AUTOMATED TELLER MACHINE (ATM) SECURITY · AI-LED M/XDR

From Blind Spots to Board Reports:

Governing ATM Exposure at Scale

How Banyax turns fragmented Automated Teller Machine (ATM) monitoring into a boardroom-ready cyber exposure governance program with measurable Key Risk Indicator (KRI) reduction, regulatory compliance, and structural client retention.

INDUSTRY Financial Services / Banking & Fintech

01 · WHAT CLIENTS ACHIEVE

Four measurable outcomes that define the value of the engagement before the client even reviews the technical architecture.

Detection Speed	False Positives	ATM Coverage	Regulatory
Minutes	**–60–80%**	**100%**	**Auto**
vs. hours with siloed tools	*via ticketing + identity correlation*	*of the network, 24×7×365*	*Comisión Nacional Bancaria y de Valores (CNBV)-ready evidence, no manual effort*

Before Banyax, the average Mexican bank with a distributed ATM network operated with three disconnected monitoring silos: physical alarms, transaction logs, and maintenance access records. No correlation. No baseline. No board-level reporting.

After Banyax, those three silos collapse into a single exposure governance program with KRI trending available to the CISO quarterly and forensic evidence auto-generated for CNBV. The bank doesn't just detect faster. It governs.

02 · THE PROBLEM NO ONE WAS SOLVING

Three silos, zero correlation

Physical alarms, transaction logs, and maintenance access records live in separate systems. No one correlates them. Events that would be obvious across all three stay invisible inside each.

The insider threat gap

Internal technicians and contractors with authorized access are the highest-risk vector. Static rule systems cannot distinguish a legitimate service visit from a coordinated fraud attempt.

No evidence for regulators

When an incident occurs, banks lack consolidated forensic evidence for CNBV investigations or internal audits, creating regulatory exposure on top of the operational one.

03 · EIGHT CORRELATED CAPABILITIES — ONE GOVERNANCE PROGRAM

Banyax instruments each Automated Teller Machine (ATM) with Lookwise (or equivalent agent), ingests telemetry into the Security Operations Center (SOC) Security Information and Event Management (SIEM) platform — Exabeam or Securonix — and runs eight correlated detection use cases through Banyax Quest, our proprietary platform. AI-led processing handles the volume; human analysts validate every high-priority escalation.

01 Behavioral baseline per ATM & technician

User and Entity Behavior Analytics (UEBA) learns the normal pattern of each machine and each technician — hour, duration, command sequence, endpoint. Deviations trigger anomaly scoring, not static rules.

02 Identity & HR correlation

Every physical event is cross-referenced against HR and ticketing systems: is the technician active, on shift, with a valid work order? Closes the credential vector that never gets deactivated.

03 Geo-velocity & route validation

Detects physically impossible openings between two ATMs and routes that don't match field service planning — catching coordinated fraud attempts before they execute.

05 Firmware integrity & anti-skimming

Hash monitoring on the card reader, dispenser, and Encrypting PIN Pad (EPP). Any unauthorized software modification triggers an alert within minutes — before the device is compromised at the customer level.

07 Sensor & camera manipulation detection

Disconnected sensors, offline cameras, silenced alarms from the console: classic pre-fraud manipulation patterns. Banyax correlates them as a chain, not isolated noise.

08 Out-of-hours with calendar context

Dynamic rules for holidays, long weekends, and payroll dates. High-risk window + event + no assigned ticket — automatic escalation to physical response.

09 Awareness training for field staff (M/AT)

KnowBe4 modules built specifically for ATM technicians: targeted phishing, coercion protocols, duress keywords. Closes the human loop that no SIEM resolves.

10 Compliance & CNBV reporting

Automatic generation of forensic evidence with log integrity (hash) — ready for regulatory reporting and internal audit the moment an incident closes.

04 · HOW THE SERVICE OPERATES

1	2	3	4	5
CAPTURE	**INGEST**	**CORRELATE**	**SOC 24/7**	**RESPOND**
Lookwise agent on each ATM	SIEM Exabeam / Securonix	UEBA + HR + ticketing + calendar	Triage, validation, escalation	Client + CNBV evidence package

05 · WHY BANYAX — THE STRUCTURAL MOAT

- **Behavioral baseline moat.**
  The value is not the tool — it's months of accumulated normal behavior per ATM and per technician. A competitor entering today would need 60–90 days to detect what Banyax detects from week one.
- **Mexican SOC, banking context.**
  Analysts with direct experience in local financial fraud, CNBV regulatory context, and 24/7 operation in Spanish. Response times in minutes, not hours.
- **Integrated stack, not another SIEM.**
  Exabeam/Securonix (UEBA) + Cyberint (LATAM ATM threat intel) + KnowBe4 (field staff) + AI-led detection through Banyax Quest. One console, one SLA, one team.
- **Managed service, not a product.**
  The client buys outcomes — qualified alerts, contained incidents, regulatory reports under contractual SLA. No licenses for their team to operate.

06 · IDEAL CLIENT PROFILE

Banks, SOFIPOs, fintechs, and independent ATM operators with a network of 200+ ATMs in Mexico. Particularly relevant for institutions that have already faced jackpotting incidents, internal technician fraud, or are under regulatory pressure to strengthen their operational security program.

07 · NEXT STEP & CONTACT

45-Minute ATM Security Assessment

A live simulation of three real attack scenarios against your current ATM stack — no commitment required. We map your exposure gaps and show you exactly what Banyax would detect that your current tools miss.

Learn more about Banyax M/XDR: banyax.com

Want to learn more?

If this document was forwarded to you and you'd like to explore how Banyax can help your organization reduce ATM cyber exposure — reach out directly.

Email: comercial@banyax.com

Website: banyax.com