GATEWATCHER
NDR PLATFORM

GATEWATCHER

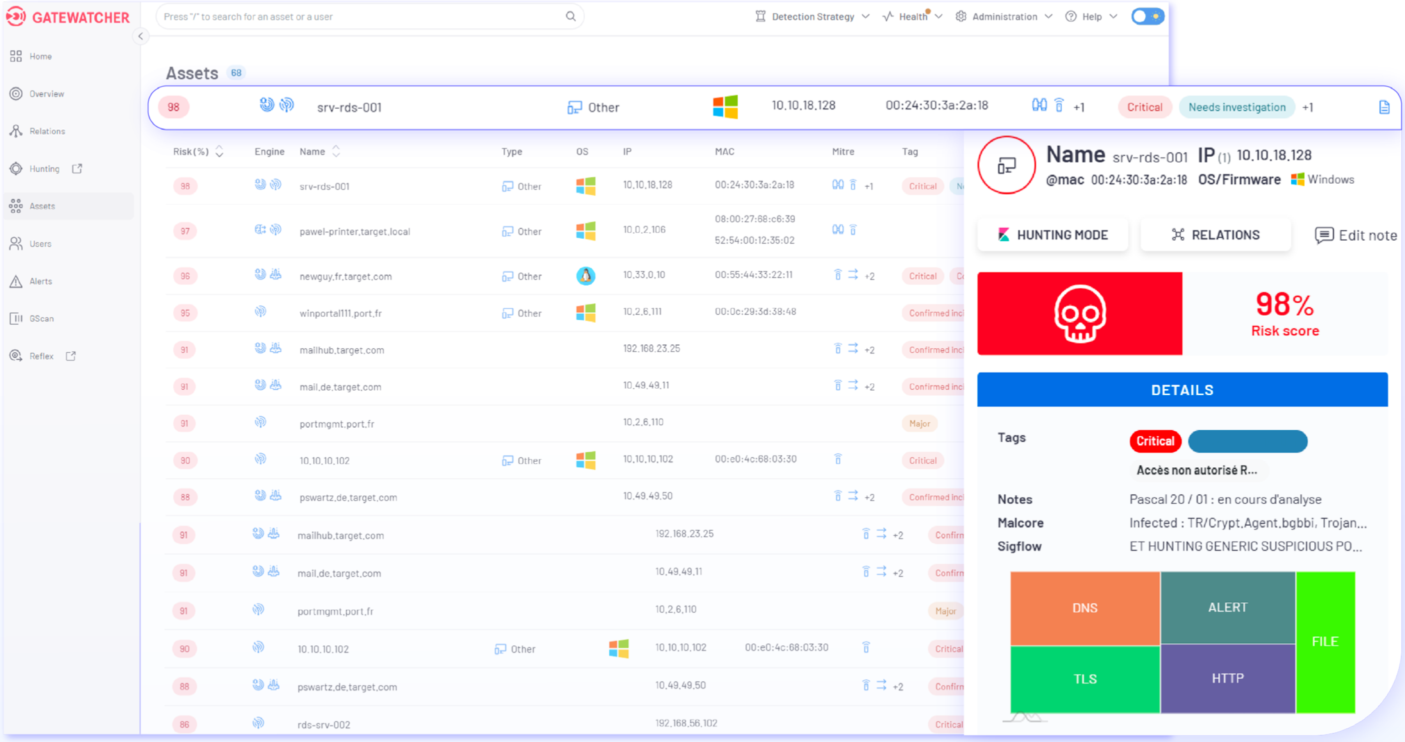
Network never lies

Leverage network truth to *unlock your actions_*

✓ **Capture and normalize all threat activities**
Enhance decision-making with full behavioral analysis and deep network visibility, including insights into users, assets, and applications, across IT, OT, and cloud infrastructures

✓ **Reduce biased analysis to deliver accurate AI reasoning**
Extract raw insights and deep network inspection to reinforce orchestrated AI context analysis leaving no place for threat actors

✓ **Protect business with strong confidence**
Defeat threats at speed with complete certainty, grounded in cross-signal, autonomous analysis



Assets 68

98	srv-rds-001	Other		10.10.18.128	00:24:30:3a:2a:18	+1	Critical	Needs investigation	+1

Risk (%)	Engine	Name	Type	OS	IP	MAC	Mitre	Tag
98		srv-rds-001	Other		10.10.18.128	00:24:30:3a:2a:18	+1	Critical N
97		pawel-printer.target.local	Other		10.0.2.106	08:00:27:68:c6:39 52:54:00:12:35:02		
96		newguy.fr.target.com	Other		10.33.0.10	00:55:44:33:22:11	+2	Critical C
95		winportal111.port.fr	Other		10.2.6.111	00:0c:29:3d:38:48		Confirmed inci
91		mailhub.target.com			192.168.23.25		+2	Confirmed inci
91		mail.de.target.com			10.49.49.11		+2	Confirmed inci
91		portmgmt.port.fr			10.2.6.110			Major
90		10.10.10.102	Other		10.10.10.102	00:e0:4c:68:03:30		Critical
88		pswartz.de.target.com			10.49.49.50		+2	Confirmed inci
91		mailhub.target.com			192.168.23.25		+2	Confirm
91		mail.de.target.com			10.49.49.11		+2	Confirm
91		portmgmt.port.fr			10.2.6.110			Major
90		10.10.10.102	Other		10.10.10.102	00:e0:4c:68:03:30		Critical
88		pswartz.de.target.com			10.49.49.50		+2	Confirm
86		rds-srv-002			192.168.56.102			Critical

Name srv-rds-001 **IP** (1) 10.10.18.128
@mac 00:24:30:3a:2a:18 **OS/Firmware** Windows

98%
Risk score

DETAILS

Tags: Critical, Accès non autorisé R...
Notes: Pascal 20 / 01 : en cours d'analyse
Malcore: Infected : TR/Crypt.Agent.bgbbi, Trojan...
Sigflow: ET HUNTING GENERIC SUSPICIOUS PO...

Turn data into *actionable decision_*

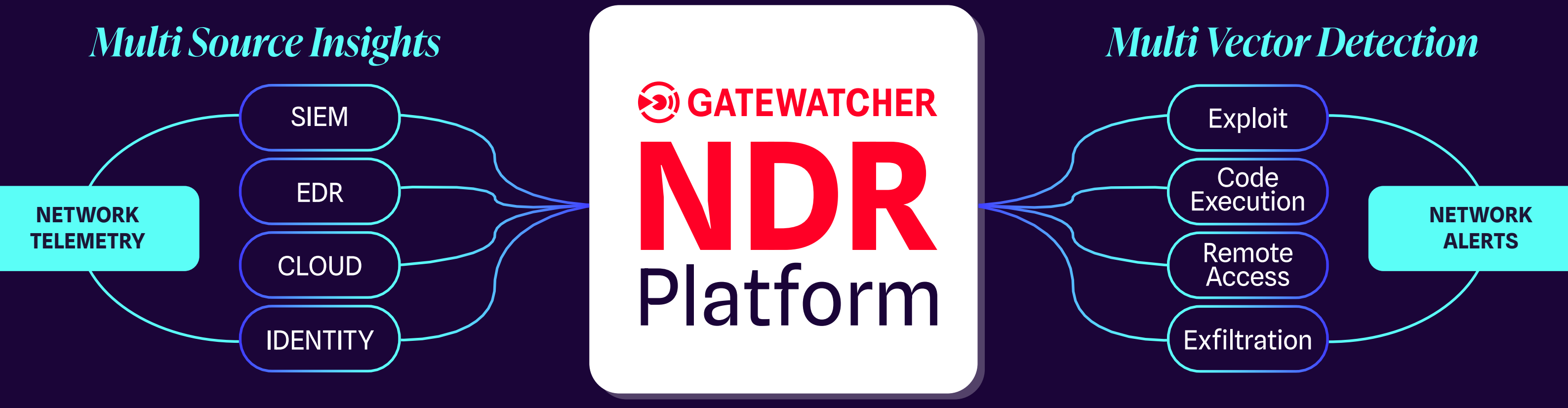
> ***High-fidelity telemetry for decision quality***
Build a complete inventory of network assets (IP, MAC, hostname, OS) and identify user flows, so every alert can be tied to who/what is affected, a prerequisite for asset-centric decisioning

> ***Content extraction for deeper evidence***
Reconstruct files in transit (HTTP/SMTP/SMB/FTP, etc.) so detection engines can produce higher-confidence evidence (critical for downstream scoring and AI verdicts)

> ***Richer context even when traffic is encrypted***
Collect extensive flow metadata (timestamps, src/dst, protocol, app context, fingerprints, SNI, JA3, etc.), enabling correlation and reasoning when payload visibility is limited

> ***From zero to full visibility in minutes***
Deliver broad network coverage so SOC gain full visibility fast and take decisions with high-fidelity signals from day one

From noise to action



Multi Source Insights

NETWORK TELEMETRY

SIEM

EDR

CLOUD

IDENTITY

GATEWATCHER

NDR Platform

Multi Vector Detection

Exploit

Code Execution

Remote Access

Exfiltration

NETWORK ALERTS

The power to decide across *all your security signals*_

Built on strong context

- **Consolidate multi-source security signals**
  Enhance insights across your security stack (NDR, SIEM, EDR, Cloud and identity security providers...)
- **Orchestrate security and business context analysis at speed**
  Qualify threat based on autonomous reasoning forged on real time signals
- **Protect business with strong confidence**
  Defeat threats at speed with complete certainty grounded on multi-source and autonomous signal analysis

Trusted security decision

- **Determine what matters**
  Turn multi-sourced AI analysis into actionable protection measures
- **Governed Decision-to-Action Orchestration**
  Supports controlled execution workflows with full lifecycle tracking and human oversight
- **Introducing a Decision Contract framework**
  Explain and track evidences and executed actions to engage continuous cyber resilience improvement plan

Your Business Impact

95% Alert Noise Reduction + **10x** Faster triage + **60%** Cost reduction = **Reduce** ambiguity & SOC fatigue + Mean time to *Decide* **< 5 min**

> *Alert compression, reducing noise*
Transform alert floods into a short, manageable set of actionable decisions

> *Asset-centric prioritization*
Rank the most at-risk assets first, so teams focus where impact is highes

> *Automated enrichment & contex*
Unify threat intelligence with technical and business context to take the guesswork out of security decisions

> *AI-assisted decisioning*
Deliver a clear verdict with confidence, plus “what to do next” guidance

> *Faster triage and response*
Standardize investigation workflows and reduce time-to-containment (MTTR) with trust

> *Governance & reporting-ready outputs*
Produce consistent, explainable decisions for SOC KPIs, risk reporting, and audits

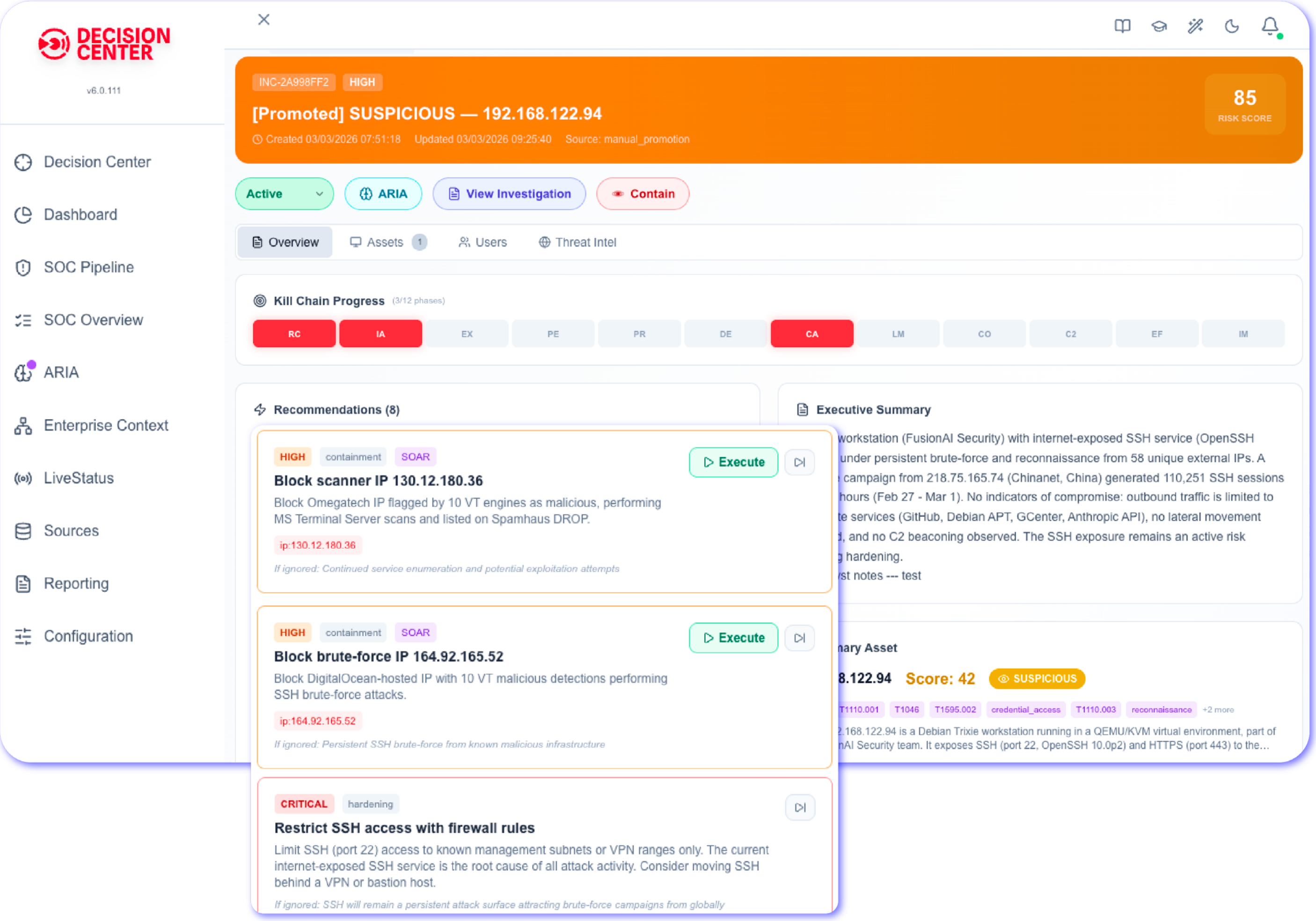
Ahead of threats

Network signals become *decision-ready_*

- **Silence the noise, amplify the action**
  Turn alert floods into a short, prioritized list of at-risk assets preserving evidence, sharpening analyst focus, and standardizing decisions

- **Detect everywhere, decide once**
  Multiple detections and sources are merged into one coherent case per asset—single verdict, single priority, single action path

- **Evidence-rich decisions, not just another alert**
  Catch intrusions at the first weak signals, then auto-gather proof and AI-driven prioritization so the SOC reacts fast, cuts noise, and lowers workload



[Promoted] SUSPICIOUS — 192.168.122.94

Created 03/03/2026 07:51:18 Updated 03/03/2026 09:25:40 Source: manual_promotion

Block scanner IP 130.12.180.36

Block Omegatech IP flagged by 10 VT engines as malicious, performing MS Terminal Server scans and listed on Spamhaus DROP.

ip:130.12.180.36

If ignored: Continued service enumeration and potential exploitation attempts

Block brute-force IP 164.92.165.52

Block DigitalOcean-hosted IP with 10 VT malicious detections performing SSH brute-force attacks.

ip:164.92.165.52

If ignored: Persistent SSH brute-force from known malicious infrastructure

Restrict SSH access with firewall rules

Limit SSH (port 22) access to known management subnets or VPN ranges only. The current internet-exposed SSH service is the root cause of all attack activity. Consider moving SSH behind a VPN or bastion host.

If ignored: SSH will remain a persistent attack surface attracting brute-force campaigns from globally

workstation (FusionAI Security) with internet-exposed SSH service (OpenSSH
under persistent brute-force and reconnaissance from 58 unique external IPs. A
campaign from 218.75.165.74 (Chinanet, China) generated 110,251 SSH sessions
hours (Feb 27 - Mar 1). No indicators of compromise: outbound traffic is limited to
te services (GitHub, Debian APT, GCenter, Anthropic API), no lateral movement
d, and no C2 beaconing observed. The SSH exposure remains an active risk
g hardening.
st notes --- test

nary Asset

8.122.94 Score: 42

2.168.122.94 is a Debian Trixie workstation running in a QEMU/KVM virtual environment, part of
nAI Security team. It exposes SSH (port 22, OpenSSH 10.0p2) and HTTPS (port 443) to the...

When detection is strong, *decisions become simple_*

> ***Multi-engine detection across the kill chain***
Combine complementary engines (signature, behavioral, content, threat-intelligence) to provide end-to-end coverage of modern attacks

> ***Evidence-rich alerts, not just triggers***
Provide analyst-grade artifacts and context, so investigations start with evidence, not assumptions

> ***Noise reduction through fine-tuning***
Calibrate granularly (thresolds, frequency, and context), to align detection with real environments and reduce false positives.

> ***Plug into your security ecosystem and close the loop***
Drive response through automated playbooks and containment actions so detection turn into consistent, auditable outcomes

DECIDE AT SPEED WITHOUT TRADE-OFF

Why sift through noise when you could be driving decisions?_

Decision Center turns fragmented signals into **Decision Contracts Framework**: structured outcomes that are traceable, auditable, and operationally actionable.

By correlating alerts from multiple sources into an asset-centric case file (context + history + threat intelligence), it eliminates noise at scale and delivers consistent, explainable next steps, so your team executes with confidence instead of debating uncertainty.

Decision Center runs an always-on pipeline **FETCH → DEDUPLICATE → ENRICH → ANALYZE → CONCLUDE** to convert high-volume telemetry into a prioritized queue of at-risk assets, not endless alert lists.
The result: **false positives removed**, triage reduced to seconds, and faster containment through integrated response paths.

How much time do you spend rebuilding context — before you can even make a decision?_

Security stacks generate massive volumes of network, identity, cloud and threat signals. In isolation, they create noise and force every organization to rebuild context manually. Decision Center turns that overload into actionable and **intelligent outcomes by unifying, deduplicating and correlating multi-source signals into a single, asset-centric decision flow**, so you act on what matters, not on what shouts the loudest.

What makes it different is how it qualifies risk in real time. **Decision Center continuously factors in the customer's business context**, asset criticality, ownership, production vs. non-production environment, exposure and identity context, alongside threat intelligence and behavioral evidence. The outcome is a structured, evidence-backed verdict with confidence and clear "what to do next" guidance, aligned with true business impact.

And it does all of this with total human control. Decision Center can recommend, orchestrate and accelerate response, but enforcement remains governed by the SOC: approval gates, analyst oversight, and fully traceable decision trails. You scale speed and consistency without surrendering accountability, **delivering security actions that are explainable, auditable, and defensible.**

What if the fastest decision were also the best one?_

Instead of forcing analysts to trade time for confidence, Decision Center correlates and contextualizes signals into a single decision space, applies business-aware risk qualification, and delivers **consistent, explainable decisions.** The result: **faster containment**, fewer errors, and decisions you can stand behind.

Move fast and you risk disruption. Investigate longer and you increase exposure. Decision Center removes the trade-off by turning fragmented network, identity, cloud and exposure signals into **structured, evidence-based decisions**—with **business context, confidence scoring, and guided next steps under human control.**

Take a look at our use cases

gatewatcher.com

Cybersecurity for business *serenity*_

Explore our solutions...

✉ contact@gatewatcher.com
☎ +33 (0)1 44 51 03 93
Campus Cyber • Puteaux, France

in GATEWATCHER
GATEWATCHER Official
X @GATEW4TCHER