ONELAYER

ONELAYER × UTCAL · SEGURANÇA DE REDES CELULARES PARA UTILITIES

device: ?

A rede que o seu SOC não consegue ver.

DOIS CENÁRIOS · DOIS DISPOSITIVOS
UM WEBINAR AO VIVO

FELIPE MAHATMA · ENGENHEIRO DE PRÉ-VENDAS · 06 DE AGOSTO DE 2026 · 14H · ZOOM

ONELAYER.COM

A rede que mais cresce na sua operação nasceu fora do seu SOC.

AMI, automação de distribuição, teleproteção e equipes de campo já rodam sobre celular — LTE privado ou APN de operadora. E as ferramentas em que o seu SOC confia não foram feitas para enxergar dentro dessa rede.

250+

projetos de redes celulares privadas só no Brasil — o maior mercado da América Latina

US$ 629mi

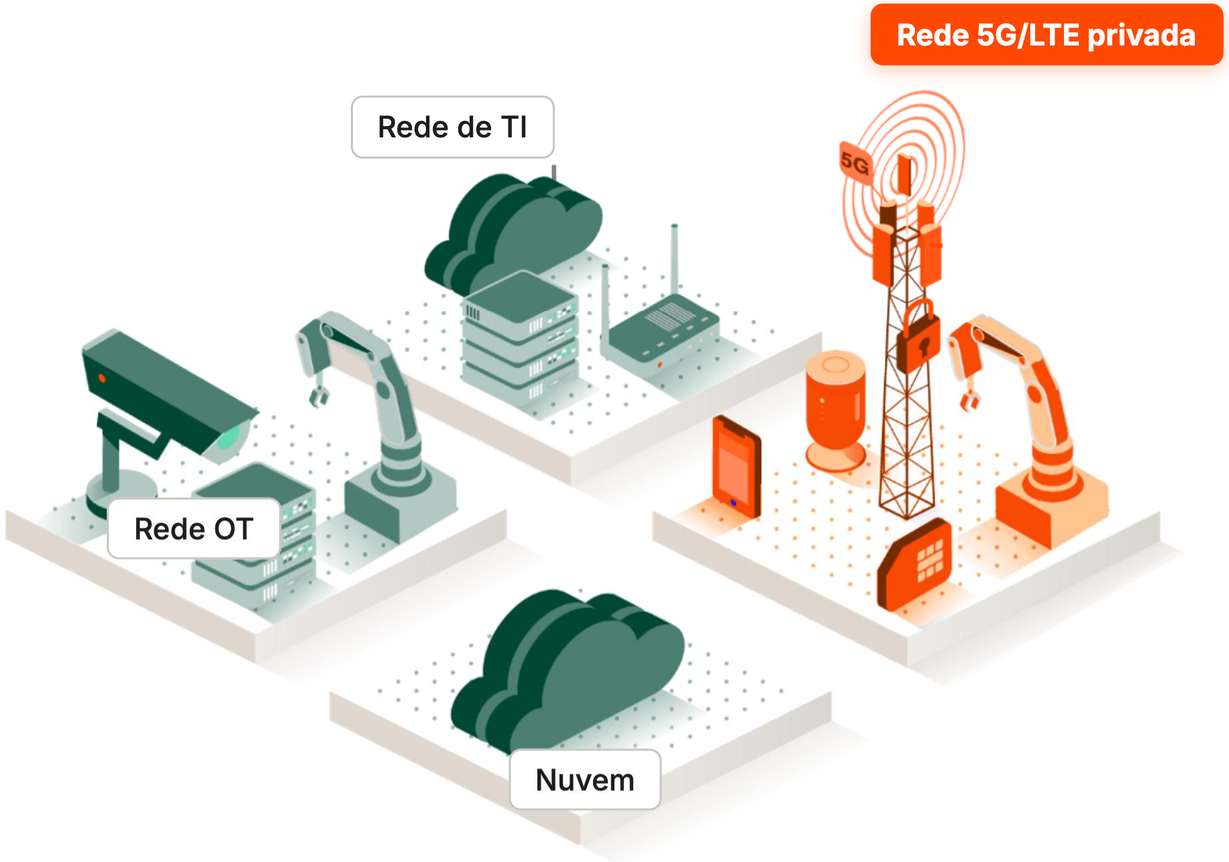
mercado LATAM de redes privadas até 2030 — CAGR de 43%

66

licenças de espectro privado emitidas pela ANATEL

0

sensores do seu SOC dentro dessa rede — hoje



Fontes: Grand View Research · RCR Wireless · Mobile Time · ANATEL

Sua rede autentica chips. Este webinar segue dois dispositivos.

MED-0441

APN PRIVADO

O QUE É	Medidor inteligente · AMI
IDENTIDADE	eSIM · IMSI 724 06 ···
INSTALADO	2026 · Brasilia, DF
REDE	APN privado · operadora

Um entre **milhões** do rollout de AMI. O que acontecer com ele, acontece em escala.

SUB-112

LTE PRIVADO

O QUE É	Roteador de subestação
IDENTIDADE	SIM própria · LTE privado
INSTALADO	2021 · subestação · PR
REDE	Core próprio · seus sites

Atrás dele: RTUs, câmeras e HMIs — **uma LAN que nenhum painel vê**.

MED-0441 vive na rede de uma operadora; SUB-112, na rede que você mesmo opera. **Dois cenários, o mesmo ponto cego** — e os dois atravessam os três atos deste webinar.

Em cada ato: **o que acontece → o que a rede vê → o que a OneLayer muda.**

A LINHA DOS ATOS — O MAPA DESTE WEBINAR

1. O ponto cego
2. Por que o SOC não vê
3. Estender sem reconstruir
4. **O placar**

Seu SOC vê tudo. Quase.

> **Uma lacuna de visibilidade é uma lacuna de resposta.**

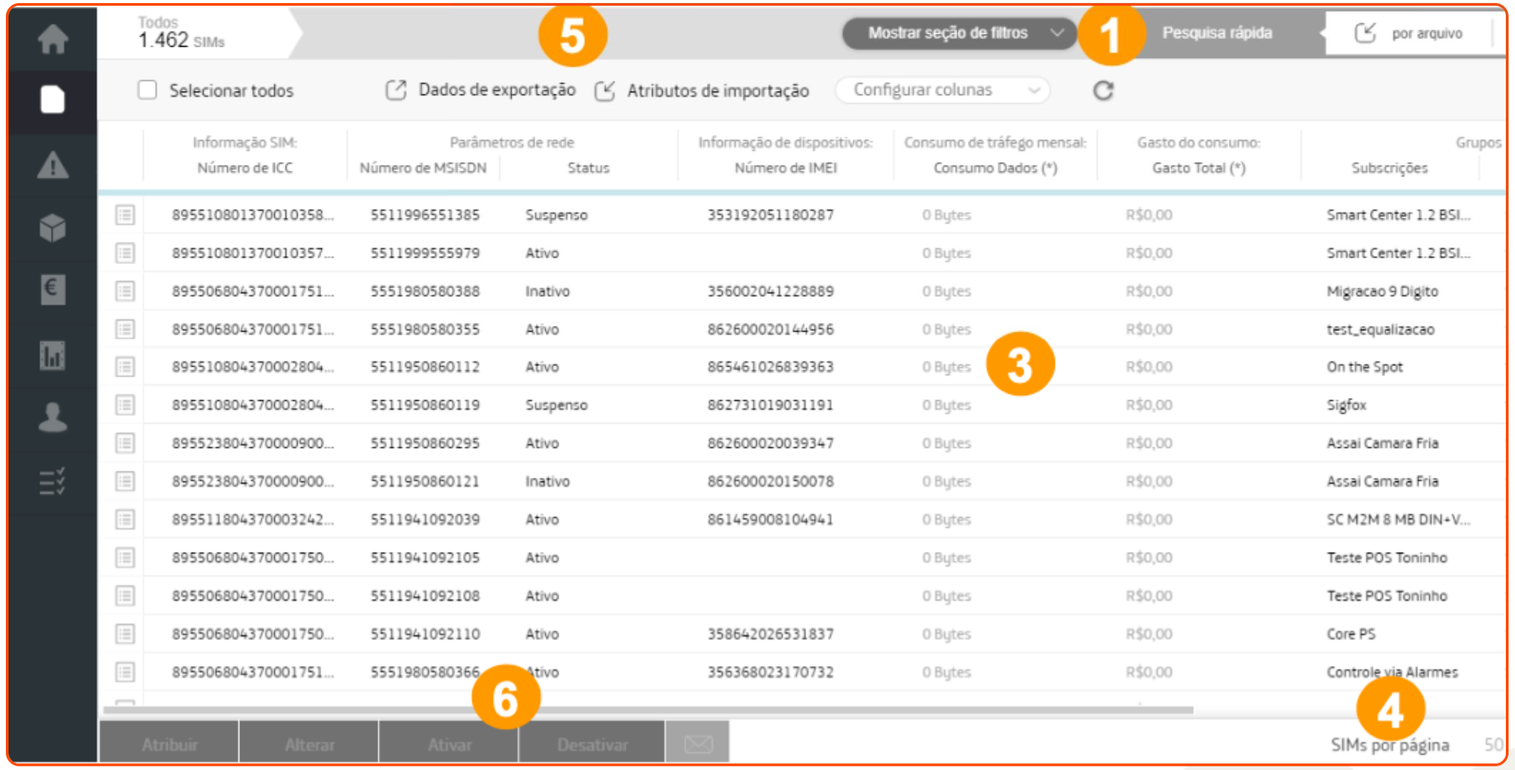
O PARADOXO

Privado ≠ Seguro

Isolamento não é segurança.

Dois painéis, a mesma resposta: um chip saudável.

As redes celulares foram projetadas para operadoras cobrarem assinantes — não para empresas protegerem infraestrutura crítica. MED-0441 mede consumo num poste em Brasília; SUB-112 conecta RTUs, câmeras e HMIs numa subestação no Paraná. Para os dois painéis, a resposta é a mesma: **status, IP e consumo. Nunca o dispositivo — nunca o que vive atrás dele.**



Painel da operadora · 1.462 SIMs. Nenhuma coluna diz o que o dispositivo é, onde está, ou o que deveria fazer.

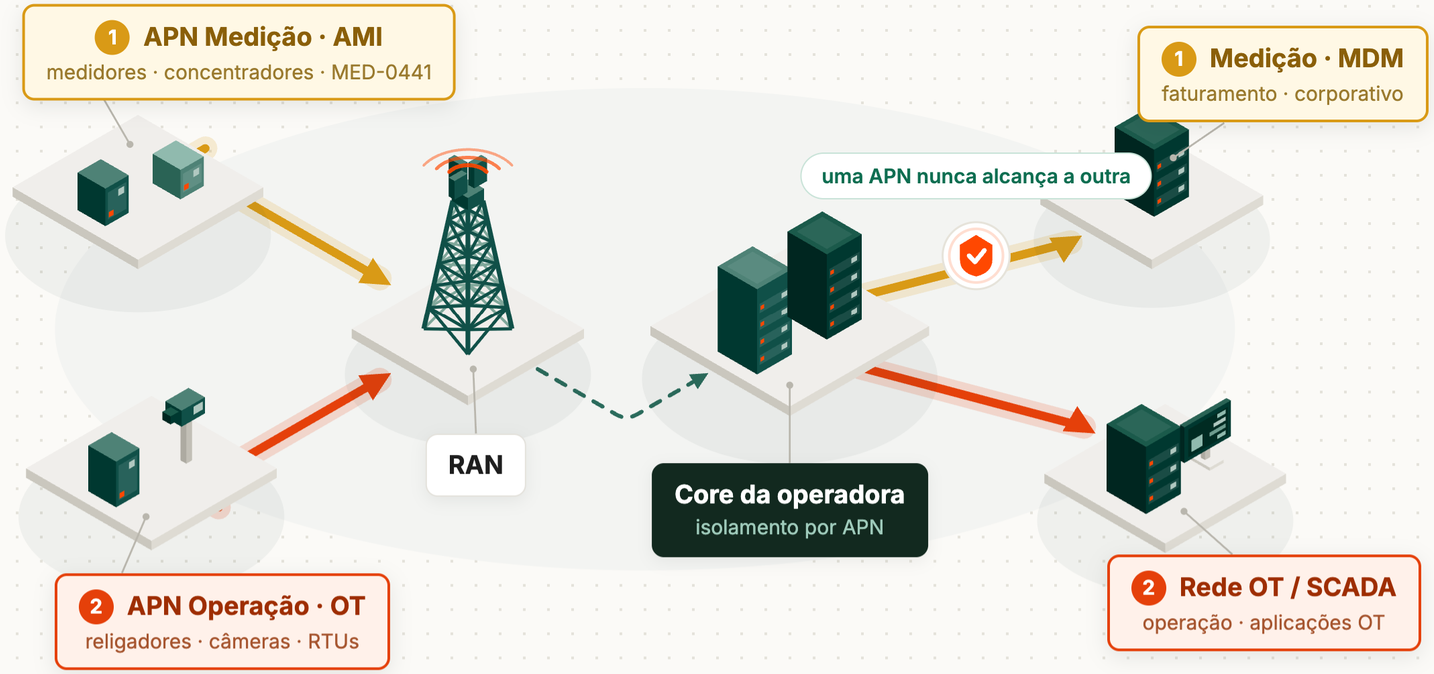
> **Invasores não entram pelos ativos que você monitora. Entram pelos que você esqueceu.**

Segmentar por APN funciona — para o que foi desenhado.

A PROMESSA · UMA REDE PARA CADA APN

1 APN MEDIÇÃO

2 APN OPERAÇÃO



Separadas de verdade

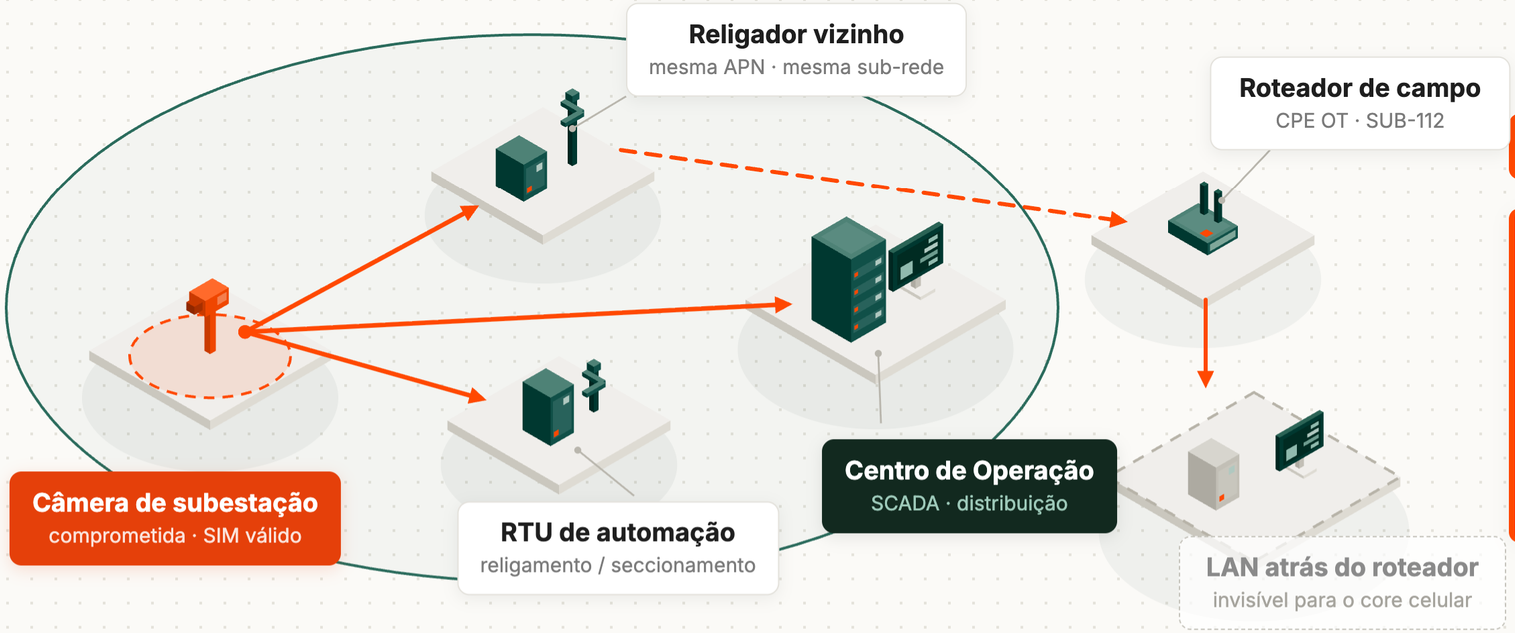
Uma APN nunca alcança a outra — o core garante o isolamento entre redes. A promessa se cumpre.

E dentro de cada uma? Nada separa dispositivo de dispositivo.

> A APN separa rede de rede. **E dentro de cada uma?**

Dentro da APN, a movimentação lateral é a configuração de fábrica.

DENTRO DE UMA APN · UMA ZONA DE CONFIANÇA



movimento lateral · leste–oeste

INCIDENTE REAL · INDÚSTRIA

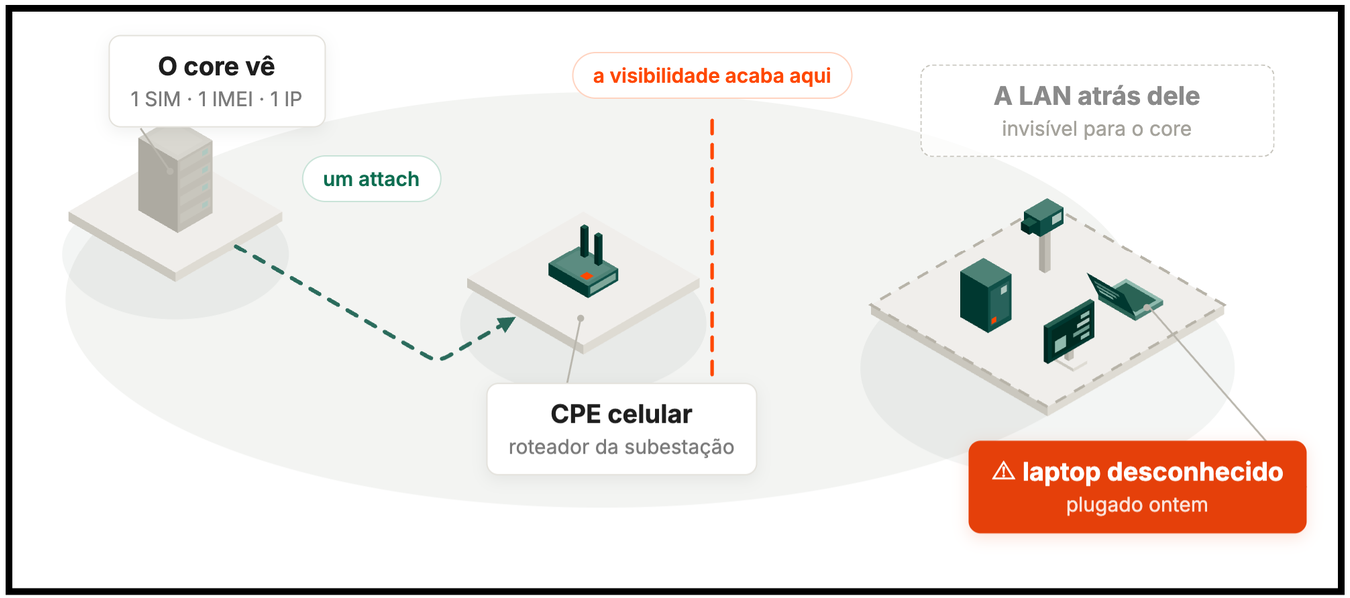
LockerGoga · Norsk Hydro, mar 2019 — 170 plantas em operação manual, ~US$ 70 mi de prejuízo. Confiança plana foi o multiplicador.

↗ news.microsoft.com/source/features/digital-transformation/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/

Um dispositivo comprometido alcança religadores, RTUs e o SCADA — a APN só separa quem está fora dela.

Um SIM pode esconder um segmento de rede inteiro.

O core vê SUB-112 como um attach saudável: um SIM, um IMEI, um IP. Atrás dele: RTUs, câmeras, HMIs — e o laptop que um terceirizado plugou ontem. **Troque, adicione, substitua: o SIM segue válido e a rede nunca percebe.** Em termos Purdue: a rede não reflete mais o que está conectado.



A dois saltos do seu monitoramento — em cada subestação, cada site, cada caminhão.

ACONTECEU DE VERDADE · MAI 2025 · REUTERS

Rádios de comunicação **não documentados** encontrados em inversores solares importados — direto na cadeia do grid.

↗ reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/

> **“ O que vive atrás do roteador não existe — até o dia em que ataca.**

Um SIM movido para outro dispositivo herda toda a confiança dele.

A autenticação celular acontece no SIM, não no dispositivo. Mova um chip válido para outro hardware — o SIM de um CPE furtado em um laptop, um módulo trocado em campo — e a rede o acolhe: mesmo IMSI, mesma APN, mesmo acesso. Nada nos logs do core parece errado, porque **pela definição da rede nada está errado**.

O QUE A REDE VÊ

```
imsi: válido ✓ · apn: correta ✓
Dispositivo: ??? · alerta: nenhum
```

INCIDENTE REAL · CASO PÚBLICO — 2018

SIM swap de Michael Terpin: US$ 24 mi roubados depois que a operadora moveu o número dele para um invasor.

Por que importa aqui: Um SIM válido no dispositivo errado autentica sem ressalvas. Identidade na camada do SIM não é identidade do dispositivo.

↗ law.justia.com/cases/federal/appellate-courts/ca9/23-55375

> **A rede autentica um SIM. Você precisa autenticar um dispositivo.**

«Travamos o SIM no IMEI do dispositivo.» Vamos testar.

O IMEI é autodeclarado: um dispositivo com root transmite o número que quiser. Os controles no caminho — lista de permissão, SIM-lock — conferem essa string e liberam, **sem nunca verificar o hardware por trás**.

```
O QUE A REDE VÊ
imei declarado: 35—20⋯23 ✓ aceito
hardware real: desconhecido
acesso: liberado
```

A TI viveu esse mesmo problema com MAC spoofing — e resolveu com NAC, que faz fingerprint do dispositivo, não do endereço que ele alega. **A celular privada não tem NAC.**

> Gratuito, um comando. Se um invasor casual derrota o controle, **não é um controle — é teatro de segurança.**

ACONTECEU DE VERDADE — 2023– · GitHub

Clonar um IMEI está a um repositório público de distância.

↗ github.com/Untouchable17/Android-IMEI-Changer

Um eSIM confiável ainda pode estar dentro de um dispositivo vulnerável.

Se você considera o eSIM uma bala de prata, pense de novo.

A PILHA QUE O ESIM NÃO COBRE

Camada SIM — eSIM / eUICC	credenciais ancoradas no silício.	✓ BLINDADO
Firmware do modem	CVEs genéricas de modem LTE / 5G — ciclos de patch lentos.	✕ EXPOSTO
SO do host · aplicações	CVEs de camada de aplicação no dispositivo atrás do SIM.	✕ EXPOSTO
Hardware não autorizado	um dispositivo intruso com um eSIM legítimo continua sendo intruso.	✕ EXPOSTO

NOSSA VISÃO

O eSIM resolve identidade do assinante. Não resolve postura do dispositivo. A superfície de ataque migra para cima na pilha — para o firmware do modem, o SO do host e a pergunta que sua rede nunca faz: **esse dispositivo deveria estar aqui?**

EXEMPLO · EXPLORAÇÃO ATIVA

CISA KEV · dez 2025

Sierra Wireless AirLink ALEOS

Um eSIM blindado não teria impedido isso.

CVE	CVSS
CVE-2018-4063	8.8 / 9.9

O QUE É

Upload irrestrito de arquivos na interface de gestão do roteador AirLink — uma requisição HTTP forjada instala um executável no dispositivo. O ACEManager roda como root, então o upload roda como root.

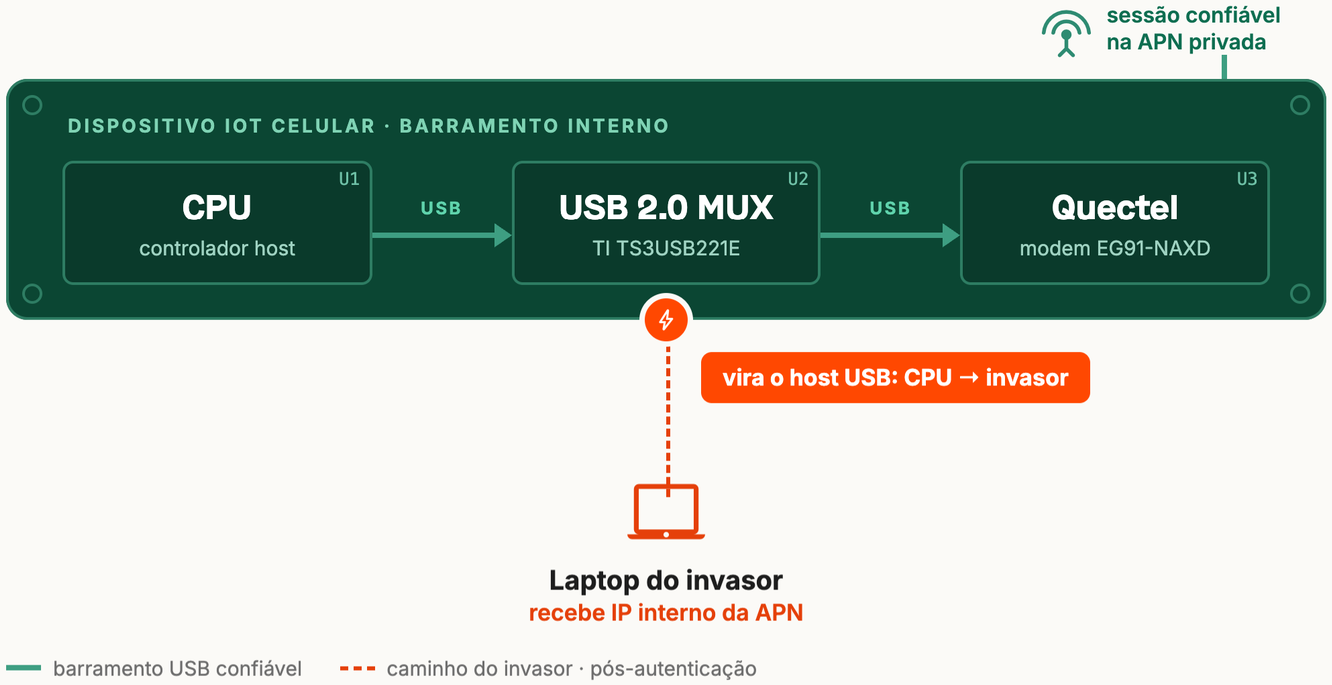
POR QUE IMPORTA AQUI

Uma falha de seis anos em um roteador celular — a CISA confirmou exploração ativa e a incluiu no KEV em dezembro de 2025. eSIM, SIM-Lock e regras de firewall da APN são todos ortogonais a isso. **O SIM está bem. O dispositivo está dominado.**

↗ Fonte · Catálogo CISA KEV · Relatório Cisco Talos (2019) · Análise de honeypot Forescout Vedere Labs (2025)

> “ **O eSIM acaba com o SIM removível — não com o risco. Ele blinda o provisionamento; a exposição só sobe na pilha.**

Um invasor sequestra o próprio modem, depois que a autenticação termina.



Rapid7 (2026): após a autenticação, um multiplexador USB entrega o modem ao laptop do invasor — que ganha um IP interno da APN pelo caminho confiável.

1. Dispositivo autentica na APN privada — o eSIM é válido, a sessão é confiável
2. O MUX vira o host USB: CPU → invasor — multiplexador TI TS3USB221E, pós-auth
3. O ECM atribui ao laptop do invasor um IP interno da APN
4. O tráfego passa pelo modem confiável — para dentro da rede privada

CONTROLES DERROTADOS

SIM-Lock · eSIM · vínculo de IMEI · regras de firewall da APN. **Todos irrelevantes quando a própria confiança do dispositivo é a arma.**

NOSSA VISÃO

A IA está baixando a barreira — exploração de hardware que era coisa de especialista agora é reproduzível com engenharia reversa assistida por IA.

OBSERVAÇÃO ONELAYER · NÃO DA RAPID7

"The Weaponization of Cellular-Based IoT Technology" · Heiland & Bindner · Black Hat USA 2025 · whitepaper Rapid7, mar 2026
↗ https://www.rapid7.com/blog/post/tr-new-whitepaper-exploiting-cellular-based-iot-devices/

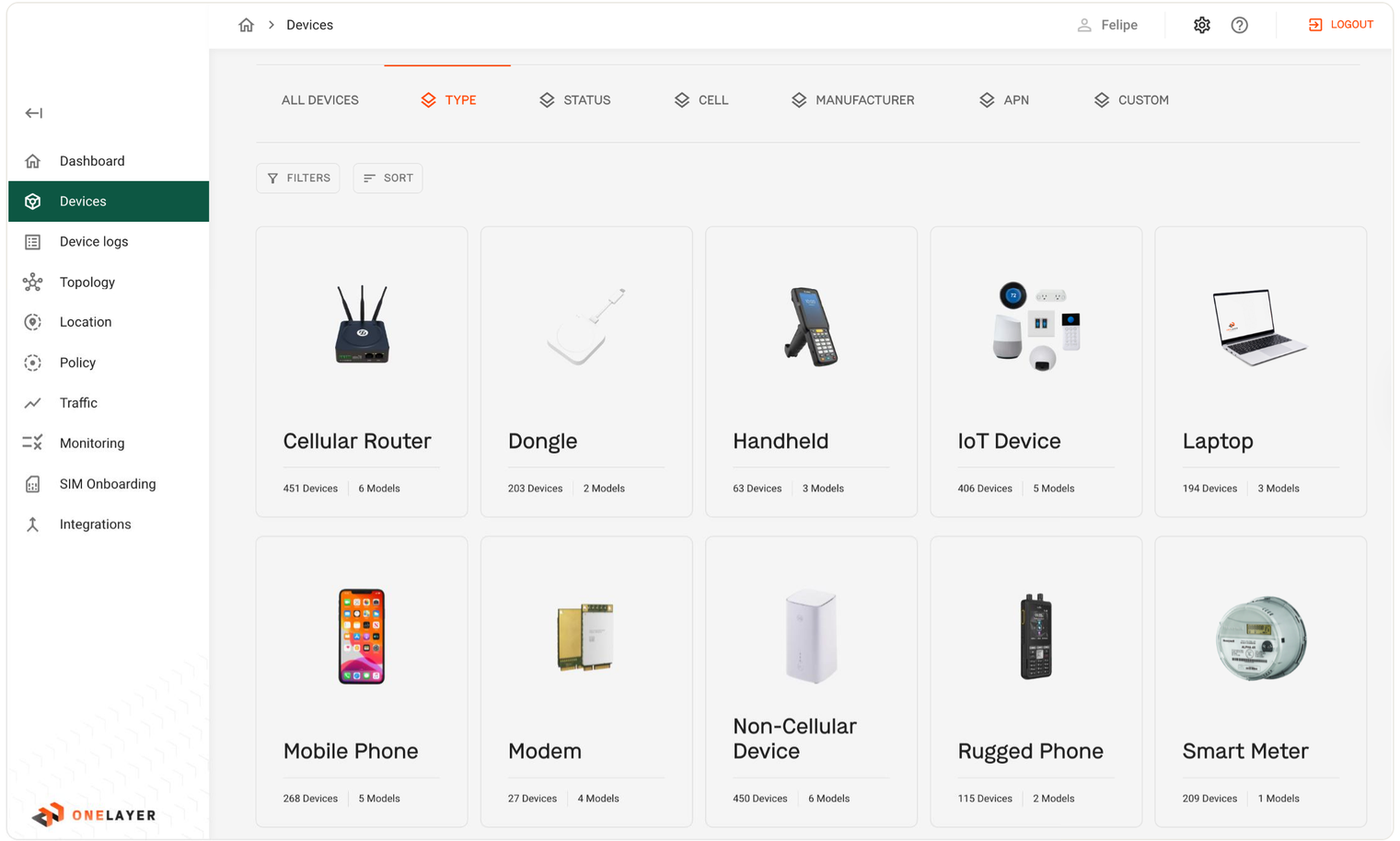
ATO 3 DE 3

Estender.
Não reconstruir.

A visibilidade que falta cabe no stack que o seu SOC já opera.

Com a OneLayer, cada attach vira um dossiê — nas duas redes.

ONELAYER



Um inventário só — rede privada e APN de operadora.

O QUE O SEU SOC GANHA

- ✓ eSIM e SIM física, LTE privado e APN Vivo · Claro · TIM — **numa tela só**
- ✓ Dispositivos atrás do roteador **identificados sem agente** — MED-0441, SUB-112 e a LAN inteira
- ✓ Cada alerta cai no seu SIEM **com dispositivo, site e SIM** — não em mais um console

IEC 62443-2-1 · NIST CSF · ID.AM · ISO 27001 · A.5.9 · LGPD / ANPD

SUB-112 segue aprovado e válido — falando com quem nunca falou.

cada pacote passou na regra do firewall — o que mudou foi o padrão, e padrão nenhuma regra vê

INCIDENTE REAL · INDÚSTRIA PESADA · JUN 2022

Predatory Sparrow faz siderúrgica derramar metal fundido — comandos válidos, padrão errado. Só o comportamento avisou.

↗ cyberlaw.ccdcoe.org/wiki/Predatory_Sparrow_operation_against_Iranian_steel_maker_(2022)

Mesmo volume, mesma regra — destinos que nunca fizeram sentido. É isso que a linha de base captura.

Um CPE aprovado e válido pode estar falando com quem nunca falou.

Traffic Logs

Last update: 0 minutes ago
03/19/2026 12:41:43 AM

REFRESH | EXPORT

Time: 1 | Rule: All | Source: All | Destination: All | Action: All

More than **10,000 results** matched your criteria

Date	Source	Source port	Destination	Destination port	Protocol	Rule name	Action	Bytes
03/19/2026 12:10:30 AM	Apple iPad Pro 11 (A2068) #dcc922eb (130.10.125.134)	443	EX50 Series #610a7274 (130.10.197.11)	683	TCP	-	None	128.71KB
03/19/2026 12:10:30 AM	Cala kIQ (SW100) #10373254 (130.10.74.67)	443	Apple iPad Pro 11 (A2068) #4c62e745 (130.10.122.185)	683	TCP	-	None	94.26KB
03/19/2026 12:10:30 AM	Apple iPhone 14 Pro (A28... #97b6adac (130.10.4.85)	443	Apple iPad Pro 11 (A2068) #4c62e745 (130.10.122.185)	683	TCP	-	None	87.54KB
03/19/2026 12:10:30 AM	Birdie Plus (SM-X608B) #54eed197 (130.10.206.237)	443	EX50 Series #21ddb7cd (130.10.190.52)	683	TCP	-	None	147.75KB
03/19/2026 12:10:30 AM	MTCM2 #2c20ab44 (130.10.155.111)	443	TC10AN3FUN8 (Gen10BL) #83a72036 (130.10.118.7)	683	TCP	-	None	284.28KB
03/19/2026 12:10:30 AM	SARA-R410M-52B #0b02e4dc (130.10.86.253)	443	SARA-R410M-52B #dbd1b464 (130.10.43.33)	683	TCP	-	None	215.49KB
03/19/2026 12:10:30 AM	MC2-21A12 #3a092161 (130.10.222.43)	53	192.168.20.54	443	ICMP	-	None	239.60KB
03/19/2026 12:10:30 AM	TC10AN3FUN8 (Gen10BL) #83a72036 (130.10.118.7)	443	SARA-R410M-52B #0b02e4dc (130.10.86.253)	683	TCP	-	None	155.47KB

Mesmo volume, mesma regra — destinos que nunca fizeram sentido.

O QUE NENHUMA REGRA VÊ

- ✓ O dispositivo **sempre falou** com o dispatch de frota — todos os dias, kilobytes
- ✓ **Esta semana** passou a falar com um CPE par na mesma APN, um servidor de TI no datacenter e um destino fora do padrão do grupo
- ✓ **Cada pacote passou na regra do firewall** — o que mudou foi o padrão, e padrão nenhuma regra vê

Incidente real · jun 2022 · comandos válidos, padrão errado — só o comportamento avisou

O alerta dispara. E aí tudo fica mais difícil.

Tráfego anômalo na faixa da subestação. O SOC segue o playbook, e o playbook quebra em cada etapa: nada olha leste-oeste, o inventário devolve um serial de SIM, um único botão derruba (contenção) o APN inteiro e **a trilha forense termina no firewall.** MED-0441 e SUB-112 seguem “saudáveis” nos painéis o tempo todo.

03:12 — alerta no SIEM: tráfego anômalo na faixa de IPs da subestação

1 DETECTAR	2 IDENTIFICAR	3 CONTER	4 INVESTIGAR
Um alerta no perímetro. Dentro da rede celular, o tráfego leste-oeste não cruza sensor nenhum.	O inventário responde: SIM 8955…0358. Qual dispositivo? Qual subestação? Silêncio.	Não há controle por dispositivo. O único botão derruba o APN inteiro — e o campo junto.	Sem histórico de pacotes, sem linha do tempo. A trilha forense termina no firewall.

O QUE A REDE VÊ	O PLAYBOOK DE RESPOSTA
detectar: sem sensores leste-oeste	
identificar: SIM 8955…0358 — qual dispositivo?	

> **Cada minuto dessa linha do tempo é permanência do atacante no grid.**

Cinco pontos cegos. Uma causa raiz.

01	**Inventário**	O painel lista chips, não dispositivos. Você não sabe o que está conectado.
02	**Segmentação**	A APN separa grupos de SIMs, não dispositivos. Dentro dela, tudo se alcança.
03	**SIM swap**	O chip válido em outro hardware herda toda a confiança — e nada alerta.
04	**Dispositivo atrás do CPE**	O roteador tem SIM; o que está atrás dele, não. O core nunca o vê.
05	**Anomalia comportamental**	Identidade válida, volume normal, destinos novos. Nenhuma regra vê padrão.

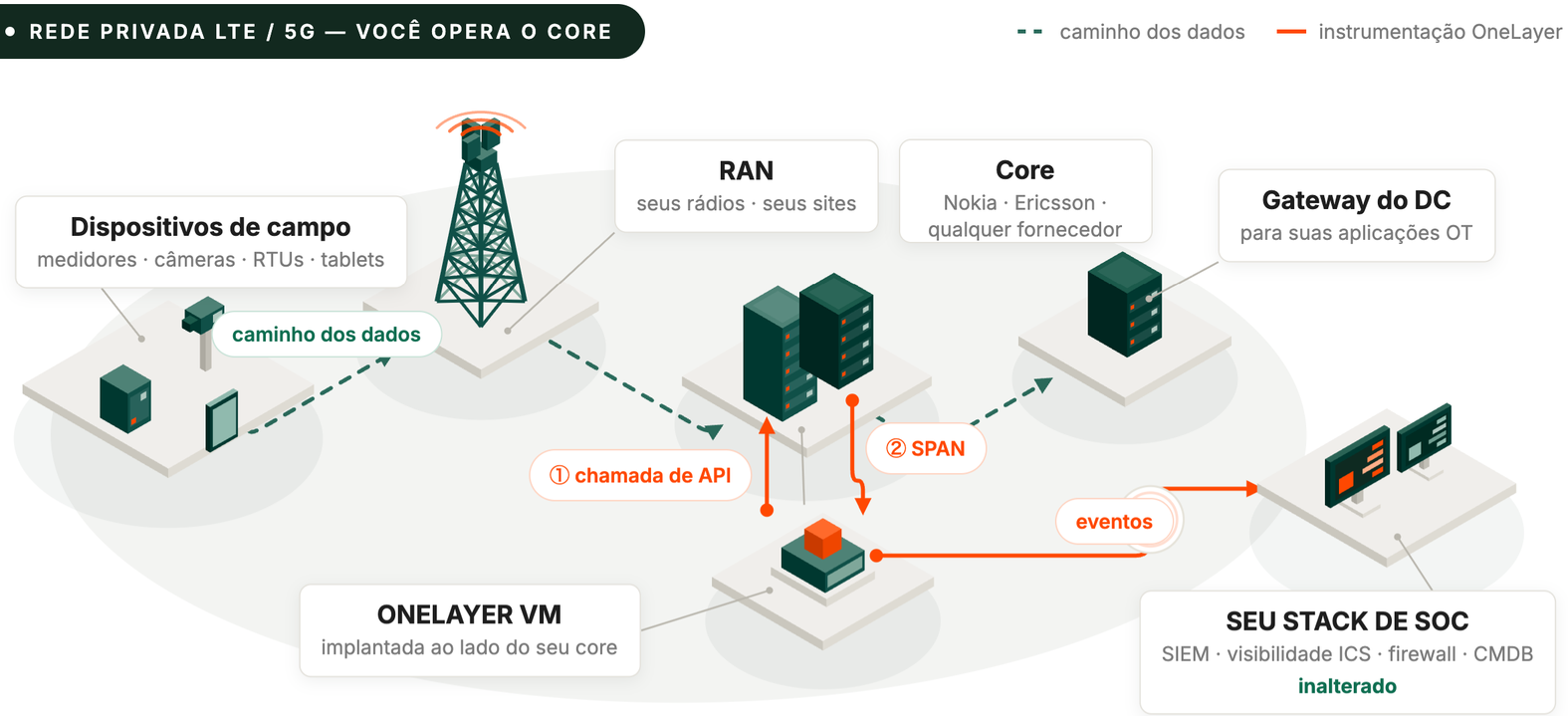
A rede vê o SIM — nunca o dispositivo.

Cinco problemas distintos, cinco incidentes documentados — e a mesma lacuna por baixo de todos: monitoramento de TI não é monitoramento de telecom, e nenhum dos dois é identidade de dispositivo.

Com a OneLayer na rede privada: o core monitorado, sem tocar em nada.

ONELAYER

• REDE PRIVADA LTE / 5G — VOCÊ OPERA O CORE



Seu core, monitorado de forma passiva — cada dispositivo identificado. Sem agentes, sem risco inline, qualquer fornecedor.

① chamada de API + ② espelhamento de porta — os pacotes ficam no site.

O QUE O SEU SOC GANHA

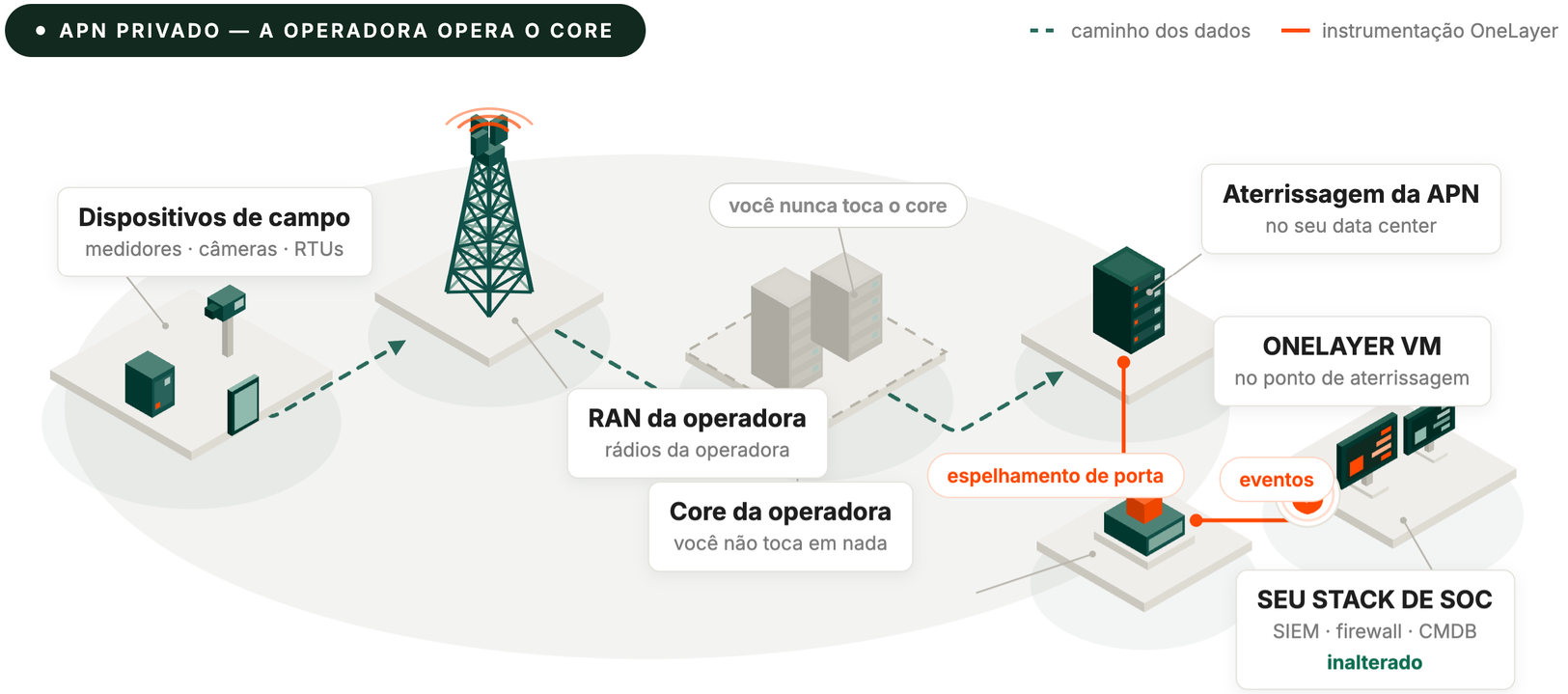
- ✓ VM ao lado do seu core — **Nokia, Ericsson, qualquer fornecedor**
- ✓ Detecção em sinalização e tráfego — **IMEI trocado, intrusos, anomalias**
- ✓ Enforcement por dispositivo — **quarentena sem derrubar o APN**

IEC 62443 · SR 6.2 | NIST CSF · DE.AE | ISO 27001 · A.8.16 | LGPD / ANPD

Com a OneLayer no APN privado: a mesma plataforma, sem tocar o core da operadora.

ONELAYER

• APN PRIVADO — A OPERADORA OPERA O CORE



Sem acesso ao core da operadora — as APIs dela, mais um SPAN onde o tráfego do seu APN aterrissa.

APIs da operadora + um SPAN onde o seu tráfego aterrissa.

O QUE O SEU SOC GANHA

- ✓ Um inventário para **toda operadora e todo APN**
- ✓ A fronteira respeitada — **você nunca toca o core da operadora**
- ✓ Resposta: **suspensão via API + bloqueio no seu firewall**

NIST CSF · ID.AM / PR.AA | IEC 62443-2-1 | LGPD / ANPD

ONELAYER

Com a OneLayer, o firewall vê dispositivos — não sub-redes.

O FIREWALL QUE VOCÊ JÁ OPERA
política sobre objetos vivos de dispositivo — não sobre IPs · modo simulação primeiro

ORIGEM	DESTINO	SERVIÇO	AÇÃO
`OneLayer.Religadores`	ADMS · centro de operação da distribuição	TCP/443 · TLS	✓PERMITIR
`OneLayer.Cameras`	VMS · head-end de vídeo	TCP/554 · RTSP	✓PERMITIR
`OneLayer.Cameras`	OneLayer.Religadores	qualquer	✕NEGAR
`OneLayer.Sensores`	OneLayer.*	qualquer	✕NEGAR

A composição de cada objeto fica viva — o firewall aplica no dispositivo, não em um IP.

Menor privilégio por dispositivo, na rede como ela é hoje.

O QUE O SEU SOC GANHA

- ✓ **Sem APNs novas, sem MOC, sem ativo parado** — a rede fica como foi desenhada
- ✓ **Modo simulação primeiro** — veja o que seria bloqueado antes de qualquer bloqueio
- ✓ Os grupos se atualizam sozinhos quando dispositivos entram ou saem — **a regra nunca envelhece**

IEC 62443 · zonas & conduítes | NIST CSF · PR.IR | ISO 27001 · A.8.22 | LGPD / ANPD

Com a OneLayer, o SIM fica casado com o hardware.

ONELAYER

Date	Event ID	Rule Name	Event details	Action
03/18/2026 12:31:01 PM	Alert774	**SIM swap**	MTCM2 IMEI (352204110054513) → EX50 Series IMEI (353529102666861)	DETAILS
03/16/2026 12:31:01 PM	Alert856	**SIM swap**	EX50 Series IMEI (353529102666726) → EX50 Series IMEI (353529102666670)	DETAILS
03/15/2026 12:31:01 PM	Alert214	**SIM swap**	Apollo IMEI (350027073441099) → Sierra Wireless E... IMEI (353533100441241)	DETAILS
03/14/2026 12:31:01 PM	Alert109	**SIM swap**	MTCM2 IMEI (352204110080323) → EX50 Series IMEI (353529102666604)	DETAILS

Um comprometimento silencioso vira um alerta imediato e atribuível.

O QUE O SEU SOC GANHA

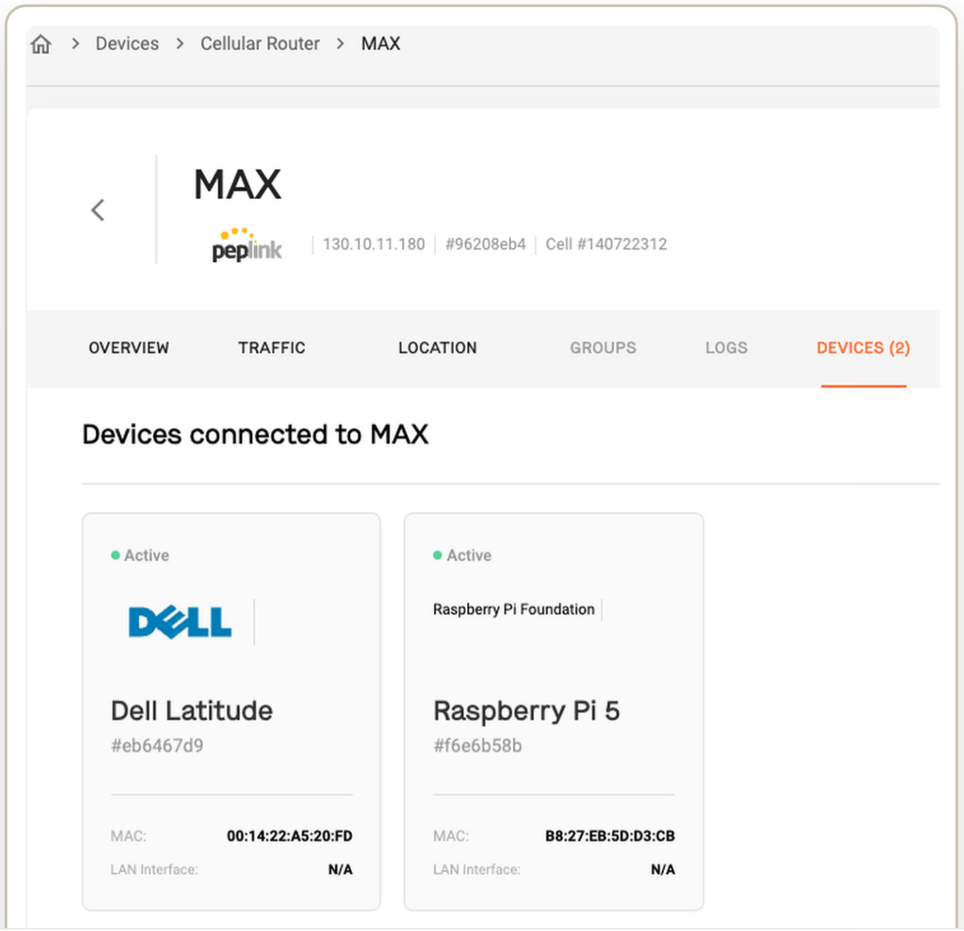
- ✓ **Vínculo IMSI ⇄ IMEI verificado continuamente** — a troca aparece em segundos
- ✓ O alerta chega com **contexto de dispositivo anexado** — origem, destino, site
- ✓ A resposta pode ser automatizada — **suspensão do SIM, bloqueio no firewall, alerta no SIEM** — ou mantida só em alerta

NIST CSF · PR.AA | IEC 62443 · SR 1.2 / 1.5 | ISO 27001 · A.5.16 | LGPD / ANPD

03

Com a OneLayer, o que está atrás do roteador tem nome, MAC e identidade.

ONELAYER



A metade invisível do parque celular vira inventário.

O QUE O SEU SOC GANHA

- ✓ **Rogue devices sinalizados no momento em que aparecem** — hardware não autorizado com identidade emprestada não passa despercebido
- ✓ Cada dispositivo novo atrás de um CPE **gera alerta na hora** — não numa auditoria depois
- ✓ As fronteiras do Purdue voltam a ser aplicáveis: **o dispositivo, não só o roteador, tem identidade**

IEC 62443 · SR 1.x | NIST CSF · ID.AM / DE.CM | ISO 27001 · A.8.16 | LGPD / ANPD

Conectar não é autorizar. O onboarding passa a provar isso.

ONELAYER

FROTAS COM PERFIL CONHECIDO NA APN

Medidores AMI
1.204 dispositivos · perfil estável

Câmeras e CPEs OT
386 dispositivos · perfil estável

OneLayer · NAC para celular privado
fingerprint de dispositivo + modelo de comportamento, sem agente

decisão na entrada

Dispositivo verificado
IMEI casa com o fabricante homologado e com a ordem de serviço; o padrão de tráfego bate com o do grupo de pares.

→ APN de produção · segmentado

«Eu sou um CPE OT»
IMEI declarado aceito pela rede — mas o fingerprint e o padrão de tráfego não conferem com nenhum CPE OT do parque.

→ APN de staging · retido e sinalizado

O FLUXO DE APROVISIONAMENTO

HOJE

~30 minutos por chip — chamado, digitação manual no core, ferramenta de IP separada, atualização manual do CMDB. **Quatro sistemas, uma pessoa, toda vez.**

COM A ONELAYER + CMDB

Chamado → ativação → CMDB, **um fluxo só.** Minutos, auditável, e cada dispositivo validado na entrada.

NIST SP 800-207 · Zero Trust

IEC 62443 · SR 1.1

ISO 27001 · A.5.15

A rede vê o chip. A OneLayer vê o dispositivo.

A PERGUNTA	HOJE	COM A ONELAYER
O que está conectado agora? ATO 1	status, IP e consumo — sem dispositivo, sem localidade	✓ **dossiê vivo por dispositivo** — as duas redes numa tela
O que vive atrás do roteador? ATO 2	um attach saudável — a LAN é invisível	✓ **dois saltos adentro** — a LAN inteira no mapa
Este chip está no hardware certo? ATO 2	ninguém pergunta — autenticou, entrou	✓ **vínculo IMSI ⇆ IMEI** — a troca vira alerta na hora
Quem pode falar com o quê? ATO 3	a sub-rede permite; o gateway não pergunta	✓ **menor privilégio por dispositivo** — leste–oeste negado por padrão
Ele age como um medidor? ATO 3	sem linha de base — regra aprovada, tráfego passa	✓ **pontuado contra os pares** — desvio antes do dano

Cinco perguntas, uma causa raiz: identidade e política paravam no chip. A OneLayer as leva até o dispositivo.

COMPLIANCE · VISÃO CONSOLIDADA

Cada controle mapeia para os frameworks aos quais você responde.

CONTROLE ONELAYER	IEC 62443	NIST CSF 2.0	ISO/IEC 27001	LGPD / ANPD
Visibilidade de inventário Ato 1 · ID.AM · A.5.9	✓	✓	✓	✓
Descoberta atrás do roteador Ato 2 · ID.AM · A.8.8	✓	✓	✓	—
Vínculo chip ⇆ hardware Ato 2 · PR.AA · A.5.16	✓	✓	✓	✓
Segmentação por dispositivo Ato 3 · PR.IR · A.8.22	✓	✓	✓	✓
Anomalia comportamental Ato 3 · DE.AE / DE.CM · A.8.16	✓	✓	✓	✓

Cada detecção sai com **evidência exportável** (SIEM · relatório). **ANATEL** (homologação — Atos 77/2021 · 2.436/2023) e **INMETRO** (Portaria 155/2022) incidem sobre o equipamento, não sobre a rede — contexto regulatório, não requisito direto.

ONELAYER

O FINAL DA HISTÓRIA

MED-0441 e SUB-112 estão seguros.
E o resto das suas duas redes?

Felipe Mahatma · Engenheiro de Pré-vendas
felipe.mahatma@onelayer.com · onelayer.com

Discovery de 30 dias — tipicamente revela 30–40% mais dispositivos do que o inventário mostra.