Instituto Federal de Educação, Ciência e Tecnologia do Paraná - IFPR

disciplina de

SERVIÇOS PARA INTEGRAÇÃO DE SISTEMAS

Especialização em Internet das Coisas

CLOUD PARA IOT E ASPECTOS DE SEGURANÇA

Professor Jefferson de Oliveira Chaves
jefferson.chaves@ifpr.edu.br

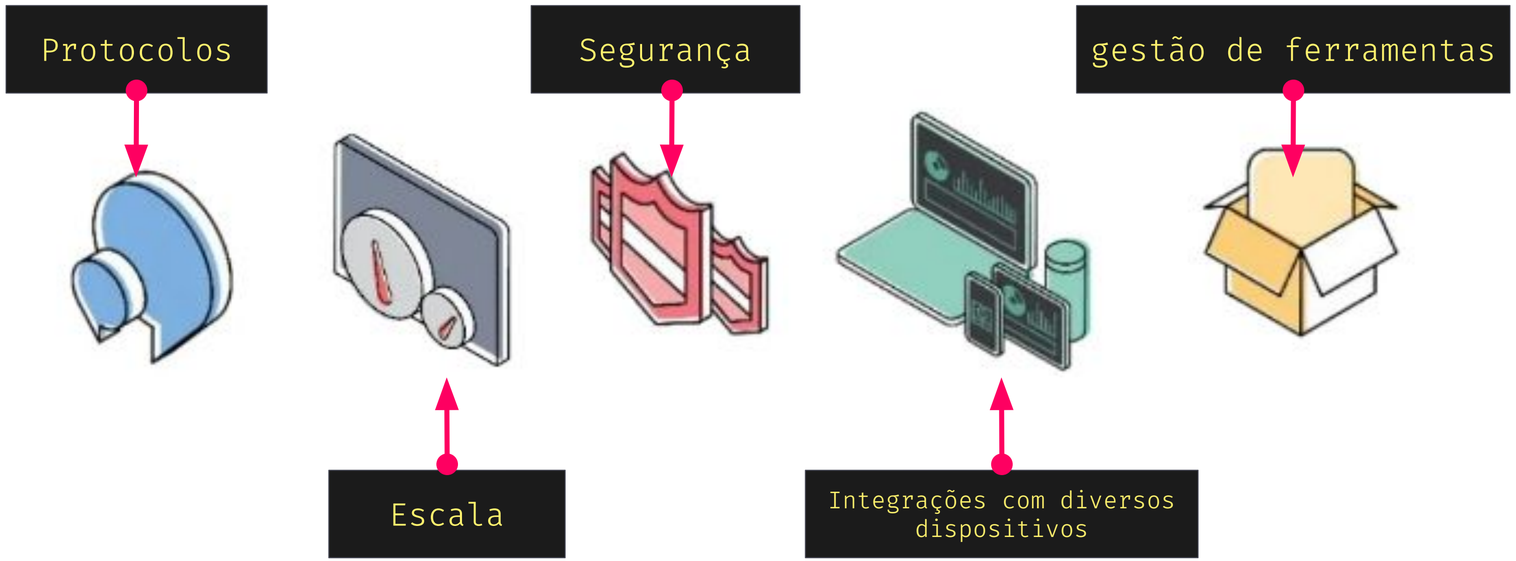
Agenda

- O que é Cloud Computing?
- Principais Características da Nuvem
- Modelos de Serviço na Nuvem
- Relação entre Cloud Computing e IoT

O que é Cloud Computing?

- Cloud Computing, ou computação em nuvem, é um modelo de entrega de recursos de tecnologia — como servidores, armazenamento, bancos de dados, redes, software, análise e inteligência — por meio da internet, sob demanda, e com pagamento conforme o uso (pay-as-you-go).
- Em vez de comprar, manter e gerenciar servidores físicos ou datacenters locais, as empresas e usuários utilizam serviços na nuvem;
- Esses serviços são oferecidos por provedores como AWS (Amazon Web Services), Microsoft Azure, Google Cloud, Oracle Cloud, entre outros.

Conexão a Nuvem pode ser um trabalho duro



Faz sentido aplicações em **Nuvem?**

O que considerar ao optar pela **Cloud**?

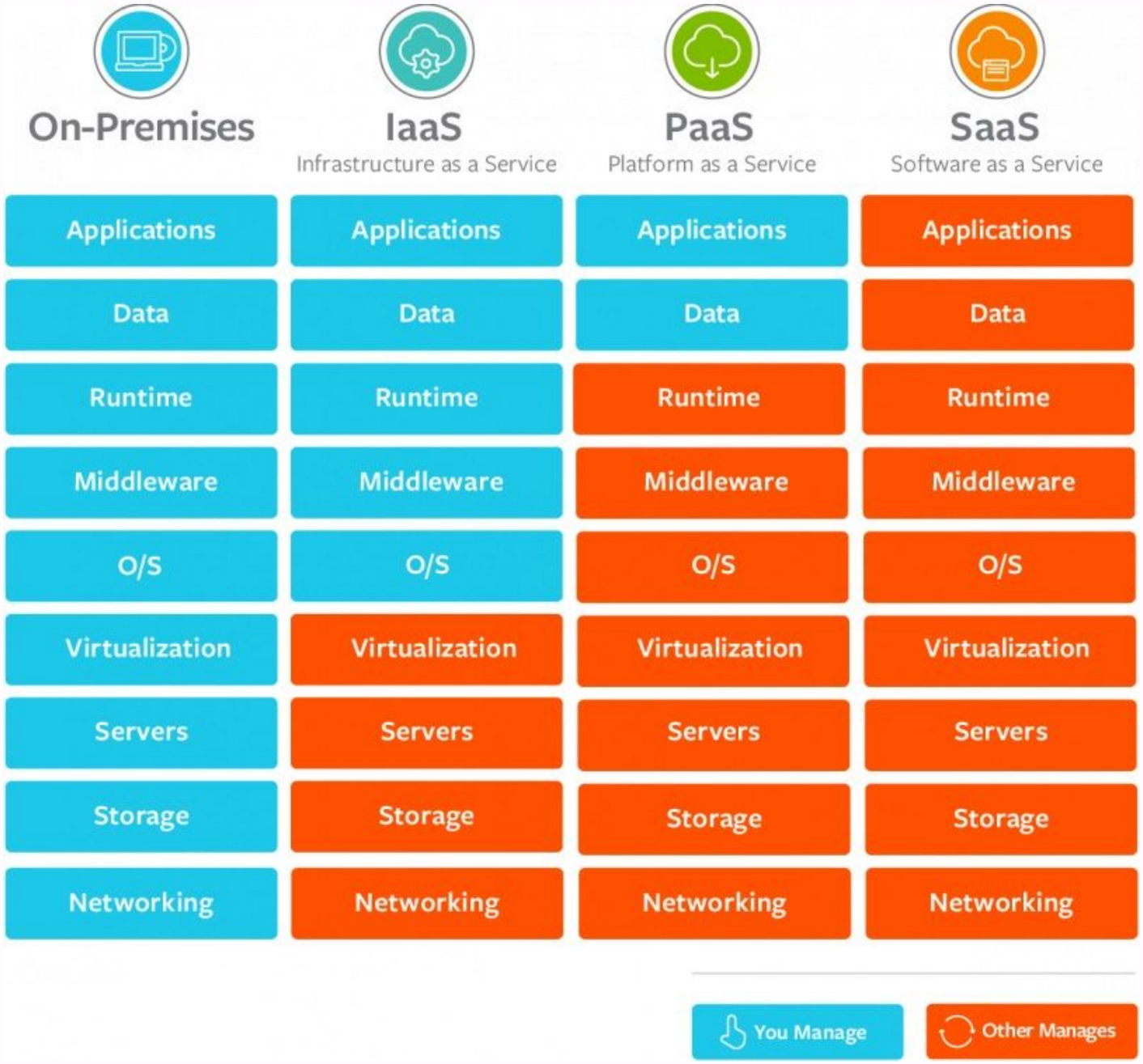
- Custo Total e Modelo de Cobrança;
- Segurança e Compliance;
- Confiabilidade e Disponibilidade;
- Escalabilidade e Flexibilidade;
- Desempenho e Latência;
- Governança e Gestão;
- Portabilidade e Dependência do Fornecedor (Lock-in);
- Suporte Técnico e Serviços Adicionais;
- Sustentabilidade e Impacto Ambiental;

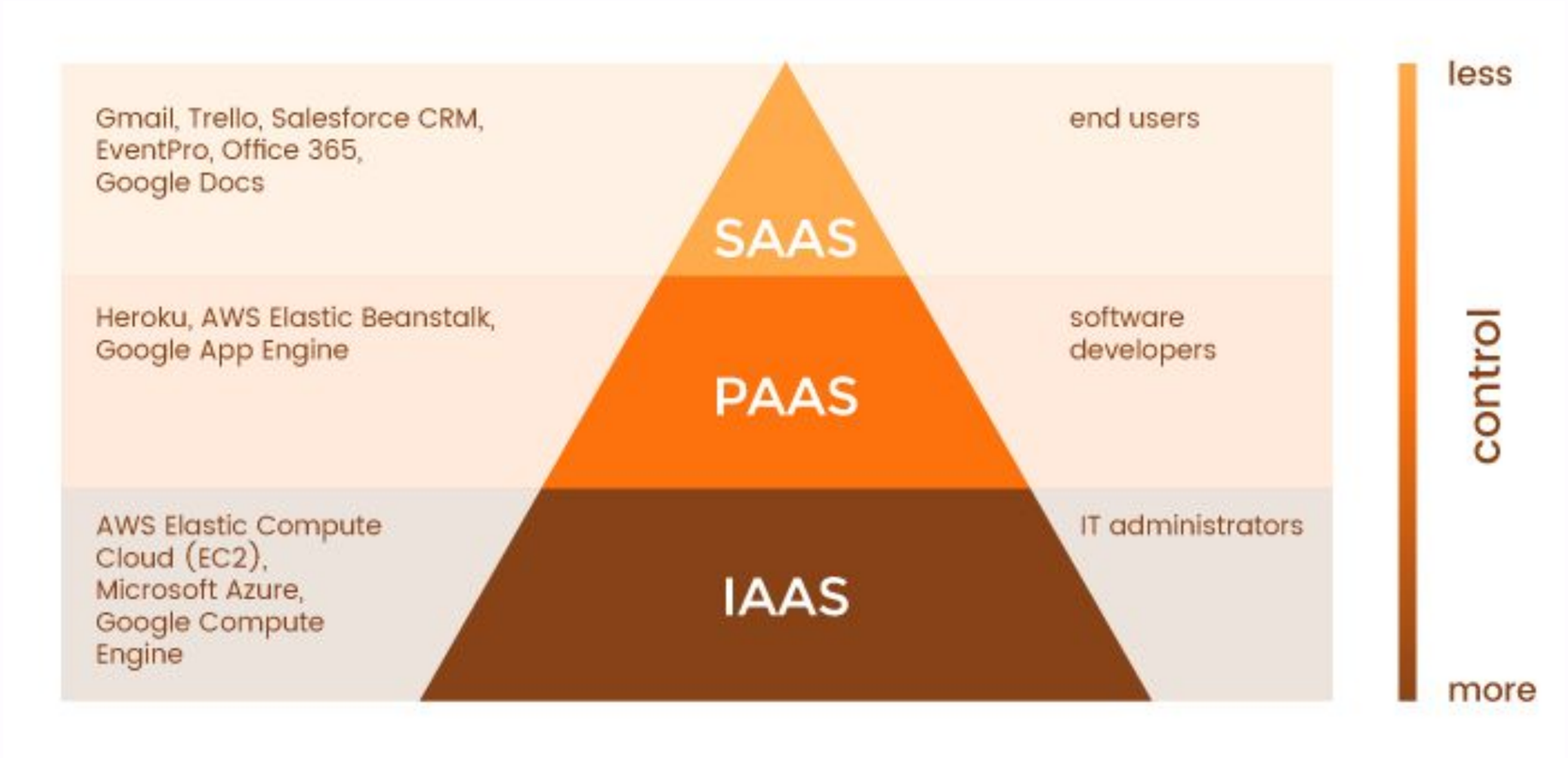
Principais Características da **Nuvem**

- Elasticidade: Aumenta ou reduz recursos conforme a demanda.
- Escalabilidade: Suporte a um grande número de usuários ou dispositivos.
- Alto Disponibilidade: Serviços acessíveis de qualquer lugar, a qualquer hora.
- Custo sob demanda: Paga-se apenas pelo que é utilizado (existem diversos modelos de contratação).
- Gerenciamento “simplificado”: Sem necessidade de manter servidores locais.

Modelos de Serviço na **Nuvem**

- Os modelos de serviço em nuvem são as formas como os serviços de cloud computing são oferecidos aos usuários;
- Eles definem **qual parte da infraestrutura**, plataforma ou software é gerenciada pelo provedor de nuvem e qual parte fica sob responsabilidade do cliente.
- Os principais modelos são:
  - IaaS (Infrastructure as a Service) – Infraestrutura como Serviço
  - PaaS (Platform as a Service) – Plataforma como Serviço
  - SaaS (Software as a Service) – Software como Serviço


On-Premises
IaaS
Infrastructure as a Service
PaaS
Platform as a Service
SaaS
Software as a Service
Applications
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking
You Manage
Other Manages


Gmail, Trello, Salesforce CRM, EventPro, Office 365, Google Docs
end users
SAAS
Heroku, AWS Elastic Beanstalk, Google App Engine
software developers
PAAS
AWS Elastic Compute Cloud (EC2), Microsoft Azure, Google Compute Engine
IT administrators
IAAS
less
control
more

Modelos de **Implantação**

- Nuvem Pública: infraestrutura compartilhada (ex.: AWS, Azure, Google Cloud).
- Nuvem Privada: infraestrutura exclusiva de uma empresa, local ou hospedada.
- Nuvem Híbrida: combinação de nuvem pública e privada.
- Multicloud: uso de vários provedores de nuvem simultaneamente.

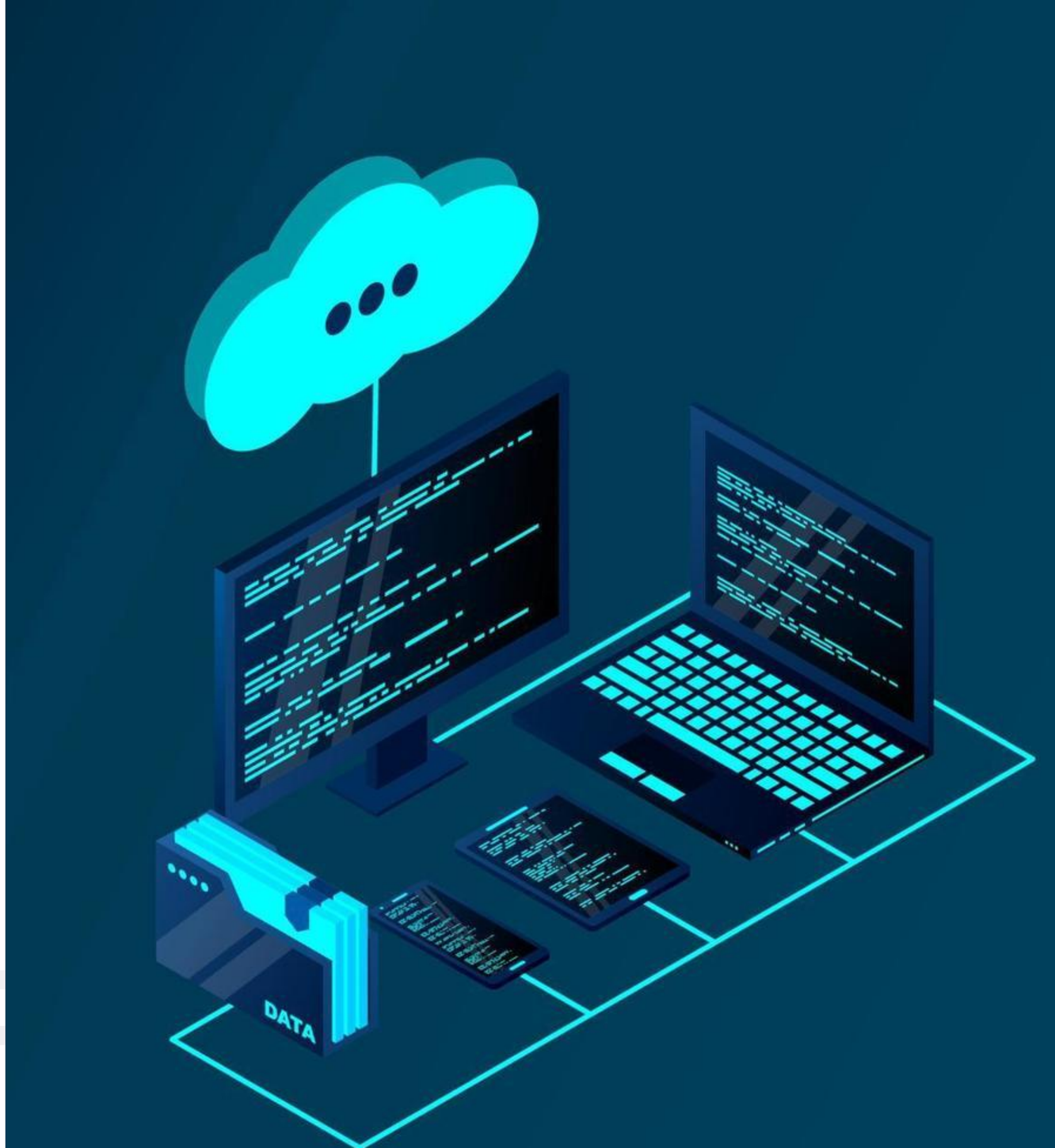
Por que IoT precisa da nuvem?

- A tendência de aplicações IoT é gerar grandes volumes de dados de sensores que precisam ser: **Coletados, Armazenados, Processados, Analisados, Disponibilizados, remotamente;**
- A nuvem fornece a infraestrutura, os serviços e a escalabilidade necessária para isso;
- Edge Computing + Cloud: Parte do processamento ocorre próximo aos dispositivos (na borda), reduzindo latência e volume de dados enviados para a nuvem.
- AIoT: Integração de Inteligência Artificial (IA) com IoT na nuvem para criar sistemas inteligentes e autônomos.

Plataformas de Cloud para IoT

- AWS IoT Core (Amazon);
- Azure IoT Hub (Microsoft);
- IBM Watson IoT;
- Google Cloud;
- Thingspeak.

Amazon Web **Services**



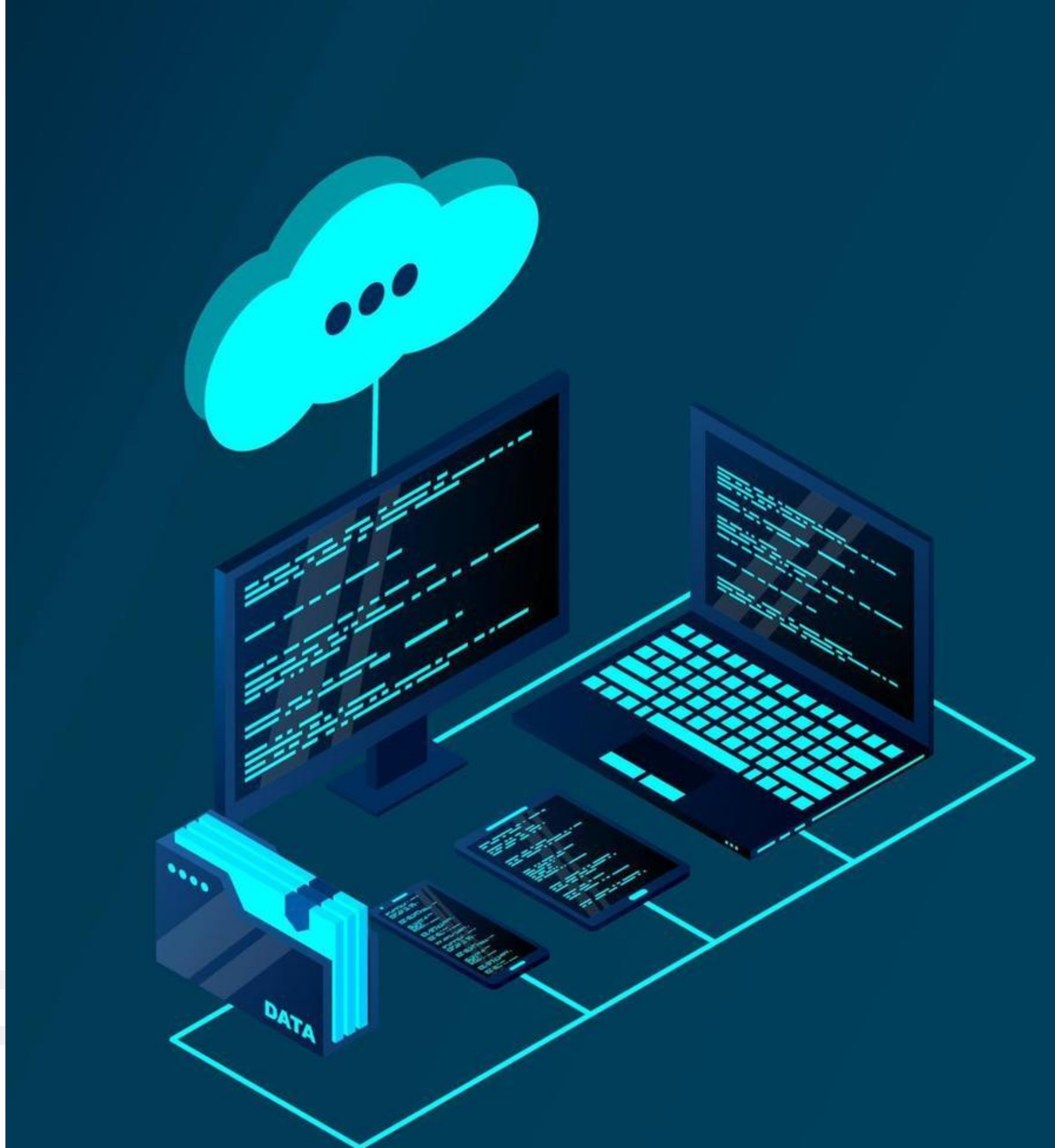
Amazon Web Services

- AWS (Amazon Web Services) é uma plataforma de serviços de computação em nuvem oferecida pela Amazon.
  - Ela fornece uma ampla gama de serviços que incluem:
  - Computação
  - Armazenamento / Banco de dados
  - Inteligência Artificial (IA) (Amazon SageMaker)
  - Internet das Coisas (IoT)
  - Análise de dados
  - DevOps e muito mais

Amazon Web Services

- AWS (Amazon Web Services) é uma plataforma de serviços de computação em nuvem oferecida pela Amazon.
- Os custos podem ser estimados:
  - https://calculator.aws/#/createCalculator/ec2-enhancement

Amazon Web **Services IoT**



Amazon Web **Services**

- O AWS IoT é um conjunto de serviços na nuvem que permite que dispositivos conectados (sensores, atuadores, máquinas, veículos, eletrodomésticos, etc.) interajam de forma segura com aplicações hospedadas na nuvem e entre si.
  - Sem instalação;
  - Escala automatizada;
  - Sem pré provisionamento;
  - Recursos da AWS;
  - Pay as you go;
  - *Milhões de dispositivos com bilhões de conexões;
- https://docs.aws.amazon.com/pt_br/iot/latest/developerguide/aws-iot-how-it-works.html;

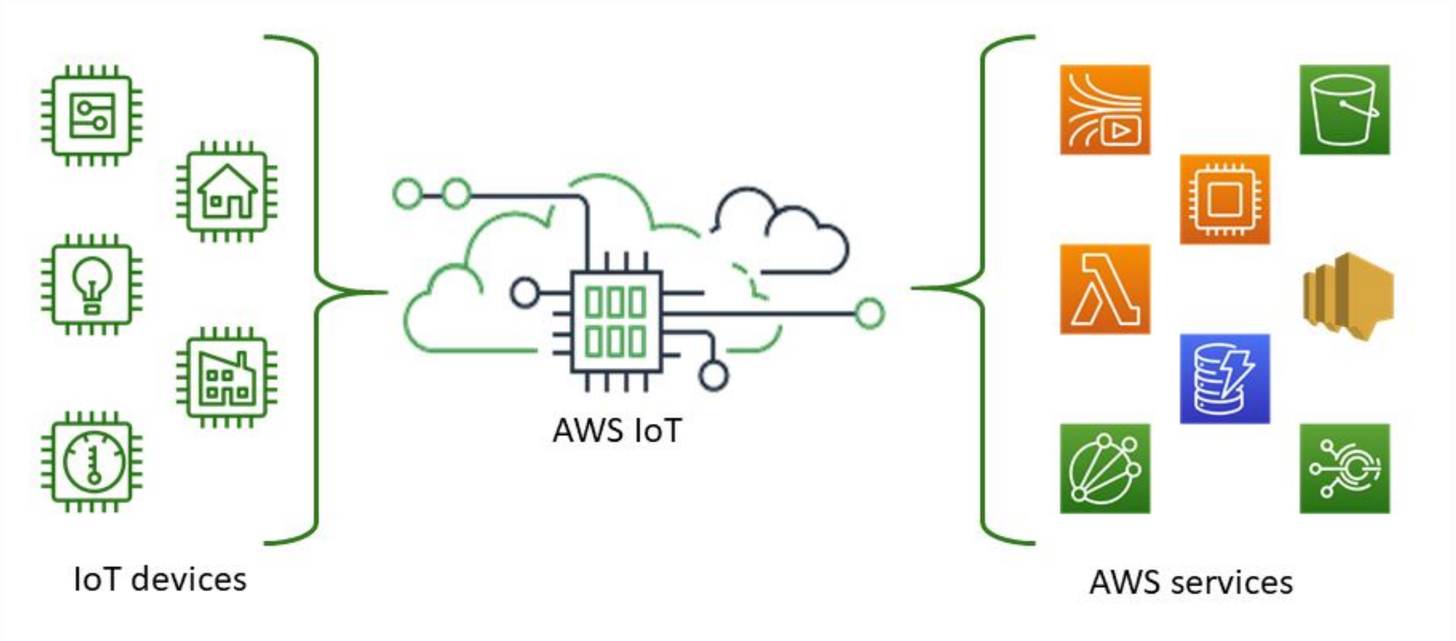
Principais Funcionalidades do **AWS IoT**

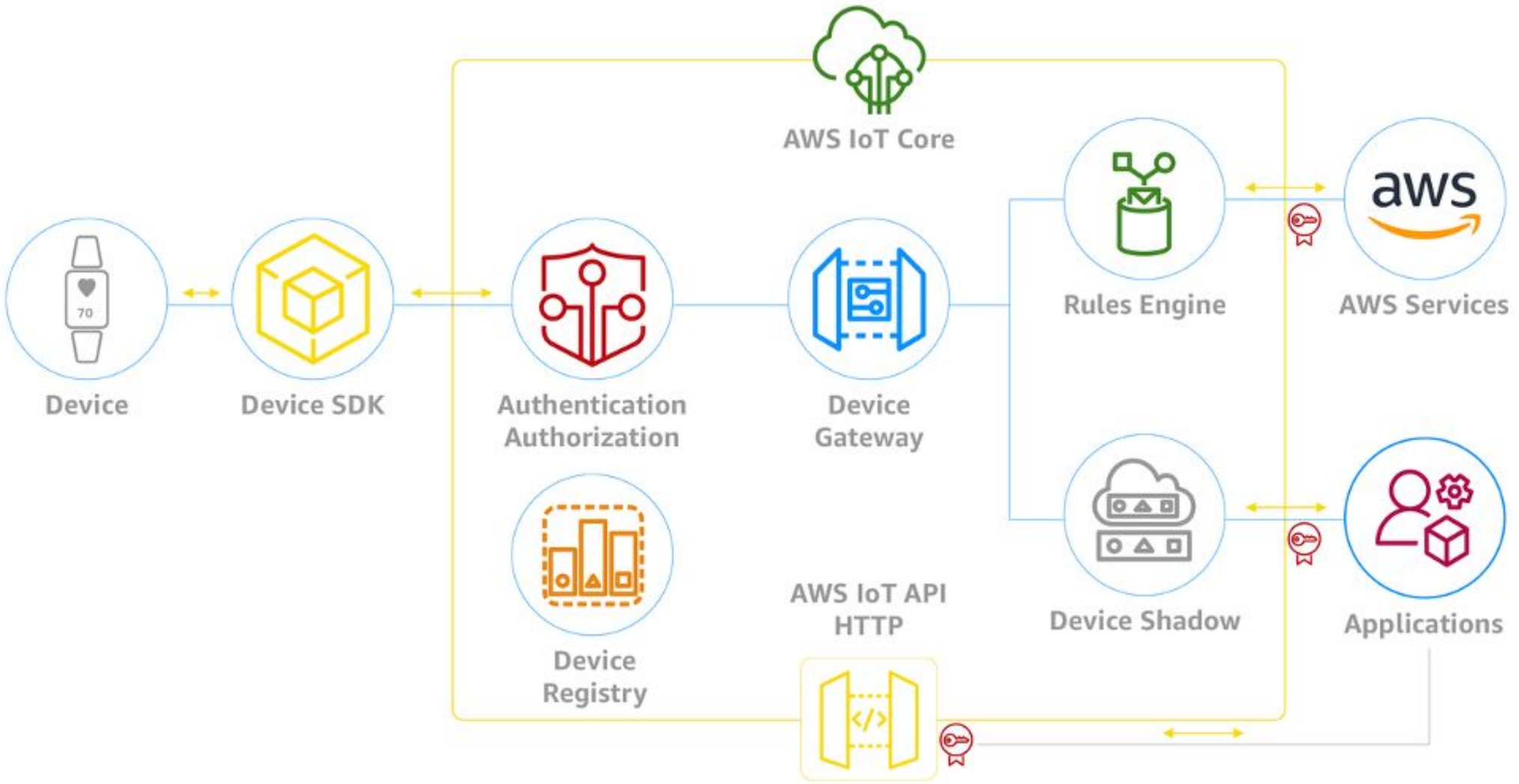
- Conectividade Segura
  - Permite a conexão de bilhões de dispositivos à nuvem via protocolos MQTT, HTTP e WebSockets.
  - Gerenciamento de identidade dos dispositivos com certificados digitais e autenticação mútua.
- Mensageria em Tempo Real
  - Usa um broker MQTT para comunicação entre dispositivos e nuvem.
  - Suporte para pub/sub (publicar/assinar tópicos) com alta escalabilidade.
- Processamento e Regras (IoT Rules Engine)
  - Permite criar regras que disparam ações, como: Enviar dados para bancos de dados; acionar funções Lambda; enviar notificações ou interagir com outros serviços AWS.
- Gerenciamento de Dispositivos
  - Cadastro, organização, monitoramento e atualização dos dispositivos.
  - Atualização remota de firmware.

Principais Funcionalidades do **AWS IoT**

- Monitoramento e Logs
  - Integração com CloudWatch para monitoramento, alertas e dashboards.
  - Logs de tráfego, erros e métricas operacionais.
- Machine Learning e Analytics: ntegra-se com serviços como AWS SageMaker, IoT Analytics e Kinesis para análises preditivas, detecção de anomalias e geração de insights.
- AWS IoT Device Shadow (Gêmeo Digital): Mantém um estado virtual dos dispositivos, permitindo consultar e modificar o estado mesmo que o dispositivo esteja offline.
- Segurança
  - Criptografia de ponta a ponta.
  - Gerenciamento de políticas de acesso detalhadas.
  - Auditorias e monitoramento de segurança.

- Broker MQTT;
- Sistema de regras;
- Dispositivos Sombreados;
- Recursos da AWS;




AWS IoT Core
Device
Device SDK
Authentication
Authorization
Device
Gateway
Rules Engine
AWS Services
Device
Registry
AWS IoT API
HTTP
Device Shadow
Applications

Como se conectar a **AWS IoT**

- AWS SDKs — Crie seus aplicativos de IoT usando APIs específicas da linguagem;
- AWS IoT API - solicitações HTTP, HTTPS ou MQTT;
- AWS Command Line Interface (AWS CLI);
- AWS IoT Core para LoRa WAN.

Publish and **Subscribe**

- Suporte aos protocolos padrões: MQTT, HTTPS, Websocket;
- Baixa latência, baixo consumo de energia, baixo uso de banda;
- Bidirecional: comunicação DE e PARA dispositivos, independente de protocolo;
- SDKS: JavaSCript, Python, Arduino, Android, Linux;

Gestão da **Segurança**

- Autenticações confiáveis com certificados x509;
- define o formato de certificados digitais usados em uma infraestrutura de chave pública;
- Autenticação mútua;
- Fácil provisonamento de certificados
- Políticas e regras para controle de acesso
- Configuração granular de operações;
- Configuração de acesso a outros serviços;

Gestão da **Segurança**

1. Anexar um certificado ao dispositivo

Um certificado de dispositivo autentica a identidade do dispositivo com o AWS IoT para que ele possa estabelecer uma conexão segura com o AWS IoT.

2. Anexar uma política ao certificado do dispositivo

As políticas concedem acesso aos recursos da AWS. A política usada para se conectar também permite que o dispositivo publique mensagens MQTT por meio do agente de mensagens do AWS IoT.

3. Seu dispositivo faz uma conexão segura

Com esses recursos definidos e configurados, o dispositivo pode se conectar com segurança ao AWS IoT e acessar seus recursos autorizados.

Gerenciamento de **Regras**

- Sintaxe similar ao SQL
- Mapeie suas entrada para diversos serviços da AWS;
- Limpe, Enriqueça e transforme seus dados;
- Diferentes formatos de payload;

AWS IoT **Shadow**

- Representação Virtual do dispositivo na nuvem
- Dispositivo sempre acessível;
- AWS armazena até um ano o estado do dispositivo;
- Baseado na última leitura ou em uma média;

Custos estimados

- Pague o que usar;
- **5$ dólares por milhão de mensagem!** Para mensagens publicadas ou recebidas em regiões como leste dos Estados Unidos (Virgínia, Ohio);
- Oregon, Alemanha, Irlanda, Inglaterra: $6 dólares na Corea do Sul e Austrália;
- Brasil: $8 dólares;
- Free tier para 250k mensagens por mês, durante um ano;

Segurança em IoT

Segurança em IoT

- Segurança em IoT é um dos assuntos mais críticos e desafiadores na área de tecnologia, principalmente porque dispositivos IoT geralmente têm limitações de processamento, memória e energia, o que dificulta a implementação de mecanismos de segurança robustos;
- É necessário um conjunto de práticas, protocolos, ferramentas e políticas destinadas a proteger:
  - Dispositivos físicos (sensores, atuadores, gateways)
  - Dados em trânsito e em repouso
  - Infraestrutura de nuvem e comunicação
  - Usuários e suas informações
- De ataques, acessos não autorizados, sequestro de dispositivos e vazamento de dados.

Segurança em IoT

- Roubo de Dados: Dados sensíveis capturados por dispositivos (ex.: localização, saúde, consumo) podem ser interceptados.
- Controle Não Autorizado: Invasores podem assumir controle de dispositivos (ex.: abrir fechaduras, desligar sensores, parar máquinas).
- Ataques DDoS (Botnets): Dispositivos comprometidos são usados para sobrecarregar sistemas (ex.: ataque Mirai).
- Vazamento de Credenciais: Dispositivos mal configurados expõem senhas, tokens ou chaves.
- Falsificação de Dispositivos (Spoofing): Um dispositivo falso se passa por legítimo.
- Ataques Man-in-the-Middle (MitM): Interceptação de comunicação entre dispositivo e nuvem.

Princípios da Segurança da Informação aplicados a IoT

- Confidencialidade: Garantir que os dados sejam acessados apenas por entidades autorizadas (ex.: criptografia de dados sensíveis). Um sensor não pode expor informações protegidas;
- Integridade: As informações fornecidas por dispositivos IoT não podem sofrem alterações em seu caminho até a nuvem;
- Disponibilidade: Assegurar que os serviços e dispositivos estejam disponíveis quando necessário (ex.: proteção contra DDoS; Uso de digital twin pode ser um ator interessante).
- Autenticidade: Verificar a identidade de dispositivos e usuários (ex.: certificados, autenticação forte).
- Não-repúdio: Garantir que uma comunicação ou transação não possa ser negada (ex.: certificados digitais)

Boas Práticas de Segurança em IoT

- Utilizar certificados digitais e autenticação mútua (TLS).
- Evitar hardcoding de senhas nos dispositivos.
- Usar protocolos seguros como MQTT sobre TLS, HTTPS, CoAP DTLS.
- Implementar firewalls, VPNs e redes isoladas para dispositivos IoT.
- Aplicar atualizações regulares (OTA) com verificação de integridade.
- Realizar auditorias e testes de segurança periódicos.
- Implementar limitação de acesso físico aos dispositivos.
- Gerenciar ciclo de vida dos dispositivos: desde a fabricação até a desativação segura.

Como a AWS IoT Trata a **Segurança**

- Autenticação mútua via certificados X.509;
- Criptografia de ponta a ponta (TLS 1.2/1.3);
- Controle fino de permissões via políticas IAM e IoT Policies.AWS IoT Device Defender: Monitoramento, auditoria e detecção de anomalias;
- Logs de conexão e operações via CloudWatch Logs e AWS Config.

Funcionamento Básico na Prática IoT

1) O dispositivo (ex.: ESP32) possui:
    a) Seu próprio certificado X.509
    b) Sua chave privada
2) Ao se conectar à nuvem (AWS IoT, neste exemplo):
3) O dispositivo apresenta seu certificado X.509.
4) A nuvem verifica se esse certificado foi emitido e assinado corretamente.
5) Ambos estabelecem uma conexão criptografada e autenticada via TLS (SSL).
6) A comunicação está protegida:
    a) Ninguém intercepta os dados.
    b) Somente dispositivos autorizados podem se conectar.

Obrigado