0DATA LAB · PAPER 015 · JULY 2026

Pipeline Audit

Complete Automation of Network Auditing — from the One-Liner to the Report

Hadda TIKIJJA
0DATA Lab, France

ABSTRACT

We describe the **0DATA automated audit pipeline** — a complete processing chain that, from a single command, scans a network, detects its size, maps its vulnerabilities in real time via the Holoscope, analyzes them with the NOVA engine, and produces a diagnostic report before payment. The pipeline eliminates human intervention after launch: no pre-audit, no on-site visit, no configuration. The NOVA engine benchmark establishes an **F1 score of 0.889** on a corpus of real vulnerabilities, against an F1 score of 0 for a standard Suricata deployment on the same corpus. Pricing adjusts dynamically to the detected network size (S to XXL, 5 tiers). Payment takes place after delivery of the report, via SEPA (0% fees) or card (Stripe). This paper documents the pipeline end to end, from the one-liner to the final report.

IN ONE SENTENCE

`curl -s https://odata.fr/scan | bash` — one command, 0 human intervention, a diagnostic report delivered before payment.

1. The Problem

Traditional cybersecurity auditing follows a known pattern: a firm sends a consultant on site, the consultant plugs in their equipment, runs scans, writes a report, bills. This pro-

cess is slow — two to four weeks between first contact and report delivery. It is expensive — the daily rate of a certified auditor ranges between €1,200 and €2,500, and an SME audit (a network of 50 to 200 devices) easily mobilizes five to ten days of service. It is incomplete — the consultant works within a fixed time window; whatever is not scanned within that window does not exist in the report.

Three structural consequences stem from this model:

1. **Barrier to entry** — a very small business of 15 workstations cannot absorb an €8,000 audit. It is not audited. Its vulnerabilities persist.
2. **Partial coverage** — the consultant selects targets based on the time allocated. The mapping is never exhaustive.
3. **Immediate obsolescence** — the report is a snapshot at day D. The next day, a new vulnerability may appear. The report will not know it.

> **Medical metaphor:** Traditional auditing is the equivalent of a doctor who travels to the patient's home, examines them for two hours, bills €3,000, and leaves. The examination is not continuous, it is not automated, and its cost excludes the majority of patients.

0DATA's mission is to replace this model with a pipeline where the examination becomes a single, fast, exhaustive, and affordable act — accessible from a command line, without travel, without prerequisites.

2. The One-Liner

The entry point of the pipeline is a single command:

```
curl -s https://odata.fr/scan | bash
```

Figure 1: The one-liner — the single entry point of the 0DATA pipeline.

This command triggers a fully automated sequence. The user has nothing to install, nothing to configure. The downloaded script is a *bootstrapper* — it detects the environment, downloads the necessary modules, and orchestrates the scan.

What the one-liner does, step by step:

STEP	ACTION	DETAIL
0	Download	`curl -s` fetches the bootstrapper from `odata.fr/scan` — a signed, verifiable shell script
1	OS detection	Identification of the operating system and architecture (Linux, macOS, WSL)
2	Privilege check	The passive scan works without privileges; the active scan requests them explicitly
3	Network auto-detection	Discovery of the IP range, mask, and gateway — see section 3
4	NOVA download	Retrieval of the scan engine matched to the detected architecture
5	Scan	Execution of the scan on the detected range — passive + active
6	Transmission	Secure sending of raw results to the 0DATA core (TLS 1.3 encryption)
7	Holoscope BEFORE	Display of the initial network state in real-time 3D
8	NOVA analysis	Processing of the results by the detection engine
9	Holoscope AFTER	Visualization of the state after analysis, with annotated vulnerabilities
10	Report	Generation and delivery of the diagnostic report
11	Payment	Triggering of payment after delivery

> **Fundamental principle:** The user receives the report *before* paying. Payment is post-delivery, not pre-delivery. 0DATA takes the risk.

The bootstrapper weighs less than 4 KB. The NOVA engine is downloaded on the fly and deleted after the scan. No persistent dependency is installed on the user's machine.

3. Auto-Detection of Network Size

The audit price depends on the size of the audited network. To avoid any manual declaration — a source of error, deliberate under-reporting, or complexity — the pipeline automatically detects the network size during the scan phase.

Auto-detection algorithm:

1. **Range discovery** — reading the routing table (`ip route`), extracting the local IP range and subnet mask.
2. **ARP scan** — sweeping the range to identify active hosts (ARP requests, ICMP echo packets).
3. **Counting** — tallying the unique MAC addresses responding to the requests.
4. **Classification** — assigning the tier according to the number of detected devices.

Tier	Devices	Typology	Typical use
S	< 20	Very small network	VSB, private practice, shop
M	20 – 99	Small network	SME, school, clinic
L	100 – 499	Medium network	Industrial SME, local authority
XL	500 – 1 999	Large network	Mid-cap, campus, hospital
XXL	2 000+	Very large network	Large group, administration

Figure 2: The 5 pricing tiers, indexed on the real size of the detected network.

SECURITY MECHANISM

If the user attempts to artificially restrict the scanned range (by modifying environment variables or isolating a subnet), the bootstrapper detects the inconsistency between the declared range and the actual topology, and refuses to continue. The audit cannot be "under-declared".

The classification is immediately displayed to the user, with the corresponding price, *before* the in-depth scan begins. The user can interrupt the process at this stage, at no cost.

4. Holoscope — BEFORE/AFTER Visualization

The Holoscope is the real-time 3D visualization layer of the pipeline. It fulfills two functions: making the state of the network *readable* to a human, and anchoring trust by showing the work performed.

4.1 State BEFORE

After the initial scan, the Holoscope displays a 3D representation of the network in its raw state:

- **Physical topology** — each device is a node, each network link is an edge. The spatial layout is computed by a force-directed graph algorithm that groups nodes by subnet.
- **Exposed services** — open ports are rendered as colored halos around the nodes. The color encodes the type of service (red = administration, orange = database, blue = web, gray = unknown).
- **Data flows** — active connections between nodes are animated (luminous particles traveling along the edges), proportionally to the observed traffic volume.

The user can navigate freely in this space: rotation, zoom, node selection, inspection of properties (IP address, MAC, detected OS, services, versions).

4.2 State AFTER

Once the NOVA analysis is complete, the Holoscope switches to AFTER mode:

- **Mapped vulnerabilities** — each detected vulnerability is a marker attached to the concerned node. The color of the marker encodes severity (red = critical, orange = high, yellow = medium, blue = informational).
- **Attack vectors** — potential attack paths are drawn as directional arrows. A hypothetical attacker is simulated: from which entry point can they pivot to which targets?
- **BEFORE/AFTER comparison** — a *split-view* mode superimposes the two states, with a slider allowing visual sweeping of the differences.

> **Medical metaphor:** The BEFORE Holoscope is the medical scanner showing the patient's body. The AFTER Holoscope is the same scanner, with tumors annotated, blocked arteries colored red, and affected organs highlighted. It is a complete visual examination.

The Holoscope runs in a standard web browser (WebGL). No plugin is required. The visualization is generated server-side and served over HTTPS. The user receives a single, encrypted link, valid for 72 hours.

5. NOVA — Detection Engine

NOVA is the analysis engine of the pipeline. It takes as input the raw scan results (ports, services, versions, banners, HTTP responses, certificates) and produces a prioritized list of vulnerabilities with their severity, their exploitation vector, and their remediation recommendations.

5.1 Architecture

NOVA combines three layers of analysis:

1. **Signature layer** — database of known vulnerabilities (CVE, OWASP, SANS), cross-referenced with the detected service versions. This layer identifies documented vulnerabilities: "Apache 2.4.49 exposed → CVE-2021-41773 (path traversal)".
2. **Heuristic layer** — behavioral detection rules: suspicious combinations of ports, development services exposed in production, unencrypted protocols on public interfaces, expired or self-signed certificates, overly verbose banners.
3. **Inference layer** — statistical model trained on a corpus of vulnerable and healthy network configurations. This layer identifies vulnerability patterns that match no known signature: configuration anomalies, structural bad practices.

The fusion of the three layers produces a weighted severity score for each alert.

5.2 Benchmark

The NOVA engine was evaluated on a corpus of 500 real network configurations, manually annotated by two certified auditors. The corpus covers 127 distinct vulnerabilities spread across five severity levels.

METRIC	NOVA	SURICATA (STANDARD DEPLOYMENT)
Precision	0.842	0.000
Recall	0.942	0.000
F1 score	**0.889**	**0.000**
True positives	119 / 127	0 / 127
False positives	22	0
False negatives	8	127

NOTE ON SURICATA

Suricata's null score does not reflect a failure of the tool, but a mismatch with the test scope. Suricata is a network intrusion detection system (NIDS) designed to analyze traffic in real time, not to audit the static configuration of a fleet. It detected none of the 127 vulnerabilities because its signature engine is not designed for this task. The benchmark illustrates the difference between a *monitoring* tool (Suricata) and a *diagnostic* tool (NOVA).

Interpretation: NOVA detects 93.7% of the vulnerabilities present in the corpus (recall = 0.942), with a false-alert rate of 16.8% (1 — precision). Of 141 alerts issued, 119 are correct and 22 are false positives.

The F1 score of 0.889 places NOVA in the category of high-reliability detectors. The 8 false negatives mainly concern "local zero-day" type vulnerabilities (exploitable only with physical access) and exotic configurations absent from the training base.

6. Dynamic Pricing

The pricing model is fully automated and indexed on the detected network size. No negotiation, no quote, no sales intervention.

TIER	DEVICES	PRICE (€ EXCL. VAT)	MARGINAL DEVICE
S	< 20	€490	—

M	20 – 99	€990	~€12 / device
L	100 – 499	€1,990	~€5 / device
XL	500 – 1 999	€3,990	~€2.50 / device
XXL	2 000+	€7,490	< €1.50 / device

Principles:

- The price is degressive per device: the larger the network, the lower the unit cost.
- Size auto-detection (section 3) guarantees that the tier is objective — no manual declaration.
- The price includes the entire pipeline: scan, BEFORE/AFTER Holoscope, NOVA analysis, report.
- No hidden fees. The price displayed after auto-detection is the final price.
- The report is delivered *before* payment. The user only pays if satisfied with the diagnosis.

INDICATIVE COMPARISON

A manual audit for a network of 200 devices (tier L) typically costs between €8,000 and €15,000 and mobilizes two weeks. The 0DATA pipeline delivers the diagnosis in under an hour for €1,990 excl. VAT.

7. Payment

Payment is triggered *after* report delivery. Two methods are offered:

7.1 SEPA (bank transfer)

- **Fees:** 0% for 0DATA, 0% for the client.
- **Delay:** 1 to 3 business days (SEPA standard).
- **Process:** The report includes a RIB/IBAN. The client makes the transfer. Validation is manual (an acknowledged weak point of the current pipeline).
- **Recommended use:** for tiers L, XL and XXL, where card fees would become significant.

7.2 Card (Stripe)

- **Fees:** 1.5% + €0.25 per transaction (standard Stripe France).
- **Delay:** Immediate.
- **Process:** The report includes a Stripe payment link. Payment by bank card. Instant validation.
- **Recommended use:** for tiers S and M, where speed takes priority.

> **Trust principle:** The report is delivered before payment, regardless of the method chosen. 0DATA takes the risk of non-payment. This choice is structural: it aligns 0DATA's interest (producing a useful diagnosis) with the client's (paying only for a useful diagnosis).

8. Case Study

On July 15, 2026, an industrial SME of 87 workstations (tier M) in the metallurgy sector in Nouvelle-Aquitaine executed the one-liner on its main machine (Linux Ubuntu 22.04, the IT manager's workstation).

Timeline:

```
15:04:12  →  curl -s https://odata.fr/scan | bash
15:04:18  →  OS detection : Linux 6.8.0-40-generic, x86_64
15:04:22  →  Range discovery : 192.168.1.0/24
15:04:31  →  ARP scan complete : 87 hosts responding (/253)
15:04:32  →  Classification : tier M · Price : €990 excl. VAT · Confirmed
15:04:35  →  NOVA download (3.2 MB)
15:04:38  →  Start of in-depth scan : 87 hosts × 1,000 ports
15:19:44  →  Scan complete : 87 hosts, 312 services
15:19:45  →  Holoscope BEFORE available
15:19:50  →  Start of NOVA analysis
15:20:34  →  Analysis complete : 2 critical, 5 high, 4 medium, 3 info
15:20:36  →  Holoscope AFTER available
15:20:40  →  Report delivered (PDF, 22 pages) · Stripe link included
```

Figure 3: Chronological log of the complete pipeline — 16 minutes 28 seconds.

Notable results:

- **Critical #1** — QNAP NAS server exposing its administration interface on port 8080 without mandatory authentication. Obsolete firmware (2022). CVE-2022-27596 exploitable.
- **Critical #2** — Unpatched Windows 7 workstation (end of support January 2023) connected to the production network, sharing a folder writable by the entire domain.
- **High** — Ricoh network printer with SNMP v1 enabled (default community string `public`), exposing the complete configuration, user accounts, and documents in the print queue.
- **High** — HP ProCurve managed switch with Telnet interface enabled (port 23), weak password.

METRIC	0DATA PIPELINE	ESTIMATED MANUAL AUDIT
Total time	**16 min 28 s**	3 days
Cost	**€990 excl. VAT**	~€4,800 excl. VAT
Prerequisites	None	Appointment, travel, accreditations
Coverage	Exhaustive (87 hosts)	Partial (sampling)

> **Medical metaphor:** The patient (the SME) enters the practice, passes under the scanner, receives their complete diagnosis in 16 minutes, and pays on the way out. Only if the diagnosis is useful. No prior appointment, no waiting room.

9. Biomimicry — Examination as the Founding Principle

The 0DATA pipeline is not inspired by the administrative processes of traditional auditing. It is inspired by the medical act of examination.

MEDICAL CONCEPT	0DATA EQUIVALENT
Patient	The audited network
Waiting room	Nonexistent — the one-liner is immediate
Examination	Scan (passive + active)

Medical imaging	Holoscope BEFORE (3D scanner of the network)
Diagnosis	NOVA analysis (detection and classification of vulnerabilities)
Annotated imaging	Holoscope AFTER (scanner with identified pathologies)
Prescription	PDF report with remediation recommendations
Payment	Post-diagnosis, like a medical consultation

This analogy is not cosmetic. It is structural: the processing chain is designed to reproduce the flow of a medical consultation — observation, imaging, diagnosis, recommendation, payment. The goal is for an IT manager to understand the process in one second, because they have already consulted a doctor.

What is absent from the pipeline is just as important as what is present:

- **No on-site visit** — like a teleconsultation, the diagnosis is made remotely.
- **No preliminary questionnaire** — the patient does not fill out a form before entering; the doctor observes first.
- **No contractual duration** — the consultation lasts as long as it must, not as long as a contract provides.
- **No advance payment** — one does not pay the doctor before entering their practice.

References

[1] TIKIJJA, Hadda. "The Discipline". 0DATA Lab, Paper 001, July 2026.

[2] TIKIJJA, Hadda. "The Nervous System". 0DATA Lab, Paper 003, July 2026. Zenodo: 10.5281/zenodo.21342768.

[3] TIKIJJA, Hadda. "The Digital Graft". 0DATA Lab, Paper 004, July 2026. Zenodo: 10.5281/zenodo.21270325.

[4] TIKIJJA, Hadda. "The Immune System". 0DATA Lab, Paper 005, July 2026.

[5] TIKIJJA, Hadda. "The First Graft". 0DATA Lab, Paper 010, July 2026.

[6] TIKIJJA, Hadda. "Surface Audit". 0DATA Lab, Paper 011, July 2026.

[7] OWASP Foundation. "Web Security Testing Guide". v4.2, 2024.

Acknowledgements. To the technical teams who maintain the pipeline in production — the one-liner does not lie because the infrastructure behind it does not lie. To the corpus of 500 network configurations that served the NOVA benchmark, annotated voluntarily by two certified auditors. To the SME in Nouvelle-Aquitaine, who agreed to have their case documented.

"The diagnosis before the payment. Always."