

Building the Cloud-Native Trust Stack

Lessons from a Real-World POS and MPoC Deployment

Gertec | FUTUREX

Bruno Simões

Head of Payment and Retail Products

Gertec



Adam Cason

VP, Global and Strategic Alliances

Futurex



About

Gertec

More than 36 years working throughout Brazil and expanding to Latin America

+ 10 million products sold and relationships with the main financial institutions

Integrated and customized solutions (POS Vendor + Platforms + Tap on phone solution)

International innovation and supply chain. largest local R&D team on the market

Recognized implementation of PCI PIN, PTS POI, DSS, SLC, SSS and MPOC requirements

PCI PO since 2015 and Regional Engagement Board Brazil Member since 2018



"Gertec is deeply committed and engaged with its security mission, having been involved with PCI, EMVCo, and Brands programs for over 15 years."

- Founder & CEO Jorge Ribeiro

20 YEARS OF SECURING PAYMENT DATA

About

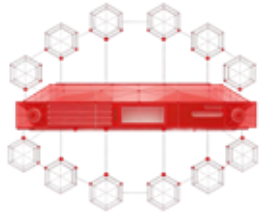
FUTUREX

45+ years

Enterprise-class data security technology

FUTUREX

- Enterprise cryptography and key management
- HSMs, PKI, signing, and tokenization
- Remote key injection for distributed POS and MPoC environments
- Cloud, on-premises, and hybrid cryptographic infrastructure
- Member of the PCI SSC 2025–2027 Board of Advisors



20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Introduction

Where Does Trust Live When the Perimeter Disappears?



The Evolution of the Physical Perimeter

Methods of accepting payments are growing, and consumers expect choice

Consequences

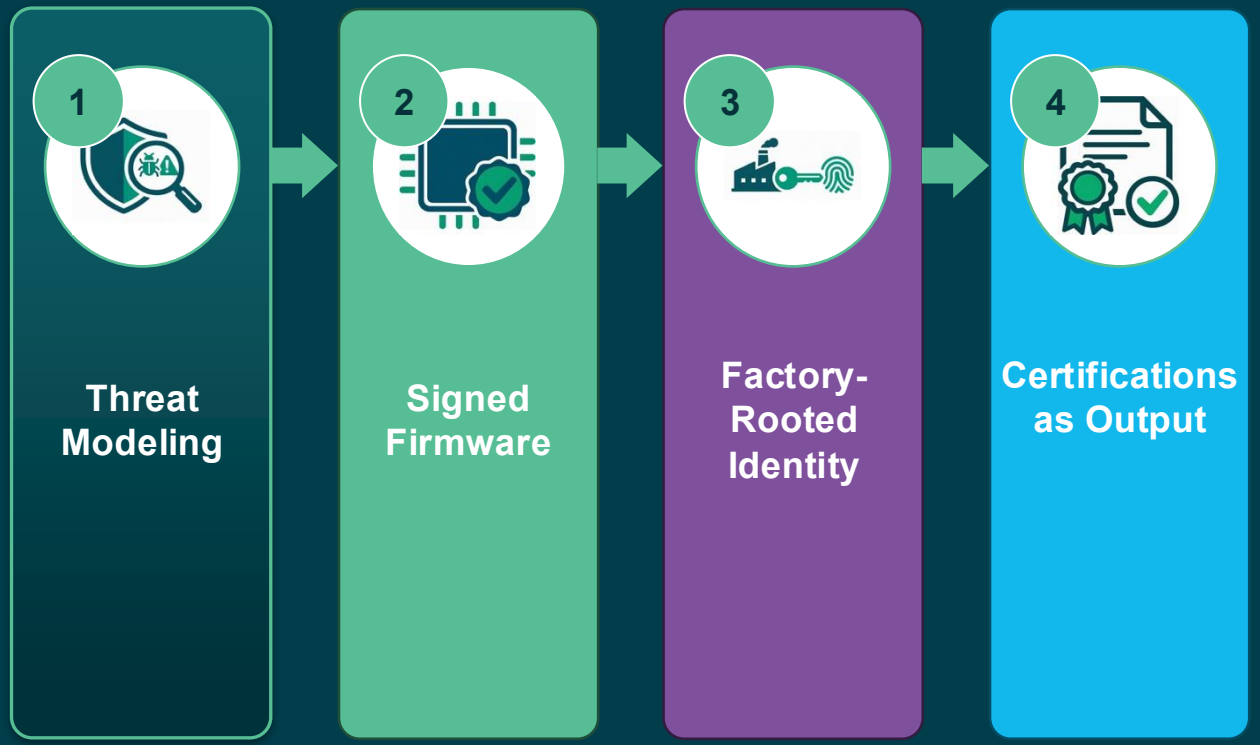
- Each type expands the attack surface
- Hardware is no longer the only trust signal
- Trust must be established, maintained, and revoked dynamically



Foundational Security

PCI standards shape engineering requirements from the start

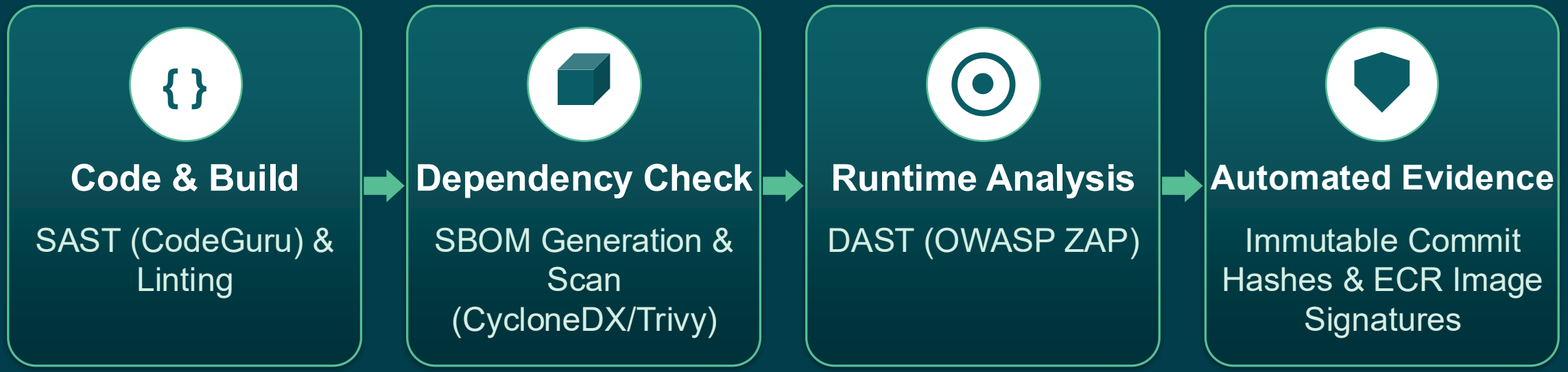
1. Threat modeling before implementation
2. Signed firmware and controlled releases
3. Factory-rooted identity and HSM-protected signing keys
4. Evidence generated continuously, not assembled later



20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Foundational Security Real-World Example:

Shifting from periodic audits to continuous, observable pipeline evidence



Audit-ready evidence as an operational output: evidence generated automatically by the CI/CD pipeline, not reconstructed manually for assessors.

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

The Four Forces in Tension

1. Security
2. Scale
3. Compliance
4. Merchant Experience

A robust MPoC architecture must satisfy all four forces without sacrificing merchant operations

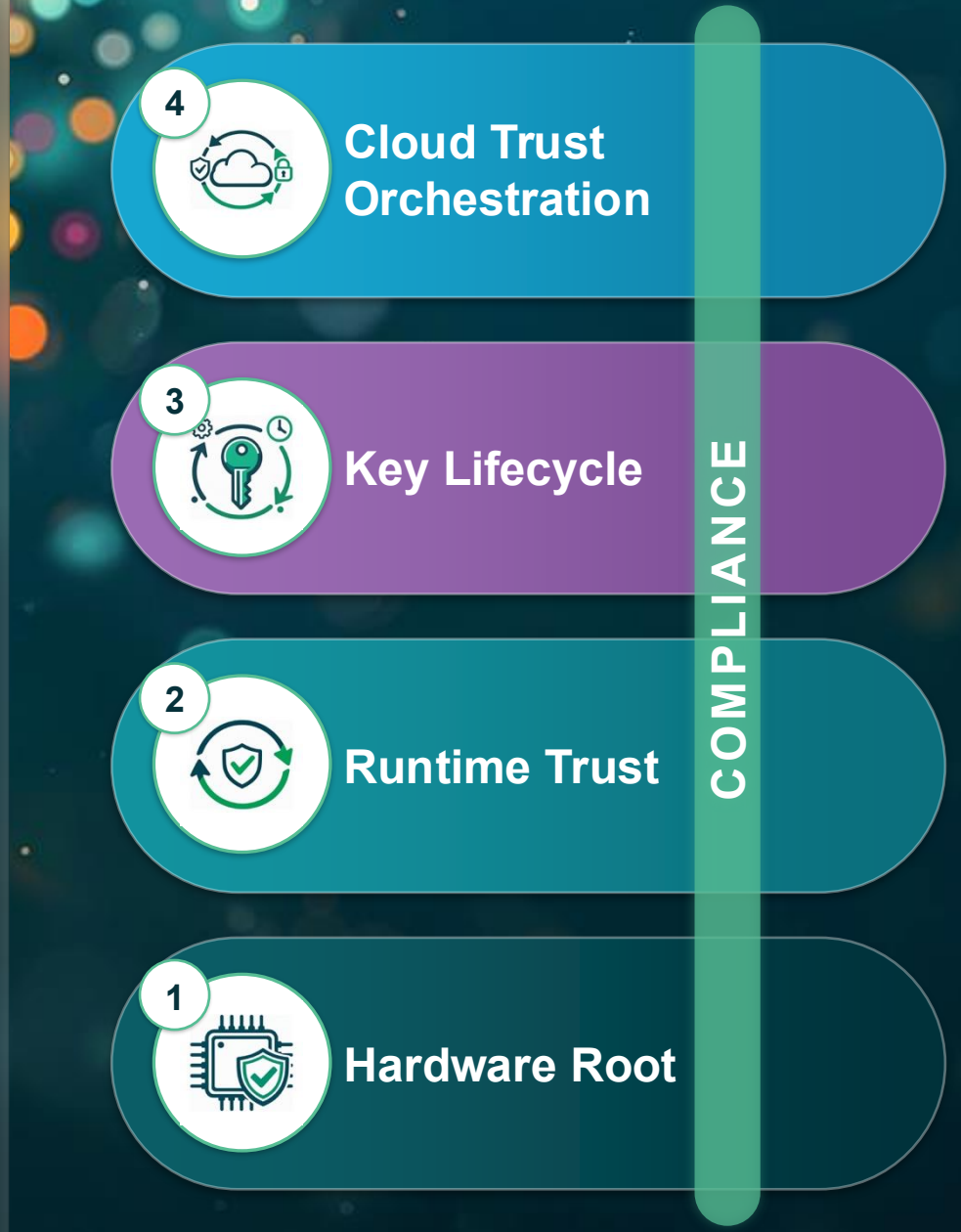


The Trust Stack

Four horizontal tiers:

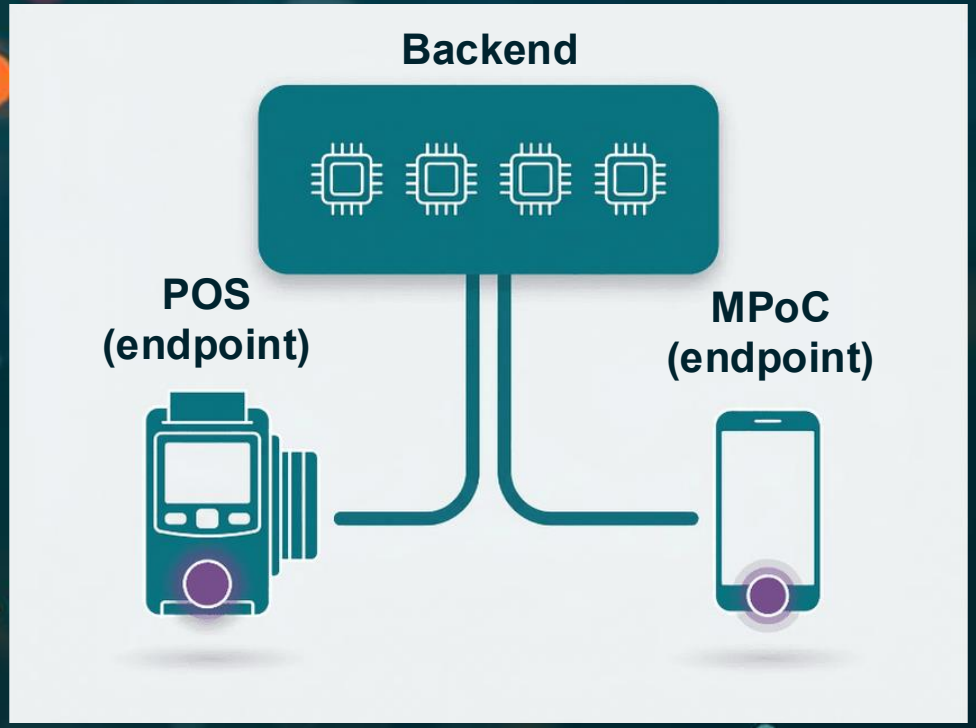
1. Device and Platform Roots of Trust
2. Runtime Trust
3. Key Lifecycle
4. Cloud Trust Orchestration

Compliance as observable evidence



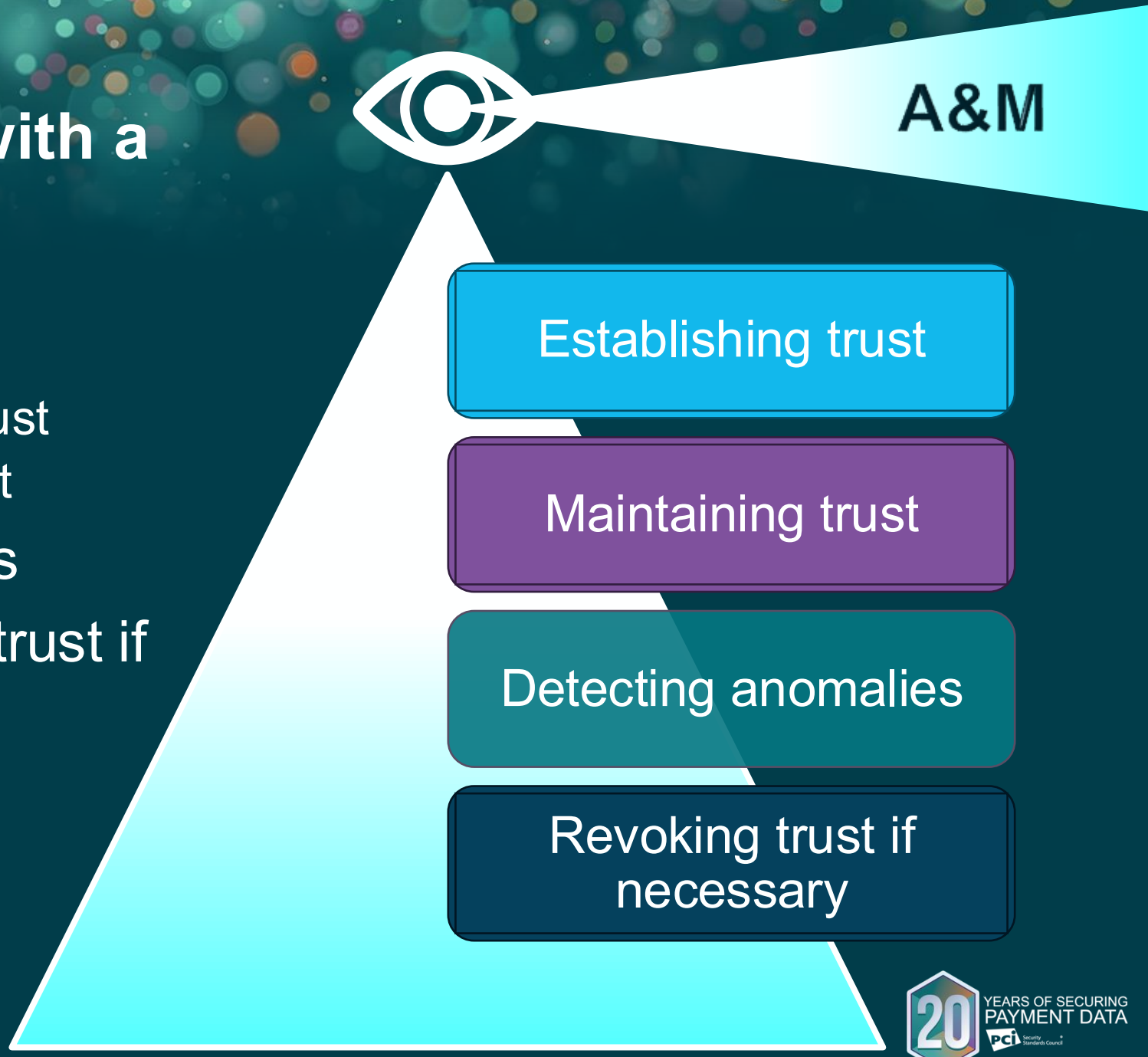
Pillar I – One Backend, Two Worlds

- Cloud-first architecture
- Retail reality is hybrid across both MPoC devices and countertop Point of Sale
- Same backend, different endpoints
- Unifies compliance evidence into one schema
- Reduced security silos



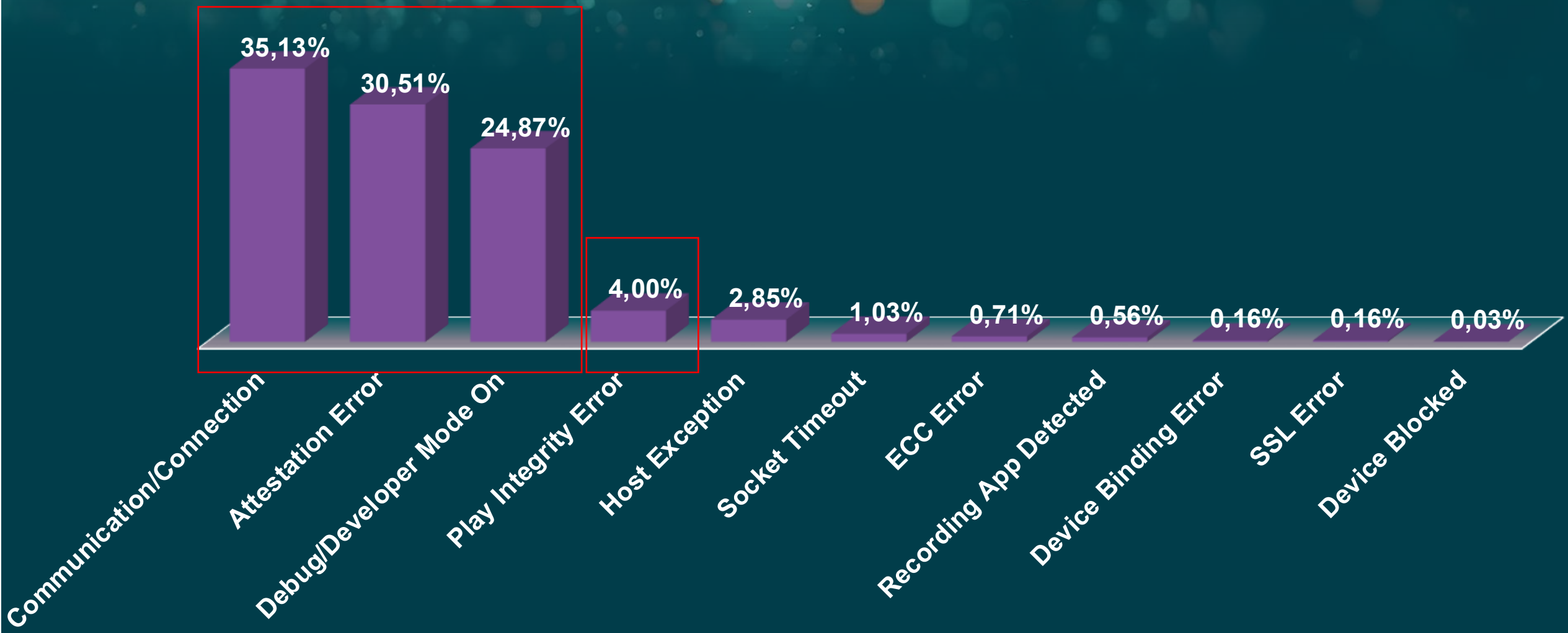
Pillar II – A Verdict with a Lifetime

- Runtime Trust – A&M
  - Attestation establishes trust
  - Monitoring maintains trust
- SDK detecting anomalies
- Cloud backend revokes trust if necessary



20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

Gertec's Attestation & Monitoring: Real-World Data



20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Graduated response reduces false declines while blocking real threats

90.5% of A&M incidents fall into three categories — and each one demands a different enforcement action.

Communication / Connection

35.13%

Isolate the session → fall back to a safe, limited mode → deny key release if unresolved.

Attestation Error

30.51%

Immediately revoke session keys → require full re-attestation before resuming.

Debug / Developer Mode

24.87%

Block sensitive operations → flag the device for remediation → no key material released.

Graduated response — proportional, not binary:

Step-up (low friction) › **Throttle** (limit) › **Revoke** (block)

Market reality: actual fraud is only ~7% of the total cost of fraud — false declines cost more. *(JP Morgan Payments)*

Source: Gertec Attestation & Monitoring field telemetry. False-decline economics: JP Morgan Payments (Data Intelligence).

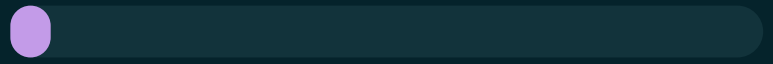
20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

Platform attestation alone covers only 4% of real threats — defense in depth is non-negotiable

Google Play Integrity errors are just 4.00% of Gertec's blocked incidents. Platform signals alone leave ~96% of operational risk unaddressed.

4%

of blocked incidents caught by platform signals alone (Play Integrity / App Attest)



96% of operational risk needs more than the platform.

1

Platform — Play Integrity / App Attest

Catches device tampering. Only ~4% of real-world blocks; has known blind spots.

2

App & SDK — in-SDK engine + Keystore

Catches debug mode, hooking, emulation, and recording apps. Handles 25%+ of incidents with app-specific context.

3

Backend verdict — server-side decision

Aggregates every signal, decides, and authorizes the HSM to release or revoke keys. Never trusts the device side alone.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Every blocked event becomes immutable, real-time audit evidence

PCI DSS 4.0.1 expects security controls to stay effective continuously, not just at an annual assessment.

Cloud-native model

Continuous automated validation

Evidence generated in real time

Automated alerting + immutable metadata

Immutable audit record

```
event        Attestation Error
timestamp    2026-09-17T11:14:03Z
device_id    3f9a…c71  (hashed)
verdict      server-side
enforcement  keys revoked → re-attest
key_lineage  traceable
integrity    SHA-256 sealed
```

QSAs can trace the key lineage and the exact enforcement action taken — at any time.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

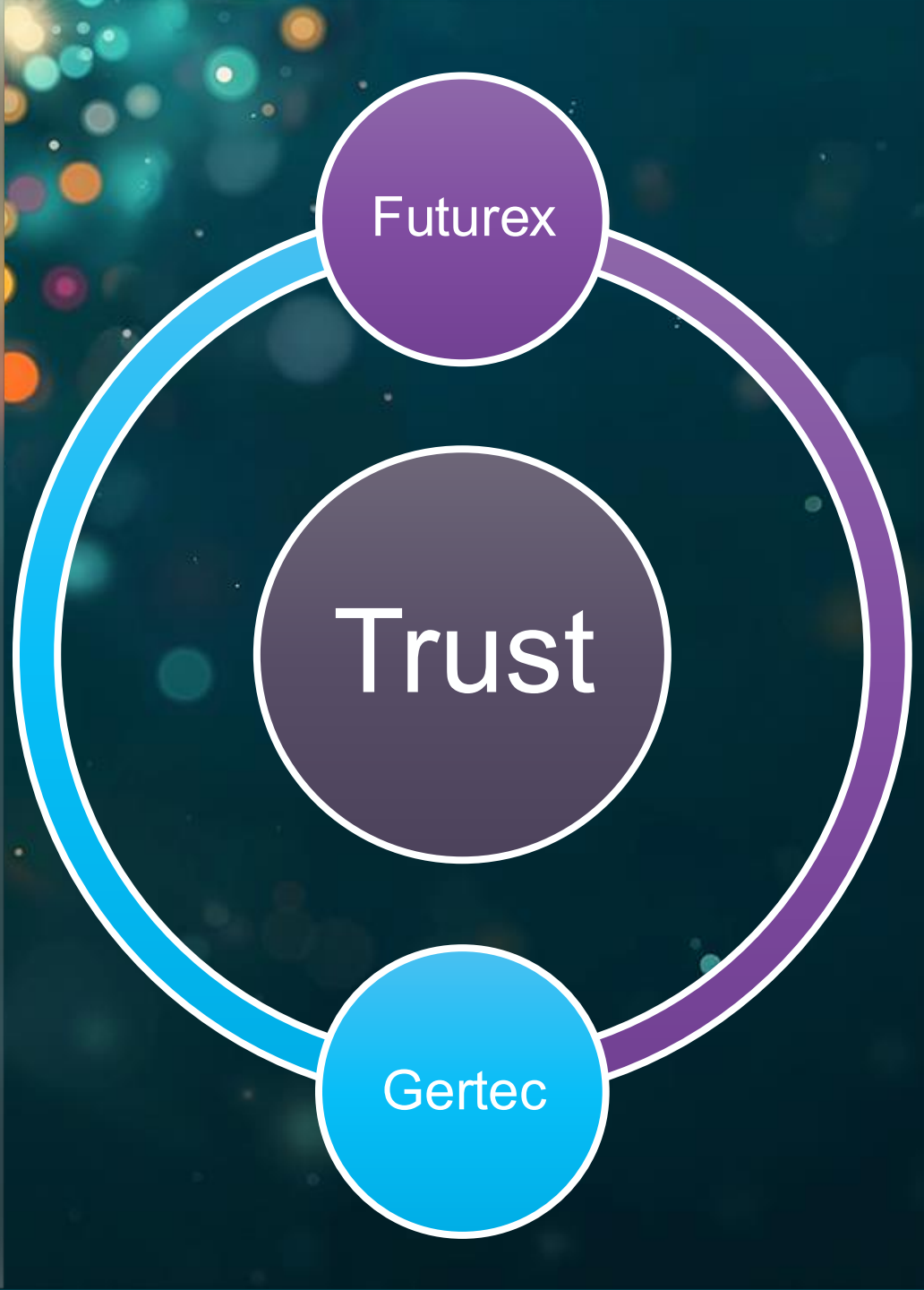
The Division of Trust

Gertec

- Endpoint
- Application
- Runtime signals
- Merchant experience

Futurex

- HSM-backed cryptographic root
- Initial trust + firmware signing
- Device attestation
- Remote key injection (RKI) for eligible POS devices



Pillar III - Remote Key Injection

Cryptographic boundary

Request → Generate → Protect → Sign → Distribute → Verify → Install



Cloud Orchestrator



Validated HSM



Signing Service



Distribution Channel (MDM)



Endpoint

Key payloads

Wrapped transport

Attestation-gated install

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Pillar IV - Eliminating the Key Injection Bottleneck

Replacing physical logistics with secure cloud services

Legacy Key Management

- Dedicated secure facilities and local loading equipment
- Physical connection of devices to injection systems
- Dual-control operating procedures
- Geographic and throughput constraints
- Additional shipping, scheduling, and staffing dependencies

Cloud HSM + RKI

- **Root of Trust:** Key lifecycle inside PCI approved HSMs, deployed as a service
- **Remote Injection:** Delivered via mutually authenticated, encrypted channels
- **Bound to Device:** Keys remain protected during remote transport
- **Lifecycle:** Policy-driven rotation and automated destruction

Recommendation: Let device makers own the endpoint; let approved crypto providers own the key foundation.

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

Last Considerations and Closing

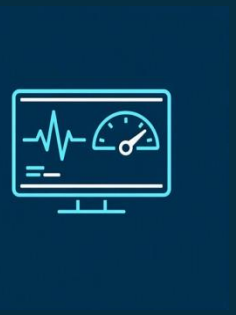
Building the Cloud-Native Trust Stack



What Did We Learn in the Field?



Explicit trust boundaries



Well-defined telemetry



Observable evidence and controls

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Thank You

Questions? Feel free to reach out:

Bruno Simões | bruno.simoes@gertec.com.br

Adam Cason | acason@futurex.com

Gertec

FUTUREX

20 YEARS OF SECURING PAYMENT DATA