Riscos e segurança em ambientes de IoT

PRESENTED BY:

Ronaldo Vieira

IoT Sales Specialist - F5 Networks

WE MAKE APPS GO FASTER. SMARTER. SAFER.

Primeiramente: O que é um dispositivo IoT?

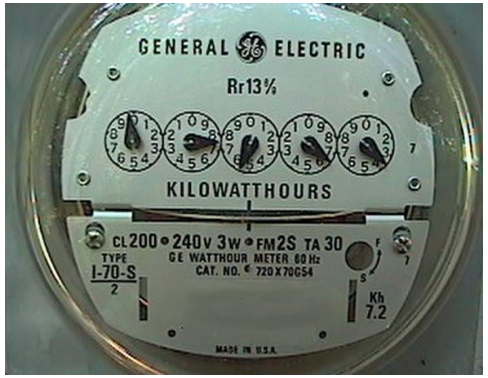
- **Qualquer “coisa” (Dispositivo) que possa gerar, armazenar, e enviar dados, ou atuar com comandos remotos, como:**
- Sensores industriais, como os de temperature ou de RPM.
- Camêras de Segurança.
- Semáforos.
- Dispositivos médicos (Bombas de insulina, Máquinas de Ressonância, etc).
- Veículos conectados (telemática, Sistemas de navegação).
- Dispositivos domésticos inteligentes e de automação (smartTVs, alarmes).
- Caixas eletrônicos.
- Dispositivos pessoais para fitness (Smart watches, fitbit, Garmin, etc).

“Coisas” conectadas a nossa volta

Passado

Transporte

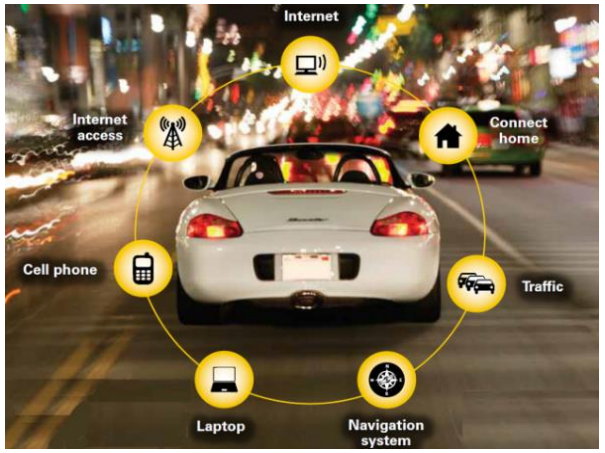
Manufatura



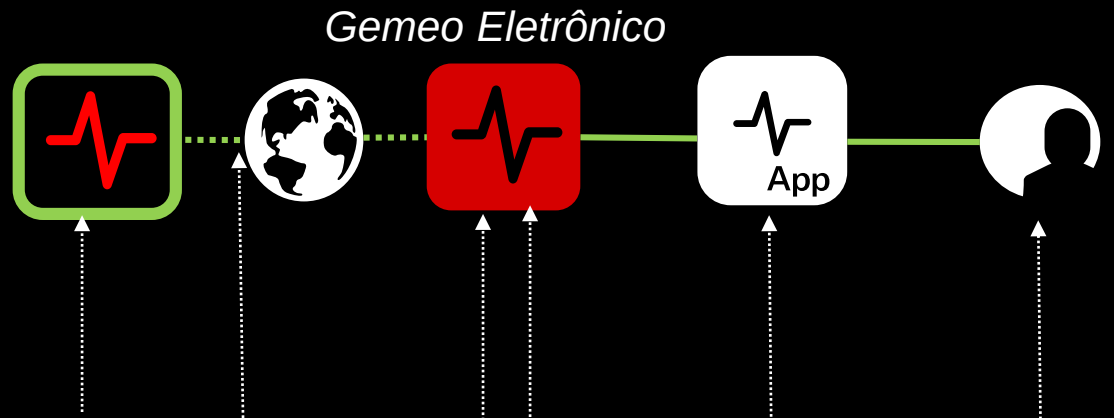
Energia

Agricultura

Hoje

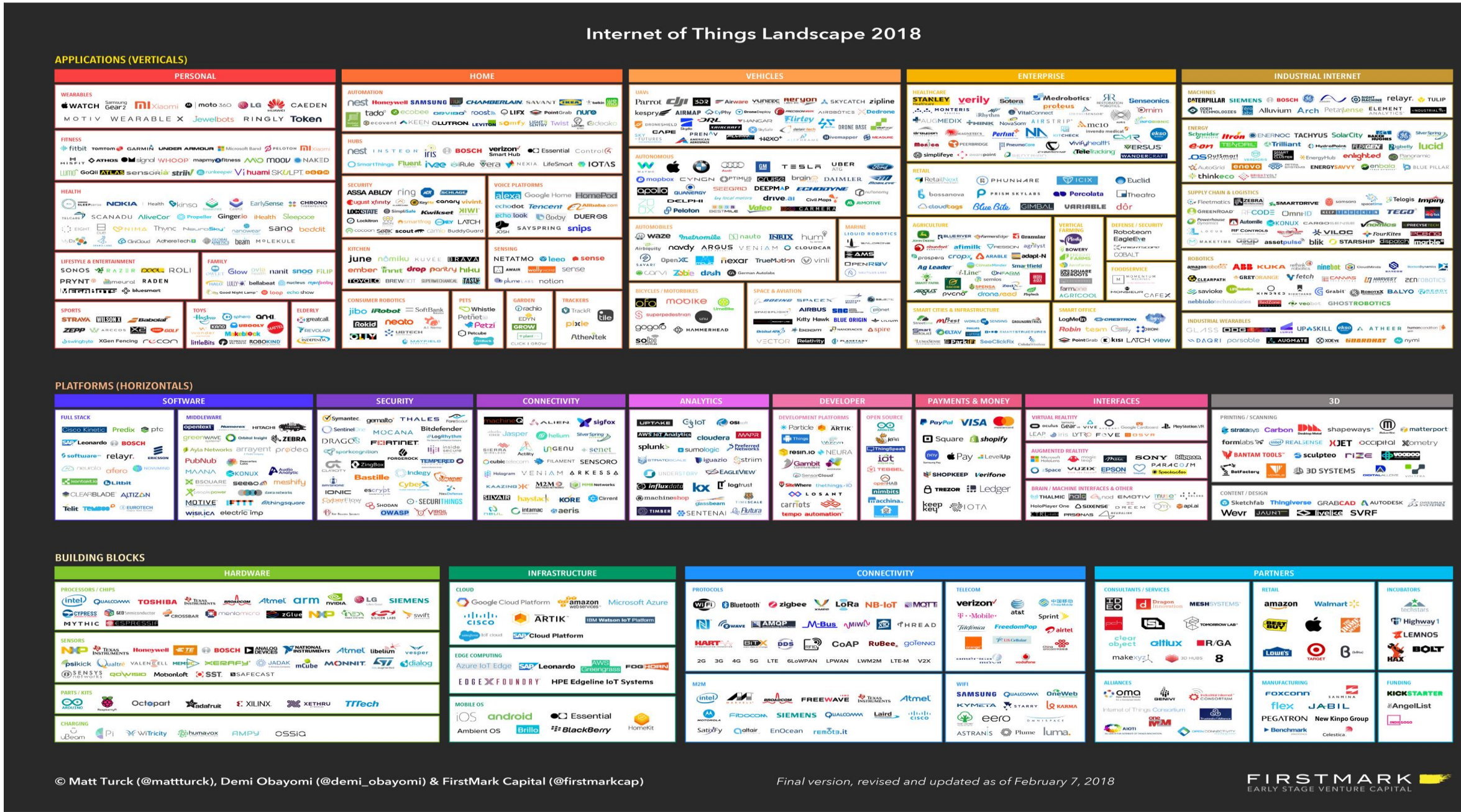


Blocos de uma aplicação IoT



- **Dispositivo**: instrumentar, ativar, assegurar, gerenciar, atualizar.
- **Conectividade** : conectar, controlar, disconectar, reconectar.
- **Dados** : coletar, transportar, proteger, armazenar, extrair.
- **Analítico :** agregar, alertar, notificar, prever, recomendar.
- **Lógica de negócio:** comparar, decidir, controlar, comandar, executar.
- **Gerenciamento de usuário**: definir perfil, dar premissões, controlar acesso.

Cenário de IoT em 2018



Agora, os fatos

- **A internet das coisas introduz novas vulnerabilidades, através da grande interatividade neste vasto ecossistema de soluções.**
- **A maioria dos dispositivos de IoT não foram desenvolvidos pensando-se em segurança.**
- **Alguns destes dispositivos não conseguem suportar controles robustos de segurança, devido a limitações de energia e memória.**

E o que torna o risco em IoT tão diferente?

- **A grande diferença entre as ameaças de IoT e a típica ameaça de cibersegurança é o fator de segurança humano:**

- 1980, um dispositivo de rádio terapia, chamado de Therac-25, possuía um defeito que administrava 100 vezes mais radiação além do recomendado.

- 2015, um time de pesquisadores foi capaz de controlar remotamente uma SUV da Jeep através de seu barramento CAN, explorando uma vulnerabilidade em um update de firmware, eles sequestraram o veículo através da rede Celular. (fonte: IBM SecurityIntelligence website).

- 2017, CNN afirma que o FDA confirmou que implantes cardíacos possuem vulnerabilidades que poderiam permitir o acesso remoto por um hacker ao dispositivo.

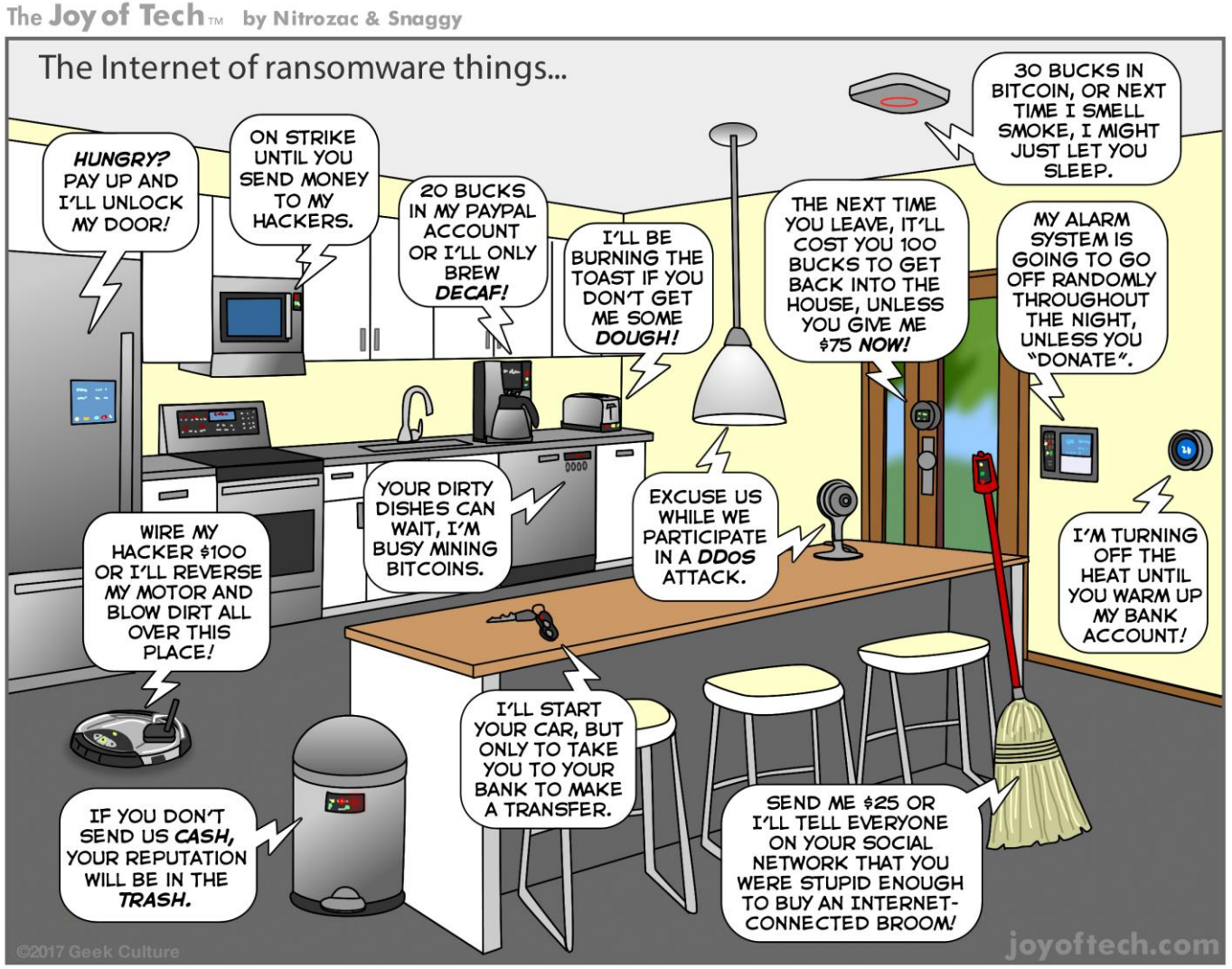
Riscos em IoT

- **Dispositivos podem ser comprometidos para enviar dados errados ou realizar ações incorretas.**
- Imagine nesse caso, veículos, hospitais ou usinas hidroeletricas.
- **Dispositivos conectados podem ser uma ameaça para a rede em si.**
- Agora, pense em uma rede composta por milhares de dispositivos comprometidos, transformada em uma botnet sendo usada para ataques DDoS.
- **As ameaças em IoT se extendem além das internas as empresas ou organizações, com o uso das suas soluções em IoT sendo usadas como parte de um grande ataque a outras companias.**
- Grande prejuízo a reputação e eventualmente financeiro.

Solução de segurança baseada em Múltiplas camadas

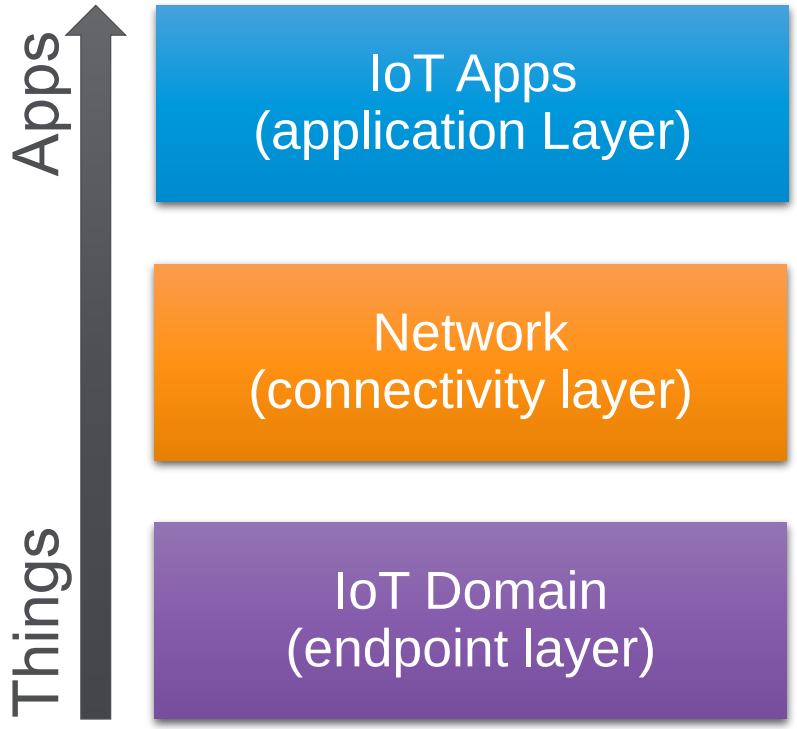
- **Não existe solução mágica para mitigação de todos os riscos de uma única vez.**
- **A única maneira sustentável é a implementação de segurança em múltiplas camadas, com esta metodologia, consideramos toda a cadeia, passando pelo dispositivo conectado, pela conexão de rede, por seus protocolos e aplicações usadas.**

A internet das coisas, sequestradas....

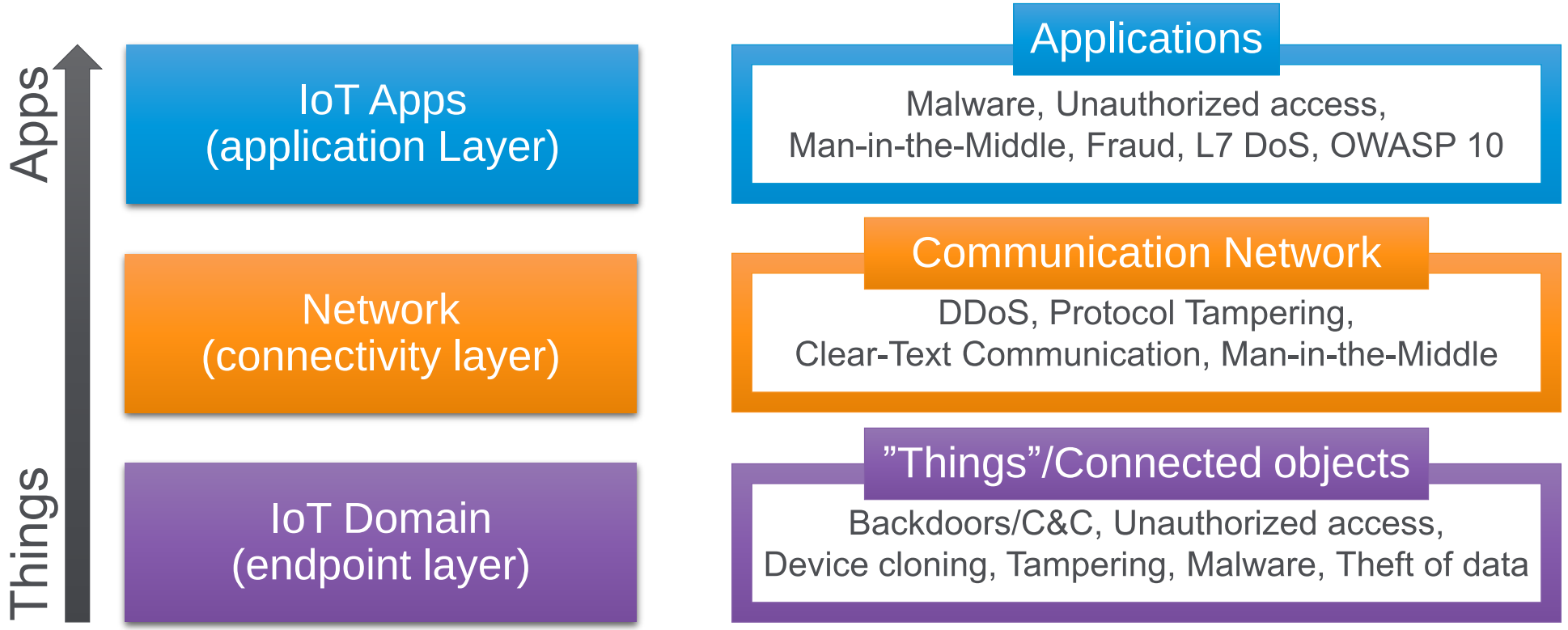


O ECOSSISTEMA DE AMEAÇAS EM IOT

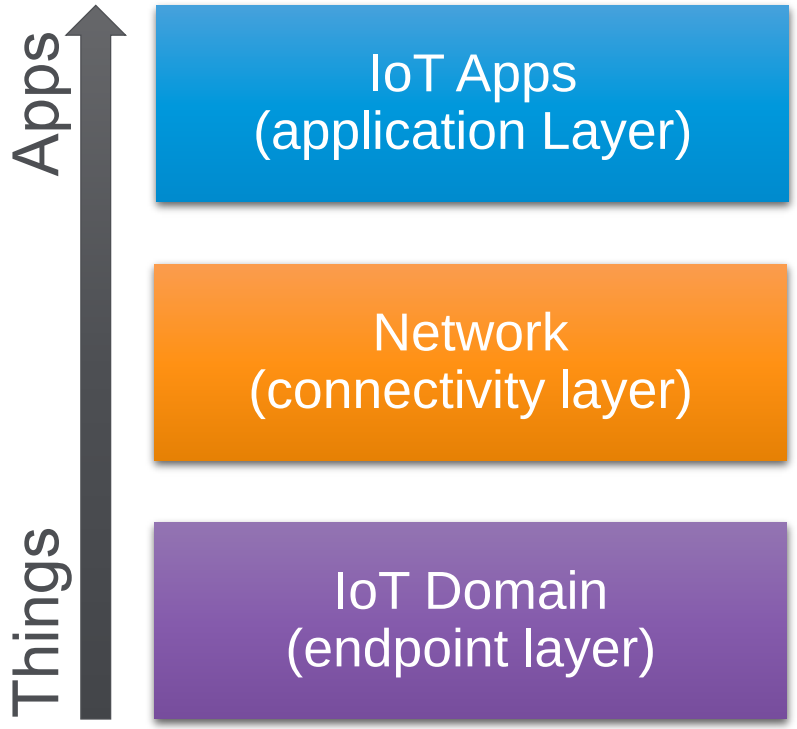
O ecossistema de ameaças em IoT



O ecossistema de ameaças em IoT



O ecossistema de ameaças em IoT



Applications

Malware, Unauthorized access,
Man-in-the-Middle, Fraud, L7 DoS, OWASP 10

Communication Network

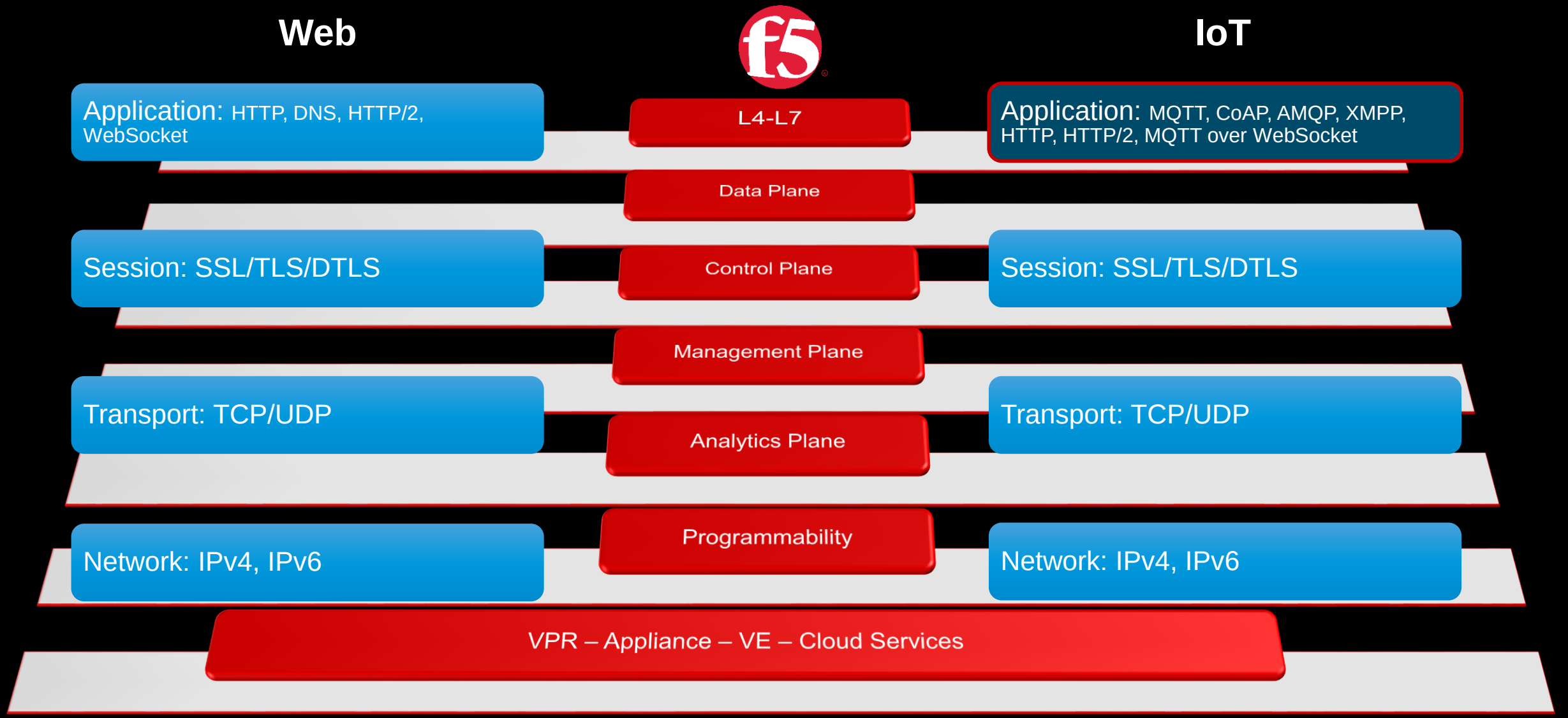
DDoS, Protocol Tampering,
Clear-Text Communication, Man-in-the-Middle

”Things”/Connected objects

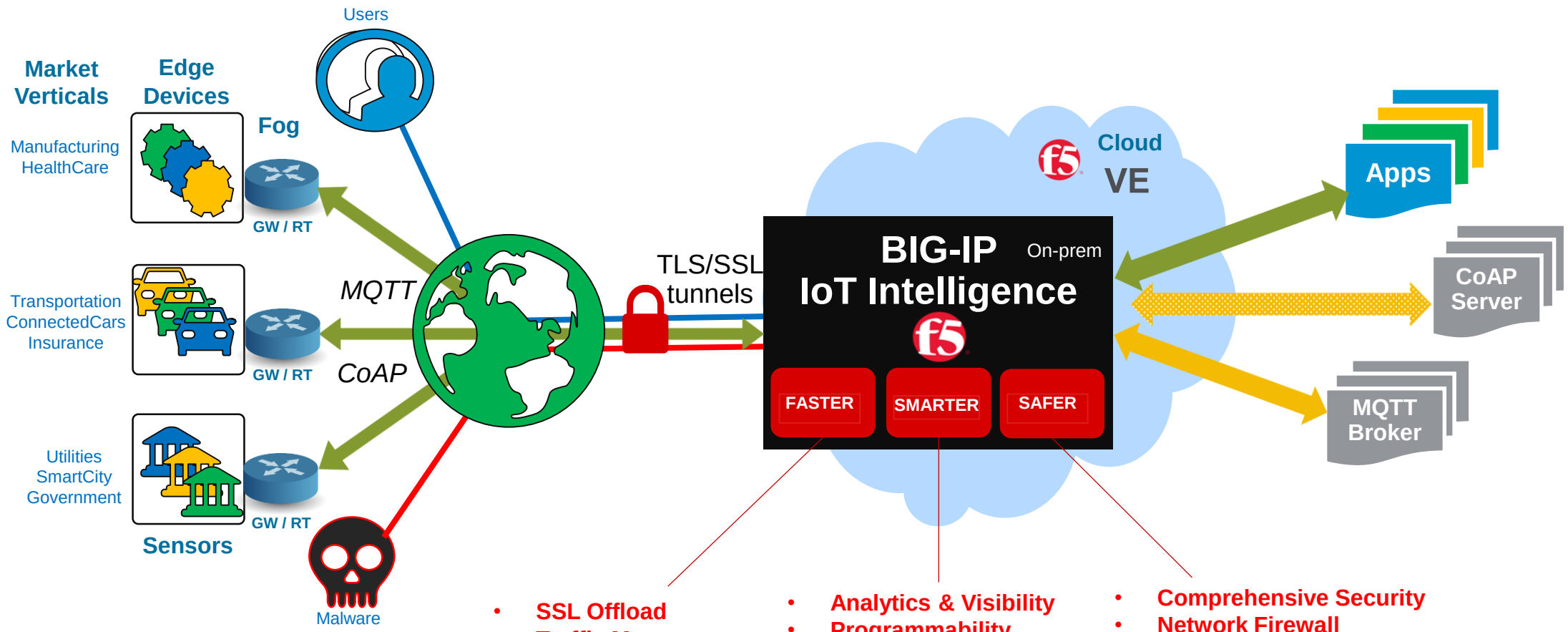
Backdoors/C&C, Unauthorized access,
Device cloning, Tampering, Malware, Theft of data

Soluções de Segurança

Camada OSI WEB versus Pilha IoT



Solução IOT



- SSL Offload
- Traffic Management
- TCP Express
- Connection Mgmt.

- Analytics & Visibility
- Programmability
- Policy Enforcement
- Access Control
- Protocol Analysis

- Comprehensive Security
- Network Firewall
- Authentication & Authorization
- Intelligent DNS
- DDoS Protection

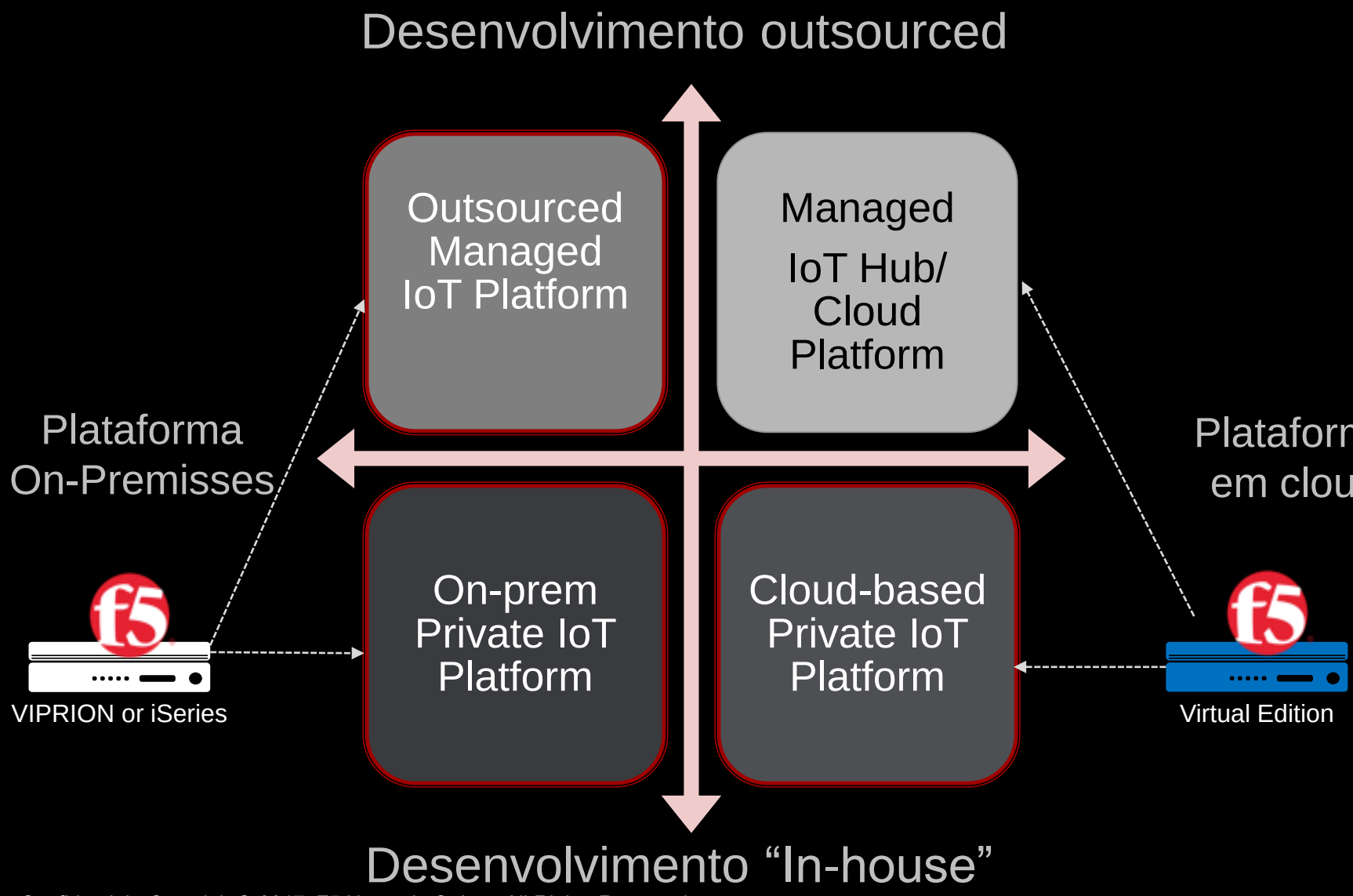
A solução IoT da F5 é agnóstica para todas as verticais

SOLUÇÃO F5

Desafio para os times de Apps/Infra em IoT

- Arquitetura, planejamento e dimensionamento.
- Custos previsíveis, TTM, performance e riscos.
- Escalabilidade e elasticidade conforme o negócio.
- Customização de segurança e privacidade.
- Otimizar performance e latência.

Desenvolvimento e entrega da plataforma IoT

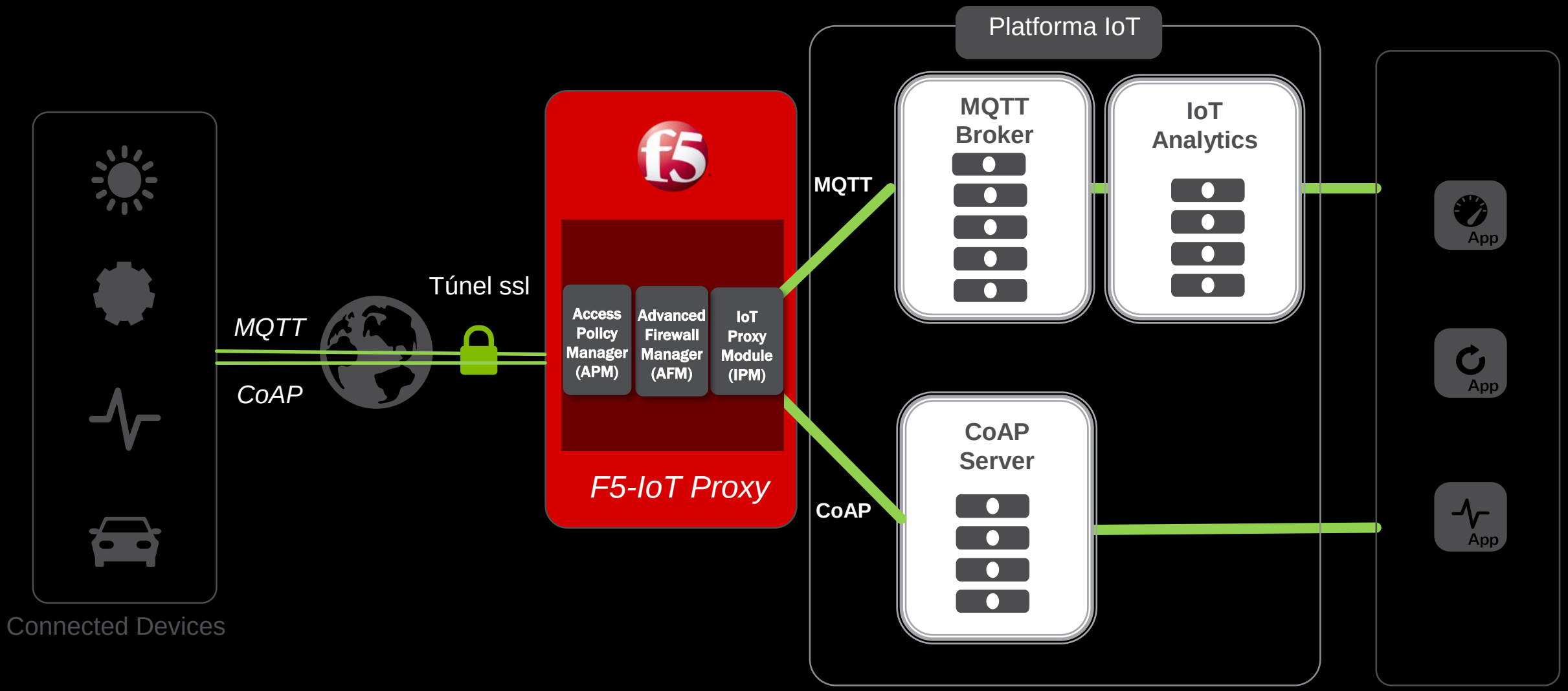


Critério

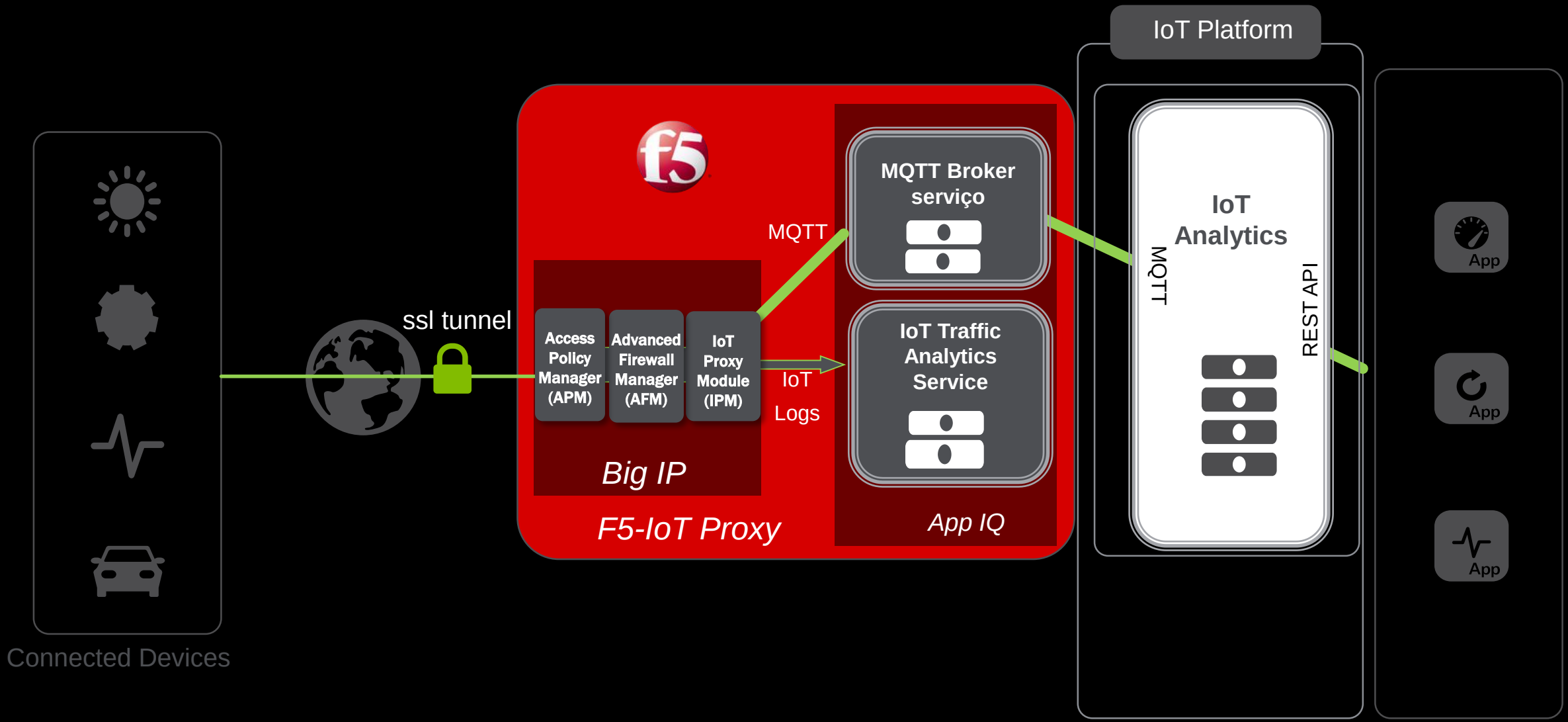
- Tempo até o mercado
- Custo
- Risco
- Performance

Princípio do Proxy F5 IoT

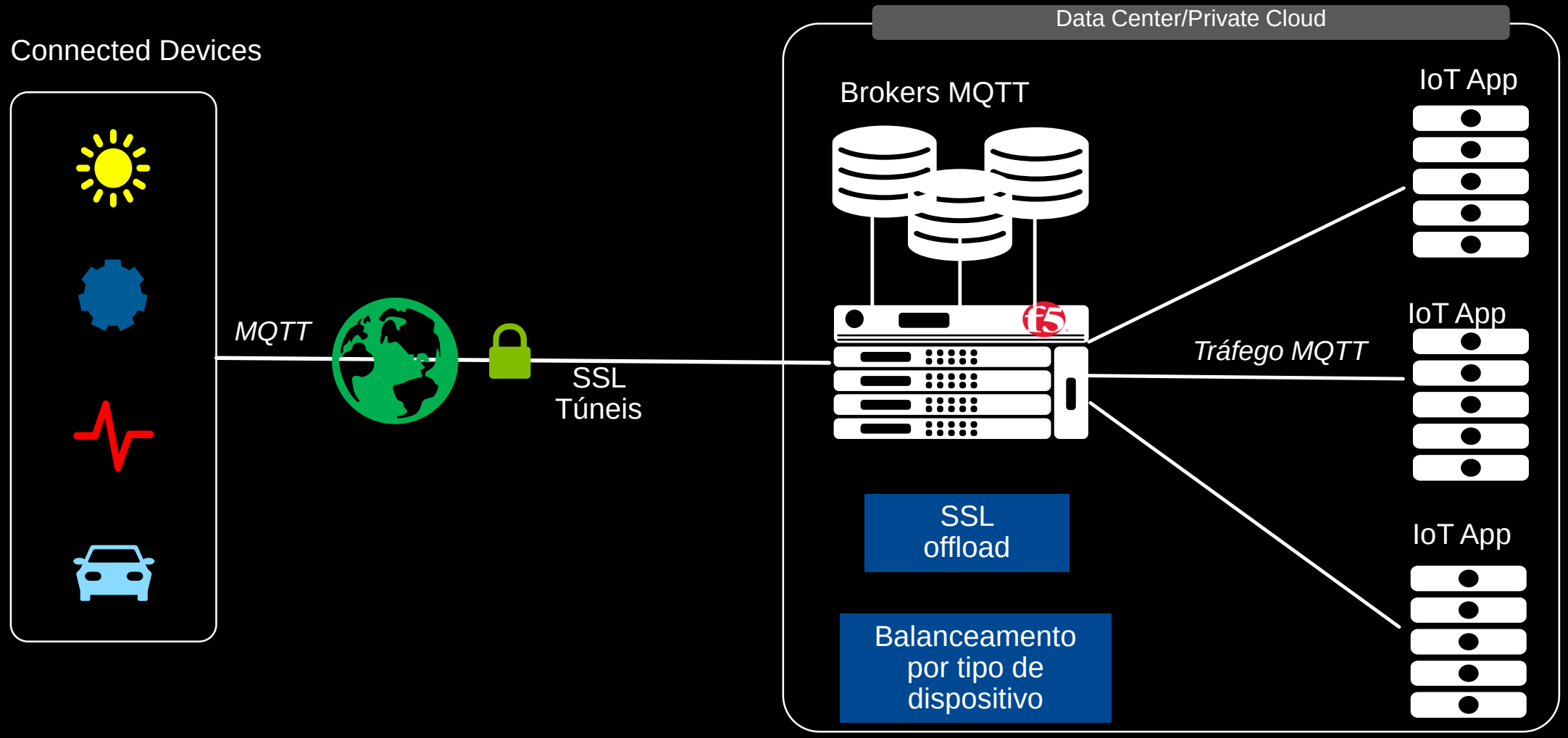
Multi-Protocolo, Acesso e Proteção



Broker MQTT e integração com Analíticos



Compilador MQTT e balanceamento de carga



BIG-IP faz a compilação da mensagem MQTT e o balanceamento por dispositivo em uma enorme escala com altos números de CPS (calls per second) e Sessões concorrentes.

Mudando o conceito do perímetro de rede

- O dispositivo IoT muda o conceito do perímetro de rede.
- No passado, comunicações além da rede eram asseguradas através de VPNs.
- Hoje, a variedade e o volume dos dispositivos, aumentam a complexidade de segurança nesta camada, forçando os times de segurança, a considerar ativos corporativos em ambientes amigáveis e hostis.

Protocolos de Comunicação de IoT

- **Existem varios protocolos de comunicação de IoT, alguns são novos, outros já estão no mercado por 20 anos, e nem todos eles foram desenvolvidos de maneira segura.**
- **O entendimento das limitações de segurança desses protocolos é peça fundamental para o design da segurança de IoT.**
- **Uma solução válida é deixar os dispositivos IoT em uma rede apartada das redes mais sensitivas.**

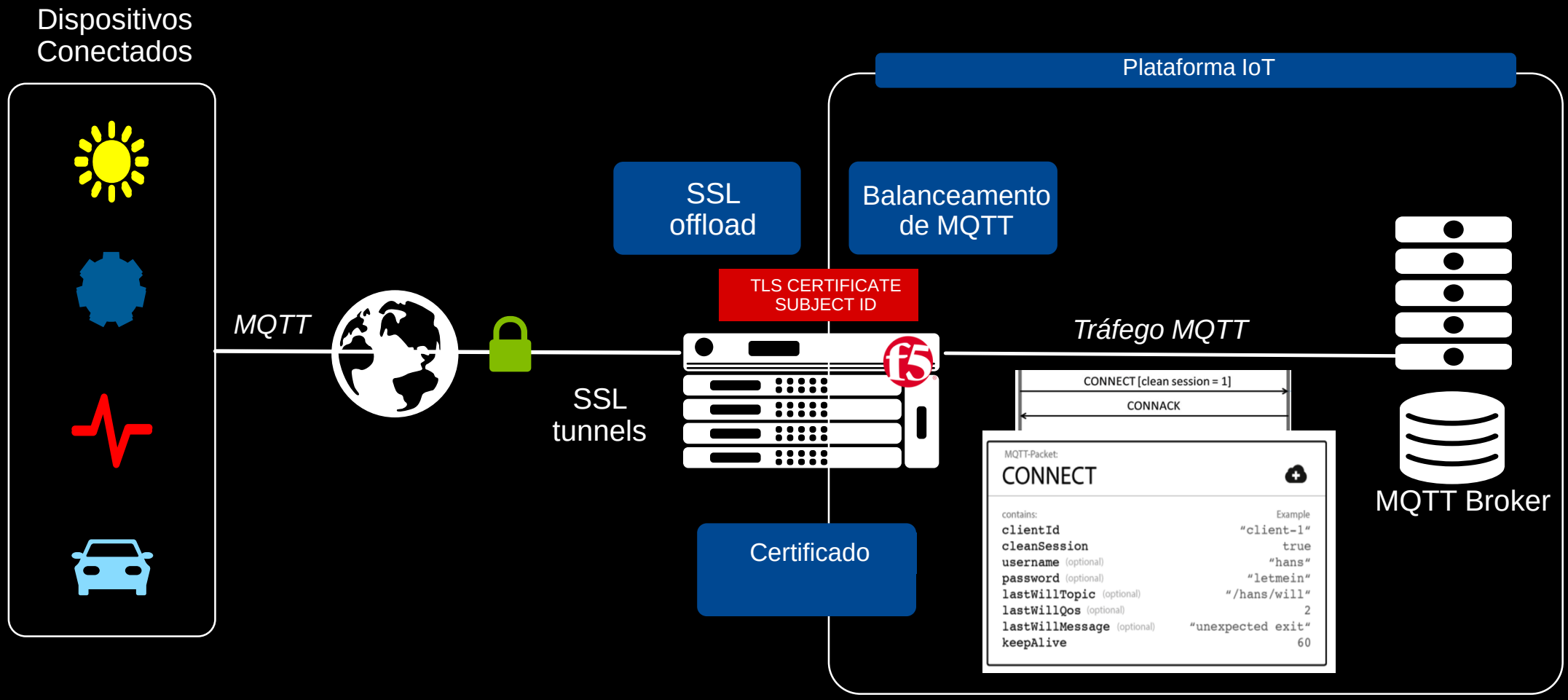
Criptografia fim-a-fim - Onipresente

- **Transmitir os dados gerados pelos dispositivos IoT, através de redes públicas ou privadas, de maneira segura, torna-se extremamente complexo em um mundo de carros, dispositivos médicos e fábricas integradas.**
- **Privacidade de dados é uma crescente preocupação.**
- **Com relação aos protocolos de criptografía, o TLS com "Elliptic Curve Cryptography (ECC)" surge como uma alternativa atrativa ao RSA, pois trabalha com chaves menores, promovendo uma rápida convergência computacional e um menor consumo energético.**

O diferencial da F5

- **Fazemos o “offload”das últimas versões de SSL e TLS, incluindo a criptografia ECC por aceleração em Hardware, promovendo os mais altos níveis de segurança e performance no ecossistema de IoT**
- **F5 permite o controle de fluxo para/do Dispositivo IoT, inclusive com detecção de ações maliciosas e malware.**
- **A camada de proteção da F5 permite a detecção e mitigação in-line de ataques volumétricos, DDoS, junto com o nosso serviço de cloud.**

Offload SSL e autenticação por certificados



Após o offload do SSL, o BIG-IP F5 insere o “Common Name” na mensagem de conexão do MQTT, e faz a autenticação no IoT Broker do Backend.

Tornando as coisas seguras (dispositivo remoto)

- Os fabricantes dos dispositivos de IoT estão focados nos aspectos econômicos e operacionais dos dispositivos de IoT, e não nos aspectos de segurança.
- Como resultado, temos endpoints de IoT, sem a mínima capacidade de segurança (Autenticação e Criptografia forte).
- Imagine uma empresa com milhares desses dispositivos, conectando-se à rede e usando as aplicações.
- Este cenário pode se tornar um pesadelo as políticas de segurança.

As consequências: A Botnet Mirai

- A Botnet Mirai (e suas variantes) assumiram o controle de milhares destes dispositivos vulneráveis.
- Escaneando a internet em busca de dispositivos com senhas padrões de fábrica e suas combinações de usuário e senha.
- Uma vez identificado, ela toma o controle de cada dispositivo, e assim formando o maior ataque de DDoS já realizado na história.

As consequências: A Botnet Mirai

- A investigação do ataque identificou 49.657 endereços IP únicos que tinham dispositivos infectados pelo Mirai, na sua maioria cameras de circuito fechado de TV.
- Estes IPs foram descobertos em mais de 164 países.

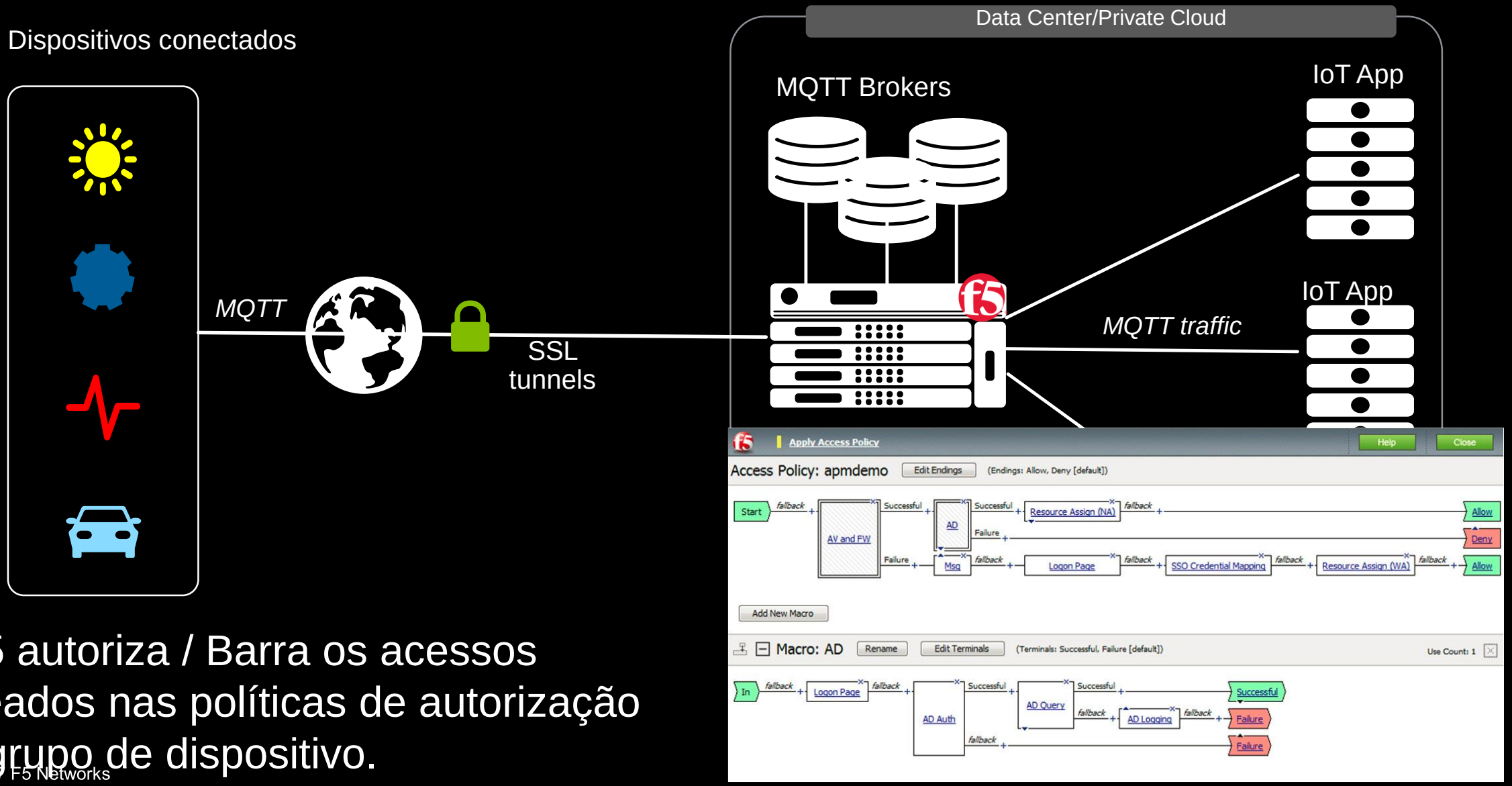
Autenticação é a solução

- Para dispositivos simples que não suportam mecanismos complexos de autenticação, o uso de soluções externas de autenticação é recomendável para que fiquemos dentro das regras de segurança.
- Esta camada adicional de autenticação, permite aos dispositivos de IoT, ficarem protegidos das suas senhas padrões de fábrica.
- Também evita que dispositivos IoT comprometidos, conectem-se à aplicação e entreguem dados maliciosos ao invasor.

Solução F5

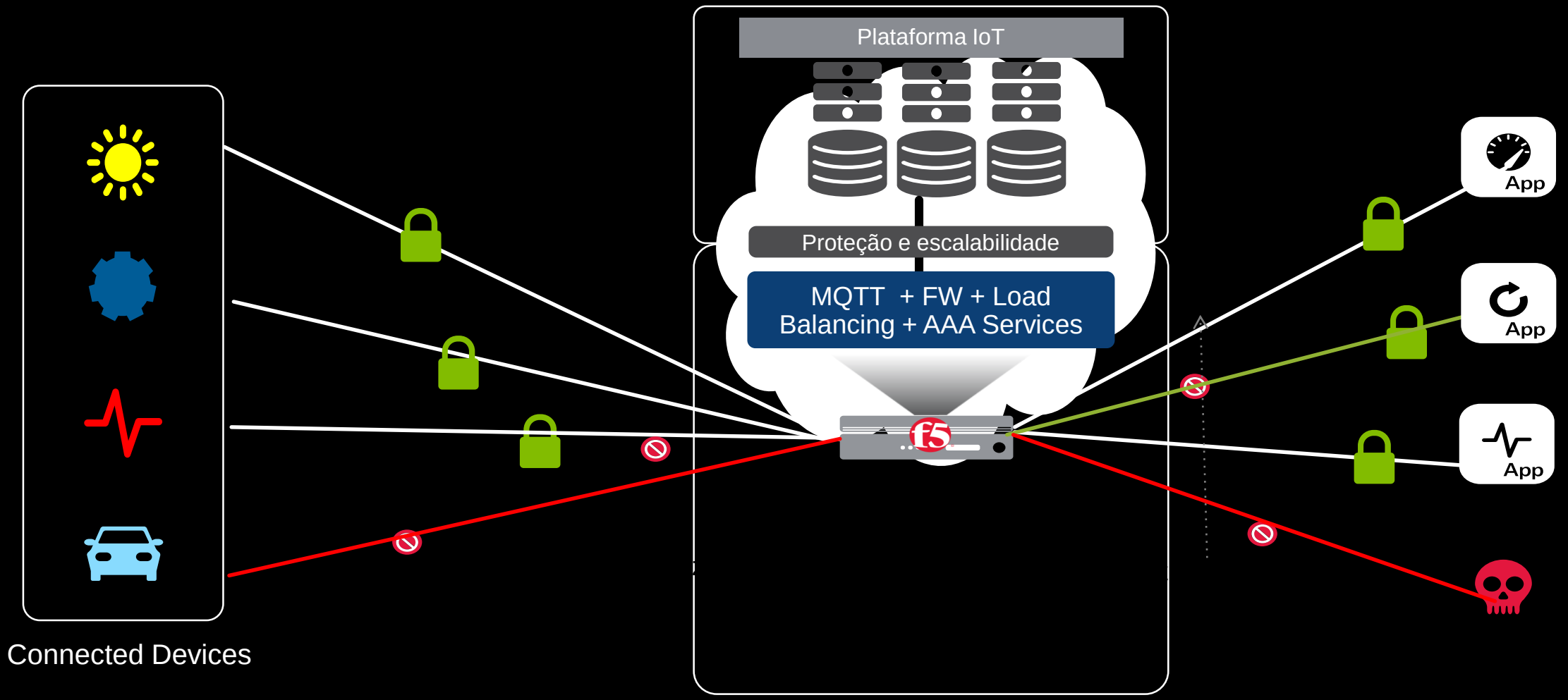
- **Senhas “Default” e “Hard-coded” às vezes são muito complexas de serem alteradas, mas muito simples de serem descobertas.**
- **A F5 te ajuda a assegurar que o acesso do dispositivo IoT, será feita de maneira segura, provendo múltiplos fatores de autenticação, autenticação por certificado do cliente, validação, etc.**
- **Ao adicionarmos esses mecanismos complexos de autenticação, o dispositivo de IoT atual, passa a proteger todo o ecossistema de acessos maliciosos e não autorizados.**
- **Evite que o seu ecossistema de IoT vire parte de uma Botnet no futuro.**

Política de acesso e controle



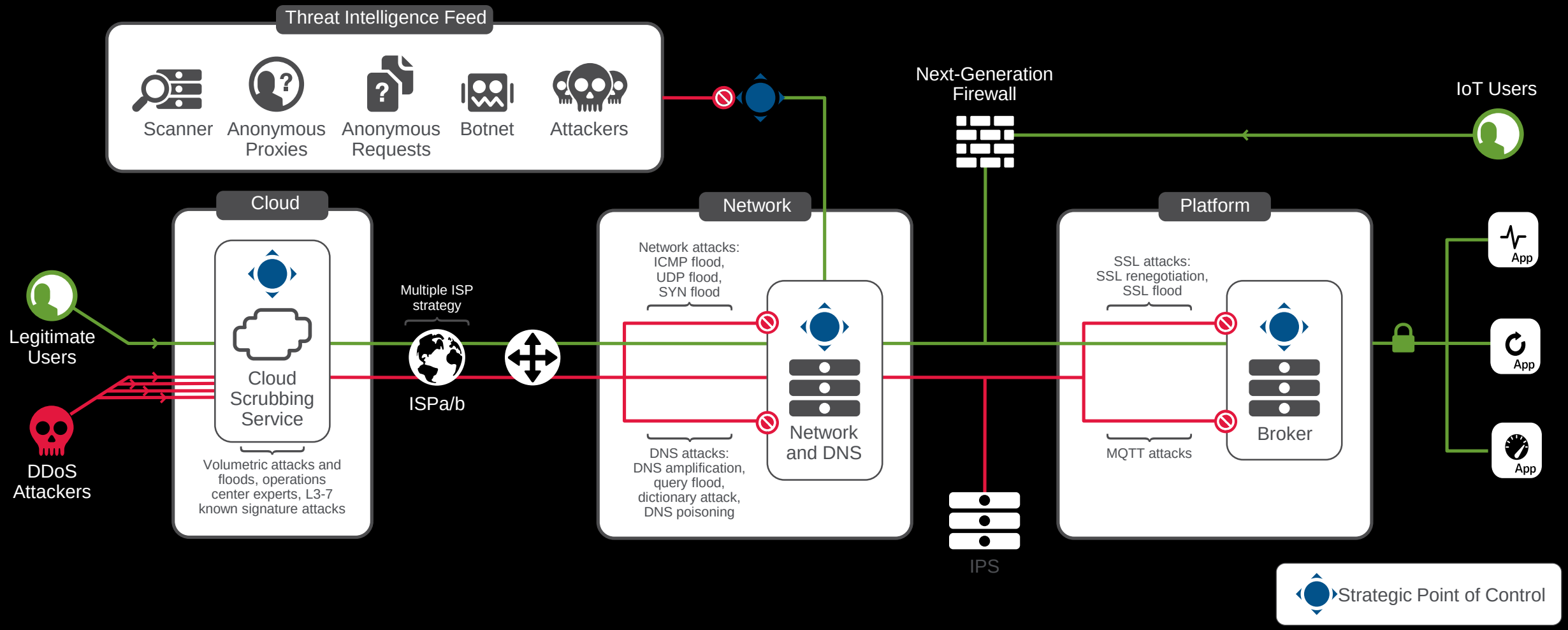
O F5 autoriza / Barra os acessos baseados nas políticas de autorização por grupo de dispositivo.

Autenticação e Gerenciamento da identidade do cliente



F5 faz a interface com os servidores de Oauth, fazendo a autenticação e a gestão de identidade.

F5 reduz os riscos de segurança de IoT e DDoS.



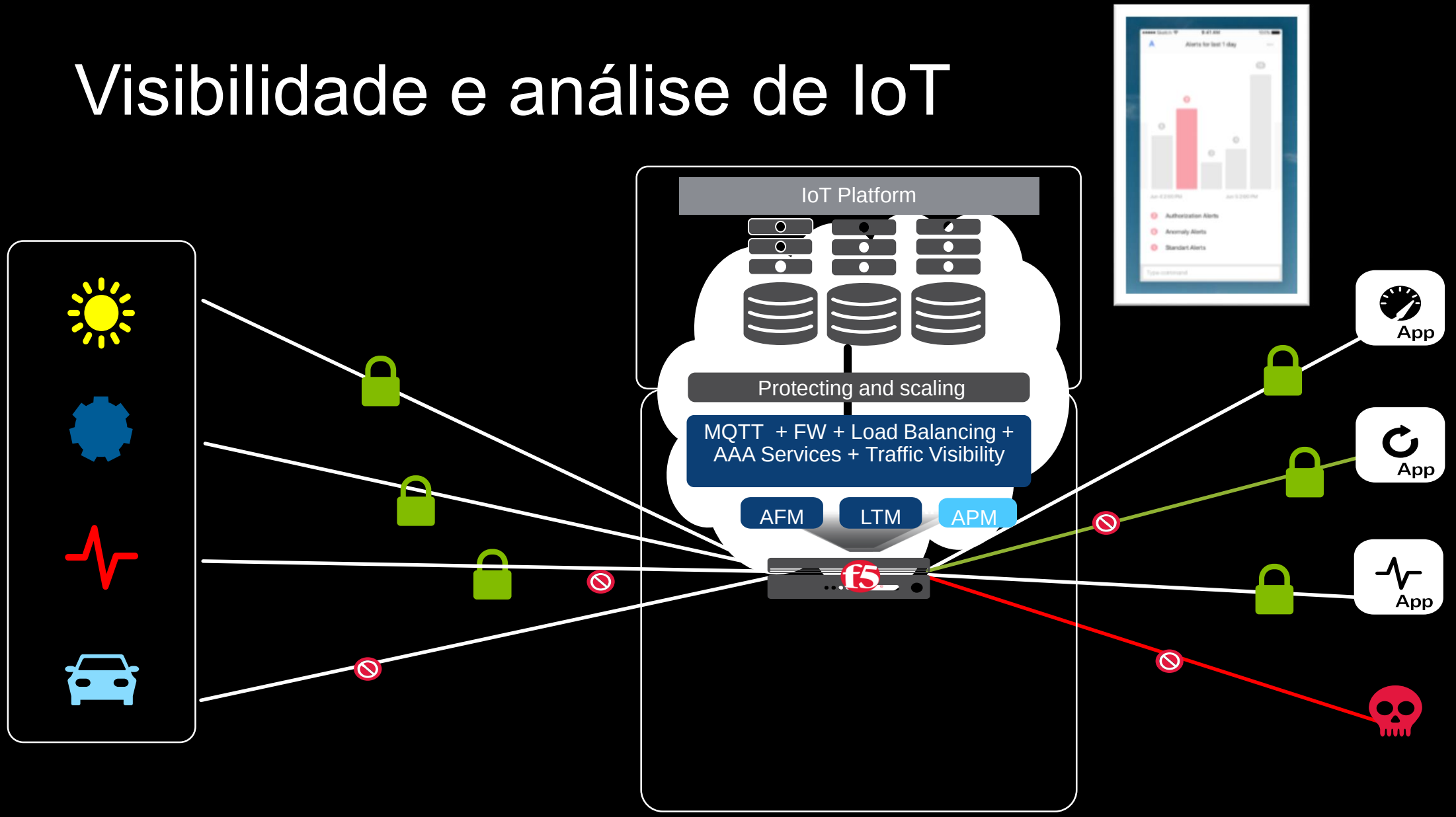
Um ciclo de vida complexo de gerenciar

- **Os dispositivos de IoT são desenhados para terem uma longa vida útil, especialmente no ambiente industrial, onde podem funcionar por 15 anos com uma única batería.**
- **A própria natureza do dispositivo IoT faz com que eles sejam complexos de sofrerem upgrades. Eles acabam tornando-se uma bomba temporizada, na medida que novas vulnerabilidades são descobertas e os fabricantes descontinuam o suporte.**
- **Para os hackers, estes dispositivos desatualizados e algumas vezes esquecidos, tornam-se seus principais alvos.**

Mantenha seu IoT sobre controle

- **Com isso, as soluções requerem um gerenciamento de vida fim-a-fim, incluindo o inventário para qualquer dispositivo IoT conectado, durante um longo período de tempo.**

Visibilidade e análise de IoT



F5 provê a visibilidade e o analytics do tráfego IoT, mas pode também ser configurado para enviar eventos/ logs / estatísticas para outras plataformas.

Aplicações seguras

- **A segurança das aplicações e seus dados, é uma parte crucial de qualquer desenvolvimento de IoT.**
- **A adoção da cloud pública, interfaces Web e aplicações móveis, trazem inovação na maneira de entregar e operar o ecosistema de IoT, mas também novas ameaças sugerem a cada minuto:**
- Agora as aplicações são acessíveis a qualquer lugar, em qualquer horário, e onde nenhuma interrupção é aceitável.
- As aplicações Web precisam ser protegidas dos ataques Web mais comuns (OWASP 10) e ataques de camada DoS.
- Estas também precisam implementar mecanismos de defesas mais complexos para ataques elaborados como: Fraude, Phishing, man-in-the-middle, etc.

E novamente ... A Solução F5

- **A F5 protege a aplicação e seus dados de ataques conhecidos e não conhecidos, e facilita compliance com PCI, FIPS, NIST, HIPPA entre outros.**
- **F5 entrega proteção avançada de aplicações:**
- Defesa pró-ativa contra Bots.
- Inteligência dinâmica para reputação de endereços IP.
- Proteção de um “Full Proxy”contra ataques DoS L7 e OWASP top 10.
- Facilidade de virtual patching com 1-click para aplicações vulneráveis, incluindo integração com DAST/VA.

CONCLUSÃO

Conclusão

- **Segurança, Privacidade e useabilidade precisam ser consideradas em conjunto, quando desenhamos e entregamos soluções / ecossistemas de IoT.**
- **O eventual potencial de risco a vida humana, exige que níveis mínimos de segurança sejam implementados em uma implantação mais ampla de IoT.**
- **A conexão de dispositivos IoT à Internet, exige que o legado e o novo, junto com a aplicação ao qual eles conectam, suportem capacidades mais elaboradas de segurança.**
- **A F5 provê as camadas específicas de segurança, para a implantação segura de dispositivos e aplicações de IoT, seja na nuvem, On premisses, ou na rede.**

Obrigado

Ronaldo Vieira

r.vieira@f5.com

+55 11 99522 5072