MOTOTRBO ION

SEGURANÇA ION

O MOTOTRBO™ Ion ajuda você a ficar protegido contra ameaças cibernéticas. Uma abordagem de defesa em profundidade fornece várias camadas de segurança para ajudar a impedir o acesso não autorizado a dispositivos e atividades maliciosas, e para proteger seus dados críticos. Com o mais alto nível de segurança de dispositivo e rede, combinado com monitoramento de ameaças em tempo real, o Ion permite que você use dados e aplicativos Android com confiança - mesmo em redes públicas.

SEGURANÇA DO DISPOSITIVO PARA EVITAR ACESSO NÃO AUTORIZADO

O MOTOTRBO ION AJUDA A EVITAR QUE O CÓDIGO HOSTIL EXECUTE NO DISPOSITIVO E QUE OS USUÁRIOS NÃO AUTORIZADOS OBTENHAM ACESSO.

AMBIENTE DE EXECUÇÃO CONFIÁVEL (TEE)

Um TEE fornece segurança ponta a ponta, implementando a tecnologia TrustZone da ARM e lida com funções e serviços essenciais. Ele roda no mesmo processador do sistema operacional Android, mas está completamente isolado do resto do sistema. Este isolamento garante que os dados críticos sejam armazenados, processados e protegidos em um ambiente seguro.

FIRMWARE DE CONFIANÇA

Um processo de inicialização segura verifica a integridade do firmware e do software. Com a inicialização segura, cada estágio do processo de inicialização é assinado criptograficamente com chaves aprovadas, o que evita ataques maliciosos e atualizações de software não autorizadas, proporcionando um lançamento de sistema operacional seguro e protegido.

O SISTEMA ANDROID KEYSTORE

O Android Keystore impede o uso não autorizado de chaves criptográficas. Além disso, os aplicativos devem especificar os usos autorizados de suas chaves e aplicar essas restrições fora dos processos dos aplicativos, fornecendo mais restrições sobre como e quando as chaves são usadas.

SEGURANÇA DE ACESSO AO DISPOSITIVO

Mecanismos de autenticação de fator único e multifatorial são suportados no MOTOTRBO Ion - de PIN simples a outros fatores de autenticação, como senha, padrão, etc.
Os usuários válidos terão acesso apenas aos dados, aplicativos e serviços para os quais os usuários estão autorizados.

A ESTRUTURA DE SEGURANÇA DO NIST

Todos os sistemas e dispositivos MOTOTRBO aderem estritamente à estrutura de segurança cibernética do NIST.

As práticas de segurança do NIST são baseadas em monitoramento contínuo, diagnóstico, opções de mitigação e remediação. Usamos uma abordagem baseada em risco em todo o nosso ciclo de vida de desenvolvimento, implementação e suporte operacional de produtos. Nossos controles baseados em proteção e resposta são desenvolvidos em consulta com especialistas, processos e tecnologias líderes do setor.

MOTOROLA SOLUTIONS

SEGURANÇA DE APLICATIVOS PARA EVITAR ATIVIDADE MALICIOSA

O MOTOTRBO ION PERMITE UMA OPERAÇÃO SEGURA, AJUDANDO A EVITAR MALWARE, PHISHING E OUTRAS ATIVIDADES MALICIOSAS.

GERENCIAMENTO DE DISPOSITIVOS MÓVEIS E GOOGLE PLAY GERENCIADO

As políticas de segurança do dispositivo, incluindo gerenciamento de aplicativos, são melhor implementadas usando uma solução de gerenciamento de dispositivos móveis (MDM). Os administradores de TI, que normalmente são responsáveis pela configuração e gerenciamento desses dispositivos, podem usar um MDM para definir e definir políticas para o uso de aplicativos, criando uma estrutura de gerenciamento de aplicativos segura e personalizada para suas necessidades específicas.

A chave para esta implementação é o Android Enterprise e a estrutura Managed Google Play, que fornece APIs para fornecedores de MDM para gerenciar aplicativos em dispositivos Android. Isso se aplica a aplicativos públicos disponíveis na Google Play Store e aplicativos privados desenvolvidos para uso corporativo.

Por meio de MDMs, os administradores de TI podem:

- Distribuir aplicativos aprovados remotamente por meio da Managed Google Play Store e bloquear aplicativos maliciosos ou remover aplicativos
- Definir e habilitar/desabilitar o acesso ao aplicativo para usuários, dependendo de seu perfil
- Configurar notificações em tempo real sobre o uso do dispositivo para monitorar atividades maliciosas ou não conformidade com as políticas de segurança

PROTEÇÃO DO GOOGLE PLAY

O Google Play Protect é um poderoso serviço de detecção de ameaças integrado à Google Play Store, que verifica ativamente 24 horas por dia, 7 dias por semana, em busca de aplicativos prejudiciais e protege os dispositivos, seus dados e aplicativos contra malware. Os usuários são notificados após a detecção de aplicativos que contêm malware. O Google Play Protect também pode remover ou desativar aplicativos maliciosos automaticamente como parte de sua iniciativa de prevenção e usar as informações que coleta para melhorar a detecção de Aplicativos Potencialmente Nocivos (PHAs).
Além disso, o usuário também pode optar por enviar aplicativos desconhecidos ao Google para análise.

SAFETYNET

SafetyNet é um conjunto de serviços e APIs que os desenvolvedores podem usar para proteger aplicativos contra ameaças de segurança e mitigar contra adulteração de dispositivos, URLs ruins, PHAs e usuários falsos.

ASSINATURA DE APLICAÇÃO

O Android exige que todos os aplicativos sejam assinados digitalmente com uma chave de desenvolvedor antes da instalação e usa o certificado correspondente para identificar o autor do aplicativo. Quando o sistema instala uma atualização para um aplicativo, ele compara o certificado na nova versão com a versão existente e só permite a atualização se o certificado corresponder.

SEGURANÇA DE DADOS PARA PROTEGER DADOS CRÍTICOS

MOTOTRBO ION PROTEGE DADOS CRÍTICOS, EM REPOUSO E EM TRÂNSITO.

SEGURANÇA DE DADOS EM REPOUSO

ARMAZENAMENTO SEGURO

Credenciais, certificados e chaves são armazenados com segurança em armazenamento confiável com suporte de hardware no dispositivo.

MANUSEIO DE CERTIFICADO

As autoridades de certificação são essenciais para fornecer comunicações seguras em uma rede usando a infraestrutura de chave pública. Com o Android 7.0 e superior, todos os dispositivos compatíveis, incluindo o MOTOTRBO Ion, implementarão apenas as autoridades de certificação do sistema padronizado mantidas no AOSP. Todos os dispositivos Ion serão enviados com o mesmo armazenamento de autoridade de certificação.

PERFIL DE TRABALHO

Para dispositivos de propriedade da empresa, os administradores de TI podem implementar uma das duas opções de implantação para gerenciar os dados corporativos nesses dispositivos:

- Dispositivo totalmente gerenciado no qual o dispositivo é usado exclusivamente para fins de trabalho. Os administradores de TI podem aplicar toda a gama de políticas de gerenciamento a todo o dispositivo
- Opção de perfil de trabalho totalmente gerenciado, em que o dispositivo suporta o perfil de trabalho e um perfil pessoal simultaneamente

Na segunda opção, o perfil de trabalho cria um perfil separado e autocontido que contém aplicativos e dados corporativos e os isola de aplicativos e dados pessoais. Usando o MDM, as políticas do dispositivo podem ser configuradas para impedir o compartilhamento de arquivos e dados do perfil de trabalho.

POLÍTICAS DE DISPOSITIVO

O dispositivo pode ser configurado usando MDM para impedir ou restringir a transferência de dados de / para o dispositivo, como:

- Impedir a transferência de arquivos usando Bluetooth
- Impedir a transferência de arquivos do dispositivo via USB
- Impedir o acesso a armazenamento externo, como cartão SD
- Impedir a montagem de mídia externa física
- Proibir o acesso a recursos de depuração
- Definir políticas de senha de dispositivo
- Desativar a câmera
- Desativar a captura de tela
- Permitir a instalação de aplicativos de fontes conhecidas, como a Google Play Store

SEGURANÇA DE DADOS EM TRÂNSITO

O Ion implementa os protocolos seguros padrão da indústria usados para dados em trânsito, como SRTP, HTTPS, etc. Protocolos padrão da indústria disponíveis e requisitos de segurança para interfaces de conectividade como WiFi, USB, BlueTooth e VPN foram implementados. Além disso, o Android fornece comunicações seguras pela Internet para navegação na web, e-mail, mensagens instantâneas e outros aplicativos da Internet, com suporte para Transport Layer Security (TLS).

WI-FI

O Android 10 é compatível com os padrões Wi-Fi Protected Access versão 3 (WPA3) e Wi-Fi Enhanced Open da Wi-Fi Alliance, que melhoram a segurança geral do Wi-Fi ao fornecer melhor privacidade e robustez contra ataques conhecidos.

VPN

O Android oferece suporte para conexão segura a uma rede corporativa usando VPN.

MEDIDAS ADICIONAIS DE SEGURANÇA

ATUALIZAÇÕES DE SEGURANÇA PARA ANDROID

Todos os meses, o Google publica Boletins de Segurança do Android para atualizar usuários, parceiros e clientes sobre as últimas correções. Essas atualizações de segurança estão disponíveis para versões do Android por três anos a partir da data de lançamento.

PROGRAMA ANDROID ENTERPRISE RECOMMENDED

O programa Android Enterprise Recommended do Google fornece um conjunto de especificações para dispositivos e serviços empresariais para desempenho de hardware, implantação, atualizações de segurança e experiência do usuário. Isso inclui atualizações de segurança que são entregues aos dispositivos dentro de 90 dias do lançamento do Google. Além disso, os OEMs recebem um nível avançado de suporte técnico e treinamento.

PADRÕES E CERTIFICAÇÕES DO SETOR

O Android Enterprise recebeu a certificação ISO 27001 e relatórios SOC 2 e 3 para práticas e procedimentos de segurança da informação para Android Management API, registro sem toque e Google Play gerenciado.
Essa designação garante que esses serviços atendam aos rígidos padrões da indústria para segurança e privacidade.

As certificações incluem:

- FIPS 140-2 CAVP
- Critérios Comuns/Perfil de Proteção Fundamentos de Dispositivos Móveis NIAP
- Guia de implementação técnica de segurança DISA (STIG)
- Regulamento Geral de Proteção de Dados (GDPR)

Para mais informações, visite
motorolasolutions.com/ion

MOTOROLA SOLUTIONS

MOTOTRBO ION

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. 800-367-2346 motorolasolutions.com