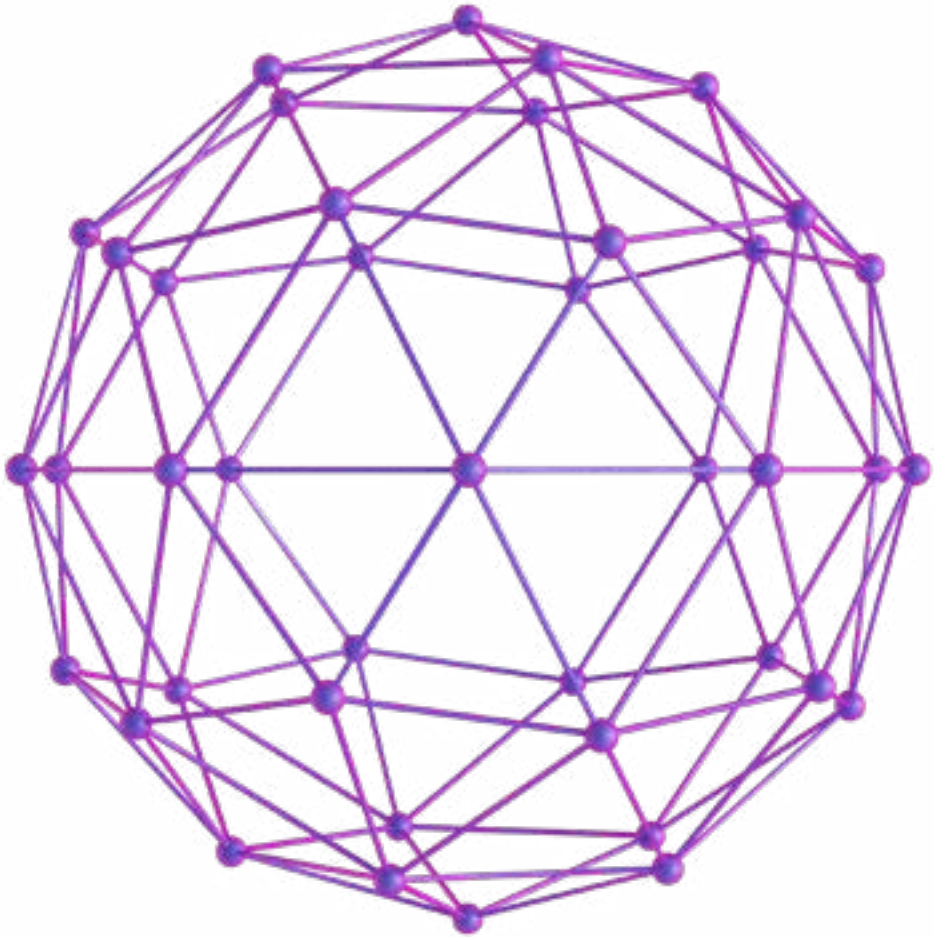
Os Pilares da Segurança na IoT

pronnus® tecnologia



A Internet das Coisas (IoT) está transformando a forma como nos conectamos com o mundo ao nosso redor, viabilizando a coleta e o envio de dados por meio de uma ampla variedade de dispositivos. Contudo, à medida que essa tecnologia evolui, surgem também questões importantes relacionadas à segurança.

Então, como os especialistas em segurança podem analisar o cenário de ameaças de IoT e estabelecer uma solução que seja não apenas suficientemente ampla para lidar com esses desafios, mas também adaptável suficiente para expandir no futuro?

A seguir, serão apresentados os elementos fundamentais que constituem uma solução de segurança para IoT, bem como maneiras de proteger dispositivos e redes contra riscos emergentes.

De Olho nas Ameaças da IoT
Definindo Requisitos para uma Solução Eficaz

À medida que a IoT expande a superfície de ataque, surgem quatro riscos fundamentais que os profissionais de segurança devem considerar:

1. Vulnerabilidades

Dispositivos IoT muitas vezes não são projetados com segurança. A falta de capacidade para executar atualizações ou implementar protocolos de segurança torna esses dispositivos alvos fáceis para ataques. Por exemplo, uma empresa jamais imaginaria que uma impressora ou um termostato poderiam estar envolvidos em um ataque de botnet, mas isso já aconteceu.

2. Comunicações Não Seguras

Muitos dispositivos IoT se comunicam sem criptografia, especialmente em redes públicas. Além disso, dispositivos que utilizam Bluetooth são um ponto de atenção: o tráfego não monitorado aumenta o risco de dados serem interceptados.

3. Vazamento de Dados

Os dispositivos IoT podem servir como pontos de entrada e saída não monitorados para a rede, permitindo que dados sensíveis sejam vazados sem detecção. Políticas definidas para prevenir vazamentos de dados podem falhar ao sinalizar dados que passam por esses dispositivos.

4. Infecções por Malware

Dispositivos não seguros podem ser infectados com malware, que se propaga pelo meio. Uma vez na rede, o malware se espalha de dispositivo para dispositivo rapidamente.

Definindo seus requisitos

- Você sabe como implementar uma solução para identificar, categorizar e gerenciar novos dispositivos?
- Você está definindo seus requisitos de segurança IoT com exposições de acesso em mente, como Wi-Fi público?
- Como sua solução aplicará e fará cumprir políticas para dispositivos que podem não estar sob seu controle?
- Você é capaz de segmentar recursos críticos na rede para que eles só acessem os dispositivos que devem acessar?

Áreas-Chave para Abordagem Estratégica

Para gerenciar os riscos, profissionais de segurança devem ter um certo grau de controle sobre a infraestrutura IoT ou, pelo menos, a sua comunicação com a rede. Veja abaixo as três áreas estratégicas devem ser abordadas ao desenvolver requisitos de solução para minimizar estas ameaças.

Aprendizagem

- **Identificação e Descoberta de Dispositivos**

Se você é como a maioria das organizações, é difícil ter uma visão completa de todos os dispositivos na rede em um único painel. Quando você acha que tem uma visão completa, as coisas mudam.

Uma boa solução deve detectar e classificar automaticamente os dispositivos da rede e criar um inventário. Depois de feita essa identificação, as equipes de segurança podem responder perguntas como:

Qual é o sistema operacional e sua configuração?

O dispositivo é gerenciado?

É confiável ou perigoso?

Com essa informação, é possível aplicar as políticas corretas.

- **Ação Preditiva**

O próximo desafio é entender comportamentos e agir antes que um ataque aconteça. Por exemplo, ao classificar dispositivos, temos três categorias: Dispositivos Gerenciados (controlados por você), Dispositivos Permitidos (aceitos, mas não controlados) e Dispositivos Não Autorizados (suspeitos e fora da política). Isso ajuda a identificar a atividade normal de cada tipo.

Além disso, isso permite dar uma pontuação de risco a cada dispositivo para aplicar políticas. Com o comportamento normal identificado, é mais fácil notar anomalias, como violações de política ou tráfego estranho.

Com uma visão geral de todos os dispositivos, um sistema inteligente pode se adaptar, tornando-se mais preditivo com o tempo.

Segmentação

- **Identificação de Riscos**

A primeira etapa da segmentação é a classificação. É preciso usar critérios como usuários, dados, dispositivos e locais para criar categorias e avaliar riscos. Por exemplo, sistemas que contêm dados de clientes ou financeiros devem ser agrupados com os recursos de rede que acessam esses sistemas diretamente.

- **Gerenciamento de Políticas e Dispositivos**

À medida que a rede cresce, novos dispositivos precisam ser descobertos e configurados conforme as políticas existentes. A solução deve permitir ver toda a atividade dos dispositivos e aplicar as políticas corretamente. Por exemplo, quando um novo switch é conectado, ele deve herdar as políticas de segurança automaticamente.

As redes crescem rápido demais para que isso seja feito manualmente. A solução precisa ser flexível, permitindo definir políticas por tipo de dispositivo, usuários, tipo de tráfego ou mesmo por localização e horário. As políticas devem ser a forma como os profissionais de segurança gerenciam os riscos na rede.

- **Exercício de Controle**

Uma vez que um intruso consegue entrar, ele pode se mover pela rede por semanas antes de agir. Segmentar a rede, isolando dispositivos IoT, servidores e as portas que usam, ajuda a organização a separar recursos conforme o risco. Tratar as partes da rede que interagem com dispositivos IoT de forma diferente em relação às políticas permite que a organização controle melhor o risco.

Proteção

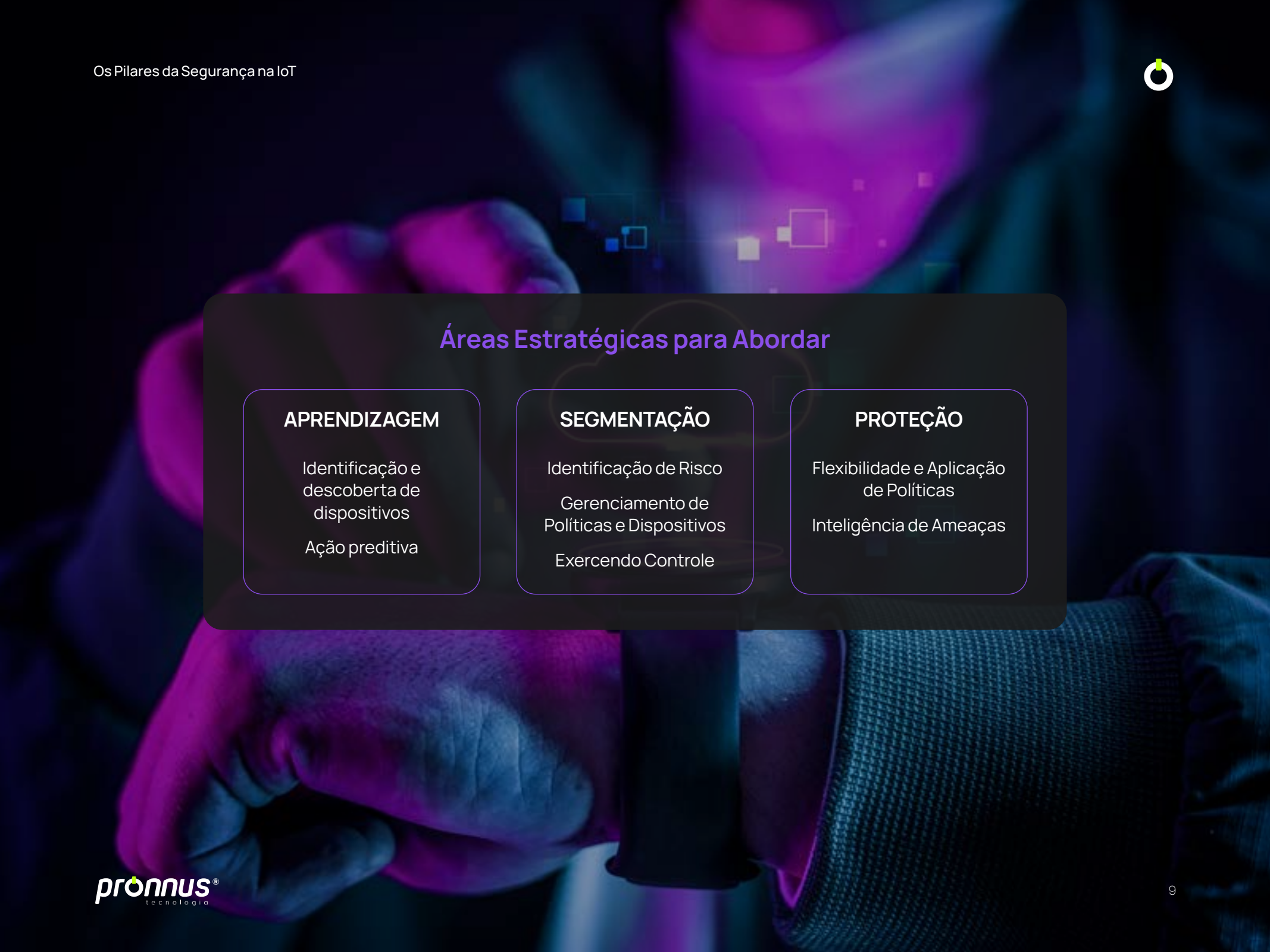
- **Flexibilidade e Aplicação de Políticas**

Uma solução flexível deve permitir definir e aplicar políticas em vários níveis, tanto por tipo de dispositivo quanto por acesso. Para lidar com os desafios da IoT, as regras devem regular o comportamento dos dispositivos, que tipo de tráfego podem gerar, onde podem estar na rede e até se podem estar conectados. Exemplos como BYOD, aplicativos de mídia social e serviços baseados na nuvem mostram onde diferentes políticas precisam ser criadas e aplicadas.

- **Inteligência de Ameaças**

Depois que os controles são estabelecidos, a solução deve aplicar as políticas de forma consistente e traduzir dados de conformidade em toda a rede, para que todos os dispositivos criem uma estrutura inteligente que aprende e responde a ameaças. Com a inteligência distribuída pela segurança, as ações podem ser tomadas perto da origem da ameaça. Além disso, essa inteligência deve buscar informações de fontes globais, incluindo outros fornecedores, para identificar ameaças antes que aconteçam e conectar dados sobre tendências e ameaças na rede.

Para uma solução abrangente, dispositivos IoT devem estar sujeitos ao mesmo monitoramento em várias camadas, inspeção e políticas de aplicação que os demais dispositivos em uma rede distribuída. Somente então todas as partes da rede poderão se comunicar entre si para compartilhar informações de políticas e inteligência de ameaças e proteger os dados dos aplicativos.



Áreas Estratégicas para Abordar

APRENDIZAGEM

Identificação e descoberta de dispositivos

Ação preditiva

SEGMENTAÇÃO

Identificação de Risco

Gerenciamento de Políticas e Dispositivos

Exercendo Controle

PROTEÇÃO

Flexibilidade e Aplicação de Políticas

Inteligência de Ameaças

A Evolução da Segurança

Uma abordagem baseada em aprendizado

Uma abordagem de segurança para a IoT precisa ser flexível e capaz de aprender e se adaptar. A solução deve aplicar políticas automaticamente e atualizar as regras conforme novas ameaças aparecem. Essas três áreas principais - aprendizado, segmentação e proteção - formam a base para os requisitos de segurança da IoT.

É importante avaliar como esses requisitos se encaixam na sua estrutura de segurança, e a Pronnus pode ajudar a proteger suas redes e dispositivos IoT agora e no futuro.

pronnus®
tecnologia

Proteja suas informações com tecnologia de última geração e reduza os riscos de ataques.

Clique aqui e conheça

www.pronnus.com.br