de negócios e dar suporte à expansão para novos mercados. Ao migrar para a nuvem, a empresa pretende aprimorar a experiência de compra para se diferenciar ainda mais dos concorrentes.

## **Como a Tailwind Traders será executada com segurança na nuvem e no datacenter?**

A Tailwind Traders executa um mix de cargas de trabalho no Azure e no datacenter da empresa.

Eles precisam verificar se todos os seus sistemas atendem a um nível mínimo de segurança e se as informações estão protegidas contra ataques. A empresa também precisa de uma forma de coletar eventos de segurança e atuar sobre esses eventos em toda a sua propriedade digital.

Vamos explorar como a Tailwind Traders pode usar algumas das ferramentas e dos recursos do Azure como parte de sua estratégia geral de segurança.

## **Objetivos de aprendizagem**

Depois de concluir este módulo, você poderá:

* Fortalecer sua postura de segurança e se proteger contra ameaças usando a Central de Segurança do Azure.
* Coletar dados de segurança de várias fontes diferentes e atuar sobre eles usando o Azure Sentinel.
* Armazenar e acessar informações confidenciais (como senhas e chaves de criptografia) com segurança no Azure Key Vault.
* Gerenciar servidores físicos dedicados para hospedar suas VMs do Azure para Windows e Linux usando o Host Dedicado do Azure.

## **Pré-requisitos**

* Você precisa estar familiarizado com a terminologia e os conceitos básicos da computação.
* Ter familiaridade com a computação em nuvem é útil, mas não é necessário.

# Proteger-se contra ameaças à segurança usando a Central de Segurança do Azure

A Tailwind Traders está ampliando o uso dos serviços do Azure. Eles ainda têm cargas de trabalho locais em que aplicam as melhores práticas de configuração e procedimentos empresariais atuais relacionados à segurança. Como a empresa pode garantir que todos os seus sistemas atendam a um nível mínimo de segurança e que suas informações estejam protegidas contra ataques?

Muitos serviços do Azure incluem recursos de segurança internos. As ferramentas no Azure também podem ajudar a Tailwind Traders com esse requisito. Vamos começar examinando a Central de Segurança do Azure.

## O que é a Central de Segurança do Azure?

A [Central de Segurança do Azure](https://azure.microsoft.com/services/security-center) é um serviço de monitoramento que fornece visibilidade da postura de segurança em todos os serviços, tanto no Azure quanto localmente. O termo postura de segurança se refere a políticas e controles de segurança cibernética, bem como à sua capacidade de prever, impedir e responder com sucesso às ameaças de segurança.

A Central de Segurança pode:

* Monitorar as configurações de segurança das cargas de trabalho locais e na nuvem.
* Aplicar automaticamente as configurações de segurança obrigatórias aos novos recursos à medida que ficarem online.
* Fornecer recomendações de segurança baseadas nas configurações, nos recursos e nas redes atuais.
* Monitorar continuamente os recursos e realizar avaliações de segurança automáticas para identificar possíveis vulnerabilidades antes que elas possam ser exploradas.
* Usar machine learning para detectar e bloquear a instalação de malwares em VMs (máquinas virtuais) e em outros recursos. Você também pode usar os controles de aplicativo adaptáveis para definir regras que listam os aplicativos permitidos a fim de verificar se somente os aplicativos que você permitir serão executados.
* Detectar e analisar possíveis ataques de entrada e investigar ameaças e qualquer atividade pós-violação que possa ter ocorrido.
* Fornecer controle de acesso just-in-time para as portas de rede. Isso reduz a superfície de ataque, garantindo que a rede só permita o tráfego exigido por você, no momento necessário.

Este vídeo rápido explica como a Central de Segurança pode ajudar a reforçar suas redes, proteger e monitorar seus recursos de nuvem e melhorar sua postura geral de segurança

## **Entender a postura de segurança**

A Tailwind Traders pode usar a Central de Segurança para obter uma análise detalhada dos diferentes componentes de seu ambiente. Como os recursos da empresa são analisados em relação aos controles de segurança das políticas de governança atribuídas, eles podem ver a conformidade regulatória geral de uma perspectiva de segurança, tudo em um só lugar.

Confira no exemplo a seguir o que você pode ver na Central de Segurança do Azure.

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Digamos que a Tailwind Traders precise cumprir o PCI DSS (Padrão de Segurança de Dados do Setor de Cartão de Pagamento). Este relatório mostra que a empresa tem recursos que precisam ser corrigidos.

Na seção **Higiene da segurança de recursos**, a Tailwind Traders pode ver a integridade dos recursos de uma perspectiva de segurança. Para ajudar a priorizar as ações de correção, as recomendações são categorizadas como baixa, média e alta. Veja um exemplo.

Uma imagem contendo Gráfico de barras

Descrição gerada automaticamente

### O que é a classificação de segurança?

A [classificação de segurança](https://docs.microsoft.com/pt-br/azure/security-center/secure-score-security-controls/) é uma medida da postura de segurança de uma organização.

A classificação de segurança é baseada em controles de segurança ou grupos de recomendações de segurança relacionadas. A pontuação é baseada no percentual de controles de segurança que você atende. Quanto mais controles de segurança você atender, maior será a pontuação recebida. Sua pontuação melhora quando você corrige todas as recomendações para um recurso dentro de um controle.

Veja um exemplo do portal do Azure mostrando uma pontuação de 57%, ou seja, 34 de 60 pontos.

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Seguir as recomendações de classificação de segurança pode ajudar a proteger a organização contra ameaças. De um painel centralizado na Central de Segurança do Azure, as organizações podem monitorar e trabalhar na segurança dos recursos do Azure, como identidades, dados, aplicativos, dispositivos e infraestrutura.

A classificação de segurança ajuda você a:

* Relatar o estado atual da postura de segurança da organização.
* Melhorar a postura de segurança fornecendo capacidade de descoberta e de visibilidade, além de diretrizes e controle.
* Comparar com parâmetros de comparação e estabelecer KPIs (indicadores chave de desempenho).

## Proteção contra ameaças

A Central de Segurança inclui funcionalidades avançadas de defesa de nuvem para VMs, segurança de rede e integridade de arquivo. Vamos ver como algumas dessas funcionalidades se aplicam à Tailwind Traders.

* **Acesso just-in-time à VM** A Tailwind Traders vai configurar o acesso just-in-time às VMs. Esse acesso bloqueia por padrão o tráfego para portas de rede específicas de VMs, mas permite o tráfego por um período especificado quando um administrador o solicita e aprova.
* **Controles de aplicativo adaptáveis** A Tailwind Traders pode controlar quais aplicativos podem ser executados em suas VMs. Em segundo plano, a Central de Segurança usa machine learning para examinar os processos em execução em uma VM. Ela cria regras de exceção para cada grupo de recursos que contém as VMs e fornece recomendações. Esse processo fornece alertas que informam a empresa sobre aplicativos não autorizados em execução em suas VMs.
* **Proteção de rede adaptável** A Central de Segurança pode monitorar os padrões de tráfego de Internet das VMs e comparar esses padrões com as configurações atuais de NSG (grupo de segurança de rede) da empresa. Em seguida, a Central de Segurança pode recomendar que os NSGs sejam bloqueados ainda mais e fornecer etapas de correção.
* **Monitoramento de integridade do arquivo** A Tailwind Traders também pode configurar o monitoramento de alterações em arquivos importantes no Windows e no Linux, de configurações do Registro, de aplicativos e de outros aspectos que possam indicar um ataque de segurança.

## Responder a alertas de segurança

A Tailwind Traders pode usar a Central de Segurança para ter uma visão centralizada de todos os alertas de segurança. Com isso, a empresa pode ignorar falsos alertas, investigar mais a fundo, corrigir alertas manualmente ou usar uma resposta automatizada com uma automação de fluxo de trabalho.

A automação do fluxo de trabalho usa os Aplicativos Lógicos do Azure e os conectores da Central de Segurança. O aplicativo lógico pode ser disparado por um alerta de detecção de ameaças ou por uma recomendação da Central de Segurança, filtrada por nome ou pela severidade. Em seguida, você pode configurar o aplicativo lógico para executar uma ação, como enviar um email ou postar uma mensagem em um canal do Microsoft Teams.

# Detectar e responder a ameaças de segurança usando o Azure Sentinel

O gerenciamento da segurança em grande escala pode se beneficiar de um sistema de SIEM (gerenciamento de evento e informações de segurança) dedicado. O sistema de SIEM agrega dados de segurança de várias fontes diferentes (contanto que essas fontes sejam compatíveis com um formato padrão aberto de registro em log). Ele também fornece recursos de detecção e resposta a ameaças.

O [Azure Sentinel](https://azure.microsoft.com/services/azure-sentinel/) é o sistema de SIEM baseado em nuvem da Microsoft. Ele usa análise de segurança e análise de ameaças inteligentes.

## Funcionalidades do Azure Sentinel

O Azure Sentinel permite que você:

* **Coletar dados de nuvem em escala** Colete dados de todos os usuários, dispositivos, aplicativos e infraestrutura, tanto locais quanto de várias nuvens.
* **Detectar ameaças não detectadas anteriormente** Minimize falsos positivos usando a análise abrangente e a inteligência contra ameaças da Microsoft.
* **Investigar ameaças com inteligência artificial** Examine atividades suspeitas em escala, aproveitando a longa experiência em segurança cibernética da Microsoft.
* **Responder a incidentes rapidamente** Use a orquestração e a automação internas para tarefas comuns.

## Conectar suas fontes de dados

A Tailwind Traders decide explorar as funcionalidades do Azure Sentinel. Primeiro, a empresa identifica e conecta suas fontes de dados.

O Azure Sentinel é compatível com várias fontes de dados, que podem ser analisadas em busca de eventos de segurança. Essas conexões são gerenciadas por conectores internos ou por APIs e formatos de log padrão do setor.

* **Conectar soluções da Microsoft** Os conectores fornecem integração em tempo real para serviços como as soluções de Proteção contra Ameaças da Microsoft, as fontes do Microsoft 365 (incluindo o Office 365), o Azure Active Directory e o Windows Defender Firewall.
* **Conectar outros serviços e soluções** Há conectores disponíveis para serviços e soluções comuns de terceiros, incluindo AWS CloudTrail, Citrix Analytics (Security), Sophos XG Firewall, VMware Carbon Black Cloud e Okta SSO.
* **Conectar fontes de dados padrão do setor** O Azure Sentinel dá suporte a dados de outras fontes que usam o padrão de mensagens CEF (Formato Comum de Evento), o Syslog ou a API REST.

## Detectar ameaças

A Tailwind Traders precisa ser notificada quando ocorre algo suspeito. A empresa decide usar regras personalizadas e análise interna para detectar ameaças.

A **análise interna** usa modelos criados pela equipe de analistas e especialistas em segurança da Microsoft com base em ameaças conhecidas, em vetores de ataque comuns e nas cadeias de escalonamento de atividades suspeitas. Esses modelos podem ser personalizados e pesquisar em todo o ambiente por qualquer atividade que pareça suspeita. Alguns modelos usam a análise comportamental de machine learning, que se baseia em algoritmos proprietários da Microsoft.

A **análise personalizada** são regras que você cria para pesquisar critérios específicos em seu ambiente. Você pode visualizar o número de resultados que a consulta geraria (com base nos eventos de log anteriores) e definir uma agenda para a execução da consulta. Você também pode definir um limite de alerta.

## Investigar e responder

Quando o Azure Sentinel detecta eventos suspeitos, a Tailwind Traders pode investigar alertas ou incidentes específicos (um grupo de alertas relacionados). Com o grafo de investigação, a empresa pode analisar informações de entidades conectadas diretamente ao alerta e ver consultas de exploração comuns para ajudar a orientar a investigação.

Veja um exemplo que mostra como seria um grafo de investigação no Azure Sentinel.

Diagrama

Descrição gerada automaticamente com confiança média

A empresa também usará as [Pastas de Trabalho do Azure Monitor](https://docs.microsoft.com/pt-br/azure/azure-monitor/platform/workbooks-overview/) para automatizar as respostas a ameaças. Por exemplo, eles podem definir um alerta que procura endereços IP mal-intencionados que acessam a rede, além de criar uma pasta de trabalho que realiza as seguintes etapas:

1. Quando o alerta for disparado, abra um tíquete no sistema de gerenciamento de tíquetes de TI.
2. Envie uma mensagem ao canal de operações de segurança do Microsoft Teams ou do Slack para verificar se os analistas de segurança estão cientes do incidente.
3. Envie todas as informações do alerta para o administrador de rede sênior e para o administrador de segurança. A mensagem de email inclui dois botões de opção do usuário: **Bloquear** ou **Ignorar**.

Quando um administrador escolhe **Bloquear**, o endereço IP é bloqueado no firewall e o usuário é desabilitado no Azure Active Directory. Quando um administrador escolhe **Ignorar**, o alerta é fechado no Azure Sentinel e o incidente é fechado no sistema de gerenciamento de tíquetes de TI.

A pasta de trabalho continua sendo executada após receber uma resposta dos administradores.

As pastas de trabalho podem ser executadas manualmente ou automaticamente quando uma regra dispara um alerta.

# Configurar e gerenciar segredos usando o Azure Key Vault

À medida que a Tailwind Traders cria cargas de trabalho na nuvem, informações confidenciais (como senhas, chaves de criptografia e certificados) precisam ser gerenciadas com cuidado. Essas informações precisam estar disponíveis para que um aplicativo funcione, mas poderiam permitir que uma pessoa não autorizada acessasse os dados do aplicativo.

O [Azure Key Vault](https://azure.microsoft.com/services/key-vault) é um serviço de nuvem centralizado para armazenar segredos do aplicativo em um só local centralizado. Ele oferece acesso seguro a informações confidenciais fornecendo controle de acesso e funcionalidades de registro em log.

## **O que o Azure Key Vault pode fazer?**

O Azure Key Vault pode ajudar você a:

* **Gerenciar segredos** Você pode usar o Key Vault para armazenar tokens, senhas, certificados, chaves de API e outros segredos e controlar com segurança o acesso a eles.
* **Gerenciar chaves de criptografia** Você pode usar o Key Vault como uma solução de gerenciamento de chaves. O Key Vault facilita a criação e o controle das chaves de criptografia usadas para criptografar os dados.
* **Gerenciar certificados SSL/TLS** O Key Vault permite provisionar, gerenciar e implantar certificados SSL/TLS públicos e privados para recursos do Azure e recursos internos.
* **Armazenar segredos com o suporte de HSMs (módulos de segurança de hardware)** Esses segredos e chaves podem ser protegidos por software ou por HSMs validados pelo FIPS 140-2 Nível 2.

Aqui está um exemplo que mostra um certificado usado para teste no Key Vault.

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Você adicionará um segredo ao Key Vault mais adiante neste módulo.

## Quais são os benefícios do Azure Key Vault?

Os benefícios de usar o Key Vault incluem:

* **Segredos de aplicativos centralizados** A centralização do armazenamento de segredos de aplicativos permite que você controle a distribuição e reduz as chances de vazamento acidental de segredos.
* **Chaves e segredos armazenados com segurança** O Azure usa algoritmos, comprimentos de chave e HSMs padrão do setor. O acesso ao Key Vault exige autenticação e autorização adequadas.
* **Monitoramento e controle de acesso** Usando o Key Vault, você pode monitorar e controlar o acesso aos segredos de aplicativos.
* **Administração simplificada de segredos de aplicativos** O Key Vault facilita o registro e a renovação de certificados de CAs (autoridades de certificação) públicas. Você também pode escalar verticalmente e replicar o conteúdo dentro das regiões e usar ferramentas padrão para o gerenciamento de certificados.
* **Integração com outros serviços do Azure** Você pode integrar o Key Vault com contas de armazenamento, registros de contêiner, hubs de eventos e muitos outros serviços do Azure. Então, esses serviços podem referenciar com segurança os segredos armazenados no Key Vault.

# Hospedar suas máquinas virtuais do Azure em servidores físicos dedicados usando o Host Dedicado do Azure

No Azure, as VMs (máquinas virtuais) são executadas em hardware compartilhado gerenciado pela Microsoft. Embora o hardware subjacente seja compartilhado, suas cargas de trabalho de VM são isoladas das cargas de trabalho executadas por outros clientes do Azure.

Algumas organizações precisam aderir à conformidade regulatória que exige que elas sejam o único cliente usando o computador físico que hospeda as máquinas virtuais. O [Host Dedicado do Azure](https://azure.microsoft.com/services/virtual-machines/dedicated-host/) fornece servidores físicos dedicados para hospedar as VMs do Azure para Windows e Linux.

Veja um diagrama que mostra como as VMs se relacionam com hosts dedicados e grupos de hosts. Um *host dedicado* é mapeado para um servidor físico em um datacenter do Azure. Um *grupo de hosts* é uma coleção de hosts dedicados.

Uma imagem contendo Interface gráfica do usuário

Descrição gerada automaticamente

## **Quais são os benefícios do Host Dedicado do Azure?**

O Host Dedicado do Azure:

* Fornece visibilidade e controle sobre a infraestrutura de servidor que está executando as VMs do Azure.
* Ajuda a endereçar os requisitos de conformidade implantando as cargas de trabalho em um servidor isolado.
* Permite que você escolha o número de processadores, as funcionalidades do servidor, a série de VMs e os tamanhos de VM dentro do mesmo host.

## **Considerações de disponibilidade para o Host Dedicado**

Depois que um host dedicado é provisionado, o Azure o atribui ao servidor físico no datacenter de nuvem da Microsoft.

Para alta disponibilidade, você pode provisionar vários hosts em um grupo de hosts e implantar suas VMs nesse grupo. VMs em hosts dedicados também podem aproveitar o controle de manutenção. Esse recurso permite controlar quando ocorrem atualizações de manutenção regulares, dentro de uma janela ininterrupta de 35 dias.

## **Considerações de preço**

Você é cobrado pelo host dedicado, independentemente do número de VMs implantadas. O preço do host é baseado na família, no tipo (tamanho do hardware) e na região da VM.

O licenciamento de software, o armazenamento e o uso de rede são cobrados separadamente do host e das VMs. Para obter mais informações. Confira os [preços do Host Dedicado do Azure](https://aka.ms/ADHPricing/).

# Verificação de conhecimentos

Considere este cenário.

A Tailwind Traders está movendo seu sistema de pagamento online do datacenter para a nuvem. O sistema de pagamento é composto por VMs (máquinas virtuais) e por bancos de dados do SQL Server.

Veja alguns requisitos de segurança que a empresa identifica conforme planeja a migração:

* Eles querem garantir uma boa postura de segurança em todos os sistemas, tanto no Azure quanto no local.
* No datacenter, o acesso a VMs exige um certificado TLS. A empresa precisa de um local para armazenar e gerenciar os certificados com segurança.

Aqui estão alguns requisitos adicionais relacionados à conformidade regulatória:

* A Tailwind Traders precisa armazenar alguns dados do cliente localmente, no datacenter.
* Para determinadas cargas de trabalho, a empresa precisa ser os único cliente a executar VMs no hardware físico.
* Eles precisam executar somente aplicativos de negócios aprovados em cada VM.

Confira o diagrama a seguir que mostra a arquitetura proposta.

Interface gráfica do usuário, Aplicativo, PowerPoint

Descrição gerada automaticamente

No Azure, a Tailwind Traders usará VMs padrão e VMs executadas em hardware físico dedicado. No datacenter, a empresa executará VMs capazes de se conectar a bancos de dados dentro da rede interna.

Escolha a melhor resposta para cada pergunta. Em seguida, selecione **Verificar suas respostas**.

## Verificar seus conhecimentos

Parte superior do formulário

Texto

Descrição gerada automaticamente

Texto, Aplicativo

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

# Resumo

A Tailwind Traders enfrenta uma série de desafios de segurança. No mundo digital de hoje, as necessidades deles não são exclusivas.

O Azure fornece ferramentas e serviços capazes de ajudar você a detectar e reagir a importantes eventos de segurança. Ele também fornece maneiras de ajudar a manter os dados seguros, o que pode impedir que os incidentes de segurança ocorram.

Neste módulo, você aprendeu sobre os serviços do Azure relacionados à segurança. Confira abaixo um breve resumo:

* A Central de Segurança do Azure fornece visibilidade da postura de segurança em todos os serviços, tanto no Azure quanto localmente.
* O Azure Sentinel agrega dados de segurança de várias fontes diferentes e fornece funcionalidades adicionais para a detecção de – e a resposta a – ameaças.
* O Azure Key Vault armazena os segredos dos aplicativos (como senhas, chaves de criptografia e certificados) em um só local centralizado.
* O Host Dedicado do Azure fornece servidores físicos dedicados para hospedar as VMs do Azure para Windows e Linux.