ZERO TRUST ARCHITECTURE FOR PAYMENT PLATFORMS

Pillar	Cost	Effort	Payoff
1. Identity	$80k	6 weeks	Blocks 80% of breaches
4. Encryption	$100k	8 weeks	SOC2 compliant
2. Device	$150k	10 weeks	Insider threat detection
6. Visibility	$100k	8 weeks	Real-time fraud alerts
3. Network	$150k	12 weeks	Complete isolation
Total	$580k	12 weeks	Breach-resistant

THE PROBLEM

Legacy security = "Trust inside firewall."

Payment platforms need = 24/7 trust verification.

THE 8-PILLAR FRAMEWORK (Adapted for Fintech)

Pillar 1: Identity

MFA + SSO for all users

- Eliminates credential reuse
- Stops phishing attacks
- Forces human verification on every login

Pillar 2: Device

EDR + MDM for employee/contractor devices

- Prevents compromised devices from accessing APIs
- Detects insider threats early
- Blocks stolen credentials at source

Pillar 3: Network

Microsegmentation (payment service isolated from admin)

- Payment system can't communicate with finance system
- Lateral movement blocked
- Each service is its own "fortress"

Pillar 4: Encryption

mTLS for inter-service communication

- Machine-to-machine authentication
- Data encrypted at rest + in transit
- No plaintext API keys

Pillar 5: Access Control

Attribute-based access control (ABAC)

- Payment amount limits who can process it
- Time-based rules (no 3am transactions for humans)

- IP-based geofencing (Pakistan only, not random cloud)

Pillar 6: Visibility

SIEM + behavioral analytics for fraud detection

- Every transaction logged
- Anomalies flagged instantly
- Full audit trail for compliance

Pillar 7: Automation

Auto-response to suspicious transactions

- Automatic block, then review
- No manual review delays
- Fraud response in seconds, not hours

Pillar 8: Compliance

Continuous compliance monitoring (PCI + SOC 2)

- Real-time compliance reporting
- No month-end scramble
- Auditor-ready logs always

FINTECH PRIORITY ORDER

Implement in this sequence (not all at once):

1. Identity (CRITICAL)
- Credential compromise = payment fraud
- Start Week 1

2. Encryption (CRITICAL)
- Data in transit = SOC 2 requirement
- Start Week 2-3

3. Device (HIGH)
- Compromised device = API key theft
- Start Week 4

4. Network (HIGH)
- Lateral movement = access to payment ledger
- Start Week 6

TYPICAL 6-MONTH BUDGET: $500k-$1M

Pillar

Cost

Effort

Payoff

1. Identity

$80k

6 weeks

Blocks 80% of breaches

4. Encryption

$100k

8 weeks

SOC2 compliant

2. Device

$150k

10 weeks

Insider threat detection

6. Visibility

$100k

8 weeks

Real-time fraud alerts

3. Network

$150k

12 weeks

Complete isolation

Total

$580k

12 weeks

Breach-resistant

MINIMUM VIABLE ZERO TRUST (3 MONTHS, $200k)

If budget is tight, start with these:

- ■ Identity (MFA + SSO)
- ■ Encryption (TLS + mTLS)
- ■ Visibility (Basic SIEM)

This gives you:

- SOC 2 compliance foundation
- 60% breach prevention
- Real-time logging for auditors

Then add Pillars 2, 3, 5-8 in next phase.

NEXT STEPS

1. Audit your current state → Use Zero Trust Assessment
2. Pick your timeline → 3 months or 6 months?
3. Identify budget → $200k minimum or $500k+?
4. Assign implementation owner → CTO? Head of Infra?
5. Engage auditor early → Confirm timeline alignment

WANT STRATEGIC GUIDANCE?

Fractional CISO Service: $3,000-$5,000/month

- Monthly strategy sessions
- Zero Trust roadmap alignment
- Vendor selection + negotiation
- Executive reporting

[Get Fractional CISO →](https://securehops-website-amber.vercel.app/contact)

Securehops | Zero Trust + Fractional CISO Services for Fintech

Helping payment platforms build breach-resistant infrastructure