

© Copyright Microsoft Corporation. All rights reserved.

**FOR USE ONLY AS PART OF MICROSOFT VIRTUAL TRAINING DAYS PROGRAM. THESE MATERIALS ARE NOT AUTHORIZED
FOR DISTRIBUTION, REPRODUCTION OR OTHER USE BY NON-MICROSOFT PARTIES.**



Microsoft Security Virtual Training Day: Security, Compliance, and Identity Fundamentals



**Descreva os conceitos de segurança,
conformidade e identidade**

Objetivos de aprendizagem

- Descrever os conceitos de segurança e conformidade
- Descrever os conceitos de identidade

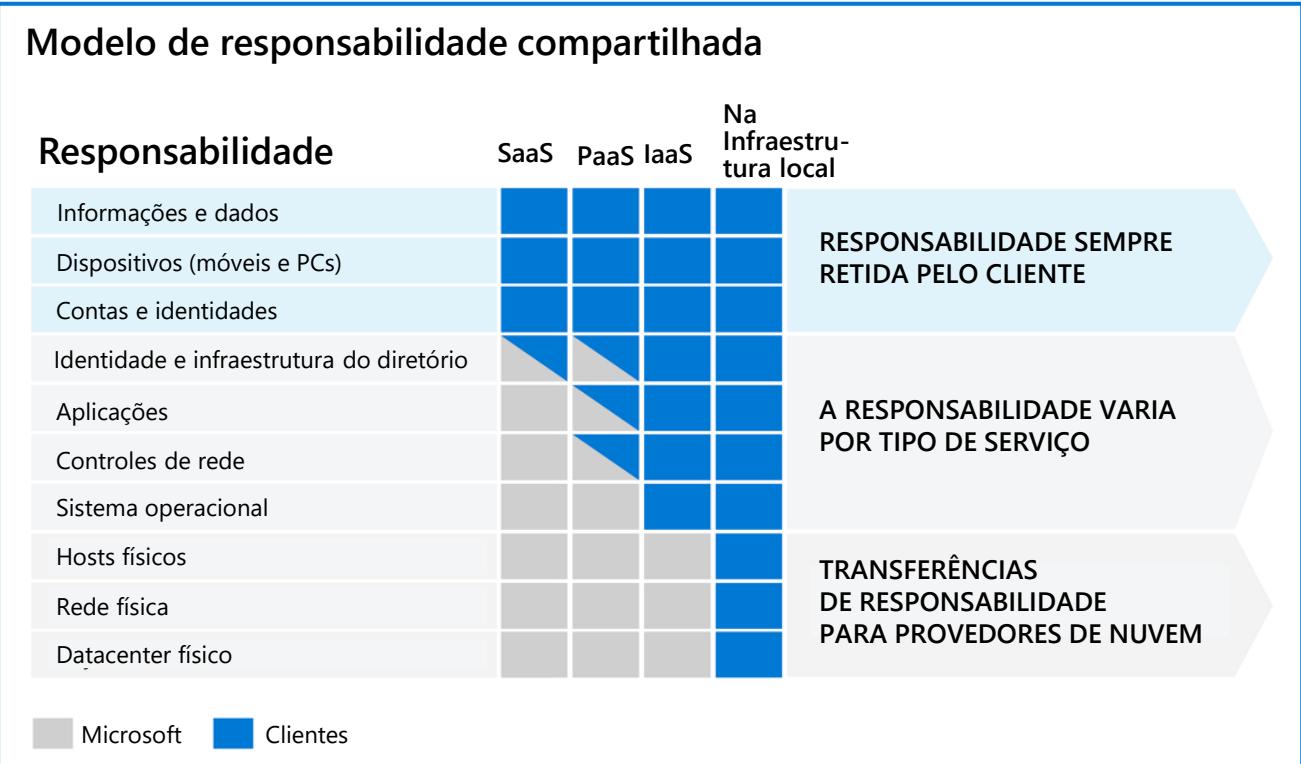
Objetivo de aprendizagem: Descrever os conceitos de segurança e conformidade

O modelo de responsabilidade compartilhada

Identifica quais tarefas de segurança são tratadas pelo provedor de nuvem e quais tarefas de segurança são tratadas por você, o cliente.

As responsabilidades variam com base no local onde o workload é hospedado:

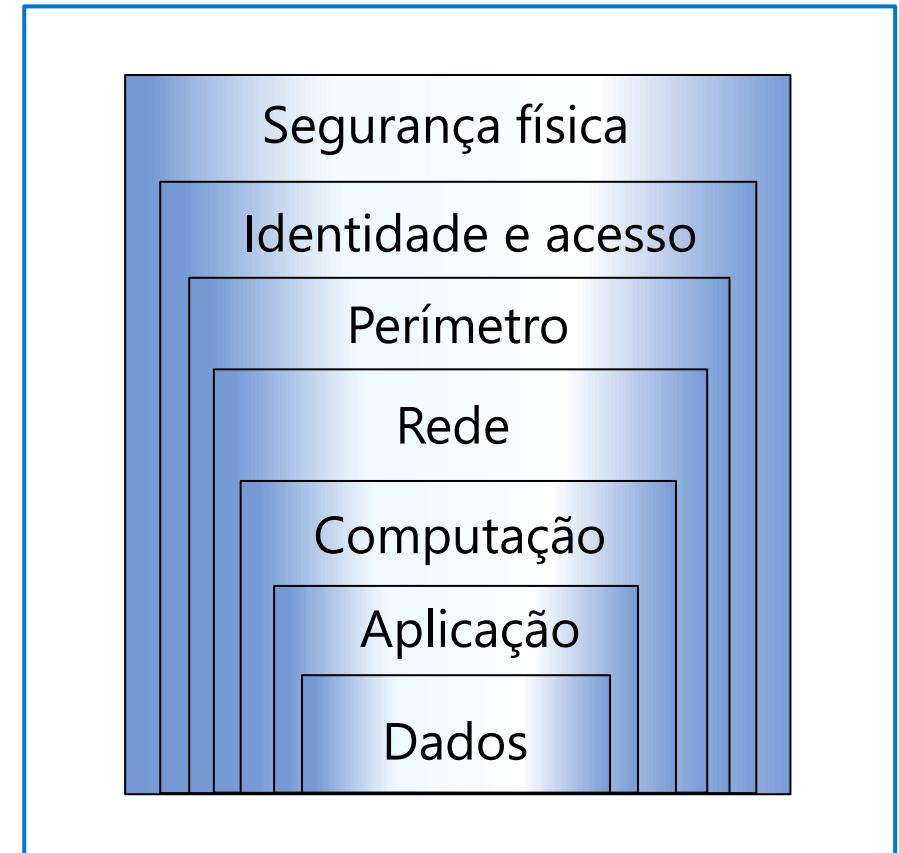
- SaaS (software como serviço)
- PaaS (plataforma como serviço)
- IaaS (infraestrutura como serviço)
- Datacenter na infraestrutura local



Proteção abrangente

A proteção abrangente usa uma abordagem em camadas para a segurança.

- Segurança física, como a limitação do acesso a um datacenter somente a funcionários autorizados.
- Segurança de identidade e acesso que controla o acesso à infraestrutura e o controle de alterações.
- Segurança de perímetro, incluindo proteção de DDoS (negação de serviço distribuído) para filtrar ataques em grande escala.
- Segurança de rede, que pode limitar a comunicação entre recursos usando controles de segmentação e acesso.
- Segurança de camada de computação, como proteger o acesso a máquinas virtuais.
- Segurança da camada da aplicação, que protege os aplicativos contra vulnerabilidades de segurança.
- Controles de segurança da camada de dados, que incluem criptografia para proteger os dados.



Confidencialidade, integridade, disponibilidade (CIA)

Confidencialidade

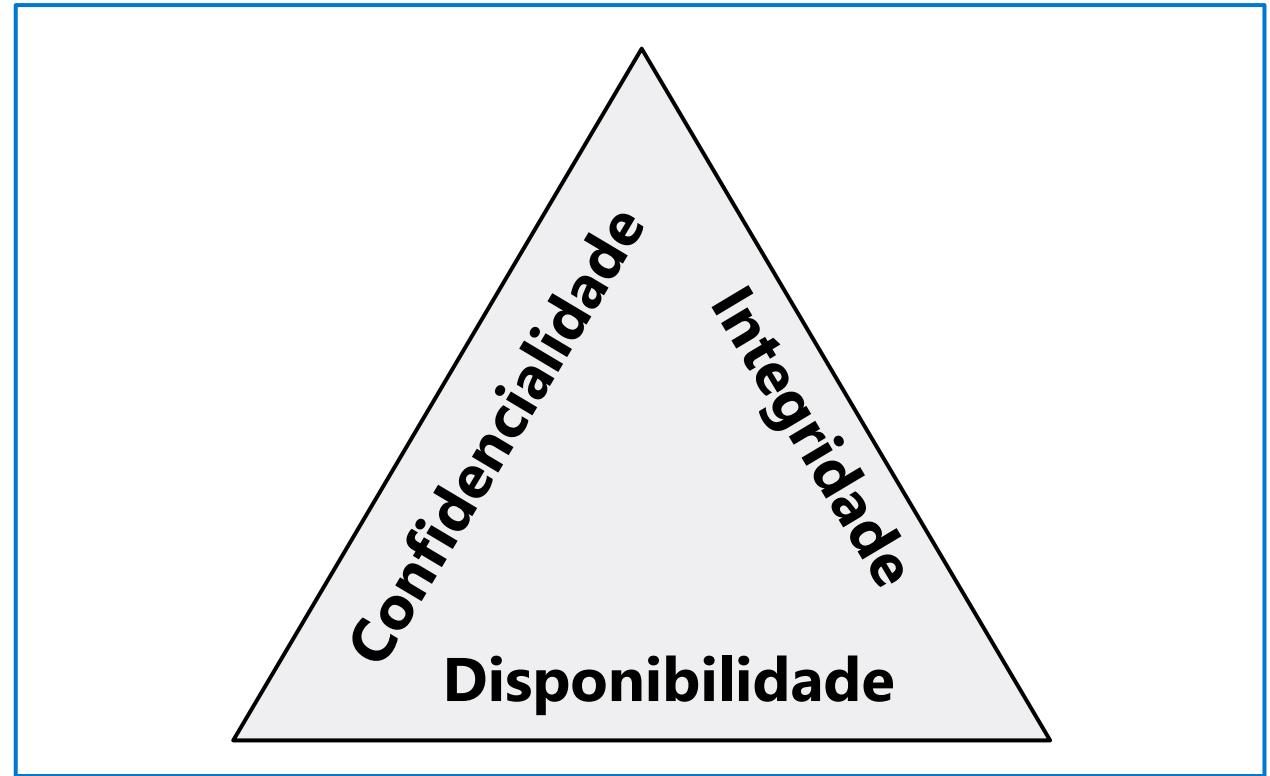
Refere-se à necessidade de manter a confidencialidade dos dados, como informações de clientes, senhas ou dados financeiros.

Integridade

Refere-se a manter dados ou mensagens corretos.

Disponibilidade

Refere-se a disponibilizar dados para quem precisa deles.



O modelo de Confiança Zero

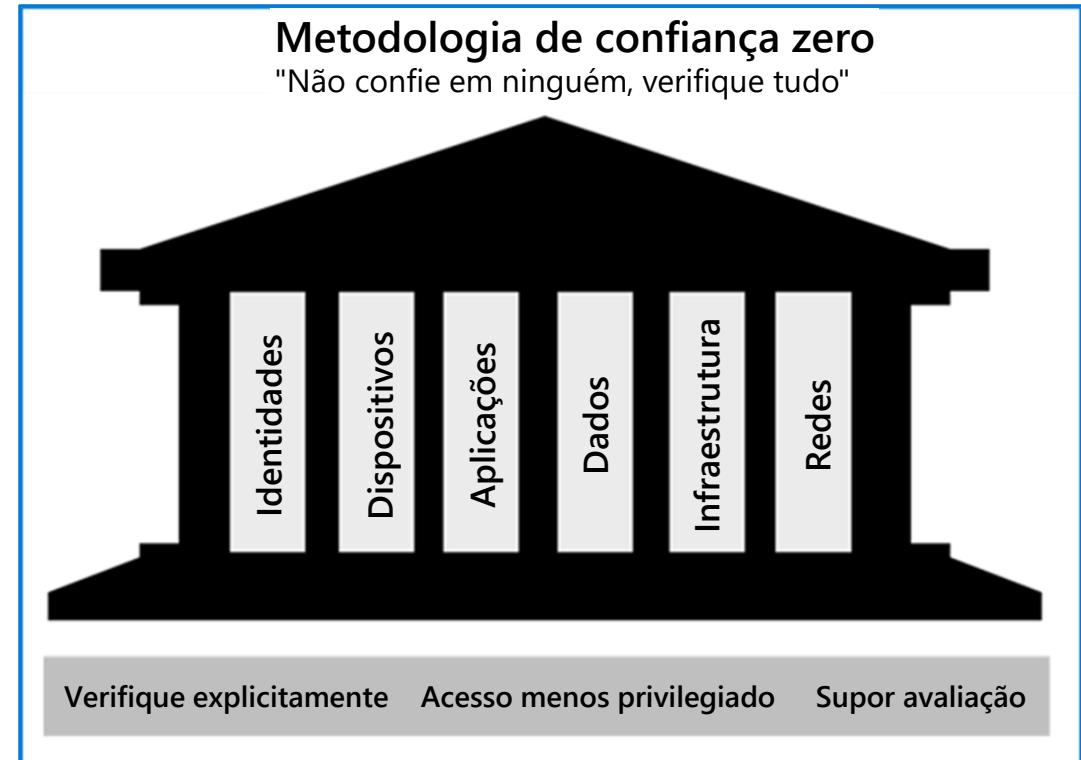
O modelo de confiança zero opera com base no princípio de "não confie em ninguém, verifique tudo".

Princípios orientadores da confiança zero

- Verificação explícita
- Acesso de privilégios mínimos
- Supor violação

Seis pilares fundamentais

- Identidades podem ser usuários, serviços ou dispositivos.
- Dispositivos criam um grande superfície de ataque como fluxos de dados.
- Aplicações são a forma como os dados são consumidos.
- Dados devem ser classificados, rotulados e criptografados.
- Infraestrutura representa um vetor de ameaça.
- Redes devem ser segmentadas.



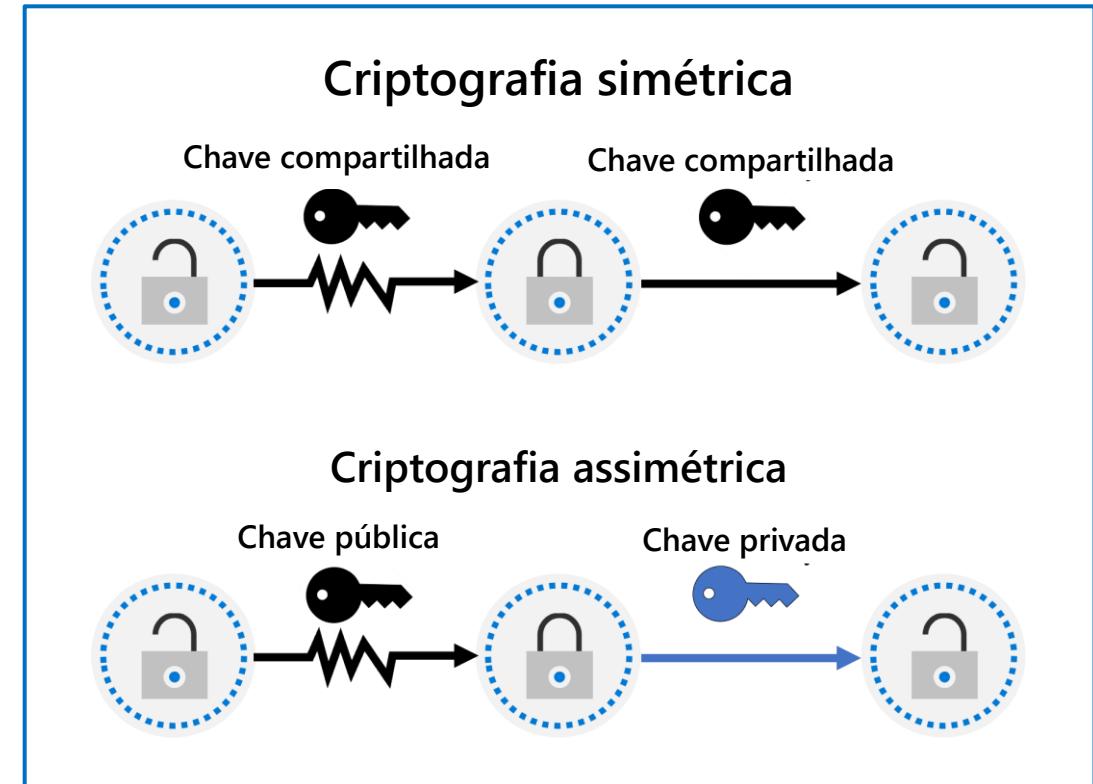
Criptografia

A criptografia é o processo de tornar os dados ilegíveis e inutilizáveis para os espectadores não autorizados.

- Criptografia de dados em repouso
- Criptografia de dados em trânsito
- Criptografia de dados em uso

Dois tipos de criptografia de nível superior:

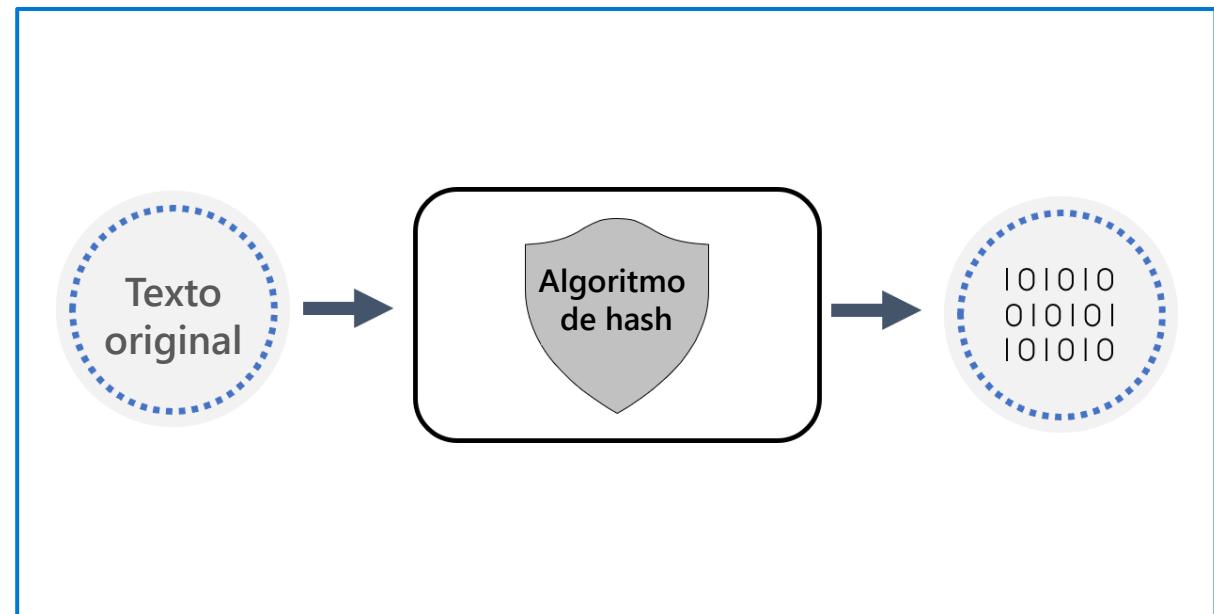
- Simétrica: usa a mesma chave para criptografar e descriptografar os dados.
- Assimétrica: usa uma chave pública e um par de chaves privadas.



Hash

O hash usa um algoritmo para converter o texto original em um valor exclusivo de comprimento fixo, chamado valor hash.

- Determinístico, portanto a mesma entrada produz a mesma saída.
- Um identificador exclusivo de seus dados associados.
- Diferente da criptografia, pois o valor do hash não é subsequentemente descriptografado de volta ao original.
- Usado para armazenar senhas. A senha é “salted” para mitigar o risco de ataque de dicionário de força bruta.



Conceitos de Governança, Conformidade e Risco (GRC)

O GRC ajuda as organizações a reduzir riscos e melhorar a eficácia da conformidade.

- **Governança:** as regras, práticas e processos que uma organização usa para direcionar e controlar suas atividades.
- **Gerenciamento de riscos:** o processo de identificar, avaliar e responder a ameaças ou eventos que podem impactar os objetivos da empresa ou do cliente.
- **Conformidade:** as leis do país/região, estaduais ou federais ou mesmo regulamentos multinacionais que uma organização deve seguir.



Objetivo de aprendizagem: Descrever os conceitos de identidade

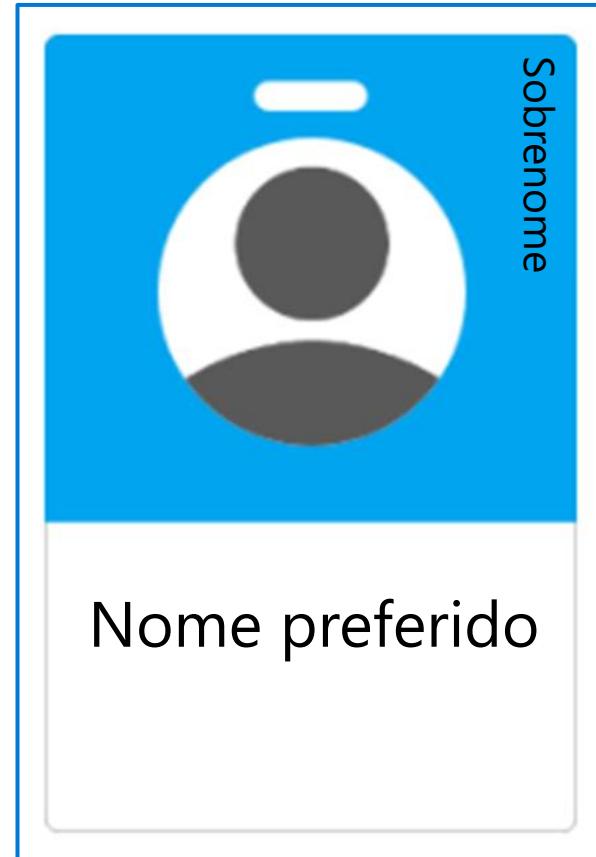
Autenticação e autorização

Autenticação (AuthN)

A autenticação é o processo de provar que uma pessoa é quem diz ser. A autenticação **concede acesso**.

Autorização (AuthZ)

A autorização determina o **nível de acesso ou as permissões** que uma pessoa autenticada tem para seus dados e recursos.



Identidade como o perímetro de segurança principal

A identidade tornou-se o novo perímetro de segurança que permite que as organizações protejam seus ativos.

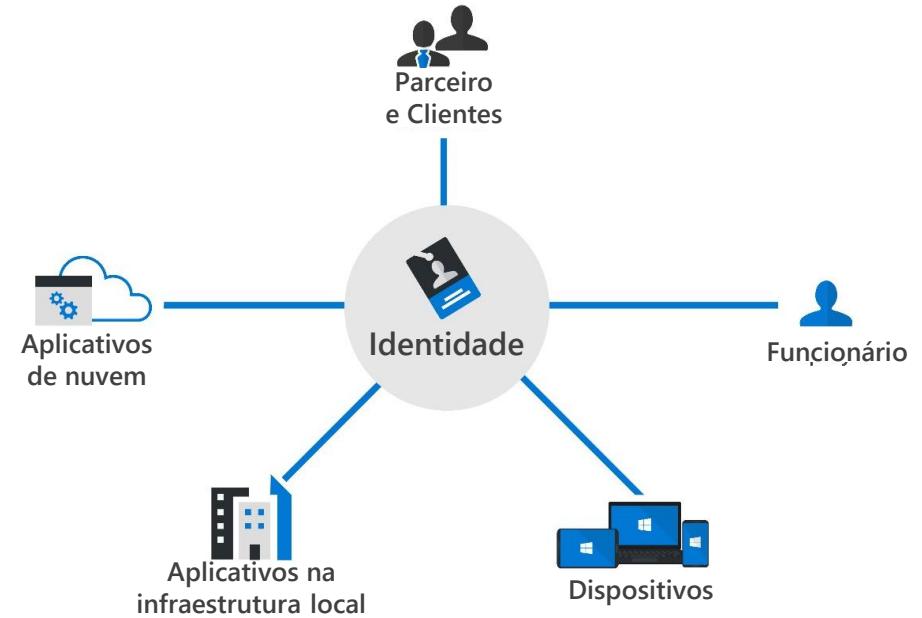
Uma identidade é como alguém ou algo pode ser verificado e autenticado e pode ser associado a:

- Usuário
- Aplicação
- Dispositivo
- Outros

Quatro pilares de uma infraestrutura de identidade:

- Administração
- Autenticação
- Autorização
- Auditoria

A identidade é o novo perímetro de segurança



Autenticação moderna e a função do provedor de identidade

Autenticação moderna é um termo genérico para métodos de autenticação e autorização entre um cliente e um servidor.

-  No centro da autenticação moderna está a função do **provedor de identidade (IdP)**.
-  O IdP oferece serviços de autenticação, autorização e auditoria.
-  O IdP permite que as organizações estabeleçam políticas de autenticação e autorização, monitorem o comportamento do usuário e muito mais.
-  Os recursos fundamentais de um IdP e "autenticação moderna" incluem suporte para métodos de autenticação seguros, logon único, federação com outros IdPs e muito mais.
-  O Microsoft Entra ID é um exemplo de provedor de identidade baseado na nuvem.

O conceito de serviços de diretório

Um serviço de diretório armazena dados de diretório e os disponibiliza para usuários, administradores, serviços e aplicações da rede.



Um diretório é uma estrutura hierárquica que armazena informações sobre objetos na rede.



Um serviço de diretório armazena dados de diretório e os disponibiliza para usuários, administradores, serviços e aplicações da rede.



O serviço mais conhecido desse tipo é o Active Directory Domain Services (AD DS), um componente central em organizações com infraestrutura de TI na infraestrutura local.

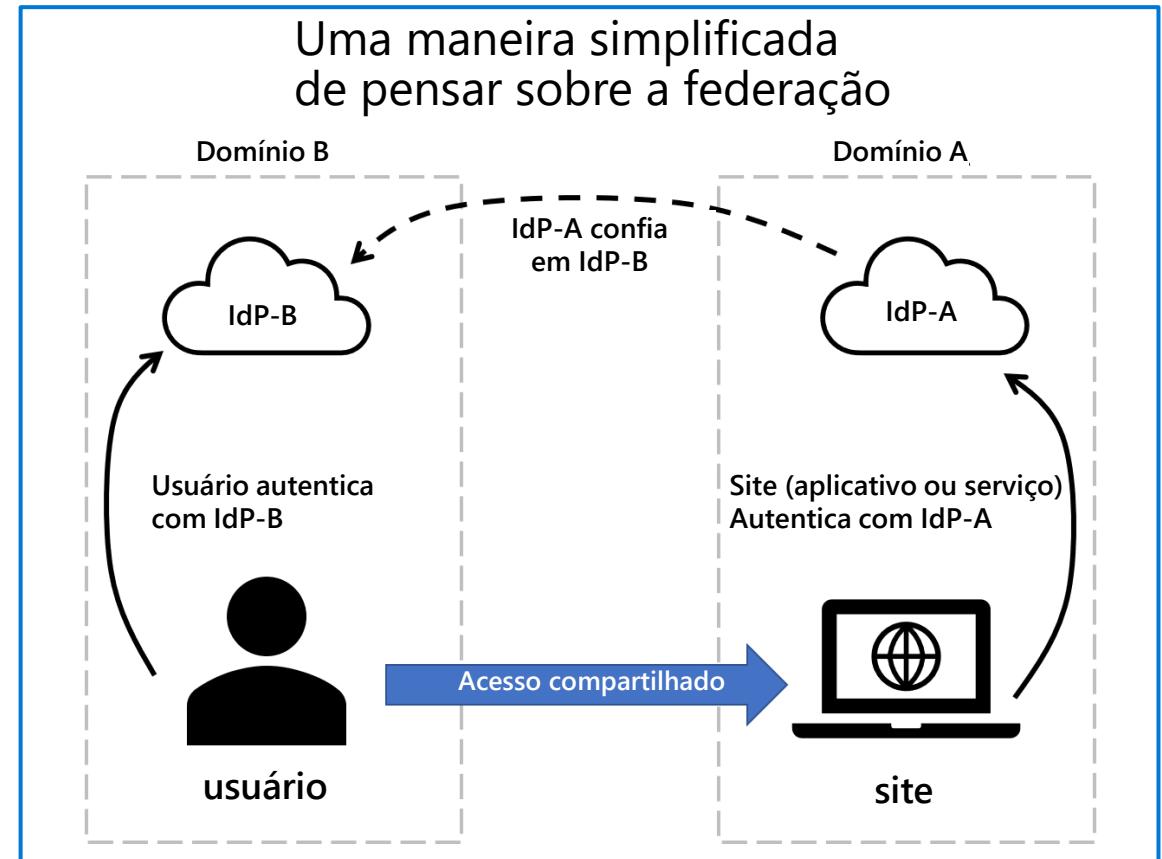


O Microsoft Entra ID é a evolução das soluções de gerenciamento de identidades e acessos, fornecendo às organizações uma solução de identidade como serviço (IDaaS) para todos os seus aplicativos na nuvem e na infraestrutura local.

O conceito de federação

Uma maneira simplificada de pensar sobre a federação:

- O site usa os serviços de autenticação do Provedor de Identidade A (IdP-A).
- O usuário autentica com o Provedor de Identidade B (IdP-B).
- O IdP-A tem uma relação de confiança configurada com o IdP-B.
- Quando o usuário entra no site, o site pode confiar em suas credenciais e permitir o acesso.



Descrever os recursos do Microsoft
Entra



Objetivos de aprendizagem

- Descrever os tipos de função e identidade do Microsoft Entra ID
- Descrever os recursos de autenticação do Microsoft Entra ID
- Descrever os recursos de gerenciamento de acesso do Microsoft Entra
- Descrever os recursos de proteção e governança de identidade do Microsoft Entra

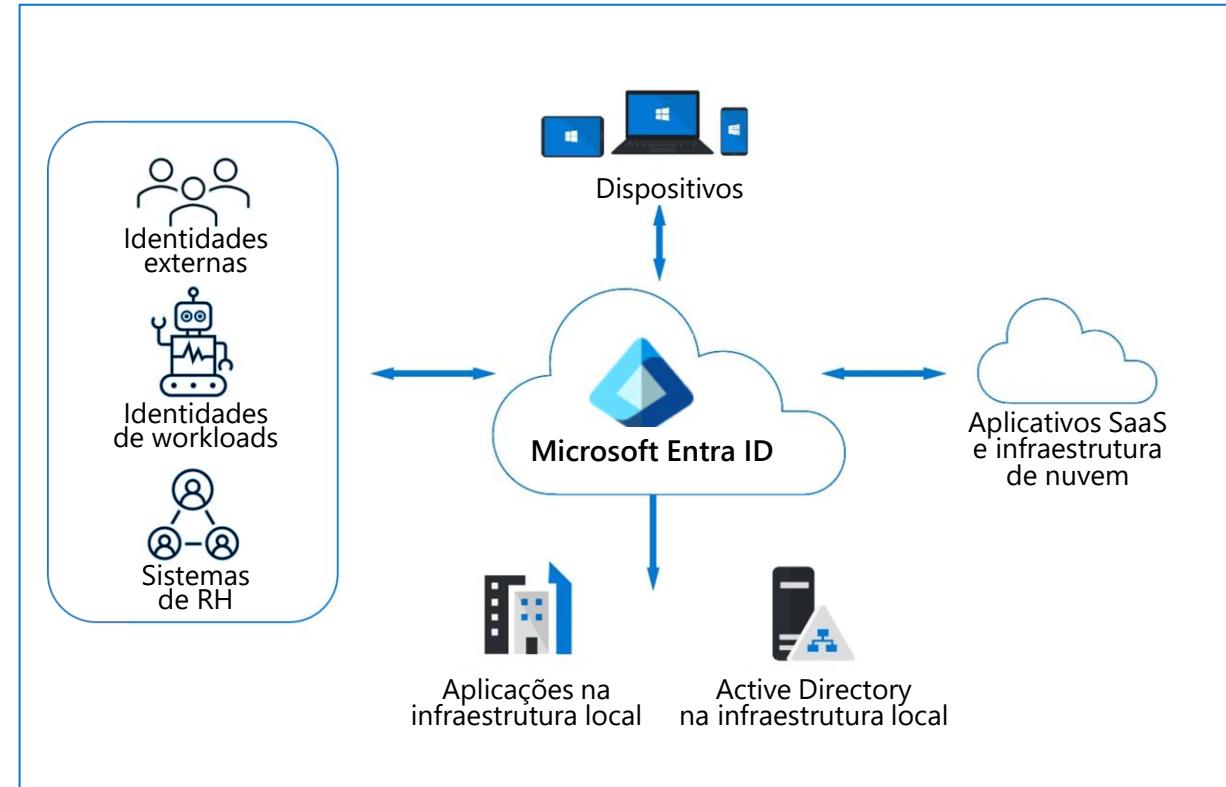


Objetivo de aprendizagem: Descrever os tipos de função e identidade do Microsoft Entra ID

Descrever o Microsoft Entra ID

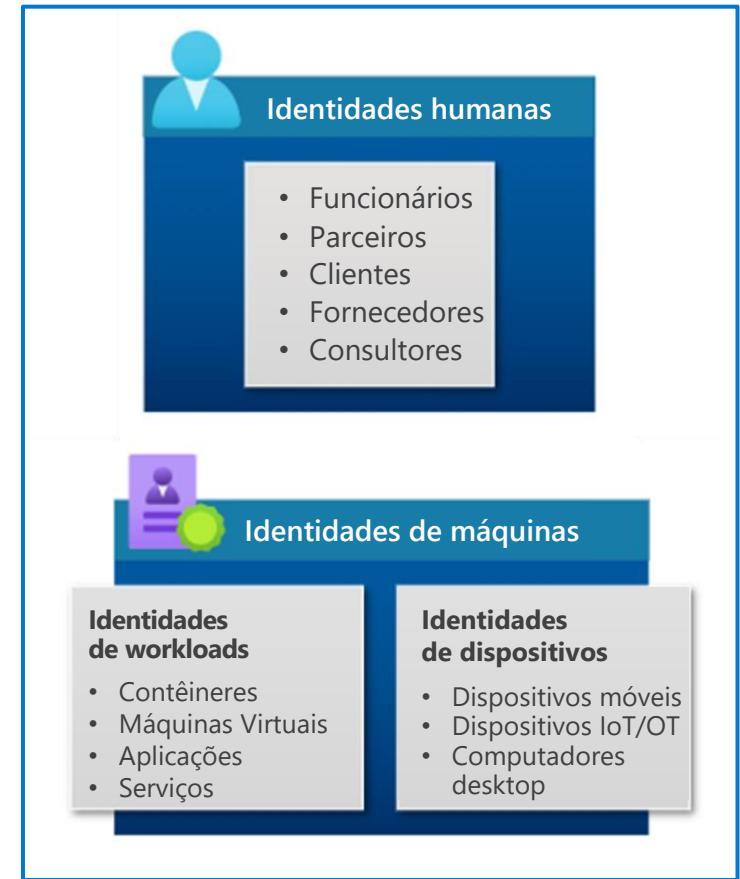
Serviço de gerenciamento de identidades e acesso baseado na nuvem da Microsoft.

- As organizações podem permitir que seus funcionários, convidados e outras pessoas entrem e acessem os recursos de que precisam.
- Fornece um único sistema de identidade para suas aplicações multinuvem e na infraestrutura local.
- Protege as identidades e as credenciais dos usuários para atender aos requisitos de governança de acesso de uma organização.
- Os assinantes dos serviços do Azure, do Microsoft 365 ou do Dynamics 365 automaticamente têm acesso ao Microsoft Entra ID.
- Pontuação de Segurança de Identidade.



Tipos de identidade

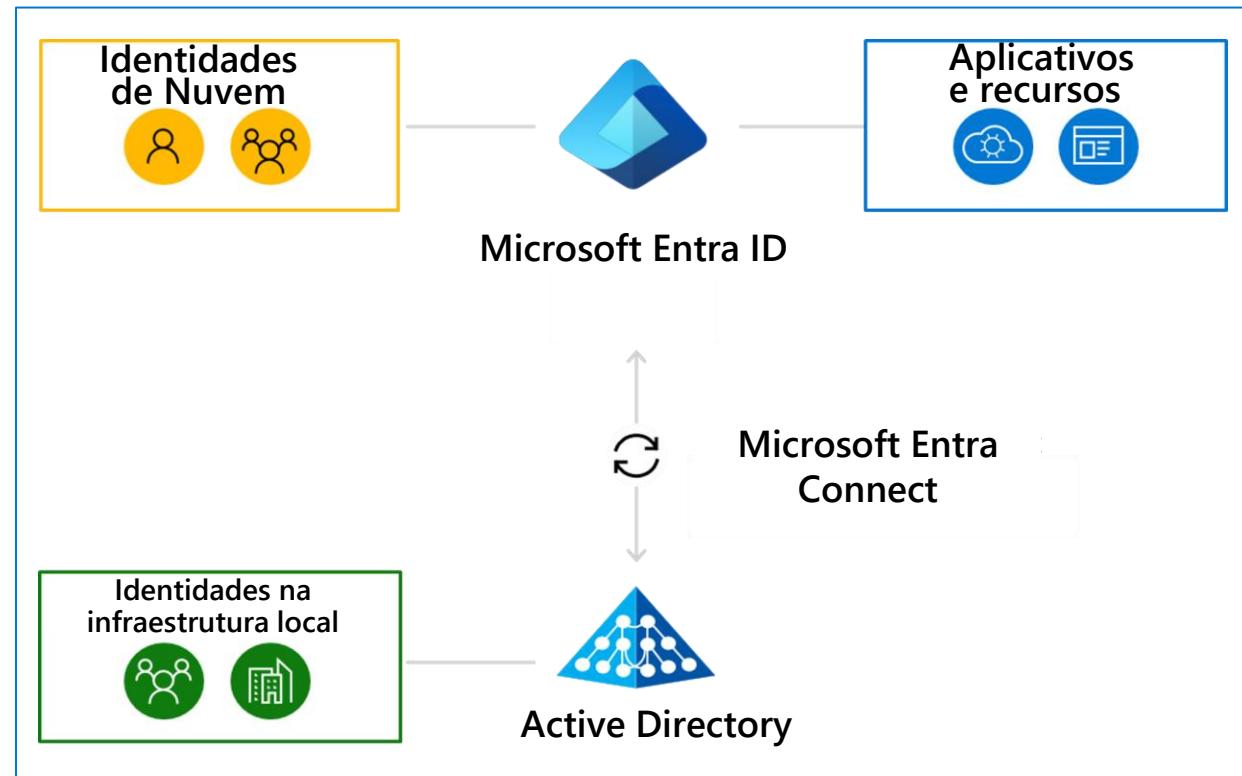
- **Identidades humanas (de usuários)**
 - Usuários internos: funcionários
 - Usuários externos: convidados, parceiros, clientes, fornecedores, consultores e assim por diante.
- **Identidades de workloads:** uma identidade atribuída a uma aplicação ou um serviço.
 - Entidade de serviço: uma identidade para uma aplicação ou um serviço que usa o Microsoft Entra ID para gerenciar funções de identidade e acesso; os desenvolvedores de aplicativos gerenciam as credenciais.
 - Identidades gerenciadas: uma entidade de serviço gerenciada no Microsoft Entra ID que elimina a necessidade de desenvolvedores de aplicativos gerenciarem credenciais.
- **Dispositivos**
 - Microsoft Entra ID registrado: suporte para cenários de BYOD (traga seu próprio dispositivo) ou dispositivos móveis.
 - Ingressado no Microsoft Entra ID: dispositivo ingressado no Microsoft Entra ID por meio de uma conta organizacional (de propriedade da organização).
 - Ingresso híbrido: os dispositivos ingressam no seu Active Directory na infraestrutura local e no Microsoft Entra ID, exigindo que a conta organizacional faça logon.



Identidade híbrida

Uma identidade de usuário comum para autenticação e autorização para recursos na infraestrutura local e na nuvem.

- A identidade híbrida é realizada por meio de:
 - Provisionamento entre diretórios: um usuário já no Active Directory é provisionado para o Microsoft Entra ID.
 - Sincronização: garantir que as informações de identidade de seus usuários e grupos na infraestrutura local correspondam às da nuvem.
- O Microsoft Entra ID Connect é um método para provisionamento e sincronização com o Microsoft Entra ID.



Demonstração

- Configurações de usuário do Microsoft Entra ID



Objetivo de aprendizagem: Descrever os recursos de autenticação do Microsoft Entra ID

Métodos de autenticação do Microsoft Entra

Senhas (autenticação primária)

Autenticação baseada em smartphone

- SMS (autenticação primária e secundária)
- Voz (autenticação secundária)

OATH: padrão para como os códigos de senha de uso único são gerados (autenticação secundária)

- Tokens SW
- Tokens HW

Sem senha (autenticação primária e secundária)

- Windows Hello
- Microsoft Authenticator
- FIDO2
- Certificados (autenticação primária)

Ruim:

Somente senha

123456

admin

quertyuiop

P@ssword2024!

Regular:

Senha e...



SMS



Voice

Melhor:

Senha e...



Notificações por push
do Microsoft
Authenticator



Tokens de software OTP



Hardware Tokens OTP



Melhor:

Sem senhas



Entrada pelo telefone
do Microsoft
Authenticator

O melhor de tudo:

Resistente a phishing



Windows Hello
for Business



Chave de
segurança FIDO2



Autenticação
baseada em
certificado
(multifatorial)



Chave de acesso
no Microsoft
Authenticator (vinculado
ao dispositivo)



Credencial
de plataforma para
macOS

Autenticação multifatorial (MFA)

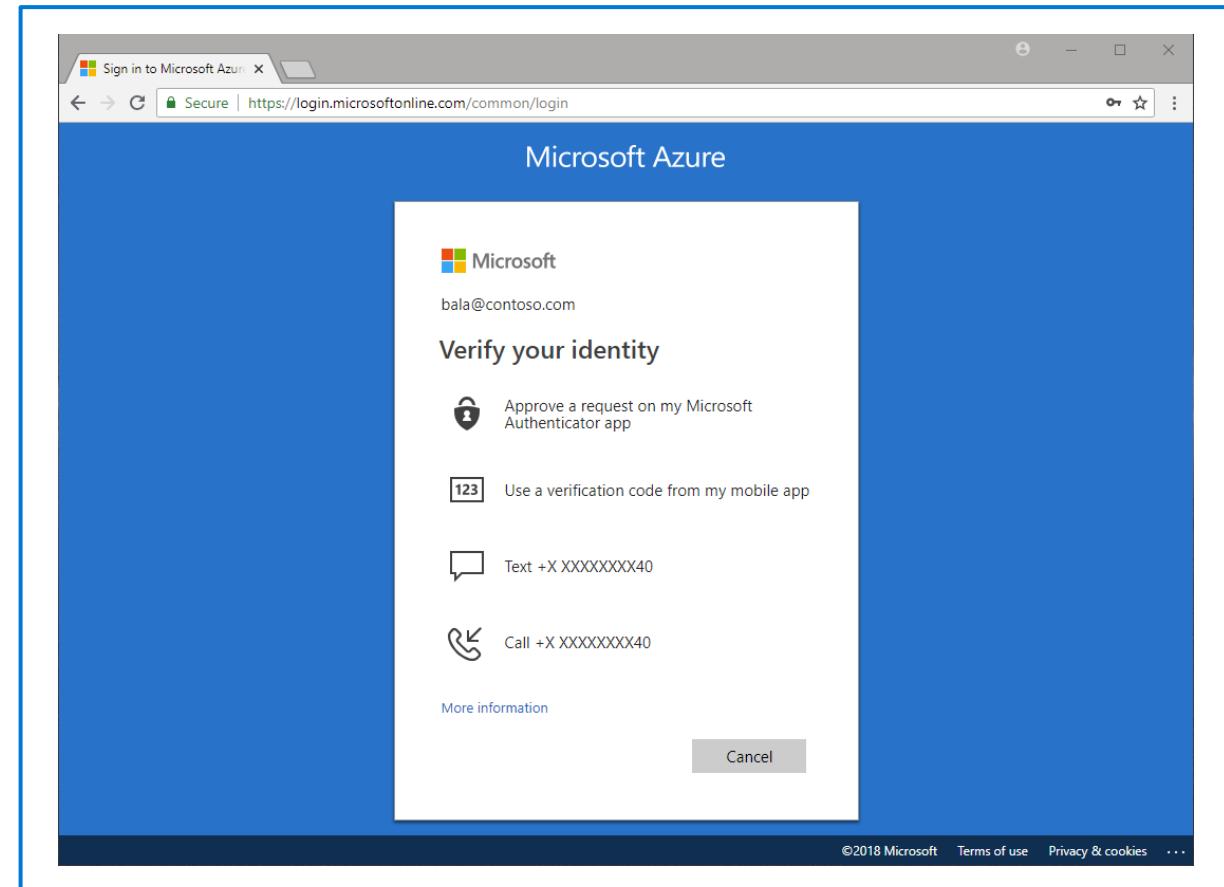
Melhora drasticamente a segurança de uma identidade, embora ainda seja simples para os usuários.

A MFA requer mais de uma forma de verificação:

- Algo que você sabe
- Algo que você tem
- Algo que você é

Padrões de segurança

- Requer que todos os usuários completem a MFA conforme necessário.
- Forçando os administradores a usar a MFA.
- Aplicando MFA para todos os usuários.



Recursos de proteção e gerenciamento de senhas

Reduza o risco de usuários definirem senhas fracas.

- Lista global de senhas proibidas.
- Listas personalizadas de senhas proibidas.
- Proteção contra spray de senha.
- Integra-se a um ambiente na infraestrutura local do Active Directory.

Custom smart lockout

Lockout threshold ⓘ 10

Lockout duration in seconds ⓘ 60

Custom banned passwords

Enforce custom list ⓘ

Yes No

Custom banned password list ⓘ

contoso
fabrikam
tailwind
michigan
wolverine
harbaugh
howard

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ

Yes No

Demonstração

- Métodos de autenticação e MFA



**Objetivo de aprendizagem: Descrever
os recursos de gerenciamento de acesso
do Microsoft Entra**

Acesso Condisional

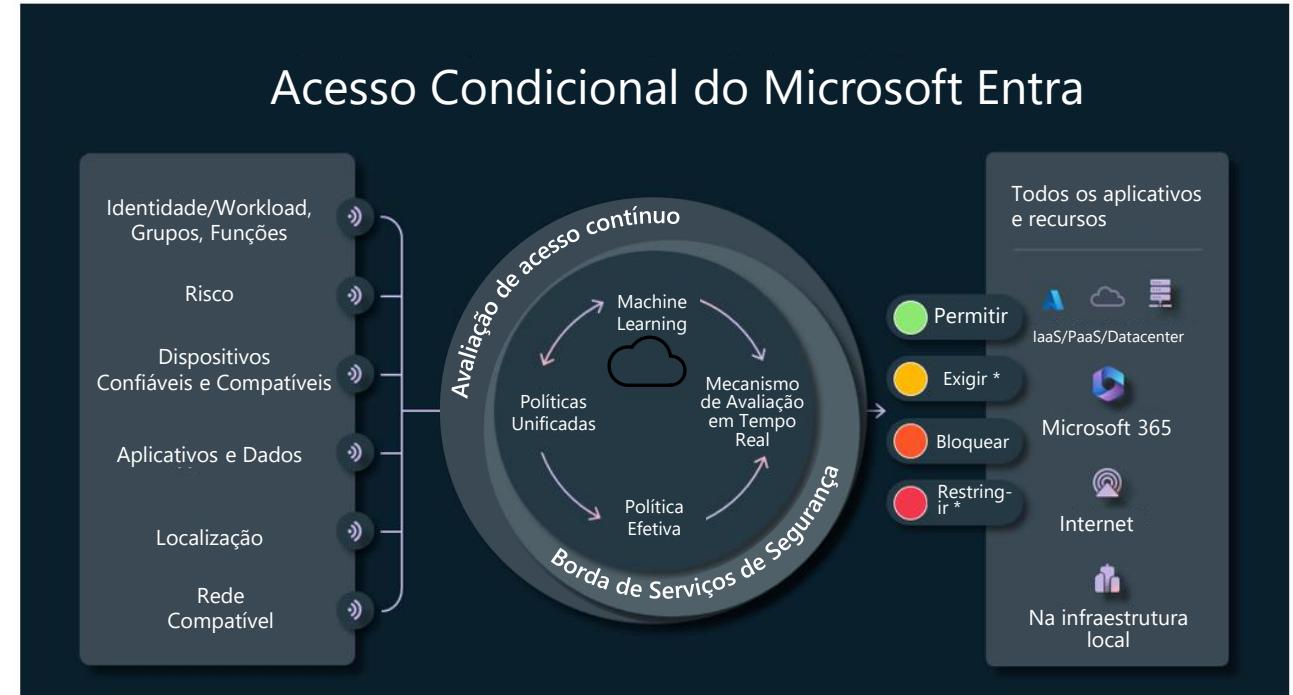
Na sua forma mais simples, as políticas de acesso condicional (CA) são instruções if-then.

As atribuições determinam quais sinais usar:

- Usuários, grupos, identidades de workloads, funções de diretório
- Aplicativos ou ações na nuvem
- Detecção dos riscos de entrada e do usuário
- Dispositivo ou plataforma de dispositivos
- Localização IP
- Mais..

Os controles de acesso determinam como uma política é aplicada:

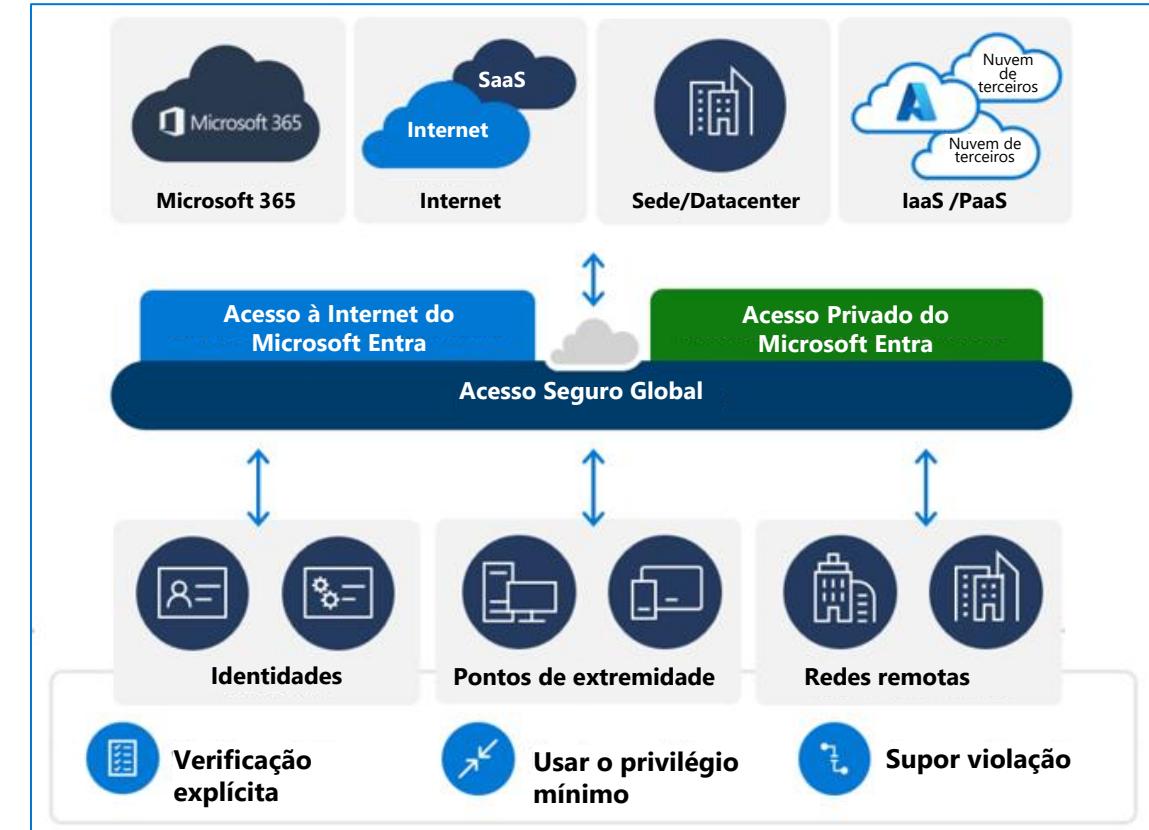
- Bloquear acesso
- Conceder acesso: exija que uma ou mais condições sejam atendidas antes de conceder acesso.
- Controle de sessão: habilite uma experiência limitada.



Acesso seguro global do Microsoft Entra

A GSA converge controles de acesso de rede, identidade e ponto de extremidade de Confiança Zero para proteger o acesso a qualquer aplicativo ou recurso, de qualquer local, dispositivo ou identidade.

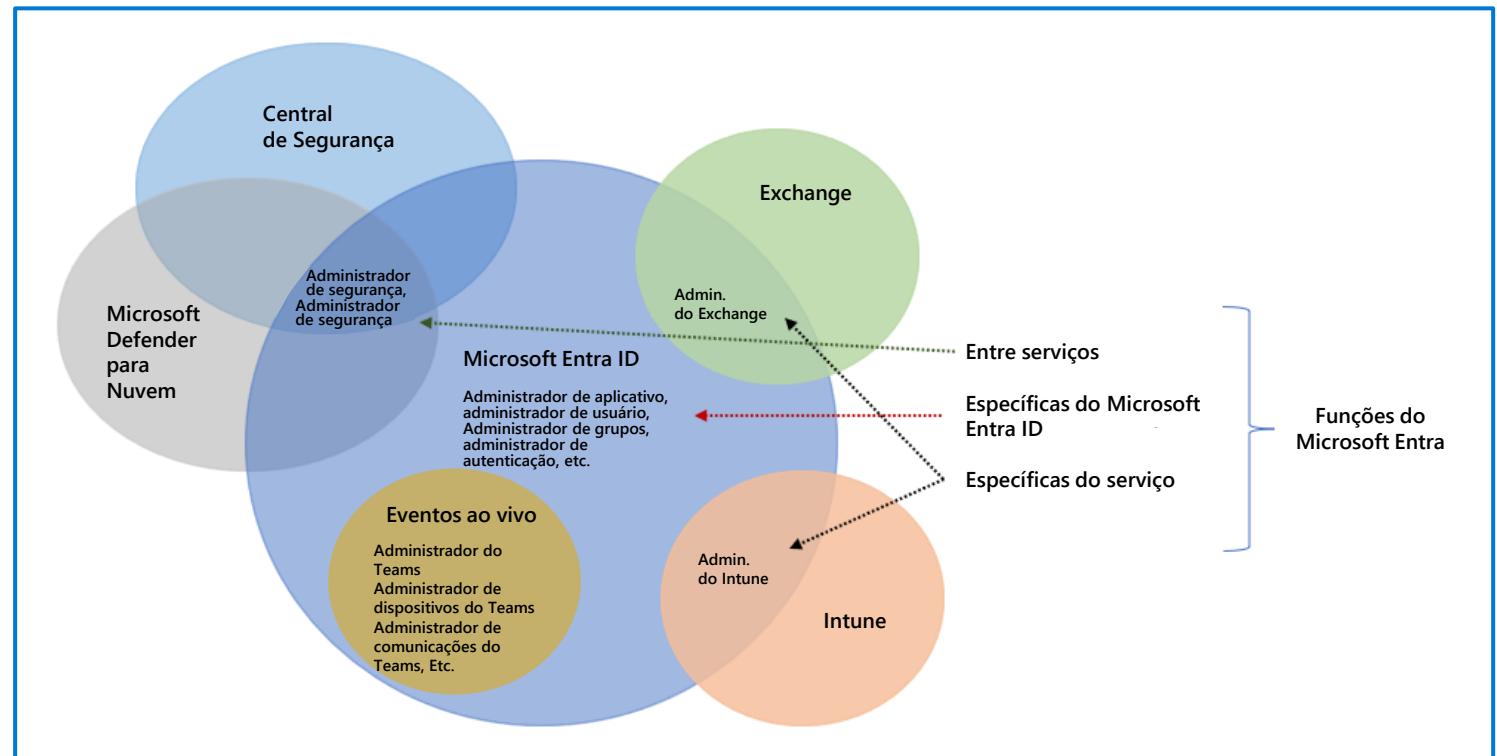
- **O Acesso à Internet do Microsoft Entra** protege o acesso a aplicações SaaS, incluindo serviços de Microsoft e aplicativos públicos de Internet.
- **O Acesso Privado do Microsoft Entra** fornece aos usuários acesso seguro aos seus recursos privados e corporativos.



Funções e controle de acesso baseado em função do Microsoft Entra

Funções do Microsoft Entra controlam permissões para gerenciar recursos do Microsoft Entra.

- Funções internas
- Funções personalizadas
- Categorias de funções do Microsoft Entra:
 - Específicas do Microsoft Entra
 - Específicas do serviço
 - Entre serviços
- Conceda somente o acesso de que os usuários precisam



Demonstração

- Acesso Condicional do Microsoft Entra



Objetivo de aprendizagem: Descrever os recursos de proteção e governança de identidade do Microsoft Entra

Governança de identidade no Microsoft Entra

Certifique-se de que as pessoas certas tenham acesso certo aos recursos certos.

As tarefas da governança de identidade do Microsoft Entra

- Administrar o ciclo de vida da identidade.
- Administrar o ciclo de vida do acesso.
- Proteger o acesso privilegiado para administração.

Ciclo de vida de identidade

- Ingressar: uma nova identidade digital é criada.
- Mover: atualize autorizações de acesso.
- Sair: o acesso pode precisar ser removido.



Análises de acesso

Análises de acesso

- Gerenciar com eficiência as associações de grupo, o acesso a aplicações corporativas e a atribuição de funções.
- Garantir que apenas as pessoas certas tenham acesso aos recursos.
- Usado para revisar e gerenciar o acesso de usuários e convidados.

Avaliações de acesso de vários estágios

- Oferecer suporte a até três estágios de revisão.
- Fluxos de trabalho de suporte para atender aos requisitos de nova certificação e auditoria que exigem vários revisores.
- Reduzir o número de decisões pelas quais cada revisor é responsável.

Contoso

Please review users' access to the Finance Web app in FrickelsoftNET

Sarah Hoelzel, your organization requested that you approve or deny continued access for one or more users to the Finance Web app in the FinanceWeb access review. The review period will end on September 5, 2020.

Hi FinanceWeb team - please review the list of users who can access your FinanceWeb application. Help us remove any unwanted access from users that no longer work with the app. More information:
<https://finweb.contoso.com/access/reviews>

[Start review >](#)

Learn how to [perform an access review](#) and more about [Azure Active Directory access reviews](#).

[Privacy Statement](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Facilitated by



Privileged Identity Management (PIM)

Gerencie, controle e monitore o acesso a recursos importantes em sua organização.



Just in time, fornecendo acesso privilegiado somente quando necessário, e não antes.



Limite de tempo, atribuindo datas de início e término que indicam quando um usuário pode acessar recursos.



Baseado em aprovação, exigindo aprovação específica para ativar privilégios.



Visível, enviando notificações quando as funções privilegiadas forem ativadas.



Auditável, permitindo que um histórico de acesso completo seja baixado.

Proteção de identidade do Microsoft Entra

Detectar

- Categorize o risco em três camadas: baixo, médio e alto.
- Calcule o risco de entrada e o risco do usuário.

Investigar

- Relatório de detecções de riscos
- Relatório de entradas arriscadas
- Relatório de usuários arriscados
- Relatório de identidades de workloads arriscadas

Corrigir

- Correção automatizada
- Correção manual

Exportar

- Exporte dados de detecção de risco para utilitários de terceiros para análise posterior.

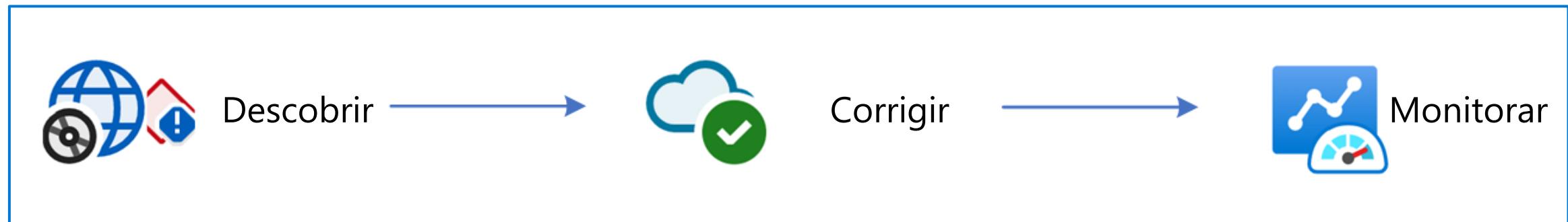
The screenshot shows a detailed view of a risky user in the Microsoft Entra portal. The user is identified as 'Vjekoslav Vlasic' with a User ID of 'abcdefg-xxxx-zzzz-1111-xxxxxxxxxx'. The user has been categorized as 'At risk' with a 'Low' risk level. The last update was on '12/16/2021, 10:25:59 AM'. The interface includes tabs for 'Basic info', 'Recent risky sign-ins', and 'User's sign-ins', along with other navigation options like 'Office location', 'Department', and 'Mobile phone'.

| Risky User Details | |
|--------------------|-----------------------------------|
| User | Vjekoslav Vlasic |
| Roles | Limited admin |
| Username | vvlasic@woodgrove.ms |
| User ID | abcdefg-xxxx-zzzz-1111-xxxxxxxxxx |
| Risk state | At risk |
| Risk level | Low |
| Details | - |
| Risk last updated | 12/16/2021, 10:25:59 AM |
| Office location | |
| Department | |
| Mobile phone | |

Gerenciamento de permissões

Fornece visibilidade e controle abrangentes sobre permissões para qualquer identidade e qualquer recurso no Microsoft Azure, Amazon Web Services (AWS) e Google Cloud Platform (GCP).

- Descobrir: avalie os riscos de permissão analisando a lacuna entre as permissões concedidas e as permissões usadas.
- Corrigir: permissões de tamanho certo com base no uso, conceda permissões sob demanda.
- Monitorar: detecte atividades anômalas com alertas alimentados por aprendizado de máquina e gere relatórios forenses detalhados.



Integração do Microsoft Entra com o Copilot da Segurança da Microsoft

Experiência autônoma:

- Os recursos em experiência autônoma são prompts internos.
- Use a de linguagem natural para criar seus próprios prompts.

Experiência inserida:

- Com suporte no relatório Usuários arriscados.
- Resuma o nível de risco de um usuário, forneça insights e forneça recomendações para mitigação rápida.

MICROSOFT ENTRA

[Explore a summary of a users active risk with Entra ID Protection.](#)

View a detailed summary of a Microsoft Entra ID users risk.

[Explore diagnostic log collection in Microsoft Entra](#)

View settings for diagnostic log collection and streaming of activity logs in Microsoft Entra ID

[Explore Microsoft Entra audit log details](#)

View changes to applications, groups, users, and licenses in Microsoft Entra ID

[Find group details in Microsoft Entra](#)

View Microsoft Entra ID group ownership and membership details

[Find sign-in logs in Microsoft Entra](#)

View Microsoft Entra ID sign-in log details including policy evaluation results, and details on the loc...

[Find user details in Microsoft Entra](#)

View contact information, authentication method registration, and account details for users in Micr...

[Investigate identity risks with Entra ID Protection](#)

View details of Microsoft Entra ID users with high, medium, or low risk of compromise

**Descrever as recursos das soluções
da segurança da Microsoft (parte 1 de 3)**

Objetivos de aprendizagem

- Descrever o Copilot da Segurança da Microsoft
- Descrever os principais serviços de segurança de infraestrutura no Azure

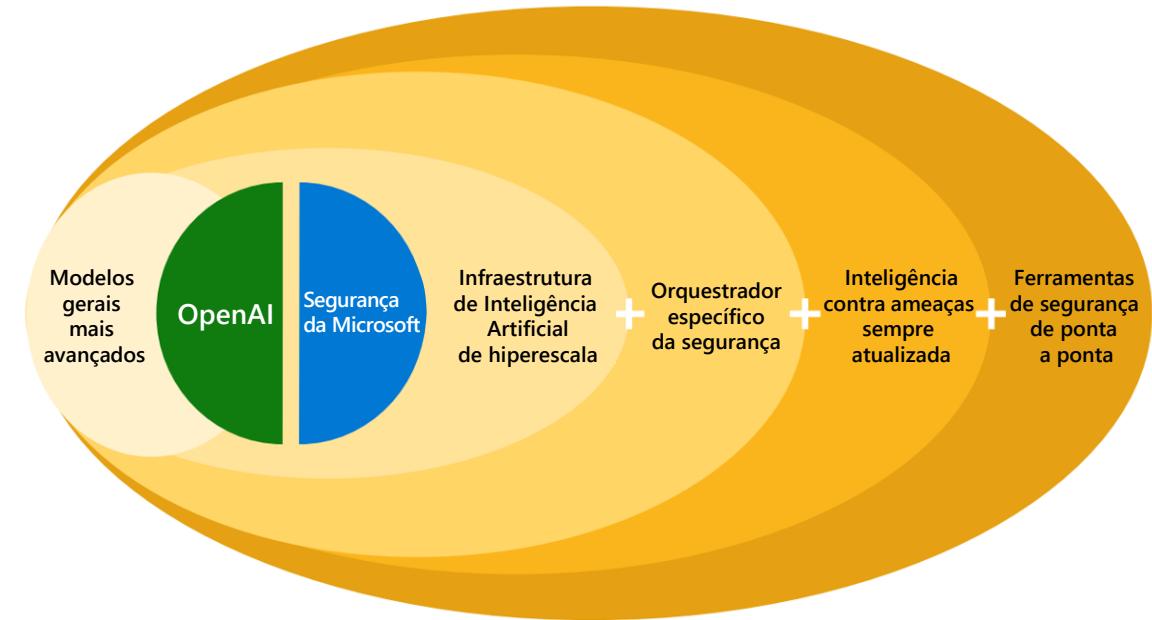


Objetivo de aprendizagem: Descrever
o Copilot da Segurança da Microsoft

Descrever o Copilot da Segurança da Microsoft – o que é isso?

Uma ferramenta de análise de segurança baseada na nuvem com IA que permite que os analistas respondam a ameaças rapidamente, processem sinais na velocidade da máquina e avaliem a exposição ao risco mais rapidamente do que nunca.

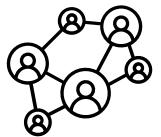
- O Copilot combina LLMs eficientes com um modelo específico de segurança da Microsoft.
- O Copilot integra-se a fontes da Microsoft e que não são da Microsoft.
- O Copilot aprende na velocidade da máquina para ajudar os analistas a identificar e responder às ameaças que surgem.
- Dados corporativos são protegidos por controles de conformidade e segurança corporativos abrangentes.



Descreva o Copilot da Segurança da Microsoft (casos de uso)



Resumo do incidente. Envie alertas de segurança complexos em resumos acionáveis concisos.



Análise de impacto. Avalie o possível impacto de incidentes de segurança para permitir tempos de resposta mais rápidos e tomadas de decisões simplificadas.



Engenharia reversa de scripts. Analise scripts complexos de linha de comando e traduza-os em linguagem natural com explicações claras de ações.

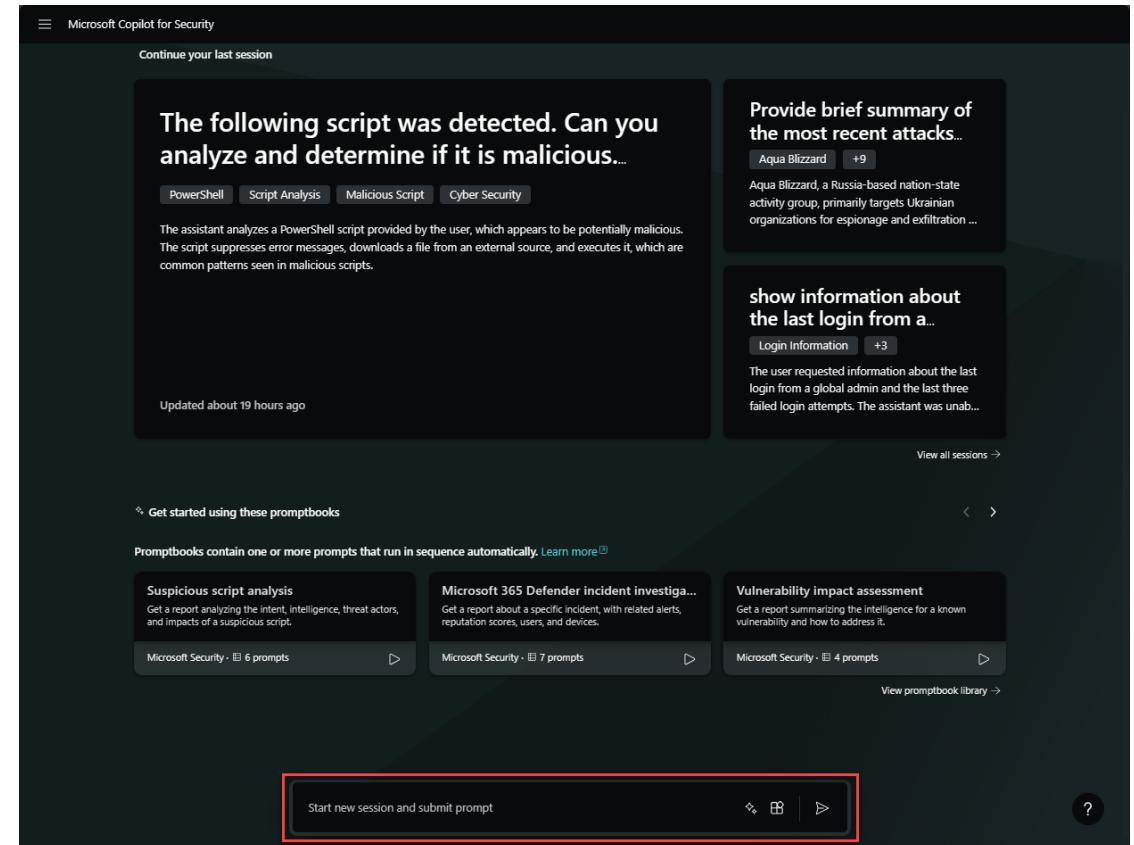


Respostas guiadas. Orientações passo a passo acionáveis para resposta a incidentes, incluindo instruções para triagem, investigação, contenção e correção.

Descreva a experiência autônoma do Copilot da Segurança da Microsoft

Experimente o Copilot por meio de um site dedicado (experiência autônoma).

Os usuários fazem solicitações em linguagem natural e recebem respostas como texto, imagens ou documentos.



Descreva o Copilot da Segurança da Microsoft – Experiência incorporada

Alguns produtos da Microsoft incorporam o Copilot diretamente em sua interface do usuário.

The screenshot shows the Microsoft 365 Defender interface for 'contosohotels.com'. The left sidebar includes sections like Home, Incidents & alerts, Hunting (Advanced hunting selected), Actions & submissions, Threat intelligence, Learning hub, Trials, Partner catalog, Exposure management, Overview, Attack surface, Exposure insights, Assets, and Devices. The main area is titled 'Advanced hunting' and contains a 'Query' section with a Kusto query:

```
1 let logonAttempts = DeviceLogonEvents  
2 | where ActionType == "LogonAttempted"  
3 | project Timestamp, DeviceId, AccountDomain;  
4 let credentialTheftEvents = DeviceEvents  
5 | where ActionType in ("AsrlsassCredentialTheftAudited", "AsrlsassCred  
6 | project Timestamp, DeviceId, InitiatingProcessAccountDomain;  
7 logonAttempts  
8 | join kind=inner credentialTheftEvents on $left.DeviceId == $right.De  
9 | summarize count() by AccountDomain  
10 | order by count_ desc  
11
```

Below the query, it says 'No results found in the specified time frame.' To the right, there's a 'Security Copilot' pane with a red border, showing generated queries and an 'Ask a question to generate a query' input field at the bottom.

Descreva a terminologia do Copilot da Segurança da Microsoft

- **Sessão:** uma conversa particular no Copilot da Segurança da Microsoft.
- **Prompt:** uma declaração de usuário ou uma pergunta específica dentro de uma sessão.
- **Recurso:** uma função que o Copilot da Segurança da Microsoft usa para resolver parte de um problema.
- **Plug-in:** uma coleção de funções de um recurso específico, como o Microsoft Intune.
- **Orquestrador:** usado para compor habilidades em conjunto, para responder à solicitação de um usuário.



A barra de prompts, usada para inserir prompts.

Exemplo: plug-ins e recursos

Manage sources

Plugins Manage plugins
Turn on or create your own plugins to give Copilot access to the security services and websites you use. [Learn more](#)

All (60) On (11) Off (49)

Microsoft ⚡

- Azure Firewall** Preview
Intrusion Detection and Prevention System (IDPS) signature analysis and fleet-wide IDPS attack investigation
- Azure Web Application Firewall** Preview
SQL injection block summaries, XSS block summaries, top WAF rules summaries and top malicious IP summaries
- Microsoft Defender External Attack Surface Management**
Attack surfaces, vulnerable assets, and attack surface insights

Show 11 more ▾

← Search

SYSTEM CAPABILITIES

Capabilities are based on the plugins you have set up.

AZURE FIREWALL Preview

- Get details on an IDPS signature**
Expand on the description of an IDPS signature in the Azure Firewall logs.
- Get top IDPS signature hits**
Retrieve the top IDPS signature hits for an Azure Firewall.
- Search across firewalls for an IDPS signature**
Look for a given IDPS signature across your tenant, subscription, or resource group.
- Secure your environment using IDPS**
Generate recommendations to secure your environment using Azure Firewall's IDPS feature.

Descreva como o Copilot da Segurança da Microsoft processa solicitações de prompt



Descreva os elementos de um prompt eficaz

Meta

Quais são as informações específicas relacionadas à segurança de que você precisa?



"Dê-me informações sobre o incidente 18718..."

Contexto

Por que você precisa delas e como você usará as informações?

"... para um relatório que eu possa enviar para o meu gerente".

Expectativas

A qual formato ou público-alvo você deseja ajustar a resposta?

"Compile as informações em uma lista, com um breve resumo".



Origem

Existe um plug-in, informações conhecidas ou fonte de dados que o Copilot da Segurança deve usar?



"Procure incidentes do Defender".

Habilite o Copilot da Segurança

1. Provisionamento da capacidade do Copilot
 - i. O Copilot da Segurança da Microsoft é vendido como uma oferta de consumo.
 - ii. Provisione unidades de computação de segurança (SCUs), o poder de computação usado para executar o Copilot.
2. Configuração do ambiente padrão
 - i. Capacidade de SCU de alocação.
 - ii. Defina a localização geográfica para o armazenamento de dados.
 - iii. Configure as opções de compartilhamento de dados.
3. Atribuição de permissões

Home > Microsoft Copilot for Security compute capacities >
Set up your Copilot capacity ...

Basics Review + Create

This capacity will provide the computing power that drives the Microsoft Copilot for Security experience.

Project Details

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Capacity details

Name your capacity and select a location

Capacity name * ⓘ Enter a name
This name must be unique and contain only lowercase letters and numbers with no spaces.

Prompt evaluation location * ⓘ United States (US)

If this location is busy, allow Copilot to evaluate prompts anywhere in the world (recommended for optimal performance).

Capacity region ⓘ US East

Security compute units

Security compute units provide the computing power that drives the Security Copilot experience (\$4 per unit). Read more about [security_capacity_units](#) and the recommended number based on your organization's size and probable usage.

Security compute units per hour * ⓘ 1
Estimated monthly cost \$2880/month

I acknowledge that I have read, understood, and agreed to the [Terms and Conditions](#)

[Previous](#) [Next](#) **Review + create**

Demonstração

- Copilot da Segurança da Microsoft – explore a experiência autônoma.

Objetivo de aprendizagem: Descrever os principais serviços de segurança de infraestrutura no Azure

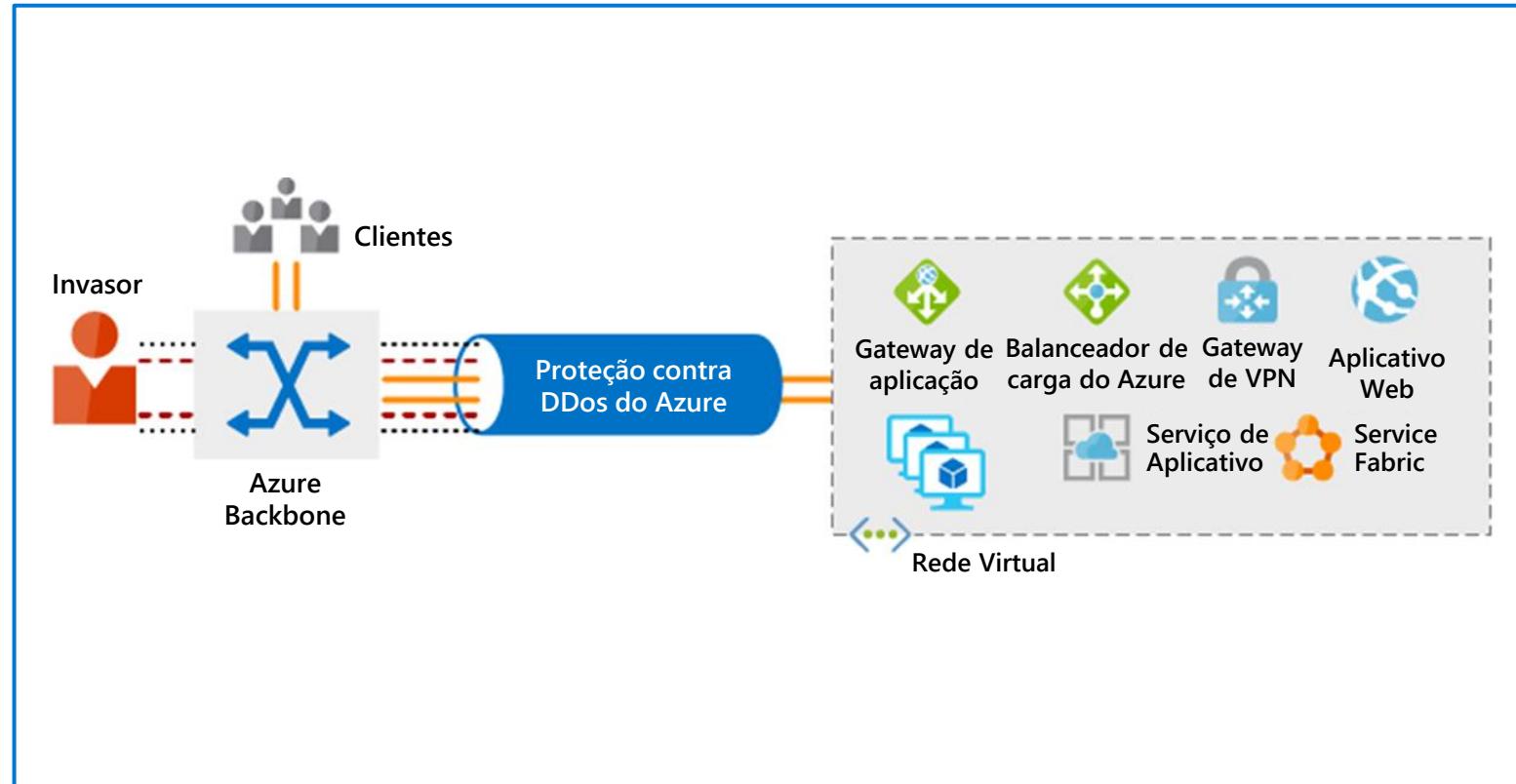
Proteção contra Negação de Serviço Distribuído (DDoS) do Azure

Negação de serviço distribuído (DDoS)

- Ataques que tornam os recursos sem resposta.

Proteção contra DDoS do Azure

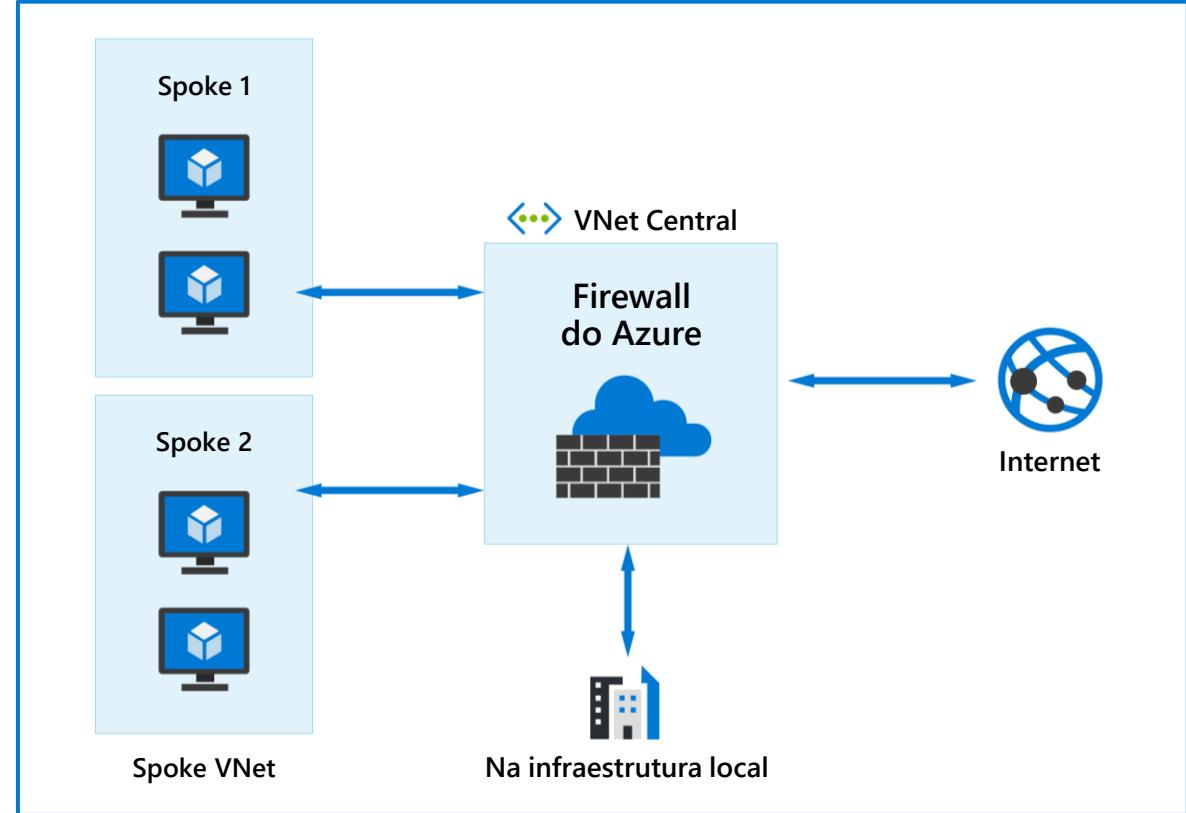
- Analisa o tráfego de rede e descarta qualquer coisa que pareça um ataque DDoS.
- Monitoramento de tráfego Always-on.
- Ajuste adaptável em tempo real.
- Telemetria, monitoramento e alertas de proteção contra DDoS.



Firewall do Azure

O Firewall do Azure protege seus recursos de Rede Virtual do Azure (VNet) contra invasores.

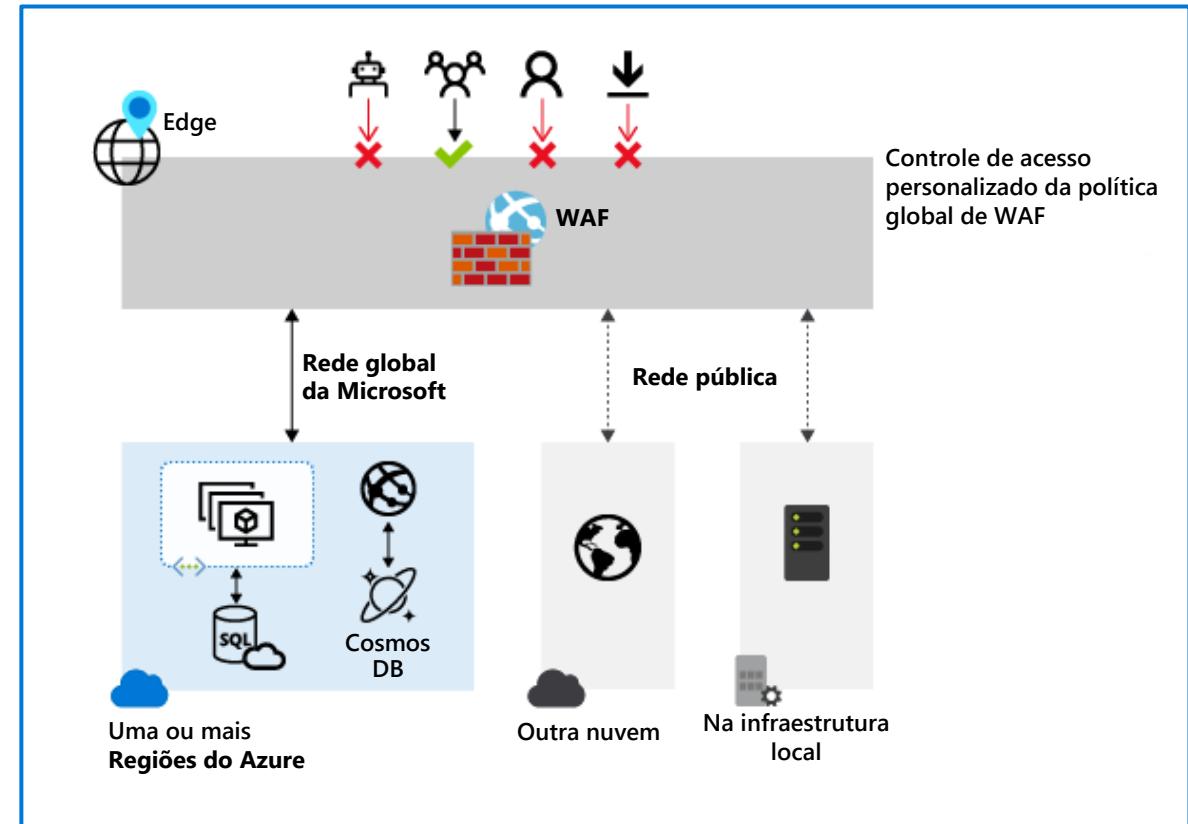
- Crie regras para permitir ou negar a filtragem de rede.
- Use o feed da Informações sobre ameaças da Microsoft para alertar ou filtrar o tráfego de/para domínios e endereços IP mal-intencionados conhecidos.
- Todos os endereços IP de tráfego de rede virtual de saída são traduzidos para o IP público do Firewall do Azure para tornar mais difícil para os invasores visarem dispositivos de rede internos.
- Integração com o Microsoft Copilot para Segurança
- E muito mais...



WAF (Firewall de Aplicativo Web)

Proteção centralizada de suas aplicações Web contra explorações e vulnerabilidades comuns.

- Proteção contra ameaças e invasões.
- Protege aplicações Web contra ataques de DDoS.
- Aplicação de patches de uma vulnerabilidade conhecida em um só lugar.
- Integração com o Microsoft Copilot para Segurança
- E muito mais..



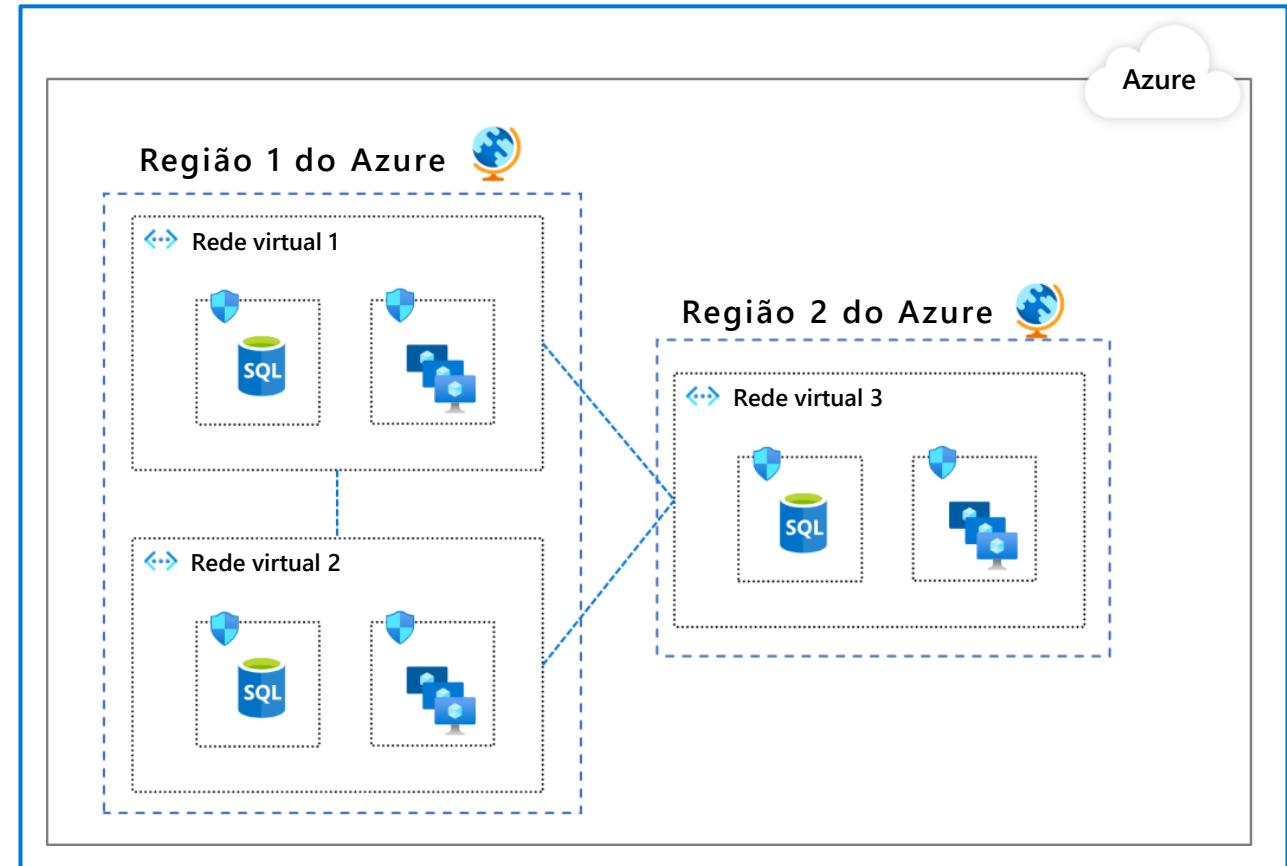
Segmentação de rede e Rede Virtual Azure (VNet)

Motivos para a segmentação da rede

- A capacidade de agrupar ativos relacionados.
- Isolamento de recursos.
- Políticas de governança definidas pela organização.

Rede Virtual do Azure (VNet)

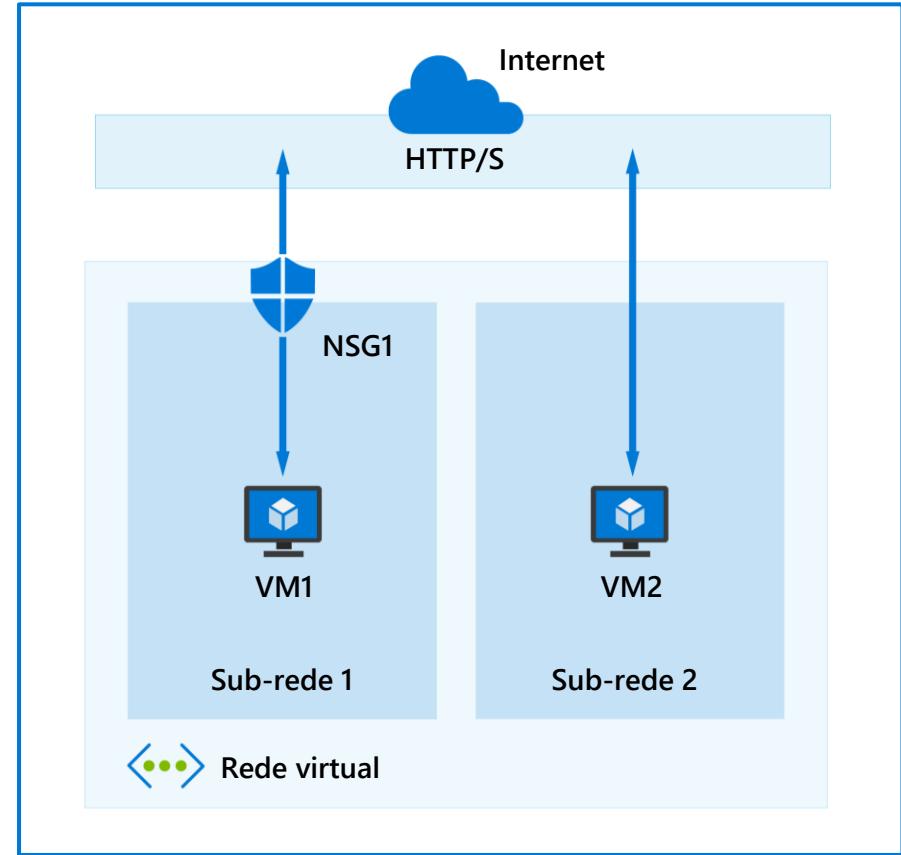
- Contenção de recursos no nível de rede, sem tráfego permitido por meio de VNets ou de entrada para VNet.
- A comunicação precisa ser explicitamente provisionada.
- Controle como os recursos em uma VNet se comunicam com outros recursos, a Internet e redes na infraestrutura local.



Grupo de segurança de rede do Azure (NSGs)

Filtre o tráfego de rede entre os recursos do Azure em uma rede virtual do Azure.

- Um NSG é composto por regras de segurança de entrada e saída que permitem ou negam o tráfego.
- Um NSG pode conter muitas regras, as regras são processadas com base em sua prioridade atribuída.
- Quando um NSG é criado, ele inclui regras padrão de entrada e saída.
- Você não pode remover as regras padrão, mas pode substituí-las criando novas regras com prioridades mais altas.



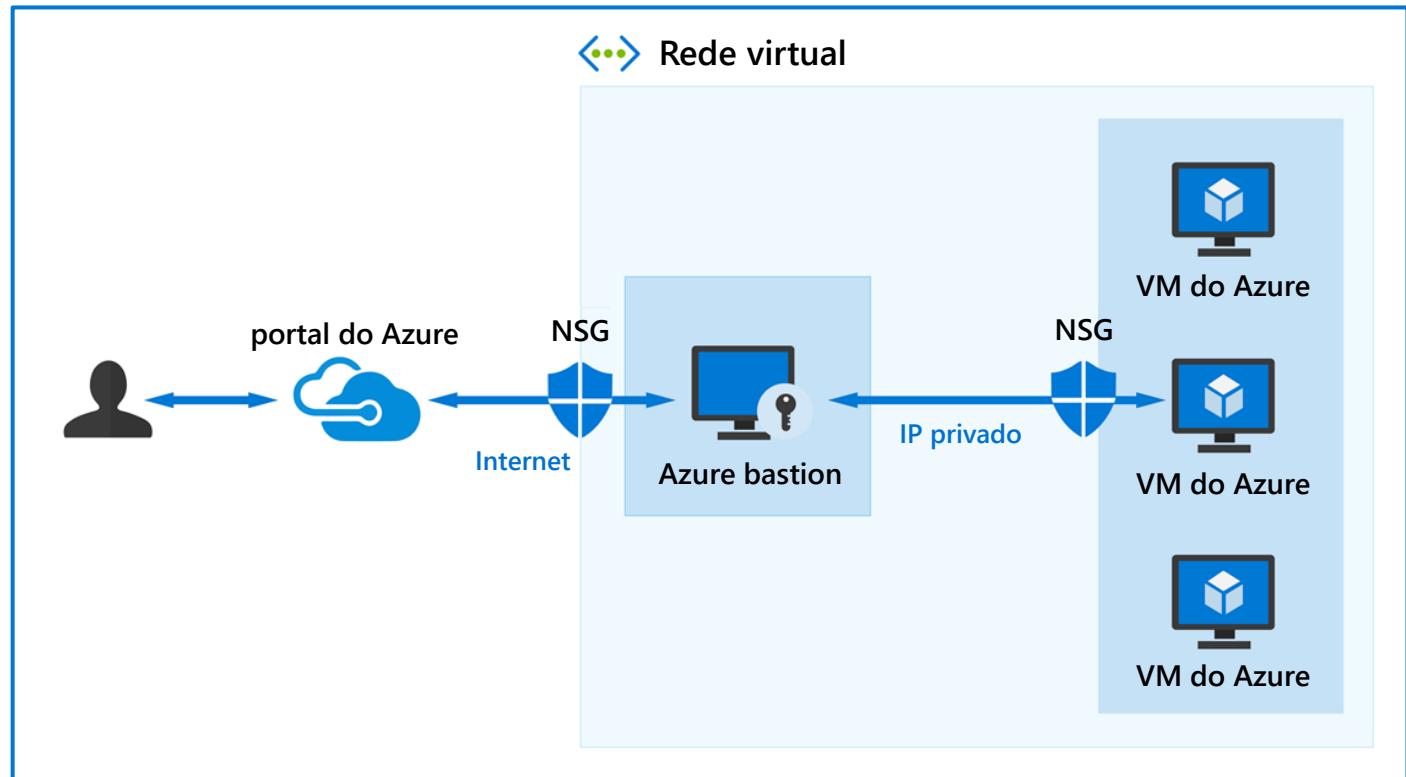
Demonstração

- Grupo de segurança de rede do Azure (NSGs)

Azure Bastion

O Azure Bastion oferece conectividade segura às suas máquinas virtuais (VMs) do portal do Azure.

- Remote Desktop Protocol (RDP) e Secure Shell (SSH) diretamente no portal do Azure.
- Atravesse os firewalls corporativos com segurança.
- Nenhum IP público é necessário em uma VM do Azure.
- Não é necessário gerenciar grupos de segurança de rede (NSGs).
- Proteções contra digitalização de porta.
- Protege contra explorações de dia zero.

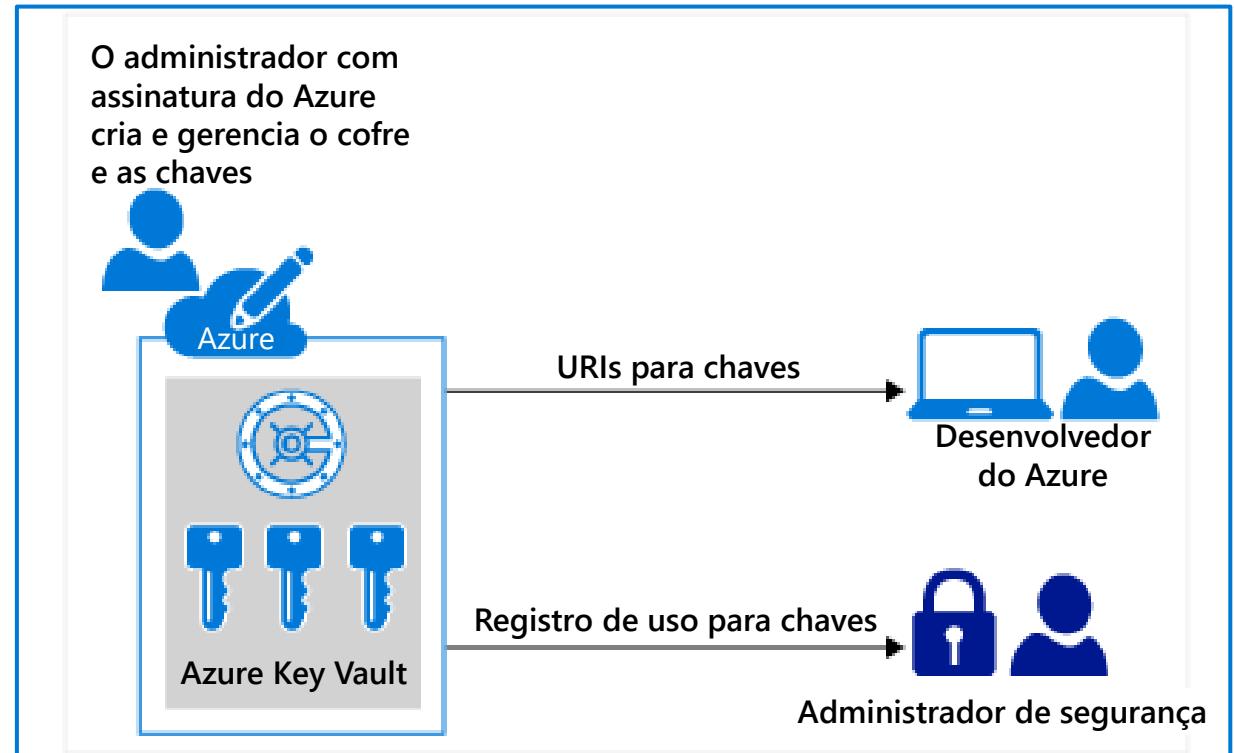


Azure Key Vault

Um serviço em nuvem para armazenar e acessar segredos com segurança, como chaves de API, senhas, certificados ou chaves criptográficas.

Benefícios do Key Vault

- Centralize os segredos da aplicação.
- Armazene segredos e chaves com segurança.
- Monitore o acesso e o uso.
- Administração simplificada de segredos da aplicação.
- Duas camadas:
 - Standard: criptografia baseada em software.
 - Premium: chaves protegidas do módulo de segurança de hardware (HSM).



**Descrever os recursos das soluções da
segurança da Microsoft (parte 2 de 3)**

Objetivos de aprendizagem

- Descrever os recursos de gerenciamento de segurança no Azure
- Descrever os recursos do Microsoft Sentinel

Objetivo de aprendizagem: Descrever os recursos de gerenciamento de segurança no Azure

Microsoft Defender para Nuvem

Uma plataforma de proteção de aplicações nativa da nuvem (CNAPP) com um conjunto de medidas e práticas de segurança projetadas para proteger aplicativos baseados em nuvem contra diversas ameaças e vulnerabilidades cibernéticas.

Gerenciamento de posturas de segurança na nuvem (CSPM)

Apresenta as medidas que você pode tomar para evitar violações.

Plataforma de proteção de workload da nuvem (CWPP)

Oferece proteções específicas para servidores, contêineres, armazenamento, bancos de dados e outros workloads.

Operações de segurança de desenvolvimento (DevSecOps)

Unifica o gerenciamento de segurança no nível do código em ambientes multinuvem e de vários pipelines.



Como as políticas e iniciativas de segurança melhoram a postura de segurança na nuvem

Iniciativas de segurança

- Uma coleção de políticas.
- Atribuído a recursos, assinaturas e muito mais.

Benchmark da segurança na nuvem da Microsoft (MCSB)

- Iniciativa de segurança padrão no Defender para Nuvem.
- Fornece práticas recomendadas e recomendações para melhorar a segurança de workloads, dados e serviços no Azure e em outras nuvens.

Microsoft Defender para Nuvem

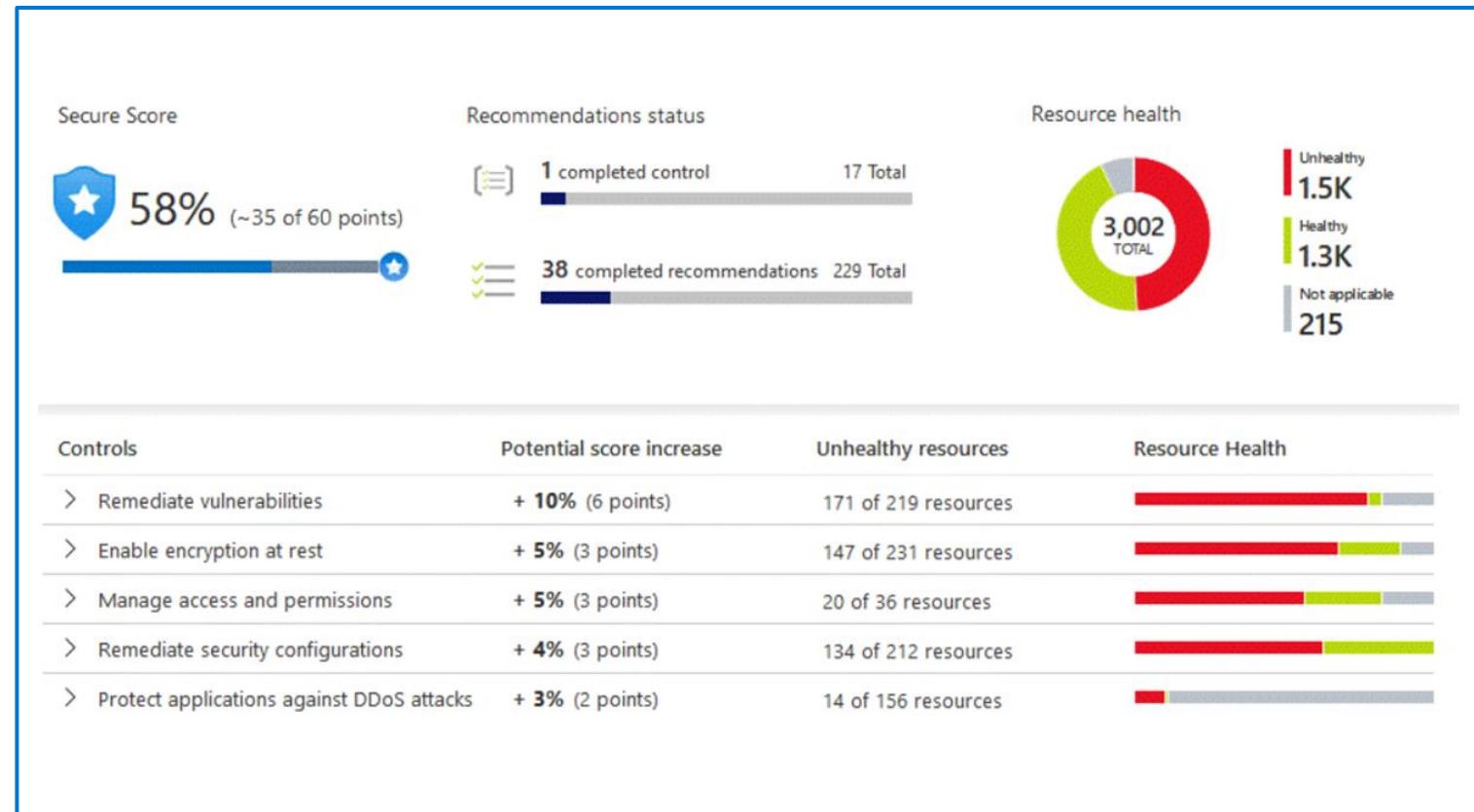
- Avalia continuamente seu ambiente em relação ao MCSB e outras iniciativas de segurança.

The screenshot shows the Microsoft Defender for Cloud Regulatory Compliance dashboard. On the left, there's a sidebar with navigation links like Home, Microsoft Defender for Cloud, General, Overview, Getting started, Recommendations, Security alerts, Inventory, Cloud Security Explorer (Preview), Workbooks, Community, Diagnose and solve problems, Cloud Security, Security posture, Regulatory compliance, Workload protections, Firewall Manager, DevOps Security (Preview), Management, Environment settings, Security solutions, and Workflow automation. The main area has a header "Microsoft Defender for Cloud | Regulatory compliance" and a sub-header "Showing subscription 'Azure Pass - Sponsorship'". It features a search bar and several buttons: Download report, Manage compliance policies, Open query, Compliance over time workbook, Audit reports, and Compliance offerings. A message says, "You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above." Below this is a section titled "Microsoft cloud security benchmark (preview)" with a progress bar showing "48 of 59 passed controls". To the right is a section titled "Lowest compliance regulatory standards" with three cards: SOC TSP (13/13), PCI DSS 3.2.1 (43/43), and ISO 27001 (20/20). At the bottom, there's a survey question "Is the regulatory compliance experience clear to you?", a "Microsoft cloud security benchmark" link (which is highlighted with a red box), and a note about the benchmark not being a guarantee of compliance. There are also sections for "Audit reports" and "Expand all compliance controls".

Gerenciamento de posturas de segurança na nuvem (CSPM)

Visibilidade e recomendações

- Avalia continuamente seus recursos, assinaturas e organização para verificar se há problemas de segurança.
- Agrega todas as descobertas em uma única classificação de segurança.
- Faz recomendações de reforço sobre quaisquer configurações incorretas e pontos fracos de segurança identificados.
- Fornece visibilidade e recomendações em seu ambiente multinuvem.
- Insere os recursos do Copilot da Segurança da Microsoft na página de recomendações.



Plataforma de proteção de workload da nuvem (CWPP)

Os planos CWPP oferecem recursos de segurança aprimorados para seus workloads.

- Detecção e resposta de pontos de extremidade
- Verificação de vulnerabilidades
- Segurança multinuvem
- Segurança híbrida
- Alertas de proteção contra ameaças
- Controles de acesso e aplicações

 Enable the enhanced security features of Microsoft Defender for Cloud. [Learn more >](#)

| Enhanced security off | Enable all Microsoft Defender for Cloud plans |
|--|--|
| ✓ Continuous assessment and security recommendations | ✓ Continuous assessment and security recommendations |
| ✓ Secure score | ✓ Secure score |
| ✗ Just in time VM Access | ✓ Just in time VM Access |
| ✗ Adaptive application controls and network hardening | ✓ Adaptive application controls and network hardening |
| ✗ Regulatory compliance dashboard and reports | ✓ Regulatory compliance dashboard and reports |
| ✗ Threat protection for Azure VMs and non-Azure servers (including Server EDR) | ✓ Threat protection for Azure VMs and non-Azure servers (including Server EDR) |
| ✗ Threat protection for supported PaaS services | ✓ Threat protection for supported PaaS services |

Operações de segurança de desenvolvimento (DevSecOps)

Capacita as equipes de segurança para gerenciar a segurança das operações de desenvolvimento (DevOps) em ambientes de vários pipelines.

- Visibilidade unificada da postura de segurança de DevOps.
- Fortaleça as configurações dos recursos da nuvem no ciclo de vida de desenvolvimento.
- Priorize a correção de problemas críticos no código.



Demonstração

- Microsoft Defender para Nuvem



Objetivo de aprendizagem: Descrever os recursos do Microsoft Sentinel

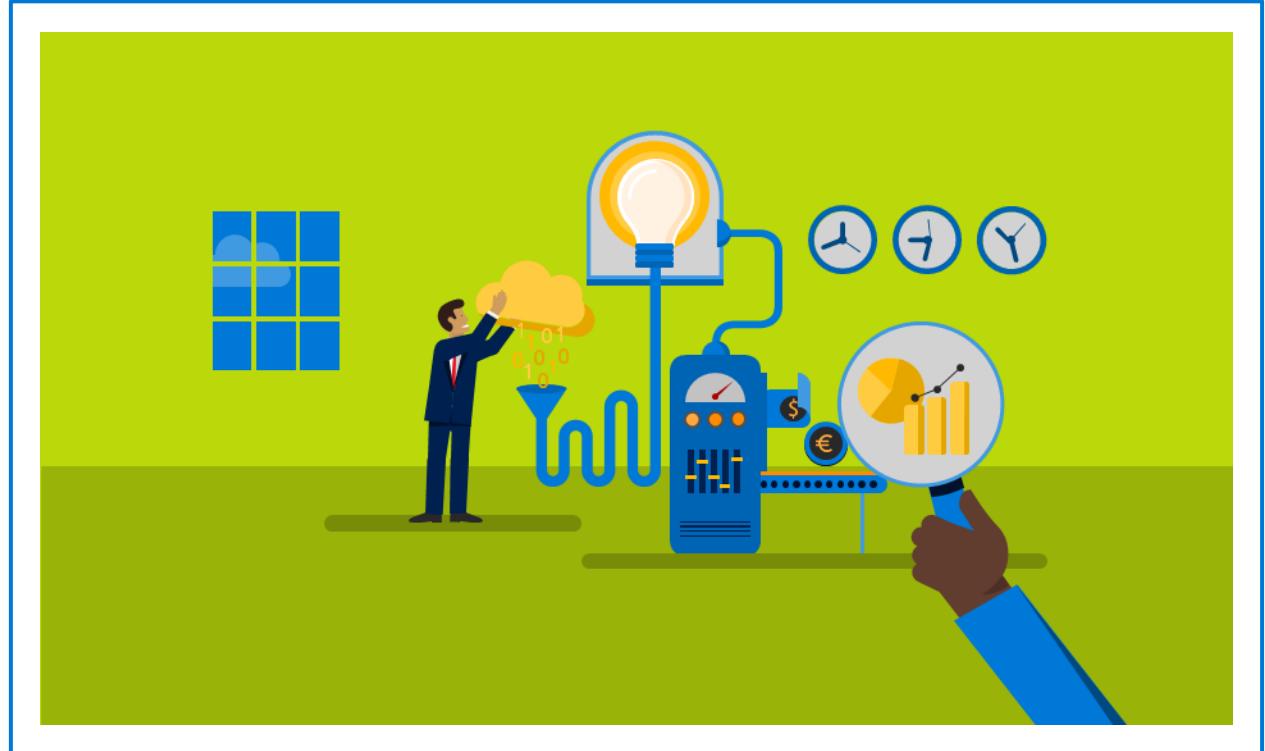
SIEM e SOAR

Gerenciamento de incidentes e eventos de segurança (SIEM)

- Coleta dados de toda a propriedade digital.
- Analisa e procura correlações ou anomalias.
- Gera alertas e incidentes.

Orquestração, automação e resposta de segurança (SOAR)

- Recebe alertas de várias fontes, como sistemas SIEM.
- Aciona processos e fluxos de trabalho automatizados orientados por ação.
- Executa tarefas de segurança que mitigam o problema.



Detecção e mitigação de ameaças do Microsoft Sentinel

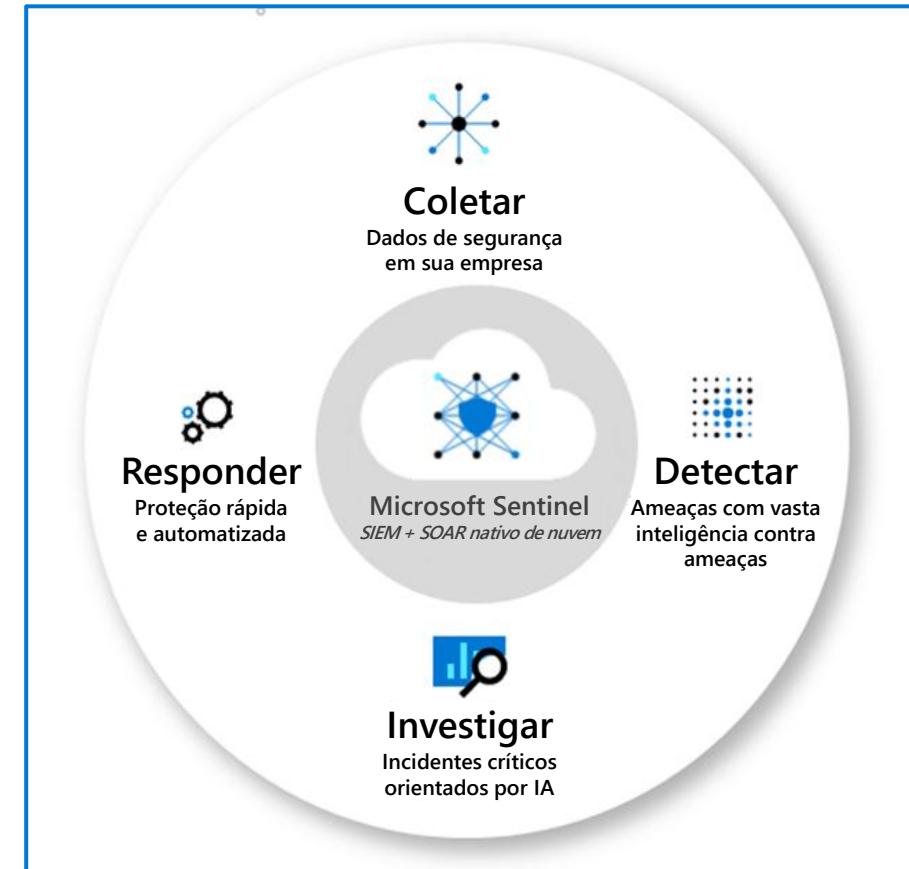
Colete dados em escala de nuvem de todos os usuários, dispositivos, aplicações e infraestrutura, tanto na infraestrutura local quanto em várias nuvens.

Detecte ameaças previamente descobertas e minimize falsos positivos usando análises e inteligência contra ameaças incomparáveis.

Investigue ameaças com IA e buscar proativamente atividades suspeitas em grande escala, explorando décadas de trabalho de segurança cibernética da Microsoft.

Responda rapidamente a incidentes com orquestração e automação integradas de segurança comum.

O Microsoft Sentinel agora pode ser acessado do portal do Microsoft Defender, que oferece a plataforma de operações de segurança unificada da Microsoft.



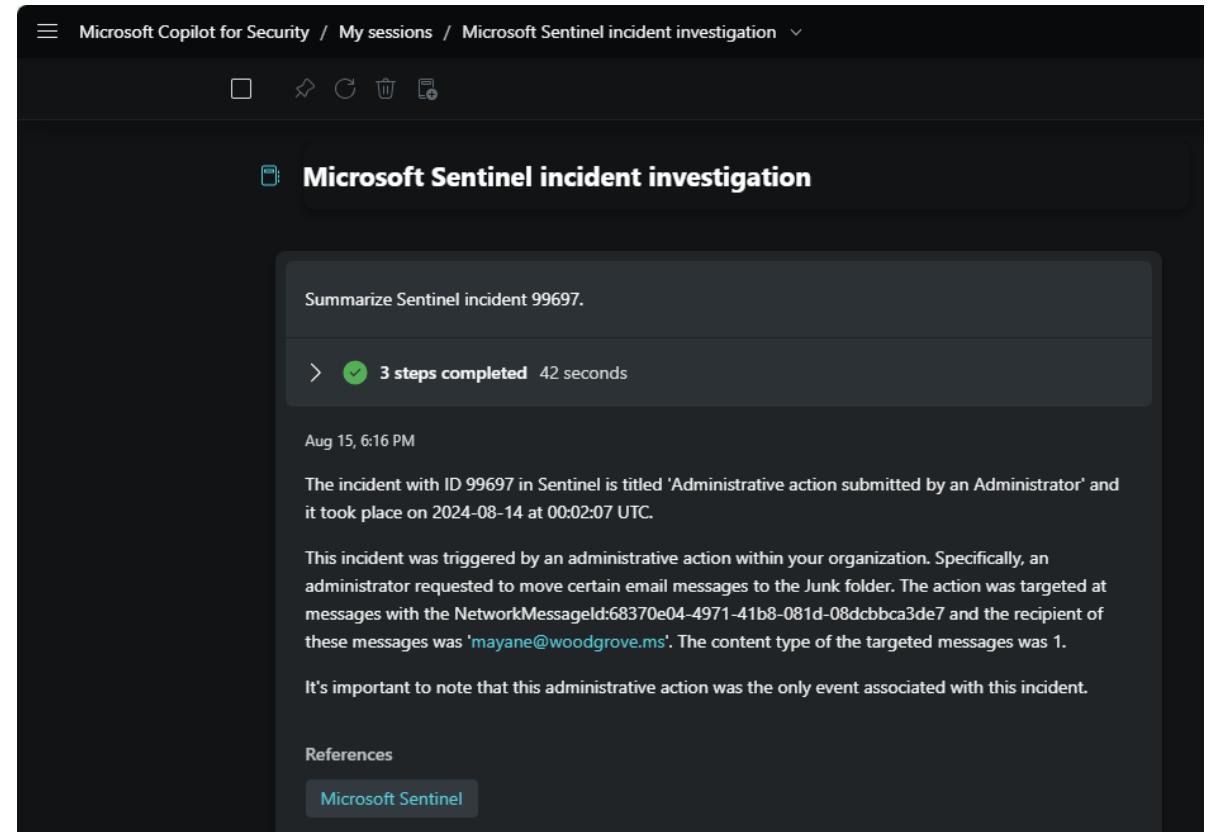
Integração do Copilot da Segurança da Microsoft com o Microsoft Sentinel

Plug-ins do Copilot:

- Microsoft Sentinel
- Linguagem natural para o KQL para Microsoft Sentinel

A integração do Copilot com suporte por meio de:

- Experiência autônoma
- Experiência inserida no Portal do Microsoft Defender



Demonstração

- Microsoft Sentinel

**Descrever os recursos das soluções da
segurança da Microsoft (parte 3 de 3)**

Objetivos de aprendizagem

- Descrever a proteção contra ameaças com o Microsoft Defender XDR



Objetivo de aprendizagem: Descrever a proteção contra ameaças com o Microsoft Defender XDR

Microsoft Defender XDR

Um pacote de defesa corporativa que coordena nativamente a detecção, a prevenção, a investigação e a resposta em seu ambiente para fornecer proteção integrada contra ataques sofisticados.

O Defender inclui:

- Microsoft Defender para Ponto de Extremidade
- Microsoft Defender para Office 365
- Microsoft Defender para Identidade
- Microsoft Defender para Aplicativos de Nuvem
- Gerenciamento de Vulnerabilidades do Microsoft Defender

Portal do Microsoft Defender XDR

- Entrega uma plataforma unificada de operações de segurança.
- Inclui o Defender XDR, o Microsoft Sentinel e muito mais.

Microsoft
Defender
XDR



Integração com o Copilot da Segurança da Microsoft:

- Habilitado por meio de plug-ins
- Experiências autônomas e inseridas.

Microsoft Defender para Office 365

Integração perfeita à sua assinatura do Office 365 que fornece proteção contra ameaças que chegam em emails, links, anexos ou ferramentas de colaboração.

Prevenir e detectar

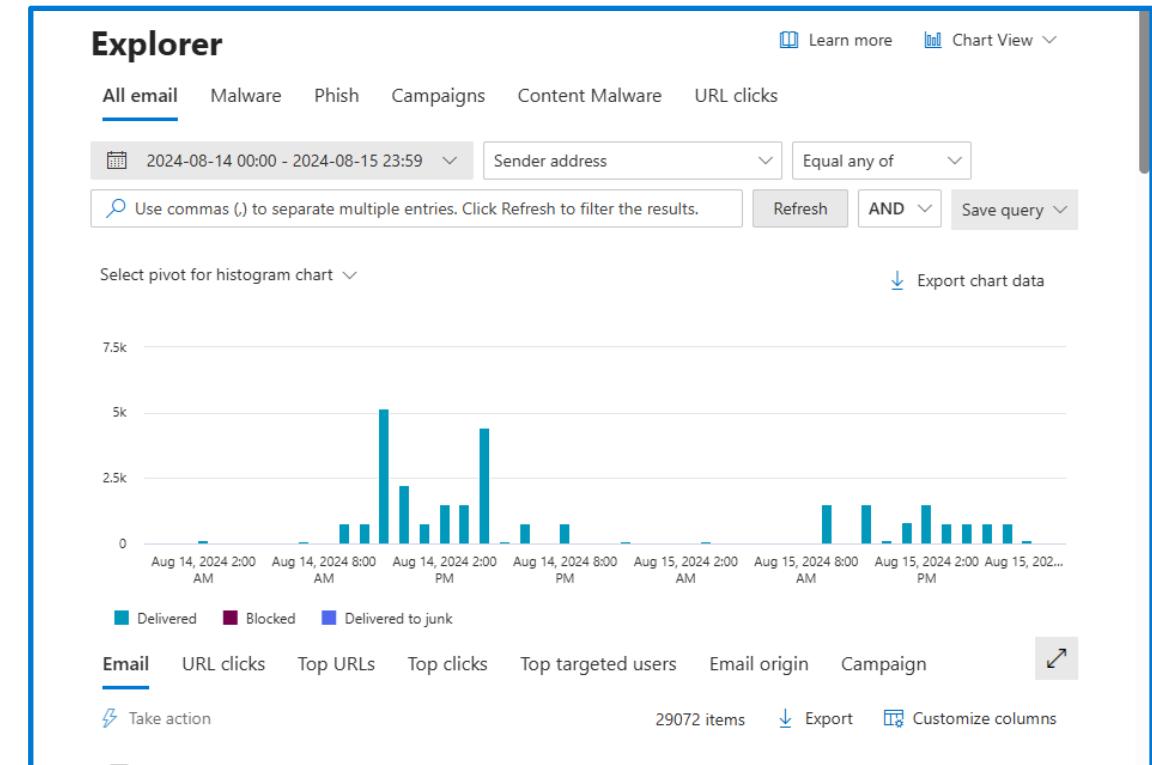
- Políticas para antimalware, antispam, antiphishing
- Anexos seguros
- Treinamento de simulação de ataque
- Mais..

Investigar

- Pesquisa de logs de auditoria
- Rastreamento de mensagens
- Gerenciador
- Mais...

Responder

- Limpeza automática de zero hora (ZAP)
- Investigação e resposta automatizadas
- Mais..



Microsoft Defender para Ponto de Extremidade

O Microsoft Defender para Ponto de Extremidade é uma plataforma projetada para ajudar as redes corporativas a proteger os pontos de extremidade.

Microsoft Defender para Ponto de Extremidade



Gerenciamento
de ameaças
e vulnerabilidades



Redução da
superfície
de ataque



Proteção de
última geração



Detecção e resposta
de pontos de
extremidade



Investigação
e correção
automatizadas



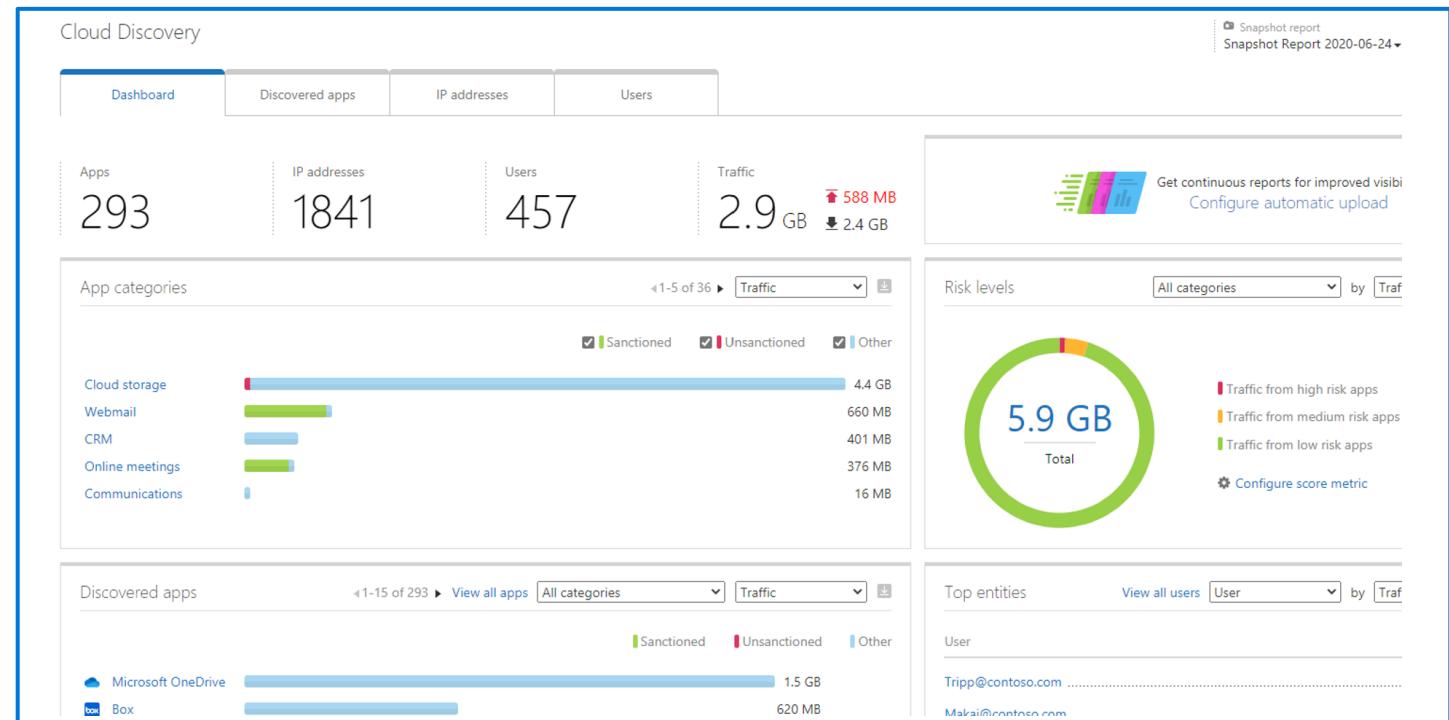
Especialista
em Ameaças
da Microsoft

Configuração e administração centralizadas e APIs

Microsoft Defender para Aplicativos de Nuvem

Fornece visibilidade avançada dos serviços de nuvem, controle sobre o tráfego de dados e análise sofisticada para identificar e combater ameaças cibernéticas em todos os seus serviços de nuvem da Microsoft e de terceiros.

- Descubra aplicações SaaS
- Proteção de informação
- Gerenciamento da Postura de Segurança de SaaS (SSPM)
- Proteção avançada contra ameaças
- Proteção de aplicativo para aplicativo



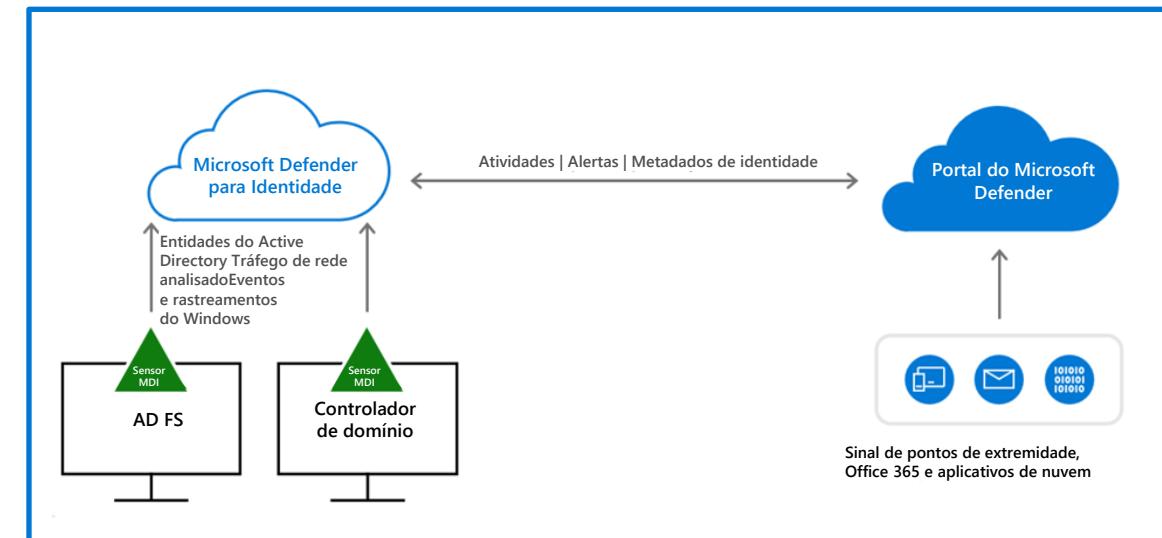
Demonstração

- Microsoft Defender para Aplicativos de Nuvem

Microsoft Defender para Identidade

Uma solução de segurança baseada em nuvem que usa sinais de seus servidores de infraestrutura de identidade na infraestrutura local para detectar ameaças e relatórios sobre problemas de identidade facilmente explorados.

- Os sensores baseados em software instalados na infraestrutura local enviam sinais ao serviço Defender para Identidade.
- O Defender para Identidade usa sinais para fornecer detecção e resposta a ameaças de identidade (ITDR) que permitem aos profissionais de segurança:
 - Avaliar proativamente sua postura de identidade
 - Detectar ameaças usando análise em tempo real e inteligência de dados
 - Investigar alertas e atividades de usuários
 - Ações de correção
- O portal do Microsoft Defender fornece às equipes de segurança uma plataforma de operações de segurança unificada para investigar e responder a ataques.



Gerenciamento de Vulnerabilidades do Microsoft Defender

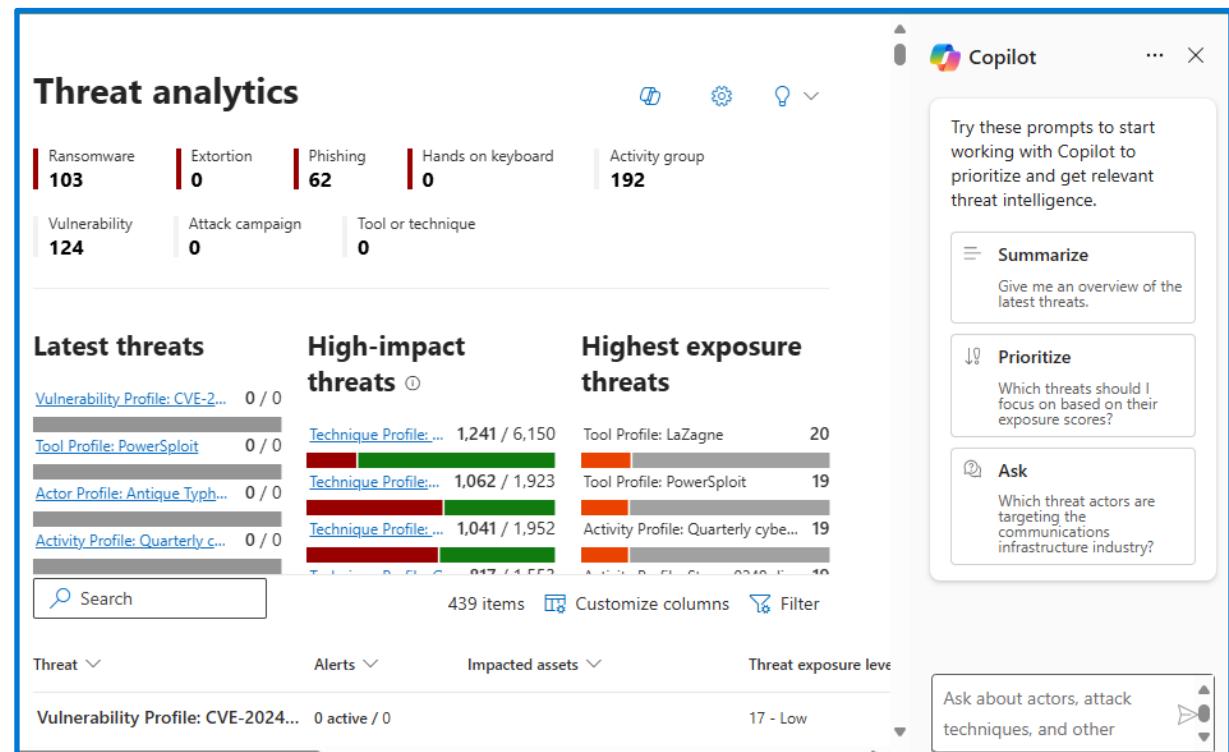
Oferece visibilidade de ativos, avaliações inteligentes e ferramentas de correção internas para Windows, macOS, Linux, Android, iOS e dispositivos de rede.



Informações sobre Ameaças do Microsoft Defender

Agrega e enriquece fontes de dados de inteligência contra ameaças críticas e é integrado ao Copilot da Segurança da Microsoft para ajudar o analista de segurança na medida em que eles fazem triagem, investigam e remediam vulnerabilidades.

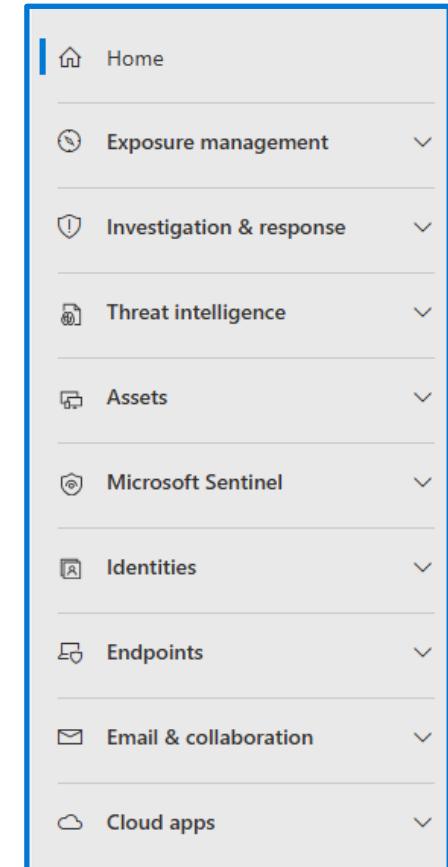
- Análise de ameaças - entenda como as ameaças emergentes afetam o ambiente da sua organização.
- Perfis de informação - uma fonte definitiva do conhecimento compartilhável da Microsoft sobre agentes de ameaças rastreados, ferramentas maliciosas e vulnerabilidades.
- Gerenciador de informações - onde os analistas podem rapidamente digitalizar novos artigos em destaque e realizar a pesquisa para coleta de inteligência.
- Projetos de informação – os usuários podem criar projetos que organizam indicadores de comprometimento (IOCs) a partir de uma investigação e contêm artefatos associados e um histórico detalhado.



Portal do Microsoft Defender

O portal do Microsoft Defender oferece uma plataforma unificada de operações de segurança.

- O melhor do SIEM, do XDR, do gerenciamento de posturas e da inteligência com ameaças com IA generativa avançada como uma única plataforma.
- Combina proteção, detecção, investigação e resposta a ameaças em toda a sua organização e todos os componentes dela em um só lugar.



Integração do Copilot ao Microsoft Defender XDR

A integração do Copilot é vivenciada por meio das experiências autônomas e inseridas.

Experiência autônoma:

- Habilite plug-ins para oferecer suporte à integração com o Microsoft Defender XDR
- Os recursos do sistema servem como prompts internos.
- Use o promptbook interno de investigação de incidentes do Defender ou crie o seu próprio.

Manage sources

Plugins

Microsoft Defender XDR
Alerts and incidents

Files

Natural language to KQL for Microsoft Defender XDR
Query-generating capability (for Defender)

≡ SYSTEM CAPABILITIES

MICROSOFT DEFENDER XDR

Analyze a file
Inspect a file using available information, including API calls, certificates...

Generate an identity summary
Get identity insights, security concerns and potential anomalies

Generate an incident report
Get a report about an attack and your response, including who took act...

Generate guided response
Get step-by-step response recommendations for an incident.

List incidents and related alerts
Get the list of incidents or find specific incidents.

How can Copilot for Security help?

Integração do Copilot ao Microsoft Defender XDR (cont.)

A integração do Copilot é vivenciada por meio das experiências autônomas e inseridas.

Experiência inserida:

- Resumir incidentes
- Respostas guiadas
- Análise de script
- Linguagem natural para consulta KQL
- Relatórios de incidentes
- Analisar arquivos
- Resumos de dispositivo e identidade

The screenshot displays the Microsoft Defender XDR interface. On the left, a main panel shows an incident summary for "Plaid Rain activity with multi-stage incident involving Execution & Lateral movement on one endpoint reported by multiple sources". It includes a shield icon, severity levels (High, Resolved), and tags (Plaid Rain, Defender Experts). Below this are sections for "Incident details" (Assigned to baat18@woodgrove.ms, Incident ID 30358) and "Classification" (Not set). To the right, a sidebar titled "Copilot" provides an "Incident summary" from Sep 10, 2024, at 4:16 PM. It details the incident and notes it was attributed to the threat actor PLAID RAIN. A section titled "Guided response" is also present, with a note about AI-generated content being incorrect and a status bar indicating "Completed recommendations 0/4".

Demonstração

- O portal do Microsoft Defender XDR

**Descrever os recursos do Microsoft Priva
e do Microsoft Purview**



Objetivos de aprendizagem

- Descrever os recursos de privacidade do Microsoft Priva e o Portal de Confiança do Serviço da Microsoft.
- Descrever as soluções de segurança de dados do Microsoft Purview.
- Descrever as soluções de conformidade de dados do Microsoft Purview.
- Descrever as soluções de governança de dados do Microsoft Purview.



Objetivo de aprendizagem: Descrever os recursos de privacidade do Microsoft Priva e o Portal de Confiança do Serviço da Microsoft.

Portal de Confiança do Serviço da Microsoft

Site da Microsoft para publicar relatórios de auditoria e outras informações relacionadas à conformidade associadas aos serviços de nuvem da Microsoft.

- Certificações, regulamentos e padrões.
- Relatórios, white papers e artefatos.
- Recursos regionais e da indústria.
- Recursos para sua organização.



The screenshot shows the Microsoft Service Trust Portal homepage. At the top, there is a navigation bar with the Microsoft logo, the text "Portal de Confiança do Serviço", "Minha Biblioteca", and "Todos os Documentos". The main content area has a blue background and features the text "Portal de Confiança do Serviço" and "Saiba como serviços de nuvem da Microsoft protegem seus dados e como você pode gerente de segurança e conformida de de dados na nuvem para sua organização."

Demonstração

- Portal de Confiança do Serviço

Princípios de privacidade da Microsoft

-  Controle: colocar você, o cliente, no controle da sua privacidade com ferramentas fáceis de usar e escolhas claras.
-  Transparência: seremos transparentes quanto à coleta e ao uso de dados para que você possa tomar decisões embasadas.
-  Segurança: proteger os dados que são confiados à Microsoft usando segurança e criptografia fortes.
-  Proteções legais fortes: respeitar as leis locais de privacidade e lutar pela proteção legal da privacidade como um direito humano fundamental.
-  Nenhum direcionamento baseado em conteúdo: não usar emails, chats, arquivos ou outro conteúdo pessoal para direcionar anúncios.
-  Benefícios para você: quando a Microsoft coleta dados, eles são usados para beneficiar você, o cliente, e para aprimorar suas experiências.

Microsoft Priva

Ajuda as organizações a proteger dados pessoais e criar um local de trabalho resiliente à privacidade.

Gerenciamento de Riscos de Privacidade: visibilidade dos dados e modelos de política da sua organização para reduzir riscos.

Solicitações de Direitos de Titular: ferramentas de automação e fluxo de trabalho para atender às solicitações de dados.

Gerenciamento de Consentimento: acompanhe efetivamente o consentimento do consumidor em toda a sua propriedade de dados.

Verificação do Rastreador: automatize a identificação de tecnologias de rastreamento em várias propriedades da Web, promovendo a conformidade de privacidade do site.

Avaliações de Privacidade: automatize a descoberta, a documentação e a avaliação do uso de dados pessoais em todo o seu cenário de dados.



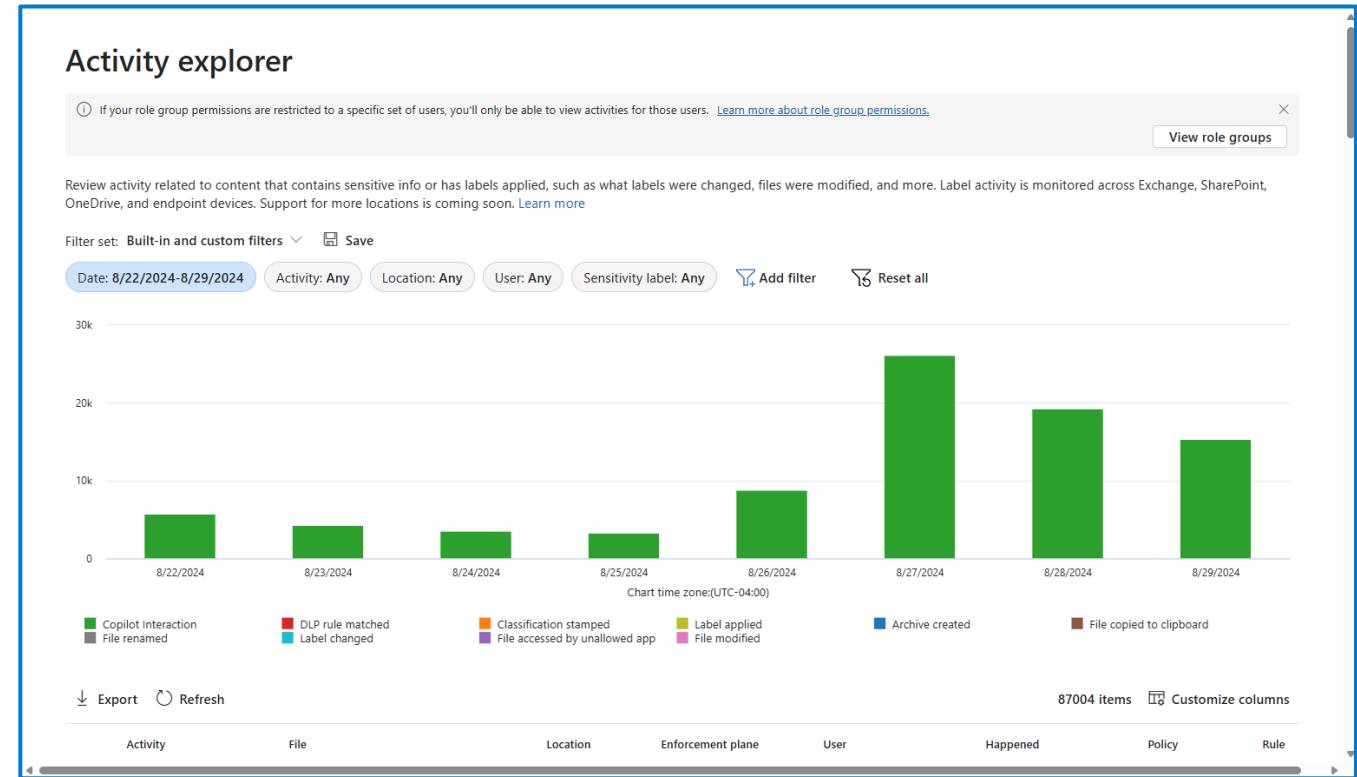


Objetivo de aprendizagem: Descrever as soluções de segurança de dados do Microsoft Purview

Classificação de dados na Proteção de Informações do Microsoft Purview

Identifique informações importantes em toda a propriedade e garanta que os dados sejam tratados de acordo com os requisitos de conformidade.

- Tipos de informações confidenciais.
- Classificadores de EDM (correspondência de dados exata)
- Classificadores treináveis: classificadores pré-treinados e classificadores treináveis personalizados.
- Gerenciador de conteúdo: um instantâneo dos itens com rótulo de confidencialidade, um rótulo de retenção ou que foram classificados como contendo um tipo de informação confidencial.
- Gerenciador de atividades: monitore o que está sendo feito com conteúdo rotulado em toda a organização.



Rótulos e políticas de confidencialidade

Os rótulos de confidencialidade são:

- Personalizáveis
- Texto claro
- Persistentes

Os rótulos de confidencialidade podem:

- Criptografar
- Marcar o conteúdo (marca d'água)
- Aplicar rótulos automaticamente
- Proteger o conteúdo em contêineres
- Estender para aplicativos/serviços de terceiros
- Classificar o conteúdo sem proteção

Políticas de rótulo

- Escolha os usuários e grupos que podem ver rótulos.
- Aplique um rótulo padrão a todos os novos emails e documentos.
- Exija justificativas para alterações de rótulo.
- Exija que os usuários apliquem um rótulo (rotulagem obrigatória).
- Vincule usuários a páginas de ajuda personalizadas.

Confidential - Finance

Name
Confidential - Finance

Display name
Confidential - Finance

Description for users
This file was automatically labeled because it contains confidential data.

Description
Documents with this label contain sensitive data.

Scope
File, Email

Encryption
Encryption

Content marking
Watermark: CONFIDENTIAL FINANCIAL DATA

Auto-labeling for files and emails
Automatically apply the label

Auto-labeling for schematized data assets (preview)
None

Demonstração

- Rótulos de confidencialidade

Prevenção contra perda de dados (DLP) do Microsoft Purview

Identificar, monitorar e proteger itens confidenciais em:

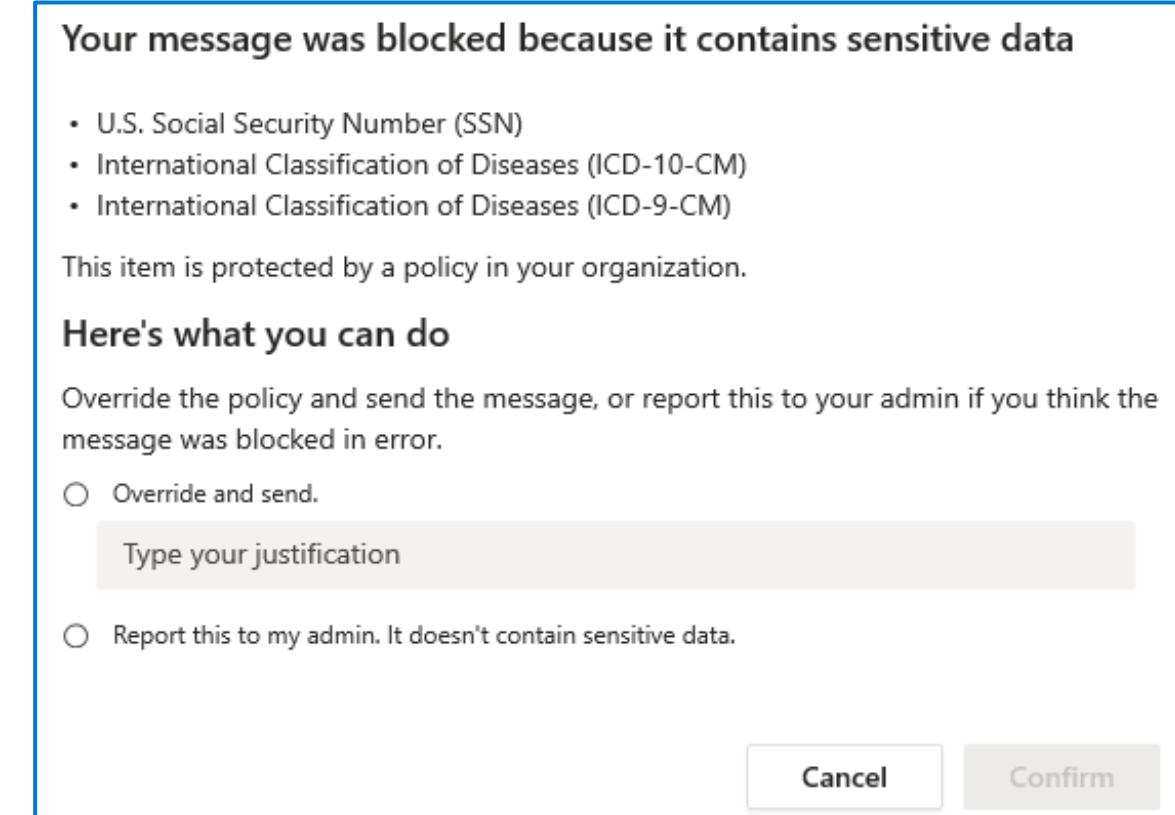
- Serviços do Microsoft 365 – aplicações do OneDrive for Business, do SharePoint Online, do Exchange Online e do Office 365.
- Microsoft Teams – Chat do Teams e mensagens de canal.
- Dispositivos — Windows 10, Windows 11 e macOS.
- Microsoft Defender para Aplicativos da Nuvem.
- Repositórios na infraestrutura local.
- Power BI.

As ações de proteção que as políticas DLP podem executar:

- Mostrar uma dica de política pop-up.
- Bloquear o compartilhamento de itens confidenciais com ou sem opção de substituição.
- Mover dados em repouso para um local de quarentena seguro.
- Para o chat do Teams, as informações confidenciais não serão exibidas.

Integração do Copilot da Segurança:

- Experimente a integração do Copilot por meio das experiências autônomas e inseridas.
- A experiência inserida oferece suporte ao resumo de alertas.



Gerenciamento de riscos internos do Microsoft Purview

Ajuda as organizações a identificar, investigar e abordar riscos internos, como vazamentos de dados, roubo de propriedade intelectual, fraude, negociação de informações internas e muito mais.

Fluxo de trabalho do gerenciamento de riscos internos

- Crie *políticas* para definir quais indicadores de risco são examinados.
- *Os alertas* são gerados automaticamente por indicadores de risco que correspondem às condições da política.
- *Faça triagem* de alertas com um status "precisa de revisão".
- As ocorrências são criadas para alertas que exigem uma revisão e *investigação* mais profundas.
- Os revisores podem *agir* rapidamente para resolver a ocorrência.



Integração com o Copilot da Segurança

- Integração por meio das experiências autônomas e inseridas.
- A experiência inserida oferece suporte ao resumo de alertas.

Proteção Adaptável no Microsoft Purview

A Proteção Adaptável no Microsoft Purview usa o ML (machine learning) para identificar os riscos mais críticos e aplicar de forma proativa e dinâmica os controles de proteção.

Com base nos níveis de risco no Gerenciamento de Riscos Internos, a Proteção Adaptável no Microsoft Purview aplica controles de:

- Prevenção contra Perda de Dados
- Gerenciamento do Ciclo de Vida dos Dados no Microsoft Purview (versão preliminar)
- Acesso Condisional do Microsoft Entra (versão preliminar)

Reduza os riscos potenciais usando:

- Detecção com reconhecimento de contexto.
- Controles dinâmicos
- Mitigação automatizada





Objetivo de aprendizagem: Descrever as soluções de conformidade de dados do Microsoft Purview

Auditoria do Microsoft Purview

Ajude as organizações a responder de forma eficaz a eventos de segurança, investigações forenses, investigações internas e obrigações de conformidade.

Auditoria (Standard)

Auditoria (Premium)

Registrar e pesquisar atividades auditadas:

Baseia-se nos recursos da Auditoria (Standard) com:



- Habilitado por padrão
- Milhares de eventos de auditoria pesquisáveis
- Período de retenção padrão de 90 dias
- Acesso por GUI, cmdlet e API

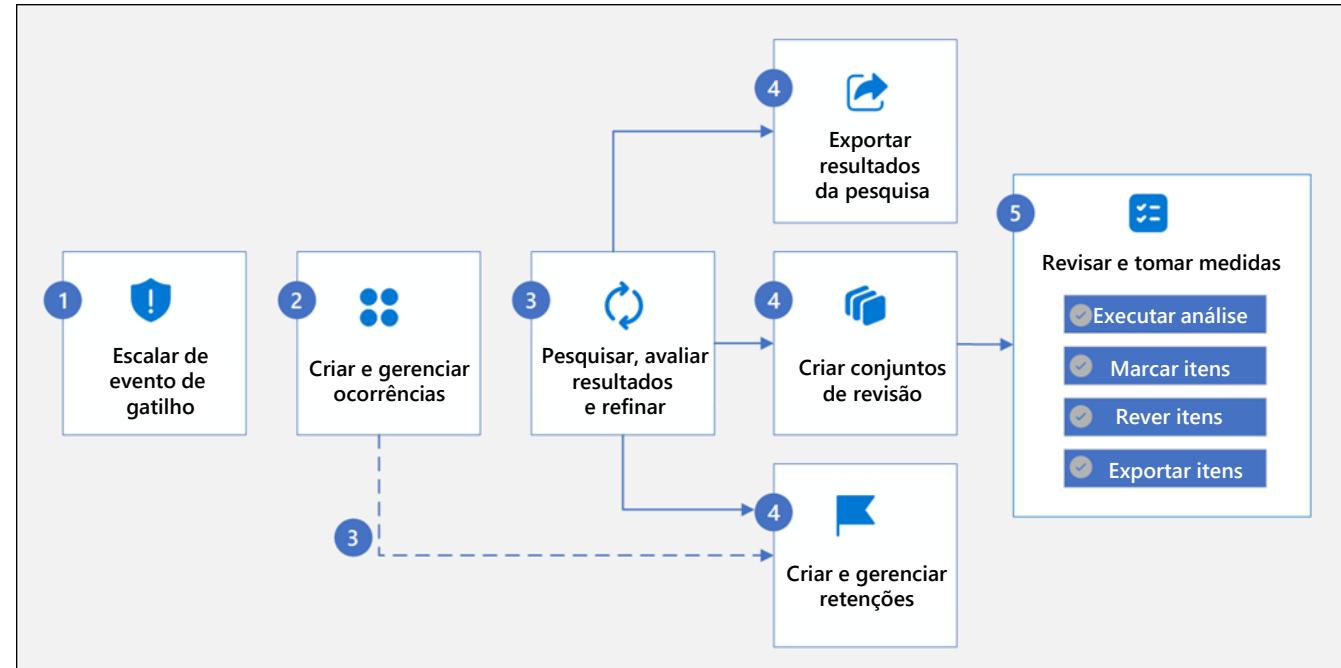


- Período de retenção padrão de 1 ano
- Políticas de retenção personalizadas
- Insights inteligentes
- Acesso de largura de banda maior à API

Descoberta eletrônica do Microsoft Purview

O processo de identificação e fornecimento de informações eletrônicas que podem ser usadas como evidência em ocorrências legais.

1. Os eventos de gatilho solicitam a criação de uma nova ocorrência na Descoberta Eletrônica (versão preliminar).
2. Criar e gerenciar ocorrências
3. Pesquise os locais de conteúdo em sua organização usando ferramentas de pesquisa internas.
4. As ações incluem:
 - Exportar resultados da pesquisa
 - Criar conjuntos de revisão
 - Criar retenções
5. Revisar e tomar medidas de conjuntos de revisão.
 - Executar análise
 - Marcar itens
 - Exportar itens



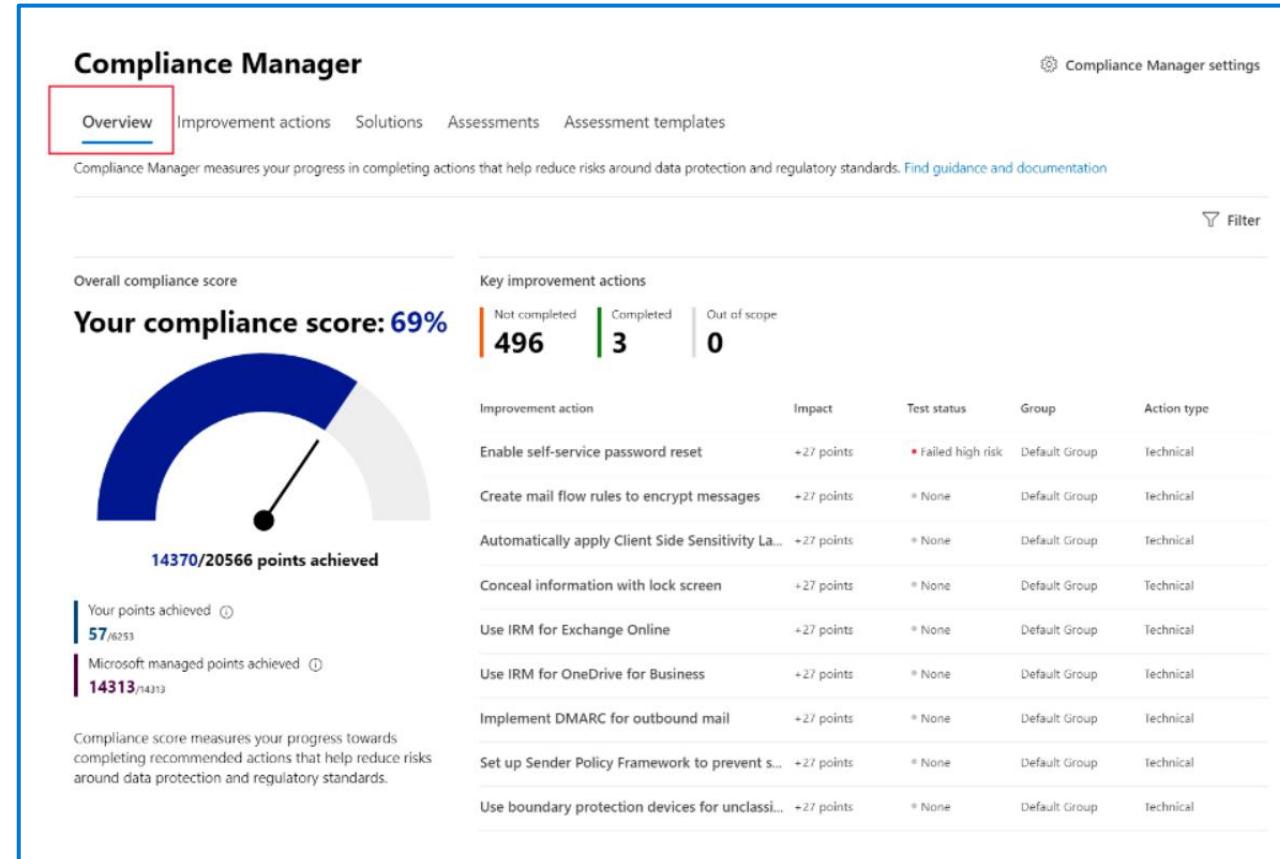
Gerenciador de Conformidade

O Gerenciador de Conformidade simplifica a conformidade e reduz riscos fornecendo o seguinte:

- Avaliações pré-criadas com base em padrões comuns.
- Recursos de fluxo de trabalho para concluir avaliações de risco.
- Ações de melhoria passo a passo.
- Pontuação de conformidade, que mostra a postura geral de conformidade.

Principais elementos do Gerenciador de Conformidade

- Controles
- Avaliações
- Regulamentos
- Ações de melhoria



Demonstração

- Gerenciador de Conformidade

Conformidade de Comunicações do Microsoft Purview

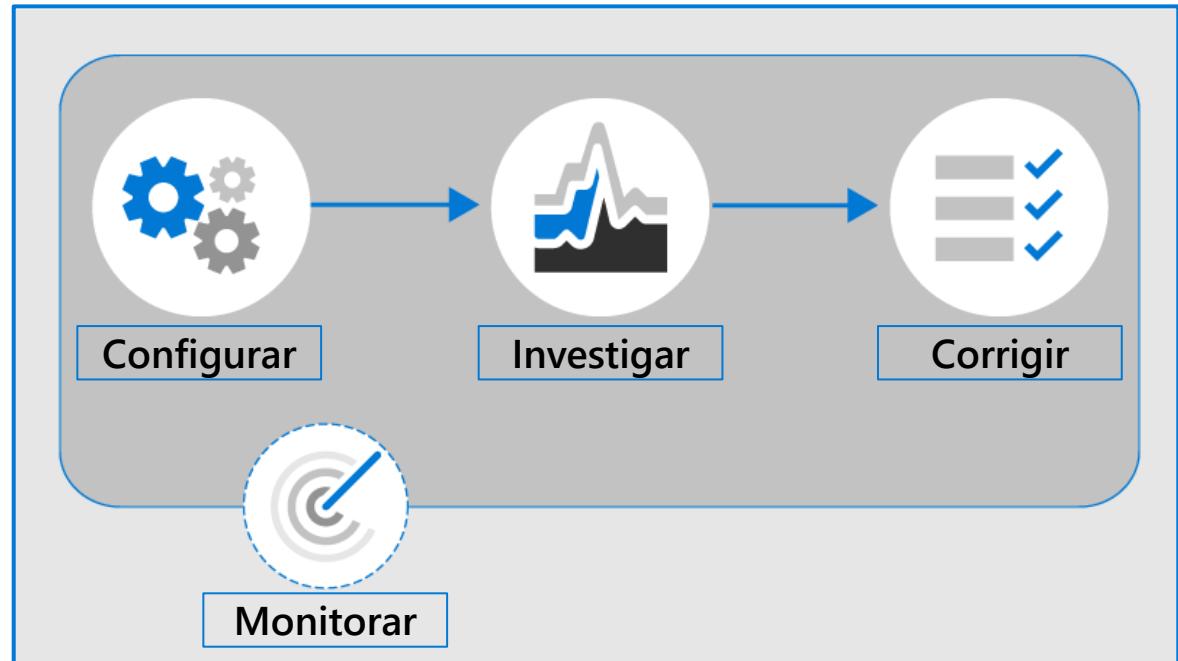
Detecte, capture e tome medidas em relação a mensagens inadequadas que podem levar a possíveis incidentes de segurança de dados ou conformidade em sua organização.

As políticas de conformidade de comunicação ajudam com o seguinte:

- Políticas corporativas: verificar mensagens em busca de problemas em relação a linguagem ofensiva ou assédio.
- Gerenciamento de riscos: verifique se há comunicação não autorizada sobre projetos confidenciais.
- Conformidade regulatória: proteja-se contra possíveis negociações de informações internas, lavagem de dinheiro e assim por diante.

Fluxo de trabalho:

- Configurar políticas.
- Investigar problemas.
- Corrigir problemas.
- Monitorar continuamente.



Integrado ao Copilot da Segurança da Microsoft

Gerenciamento do ciclo de vida de dados com rótulos e políticas de retenção

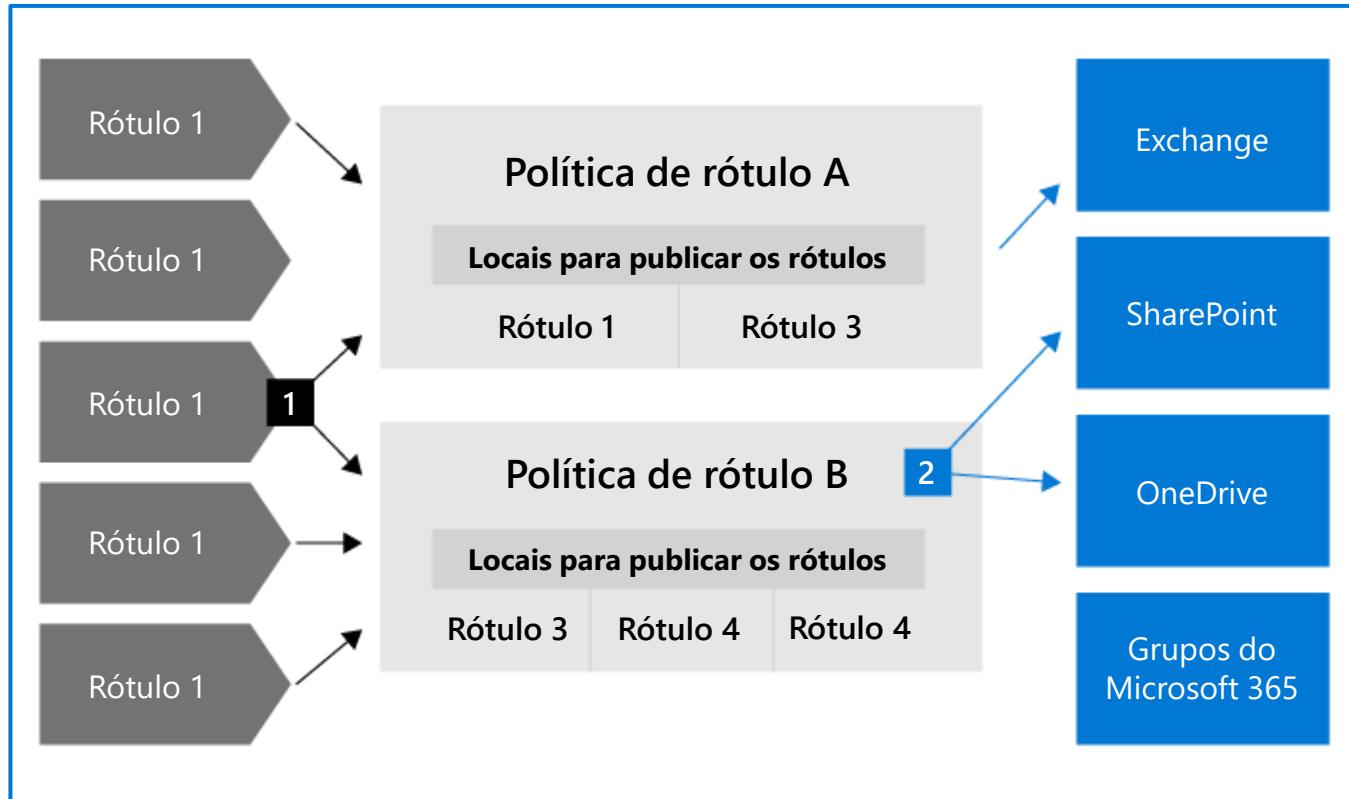
Gerencie e administre informações garantindo que o conteúdo seja mantido somente pelo tempo necessário.

Rótulos de retenção:

- Atribuído em um nível de item.
- Apenas um rótulo pode ser atribuído por vez.
- As configurações de retenção acompanham o conteúdo.
- Pode ser aplicado automaticamente.
- Suporta uma revisão de disposição.
- Publicado através de política de rótulo.

Políticas de retenção:

- Atribuído em nível de site ou caixa de correio.
- Uma única política pode ser aplicada a vários locais ou a locais ou usuários específicos.
- Os itens herdam as configurações de retenção de seu contêiner.



Gerenciamento de registros do Microsoft Purview

Ajuda uma organização a cuidar de suas obrigações legais e ajuda a demonstrar a conformidade com os regulamentos.

- Para conteúdo rotulado como um registro:
 - Restrições são implementadas para bloquear determinadas atividades.
 - As atividades são registradas.
 - A prova de disposição é mantida no final do período de retenção.
- Para que os itens sejam marcados como registros, um administrador configura rótulos de retenção.

During the retention period

Retain items even if users delete

Mark items as a record

Users won't be able to edit or delete emails, and only certain users will be able to change or remove the label. They won't be able to delete SharePoint or OneDrive files, but other actions are blocked or allowed based on whether the item's record status is locked or unlocked. [Learn more](#)

Mark items as a regulatory record

At the end of the retention period

Delete items automatically

We'll delete items from where they're currently stored.



Objetivo de aprendizagem: Descrever as soluções de governança de dados do Microsoft Purview

Benefícios da governança de dados

Para consumidores de dados em toda a organização:

- Descoberta de dados: ajuda você a encontrar com facilidade os dados de que precisa.
- Acesso seguro: facilita o acesso seguro aos seus dados.
- Compreensão de dados: forneça o que você precisa saber sobre os dados.

Para proprietários e administradores de dados:

- Curadoria e gerenciamento de dados: ajudam você a fornecer dados de alta qualidade que são fáceis de entender e acessar com segurança para aplicações em toda a organização.
- Uso responsável de dados: ajuda a garantir que seus dados sejam usados por usuários pretendidos para fins pretendidos.
- Análise de impacto: entenda as ações nos dados que podem afetar seus dados.

Para administradores de dados e stakeholders de CxO:

- Criação de valor de dados: maximize a criação de valor de seus dados e, ao mesmo tempo, reduza os gastos com operações.
- Padronização de propriedade de dados: crie controles comuns em sua propriedade de dados com responsabilidade federada para que seus dados estejam íntegros e seguros.



Consumidores de Dados

Encontram e usam rapidamente conjuntos de dados relevantes e confiáveis por meio do fluxo de trabalho de solicitação de acesso simplificado.



Proprietários de Dados

Registram ativos de dados para uso, gerenciam classificações e acesso, e garantem padrões de alta qualidade.



Administradores de Dados

Garantem a qualidade dos dados e a descoberta de dados contínua, a consistência do glossário e a linhagem.



Escritório de Dados Central

Estabelece e garante políticas de governança, metadados ativos, conformidade e insights sobre a integridade geral da governança.

Catálogo de Dados do Microsoft Purview

A meta do Catálogo de Dados do Microsoft Purview é fornecer uma plataforma para governança de dados e impulsionar a criação de valor comercial em sua organização.

- Organize os dados com **domínios de negócios** (vendas, finanças etc.) que tornam os dados familiares e acessíveis e defina objetivos e resultados-chave (OKRs) para vincular os objetivos de negócios ao catálogo de dados.
- Agrupe os ativos relacionados a **produtos de dados** para que os usuários possam encontrar facilmente a imagem completa dos dados.
- Defina **elementos de dados críticos** e anexe regras e políticas que se alimentam do **acesso a dados self-service**, garantindo que os usuários tenham acesso aos dados certos.
- Habilite a **descoberta de dados** em toda a empresa com recursos de pesquisa e navegação, com eficiências adicionais oferecidas pelo Copilot no Purview para interação simples e rápida.