ShieldiT Black: Segurança máxima para celulares

A Avitec apresenta o ShieldiT Black, uma solução de segurança fortificada projetada para proteger dados e comunicações confidenciais em ambientes de alto risco.

Com o ShieldiT Black você consegue:

1. **Evitar extração de dados via qualquer solução forense (Por exemplo UFED, XRY, Oxigem, MobileEdit, etc)**
2. **Evitar qualquer tipo de intrusão ao seu celular**
3. **Fazer ligações seguras entre portadores da mesma solução ou que possuem o aplicativo ShieldiT nos seus celulares**
4. **Trocar informação via Chat ou arquivos de uma forma 100% segura**

Quando um usuário recebe um telefone com ShieldiT Black, ele vem pré-configurado com todos os recursos de segurança aprimorados. Veja o que o usuário pode esperar:

Principais recursos do ShieldiT

O **ShieldiT Black** foi projetado para proteger dispositivos móveis e comunicações contra ameaças avançadas com os seguintes recursos principais:

Comunicações criptografadas: a tecnologia VoIP segura garante chamadas de voz e vídeo privadas. A criptografia de ponta a ponta protege mensagens de texto, arquivos e mídia, incluindo chamadas em grupo e conferências.

Segurança de dispositivos móveis: detecção de ameaças em tempo real com recursos antimalware. A detecção de movimento e o rastreamento de dispositivos impedem acesso não autorizado. O gerenciamento de vulnerabilidades do sistema operacional identifica e corrige vulnerabilidades do sistema.

Sistema de gestão abrangente: Oferece opções de gestão flexíveis com monitoramento em tempo real da atividade dos usuários. Integra-se perfeitamente aos sistemas de TI existentes, incluindo sincronização com diretórios de usuários.

Backbone de rede seguro: suporta chamadas PSTN criptografadas por meio de gateways seguros, permitindo transferências e armazenamento de arquivos grandes e criptografados. Utiliza TLS 1.2 para garantir a comunicação segura entre os componentes do servidor.

Detecção de Rede Neural Patenteada: Técnicas avançadas de detecção identificam ameaças de dia zero. Monitora chamadas de sistema e rede em busca de anomalias, fornecendo defesa proativa.

Certificado ISO 27001: Adesão aos padrões internacionais de segurança, garantindo conformidade e proteção de dados.

Caracteristicas avançadas do ShieldiT Black

O ShieldiT Black inclui vários recursos avançados para fornecer um nível de segurança incomparável:

Aplicativo ShieldiT não removível: O aplicativo ShieldiT é incorporado ao firmware do sistema, dificultando sua desinstalação ou desativação. Mesmo que o aplicativo seja removido, ele será reinstalado imediatamente. Quaisquer modificações no aplicativo exigem autorização para garantir que os protocolos de segurança permaneçam intactos.

Perfil seguro para aplicativos corporativos: Uma partição criptografada dedicada no dispositivo é reservada para aplicativos corporativos. Esse perfil seguro garante que os dados e aplicativos corporativos sejam isolados do uso pessoal, permitindo apenas aplicativos aprovados. Medidas de segurança aprimoradas, como criptografia de dados, bloqueio de tela e apagamento remoto, garantem a proteção dos dados.

Gerenciamento de Senhas e Chaves: Aplica políticas de senha complexas para garantir senhas fortes e seguras. Gerencia chaves de criptografia com segurança, adicionando uma camada extra de proteção para dados confidenciais.

Proteção Anti-UFED: Utiliza medidas avançadas para impedir a extração não autorizada de dados, controlando as políticas de acesso à porta USB e implementando mecanismos de criptografia reforçados, garantindo que os dados permaneçam seguros contra tentativas de extração física.

Controles de compartilhamento de dados: Restringe o compartilhamento de dados entre aplicativos corporativos e pessoais, impedindo transferências não autorizadas de dados. Políticas rígidas regem a exportação e importação de dados para manter a integridade dos dados.

Perfil seguro para aplicativos corporativos: Uma partição criptografada dedicada no dispositivo é reservada para aplicativos corporativos. Esse perfil seguro garante que os dados e aplicativos corporativos sejam isolados do uso pessoal, permitindo apenas aplicativos aprovados. Medidas de segurança aprimoradas, como criptografia de dados, bloqueio de tela e apagamento remoto, garantem a proteção dos dados.

Preparação e operação

O ShieldiT Black já vem pré-instalado e configurado com todos os recursos de segurança:

Preparação do dispositivo: O ShieldiT Black e todos os seus recursos de segurança são pré-instalados.

Configuração: O telefone é configurado para aplicar políticas de segurança, gerenciar instalações de aplicativos e receber atualizações, garantindo a conformidade com os padrões de segurança corporativa.

Gerenciamento contínuo: o sistema monitora continuamente o telefone para verificar a conformidade, envia atualizações e aplica políticas para manter o dispositivo seguro e atualizado com as medidas de segurança mais recentes.