

Operational Strategies for Preemptive Cyber Defense Across Industries

# MDR: What Matters Now Is **How** You Operate



**Byline Network**

SPECIAL REPORT | **USE CASE INSIGHTS**



# Contents

## PART 1.

---

<b>Why MDR?</b>	<b>02</b>
<b>Why MDR Is Needed Beyond Security Monitoring</b>	<b>04</b>
<b>Why PAGO MDR Is Designed Differently</b>	<b>06</b>

## PART 2.

---

### Industry Use Case Analysis

**11-23**

- Retail & E-commerce: How to Protect Customer Trust
- Manufacturing (Global OT Operations): Prepare for Threats Across Borders
- Food & Beverage (OT Environment): Small but Critical Warning Signs
- Healthcare & Pharma: If Regulations Cannot Be Avoided, Respond Preemptively
- Energy & Chemical: Protect Control Systems to Keep Industry Running
- Public & Finance (Overseas): Post-Ransomware Recovery and Strengthening Resilience

## PART 3.

---

<b>In MDR, the application matters more than the technology.</b>	<b>24</b>
--	-----------

## PART 1.

# Why MDR?

*Security manager A has been working at a major financial company for five years. His main responsibility is to monitor security events across the company's networks, servers, and endpoints, detect risks, and respond immediately. Over the past few years, the company increased its security investment by introducing SIEM for log management, EDR for endpoint detection and response, and IPS for intrusion prevention systems.*

*But as more systems were added, the number of alerts exploded. Unpatched ports, unauthorized access attempts, suspicious process executions, and abnormal overseas traffic overwhelmed his dashboard.*

*At first, he carefully reviewed every log and alert, but as the volume grew, it became impossible. Critical threats were buried, alerts piled up, and his team missed real attacks. One such oversight caused significant damage.*

Today's VUCA (Volatility, Uncertainty, Complexity, Ambiguity) threat environment, marked by volatility, AI-powered attackers, and night-time/holiday blind spots demands more than alert-centric detection. Security must be built on execution, not just monitoring. Analysts faced countless logs and alerts, often missing the truly critical threats.

Meanwhile, attacks became more advanced. Instead of simple brute force, adversaries now use AI to generate malicious payloads in real time, mimic legitimate behaviors, and hide through lateral movement. Security systems produce endless alerts automatically, but without prioritization, organizations waste time chasing noise while genuine threats slip through.

Most companies already own dozens of tools such as SIEM, EDR, SOAR, IAM, and CSPM. Yet many still fail to connect them into a unified system that prevents real damage.

## The Problem: Not Tools but How They Are Applied

It is no longer enough to own the latest tools. The key question is whether those tools are actually working together to stop attacks.

The focus must shift from simply detecting to fully operating. Security should be built on execution that connects detection, judgment, and action in one continuous flow.

This is the difference between MDR, which is Managed Detection and Response, and MSS, which is Managed Security Services. MSS mostly monitors and alerts. MDR goes further by detecting, analyzing, hunting, and even executing preemptive responses in real time. MDR ensures that even if an attack occurs at three in the morning, the system still responds instantly before analysts are awake.



## The Core Value of MDR

### CTEM (Continuous Threat Exposure Management): Designing for Prevention

Responding only after an attack occurs is no longer enough. CTEM emphasizes reducing exposure at the design stage so that attacks cannot reach our systems. For example, intelligence from StealthMole revealed leaked credentials, which DeepACT combined with ASM to close exposed assets blocking an intrusion before any alerts were triggered. Organizations should identify external vulnerabilities in advance through ASM, manage attack surfaces, detect leaked information with DRP, and run penetration testing to discover weaknesses before attackers exploit them.



MDR is not about outsourcing security tasks. Gartner defines MDR as “a strategic partner that reduces exposure and builds resilience by designing for preemptive defense.” The value comes not from adding more tools but from running them within an integrated security operations system.

### Real-time Detection and Response: Protection that Never Sleeps

Attackers no longer wait until business hours. Targeting after-hours systems is increasingly common. Security must automatically detect and respond at any time, within 24 hours, on holidays, and even during nights. This is now a baseline requirement.

### AI-driven Integrated Security: Seeing the Whole Picture

Enterprises often use multiple tools such as EDR, NDR, XDR, cloud security, and AI-driven SIEM. The problem is that each tool only provides a fragmented view. To respond effectively, organizations must unify all of these signals into a single, context-based picture.


### A Hybrid of Human Judgment and Automated Action: Fast and Accurate Decisions

Automation alone is not reliable, and human judgment alone is too slow. The ideal approach is a hybrid structure. Machines filter and correlate data, humans make final judgments, and automated systems instantly execute containment and response.

Unlike traditional models, MDR is designed around structure, not just technology. It is not a matter of owning the right tools, but of executing the right operational model. MDR builds a partner-driven ecosystem where prevention and execution are unified, not separated.

MDR is therefore not reactive security. The purpose is not only to detect and respond after an incident occurs but also to prevent attacks before they begin.

The demand for MDR is growing as organizations realize that detection without execution leaves them exposed. True MDR combines analyst expertise, automation, and structural design so that detection, judgment, and response are always connected.

In short, security must move beyond simply “working” toward “working as designed.” MDR offers the most effective structure to make that possible. 

**PART 1.**

# Why MDR Is Needed Beyond Security Monitoring

"We use well-known security programs like EDR, rely on external security companies for MSS, and yet we still keep experiencing incidents. Why does this happen? Which service is truly right for us?"

This is a common concern among security managers. The answer lies in the limitations of traditional MSS (Managed Security Services).

## MSS vs MDR: The Difference in Method Changes the Outcome

Many organizations have SOC (Security Operations Centers) or outsource monitoring to external providers. The purpose is to monitor the company's systems 24/7 and detect suspicious activities. However, most companies cannot operate a fully staffed SOC internally due to budget and expertise limitations. That is why they rely on MSSPs.

MSS focuses on monitoring and detecting events based on predefined rules. When anomalies are detected, alerts are sent to customers, who must then decide what action to take.

The problem is response time. Even if an alert is generated, a real attack can succeed while staff are still analyzing the situation, especially if the incident happens at night or during holidays.



Unlike MSS, which only alerts, MDR includes proactive response. The moment MDR detects a threat, it automatically isolates the suspicious file, cuts off the affected computer from the network, or locks the compromised account. Analysts investigate the incident in real time and refine detection rules so that future threats are contained more quickly.

MDR is built to function continuously, 24h a day, 7 days a week, all year round. Even when security staff are unavailable, MDR ensures that threats are blocked automatically.

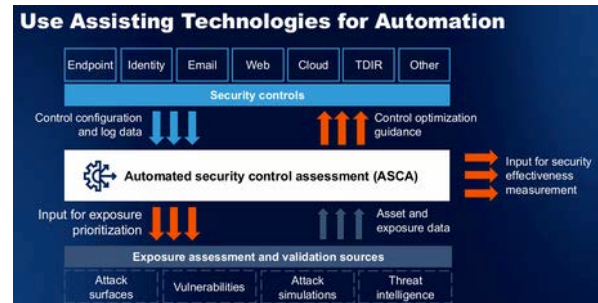
Category	MSS	MDR
Detection method	Rule-based, event matching	AI-driven, contextual analysis and threat hunting
Hours of operation	Often business hours 8x5 or partial 24/7	True 24/7/365
Response	Sends alerts, customer must act	Automatic preemptive response and containment
Depth of analysis	Fragmented event-based	Contextual, behavior-based
Automation	Manual response by customer	Automated end-to-end from detection to isolation
Customization	Limited	Industry-specific tailored detection and response



## Which MDR Is Right for Us?

There is no doubt MDR is needed. But finding a service that truly works as a security structure is not simple. The key to selecting the right MDR is verifying the following:

- Do they only send alerts, or do they actually contain and resolve threats before passing them on? If they only send alerts, they are no different from MSSPs. Real MDR must execute actions within the process.
- Do they truly operate around-the-clock? Check if they have both expert analysts and automated systems that run continuously, even at night and on weekends.
- Do they integrate multiple platforms? EDR, NDR, XDR, cloud security, identity protection, AI SIEM—are these correlated into a single picture to understand the full situation?
- Can they reduce exposure before an attack begins? Check whether ASM, PenTesting, or DRP are included as preventive functions.
- Do they provide industry-specific scenarios? Each sector such as healthcare, manufacturing, transportation, and finance faces different threats. Ensure the service adapts detection and response to your industry's environment.




## PAGO Case: The Power of a Service That Truly Works

PAGO's MDR is not just a collection of tools. It strategically integrates EPP, EDR, NDR, Open XDR, dark web intelligence, ASM, and PenTesting, with analysts interpreting and responding to incidents in real time.

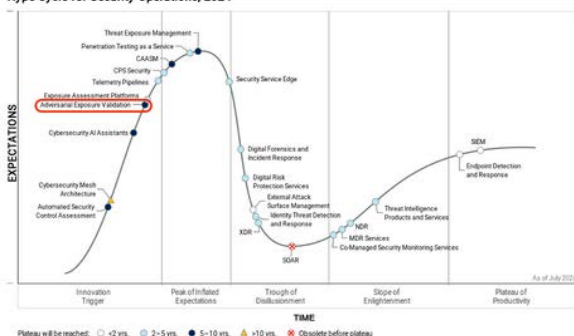
- Threat detection → Risk judgment → Immediate isolation → Real-time root cause analysis → Direct response → Results fed back into the system
- Because all these steps are connected through automation, analysts can focus on critical decisions while the system executes instant containment.
- PAGO currently protects more than 350 organizations across industries. Each scenario is tailored to match the client's unique threats, ensuring that MDR is not a one-size-fits-all service but a true operational model.

## The Core: Execution Matters More Than Tools

Detection is only part of the equation. The real challenge is how containment and response are carried out. Tools may look similar, but if they are not operationally integrated, they cannot prevent damage.

That is why the most important aspect is an MDR that operates as designed. Security must adapt to each organization's threat landscape and respond with a coherent, predesigned structure. 

Hype Cycle for Security Operations, 2024



## PART 1.

# Why PAGO MDR Is Designed Differently

PAGO has built a strategic security operations framework called PAGO DeepACT MDR as a Service Framework (PAGO DeepACT) to plan and execute all phases of defense before an attack begins, not after it ends.

The purpose of PAGO DeepACT is to create a partner-based structure where internal security experts can block attacks in real time and recover quickly even if incidents occur.

Most organizations already own multiple security tools, but they fail to function as intended. *DeepACT* consolidates these into a unified operating model, addressing skill shortages and tool sprawl, delivering enterprise-grade security without the overhead of building large internal teams.



## PAGO DeepACT: A Security System Designed on "Operation" Not Just Technology

PAGO DeepACT is not a single security product or a vendor tool. It is a system that strategically connects and manages all security technologies so that they operate as one. The key technologies deeply integrated with PAGO DeepACT are:

### SentinelOne: An AI-driven Security Platform Beyond Endpoints

Many MDR vendors use SentinelOne only as an endpoint defense tool. PAGO leverages SentinelOne as a comprehensive platform covering all digital assets across the company, including computers, cloud, employee accounts, and networks.

PAGO does not simply use SentinelOne as an endpoint tool. It strategically integrates SentinelOne with DeepACT to detect, isolate, and respond immediately to attacks in real time.

#### The Role of SentinelOne

- **Endpoint protection:** Detects attack patterns on all devices using behavioral analysis, not just rules.
- **Cloud-native protection:** Secures assets across multi-cloud environments, detecting abnormal programs or misconfigurations.
- **Identity protection:** Monitors employee account activity, prevents privilege escalation, and detects MFA bypass attempts.
- **AI SIEM:** Collects all security events across the company, correlates them, and detects threats without relying on traditional signatures.
- **Automation and Purple AI:** Executes responses automatically, while human analysts verify and refine outcomes. This human-in-the-loop design reduces false positives/negatives and ensures AI-driven actions remain explainable, accountable, and transparent.



## Stellar Cyber: AI-driven Integrated Analytics Hub (Open XDR)

PAGO uses Stellar Cyber as a core engine to reconstruct full attack flows. Stellar Cyber integrates all users, assets, policies, and events across the environment.

It provides real-time attack correlation, classifies threats by MITRE ATT&CK framework, and connects directly with DeepACT to trigger containment and response.

### The Role of Stellar Cyber

- **Open XDR Integration:** Integrates all security data from endpoints (EDR), network (NDR), log management (SIEM), firewalls, and identity (IAM) into one hub.
- **Attack Flow Analysis:** Goes beyond isolated events to connect activities across time, assets, and users, reconstructing the full attack flow.
- **AI-driven Threat Classification:** Uses frameworks like MITRE ATT&CK to classify threats, and machine learning to identify suspicious behavior. Especially effective for detecting subtle techniques such as living-off-the-land attacks or lateral movement.
- **PAGO DeepACT Integration:** Suspicious flows detected by Stellar Cyber are delivered to DeepACT in real time. Analysts verify whether these are real attack scenarios, and if needed, DeepACT triggers responses via SentinelOne or StealthMole.

This allows analysts to see not just “what event occurred,” but also “who, when, where, why, and how” the attack happened. Unlike MSS that only reports raw alerts, Stellar Cyber with DeepACT offers real context.

## StealthMole: Dark Web Intelligence

PAGO uses StealthMole to monitor from the attacker's perspective whether sensitive company information is leaked. If stolen information is detected, DeepACT automatically investigates the exposure with ASM, EDR, NDR, and Open XDR, then recommends remediation strategies.

### Role of StealthMole

- **Attacker activity tracking:** Detects hacking forum chatter, stolen data sold on botnets, and underground marketplaces.
- **Information verification:** Identifies leaked customer domains, employee IDs, sensitive data, source code, and API keys in real time.
- It is automatically registered in DeepACT and automatically generates new security rules.
- **Vulnerability remediation:** It is used to conduct additional investigations in connection with other systems such as Attack Surface Management (ASM), EDR, NDR, and Open XDR, and to remediate the vulnerable areas identified.

Through this structure, organizations can respond proactively to threats even before they actually occur.

## Aurora Protect: OT-Specific Security Agent

Aurora Protect is designed for OT (Operational Technology) environments such as factories, energy plants, and food production facilities. It detects and blocks threats targeting industrial systems.

### Role of Aurora Protect

- **ICS Network Protection:** Blocks intrusions aimed at industrial control systems.
- **Legacy OS Support:** Works on older systems still in use at factories, providing AI-driven security without requiring upgrades.
- **Integration with SentinelOne and Stellar Cyber:** Combines endpoint and network analytics with OT-specific scenarios to form a unified defense across the entire company.

### PAGO DeepACT: The Core of Judgment and Execution

Over nine years of MDR service experience have been built into DeepACT. It ensures security strategies are not just planned but actually executed.

#### Role of DeepACT

- **Detection event normalization, priority scoring, and threat context analysis:** Collects and organizes numerous security alerts, then prioritizes them to identify which threats are more critical.
- **Automated response scenario recommendations for analysts:** When a threat is detected, it suggests the most effective response actions so that security experts can act immediately.
- **Proactive threat hunting:** Continuously updates the detection engineering engine and applies it across all security technologies to actively uncover unknown threats.

- **AI-driven rule recommendations for IOC/IOA redesign:** Uses AI to automatically propose and apply new security rules tailored to emerging threat patterns.
- **End-to-end workflow integration (Detection → Decision → Containment → Analysis → Reporting):** Every stage of incident handling is seamlessly executed within PAGO DeepACT.
- **Complete integration of the AI security stack:** Endpoint protection (EPP, EDR), network security (NDR), cloud security, identity security, unified analytics (Open XDR, SIEM), and automation all interconnect and operate as one system inside PAGO DeepACT.
- **Unified operation of preventive security layers:** Identifies potential attack surfaces through ASM, tests organizational defenses through penetration testing, and leverages dark web intelligence (StealthMole) for DRP to detect threats in advance - all managed inside PAGO DeepACT before an attack can occur.

PAGO DeepACT is not simply a tool for "automation." It systematizes security decisions and execution, ensuring the organization's defenses remain active even during normal times without incidents. The true measure of security is not only whether you have good detection technology, but whether that technology can operate effectively to actually prevent real incidents.

### Real-world cases where PAGO DeepACT blocked attacks

The unique operational approach built on PAGO DeepACT vividly demonstrates the remarkable results it has delivered in the field.



## Manufacturing customer

Detected suspicious communication between IT systems and factory equipment (OT) early, successfully preventing internal movement into industrial control systems (ICS) at the initial stage.



## Retail company

Quickly identified attempts to hijack accounts in POS and CRM systems, blocking data breaches before customer information could be exposed.



## Healthcare & Pharmaceutical customer

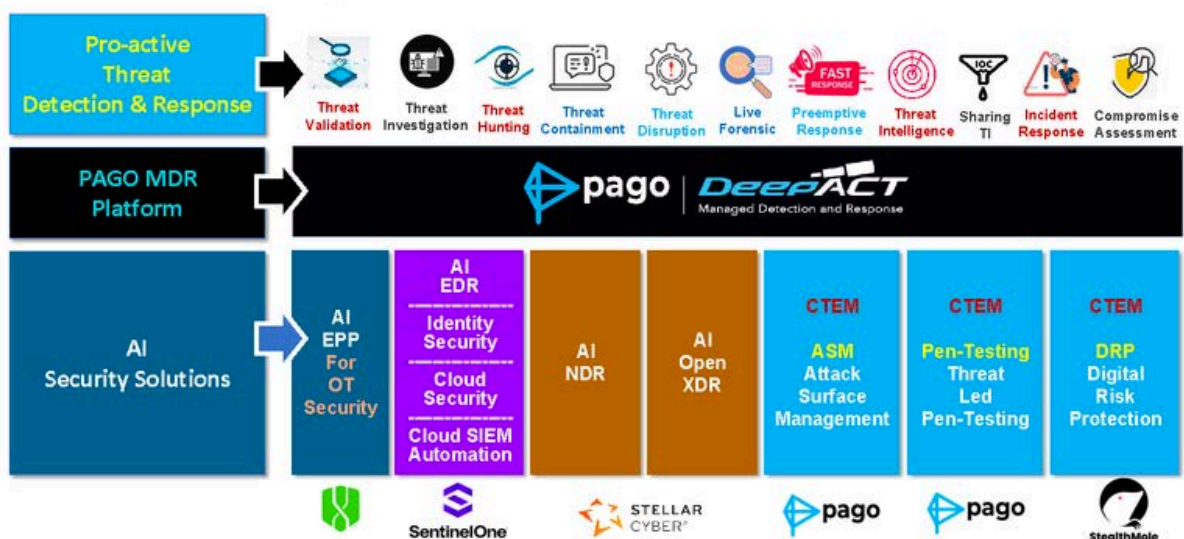
Detected attempts to escalate employee account privileges, stopping potential leaks of sensitive personal information and regulatory violations.

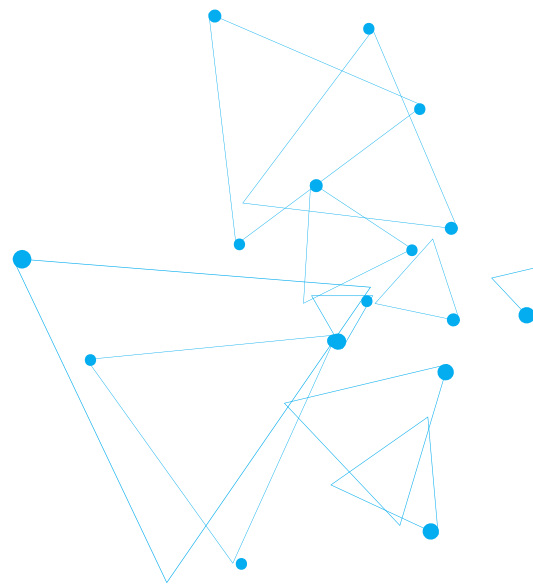
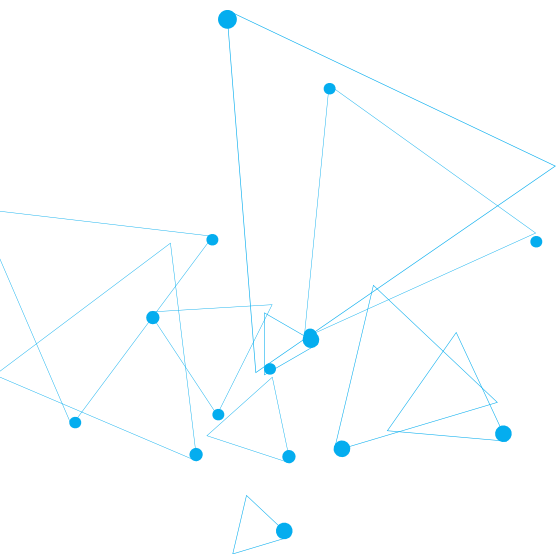


## Public sector and financial institutions

When ransomware infiltrated, PAGO DeepACT immediately isolated affected systems, analyzed root causes, and even led the redesign of systems during recovery, enabling rapid restoration of operations. <sup>BN</sup>

## PAGO DeepACT MDR-as-a-Service Framework





# USE CASE INSIGHTS



Introducing real-world cases where PAGO DeepACT MDR service was applied across 6 industries.



12-13

---

**Retail & E-commerce:**  
How to Protect Customer Trust



14-15

---

**Manufacturing (Global OT Operations):**  
Preparing for Threats Across Borders



16-17

---

**Food & Beverage (OT Environment):**  
Small but Critical Warning Signs



18-19

---

**Healthcare & Pharma:**  
If Regulations Cannot Be Avoided, Respond Preemptively



20-21

---

**Energy & Chemical:**  
Protect Control Systems to Keep Industry Running



22-23

---

**Public Sector & Finance (Overseas):**  
Post-Ransomware Recovery and Strengthening Resilience

## Retail &amp; E-commerce

# How PAGO Protects Customer Trust

## How Mid-sized Retail Company A Overcame a Customer Data Breach Threat

### INDUSTRIAL CASE SUMMARY



#### Pain Point

Retailer A, with over 300 stores nationwide, connected store POS systems to headquarters with a very weak VPN. On top of this, traces appeared on the dark web showing some CRM accounts had been leaked, creating a major crisis of possible customer data exposure.

#### PAGO's Solution

PAGO installed the advanced AI security program (SentinelOne) on store POS, and activated a structure that analyzed threat detection events in real time through PAGO DeepACT. At the same time, the dark web monitoring solution (StealthMole) was used to precisely confirm the scope of CRM data leaks. In addition, the integrated security analysis system (Open XDR) detected and tracked suspicious logins made with the leaked accounts.

#### Implementation Effect

As PAGO DeepACT operated, within 24 hours the infiltrated accounts were found and isolated. Although there was a serious risk of a massive customer database leak, it was successfully prevented. A gained very high ROI since instead of replacing existing security systems, it added an "operational system that blocks threats."

### Security Threats Most Common in Retail and E-Commerce

Through work with retail and e-commerce firms in Korea and across Asia, PAGO has identified the following main threats:

- **Customer data leaks:** exposure of sensitive customer information
- **Application vulnerability attacks:** external attacks exploiting weaknesses created by many connected apps
- **Supply chain attacks:** intrusions through partner companies or service providers we work with
- **Ransomware attacks:** disabling core service systems or store POS systems while demanding payment

### Security Solutions, Investments Are High but...

Retail and e-commerce companies that handle customer data have invested heavily in security. They have continuously deployed DLP, vulnerability management, VPN, and DRM solutions.

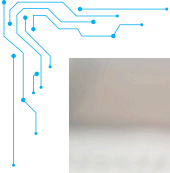
Yet these critical solutions are not connected and operate separately. For example, DRM or DLP is used only for blocking data leaks, while endpoint security on POS is used only for ransomware defense. In other words, companies tend to focus too much on the performance of each individual solution.

As the number of separate solutions increases, companies rely more on reseller technical support to manage them. But technical support for solutions is different from detecting and responding to threats. To fill this gap, some companies build their own SOC, or if staff is lacking, outsource monitoring to external providers.

### PAGO's Diagnosis of Retail & E-Commerce Security Operations

Retail and e-commerce customers placed their security solutions properly. But they lacked metrics or processes to see how those solutions connected. Most work focused only on detection events from each solution, and reports were simple counts like "X number of security events occurred."





When one solution detected a threat, there was no system to integrate data from others for investigation and response. Since most customers relied only on solution events, they could not clearly know if no events meant no threats, or if the solutions had errors. Modern attacks are connected across stages such as reconnaissance, infiltration, spread, data leak, and destruction. So each event must be further analyzed with the context of who, when, where, why, how, and what. For this, information from other solutions must also be included, but very few customers had such a process. Their security solutions ran separately, with no correlation.

### PAGO MDR Approach

Retail and e-commerce firms run frequent marketing activities, so they use many cloud systems. They also create and shut down new web services and apps often, which exposes many internet-facing weaknesses. Offline retailers are also vulnerable since POS, Wi-Fi, and order systems are physically exposed. PAGO assumes “threats can easily penetrate” and offers realistic defense measures tailored to retail.

### AI Endpoint Security Stack Proposal

The final place threats act is endpoints like user computers, POS terminals, and servers in data centers or cloud. PAGO proposes an AI-based endpoint detection and response (EDR) system optimized here. This EDR is not just one function. It provides extra investigation when events occur, links threat intelligence, correlates user, process, and network behavior, supports threat hunting, and enables custom rule settings. It covers file-based, fileless, and behavior-based attacks, serving as a system security experts can use effectively.

### AI NDR and Open XDR Security Stack Proposal

When NDR directly correlates and analyzes events from key systems such as AD, firewalls, and VPN, the ability to understand threat flows becomes much stronger. When AI EDR works together with AI NDR and Open XDR, the effect grows dramatically.

### Continuous Threat Exposure Management (CTEM) Security Stack

Retail and e-commerce firms use many cloud-based development systems, which means many areas are exposed to the internet. Because infrastructure changes constantly, it is important to always check which applications or services are externally exposed. PAGO considers this and proposes Attack Surface Management (ASM) to automatically find and manage exposed systems, DRP/Dark Web Intelligence to check if data is already leaked, and scenario-based Threat-Led Penetration Testing (TLPT) on exposed assets.

### Expert-Led, Automated Threat Detection and Response

PAGO provides advanced security technologies and a service methodology to run them effectively. Alerts are verified and root causes analyzed, while continuous threat hunting uncovers unknown threats even when no alerts appear. In response, PAGO works with customer teams, and in urgent cases its MDR team leads the first action. Though incidents may seem separate, threats are interconnected. Simply running individual systems is not enough, so PAGO helps customers build processes and systems that respond to real threats. **BN**

## Manufacturing (Global OT Operations)

# Preparing for Threats Across Borders

## Case of Blocking OT Intrusion and Achieving Global Integrated Detection at Electronics Manufacturer B

### INDUSTRIAL CASE SUMMARY



#### Pain Point

Electronics manufacturer B, operating global branches, suffered an account takeover of an IT system administrator at its Vietnam plant. The attacker then moved into the OT equipment network, showing lateral movement signs and causing system failures. The existing security setup only raised partial system alerts, without showing the full attack flow, and could not prepare against the intrusion.

#### PAGO's Solution

PAGO immediately deployed the integrated analysis hub (Stellar Cyber Open XDR) in IT and OT, analyzing distributed traffic from Vietnam, India, and Korea headquarters. Unauthorized access, malware downloads, internal scanning, port misuse, and reuse of valid commands after account theft were automatically correlated into scenarios and visualized. These were passed to PAGO DeepACT to connect the full process of detection, isolation, and forensics. On OT devices, Aurora Protect EPP was applied to legacy OS and SentinelOne EDR to modern OS, blocking spread without harming equipment availability.

#### Implementation Effect

The attacker tried to dominate the internal network by bypassing detection with stolen admin rights. But Stellar Cyber NDR and Open XDR correlation identified the attack flow in real time, and factory-level isolation stopped further spread. In addition, AI EPP/EDR was deployed to OT production networks, handling both infiltrated threats and abnormal endpoint behavior. Company-wide detection policies were then distributed through PAGO DeepACT. A unified MDR environment with consistent detection and response standards was established across global branches.

## Security Threats Commonly Faced by Manufacturers

PAGO MDR customers in manufacturing are spread across Korea, ASEAN, China, North America, and Europe. Though geographically distant and culturally different, they show common patterns of threat cases.

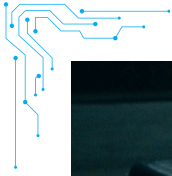
- **Shared major accounts:** administrator accounts shared internally and externally, leading to leaks
- **IT to OT connectivity threats:** intrusions into OT through IT networks
- **Non-isolated OT environments:** risks from OT environments already accessible by multiple routes
- **Ransomware attacks:** shutdown of production networks, with encryption and destruction of IT data needed for manufacturing

## Reality of Security Investment in Manufacturing

Manufacturers assign highest priority to production and sales. IT and cybersecurity are treated as support units for revenue departments. When cost-cutting is needed, security investment is pushed back. Even firms hit by major incidents often blame the security team rather than strengthen investment. After response, cybersecurity usually returns to its support role.

Investment in OT production networks remains focused on availability and production activity. In small, mid-sized, and even large enterprises, the level is weak, often no stronger than tolerating exposure.

With growing incidents, awareness of security investment in manufacturing is slowly improving, expanding from IT to OT.



Still, with investment focused on availability, it is difficult to defend efficiently against advanced threats. Basic network, email, and endpoint security exist only at a “we have security solutions” level. DRM and DLP for sharing data with vendors work only at a “our data is safe” perception level. VPN accounts shared with partners carry only the meaning “vendors can access us only through VPN.”

Looking at recent attacks on small and mid-sized firms, the end result was ransomware and data theft, but the start was first account compromise of weak infrastructure systems. The clear attacker goal was to gain second-level accounts with admin rights and create new ones to reach more critical systems. IT network damage indirectly affects OT production. Global OT networks, especially, often run security in their own way instead of following HQ policy.

Among PAGO MDR customers, there have been cases where overseas IT breaches damaged domestic IT and OT, and cases where differing global policies blocked joint response. Attackers can even use methods that have worked for decades to gather initial information. Malware distribution, brute-force, phishing, and backdoors via remote shells are typical. These are not new threats. The reality is that even such basic attack forms are breaking into the security of small and mid-sized firms and reaching their infrastructure with ease.

### **PAGO MDR Approach**

It is necessary to decide whether to solve these issues with security solutions or with operations, and find the most practical option. Compared to the fast-changing level of attacker threats, small, mid-sized, and even

some enterprise manufacturers have been slow to invest in security. Rapid, large-scale solution deployment in a short time is unrealistic. PAGO sees MDR as the best alternative now, bringing efficient results, guiding security investment, and applying methods to better detect and respond to advanced threats.

#### **• People**

The hardest part for manufacturers is expert staff. PAGO MDR’s expert-driven, automated detection and response service directly supports this challenge.


#### **• Technology stack**

Steps include:

1. Find and respond to threats already inside the company
2. Detect and block attempts to infiltrate
3. Detect and respond to threats using account theft as normal access
4. Build an OT security stack aligned with IT levels
5. Assess infrastructure from an external attacker view and propose countermeasures

This stack includes AI EDR, NDR, Open XDR, ASM, DRP, and PenTest, run by experts on automated platforms.

#### **• MDR Operations**

Manufacturers usually have HQ, factories, labs, and offices, often minimally separated or globally dispersed. PAGO MDR uses cloud-based AI, expert skills, automation, and nonstop services to deliver optimized detection and response. It also offsets limited staff and skills, while guaranteeing support for production and research sites in distant locations. 

## Food &amp; Beverage (OT Environment)

# Small but Critical Warning Signs

## Case of Anomaly Detection and OT Network Defense at Food Manufacturer C

### INDUSTRIAL CASE SUMMARY

#### Pain Point

Mid-sized food manufacturer C, during smart factory transition, faced repeated small errors in automated equipment and abnormal API calls in the ERP system. The IT-OT link area was a blind spot, and it was hard to judge incidents from single events.

#### PAGO's Solution

PAGO applied the Stellar Cyber Open XDR platform as the core. It precisely collected network flows in the production network and automatically analyzed correlations of abnormal behaviors disguised as normal. It identified threats in advance through behavior-based detection such as delayed control responses from equipment receiving external commands, and executed automated playbooks via PAGO DeepACT. SentinelOne EDR was used to block processes at the endpoint level and for additional threat investigation and hunting. Aurora Protect, a lightweight OT EPP agent, was stably applied to critical field equipment sensitive to system performance.

#### Implementation Effect

Attackers attempted to distort ERP - production equipment control commands with malicious scripts, but Stellar Cyber's L3-L7 correlation analysis detected and blocked the disguised threat. PAGO DeepACT completed cause analysis, investigation, and real-time response without halting operations, and established a recurrence prevention system by reflecting automatic rules for similar flows, together 24/7 service.

## Security Threats in the Food and Beverage Industry

The end customers of food and beverage manufacturers are individual consumers. This creates different security needs and compliance areas compared to hardware-based general manufacturers. The industry is connected not only to production, sales, and marketing but also to retail and distribution. It faces supply chain issues unique to this sector, and with growing reliance on automation, it has become a new target for cyberattacks.

The main threats to the food and beverage industry are:

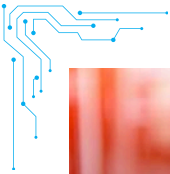
- **Smart factory vulnerabilities:** increased external connection points and weaknesses due to factory automation and modernization

- **Supply chain threats:** rising risks linked to complex food ingredient supply chains
- **Data integrity risks in production:** threats of direct data manipulation that affect human health
- **Ransomware attacks:** shutdown of production networks and encryption or destruction of IT data required for operations

## Security investment by food and beverage manufacturers

As the food and beverage industry moves toward smart factories, cybersecurity investment is being newly defined. Yet many systems still run on old OS versions no longer supported. Since traditional distribution systems and production processes were mostly designed for availability, it is now necessary to build security that considers both legacy and smart environments together.





A key characteristic is that production, sales, and distribution each operate separately while maintaining close connections. From an IT viewpoint, these areas must be optimally linked to run the best possible security framework.

### PAGO's Assessment of Security Systems in Food and Beverage Manufacturing

Recently, IT systems in the food and beverage sector place higher priority on compliance than on applying practical security or finding optimal operations. They often respond to audits before building full security systems. PAGO's clients also start with audit response but soon discuss real threat detection and response. This is only possible if management shows strong commitment to security investment. Awareness of security investment is improving, with scope expanding from IT into OT. In smart factories, companies often secure IT availability first, then design cybersecurity.

In IT, endpoint, network, data, and system security are usually in place. In OT, investment is almost absent. Even in IT, tools are built separately, without integration or joint operation. To face AI-driven threats, IT and OT must be approached together, solutions interconnected, and optimal methods applied.



### PAGO's MDR Approach

For food and beverage companies, PAGO presents its MDR model as a way to maintain compliance-level security while also countering advanced threats. It covers both IT and OT security and provides top-level PAGO MDR analyst expertise to customers with limited staff.

#### • People

The hardest part for manufacturers is investing in expert staff. PAGO MDR's expert-driven, automated detection and response service addresses this real difficulty.

#### • Technology stack

The MDR stack includes AI EDR, NDR, Open XDR, ASM, DRP, and PenTest, supported by expert operations and automated platforms. For OT, AI EPP is applied to legacy (end-of-support) OS systems, and AI EDR to newer OS and systems, under one common method to deliver advanced SOC capabilities. With many rapidly developed service applications and new development servers, attack surface management is also proposed. NDR and Open XDR are not separated by IT or OT use but applied flexibly to cover both.

#### • MDR Operations

Like other manufacturers, food and beverage firms have HQs, factories, labs, and offices, often minimally segmented or globally dispersed. PAGO MDR uses cloud-based AI, expert skills, automation, and around-the-clock services to deliver optimized detection and response. It also offsets customer limits in staff and skills while supporting geographically distant production and research sites. **BN**

## Healthcare &amp; Pharma

# If Regulations Cannot Be Avoided, Respond Preemptively

## Case of Strengthening Regulatory Response at Hospital D Operating a Medical Imaging AI Service

### INDUSTRIAL CASE SUMMARY



#### Pain Point

Hospital D introduced a cloud-based medical imaging AI diagnostic system, but it had to comply with both HIPAA in the US and Korea's Personal Information Protection Act. Although multiple security solutions were in place, there was no structure for real-time detection or regulatory response.

#### PAGO's Solution

PAGO applied Stellar Cyber NDR and Open XDR to detect network traffic threats in the hospital network connected to the cloud. All endpoint systems were protected with SentinelOne EDR. Threat monitoring and analysis of every event accessing the AI diagnostic system were continuously performed with PAGO DeepACT. To prevent external leakage of diagnostic images, StealthMole dark web intelligence monitoring was applied, and regulatory documentation was automated to streamline audit responses.

#### Implementation Effect

Response time to medical device certification and data access audit requests was reduced from five days to one. Audit compliance rate improved to 100 percent. The hospital management reset its internal security KPI from "audit pass" to "trust built on security."

### Security Threats in Healthcare and Medical Industry

Awareness of cybersecurity in healthcare and pharmaceutical industries is rising. Factors include poor security policies in legacy medical devices, ransomware attacks, cloud adoption, digital transformation, and expanded connectivity of equipment.

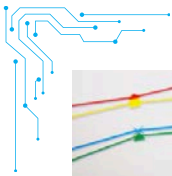
Because these industries hold large amounts of critical data, compliance issues are significant. As a result, they face strong pressure in regulatory response and must strengthen security standards across medical and research systems and documents. Since attacks mainly target critical systems or data, the impact of incidents is very high. Key cyber threats observed in PAGO MDR healthcare customers include:

- **Ransomware:** system paralysis, disruption of patient care
- **Data theft:** leakage of critical medical data, research data, patient data
- **Medical device vulnerabilities:** remote monitoring and control of patient devices, data exfiltration

### Security Solution and Investment in Healthcare and Pharmaceutical Companies

Healthcare and pharmaceutical industries prioritize R&D and workforce, while also applying various security solutions mainly for compliance. Yet security is often implemented at a checklist level, focused more on compliance than on actual threat defense.





To block advanced attacks, they must secure proper use of AI security stacks, skilled security staff and analysts, real-time detection and response, and frameworks that protect IT, medical, and research systems together. But since business investment comes first, it is hard to create a fully ideal environment. Many companies therefore adopt security solutions as urgent compliance measures.

Realistic challenges include lack of methods to protect both legacy and modern systems, limits of compliance-only measures, and difficulty proving ROI. Executives are usually medical or research experts, which also limits investment decisions. Today many hospital and research devices connect directly to doctors' and nurses' PCs and IT systems. As more devices link to internal and external networks, cyber risks grow fast. It is time to change the current investment model and prepare for future threats. Home healthcare devices, cloud AI diagnostic systems, and mobile health monitoring are now inseparable from cybersecurity.

### Security Solution Operations in Healthcare and Pharmaceutical Companies

Awareness of security investment is gradually improving, but because many cases focus on compliance, operations are also shaped around compliance. Examples include report-centered practices, treating security events simply as issues to be closed, reducing failed login attempts, recording critical data access, storing all system events, and keeping original data. There is demand for continuous improvement in detection and response against advanced threats,

but challenges remain due to lack of specialized solutions, absence of proper deployment, and limited staff that prevent true real-time operations.

### PAGO's MDR Approach

#### • People

The hardest area for healthcare and pharmaceutical firms to invest in is skilled experts. PAGO MDR's expert-driven and automated detection and response services directly support these real challenges.

#### • Technology stack

The platform simultaneously supports AI EDR, NDR, Open XDR, ASM, DRP, and PenTest for IT, R&D, and medical device cybersecurity, run by experts on an automated base. For medical devices, PAGO jointly applies OT-specialized AI EPP for legacy (end-of-support) OS systems and AI EDR for modern OS and systems, using the same methodology to strengthen SOC capabilities. NDR and Open XDR are applied flexibly as AI-based technologies that cover both IT and OT without dividing them.

#### • MDR Operations

PAGO MDR provides optimized services and methodologies through cloud-based AI technology, expert capability, automation, and uninterrupted service coverage. It offsets limited customer staff and resources, while guaranteeing structured support for geographically dispersed research and production sites. It also actively shares threat intelligence specific to healthcare and pharmaceutical industries, and raises security maturity through continuous threat hunting even when no incidents are present. **BN**

**Energy & Chemical**

# Protect Control Systems to Keep Industry Running

## Preventing a Cyber Incident in the Facility Control Network of Chemical Company E's Industrial Complex

### INDUSTRIAL CASE SUMMARY



#### Pain Point

Mid-sized Chemical Company E operated OT facilities in a closed network structure. However, malware was introduced through USB update tools, and malicious code and suspicious traffic also continued to appear through access by external maintenance partners. Internally, there was a SIEM, but it only integrated threats detected by existing security solutions. The company had no alert system for threats disguised as normal activity and lacked behavior-based analysis or isolation capabilities.

#### PAGO's Solution

PAGO integrated Stellar Cyber NDR and Open XDR correlation flow analysis with SentinelOne EDR, then analyzed the attacker's lateral movement within PAGO DeepACT. In addition, Aurora Protect EPP was urgently deployed on OT terminals running end-of-support legacy operating systems, completing isolation, recovery, and rule feedback within four hours.

#### Implementation Effect

Threats were removed without disrupting operations, and USB-based vulnerabilities were reflected in the rule set, automating recurrence prevention. Company E expanded from SIEM-centered event collection and manual response analysis to a dynamic response framework powered by PAGO DeepACT. This case demonstrates layered detection and response at OT connection points and external access channels.

### Key Security Threats in the Energy and Chemical Industry

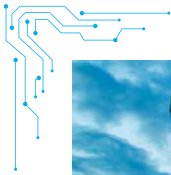
PAGO MDR customers in energy and chemical industries are located not only in Korea but also in ASEAN countries such as Malaysia, Indonesia, and the Philippines, as well as in China, Europe, and North America. Each customer has implemented IT and OT MDR. Most are mid-sized or large enterprises, and show similarities in adoption background and system/network architecture. Main threats include:

- OT production network DDoS attacks disguised as ransomware
- Annual shifts in attack methods
- Ongoing external scanning attacks
- Data leaks through third-party supply chain hacks
- Phishing emails impersonating executives or departments (malicious attachments, malicious links)

Especially, many attacks aim to destroy or paralyze OT manufacturing networks, with continuous infiltration of malware variants. Infection paths vary: brute-force attacks, distributed scans for open ports/services/applications, SMB vulnerability exploits, USB media spread, malicious activity via VPN tunnels shared with partners, and malware embedded in original or OS backup images.

Because company size is larger than in other industries, energy and chemical firms budget for regular penetration tests and security checks. Often, security tools, hacking tools, or check scripts used in tests remain undeleted. Attackers who infiltrate can use them immediately. Security checks thus become a threat factor.

Also, during regular tests, existing policies or solutions are often disabled to avoid interference. This repeated disabling for accurate reports is itself a problem.



## Reality of Security Solution Investment in Energy and Chemical Companies

In the energy and chemical industry, companies generally invest well in security solutions due to their size. However, investments are made by individual domains, and projects like SIEM are carried out to integrate each area. Endpoint, network, email, system, and data security are established, but SIEM projects are pursued in the name of integrated detection and response. Yet SIEM projects, which gather events from all security solutions, are not easy to turn into effective detection and response processes.

Mid-sized and large enterprises mainly rely on outsourced SOC. These SOC providers deliver managed services by each security solution, such as managed firewalls, managed IPS, managed endpoint services, and reporting. Such services are generally based on events from each system. If no events occur, additional detection and response services like threat hunting are not provided. Their top priority is maximizing system availability, which creates blind spots in detection and response and makes it difficult to apply urgent new policies. SOC outsourcing is often outsourced again at the major vendor level, showing that SOC providers are not composed only of highly skilled analysts.



## PAGO's MDR Approach

PAGO proposes applying MDR to the energy and chemical industry by keeping existing SOC outsourcing while adding specialized services for detection and response. This is not a replacement but a hybrid model that strengthens response capabilities for customers.


### • People

PAGO MDR provides expert analysts who can be maintained as essential SOC staff, delivering threat detection and response with sustainable expertise to address customers' real pain points.

### • Technology stack

AI EPP/EDR, NDR, Open XDR, ASM, DRP, and PenTest support both IT and OT simultaneously, operated by experts on an automated platform. For OT, AI EPP is applied to legacy (end-of-support) OS systems and AI EDR to modern OS and systems, with a unified methodology to strengthen SOC capability. NDR and Open XDR are applied as AI-based stacks that flexibly expand to cover both IT and OT without strict separation.

### • MDR Operations

PAGO MDR delivers optimized detection and response through cloud-based AI technology, expert capability, automation, and 24h service. This covers limited customer staff and supports globally distributed OT networks in a structured way. It actively shares threat intelligence within the industry and provides ongoing threat hunting even without active incidents, raising security levels. Ultimately, it operates in close cooperation with existing SOC outsourcing, and already provides systematic and stable MDR service to many customers. 

**Public Sector & Finance (Overseas)**

# Post-Ransomware Recovery and Strengthening Resilience

## ASEAN Government Agency F: Ransomware Response and Recovery INDUSTRIAL CASE SUMMARY

### Pain Point

ASEAN Government Agency F, which manages a public database linked to regional transportation systems, experienced a ransomware incident that led from temporary system paralysis to attacker ransom demands. Distributed backup systems across key regions were also infected, causing significant delays in recovery, while the added pressure of responding to external audits further intensified the crisis.

### PAGO's Solution

At the onset, PAGO rapidly collected Indicators of Compromise (IOCs) and extended forensics to both infected and non-infected systems, while also tracking dark web sources to uncover ongoing Indicators of Attack (IOAs). It then deployed Stellar Cyber NDR/Open XDR across headquarters and key regions, rolled out SentinelOne EDR company-wide, and used Attack Surface Management (ASM) to eliminate exposed assets and update threat-hunting rules. All response routines were automated through PAGO DeepACT.

### Implementation Effect

Although a second wave of attacks was attempted, it was successfully blocked, enabling full recovery without secondary infections. With the introduction of an MDR analyst-driven response system, a 24x7 threat response routine became operational. Two similar attacks were later preemptively blocked, and the agency earned the highest rating in the national cyber resilience assessment. This case demonstrates how critical threats can be transformed into long-term cyber resilience.

## Key Security Threats in Public and Financial Sectors

Cyber threats targeting public and financial institutions often have clearer objectives and cover wider, critical areas. These include threats against national infrastructure, social infrastructure, and even cross-border attacks.

Case studies of PAGO MDR adoption in these sectors are largely tied to targeted ransomware incidents, such as attacks on entire datacenter servers, transportation infrastructure, Active Directory servers, and core control systems. Many organizations first engaged PAGO through ransomware incident response and then continued with MDR to strengthen cyber resilience and address persistent threats.

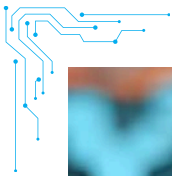
## PAGO's Ransomware Response Proposal for Public and Financial Institutions

When ransomware occurs, organizations typically focus on recovery through backup data. Public and financial institutions are no exception, but recovery can be disrupted by additional incidents unfolding elsewhere in the infrastructure.

To counter this, PAGO MDR recommends parallel actions:

- Restore services using backup data
- Conduct forensics on affected systems and extract IOCs
- Deploy the PAGO MDR technology stack (AI-EDR, NDR, Open XDR) to detect malware and malicious behavior even in unaffected systems





- Perform Attack Surface Management (ASM) to identify externally exposed assets and define actionable countermeasures
- Use dark web intelligence to monitor leaked customer data, track attacker-tagged system or network information, and collect additional IOCs
- Conduct further threat investigations based on newly acquired dark web intelligence

During recovery, PAGO MDR performed forensic analysis, extracted IOCs, and proposed response measures. It identified and removed malware and malicious behavior that had spread inside the infrastructure, and mitigated unnecessary exposure such as open applications, services, and ports. Dark web monitoring was also conducted for leaked customer data.

Following containment, PAGO MDR deployed its full methodology, extending AI-EPP/EDR, NDR, Open XDR, ASM, DRP, and PenTest capabilities across the infrastructure.



## PAGO MDR Approach

With PAGO MDR, public and financial institutions gain access to nonstop managed detection and response. The service continuously detects, defends, and responds to threats while maintaining close communication with customers to reduce risks. When required, PAGO also provides containment, live forensics, and proactive countermeasures with customer consent.

### • MDR Expertise

PAGO MDR supplies professional analysts as an extension of the customer SOC, ensuring continuity in threat detection and response, and addressing real-world staffing challenges.

### • MDR Operations

Leveraging cloud-based AI, expert skills, automation, and a uninterrupted service model, PAGO MDR optimizes threat detection and response. It compensates for limited internal resources, actively shares industry threat intelligence, and delivers ongoing threat-hunting services even when no live incident is present, thereby continuously raising the security baseline. **BN**

**PART 3.**

# In MDR, the application matters more than the technology.

“We have all the latest security tools, so why do we still keep getting breached?”

EDR, NDR, XDR, cloud security, identity security, SOAR, SIEM, AI detection, automation... New security technologies keep appearing, yet incidents and damages continue.

Why?

Because the real key is not what technologies you have, but how you connect them and make them work together. That is why companies must focus less on the technology itself and more on its application and operation.

Today's enterprise security environment is extremely complex. Internal systems and cloud, internal networks and external partners, countless user accounts and devices, humans and AI. Attackers are becoming smarter and faster at all of these boundaries. They also use AI. They disguise themselves as normal logins, bypass MFA, and steal privileged accounts with new tactics. They often strike when security staff are away, at night, on weekends, and during holidays.

Inside companies, there are many security tools, but they work in silos. They fail to show the full threat flow. Alerts keep going off, but it is unclear which ones really matter, and taking real action is even harder. This is the reality many companies face.

## The limits of MSS, the fatigue of SOC, and the need for MDR

Many companies outsource their security operations to reduce the burden of running a SOC in house. Most MSS offerings stop at detection. They spot suspicious activity based on preset rules and send alerts, but the judgment and action are left to the customer. Most of these services also focus on daytime working hours. That is why major incidents often occur late at night, on weekends, or during long holidays.

MDR, which stands for Managed Detection and Response, was created to close this gap. MDR is designed to go beyond alerts. It detects, analyzes, and acts on threats in real time. From detection to analysis, isolation, forensic investigation, and even redesigning systems to prevent recurrence, MDR executes a full cycle by combining automation with expert human judgment.

## The flood of fake MDR

Many providers now claim to offer MDR. But when you look closely, what they actually deliver is very different. Some just combine logs in a SIEM and call it MDR. Others enhance rule based alerts in their monitoring service and label it MDR. Some even operate a single tool such as Managed EDR or Managed NDR and market it as MDR.

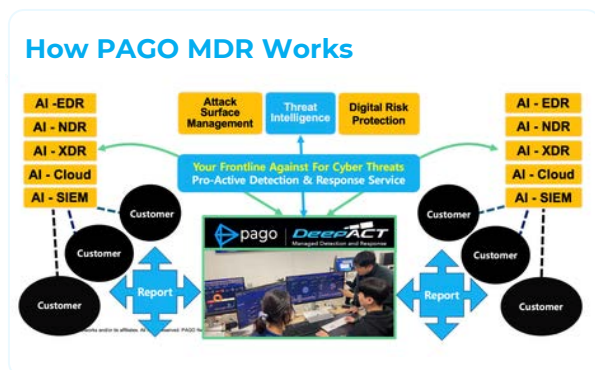




## The Standard of True MDR

A true MDR must be able to answer “yes” to all of the following questions. To achieve this, it is not technology alone that matters but the presence of a solid operating structure.

- When a threat is detected, can it be acted upon immediately?
- Can it automatically block and respond without human intervention?
- Can it detect not just individual events but the entire flow of the threat?
- Is detection and response connected as a single, seamless process?
- Can it identify and address security weaknesses before attackers strike?



## PAGO DeepACT: Designing the Conditions for MDR that Works

PAGO has embodied this concept of an “operating security structure” in the PAGO DeepACT MDR as a Service Framework. Built on eight years of experience managing more than 300 customers, it is not technology-centered but optimized for real-world conditions. Its key elements are:

- **SentinelOne:** An AI platform covering endpoints, cloud, accounts, SIEM, and Purple AI across the enterprise
- **Stellar Cyber:** Open XDR correlation analysis that brings together multiple security systems, revealing attack context and scenarios
- **StealthMole:** Detects early warning signs from the dark web and automatically reflects them in security rules

- **Aurora Protect:** Detects and resolves threats unique to OT environments such as factories and energy systems
- **PAGO DeepACT Platform:** The core that integrates threat analysis, decision-making, automated response, forensic investigation, and continuous rule learning
- Preventive measures such as attack surface management, dark web intelligence, and penetration testing, woven into one structure

## Industry-Specific Security: Why It Makes a Real Difference

Every industry has different needs. The threat points, asset structures, and speed and purpose of attacks vary across sectors. This is why MDR must be a security operating model tailored to each company. PAGO DeepACT provides such a tailored model in a form that can be designed and customized.

Many threats blocked by PAGO DeepACT were stopped not because of technical specifications but because of how the system was structured to operate. Technologies may look similar, but their application is what makes the real difference. Anyone can adopt XDR, use AI detection, and implement automation. What truly matters is whether these tools actually prevent incidents, whether they are designed to work properly within the company, and whether they are intelligently operated to fit the specific industry and situation.

Technology alone no longer differentiates security leaders. The ability to operationalize technology into an MDR model that prevents, contains, and adapts does. This is the foundation of PAGO DeepACT. Only an MDR that has been designed and built with this in mind can prevent or respond quickly to attacks. The key question is no longer which technology is the best but how that technology will actually operate inside the company. The MDR that has been answering this question first and longest is the **‘PAGO DeepACT MDR as a Service Framework’**. BN

Free Service

# PAGO Freemium

**Noticing unusual signs? It could be more than you think. If you're worried about potential threats, experience the protection of PAGO Freemium, free.**

PAGO Freemium is a free Threat Cleaning Service that uncovers, analyzes, and removes hidden risks in your environment, delivering immediate proof of value.

## **Immediate Threat Cleaning**

Scan and remediate suspicious activity in real time, eliminating dormant malware, misconfigurations, and overlooked exposures before they escalate

---

## **Operational Transparency**

Receive a clear report of what was detected and cleaned, providing visibility into threats your existing tools may have missed.

---

## **Proven Business Impact**

More than 80% of organizations that experienced Freemium converted into paying customers, representing a significant share of our client base. Among them, an outstanding 99.8% renew annually, demonstrating enduring trust and measurable value.

---

## **Foundation for MDR**

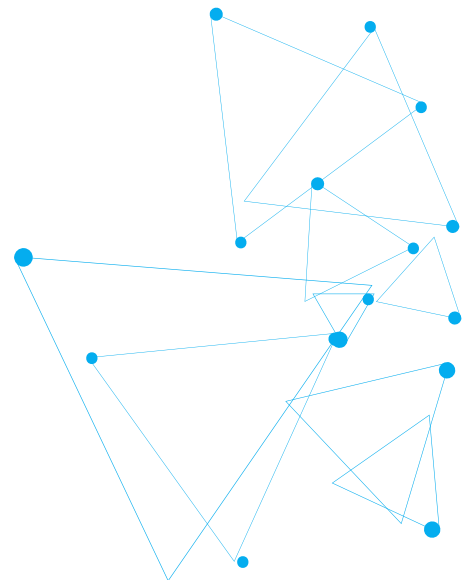
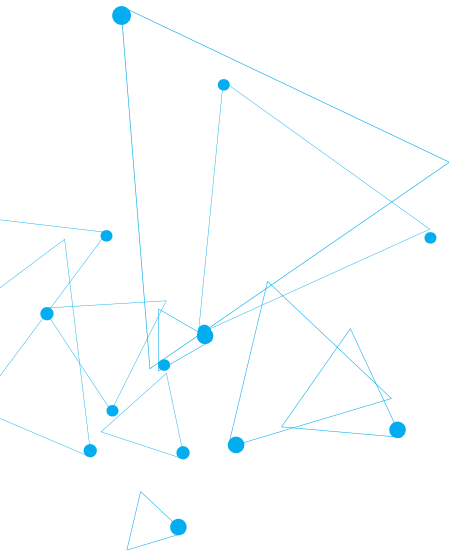
Freemium is seamlessly connected to PAGO DeepACT MDR. What begins as a one-time cleaning service evolves into a proactive, around-the-clock defense framework without requiring additional infrastructure or complexity.


---


## **Why it matters**

Freemium turns suspicion into certainty. By detecting and cleaning real threats, it proves how PAGO MDR delivers trust, resilience, and business impact from day one.

---



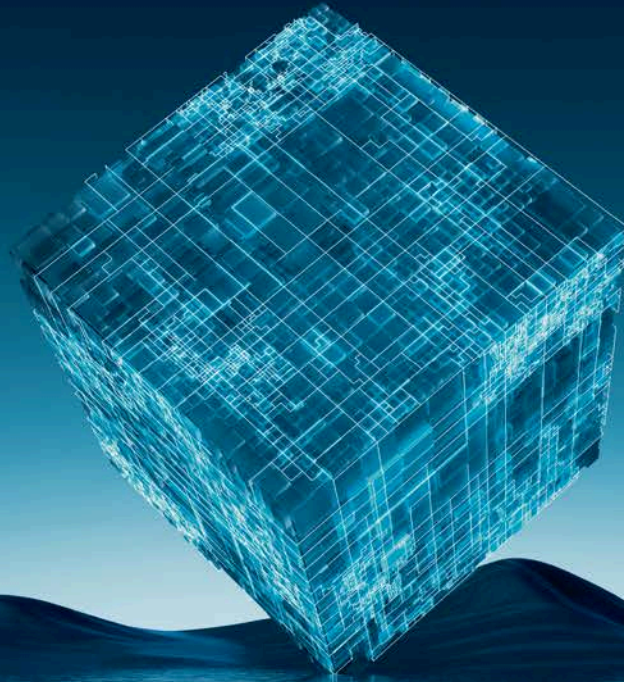
 65 Hoenamu-ro, Yongsan District, Seoul

 80-077-5171

 [sales@pagonetworks.com](mailto:sales@pagonetworks.com)

 [www.pagonetworks.com](http://www.pagonetworks.com)





# Cyber threats evolve. Are you ready?

**Beyond MDR: Threat Hunting Beyond EDR, NDR,  
XDR, ASM, Dark Web Monitoring, and AI SIEM**

PAGO 24/7 Security Operations Centers in Korea, Philippines and Malaysia  
prioritize your cybersecurity, offering comprehensive protection anytime, anywhere.  
Stay ahead. Stay protected. Stay with PAGO DeepAct.



## **From detection to prevention.**

We redefine modern cybersecurity solutions by moving beyond traditional threat detection to a comprehensive, proactive, prevention-first approach.



## **AI-driven threat intelligence.**

We leverage AI-driven threat intelligence for real-time monitoring, rapid response, and advanced defense, keeping organizations secure against cyber risks.



---

**PAGO Networks Inc.**

65 Hoenam-ro, Yongsan-gu, Seoul, Republic of Korea  
Phone: 080 077 5171

Website: <https://www.pagonetworks.com>

Copyright © 2025 PAGO Networks. All rights reserved.



---

**Byline Network**

30 Tojeong-ro 5-gil, Mapo-gu, Seoul (356-21 Hapjeong-dong), 2F  
Email: [byline@byline.network](mailto:byline@byline.network)

Website: <https://byline.network>

Copyright © 2025 Byline Network. All rights reserved.

**Byline Network**

---