

WHITEPAPER PAKAROS

# From noise to clarity and control

How PAKAROS orchestrates continuity,  
compliance and boardroom control  
across your security stack.

LONDON

PARIS

BERLIN

BRUSSELS

RIGA

MADRID

LISBON



In every context. On every event.  
Always in control.

# From noise to calm and control

*How PAKAROS uses an orchestration layer to bring continuity, compliance, and control on top of your existing security stack*

## Executive summary

Most organisations rarely lack technology. The problem lies in the connection: separate security applications running side by side without coordination, producing fragmented reports that nobody at board level understands, with responsibility falling between vendors.

PAKAROS is an AI-driven, human-led security orchestration and control platform. It does not replace your existing vendors, but connects them into one coherent picture, with reporting that fits analyst, management, and board level. It is a valuable addition to the IT security team, so breaches are detected at the earliest possible stage, and resolved when they do occur. This document describes what PAKAROS is, how the platform works, what sets it apart, and what you can expect from the collaboration.

## The problem PAKAROS solves

Most organisations already have all kinds of solutions in place. The problem is not a lack of technology, but the absence of a connecting layer between those separate applications. Each application runs on its own, with its own dashboard and its own definition of an incident.

- Security applications work alongside each other, not with each other. Every tool has its own dashboard and its own definition of an incident.
- As a result, reporting is technical and incidental, not strategic and periodic. A board rarely sees a fixed quarterly rhythm.
- Compliance: under the EU NIS2 Directive, organisations must meet a duty of care. This requires them to record security-relevant and operational events in a way that is demonstrable and traceable.
- Visibility stops at known, managed devices, while unmanaged devices and AI tooling often stay out of sight.

**PAKAROS is not an extra tool next to your stack, but the layer that connects your existing stack and translates it into overview and control.**

## The numbers behind the urgency

This is not a theoretical risk. Recent research shows how large the impact is, specifically for SMEs.

- Nearly six in ten SMEs in Europe experienced a cyberattack in the past 12 months. Attackers increasingly go after the least protected organisations, not the largest.<sup>1</sup>
- A security incident costs a European SME an average of close to €220,000<sup>2</sup>. Source: ESET, SMB Digital Security Sentiment Report.
- Organisations worldwide need an average of 241 days to identify and contain a data breach, the lowest figure in nine years, but still eight months<sup>3</sup>.

The longer an application landscape stays fragmented, the longer those 241 days last in practice. Connected visibility and correlation is exactly where that time is won back.

<sup>1</sup> <https://www.hiscoxgroup.com/news/press-releases/2025/29-09-25>

<sup>2</sup> <https://www.eset.com/uk/about/newsroom/press-releases/eset-releases-new-smb-research-finds-businesses-lose-hundreds-of-thousands-of-euros-in-data-security-1/>

<sup>3</sup> [www-api.ibm.com/adobe/assets/urn:aaid:aem:607b9590-38e0-4c91-b433-aa8a17f5b5e8/original/as/cost-of-a-data-breach-2025-full-report.pdf](https://www-api.ibm.com/adobe/assets/urn:aaid:aem:607b9590-38e0-4c91-b433-aa8a17f5b5e8/original/as/cost-of-a-data-breach-2025-full-report.pdf)

## PAKAROS in numbers: performance and KPIs

Where the sector average for detection and containment stands at 241 days, PAKAROS works with fixed, hard service levels. The figures below are not targets, but the service levels at which PAKAROS is delivered.

**From a 241-day sector average to identification, to a maximum of 9 hours for a substantiated verdict from PAKAROS.**

- On average, 92% of relevant alerts are automatically remediated by the platform, without manual intervention.
- Alerts flagged as relevant are investigated by PAKAROS analysts. That analysis always results in a verdict.

| Verdict        | Meaning                                          |
|----------------|--------------------------------------------------|
| False Positive | No actual security incident.                     |
| Maintenance    | Legitimate IT activity.                          |
| Incident       | Confirmed security incident, follow-up required. |

For response times, PAKAROS applies fixed service levels, with P1 and P2 as the highest priority levels.

| Activity              | Service level                                   |
|-----------------------|-------------------------------------------------|
| Alert detection       | Real-time                                       |
| Alert handover        | Immediate                                       |
| Root cause analysis   | As discussed within the Service Level Agreement |
| Verdict communication | As discussed within the Service Level Agreement |

That means an analysis and verdict is available within a short amount of time. Response time is within minutes. Against a sector average of 241 days to identify and contain a breach, that is the difference between months of uncertainty and a concrete answer within the same part of the day. The comparison is not one to one: the 241 days measures the full lifecycle of a breach, the PAKAROS service level measures the time to a first substantiated verdict. It is precisely that verdict that shortens the lifecycle afterwards.

## Automated response (containment)

Where technically possible, the platform applies automated security measures to limit the impact of attacks. Automated measures are only applied when they are technically supported, agreed with the customer in advance, and part of the environment's configuration.

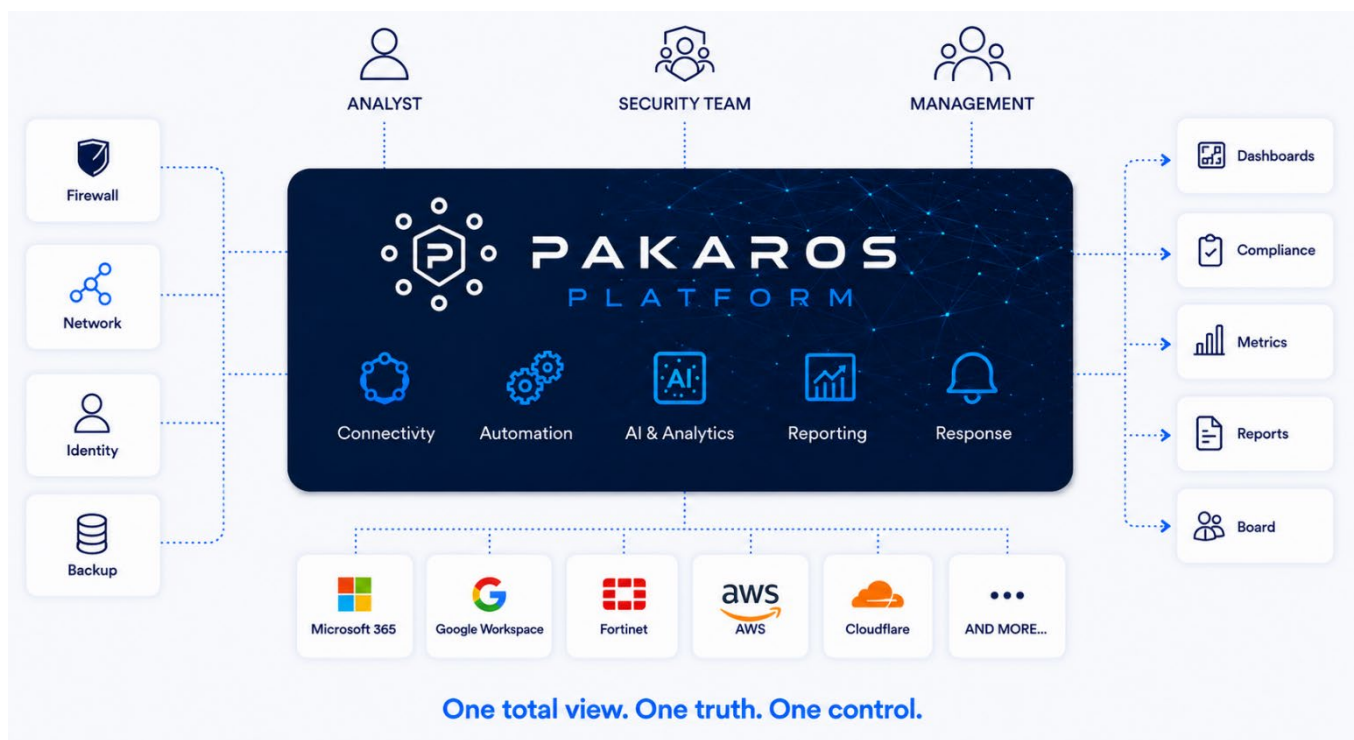
- Endpoint protection: blocking malware, stopping malicious processes, quarantining malicious files, isolating endpoints.
- Network protection: blocking IP addresses, blocking domains, blocking command-and-control communication.
- Identity protection: blocking accounts, terminating suspicious sessions, forcing password resets.

All automated actions are logged and included in the alert notification, so every intervention is demonstrable and traceable.

## What is PAKAROS

PAKAROS was created from the idea that security no longer needs more technology, but more control. The platform positions itself as a non-competitive orchestration layer that connects endpoint, cloud, identity, and compliance controls from existing vendors into one coherent picture.

- Built for organisations with 10 to 1,500 workstations, with a focus on SMEs.
- Available through direct platform subscriptions, consultancy, and a partner channel of MSPs.
- More than 525 vendor integrations, making the platform easy to connect.
- Fully European cloud storage, with no dependency on US cloud providers.



## The four modules

PAKAROS delivers coverage that grows with your organisation's maturity, through four modules that can be deployed separately or combined.

| Module                 | For whom                                                                                                                                                                                           |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>AV + EDR</b>        | Endpoint protection and detection as a foundation, suited to organisations starting with structured security.                                                                                      |
| <b>Managed EDR</b>     | Detection and response carried out by PAKAROS, so your own team can focus on the organisation.                                                                                                     |
| <b>AV + EDR + SIEM</b> | Endpoint protection combined with central logging and correlation for broader oversight.                                                                                                           |
| <b>Managed SOC</b>     | Full orchestration, monitoring, and incident response by PAKAROS, built into the module, with reporting at multiple levels and periodic consultation with the IT team to optimise the environment. |



### AV + EDR

Endpoint protection that sees further.

- ✓ Prevention, detection and response on endpoints
- ✓ Advanced threat analysis and hunting
- ✓ Automatic isolation and remediation

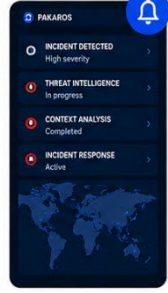




### Managed EDR

Detection and response delivered by PAKAROS.

- ✓ 24/7 monitoring by security experts
- ✓ Threat intelligence and contextual analysis
- ✓ Proactive incident management



#### YOUR BENEFITS

-  One view & control
-  Complete protection from endpoint to cloud
-  Faster detection and response
-  Lower costs through efficiency and scale
-  Reliable compliance and audit readiness
-  NL-based SOC with local experts
-  Continuous visibility & 24/7 monitoring



### AV + EDR + SIEM

Endpoint protection combined with central logging and full visibility.

- ✓ Complete log collection and correlation
- ✓ Real-time detection and alerts
- ✓ Full visibility across users, systems and cloud





### Managed SOC

Complete detection, monitoring and incident response by PAKAROS.

- ✓ 24/7 SOC service from the Netherlands
- ✓ Incident response and root cause analysis
- ✓ Reporting and continuous improvement



## Product matrix: functionality per module

The matrix below shows exactly what each module includes, built around four layers: protect, see, understand, and act. In the self-service modules AV+EDR and EDR+SIEM+SOAR, your own team or partner carries out certain tasks; in Managed EDR and Managed SOC, PAKAROS takes them over.

| Functionality                                  | AV + EDR | Managed EDR | EDR+SIEM+SOAR | Managed SOC |
|------------------------------------------------|----------|-------------|---------------|-------------|
| <b>PROTECT</b>                                 |          |             |               |             |
| Endpoint protection                            | ✓        | ✓           | ✓             | ✓           |
| Ransomware protection                          | ✓        | ✓           | ✓             | ✓           |
| Device isolation / containment                 | ✓        | ✓           | ✓             | ✓           |
| <b>SEE - LOGS &amp; MONITORING</b>             |          |             |               |             |
| European log storage                           | ✓        | ✓           | ✓             | ✓           |
| 90-day log retention                           | ✓        | ✓           | ✓             | ✓           |
| Identity logging                               | –        | –           | ✓             | ✓           |
| Cloud logging                                  | –        | –           | ✓             | ✓           |
| Network logging                                | –        | –           | ✓             | ✓           |
| <b>UNDERSTAND - CORRELATION &amp; ANALYSIS</b> |          |             |               |             |
| Event correlation                              | –        | ✓           | ✓             | ✓           |
| Threat Intelligence                            | –        | ✓           | ✓             | ✓           |
| User and Entity Behavior Analytics             | –        | –           | ✓             | ✓           |
| Incident Timeline                              | –        | ✓           | ✓             | ✓           |
| Breach reconstruction                          | –        | –           | ✓             | ✓           |
| Compliance Dashboard                           | ✓        | ✓           | ✓             | ✓           |
| Audit Trail                                    | ✓        | ✓           | ✓             | ✓           |
| <b>ACT - RESPONSE &amp; OPERATIONS</b>         |          |             |               |             |
| Threat Hunting                                 | Customer | Customer    | Customer      | ✓           |
| Incident Response                              | Customer | ✓           | Customer      | ✓           |
| Security Monitoring                            | Customer | ✓           | Customer      | ✓           |
| 24x7 Monitoring                                | Customer | ✓           | Customer      | ✓           |
| SOAR Playbooks                                 | –        | –           | ✓             | ✓           |
| Dedicated Security Team                        | –        | ✓           | –             | ✓           |
| Security Experts On Demand                     | *        | ✓           | *             | ✓           |

✓ included – not included Customer = carried out by your own team or partner \* available as an optional service

|                                                                              |                                                                                                    |                                                                                         |                                                                                                |
|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| <b>DATA IN EUROPE</b><br>Full processing and storage of your data in Europe. | <b>FULLY VISIBLE</b><br>From endpoints to identities, cloud, network, and OT, all in one platform. | <b>SMARTER AND FASTER</b><br>Correlation and automation bring the truth to the surface. | <b>AUDIT READY</b><br>With the PAKAROS SOC solution, you meet compliance requirements quickly. |
|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|

## What sets PAKAROS apart

- Visibility into AI tooling used within the organisation, a blind spot for most existing stacks.
- Visibility into unmanaged devices on the network, often where incidents begin unnoticed.
- The foundation PAKAROS uses has existed since 2019, making it a proven technology.
- Sovereign cloud as the foundation, not as an option.
- Predictable costs, no cloud consumption surprises.
- Incident response is built into Managed SOC, not a service booked separately. During an incident, the response extends beyond PAKAROS's own environment, into the customer's broader environment.
- Positioned as a team alongside your IT team, not as an external supplier reporting from a distance. Continuity is a shared responsibility, not an outsourced task.
- Board-accessible reporting: where most security platforms stop at analyst level, PAKAROS offers several reporting options that can be generated at any moment.
- Product development driven by customer demand, not by commercial motives.
- 525 standard integrations, for better performance, less maintenance, and faster threat detection.
- Maximum support, minimum investment

**PAKAROS is a valuable addition to the security team, with both technology and expertise**

## Fragmented approach versus PAKAROS

| Element                  | Fragmented approach                                         | PAKAROS approach                                                        |
|--------------------------|-------------------------------------------------------------|-------------------------------------------------------------------------|
| <b>Reporting</b>         | Technical, incidental, per tool                             | Fixed rhythm: monthly and quarterly, at board level                     |
| <b>Overview</b>          | Fragmented across separate dashboards                       | One coherent picture across endpoint, cloud, identity, and compliance   |
| <b>Responsibility</b>    | Held by separate vendors, or by nobody specifically         | PAKAROS as a team alongside your IT team, with fixed points of contact  |
| <b>Continuity</b>        | Dependent on a single system or vendor                      | Secured in an ongoing rhythm of monitoring, reporting, and response     |
| <b>Visibility</b>        | Limited to managed devices and known tools                  | Also covers unmanaged devices and AI tooling within the organisation    |
| <b>Infrastructure</b>    | Often US cloud providers                                    | Fully European infrastructure                                           |
| <b>Response time</b>     | Unstructured, dependent on who notices first                | Fixed service level: as agreed within the SLA or 9 hours (P3/P4)        |
| <b>Incident response</b> | Separate service, stops at the boundary of its own platform | Built into Managed SOC, extends into the customer's broader environment |

## Continuity as a starting point

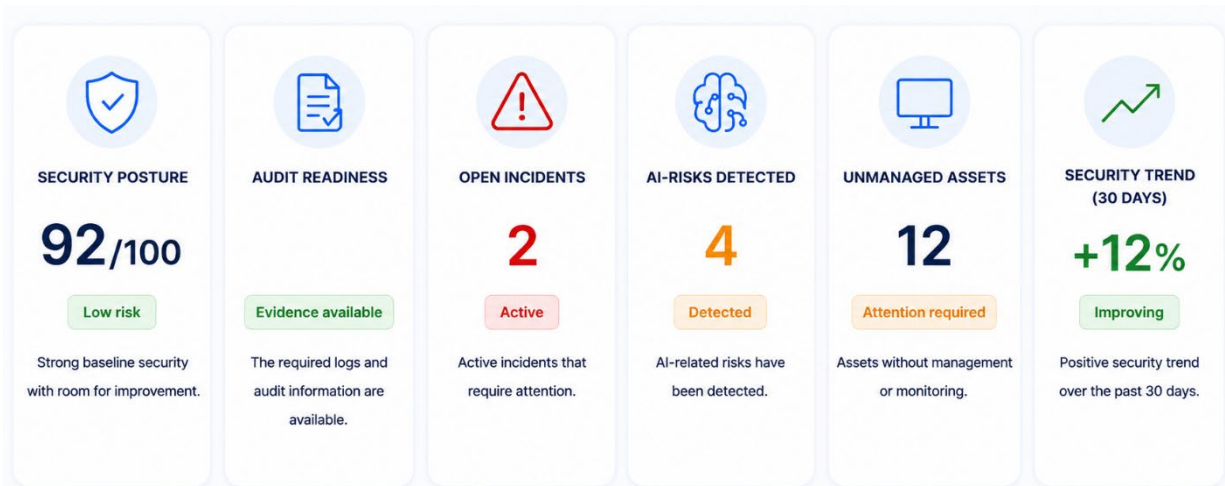
Calm and control start with continuity. PAKAROS is built on an ongoing rhythm of monitoring, reporting, and response, not on incidental interventions. That rhythm ensures continuity does not depend on a single system, a single person, or a single incident, but is structurally embedded in the collaboration.

- Continuous monitoring instead of periodic sampling, so deviations become visible early.
- Incident response built into Managed SOC, so response does not wait for a separate escalation or procurement process.
- A fixed reporting cycle that makes continuity demonstrable, instead of an annual snapshot.

## Reporting for every level

Continuity requires a fixed rhythm, not incidental reporting. PAKAROS builds in that rhythm and aligns with three levels within the organisation. On-demand reporting is always possible as well.

- Analyst level: technical dashboards with logs, detections, and response, for the team working in the details every day.
- Management level: aggregated reporting on trends, open risks, and progress on earlier recommendations.
- Board level: monthly reporting conversations on the current state of the environment, supplemented with quarterly deep-dives and concrete recommendations for the board.



## Compliance as a result, not a goal

Legislation such as the EU NIS2 Directive and ISO 27001 requires demonstrable technical measures and structural reporting, such as logging, monitoring, and response. PAKAROS is specifically built for this.

## What this means for you

You get one coherent picture instead of separate dashboards, and a fixed reporting rhythm instead of incidental updates. The board gets understandable reporting instead of technical logs. The organisation gets continuity that does not depend on a single standalone system, and your IT team gets a team alongside it, with incident response built in, instead of yet another supplier.

## Next step

Request a conversation. In a 45-minute conversation, we map out what PAKAROS can mean for you: where your organisation currently stands, and which challenges we can solve, or not. With our extensive experience in the security domain, we give practical advice on the possibilities. That is immediately useful, even if you don't move forward with PAKAROS.