From Detection to Decision
Security Fails Without Execution

INCIDENT RESPONSE INSIGHTS

How Should Security Respond To Attacks Already In Progress?
6 Real IR Cases From Enterprise Environments.

2026

pago

The Global MDR Frontline
Owning the Decisions That Matter Most

Table of Contents

ABOUT THIS REPORT

This report is based on real Incident Response cases observed across a wide range of industry environments.

Through years of frontline experience, PAGO has continuously examined where enterprise security becomes vulnerable and at what moments the outcome of an incident begins to change. Throughout this process, we identified recurring patterns that extend beyond isolated technical issues and consistently appear across broader security operations and response structures.

In recent security environments, both the speed and complexity of attacks are increasing rapidly, while the time gap between detection and response has become a far more critical variable. Behind this shift is the rapid rise of automation across both attack and defense operations, driven in part by the emergence of Agentic AI capable of autonomous decision making and execution. As a result, the limitations of traditional detection focused security models are becoming increasingly visible.

Within this changing environment, this report examines the flow and implications of real world security incidents through the following perspectives.

Key Topics

- The detailed progression of how real security incidents begin and spread;
- Common attack and response patterns observed across different cases;
- Operational limitations that are often overlooked within traditional security frameworks;
- Practical challenges revealed throughout the Incident Response process.

1. EXECUTIVE SUMMARY

Security environments are changing rapidly, with the methods, speed, and scale of attacks increasing beyond anything seen in the past. This shift reflects more than a simple rise in threats. It signals a broader change in how security itself operates.

In particular, the growing use of automated attack techniques and the emerging impact of Agentic AI capable of autonomous decision making and execution are exposing the limitations of traditional response models at an accelerating pace.

PAGO MDR is a security operations model designed to address these changes.

Rather than stopping at threat detection alone, it aims to connect detection with the decisions and actions that follow, helping minimize the spread of attacks and improve real security outcomes. However, many organizations still face structural limitations such as the following.

Security events are detected, but the response process is delayed before action is taken.

Response delays occurring during operational gap periods such as nights and weekends

Time loss caused by decision making and approval processes following detection

In these environments, threats are often identified but never fully contained in practice. The 6 Incident Response cases analyzed in this report clearly illustrate this reality.

Rather than beginning through direct external intrusion, many attacks started through already compromised accounts or seemingly legitimate access methods. From there, delays following detection created conditions that allowed threats to spread internally. These cases demonstrate that security weaknesses do not stem solely from the absence of technology.

In many situations, the scale of an incident is shaped by a combination of operational gaps and limitations within decision making structures. In this context, the key factor that expands damage is not simply a lack of detection capability, but a structural issue surrounding who responds, when they respond, and what criteria guide that response.

As AI driven automation and Agentic AI continue to accelerate the speed and repetition of attacks, security operations structures that include post detection judgment and execution are becoming increasingly critical.

Ultimately, the question raised by this report is simple.

Is your organization capable of detecting threats? Or is it truly prepared to respond?

This is not a challenge limited to specific organizations. It represents a broader structural issue appearing across today's security environments. At the same time, these changes are closely tied to wider shifts across the security market itself. The market is rapidly restructuring, with operational models increasingly becoming standardized around several large platform centered ecosystems.

Within this environment, organizations are being pushed beyond simple technology selection toward a more fundamental decision about how security operations should be defined and executed.

In the end, the real difference is not the technology itself, **but whether an organization has a structure capable of taking responsibility for what happens after detection and carrying response through to execution.**

2. REAL INCIDENT CASES

Part 1

Detection Gaps and Delayed Response

- Case 1. Ransomware Spread Through a Legitimate Account
- Case 2. Thousands of Threats Hidden Behind Security Tools

Part 2

Attack Speed and Response Timing

- Case 3. Large Scale Attack Stopped Before Expansion
- Case 4. Ransomware Attack Stopped Before Encryption

Part 3

Invisible Threats and the Challenge of Time

- Case 5. Persistent System Control Without Detection
- Case 6. Attack Attempt Contained Within 30 Minutes

Detection Gaps and Delayed Response

This section examines real Incident Response cases to understand how attacks begin, how they spread across the environment, and which factors ultimately influence the outcome. While each case is different, they also reflect structural patterns that continue to appear across modern enterprise environments.

Recent security environments are also seeing a rise in automated attacks and Agentic AI driven activity capable of making decisions and executing actions autonomously. As attacks become faster and more sophisticated, delays between detection and response can lead to far more serious consequences.

CASE 01

Ransomware Spread Through a Legitimate Account

Many attacks now begin through normal looking activity rather than obvious intrusion attempts.

WHAT HAPPENED

The attacker accessed the internal environment using a valid VPN account. The login generated no alerts and appeared to be normal user activity.
After gaining access, the attacker performed Windows credential dumping to obtain additional account credentials and gradually expanded access across the network.
Lateral movement through shared accounts eventually led to ransomware deployment across multiple systems and major business disruption.

WHAT WENT WRONG

This incident resulted from multiple operational weaknesses occurring at the same time.

- The attack occurred during off hours, delaying response;
- Shared accounts enabled easier lateral movement;
- Some critical systems lacked sufficient visibility;

Early signs of compromise existed, but response was delayed before the activity was recognized as an active threat.

WHAT CHANGED

PAGO identified the activity as a high risk threat with potential enterprise wide impact.

Immediate containment actions were applied while forensic analysis traced the attacker's movement across the environment.

This helped limit further spread and identify the attack path and root cause. **Fast response after detection became the key factor in reducing the impact of the incident.**

KEY TAKEAWAY

In attacks involving legitimate accounts, the outcome often depends on how quickly organizations can make decisions and respond after detection. Once response is delayed, attackers can rapidly expand further into the environment.

CASE 02

Thousands of Threats Hidden Behind Security Tools

Having security solutions in place does not always mean the environment is secure.

WHAT HAPPENED

The organization was operating antivirus solutions and believed the environment was adequately protected. However, the Incident Response process revealed thousands of hacking tools, trojans, and cryptominers already active across the environment.
Administrator account compromise attempts and internal network scanning were also underway.
The attackers had already established a foothold inside the environment, and threats had remained undetected for an extended period.

WHAT WENT WRONG

This incident was caused by multiple structural weaknesses operating together.

- Externally exposed web services and vulnerabilities remained unmanaged;
- Reliance on traditional antivirus reduced additional detection visibility;
- Attack surface management was not continuously maintained;

Under these conditions, attackers were able to operate internally for long periods without detection.

WHAT CHANGED

PAGO focused on improving visibility and strengthening response operations.

- Enterprise wide visibility through EDR and NDR;
- Identification of exposed assets through EASM analysis
- Removal of dormant threats and containment of further spread

This response helped eliminate active threats inside the environment and reduce the risk of a larger scale attack. The process also helped improve the organization's overall security operations structure.

KEY TAKEAWAY

Threats that are not visible may still already exist inside the environment. Organizations with limited visibility should always consider the possibility of existing compromise.

Case Summary

Although the 2 cases occurred in different environments, the attack patterns were similar. The main issue was the delay between detection and response.

- Attacks began through legitimate account access;
- Early signs existed, but response was delayed;
- Attackers had already established internal footholds before detection;

Attack Speed and Response Timing

The earlier cases focused on initial compromise and delayed response. This section examines how attack speed and the timing of intervention can directly affect the outcome.

In real incidents, the key factor is often not whether an attack occurred, but when response actions were taken during the attack progression.

CASE 03

Large Scale Attack Stopped Before Expansion

Most attacks do not begin as a single event. They progress through multiple stages before reaching the final execution phase.

WHAT HAPPENED

The attacker gained access through an externally exposed RDP service and compromised an administrator account. After access was established, security controls were disabled and preparation for large scale lateral movement began across the internal environment. Thousands of systems had already been included in the attack scope, and the ransomware deployment stage was approaching.

WHAT WENT WRONG

The issue was the failure to stop the attack during its preparation stage.

- Externally exposed RDP access was not properly controlled
- Malicious activity after administrator compromise was not blocked
- Security tools could be disabled within the environment

As a result, the attack progressed to the final execution stage without interruption.

WHAT CHANGED

Specific attack behavior helped identify the primary attacker controlled system, which was immediately isolated. At the same time, internal spread paths were analyzed and the attack chain was interrupted just before large scale deployment.
The deciding factor was not simply response speed, but the timing of intervention within the attack progression.

KEY TAKEAWAY

Attacks do not happen all at once. They progress through stages of Preparation → Control → Execution, and the outcome can change entirely depending on when intervention occurs.

CASE 04

Ransomware Attack Stopped Before Encryption

Many ransomware attacks go through extensive preparation before encryption begins.

WHAT HAPPENED

Late at night, suspicious access using a legitimate account was identified.
The attacker attempted to gain administrator privileges and create backdoor accounts.
This activity matched the typical preparation stage of a ransomware attack, where delays in response can quickly lead to encryption and large scale impact.

WHAT WENT WRONG

The issue was the failure to recognize these actions as the start of an active attack.

- Legitimate account access lowered the perceived risk
- The attack occurred during off hours
- Attempts to gain administrator privileges were not treated as immediate threats

As a result, early intervention was delayed.

WHAT CHANGED

The activity was identified as an early stage attack rather than a simple anomaly, allowing immediate intervention before execution.
Administrator related activity was blocked, and further privilege escalation and lateral movement attempts were contained.
As a result, the attack was stopped before causing business impact.

KEY TAKEAWAY

The outcome of a ransomware attack is often determined before encryption begins. Delays during the preparation and control stages can quickly lead to full execution.

Case Summary

These 2 cases highlight the importance of attack speed and timing of intervention. Attacks can rapidly escalate into large scale spread, but preparation and control stages almost always appear beforehand. Even when early signs are detected, delayed intervention can significantly reduce the effectiveness of response.

The scale of an incident is often determined less by the attack itself and more by when intervention occurs.

Invisible Threats and the Challenge of Time

The earlier cases focused on how attacks begin and when intervention occurs. This section examines threats that are difficult to detect and the importance of response timing.

Modern attacks are evolving beyond simple intrusion methods. Many are designed to hide traces, blend into normal activity, or avoid detection entirely.
In these environments, the critical factor is not only what was detected, but whether organizations can accurately interpret what is actually happening inside the environment.

CASE 05

Persistent System Control Without Detection

Attacks are not always visible. This case reflects how attackers can maintain long term control while leaving minimal evidence behind.

WHAT HAPPENED

The attacker gained access through a web shell, removed traces of the initial compromise, and maintained a memory based backdoor inside the system.
Most file based malware had already been deleted, and some logs were manipulated to reduce visible indicators of compromise.
While the environment appeared normal on the surface, external control was still actively maintained.

WHAT WENT WRONG

The main challenge was the lack of clearly identifiable indicators.

• File based detection struggled to identify memory based attacks
• Compromised logs were still treated as trustworthy
• Events were analyzed individually without understanding behavioral relationships

Under these conditions, active attacks can remain hidden even while ongoing compromise continues.

WHAT CHANGED

PAGO reconstructed the attack based on behavioral flow and contextual analysis rather than isolated events. Suspicious relationships between seemingly normal activities were identified, allowing the full attack chain to be traced.
This process uncovered the hidden backdoor and external control path, leading to immediate isolation and containment.
As a result, the hidden threat was removed before it could develop into long term compromise.

KEY TAKEAWAY

Invisible threats are often threats that have not yet been identified. Effective response depends on understanding behavioral flow, not isolated events alone.

CASE 06

Attack Attempt Contained Within 30 Minutes

Not all attacks unfold over long periods of time. Some can spread within minutes.

WHAT HAPPENED

The attacker uploaded a malicious file through a vulnerable web upload function and attempted to establish an external connection through a reverse shell.
This type of attack can quickly lead to internal control and further command execution once the connection is established.

WHAT WENT WRONG

The main issue was not attack complexity, but the extremely limited response window.

• Web application vulnerabilities were not properly managed
• External connection attempts were not immediately blocked
• Rapid attack progression was difficult to interpret in real time

Under these conditions, even a short delay can lead to lateral spread.

WHAT CHANGED

The attack was detected within approximately 30 minutes, and the external connection and related sessions were immediately terminated.
The attack flow was stopped before additional command execution or internal spread could occur.
The key factor was the ability to make decisions and execute response actions within a very short timeframe.

KEY TAKEAWAY

The key factor is often not attack sophistication, but response time. Even a few minutes of delay can allow the attack to move to the next stage.

Case Summary

These 2 cases show how attacks are becoming harder to detect while moving much faster. Threats increasingly appear through behavior rather than obvious malware or visible indicators, making isolated events difficult to interpret on their own.

Effective response depends on understanding context, behavioral flow, and what is actually happening inside the environment.

3. PATTERNS BEHIND THE INCIDENTS

The 6 Incident Response cases covered earlier occurred across different industries and environments, yet the attack progression and outcomes were remarkably similar.

These incidents reflect recurring structural patterns increasingly seen across modern enterprise environments.

1 Attacks Begin with Logins, Not Intrusions

In the past, the primary concern was external intrusion into internal systems. Recent cases show a different pattern. Attacks increasingly begin through legitimate looking access using compromised accounts or stolen credentials.

Common Attack Methods Identified Across Cases

VPN access through compromised accounts

Access through stolen RDP admin accounts

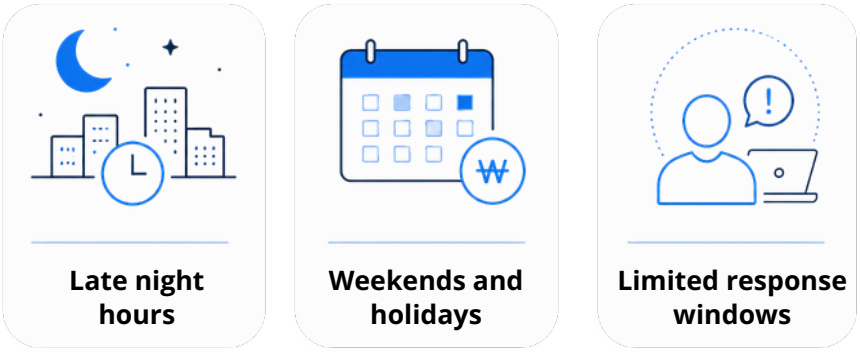
Lateral movement through internal accounts

From the system's perspective, these activities often appear normal. Attacks now begin not by breaking in, but by operating from inside the environment.

2 Attacks Exploit Operational Gaps

Another pattern consistently seen across the cases was attack timing. Most attacks occurred during periods when organizational response capability was reduced.

Common Attack Timing

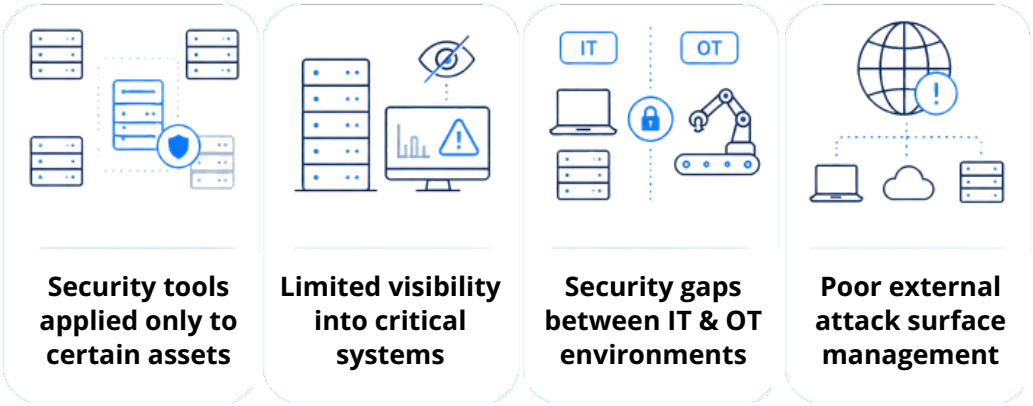


During these periods, analysis and response after detection are more likely to be delayed. Attackers target more than technical vulnerabilities. They also take advantage of operational gaps and delayed response windows.

3 Security Exists, But Visibility Remains Incomplete

Another common pattern was that incidents occurred even in environments already operating security solutions. The issue was not the absence of security, but incomplete coverage and visibility.

Common Environmental Weaknesses



Attackers can use unmonitored areas as entry points and lateral movement paths. Security blind spots often become intentional attack paths.

4 Traditional Security Models Struggle to Keep Up

The attack techniques identified across the cases continue to evolve in ways designed to bypass traditional security assumptions.

Common Attack Characteristics

Fileless attacks

Living off the Land (LotL) techniques

Log tampering and evidence removal

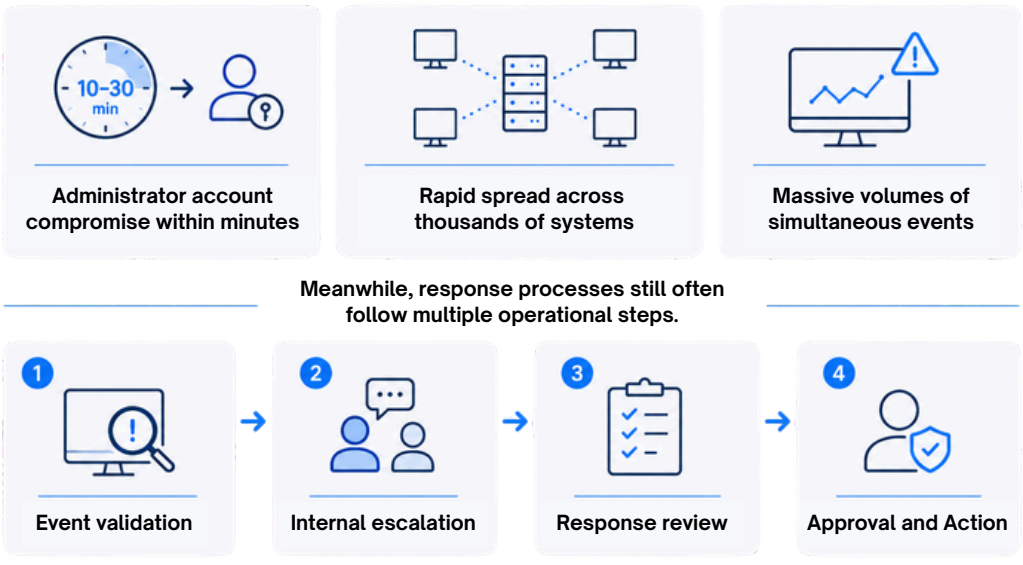
Attempts to disable security controls

These attacks are difficult to detect through signature based methods or isolated event analysis alone. Recent environments are also seeing growth in automated and autonomous attack techniques capable of making decisions and executing actions rapidly. Detection technologies continue to advance, while attacks continue evolving to bypass them.

5 Attack Speed and Response Speed Move Differently

One of the biggest operational challenges seen in real incidents is attack speed.

Common Attack Progression Patterns



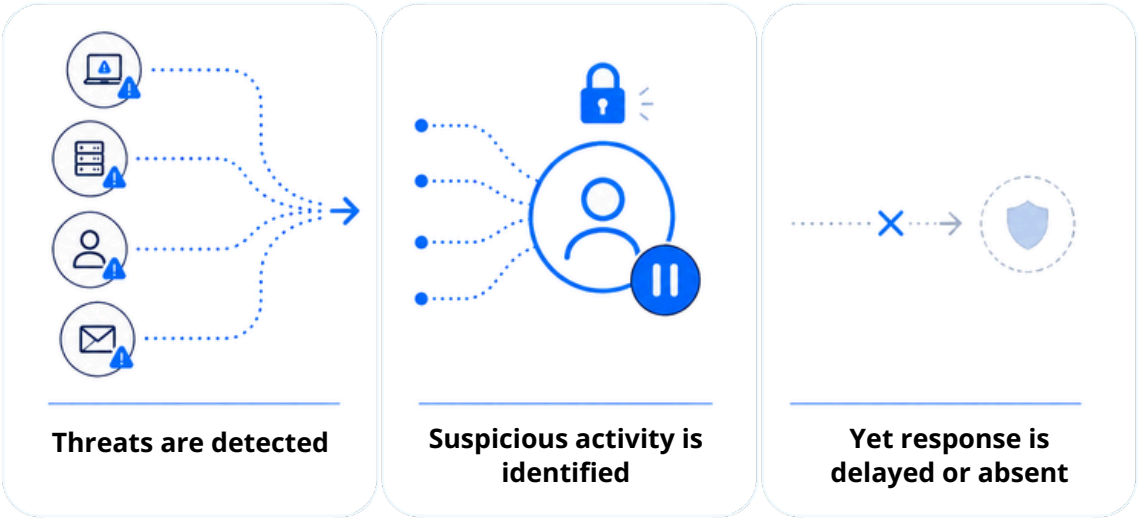
During this process, time continues to pass. Attacks progress in real time, while response actions are often delayed by operational processes. This gap frequently determines the overall scale of the incident.

Detection technologies continue to advance, but attacks are evolving in ways designed to bypass those assumptions.

6 The Most Important Question

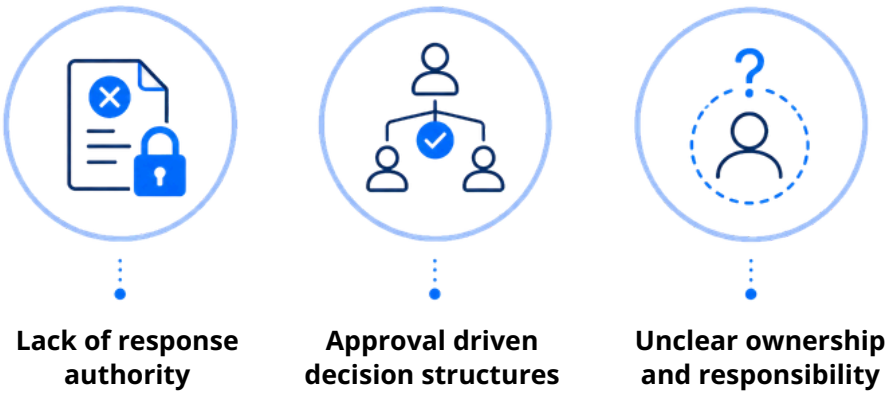
When all of these patterns are combined, they ultimately lead to one central question: **Who has the authority to act?**

Response Delayed at the Decision Stage

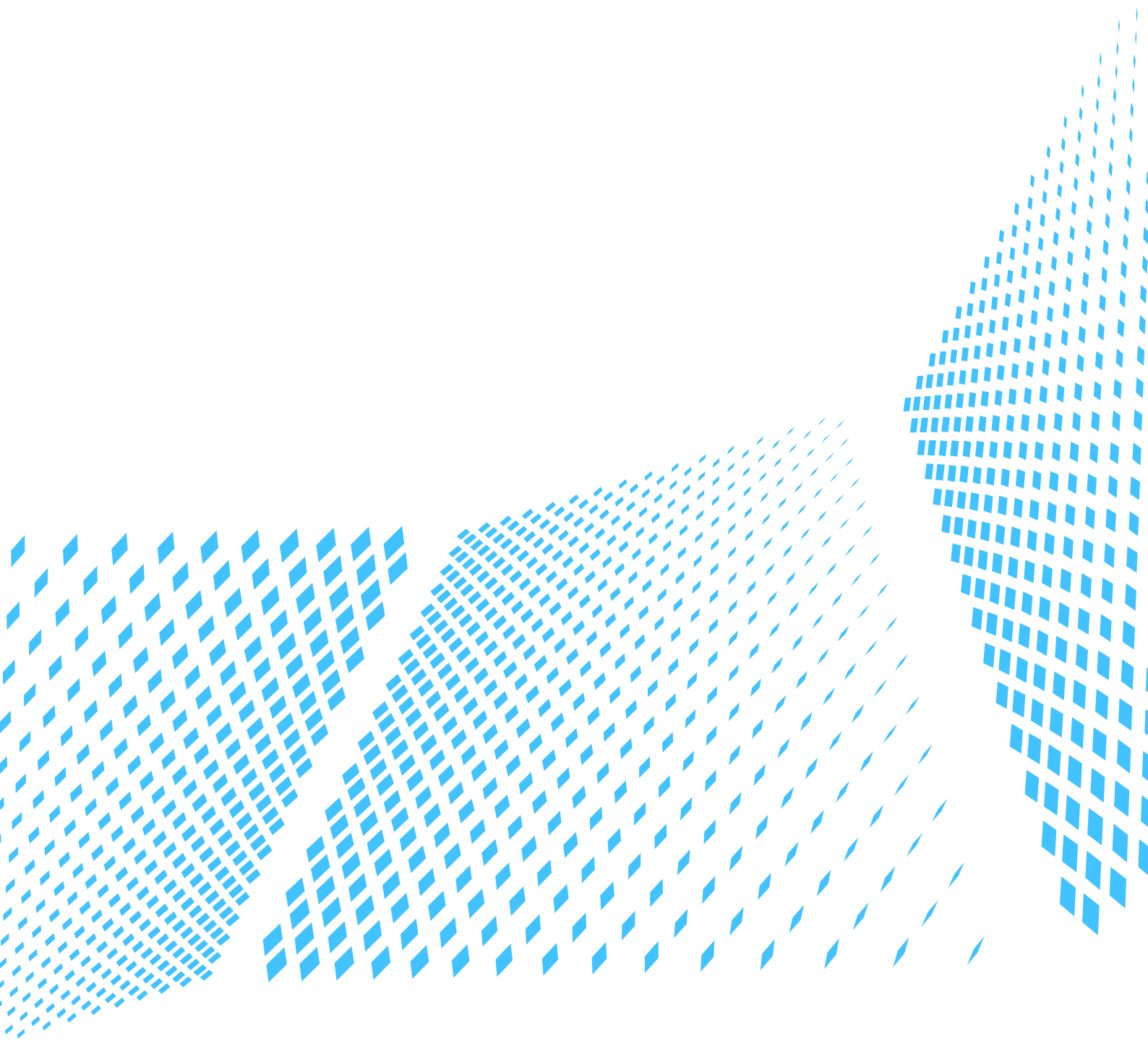


Threats are detected, but response often stops at the decision stage before action is taken. The reasons are often the same.

Common structural causes



In many organizations, threats are detected but still remain unresolved because response actions are delayed. The 6 cases ultimately point to the same reality. Security outcomes increasingly depend on who can respond, how quickly decisions are made, and how fast action can be executed.



4. WHAT FREE INCIDENT RESPONSE REVEALS

Many organizations operate security systems while still maintaining only limited visibility into how real threats emerge and spread. As a result, breaches can occur without the organization fully recognizing that they have already been compromised.

1 The Assumption That "We Are Secure"

Most organizations consider their security posture to be relatively stable for reasons such as the following.

Deployment of security solutions including antivirus and EDR

Operation of firewalls and network security systems

Establishment of log collection and monitoring processes

These elements are clearly important foundations. However, what is repeatedly observed during Incident Response engagements is that these foundations do not automatically translate into real security.

In actual investigations, situations such as the following are frequently identified:

- Threats already present within the internal environment;
- Attackers operating through legitimate accounts;
- Security structures where certain assets remain outside protection coverage;

> **The existence of security controls and being truly secure are two very different things.**

2 Why do many organizations fail to recognize this?

The reasons behind this gap are not simple. However, across multiple real world cases, several recurring patterns continue to emerge.

Undetected threats are often treated as if they do not exist	Response after detection remains a separate challenge	Visibility gaps emerge as a structural issue
		
• Fileless attacks • Access through legitimate accounts • Log tampering and evidence removal	• Delays in decision making • Time consumed by approval processes • Unclear ownership and responsibility	• Lack of monitoring across certain assets • Poor management of externally exposed attack surfaces • Disconnected security domains and systems
These types of attacks often leave no clear warning signs within existing detection systems. As a result, threats remain active inside the environment while organizations continue operations without recognizing their presence.	In many cases, the threat remains only as an “alert,” while the actual attack continues to progress.	As a result, organizations often have a different view of their security posture than what actually exists inside the environment.

3 What Can Be Identified Through Free Incident Response

PAGO’s Free Incident Response gives organizations a way to reassess their security posture based on what is actually happening inside the environment.

Key Areas Identified Through Free IR

- Active compromise and ongoing threats
- Blind spots missed by existing security controls
- Initial intrusion points and lateral movement paths
- Gaps in response and decision making processes

Many organizations realize the same issue for the first time. The challenge is not detection, but what happens after it.

4 Changes After Free IR

Organizations that go through an actual Incident Response process often begin to reassess their entire view of security.

- A new understanding of security posture;
- A shift from detection to response;
- The need to strengthen response operations and processes;

These changes often reshape how organizations approach security strategy overall. **Free IR helps organizations clearly understand the real security challenges they are facing.**

5 A Critical Question

This brings us back to the original question:

Is the organization truly secure, or have the risks simply not been identified yet?

Routine monitoring and reports alone are often not enough to answer that question. Organizations need to assess their actual environment to understand their real security posture.

5. FROM INCIDENT RESPONSE TO MDR

Many organizations only recognize the problem after an incident occurs, and begin responding from that point onward. In many cases, this approach is difficult to avoid.

The cases and analysis discussed earlier point to a clear reality. Many organizations only recognize the problem after an incident occurs, and begin responding from that point onward. In many cases, this is difficult to avoid.

Incident Response (IR) remains essential for identifying compromise, analyzing attack paths and root causes, and removing active threats. However, in real world environments, IR often functions less as a stage for resolving the problem and more as a process for understanding how far the incident has already progressed.

5.1 The Role and Limitations of Incident Response

Incident Response (IR) is an essential part of security operations, but it also carries several structural limitations. Most importantly, IR is inherently a post incident process. By the time IR begins, there is a high likelihood that the attacker is already inside the environment or has already established a certain level of operational foothold.

IR processes often involve difficult decisions such as:

- Whether to isolate affected assets
- Whether to shut down services
- Whether to block compromised accounts

Most of these decisions depend on customer approval and internal review processes. While this is a reasonable approach, it also means valuable time is lost during the response process.

As a result, IR has several inherent limitations:

- It starts after the incident has already occurred
- Response actions rely on customer decisions
- Delays often occur before action is taken

Under these conditions, gaps between detection and response can easily emerge.

5.2 The Real Challenge Begins After Detection

Looking back at the earlier cases, one pattern consistently appears. The threats were detected, but response did not happen immediately.

In many cases, the issue is rooted less in the technology itself and more in the structure of security operations. Under these conditions, gaps between detection and response can easily emerge.

- Response authority is limited
- Actions require additional approval
- Ownership and responsibility are unclear

In these situations, the threat may be identified, but the attack continues while response is delayed.

During that time, attackers often continue lateral movement, gain additional privileges, and prepare for the next stage of the attack. As a result, many organizations end up in a state where they are aware of the threat, but unable to stop it effectively.

5.3 How MDR Addresses the Problem

This is where Managed Detection & Response, or MDR, comes in. MDR extends beyond detection and focuses on closing the gap between detection and response. The key difference from traditional IR is how decisions are made and how quickly response actions can be carried out.

Key Characteristics of MDR

- 24/7 security operations
- Real time threat analysis
- Immediate policy based response
- Proactive threat containment

MDR turns detected threats into immediate action, not just alerts.

5.4 The Structural Difference Between IR and MDR

While IR and MDR may overlap in certain functions, they differ significantly in both operational approach and purpose.

Category	Incident Response	MDR
Timing	After an incident	Before and during an incident
Focus	Investigation and root cause analysis	Continuous monitoring and active response
Response Model	Customer approval based	Predefined ROE based response
Speed	Response may be delayed	Rapid response and containment
Responsibility	Customer led	Shared between customer and provider

This goes beyond a difference in functionality and reflects a completely different operational approach to security.

5.5 Why MDR Is Becoming Essential

Attack methods continue to evolve at a rapid pace.

- Growing use of legitimate accounts in attacks
- Increasing use of techniques designed to avoid detection
- Faster attack execution and escalation

In particular, the rise of Agentic AI driven automation is enabling attacks to become faster, more autonomous, and increasingly repetitive.

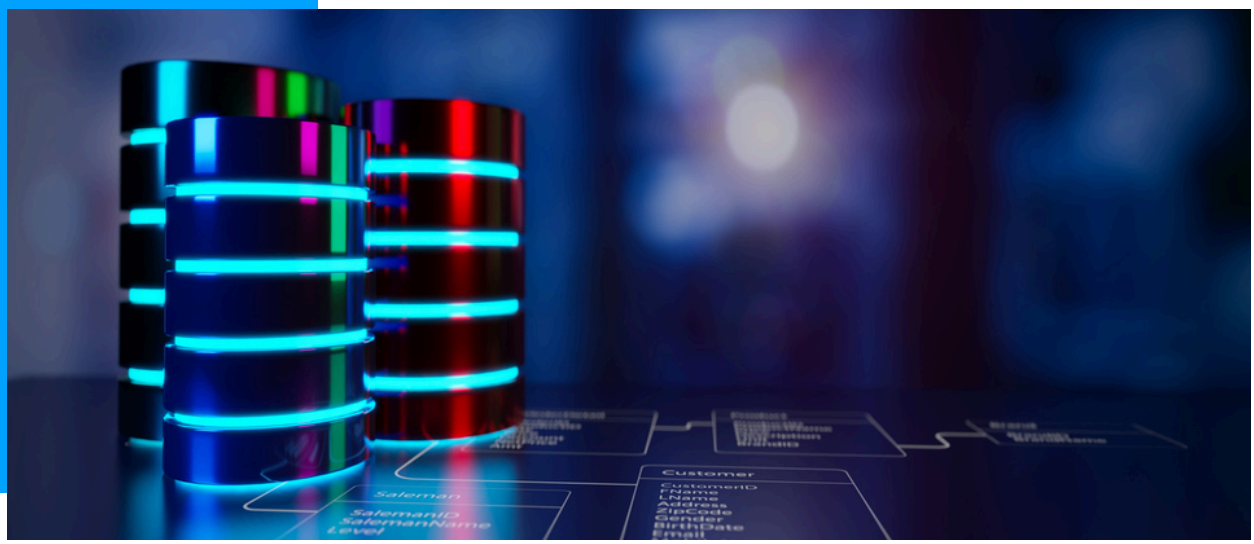
In these environments, detection alone cannot address every situation. When response is delayed, even a small compromise can quickly escalate. What organizations ultimately need is not more detection technology, but a clear operational model for how to respond after detection.

5.6 PAGO's Approach

PAGO views MDR as more than a security service. It is designed as an operational security model.

- AI driven detection and expert analysis
- Unified visibility across the environment
- Threat hunting & automated response
- Immediate isolation and containment

With this structure, detected threats can be connected directly to response actions. The core of PAGO MDR is fast decision making and execution.



6. CONCLUSION

The cases and analysis covered in this report reflect a common issue across many organizations. **Security systems are in place, but visibility into how threats actually enter and spread inside the environment often remains limited.** Even when threats are detected, response does not always happen immediately due to operational and decision making gaps.

The 6 cases reviewed in this report show how attacks are evolving. Many attacks now spread through legitimate accounts and trusted access methods within the environment. Attack speed is also increasing rapidly, which means even a short delay in response can give attackers time to move further inside the organization.

In these conditions, the outcome depends on how quickly decisions can be made and how fast response actions can be executed once a threat is identified.

As attacks continue to increase in speed and complexity, detection focused security structures face growing challenges. Organizations need faster decisions, immediate action, and response structures built for real time operations. Security is ultimately defined by decision making and execution.

7. THREAT VERIFICATION THROUGH FREE IR

Next Step

Validate your organization's actual security posture based on the reality of your current environment.

PAGO's Free Incident Response is more than a simple assessment. It is a process designed to identify what threats may already exist in the environment and how those threats are progressing.

Key Areas Identified Through Free IR

- Active threats and ongoing compromise
- Initial intrusion and attack movement
- Security blind spots and exposure gaps
- Response processes and operational gaps

Request Free IR

This process goes beyond a simple assessment and becomes the starting point for building a security operation that can respond effectively in real situations.

Now is the time to assess your organization's security posture based on the reality of your environment. The key question is not whether a compromise exists, but whether your organization has the visibility and response structure needed to detect and contain it.

www.pagonetworks.com