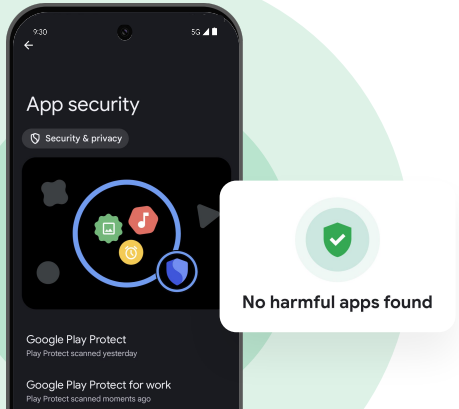
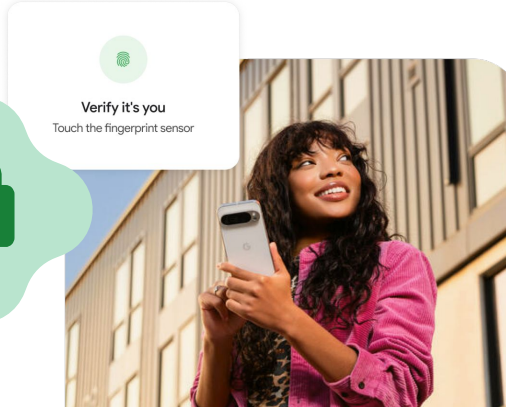
Android

Guia de segurança em dispositivos móveis para PMEs





Visão geral

Para pequenas empresas, implementar uma segurança de dados reforçada é essencial. De acordo com a Hiscox[1], 25% das pequenas empresas têm que fechar as portas após uma violação de segurança, que tem custo médio de US$ 200 mil.

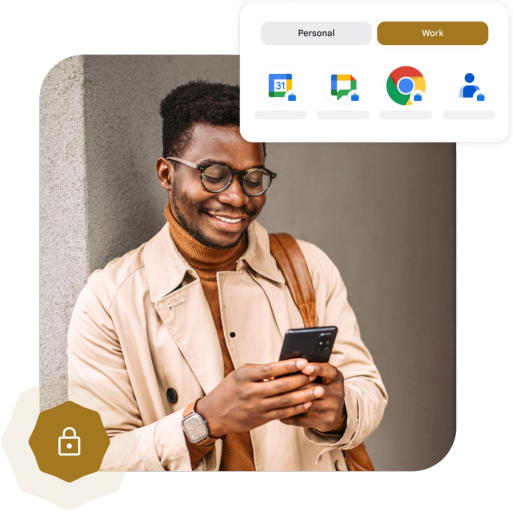
No mundo hiperconectado de hoje, smartphones e tablets são uma ferramenta poderosa, mas também um risco de segurança se não forem gerenciados corretamente.

O phishing é uma das maiores ameaças aos usuários de dispositivos móveis, que são o alvo de 83% dos sites de phishing[2]. Os invasores agora usam a IA para criar ataques sofisticados, que enganam até mesmo usuários experientes.

Gerenciar todo o ciclo de vida dos dispositivos corporativos e garantir a segurança e a privacidade dos dados da empresa e dos funcionários pode parecer complexo. Mas com as ferramentas certas, tudo fica mais simples e prático.

As proteções simples e discretas do Android ajudam a blindar os dispositivos e dados da empresa e a combater os ataques de phishing. Isso é fundamental para as empresas que não têm suporte de TI dedicado a proteger e gerenciar dispositivos.

Neste guia, compartilhamos práticas recomendadas para manter a segurança dos seus dados corporativos e reforçamos os aspectos que tornam o Android uma plataforma tão sólida e segura.



[1] Hiscox Cyber Readiness Report (Relatório de preparação cibernética da Hiscox, em tradução livre).
[2] Zimperium's 2024 Global Mobile Threat Report (Relatório global sobre ameaças em dispositivos móveis da Zimperium de 2024, em tradução livre).

Conheça os modelos de registro de dispositivos Android

As empresas podem escolher entre três caminhos, ou modelos, para proteger dispositivos e dados. Cada modelo aumenta o controle que as equipes de TI têm sobre um dispositivo.

01

O primeiro modelo, que não tem gerenciamento de mobilidade empresarial (EMM) nem funções de gerenciamento, é classificado como “iniciado pelo usuário”. A equipe de TI da empresa orienta usuários sobre práticas recomendadas ao configurar algumas definições de segurança e privacidade em seus dispositivos.

02

O segundo modelo, Device Trust do Android Enterprise, é baseado em zero trust para oferecer uma segurança reforçada. Com essa abordagem, os provedores de soluções de confiança podem inspecionar melhor o estado de segurança de um dispositivo, sendo ou não gerenciado por EMM. Isso inclui um amplo conjunto de soluções, como provedores de identidade (IdPs), defesa contra ameaças para dispositivos móveis (MTD), detecção e resposta empresarial (EDR, na sigla em inglês) e provedores de rede privada virtual (VPNs). Integradas ao Android Enterprise, essas soluções podem verificar se os critérios do dispositivo são atendidos antes de dar acesso aos recursos da empresa.

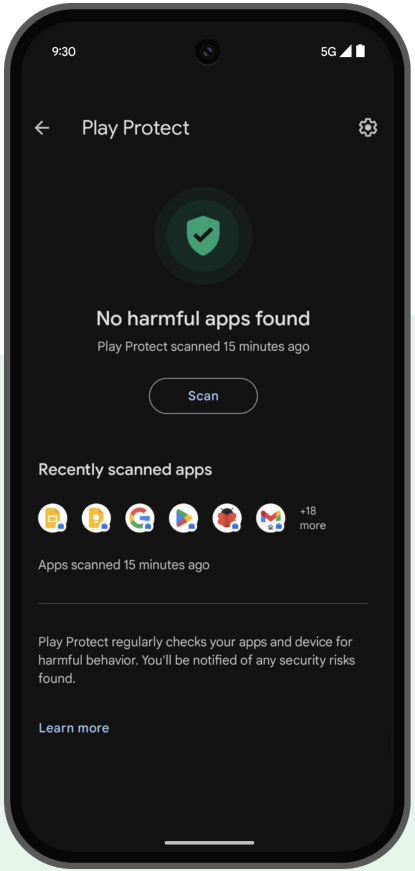
03

O terceiro modelo depende dos controles de EMM. Eles permitem que as organizações exerçam maior controle sobre os dispositivos, sejam eles da empresa ou de um programa de BYOD. Para dispositivos pessoais, a empresa registra um perfil de trabalho, que é todo controlado pela TI, preservando a privacidade da área do usuário.

O Android Enterprise oferece vários modelos de registro de dispositivos para atender às exigências dos clientes de PMEs

Cada modelo amplia as capacidades do anterior para proporcionar flexibilidade às PMEs, e todos podem ser usados juntos de acordo com as demandas da empresa. Ao usar os recursos de segurança avançados do Android e implementar as práticas recomendadas a seguir, sua empresa poderá operar com confiança no ambiente de dispositivos móveis.

Além do compromisso com os avanços em segurança, com o Android você tem flexibilidade e custo-benefício, sendo a melhor opção para pequenas e médias empresas.



Políticas e configurações de segurança recomendadas para modelos de registro

Orientações específicas para os modelos: iniciado pelo usuário, Device Trust e EMM.

Cada um é voltado para um nível específico de privacidade do usuário e de controle da empresa, com base nos seus requisitos.

01 Configurações de segurança iniciadas pelo usuário

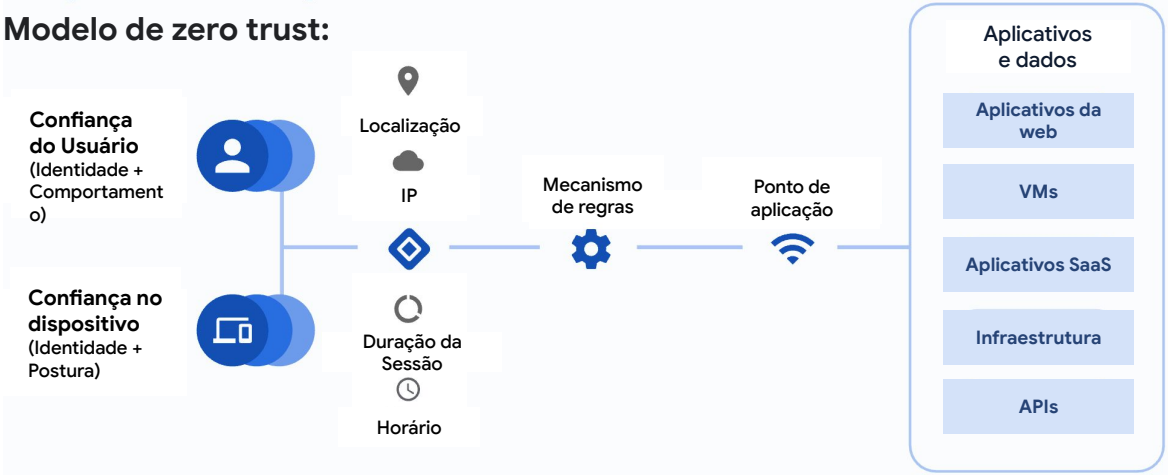
Para garantir a segurança de seus dados e da empresa, a equipe de TI fornecerá instruções detalhadas sobre a configuração manual destas opções nos dispositivos Android.

- Ativar o Bloqueio por detecção de roubo
- Ativar o Bloqueio remoto
- Ativar o Bloqueio de dispositivo off-line
- Ativar a Confirmação de identidade
- Ativar o Espaço privado
- Definir um PIN ou senha com pelo menos 6 caracteres que não se repetem
- Garantir a ativação do Google Play Protect
- Instalar apps apenas da Google Play Store

02 Modelo de zero trust

Além dos controles e restrições disponíveis com o Device Trust do Android Enterprise, o departamento de TI também precisa instruir os usuários a configurar e aproveitar todos os recursos de segurança iniciados por eles, conforme a seção 1.

Modelo de zero trust:



Veja a lista a seguir para decidir quais verificações implementar antes de permitir o acesso aos recursos da empresa. A escolha das configurações vai depender dos parceiros do Device Trust, então consulte a documentação deles.

02 Device Trust do Android Enterprise

Veja a lista a seguir para decidir quais verificações implementar antes de permitir o acesso aos recursos da empresa. A escolha das configurações vai depender dos parceiros do Device Trust, então consulte a documentação deles.

Indicador	Descrição
Modelo ou marca do dispositivo	Retorna o modelo e a marca do dispositivo.
Estado de gerenciamento	Retorna o gerenciamento e o app de gerenciamento.
Estado da rede	Retorna informações sobre todas as redes ativas no dispositivo.
Nível do patch de segurança do dispositivo	Retorna o nível atual do patch de segurança do dispositivo (incluindo o nível do patch da atualização do sistema do Google Play).
Nível do patch de segurança publicado	Retorna o nível do patch de segurança publicado pelo Google para o componente atualizável correspondente no dispositivo.*
Status de criptografia do disco	Retorna se o armazenamento do dispositivo está criptografado.
Versão do SO e OTA pendente	Retorna a versão do SO do dispositivo e se há uma atualização pendente do SO disponível.
Verificação de bloqueio de tela e de sua qualidade	Retorna a complexidade do bloqueio de tela atual do usuário.
Status do Play Protect	Retorna se o Google Play Protect está ativado.

03 Ativado por políticas de EMM

Os admins de TI podem consultar a documentação do EMM para saber como configurar esses conjuntos mínimos de políticas para proteger os usuários. Usando um EMM, o departamento de TI pode configurar dispositivos como BYOD, corporativos habilitados para uso pessoal (COPE, na sigla em inglês) ou totalmente gerenciados. Tanto o perfil de trabalho quanto o COPE oferecem controle à empresa, mas o COPE fornece mais controle sobre todo o dispositivo. Confira alguns exemplos de controles de segurança que devem ser considerados:

- Tamanho mínimo da senha = 6 caracteres
- Número máximo de tentativas para desbloquear o dispositivo = 10
- Ativar a Play Integrity
- Desativar as capturas de tela
- Não permitir a inclusão de contas no perfil de trabalho
- Desativar as Opções do desenvolvedor
- Não permitir a instalação de fontes desconhecidas
- Desativar ações de copiar/colar entre perfis
- Não permitir o Android Debug Bridge (ADB)
- Usar o Google Play gerenciado com listas de permissões
- Chrome: impedir a desativação da Navegação segura

Práticas recomendadas para implantar dispositivos Android na sua empresa

01 Instrua os funcionários a ativar os recursos de segurança integrados

Prática recomendada

Proteja seus dados contra ladrões e acessos não autorizados. Use os recursos integrados feitos para manter a segurança das informações da empresa confidenciais. São eles:

A

Ative o Bloqueio por detecção de roubo. Usando a IA, os sensores de movimento do dispositivo, o Wi-Fi e o Bluetooth, ele detecta quando o aparelho é tomado de forma brusca, efetuando o bloqueio automático.

B

Ative e use o Bloqueio remoto. Se o dispositivo for perdido ou roubado, use o Bloqueio remoto com um número de telefone verificado para ativar rapidamente o bloqueio de tela.

C

Ative o bloqueio de dispositivo off-line. Assim que o dispositivo ficar off-line, a tela será bloqueada automaticamente para proteger seus dados. Por exemplo, se alguém roubar seu smartphone e desligar a Internet para impedir que você o localize com o Encontre Meu Dispositivo, o aparelho será bloqueado depois de ficar off-line por um curto período.

01 Instrua os funcionários a ativar os recursos de segurança integrados

Prática recomendada

Proteja seus dados contra ladrões e acessos não autorizados. Use os recursos integrados feitos para manter a segurança das informações da empresa confidenciais. São eles:

D

Ative a confirmação de identidade. Ela exige a biometria e outras salvaguardas. Sua identidade é verificada quando você realiza ações sensíveis no dispositivo ou faz mudanças na sua Conta do Google fora de lugares de confiança.

E

Oculte apps sensíveis com o espaço privado. O Android oferece esse recurso para proteger seus aplicativos particulares contra acessos não autorizados. É criada uma área separada e oculta no dispositivo para você organizar seus apps pessoais. Mesmo que seu smartphone desbloqueado caia nas mãos erradas, seus aplicativos sensíveis no espaço privado vão permanecer protegidos.

F

O Google também integrou recursos contra phishing diretamente ao Google Mensagens para proteger os usuários de técnicas sofisticadas. Além disso, há novos recursos, como a proteção contra spam e o identificador de chamadas do Android, que aumentam ainda mais a proteção dos usuários.

02 Use o diretório de soluções do Android Enterprise Recommended

Prática recomendada

Crie uma lista de dispositivos aprovados para uso no trabalho com base no diretório de soluções do Android Enterprise Recommended.

Os dispositivos no diretório de soluções passam por testes de segurança rigorosos e recebem atualizações oportunas.

A validação do Android Enterprise Recommended garante que sua empresa tenha dispositivos com melhorias de segurança integradas e recursos otimizados para as demandas empresariais.

03 Implante uma solução de gerenciamento de dispositivos para ter controle centralizado

Prática recomendada

Use uma solução de EMM para aplicar políticas de segurança, apagar/bloquear dispositivos remotamente e gerenciar instalações de aplicativos. Para ver uma lista de parceiros validados e aprovados, acesse o diretório de soluções de EMM do Android Enterprise Recommended.

A integração profunda do Android com as soluções de EMM permite um controle granular e um gerenciamento eficiente da segurança para empresas de qualquer tamanho.

04 Garanta atualizações de segurança oportunas

Prática recomendada

Com um EMM, use as políticas de dispositivos do Android Enterprise para garantir que eles estejam atualizados com os patches de segurança mais recentes do Android. O Android Enterprise oferece aos admins opções para aplicar políticas de atualização de SO e de aplicativos conforme as demandas da empresa.

O Android se comprometeu a fazer atualizações de segurança regulares a cada 30 dias. Assim, o ecossistema de fabricantes de dispositivos e operadoras pode entregar atualizações rapidamente. Além disso, se você selecionar dispositivos do diretório de soluções, eles precisarão receber atualizações pelo menos a cada 90 dias. Fabricantes de dispositivos, como o Pixel e a Samsung, agora oferecem atualizações de SO e de segurança durante sete anos. Isso ajuda a garantir que as possíveis vulnerabilidades sejam corrigidas com rapidez.

05 Implemente uma autenticação forte

Prática recomendada

Os controles do Android Enterprise permitem a definição de requisitos para as senhas de desbloqueio dos dispositivos. Isso inclui PINs, padrões e senhas que podem ser combinados com opções de desbloqueio facial e por impressão digital. Os admins podem fazer com que os usuários definam requisitos específicos que atendam às demandas da organização. Exija pelo menos seis dígitos com caracteres não repetidos, de acordo com as diretrizes mais recentes do NIST SP 800-53.

O suporte biométrico do Android, aliado ao armazenamento seguro de chaves, oferece aos usuários uma experiência perfeita. Ele ajuda a proteger seu dispositivo com uma autenticação segura e robusta com suporte de hardware.

06 Implante e gerencie aplicativos com segurança

Prática recomendada

Permita que os usuários instalem aplicativos apenas da Google Play Store e exija que o Google Play Protect esteja sempre ativado. Com o Google Play gerenciado, os admins podem reunir uma lista de apps aprovados e definir permissões.

O Google Play gerenciado impede o sideload de apps não aprovados, e o Google Play Protect verifica ativamente a presença de malware em todos os aplicativos instalados.

07 Proteja os dados em trânsito

Prática recomendada

Use VPNs para ter conexões seguras com os serviços empresariais quando estiver fora do escritório. Verifique se todos os serviços estão usando HTTPS e configure corretamente as conexões Wi-Fi com a rede da sua empresa.

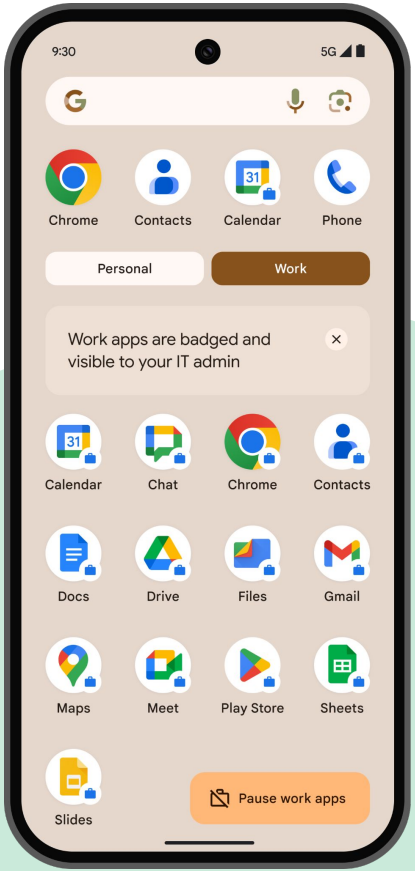
A criptografia integrada e o suporte a VPN do Android ajudam a garantir que seus dados estejam protegidos, seja no dispositivo ou transmitidos pela rede.

08 Use o perfil de trabalho do Android

Prática recomendada

Se os funcionários usarem dispositivos pessoais (BYOD), os admins devem implementar um perfil de trabalho para separar os dados pessoais e profissionais em um único dispositivo.

O perfil de trabalho, um recurso exclusivo do Android, cria um ambiente seguro e isolado para garantir a segurança dos dados comerciais e a privacidade dos dados pessoais.



Principais conclusões

Para reduzir chamados para o departamento de TI/help desk, é fundamental treinar os usuários e oferecer orientações claras de configuração para cada um dos três modelos.

Consulte o diretório de soluções do Android Enterprise para ver uma seleção de dispositivos e parceiros aprovados. Esse recurso pode ajudar você a escolher os produtos mais adequados com base nos seus requisitos específicos.

Priorize a implementação da segurança, mesmo que seja uma abordagem básica. A proteção dos dispositivos de trabalho envolve custos para cada modelo. Escolha um que equilibre a segurança necessária com as despesas de implementação e manutenção.

Android

Saiba mais em

www.android.com/enterprise/security