Endpoint Administrator

MD-102

TFTEC CLOUD

Module 05: Gerenciar autenticação e conformidade

TFTEC CLOUD

Proteger identidades no Active Directory (Entra ID)

TFTEC CLOUD

Explorar o Windows Hello para Empresas

- O Windows Hello for Business substitui senhas por autenticação forte de dois fatores em PCs e dispositivos móveis
- O Windows Hello permite que os usuários se autentiquem em:
  - Uma conta da Microsoft
  - Uma conta do Active Directory
  - Uma conta do Microsoft Azure Active Directory (Entra ID)
  - Serviços de provedor de identidade ou serviços de terceira parte confiável que suportam autenticação Fast ID Online (FIDO) v2.0 (em andamento)
- O Windows Hello fornece autenticação biométrica confiável e totalmente integrada, baseada em reconhecimento facial ou correspondência de impressão digital

TFTEC CLOUD

Implantar o Windows Hello

Você pode escolher entre três modelos de implantação:

- **Implantação somente na nuvem –** Para organizações que possuem apenas identidades na nuvem e não acessam recursos locais
- **Implantação local –** Para organizações que não possuem identidades em nuvem ou usam aplicativos hospedados no Azure AD (Entra ID)
- **Implantação híbrida –** Para organizações que possuem infraestrutura local e em nuvem

TFTEC CLOUD

Gerenciar o Windows Hello para Empresas

As configurações dos perfis de configuração do dispositivo Intune incluem:

- Comprimento mínimo/máximo do PIN
- Complexidade/expiração/histórico do PIN
- TPM/Biométrico
- Certificados

Você pode gerenciar o Windows Hello for Business de três maneiras:

- Política de grupo
  - Configuração do usuário>Modelos administrativos>Componente e Windows>Windows Hello para Empresas
- Gerenciamento do Intune (moderno)
  - Perfis de configuração de dispositivo
  - Políticas de registro de dispositivos
- Certificado do Windows Hello para Empresas

TFTEC CLOUD

Explore a proteção de identidade do Entra ID

Além de proteger dispositivos e dados críticos, também é necessário proteger as identidades dos usuários.

A Proteção de Identidade do Azure AD (Entra ID) é um recurso da licença Premium P2 do Azure AD (Entra ID) direcionada a usuários do Microsoft 365 e de outros serviços de nuvem da Microsoft.

A Proteção de Identidade do Azure AD (Entra ID) oferece a capacidade de:

- Reconheça proativamente possíveis riscos de segurança e identifique vulnerabilidades em sua organização
- Aplicar automaticamente respostas e ações quando atividades suspeitas forem detectadas
- Investigar adequadamente os incidentes e tomar medidas para resolvê-los

A Proteção de Identidade do Azure AD (Entra ID) pode notificar os administradores, tentar remediar o risco, aumentar os requisitos de segurança de autenticação ou tomar outras ações definidas pela política de risco.

TFTEC CLOUD

Gerenciar a redefinição de senha de autoatendimento no Entra ID

Redefinição de senha de autoatendimento:

- AD DS no Windows Server não oferece suporte nativo
- O Azure AD (Entra ID) oferece suporte por padrão
- Você deve habilitar esta funcionalidade no portal Azure (Entra)
- Os usuários podem registrar-se para a funcionalidade de redefinição de senha de autoatendimento, alterar sua senha e configurar métodos alternativos de verificação de identidade usando o portal de aplicativos do Azure AD (Entra ID).

A redefinição de senha de autoatendimento exige que você defina métodos de autenticação alternativos, incluindo:

- Telefone Comercial
- Celular
- Endereço de e-mail alternativo
- Questões de segurança

TFTEC CLOUD

Implementar autenticação multifator

A MFA requer uma forma adicional de autenticação:

- Autenticação de aplicativo móvel
- Chamada telefónica
- Mensagem de texto
- Token OAuth de terceiros

Solução de segurança multifatorial:

- Para aplicativos somente em nuvem
- Para aplicativos locais

O MFA vem como parte das seguintes ofertas:

- Licenças Premium do Azure Active Directory (Entra ID)
- MFA para Microsoft 365
- Administradores globais do Azure Active Directory (Entra ID)

TFTEC CLOUD

Habilitar acesso organizacional

TFTEC CLOUD

Permitir acesso aos recursos da organização

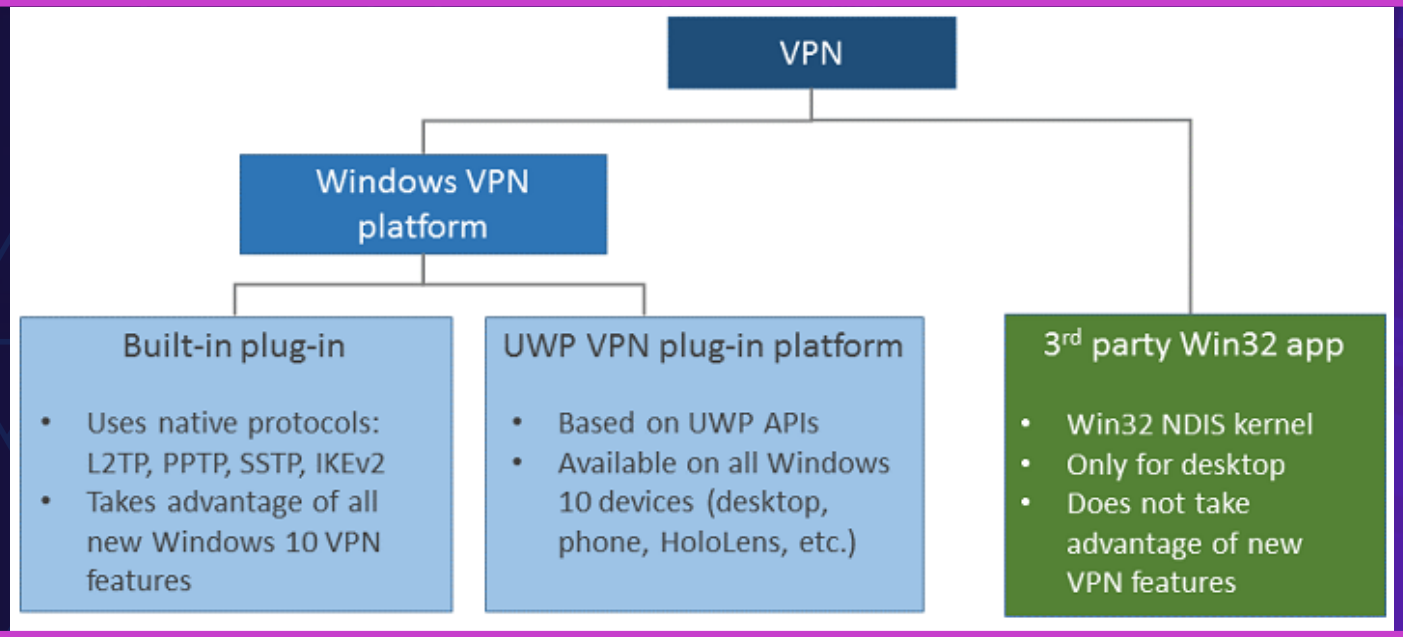
- O Windows Server tem uma função de servidor de Acesso Remoto que pode ser configurada como um servidor que encerra e roteia conexões VPN da Internet ou de outras redes externas
- A função de servidor Acesso Remoto é um agrupamento lógico destas tecnologias de acesso à rede:
  - Serviço de acesso remoto (RAS)
  - Roteamento
  - Proxy de aplicativo da Web
- Ao instalar os serviços de função DirectAccess e VPN (RAS), você está implantando o Gateway de Serviço de Acesso Remoto (Gateway RAS)
- Você pode implantar o Gateway RAS como um servidor VPN (rede privada virtual) de gateway RAS de locatário único, um servidor VPN Gateway RAS multilocatário e como um servidor DirectAccess

TFTEC CLOUD

Explore os tipos e configurações de VPN

Redes privadas virtuais (VPNs) são conexões ponto a ponto através de uma rede privada ou pública, como a Internet. Um cliente VPN usa protocolos especiais baseados em TCP/IP ou UDP, chamados protocolos de tunelamento, para fazer uma chamada virtual para uma porta virtual em um servidor VPN.

No Windows 11 e posterior, o plug-in integrado e a plataforma de plug-in VPN da Plataforma Universal do Windows (UWP) são criados sobre a plataforma VPN do Windows



Explore a VPN Always On

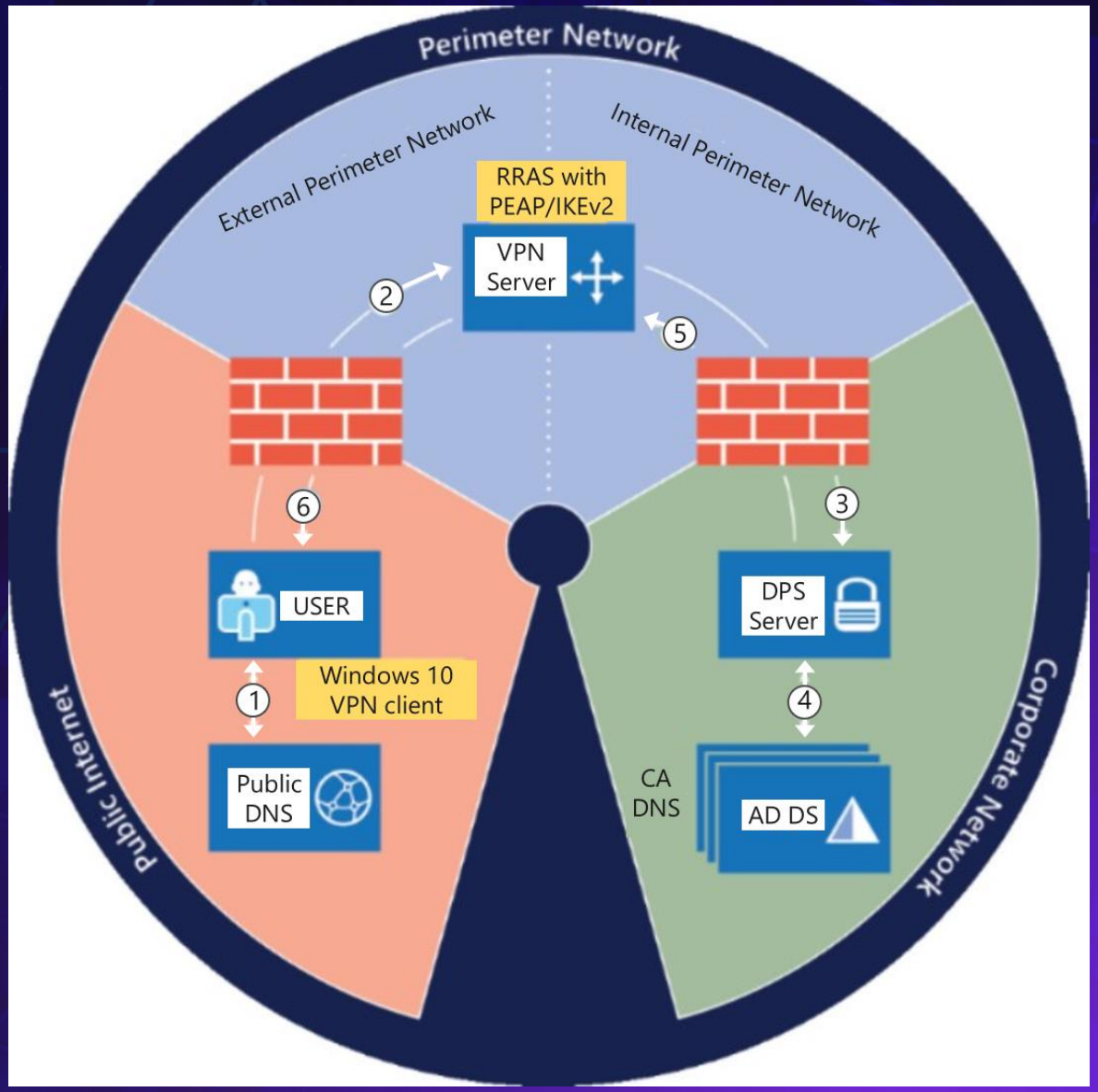
- Always On VPN é um sucessor direto da tecnologia DirectAccess que permite aos usuários permanecer conectados à sua rede interna sempre que estiverem conectados à Internet.
- Ele fornece uma solução única e coesa para acesso remoto e oferece suporte a dispositivos ingressados no domínio, não ingressados no domínio (grupo de trabalho) ou Azure AD – ingressados no Windows 10 ou 11.
- Always On VPN tem muitos benefícios em relação às soluções VPN do Windows do passado, incluindo implantação mais simples e mais flexibilidade para os clientes.
- Os Serviços de Domínio Active Directory (AD DS) ou a Política de Grupo não podem ser usados para implantar e gerenciar o Always On VPN. O Microsoft Configuration Manager, o Microsoft Intune ou o PowerShell devem ser usados.
- O Windows Server 2022 e posterior, com a função Roteamento e Acesso Remoto instalada, oferece suporte à tecnologia Always On VPN.

TFTEC CLOUD

Implantar VPN Always On

Ao se preparar para a implantação do Always On VPN, você deve garantir que possui os seguintes componentes em funcionamento

- Infraestrutura de domínio do Active Directory
- Infraestrutura de chave pública (PKI) baseada no Active Directory
- Servidor físico para instalar o Network Policy Server (NPS)
- Acesso remoto como VPN Gateway RAS
- Rede de perímetro que inclui dois firewalls
- Servidor físico ou VM em sua rede de perímetro com dois adaptadores de rede Ethernet física para instalar o Acesso Remoto como um servidor VPN Gateway RAS
- Associação em Administradores
- Plataforma de gestão à sua escolha



Implantar conformidade do dispositivo

TFTEC CLOUD

Proteja o acesso aos Recursos usando o Intune

- Permitir acesso a e-mail e documentos apenas de dispositivos gerenciados por MDM e que estejam em conformidade com a política da empresa, como especificar que as senhas dos usuários devem ser complexas, os dados locais nos dispositivos devem ser criptografados, o uso de autenticação multifator (MFA) e as atualizações mais recentes estão instaladas.
- Defina as políticas da empresa usando a política de Segurança de Dispositivos no Microsoft 365 ou Conformidade de Dispositivos no Intune.
- Use políticas de acesso condicional para controlar o acesso a e-mail, documentos e outros aplicativos em nuvem, bem como avaliar o risco de login, tipo de dispositivo, localização e aplicativos cliente.
- Se um dispositivo não estiver inscrito no Intune, a sua conformidade não poderá ser avaliada, mas pode impedir o acesso a caixas de correio, documentos e aplicações na nuvem desses dispositivos.

TFTEC CLOUD

Explore a política de conformidade do dispositivo

- Consiste em regras que incluem:
  - Configurações de senha
  - Configurações de criptografia
  - Dispositivos com jailbreak ou root
  - A versão mínima/máxima do sistema operacional
  - O nível máximo de defesa contra ameaças móveis
- As políticas de conformidade do dispositivo podem ser usadas com ou sem acesso condicional
- Implantado com base no usuário, não no dispositivo
- Monitorado a partir do painel de conformidade do dispositivo
- Ações não conformes:
  - Notificar os usuários finais por e-mail
  - Marcar dispositivo como não compatível
- É recomendável usar grupos do Azure AD (Entra ID) para usuários e dispositivos aplicarem políticas do Intune.

TFTEC CLOUD

Implantar uma política de conformidade do dispositivo

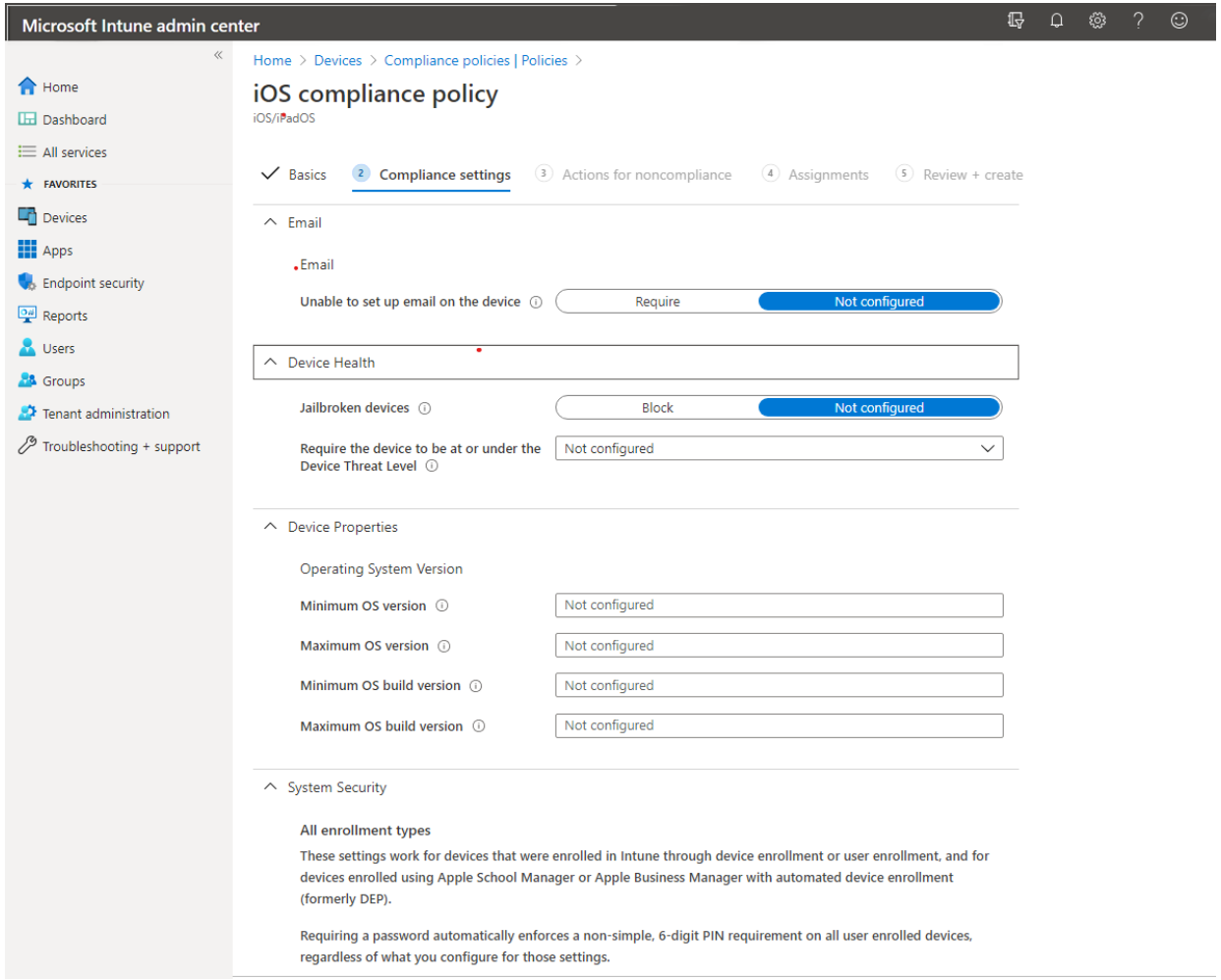
Pré-requisitos da política de conformidade do dispositivo:

- Licenciado para Azure AD (Entra ID) Premium P1 ou Azure AD (Entra ID) Premium P2 e Intune
- Os dispositivos são executados em uma plataforma compatível
- Os dispositivos devem estar registrados no Intune

Definir configurações gerais de conformidade

- Habilitar dispositivos marcados sem política atribuída
- Detecção aprimorada de jailbreak
- Status de conformidade para dispositivos que não informam

Você pode implantar a política de conformidade para usuários em grupos de usuários ou dispositivos em grupos de dispositivos.



Explore o acesso condicional

- Fornece acesso granular aos recursos baseado em políticas
- Permite que os usuários trabalhem praticamente de qualquer lugar na maioria dos dispositivos, ajudando a manter a segurança
- Requer Intune e Azure AD (Entra ID) para dispositivos móveis
- Orienta o usuário na correção de uma solicitação de acesso negado
- Os cenários comuns para acesso condicional são:
  - Acesso condicional baseado em aplicativo
  - Acesso condicional baseado em rede
  - Acesso condicional baseado na confiança do dispositivo

TFTEC CLOUD

Crie políticas de acesso condicional

- Você usa condições e controles para criar políticas de acesso condicional.
- As condições podem ser baseadas em:
  - Plataforma do dispositivo que está acessando os dados
  - Local de onde os dados estão sendo acessados
  - Aplicativos clientes usados para acessar os dados
- Os controles incluem:
  - Bloqueando acesso
  - Conceder acesso se um ou mais requisitos adicionais forem atendidos
- Configure o acesso condicional a partir da consola do Intune no centro de administração do Microsoft Intune, incluindo um controlo mais granular, como:
  - Permitir ou bloquear determinadas plataformas
  - Bloqueie imediatamente dispositivos que não são gerenciados pelo Intune

TFTEC CLOUD

Gerar relatórios de inventário e conformidade

TFTEC CLOUD

Relatar o inventário de dispositivos registrados no Intune

Você pode baixar relatórios (formato csv) para todos os seus dispositivos e aplicativos no Portal do Intune

Você também pode baixar logs de auditoria que fornecem um registro das atividades que geram uma alteração no Intune.

Para relatórios mais ricos:

- Usar o Data Warehouse do Intune e o Power BI
- A API Microsoft Graph permite acessar todos os dados do Intune
  - Crie relatórios usando Power BI ou Excel com base nos dados
  - O Microsoft Graph também permite criar scripts de quase tudo no Azure AD (Entra ID) e no Intune

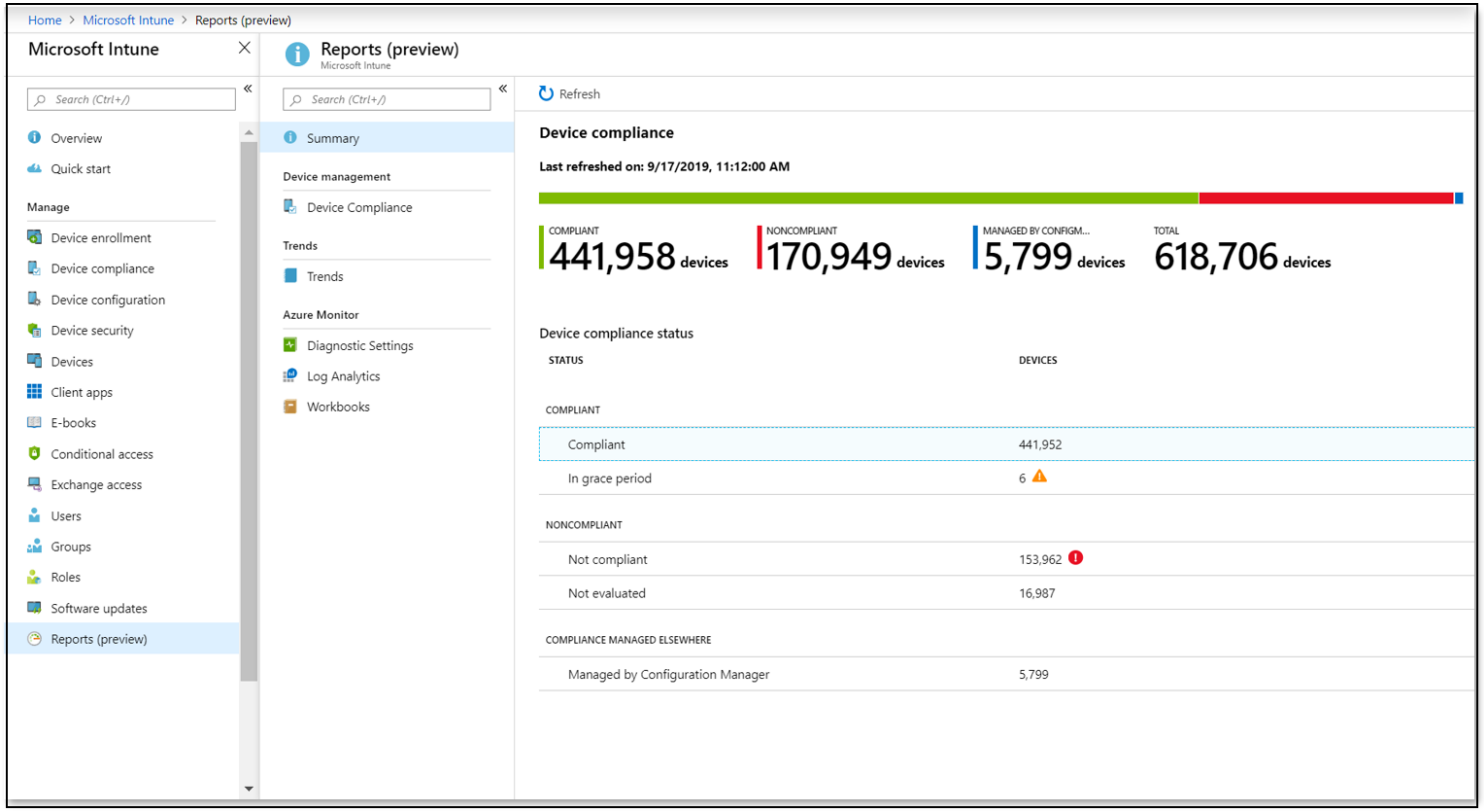
TFTEC CLOUD

Monitore e relate a conformidade do dispositivo

Você pode realizar o monitoramento básico de dispositivos no Intune

Conformidade do dispositivo

- Resumo e visualizações agregadas
- Selecione filtros e defina critérios de pesquisa
- Ver dispositivos individuais
- Veja as tendências de conformidade do dispositivo ao longo do tempo



TFTEC CLOUD

Crie relatórios de inventário personalizados do Intune

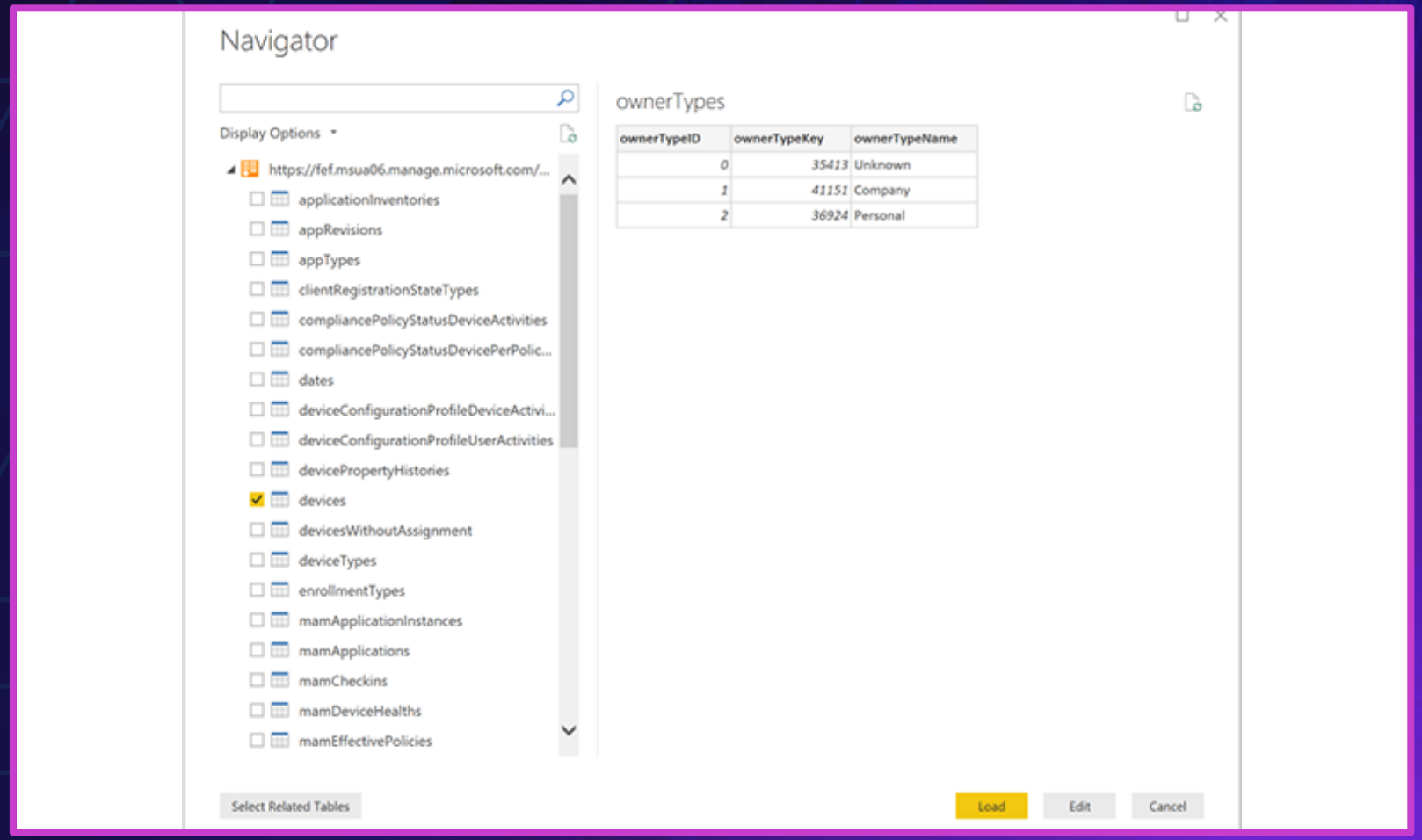
O Data Warehouse do Intune armazena dados históricos do Intune

Use o Power BI para carregar dados e gerar relatórios

- Importar arquivo do Power BI
- Conecte-se aos dados usando o link OData

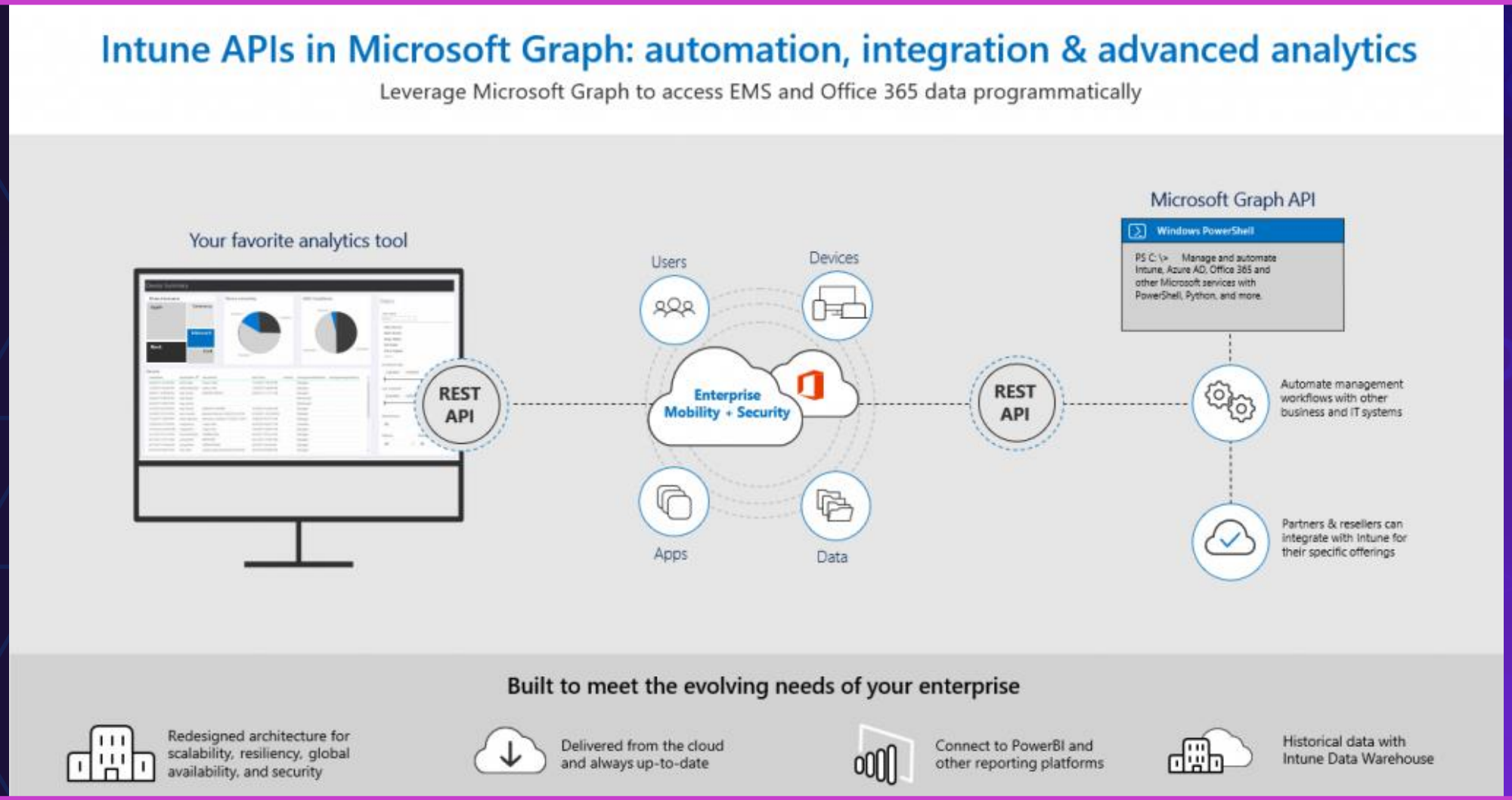
Usar o aplicativo Conformidade do Power BI Intune

- Utiliza a versão web do Power BI e permite a personalização e o compartilhamento de relatórios pré-configurados com foco em relatórios de conformidade de dispositivos



TFTEC CLOUD

Acessando o Intune usando a API do Microsoft Graph



TFTEC CLOUD

Laboratórios

TFTEC CLOUD

Lab 01

TASK01:

- Implantar o Windows Hello for Business
- Configurar o Microsoft Entra ID Protection
- Implementar autenticação multifator
- Configurar a redefinição de senha de autoatendimento (SSPR)

TFTEC CLOUD

Lab 02

TASK02:

- Implantar políticas de conformidade para dispositivos Windows
- Implantar políticas de conformidade para dispositivos Android
- Criar política de acesso condicional - Exigir que o dispositivo esteja em compliance

TFTEC CLOUD

Lab 03

TASK03:

- Relatórios Microsoft Intune

TFTEC CLOUD

Obrigado

TFTEC CLOUD