Endpoint Administrator

MD-102

TFTEC CLOUD

Módulo 06: Implantar proteção de dados do dispositivo

TFTEC CLOUD

Explore a Proteção de Informações do Windows

TFTEC CLOUD

Explorar Proteção de Informações do Windows

Nas empresas modernas, o aumento da colaboração entre usuários internos e externos e a proliferação de dispositivos de propriedade de funcionários, conhecidos como BYOD, elevou o risco de vazamento acidental ou mal-intencionado de dados. Esse risco cresceu com o uso expandido de aplicativos móveis, serviços baseados em nuvem e mídias sociais.

Tradicionalmente, as empresas têm acesso controlado aos dados atribuindo credenciais aos usuários e configurando permissões e listas de acesso em recursos. No entanto, o controle de acesso do usuário não impede que usuários autorizados compartilhem arquivos acidentalmente ou enviem dados em emails, levando a novos sistemas de proteção. Além disso, a maioria das tecnologias baseadas na autenticação/autorização para proteção depende da localização, o que significa que elas geralmente funcionam apenas enquanto os dados estão em um ambiente controlado pela empresa.

TFTEC CLOUD

Prevenção de perda de dados

As organizações usam sistemas DLP (prevenção contra perda de dados) para superar as limitações dos sistemas baseados em autenticação e autorização. Um sistema DLP detecta e controla automaticamente os dados que devem ser protegidos e fornece uma maneira de proteger os dados, apesar da localização. Um sistema DLP requer:

- Regras que identificam e categorizam dados que precisam de proteção.
- Aplicativos de software como o Microsoft Exchange ou o Microsoft SharePoint para examinar dados para ver se eles correspondem às regras.
- Uma maneira de definir quais ações os aplicativos devem executar quando encontram dados que correspondem a uma regra.

TFTEC CLOUD

Gerenciamento de Direitos de Informação

As empresas precisam proteger os dados depois que eles saem da empresa. Para atender a essa necessidade, os sistemas baseados no IRM (Gerenciamento de Direitos de Informação) são usados para tornar a proteção uma parte inerente dos documentos. Um funcionário pode criar um documento e determinar o nível de proteção que deve ser aplicado ao documento, como impedir que usuários não autorizados abram o documento. Em alguns cenários, a proteção também pode ser aplicada automaticamente, com base nas condições definidas pelo administrador.

Os sistemas IRM exigem a configuração de ambientes de cliente e servidor. O aplicativo cliente que abre um documento é responsável por processar regras de proteção após verificar com o componente de servidor do sistema as atualizações de autorização.

TFTEC CLOUD

Gerenciamento de Direitos de Informação (cont.)

Nem o IRM nem o DLP são suficientes no cenário em que um funcionário deixa a organização com um dispositivo pessoal ou simplesmente decide que não deseja mais permitir que a organização gerencie o dispositivo pessoal. A melhor opção, nesse caso, é excluir dados organizacionais do dispositivo pessoal. Os sistemas de proteção implementados na plataforma Microsoft 365 permitem que você faça isso. Esses sistemas permitem que você crie regras com base em quais aplicativos podem acessar dados organizacionais. Eles também permitem que você decida quais dados esses aplicativos podem acessar.

O Azure RMS (Azure Rights Management) estende a proteção para dados além do dispositivo de um usuário por meio de um sistema IRM que se integra à WIP, uma parte fundamental da Proteção de Informações do Azure. Intune permite o controle sobre as ações do usuário com dados protegidos, mesmo fora do ambiente organizacional.

Além disso, os aplicativos que podem diferenciar dados pessoais ou organizacionais, conhecidos como aplicativos habilitados, permitem aplicar regras da WIP somente a dados de propriedade da organização, deixando os dados pessoais intactos. Isso significa, por exemplo, que um funcionário pode usar com segurança o Microsoft Word em um dispositivo pessoal para documentos pessoais e empresariais, sem medo de perder seus dados pessoais quando sair da organização.

TFTEC CLOUD

Explore a Proteção de Informações do Windows

Prevenção contra perda de dados (DLP):

- Regras para identificar e categorizar dados protegidos
- Regras sobre o que fazer com os dados quando encontrados
- Pode interferir no fluxo de trabalho normal

Gestão de Direitos de Informação (IRM):

- Proteção viaja com documentos
- Requer aplicativos e infraestrutura compatíveis
- Nem o DLP nem o IRM removem dados dos dispositivos dos funcionários
- WIP gerencia aplicativos, dados e acesso de usuários
- WIP funciona com Azure RMS

TFTEC CLOUD

Planeje a proteção de informações do Windows

Benefícios:

- Dados profissionais e pessoais separados
- Proteja aplicativos de linha de negócios (LOB)
- Limpeza seletiva
- Auditoria
- Gerencie com Microsoft Intune, Microsoft Configuration Manager e outras soluções de gerenciamento de dispositivos móveis (MDM)

Cenários:

- Dados criptografados no dispositivo
- Controlar o acesso ao aplicativo
- Aplicativos iluminados detectam dados corporativos e pessoais
- Bloquear aplicativos e serviços pessoais
- Proteja dispositivos perdidos, roubados ou pertencentes a ex-funcionários

TFTEC CLOUD

Implementar e usar a Proteção de Informações do Windows

- As políticas WIP especificam quais aplicativos confiáveis podem usar e manipular dados
- Você pode definir quais aplicativos serão protegidos, o nível de proteção fornecido e como encontrar dados organizacionais na sua rede.
- Você pode definir quatro modos de proteção WIP para gerenciar o acesso
  - Bloquear ou ocultar substituições
  - Permitir substituições
  - Silencioso
  - Desligado
- Os modelos de regras são usados ao adicionar aplicativos à lista de aplicativos permitidos no WIP.
- Identidade corporativa, perímetro de rede e certificado DRA são aspectos importantes da configuração da política WIP.

TFTEC CLOUD

Explore a criptografia do sistema de arquivos no cliente Windows

EFS é uma ferramenta integrada de criptografia de arquivos para Windows:

- Permite criptografia, descriptografia e recuperação de arquivos criptografados transparentes
- Permite que arquivos criptografados sejam compartilhados com outros usuários

Cenários de uso comuns para EFS:

- Protegendo arquivos em computadores compartilhados
- Protegendo arquivos contra acesso de usuários privilegiados
- Limitando o acesso a arquivos para usuários específicos

Gerenciar certificados EFS

- O EFS usa criptografia de chave pública para criptografar arquivos e requer o gerenciamento correto do certificado EFS do usuário.
- Antes de usar o EFS, é importante emitir um certificado para um Agente de Recuperação de Dados (DRA).

Recursos EFS no Windows 10

- Configurações de Política de Grupo para EFS.
- Criptografia por usuário de arquivos offline.
- Limpeza seletiva.

TFTEC CLOUD

Explore o BitLocker

- O BitLocker fornece proteção criptografando volumes de disco, incluindo o sistema operacional e volumes de dados.
- O BitLocker usa um TPM para verificar a integridade do processo de inicialização:
  - Fornecer um método para verificar se a integridade do arquivo de inicialização inicial foi mantida.
  - Aprimorando a proteção para mitigar ataques offline baseados em software.
  - Bloquear o sistema quando detectar adulteração.
- Tanto o BitLocker quanto o EFS fornecem criptografia
  - O EFS fornece proteção em nível de arquivo e pasta.
  - O BitLocker fornece proteção no nível do volume ou do disco.
- BitLocker To Go estende suporte do BitLocker para dispositivos de armazenamento removíveis

TFTEC CLOUD

Obrigado

TFTEC CLOUD

Gerenciar o Microsoft Defender For Endpoint

TFTEC CLOUD

Explore o Microsoft Defender for Endpoint

O Microsoft Defender for Endpoint é uma plataforma projetada para ajudar redes corporativas a prevenir, detectar, investigar e responder a ameaças avançadas.

Use o portal Microsoft 365 Defender para gerenciar e monitorar o Microsoft Defender para Endpoint.

O Microsoft Defender for Endpoint usa a seguinte combinação de tecnologia

- Sensores comportamentais de endpoint
- Análise de segurança na nuvem
- Inteligência de ameaças

TFTEC CLOUD

Examine os principais recursos do Microsoft Defender for Endpoint

- Redução da superfície de ataque
- Proteção de próxima geração
- Detecção e resposta de endpoint
- Investigação e correção automática
- Pontuação segura
- Caça avançada
- Gerenciamento e APIs

TFTEC CLOUD

Explore o Controle de aplicativos e o Device Guard do Windows Defender

Controle de aplicativos do Windows Defender

- Em vez de assumir que todos os aplicativos são confiáveis, os aplicativos devem ganhar confiança para funcionar
- Assinado ou manifesto de executáveis aceitos

Proteção de dispositivo

- Aproveita o hipervisor para proteger processos no modo kernel
- HVCI requer hardware e drivers compatíveis

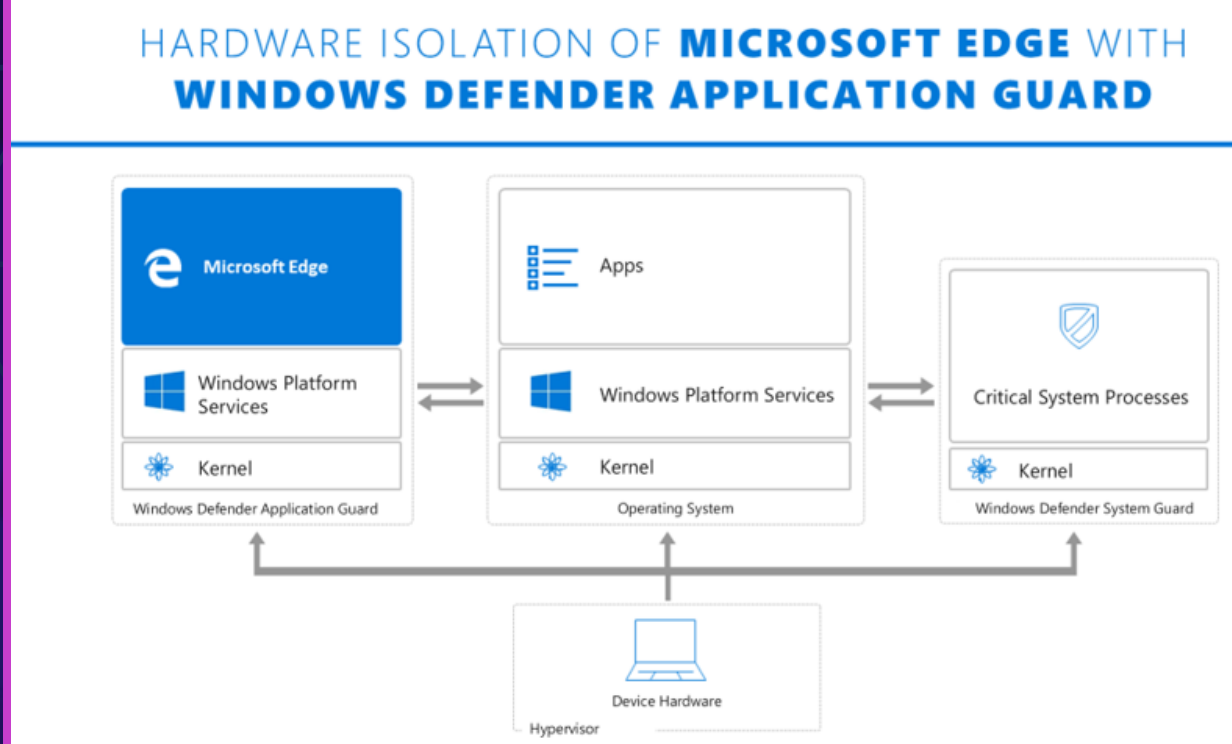
TFTEC CLOUD

Explore o Microsoft Defender Application Guard

- O Microsoft Defender Application Guard foi projetado para ajudar a prevenir ataques antigos e emergentes
- O Application Guard ajuda a isolar sites não confiáveis definidos pela empresa, fornecendo proteção enquanto seus funcionários navegam na Internet
- O Microsoft Edge abre o site em um contêiner isolado habilitado para Hyper-V, separado do sistema operacional host

Alvos do Application Guard:

- Desktops e laptops corporativos
- Dispositivos BYOD pessoais e gerenciados



Examine os principais recursos do Microsoft Defender for Endpoint

- Redução da superfície de ataque
- Proteção de próxima geração
- Detecção e resposta de endpoint
- Investigação e correção automática
- Pontuação segura
- Caça avançada
- Gerenciamento e APIs

TFTEC CLOUD

Examine o Windows Defender Exploit Guard

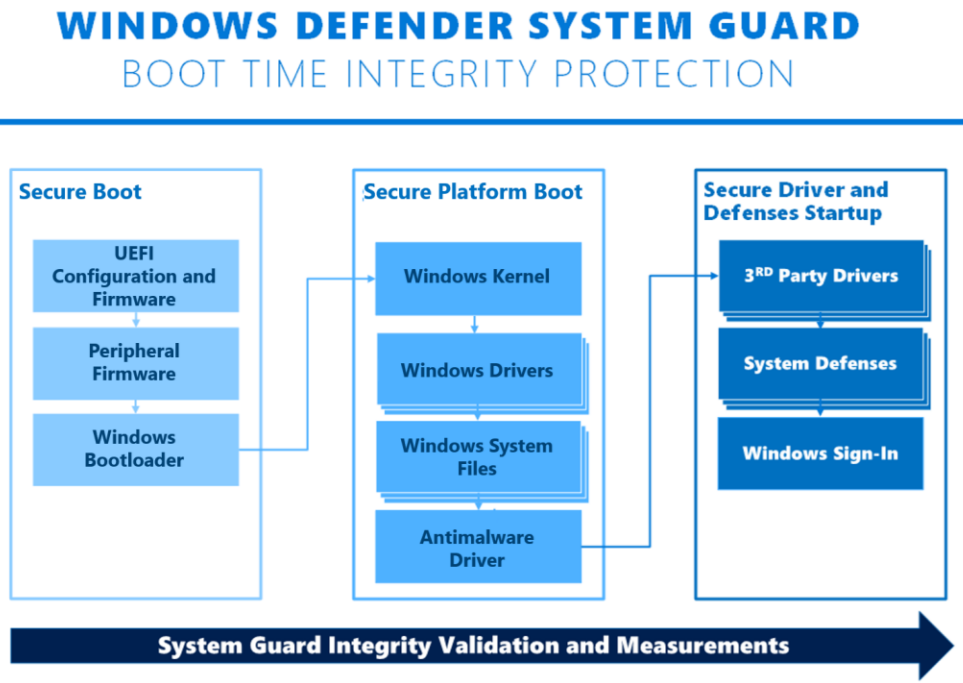
O Microsoft Defender Exploit Guard é um conjunto de recursos de prevenção de invasões de host para Windows

Os principais recursos do Microsoft Defender Exploit Guard são:

- Proteção contra exploração
- Redução da superfície de ataque
- Proteção de rede
- Acesso controlado a pastas

Explore a proteção do sistema Windows Defender

- Reorganiza os recursos existentes de integridade do sistema Windows sob o mesmo teto e configura o próximo conjunto de investimentos em segurança do Windows
- Ajuda a proteger e manter a integridade do sistema durante a inicialização
- Ajuda a proteger e manter a integridade do sistema após sua execução
- Ajuda a garantir que a integridade do sistema seja mantida por meio de verificação local e remota



Obrigado

TFTEC CLOUD

Gerenciar o Microsoft Defender no cliente Windows

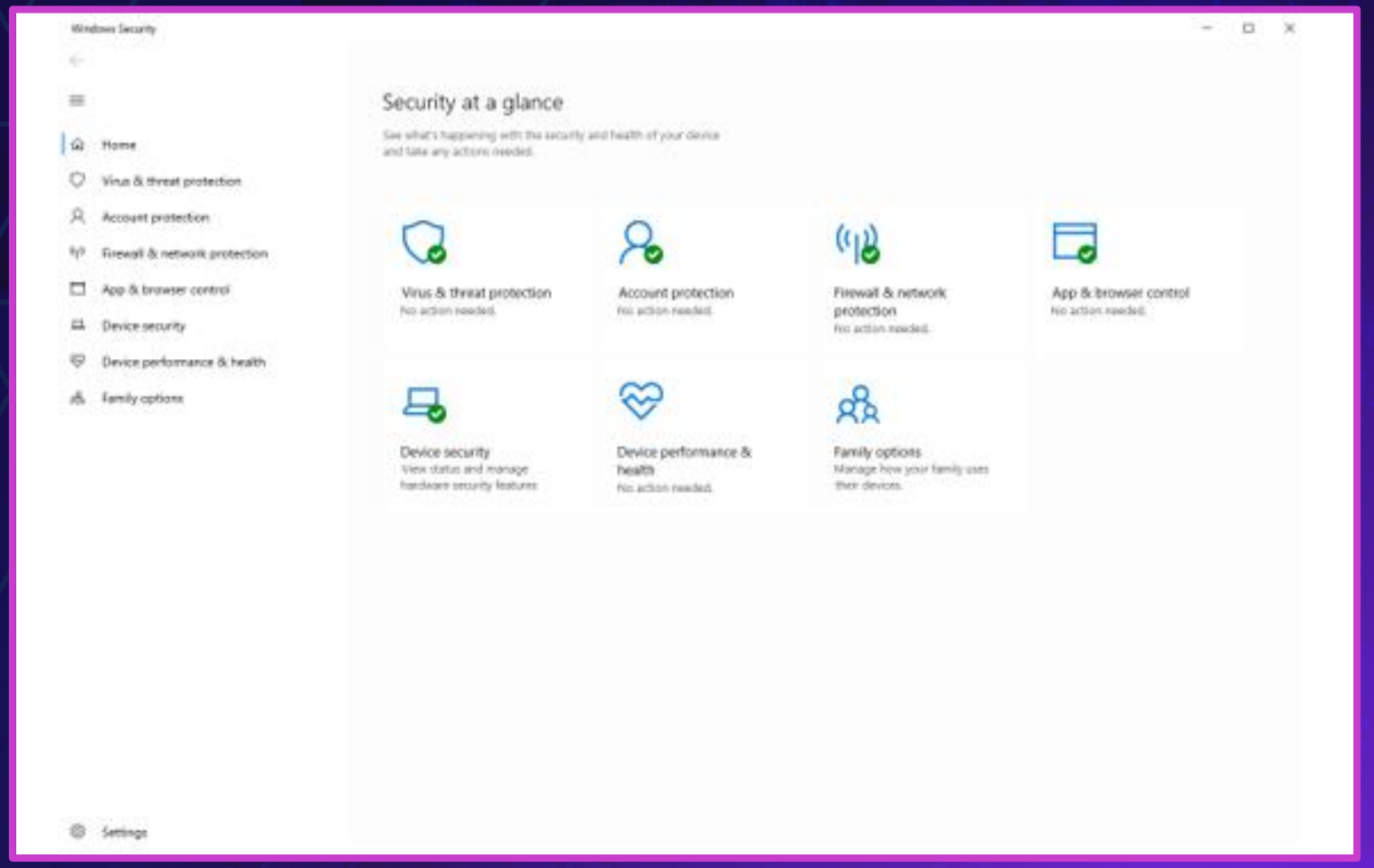
TFTEC CLOUD

Explore a Central de Segurança do Windows

A Central de Segurança do Windows cobre todos os aspectos de segurança do sistema operacional, contas e aplicativos usados em um dispositivo específico.

A Central de Segurança do Windows abrange:

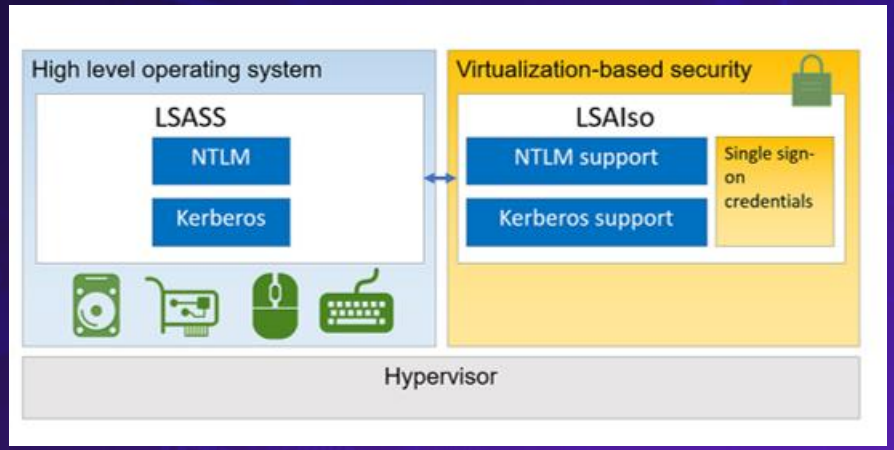
- Proteção contra vírus e ameaças
- Proteção de conta
- Firewall e proteção de rede
- Controle de aplicativos e navegadores
- Segurança do dispositivo
- Desempenho e integridade do dispositivo
- Opções familiares
- Histórico de proteção



TFTEC CLOUD

Explore o Windows Defender Credential Guard

O Windows Defender Credential Guard usa segurança baseada em virtualização para isolar segredos para que apenas softwares de sistema privilegiados possam acessá-los



O Windows Defender Credential Guard permite

- Segurança de hardware NTLM, Kerberos e Credential Manager
- Segurança baseada em virtualização Credenciais derivadas de Windows NTLM e Kerberos e outros segredos executados em um ambiente protegido
- Melhor proteção contra ameaças persistentes avançadas

TFTEC CLOUD

Gerenciar antivírus do Microsoft Defender

O Microsoft Defender Antivirus ajuda a proteger seu computador contra spyware, malware e vírus e é compatível com Hyper-V.

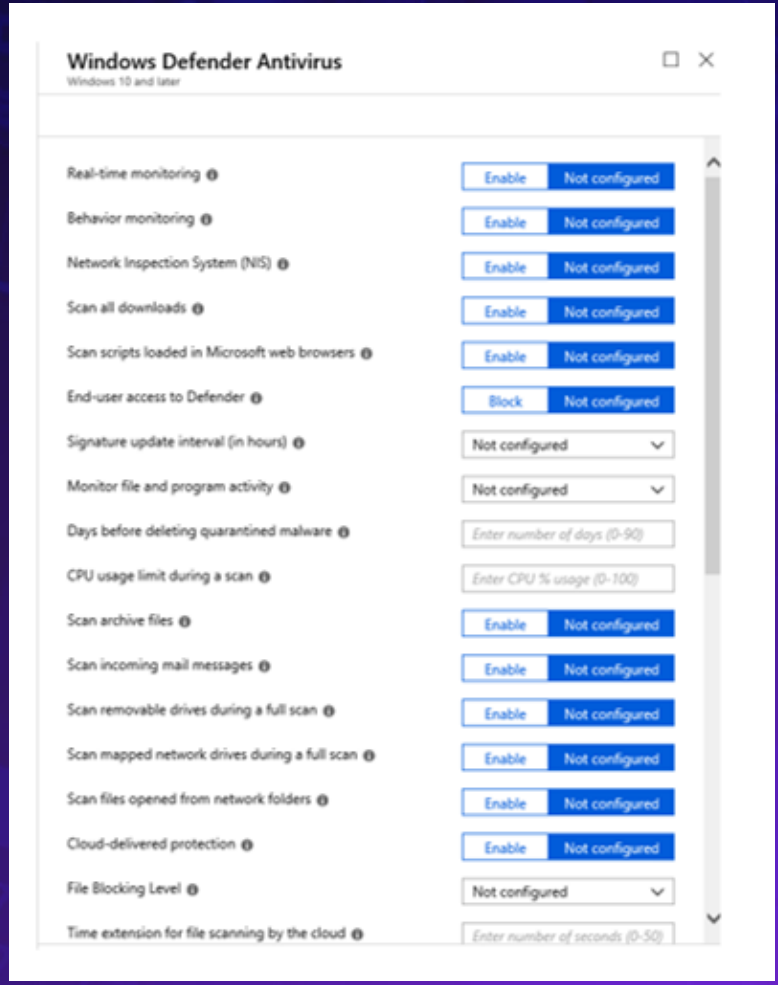
Você pode usar o Microsoft Defender Antivirus para executar uma verificação rápida, completa ou personalizada e optar por excluir processos da verificação.

Você pode configurar o Microsoft Defender Antivirus com diversas ferramentas, incluindo:

- Microsoft Intune
- Gerenciador de configuração da Microsoft

Características adicionais:

- Bloquear à primeira vista
- Detecte e bloqueie aplicativos potencialmente indesejados



TFTEC CLOUD

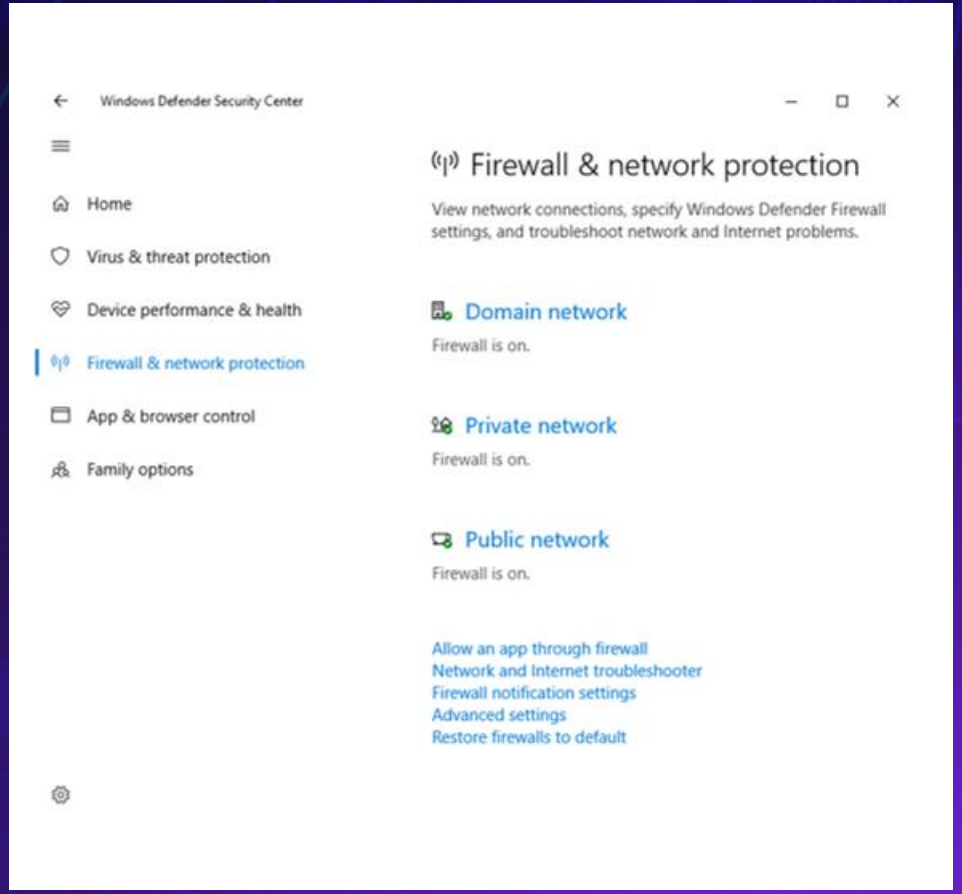
Gerenciar o Firewall do Windows Defender

As configurações do Firewall do Windows Defender podem ser acessadas na Central de Segurança do Windows ou no Painel de Controle, na Central de Rede e Compartilhamento e nos itens Sistema e Segurança.

O Microsoft Intune pode ser usado para gerenciar o Firewall do Windows Defender em computadores inscritos no Intune ou ingressados no Azure AD.

- Três tipos de perfis de localização de rede:
  - Rede de domínio
  - Rede privada
  - Rede pública

O Firewall do Windows Defender pode exibir notificações na barra de tarefas.



TFTEC CLOUD

Explore o Firewall do Windows Defender com Segurança Avançada

- Você pode executar configurações de firewall mais avançadas no snap-in Firewall do Windows Defender com Segurança Avançada.
- O Firewall do Windows Defender com Segurança Avançada é um aplicativo com reconhecimento de rede, que permite fornecer flexibilidade em uma rede interna sem sacrificar a segurança em redes externas.
- Perfis de rede pública, privada e de domínio permitem definir e agrupar configurações, incluindo regras de firewall e regras de segurança de conexão, com base no tipo de local de rede.
- Você pode configurar os seguintes tipos de regras:
  - Entrada
  - Saída
  - Regras de segurança de conexão

TFTEC CLOUD

Obrigado

TFTEC CLOUD

Gerenciar o Microsoft Defender for Cloud Apps

TFTEC CLOUD

Explore o Microsoft Defender para aplicativos em nuvem

O Microsoft Defender for Cloud Apps é uma solução versátil do Cloud Access Security Broker (CASB) com recursos avançados para ampla visibilidade e controle, juntamente com análises sofisticadas para detectar e mitigar ameaças à segurança cibernética.

Os CASBs fornecem proteções extras para serviços em nuvem, aplicando políticas de segurança corporativa, intermediando o acesso e monitorando as atividades dos usuários.

Os CASBs oferecem uma ampla gama de recursos que protegem seu ambiente em vários pilares, incluindo:

- Visibilidade
- Segurança de dados
- Proteção contra ameaças
- Conformidade

TFTEC CLOUD

Planejamento para o Microsoft Defender for Cloud Apps

O Microsoft Defender for Cloud Apps agora faz parte do Microsoft 365 Defender. O portal do Microsoft 365 Defender permite que os administradores de segurança executem suas tarefas de segurança em um local.

O Microsoft Defender for Cloud Apps não requer licenças do pacote de produtividade do Microsoft 365.

Pré-requisitos:

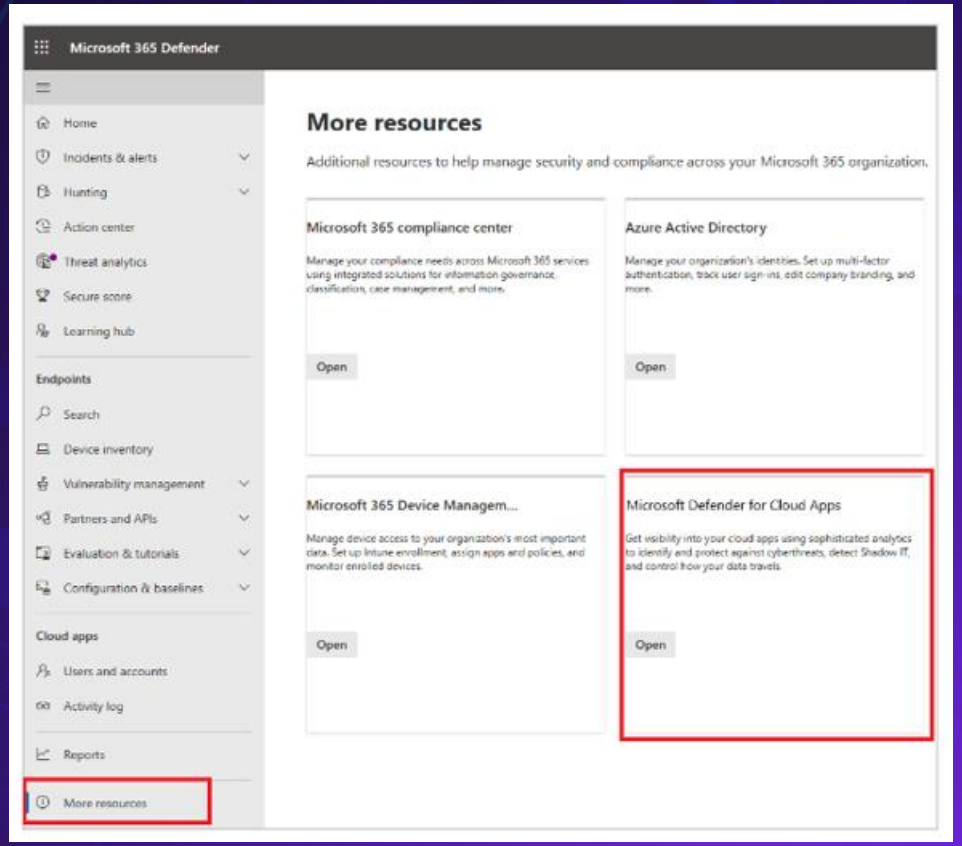
- Cada usuário protegido pelo Microsoft Defender for Cloud Apps deve ter uma licença.
- Você deve ser um Administrador Global ou um Administrador de Segurança no Azure Active Directory (ID do Entra) ou no Office 365.
- Para executar o portal do Defender for Cloud Apps, use o Microsoft Edge, Google Chrome, Mozilla Firefox ou Apple Safari.

TFTEC CLOUD

Implementar o Microsoft Defender para aplicativos em nuvem

Steps to implement Microsoft Defender for Etapas para implementar o Microsoft Defender para aplicativos em nuvem no Microsoft 365 Defender Portal: Apps in the Microsoft 365 Defender Portal:

1. Defina ações instantâneas de visibilidade, proteção e governança para seus aplicativos
2. Proteja informações confidenciais com políticas DLP
3. Controle aplicativos em nuvem com políticas
4. Configurar o Cloud Discovery
5. Implantar o Controle de Aplicativos de Acesso Condicional para aplicativos de catálogo
6. Personalize sua experiência
7. Organize os dados de acordo com suas necessidades



TFTEC CLOUD

Obrigado

TFTEC CLOUD

Laboratórios

TFTEC CLOUD

Lab 01

TASK01:

- Configurar o DLP
- Configurar o BitLocker

TFTEC CLOUD

Lab 02

TASK02:

- Onboarding Defender for Endpoint
- Integração Defender for Endpoint e Microsoft Intune
- Configurar a Redução da superfície de ataque

TFTEC CLOUD

Lab 03

TASK03:

- Gerenciar o Windows Defender Antívirus no Microsoft Intune
- Gerenciar o Firewall do Windows Defender no Microsoft Intune

TFTEC CLOUD

Lab 03

TASK03:

- Gerenciar o Microsoft Defender for Cloud Apps

TFTEC CLOUD

Lab 04

TASK04:

- Gerenciar o Microsoft Defender for Cloud Apps

TFTEC CLOUD