We are the new secure communication mindset

O Tamanho do Mercado de Cibersegurança - IoT

Violações de segurança são uma desvantagem significativa para IoT. De acordo com o IEEE, mais de 80% das organizações de saúde que usam dispositivos IoT sofreram uma falha de segurança de seus dispositivos ou infraestrutura.
Fonte: IEEE

“Cidades inteligentes" é um conceito importante e emergente em IoT. Mais de um quinto de todos os projetos de IoT anunciados publicamente envolvem "cidades inteligentes" orientadas por IoT de algum tipo, com a maioria dessas "cidades inteligentes" (45%) anunciadas na Europa.
Fonte: IoT Analytics, 2020

O Gartner prevê uma quantidade maior de "coisas conectadas" até 2020. De acordo com o Gartner, haverá mais de 14 bilhões de dispositivos conectados até o final de 2019, e mais de 25 bilhões até o final de 2021.
Fonte: Gartner, 2019

O mercado global de IoT valia mais de US$ 150 bilhões em 2018 e deve ultrapassar US$ 1,5 trilhão até 2025.
Fonte: IoT Analytics, 2020

As ameaças de segurança mais comuns à IoT foram ataques de malware (49%), erro humano (39%) e DDoS (22%).
Fonte: Aruba, 2019

Mais de um quarto de todos os ataques cibernéticos contra empresas serão baseados em IoT em 2025.
Fonte: Gartner

Gartner®

Os sistemas e serviços do segmento de IoT permitirão que provedores autorizados e administradores de clientes estabeleçam e apliquem a política de privacidade de seus dispositivos, máquinas e ativos. Incluídos no escopo deste segmento de serviços estão os serviços privados de Ponto de Acesso (APN) e serviços de rede virtual privada (VPN) gerenciada, serviços relacionados à identidade, credenciamento, autenticação e estabelecimento de confiança entre dispositivos de borda no escopo e o nuvem, incluindo recursos de acesso seguro pré-integrados com provedores públicos de nuvem.

Fonte: **Gartner 2019**

- Até 2023, 10% da conectividade gerenciada de Internet das Coisas (IoT) em todo o mundo será fornecida através de provedores de nuvem de hiperescala, superando menos de 1% em 2019.

- Até 2022, 40% dos fornecedores globais de conectividade de IoT gerenciada oferecerão redes 3GPP de baixa potência (LPWA) (NarrowBand IoT [NB-IoT] e Evolução de Longo Prazo para comunicações do tipo máquina [LTE-M]) roaming cobertura, superando 0% em 2019.

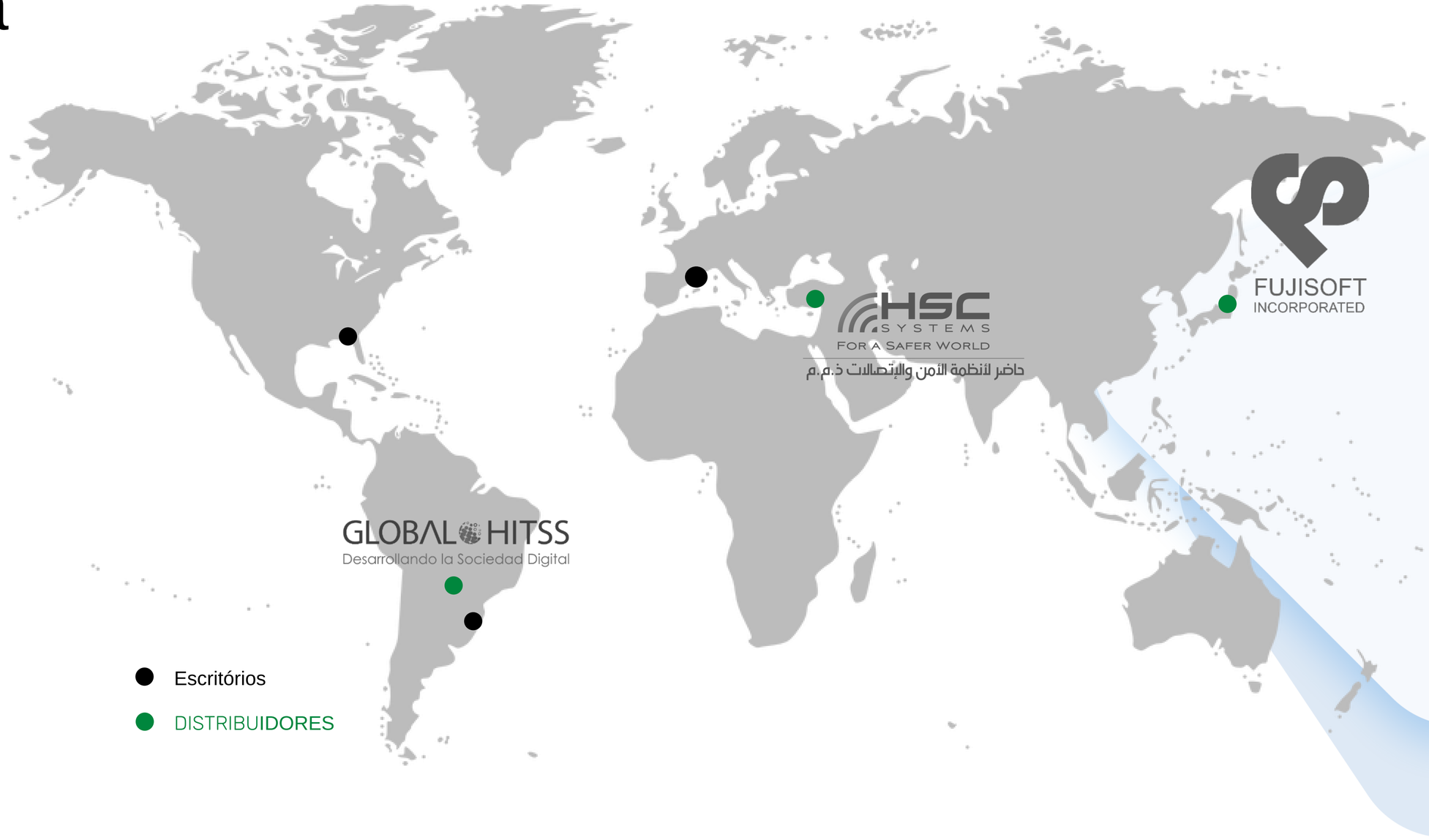
- Até 2023, mais de 60% de todos os novos veículos conectados produzidos contarão com um SIM incorporado (eSIM) para conectividade celular, acima dos menos de 5% em 2019.

- Até 2023, 80% dos fabricantes que incorporam serviços 3GPP usarão um modelo de participação de receita de parceiros, acima dos 20% em 2019.

Fonte: **Gartner 2019**

A Companhia

A Sikur está definindo o futuro da comunicação segura, operando globalmente, através de seus escritórios e distribuidores no Brasil, Estados Unidos, Europa, Oriente Médio e Japão. A Sikur trabalha ao lado de governos e corporações que acreditam que a segurança é fundamental para a integridade de seu trabalho. Acreditamos que a segurança não se trata apenas de plataformas e sistemas digitais, mas é uma mentalidade que envolve todos os aspectos de um negócio.



SIKUR LAB

O Sikur Lab é o novo laboratório de inovação e pesquisa localizado em Sophia Antipolis, França. Sikur é membro do setor de Segurança Digital do Sophia Antipolis SCS Cluster (Secure Communicating Solutions), que é um ecossistema europeu líder em microeletrônica, internet das coisas, segurança digital, inteligência artificial e big data. Estabelecemos nosso laboratório de pesquisa neste local porque é um hub de rápido crescimento em tecnologias avançadas. Agora, a digitalização é o cerne de tudo relacionado ao desenvolvimento humano, e a França está ocupando um papel central, como temos notado nos últimos anos. Isso está acontecendo em paralelo com o desenvolvimento da Sikur como empresa, e queremos participar disso, no mesmo ritmo rápido.

SOPHIA ANTIPOLIS

SECURED COMMUNICATING SOLUTIONS
A WORLD-CLASS CLUSTER

UNIVERSITÉ CÔTE D'AZUR

IMREDD
INSTITUT D'INNOVATION ET DE PARTENARIATS

Exposição Global

SIKUR: “ONE OF THE MOST EXCITING PHONES AND GADGETS FROM MWC 2018”

WIRED

Gartner®

According to Gartner, SIKUR is a vendor that has relevant solutions to this technological space

hackerone

Pushing its technology to the limit, SIKUR launched the safest smartphone ever in 2016. Not satisfied delivered it to the world best hackers and gave them a mission: break it. They failed.

Mashable

c|net

Forbes

WSJ

TechCrunch

CNBC

engadget

CNN

REUTERS®

Bloomberg

Fundação Segura – H2H/ H2M/ H2M2M

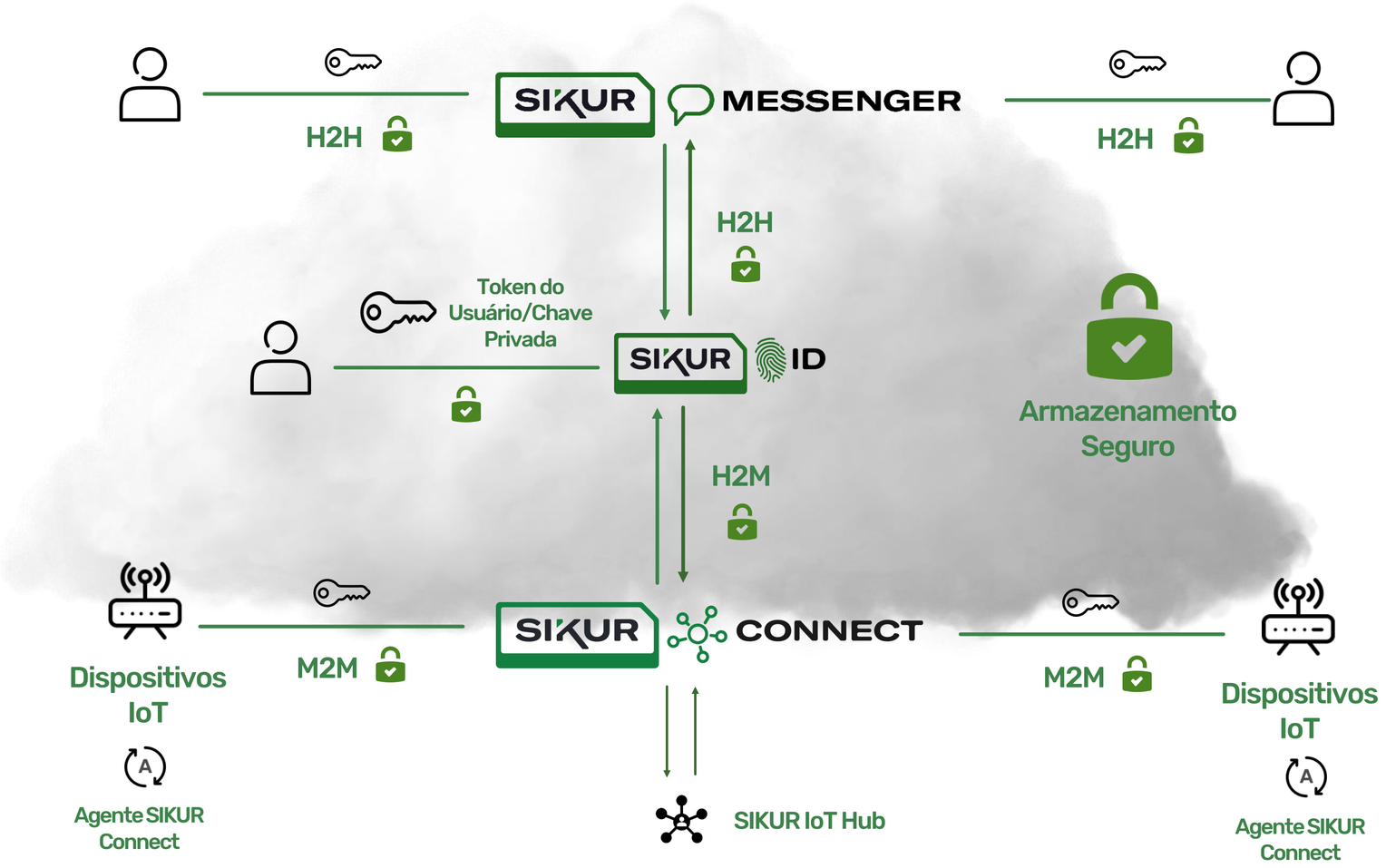
Nuvem

APPs

Endpoints

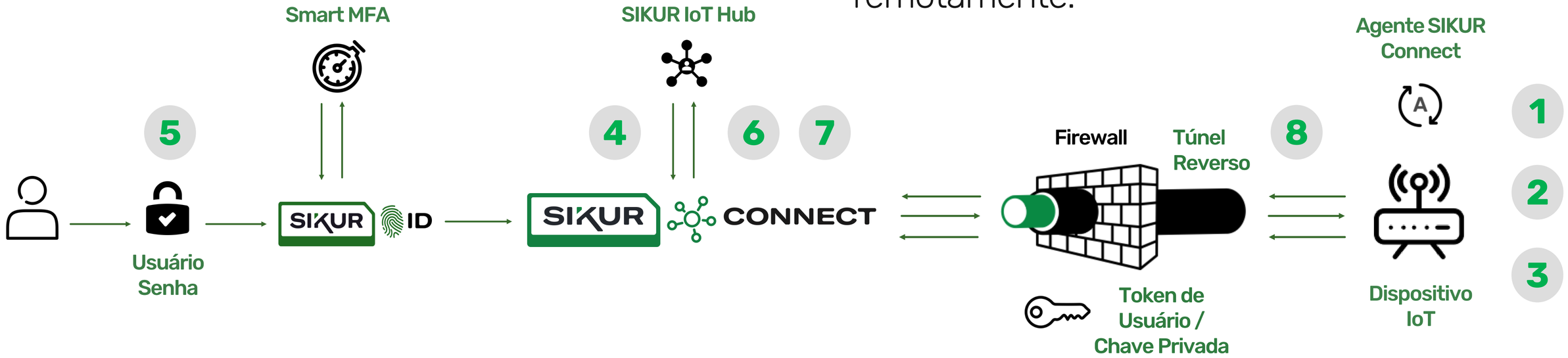
Solução de Comunicação Encapsulada

1. Autenticação forte
2. Não-repúdio
3. Armazenamento seguro
4. Comunicação segura



A Solução – H2M2M – passo a passo

Autenticação e Controle para proteger os ativos e gerenciá-los remotamente.



1. Instalação do agente de dispositivo
2. Definição do hub
3. O agente gera o par de chaves (pública e privada) e autentica no Hub de destino
4. O Administrador cadastra usuários no Sikur Connect, para gerenciamento de dispositivos
5. Os usuários criam credenciais no Sikur ID, gerando seu par de chaves (pública e privada)
6. O Administrador define as permissões de acesso do usuário aos dispositivos para cada Hub, sem credenciais visualizando o acesso
7. O usuário pede permissão para conexão do dispositivo
8. O Agente abre um túnel reverso, iniciando uma comunicação segura para que o usuário possa gerenciar o dispositivo

O Produto – Características

Gestão de Identidade

- Acesso seguro do usuário a qualquer sistema e aplicativo IoT
- Eliminação de senhas padrão

Autenticação

- Controle de usuário e permissão em aplicativos e sistemas
- Autenticação forte, usando chaves de criptografia e automação

Auditoria e Conformidade

- Monitoramento de uso e alertas de segurança
- Conformidade com as regulamentações globais

Armazenamento seguro

- Armazenamento seguro de dados coletados dos dispositivos

Túnel seguro

- Um túnel de acesso seguro para dispositivos, mesmo em redes instáveis
- Túnel de acesso reverso quando as restrições de firewall se aplicarem

Zero Touch

- Implantação automática
- Provisionamento remoto de novos dispositivos
- Registro fácil e sem contato

Gerenciamento de dispositivos

- Nenhum dispositivo será acessível anonimamente
- Atualizações seguras
- Proteção contra roubo de equipamentos

Coleta segura de dados

- Coleta segura de dados de dispositivos

O Produto – Proposta de valor para fornecedores de IoT

Segurança

- Entrega valor por meio das camadas de segurança extras
- Autenticação adequada e proteção de dados
- Túnel reverso de dados
- Criptografia de dados
- Mensagens com os algoritmos de criptografia mais atualizados
- Proteção de chaves, com hardware
- Proteção em camadas contra ataques
- Armazenamento Seguro
- Coleta segura de dados

Conformidade com GDPR

Autenticação em Nuvem Híbrida

Proteção de dados com fortes padrões de criptografia da indústria

Manutenção de acesso remoto

- Gerência de dispositivos remotos
- Otimizado para redes de baixa velocidade
- Monitoramento em tempo real
- Visibilidade de dispositivos
- Atualização e controle de firmware

O Produto – Proposta de Valor para a Indústria

Gestão Rápida

- Gerenciamento de dispositivos remotos
- Otimizado para redes de baixa velocidade
- Monitoramento em tempo real

Login único

- Controle quem tem acesso a dispositivos, de forma granular e sem senha
- Seguro e flexível. Ninguém mais – do que você – terá acesso.

Segurança

- Proteção de dados com criptografia poderosa e leve
- Proteção de informações para dados em trânsito e em repouso
- Autenticação de múltiplos fatores
- Proteção em camadas contra ataques
- Coleta segura de dados
- Armazenamento seguro

Autenticação em Nuvem Híbrida

RBAC: Controle de acesso baseado em função

Visibilidade e controle do dispositivo

Bloqueio de contas e monitoramento comportamental

Integração SIEM: fornece informações de registro para sistemas de terceiros

Padrões da indústria

Modelo de Negócio

Seguindo uma tendência mundial de
micro redes privadas com usabilidade

White Label

Nuvem Híbrida

Sikur Cloud

Azure

Private Cloud

Azure ou On-Premises

Diferenciais de Produto

1. **Zero Touch**
configuração simplificada, remota e automática

2. **Modelo de Negócio**
solução de nuvem híbrida e White Label

3. **Conformidade regulatória**
proteção de dados com chaves de usuário, privadas

4. **MFA protegido**
forte e flexível

5. **Proteção de credenciais**
automação de processos, evitando o uso indevido de credenciais

6. **Seguro desde o início**
sem senhas padrão, geração de chaves fortes

7. **Escalável e gerenciável**
arquitetura distribuída para crescer consistentemente, gerenciar e atualizar versões de software

8. **Coleta e armazenamento de dados seguros**
armazenamento e coleta segura de dados

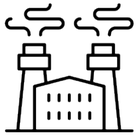
Regulação de IoT – Proposta Governamental do Reino Unido

1. **As senhas do dispositivo IoT não devem ser configuradas de fábrica, com padrão conhecido**
2. **Armazenamento e gerenciamento de credenciais seguras**
3. **Integridade do software**
4. **Acesso por autenticação segura**

SIKUR Connect cumpre (1), (2) e (4), o (3) está no roadmap

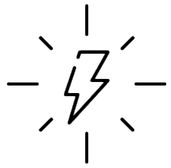
Autenticação e proteção de dados são o centro das regulamentações de dados existentes e devem ser para os próximos. O **SIKUR Connect** cumpre com a maioria deles, entregando excelente gestão.

Onde ele pode ser aplicado



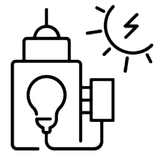
Industrial

Dispositivos IoT no chão de fábrica (indústria automotiva, sensores do agronegócio, siderúrgicas, mineradoras, etc.)



Energia

Infraestrutura de sistemas de energia e instalações (medidores inteligentes, controladores lógicos programáveis, plataformas SCADA, etc.)



Cidades Inteligentes

Veículos e transporte (carros autônomos/sem motorista, sistemas de controle de tráfego urbano, plataformas de cidades inteligentes, sensores, câmeras e sistemas de videomonitoramento, etc.)

Saúde

Sistemas e aparelhos de saúde (equipamentos hospitalares, sensores corporais, dispositivos e-Saudáveis, etc.)

Petróleo e Gás

Manutenção preditiva e preventiva, rastreamento e monitoramento de ativos, gerenciamento de dados

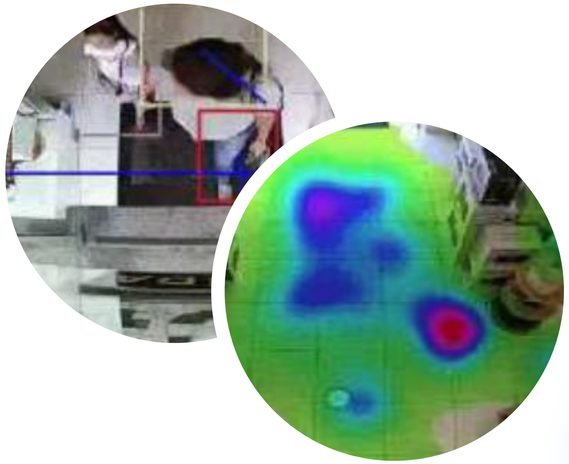
Casas e edifícios inteligentes

Dispositivos de automação residencial e predial (controle de acesso, câmeras de CFTV, dispositivos de ponto final geral, etc.)

Cases

AGVS

- Industrial, para automação e logística
- Robôs autoguiados
- Melhor controle e visibilidade



Visão do DOD

- Gerenciamento de cameras
- Lojas de varejo distribuídas
- Imagens em tempo real para gerenciamento de campanhas de marketing

Apêndice

Por que nossa solução é disruptiva?
Desafios para a IoT

SIKUR CONNECT

Por que nossa solução é disruptiva?

1. Garante segurança para dispositivos IoT e plataformas IoT
2. As soluções de mercado dependem de Firewalls e soluções de segurança tradicionais como senhas (soluções de segurança à moda antiga)
3. O Connect gerencia e controla dispositivos IoT, não deixando brechas para atacantes externos
4. A solução faz o inventário das dispositivos em um Hub de IoT criptografado
5. A solução Sikur Connect cria "túneis seguros exclusivos" para comunicação entre os dispositivos IoT e o Gerenciamento Hub IoT
6. Vai muito além e conta com uma chave de identificação única, criada em cada dispositivo IoT quando conectado pela primeira vez ao hub
7. Ele garante a conexão e comunicação H2M (Humana para Máquina) de ponta a ponta e segura

Desafios para a IoT

Personificação/Falsificação de Identidade: isso significa que o invasor usa uma identidade falsa, comunicando-se com o dispositivo IoT em nome de uma entidade legítima

Escutas: interceptação da comunicação eletrônica, que acontece porque os dispositivos IoT muitas vezes utilizam infraestrutura de comunicação pública

Adulteração de dados: modificação não autorizada de dados, que pode ocorrer no dispositivo IoT ou quando em troca de dados com a rede

Problemas de autorização e controle de acesso: o invasor ganha acesso ao dispositivo e, em seguida, manipula o próprio dispositivo e/ou a rede.

Privacidade: o invasor usa dados privados hospedados no dispositivo IoT para explorá-los por razões desconhecidas/não autorizadas

Interoperabilidade e gateways: como vários dispositivos IoT não se comunicam usando TCP/IP, mas outros protocolos, gateways e outros processos de comunicação chegam à rede, e estes são portas abertas para atacantes

Como resolver?

SIKUR CONNECT

- Apenas usuários com ID Sikur podem acessar o dispositivo

SIKUR CONNECT

- Os dispositivos só podem ser acessados através do Túnel Seguro

SIKUR CONNECT

- Sikur ID e o túnel seguro garantem que não haja adulteração.

SIKUR CONNECT

- Apenas usuários com ID Sikur podem acessar o dispositivo

SIKUR CONNECT

- Sikur ID e Túnel Seguro garantem privacidade

SIKUR CONNECT

- Os gateways externos devem estar com o Sikur Connect para serem protegidos.

Desafios para a IoT

Código comprometedor e malicioso: os atacantes podem direcionar os dispositivos IoT com código malicioso ou infecção por software, uma vez que eles geralmente não são resistentes a adulterações e, em seguida, comprometendo-os fisicamente.

Problemas de Disponibilidade Virtual e DoS (Negação de Serviço): os atacantes podem tornar os dispositivos IoT indisponíveis como resultado do ataque DoS. Um exemplo deste problema foi um ataque do DoS distribuído, tendo como alvo a infraestrutura Internet no leste dos EUA, através de milhares de dispositivos IoT elementares, como câmeras de CFTV e outros eletrodomésticos, resultando em um grande apagão de comunicações.

Disponibilidade física: o invasor pode direcionar as características físicas do dispositivo IoT para destruí-lo parcialmente ou totalmente, com o objetivo de enviar mensagens errôneas para a rede.

Como resolver?

SIKUR CONNECT

- Criamos um túnel para acessar o dispositivo usando um hub, evitando acesso descontrolado.
- Registramos sessões de acesso ao dispositivo e atividades maliciosas.

O que não fazemos: evitar instalação de código malicioso uma vez que o usuário esteja no dispositivo.

SIKUR CONNECT

- Dispositivos em nosso hub não precisam de portas abertas que possam ser exploradas, pois o fluxo de conexão ocorre de dentro para fora.

O que não fazemos: evitar ataques DDoS na infraestrutura. Soluções projetadas para este fim podem ser usadas em conjunto com a nossa.

SIKUR CONNECT

- Nós só permitimos tráfego autorizado para o dispositivo a partir da rede.

O que não fazemos: controlar o acesso ao dispositivo físico e suas portas.

ibs info
business solutions
integradora de sistemas

We are the new secure communication mindset

SIKUR CONNECT

NOSSOS CONTATOS

Para saber mais sobre adesão, entre em contato com nossa equipe comercial:

marcos.damiao@ibs1.com.br

andree.miranda@ibs1.com.br

comercial@ibs1.com.br

Telefone / Fax
55 21 2233-5374 - 21 2256-4552
21 3178-4110

Cel. WhatsApp:
21 99904-4974
21 97168-5754