APOLLO Data Auditor

WHITE PAPER · PROTECTION RISK

Would Your Data Survive an Attack?

Why Monitoring Is Not Protection — And What a Posture Audit Reveals Before the Breach

Protection Risk Module — April 2026

EXECUTIVE SUMMARY

93% of ransomware attacks now target backup repositories before encrypting production data. If your backups are not immutable, you lose both.

Most SMBs invest in reactive tools — antivirus, EDR, firewalls. These tools answer one question: "Is an attack happening right now?" But they do not answer the question that determines whether your business survives: "If an attack hits tomorrow, are your data actually protected?"

This paper examines why reactive monitoring leaves critical gaps in data protection, what a proactive posture audit reveals that monitoring cannot, and why the difference between the two is the difference between recovery and bankruptcy.

1. THE PROTECTION YOU THINK YOU HAVE

A mid-size French company had an EDR deployed, a firewall in place, and a backup solution running nightly. When ransomware hit, the backup was encrypted along with production — the attacker had accessed the backup repository first. The company had no immutable or air-gapped copies. Recovery cost: over €2 million. Time to resume operations: four months.

This is not an edge case. It is the new normal.

According to Veeam, 93–96% of ransomware attacks specifically target backup repositories before touching production systems. The attackers know: destroy the backup, and the victim has no choice but to pay or rebuild from scratch.

The Sophos State of Ransomware 2025 report confirms that recovery via backup is at its lowest point in six years. 54% of organizations attempt recovery through backups, while 49% pay the ransom — at an average payment of $1 million. The average total cost of recovery: $2.57 million. Average time to resume operations: over 130 days.

And yet, most organizations assume their backup strategy is sound because backups run without errors. They have never tested whether those backups would survive a targeted attack. They have never verified immutability. They have never measured their actual Recovery Point Objective against the one declared in their disaster recovery plan.

Backup is only one of six blind spots. Credentials, dormant accounts, encryption gaps, obsolete data, and untested breach response plans are the others. Section 3 examines each one.

But first, a number that frames the stakes: **one in five SMBs that suffer a major cyberattack file for bankruptcy** (Mastercard 2025). Two-thirds of French SMBs experienced a cyberattack in 2025 (Orange Cyberdefense). The question is not whether your tools detect threats. The question is: **would your data survive one?**

APOLLO IN ACTION — THREE REAL CASES SCORED

Each case below shows a different dimension of protection failure — backup, encryption, access control. In each case, the problem was visible in the data before the incident. Below is what APOLLO™ Data Auditor would have surfaced.

Case 1 — French Mid-Size Manufacturer, €2,000,000+ recovery cost (2025)

Scan profile: 24,000 files across 3 servers, 2 databases, daily backup running to a network share. Backup repository accessible from the same network segment as production. No immutable or air-gapped copy. 4 dormant admin accounts. No encryption at rest.

SCORE	VALUE	STATUS
Privacy Risk — S013 Global	**17 / 100**	CRITICAL
Data Protection	12 / 100	CRITICAL
Backup Resilience	8 / 100	CRITICAL
Ransomware exposure	**€ 1,900,000**	—

DIMENSION	SCORE	FINDING
Backup resilience	8 / 100	Backup reachable from production network. No immutability. No air gap.
Encryption coverage	14 / 100	0% encryption on files. 0% encryption at rest on DB volumes.
Access control	21 / 100	4 dormant admin accounts (90+ days inactive). Network share open to all users.
ROT data	35 / 100	38% of files older than 5 years with no retention policy

PRIORITY	ACTION	ESTIMATED IMPACT
P1	Isolate backup repository — move to air-gapped or immutable storage	Backup score: from 8 to 70+
P1	Disable 4 dormant admin accounts immediately	Eliminates highest-privilege attack surface
P1	Encrypt production DB volumes	Art. 32 baseline — currently 0% coverage

> *Recovery cost exceeded €2M. Time to resume operations: four months. APOLLO's Backup Resilience score was 8/100 — CRITICAL. The finding "backup accessible from production network" would have been a P1 action on day one. At €2,999/year, the scan would have paid for itself 666 times over.*

Case 2 — UK Logistics Firm, Active Directory breach via dormant account (2024)

Scan profile: Active Directory — 340 accounts, 28 with admin privileges. 67 accounts inactive for 90+ days, 11 of which retain admin access. Password audit: 19% of accounts match known breach lists. No MFA on domain admin accounts. No privileged access management in place.

SCORE	VALUE	STATUS
Privacy Risk — S013 Global	**23 / 100**	CRITICAL
Data Protection	19 / 100	CRITICAL
Access Control Hygiene	11 / 100	CRITICAL
Estimated breach exposure	**£ 780,000**	—

DIMENSION	SCORE	FINDING
Dormant accounts	4 / 100	67 inactive accounts (19.7%). 11 retain admin-level privileges.
Password hygiene	18 / 100	65 accounts match known breach credential lists (Enzoic check)
MFA coverage	0 / 100	MFA not enforced on any domain admin account
Privilege sprawl	12 / 100	28 admin accounts for 340 users — ratio 8.2% vs recommended 2%

PRIORITY	ACTION	ESTIMATED IMPACT
P1	Disable all accounts inactive 90+ days — 67 accounts flagged	Eliminates primary lateral movement path
P1	Force password reset on 65 accounts matching breach lists	Closes credential stuffing vector
P1	Enforce MFA on all domain admin accounts	Industry standard — currently 0% coverage

> *Palo Alto Unit 42 finds identity weaknesses in 90% of incident response investigations. APOLLO's access control score was 11/100. The 11 dormant admin accounts would have been P1 actions with estimated impact quantified. The breach was detected 210 days after initial compromise — 241-day average. APOLLO flags the exposure before the attacker uses it.*

Case 3 — German Healthcare Provider, ROT data breach (2024)

Scan profile: 47,000 files. 38% flagged as ROT (Redundant, Obsolete, Trivial) — files older than 5 years, no active user, no business tag. 1,400 ROT files contain health data, including patient intake forms from a decommissioned clinic. No encryption. Classified GDPR Article 9.

SCORE	VALUE	STATUS
Privacy Risk — S013 Global	**21 / 100**	CRITICAL
Data Protection	16 / 100	CRITICAL
Compliance GDPR	14 / 100	Grade F
Estimated financial exposure	**€ 620,000**	—

DIMENSION	SCORE	FINDING
ROT data	9 / 100	17,860 files are ROT. 1,400 contain Art. 9 health data from closed clinic.
Encryption coverage	0 / 100	0% of health files encrypted. Open read access on 4 shared drives.
Retention compliance	5 / 100	Files retained 8+ years. Legal basis expired. No deletion schedule.
Breach impact simulation	—	4,200 patients affected if ROT data exfiltrated

PRIORITY	ACTION	ESTIMATED IMPACT
P1	Delete 1,400 ROT health files from decommissioned clinic — no legal basis for retention	– €420,000 exposure (Art. 9 volume reduction)
P1	Encrypt remaining health files pending legal review	Art. 32: from 0 to compliant
P2	Implement automated retention policy — flag ROT files quarterly	Prevents re-accumulation

> *The health data from the decommissioned clinic had no retention basis — the clinic had been closed for 4 years. No one knew it was still there. APOLLO's ROT detection found 1,400 files containing patient data that should have been deleted years earlier. Deletion alone would have reduced GDPR fine exposure by an estimated €420,000.*

2. WHY MONITORING DOES NOT EQUAL PROTECTION

The cybersecurity market for SMBs is dominated by three categories of reactive tools:

CATEGORY	WHAT IT DOES	WHAT IT DOES NOT DO
SIEM (Security Information & Event Management)	Aggregates logs, detects anomalies, generates alerts	Does not audit backup immutability, encryption coverage, or dormant accounts
EDR (Endpoint Detection & Response)	Detects malicious behavior on endpoints, isolates threats	Does not scan data content, does not identify PII, does not assess backup resilience
XDR (Extended Detection & Response)	Extends EDR across network, cloud, and email	Same gaps as EDR — infrastructure-centric, not data-centric

These tools are essential. They are also insufficient.

They answer: "Is an attack happening right now?" They do not answer: "Are my backups immutable? Is my sensitive data encrypted? How many dormant accounts have admin privileges? How much obsolete data contains PII? What would a breach cost me — in euros, in people to notify, in regulatory fines?"

The gap is structural. SIEM, EDR, and XDR are infrastructure-centric and reactive. They monitor what happens to your systems. They do not audit what is true about your data. A proactive posture audit asks a fundamentally different question: not "are we under attack?" but "would we survive one?"

No existing tool under €50K/year combines backup resilience audit + encryption coverage verification + access control hygiene + ROT data identification + breach impact simulation based on actual scanned data.

3. THE SIX DIMENSIONS OF DATA PROTECTION

An IT director preparing for a cyber insurance renewal is asked: "Describe your data protection posture." Today, in most SMBs, the answer is a narrative — "we have backups, we have an EDR, we have a firewall." No numbers. No grades. No proof.

A posture audit replaces narratives with measurements. Six dimensions, each scored:

Backup resilience. Does your backup strategy conform to the 3-2-1-1-0 rule — 3 copies, 2 media types, 1 offsite, 1 immutable or air-gapped, 0 verification errors? Is the declared RPO consistent with the actual backup frequency and retention? When was the last successful restore test?

Encryption coverage. Which volumes, databases, and cloud containers have encryption at rest enabled? Which files containing PII are stored in cleartext? The answer is not "we encrypt everything" — it is "these 340 files with health data on server X are not encrypted." A French healthcare software company was fined €1.7 million for exactly this gap — Article 32 violations on systems that were supposed to be secured.

Ransomware readiness. If 100% of your production data were encrypted by an attacker tomorrow, how long would recovery take? How many people would need to be notified? What would the regulatory fine be? This is not a theoretical exercise — it is a calculation based on the PII types and volumes actually found in your infrastructure.

Access control hygiene. Stolen credentials are the number one attack vector — 22% of all breaches (Verizon DBIR 2025). 19% of Active Directory accounts have passwords already present in known compromise lists (Enzoic 2025). Palo Alto's Unit 42 found identity weaknesses in 90% of their investigations. How many of your accounts have not logged in for 90 days? How many have admin-level privileges? Each dormant privileged account is a door that no one is watching.

Data hygiene (ROT). Up to 70% of enterprise data is Redundant, Obsolete, or Trivial. These files have no business value, but they often contain PII: old HR exports, customer lists from 2019, test databases with real data. The intersection of ROT and PII is where risk hides — files no one remembers, containing data that regulators will ask about.

Breach impact simulation. What would happen if the data in your highest-risk zone were breached? How many individuals affected? Which PII types? What notification cost? What GDPR fine under Article 83? What CCPA exposure? Modeled from actual scan results, not from a hypothetical tabletop scenario.

4. HOW APOLLO DATA AUDITOR MEASURES YOUR POSTURE

The six dimensions described above exist today in a single tool. Here is what the Data Protection module produces.

Your data stays yours. A native agent runs locally on Windows, Linux, and macOS (arm64). It scans files, databases, cloud storage, Active Directory, and infrastructure. Only metadata and counters transit to the cloud dashboard. The agent is open source (BSL 1.1) — verifiable on GitHub.

Six scores, not a security narrative. Each of the six dimensions is graded. Backup resilience is measured against the 3-2-1-1-0 standard. Encryption coverage is mapped by volume and data type. Dormant accounts are listed with their privilege levels and last login dates. ROT files are cross-referenced with the PII scan — "these 2,340 obsolete files still contain 847 PII records."

The breach that hasn't happened yet — quantified. The breach impact simulation calculates what a breach would cost based on your actual data profile — number of individuals affected, PII types exposed, estimated GDPR/CCPA fine, notification costs. This is not an infrastructure attack simulation (that is what BAS tools do at $50K+/year). This is a data-centric impact projection based on what your scan actually found.

Fix the worst gap first. Each corrective action (P1/P2/P3) shows which dimension it improves, which specific gap it closes, and what the impact on your overall posture score would be. "Enable immutable backup on server X → Backup Resilience moves from D to B, ransomware exposure drops by 40%."

Every score is transparent, reproducible, and published. No black box.

THE PRICE COMPARISON

	SIEM/EDR/XDR	BAS (BREACH & ATTACK SIMULATION)	CONSULTING AUDIT	APOLLO DATA AUDITOR
Annual cost	$50,000 – $500,000	$50,000 – $200,000	€10,000 – €50,000 per engagement	**€2,999 / year** (Starter)
Audits data protection posture	No (monitors infrastructure)	No (tests attack paths)	Partial (interviews)	**Yes — 6 dimensions scored**
Breach impact on actual data	No	No (infrastructure-centric)	No (theoretical)	**Yes — data-centric simulation**
ROT × PII correlation	No	No	No	**Yes**
Deployment	Weeks to months	Weeks	4–8 weeks	**Under 48 hours**

5. ONE SCAN. ONE ANSWER. FOUR DIMENSIONS.

Data protection is not a standalone concern. Unencrypted PII is both a protection gap and a compliance violation. A dormant admin account is both a security risk and a financial exposure. An obsolete database full of personal data is both a data hygiene problem and an AI readiness blocker.

Most SMBs treat these as separate problems — one tool for backup, another for compliance, a third for security monitoring, a consultant for the audit. The combined cost exceeds €100K/year. That is not realistic for a company with 200 employees and no dedicated CISO.

APOLLO was built to answer all of these questions in one scan, at a price that reflects SMB reality.

→ **Protection Risk** — what this paper covers. Backup resilience, encryption coverage, ransomware readiness, access control hygiene, ROT data identification, breach impact simulation.

→ **Privacy Risk** — financial quantification in € and $, breach impact simulation, PII mapping, toxic combinations, risk zones.

→ **Compliance Risk** — GDPR scored by article (Art. 5, 9, 30, 32), CCPA, NIS2, SOC2, DORA. Grades A through F based on actual data. Remediation plan with financial impact per action.

→ **Quality & AI** — AI Readiness scoring, data quality metrics, AI Act pre-compliance (Article 10 data governance, Article 15 cybersecurity posture).

No other tool under €5,000/year covers all four. The cybersecurity market was built around reactive monitoring for enterprises. **APOLLO™ Data Auditor** exists because SMBs need proactive answers about their data — before the attack, not after.

Sources: Veeam Data Protection Trends 2024 & 2025 · Sophos State of Ransomware 2025 · Verizon DBIR 2025 · Palo Alto Unit 42 Incident Response Report 2026 · IBM Cost of a Data Breach 2025 · Enzoic AD Password Security Report 2025 · Orange Cyberdefense PME France 2025 · Mastercard SMB Study 2025 · CNIL Bilan sanctions 2025 · Fortune Business Insights BAS Market 2026

APOLLO™ Data Auditor
Every file is a risk. Measure it.

→ https://apollo.aiia-tech.com
→ GitHub: https://ggabrie2025.github.io/apollo_data_auditor/
→ contact@aiia-tech.com