

CYTOMIC

**Cytomic, your hunting  
weapon against\_**

**Wait to become a victim? or  
Respond to the attacker?**



# Cytomic\_

There is no denying the fact that the current cybercrime landscape is dire. Data reveals an increase in the number (11% more every year) and sophistication of attacks, as well as in the business costs incurred (\$550 billion). Although

the increase in cybersecurity investment (+9.8%, €100 billion) has led to a greater level of protection, there is no such thing as total security. It is no longer enough to sit and wait for the attacker.

## More sophisticated and prolific cybercrime\_

↑ 11%

Security incidents in 2019<sup>(1)</sup>

39s

Seconds between one cyberattack and another worldwide<sup>(2)</sup>

2,244

Daily cyberattacks<sup>(3)</sup>

## Greater cost of Cybercrime\_

550 € Billion

Global cost of Cybercrime in 2019<sup>(4)</sup>

71%

Of attacks were financially motivated<sup>(5)</sup>

25%

of attacks aimed at espionage<sup>(5)</sup>

## Higher budget to tackle Cybercrime\_

↑ 100 € Billion

Total cybersecurity spending in 2019<sup>(6)</sup>

981€

Average cybersecurity spending per employee<sup>(7)</sup>

50%

of budget in 2020 will go to managed services<sup>(7)</sup>

This reality forces companies to adopt a **model to actively search and hunt threats**, and to evolve their **advanced security programs**, combining:

- **Strict preventive measures** with an exhaustive reduction of the attack surface and a strict control over which applications can run.
- **Robust, proactive detection and response capabilities** for incidents caused by attackers who manage to get through existing controls.

**Cytomic and its portfolio of solutions and managed services** help these organizations and their service providers to develop and automate their advanced security programs:

- **Evolving their security teams with experience, technologies, and processes that allow them to detect, contain and efficiently respond to the attacker on the network.**

In this process, the organization's security team can already be highly specialized and mature, while in others, the organization delegates to its MDR (Managed Detection and Response) service provider, either fully or partially.

- **Adopting managed Threat Hunting services**

The managed threat hunting services are designed to fill the gap in organizations that don't have the right profile. In this scenario, the external provider with resources, technology and processes is responsible for proactively discovering evidence of the attacker on the network.

# Challenges in the evolution of the security program\_

There are several challenges facing organizations and their **security (SOC) and incident response (CSIRT) teams** when it comes to implementing and strengthening their security programs.

## Lack of cybersecurity experts

By 2021, there will be 3.5 million unfilled cybersecurity jobs in the world(8). As a result, many organizations that don't have these specialized teams will be highly susceptible to attacks. This will directly impact their transformation strategies, as well as their results.

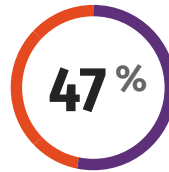
## The “fatigue” effect creates inefficiencies

SOCs are overwhelmed with multiple security solutions to managed (Platform fatigue), being forced to divide their time and attention between different programs, sensors, data sources, logs, and unfiltered and un-prioritized alerts (alert fatigue) There are too many places and elements that must be carefully analyzed to detect threats. This situation has a negative impact on operations and increases risks.

## Insufficient detection and response times

While attacks continue to become more sophisticated and more frequent, organizations spend countless hours manually identifying malicious threats. At best, this is a long process, which gives time for attacks to spread to the whole organization and cause damage.

This is why it is vital to strengthen security teams with managed **services or security platforms that automate detection and response**, and manage the Incident Response process between systems, minimizing the impact on the organization.



Of security alerts are ignored<sup>(9)</sup>



197 days

Is the time it takes to identify an attacker on the network (Global MTTD)<sup>(10)</sup>



266 days

Is how long it takes to contain the attacker (Global MTTR)<sup>(10)</sup>



Instead of waiting to resolve incidents, **security teams must make use of telemetry from EDRs** to proactively hunt for threats by identifying **suspicious behaviors** and behaviors that go against security policies.

## What is Cytomic?\_

Cytomic is a new unit of Panda Security. Its **differentiated value proposal** is built on this, combining security solutions and managed services to efficiently **hunt threats and respond to incidents in the protection** of computers, servers, virtual environments and mobile devices.

Its commitment is to support organizations in their **process of maturing towards an advanced security program**, with their own security and incident response teams, or delegating it to their security service provider (MSSP, SOC, MDR and CSIRT).

Cytomic also actively accompanies these specialized vendors, providing them with EDR platforms and tools that are unique on the market, allowing them to expand **their portfolio to hunting and incident detection and response services**, all with a reduced time.

Cytomic leverages the security model followed by Panda **3 Trillion events in the Data LakeSecurity**, which proactively neutralizes cyberattacks that use any kind of malware or exploits, or exhibit anomalous behaviors on the endpoints. With this, it offers a framework of solutions and services focused on:

- .....■ **Discovering attackers using living-off-the-Land and malwareless techniques** in their attempt to get around existing controls and compromise the organization.
- .....■ **Accelerating the endpoint investigation, mitigation and response process.** Actions that, when faced with a crisis, the SOC would otherwise have to perform manually, with no guidance, and which are costly and inefficient.

## The Cytomic platform\_

Cytomic's value proposal is based on scalable processing capacities on its cloud-native platform, which can be extended via its API.

## Scalable data analytics\_

The platform is optimized to prevent attacks, and detect, investigate and respond to incidents. It processes large volumes of events and attributes from the exhaustive monitoring of endpoint activity, using several AI algorithms and techniques, all in real time.

Cytomic's expert cybersecurity team supervises the platform and its results.

**+70,000**

**Million events per week**

**+10,000**

**Million events per day**

**3 Trillions**

**events in the Data Lake**

**2 Millions**

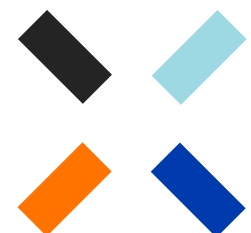
**New binaries classified every week**

**300 thousand**

**New binaries classified every day**

**365**

**Events retained every day**



# Value proposal\_



## Greater SOC efficiency, lower MTTD and MTTR

- **Real time monitoring and visibility**
- **365 days of visibility, enriched telemetry.**
- Zero compromises with malware attacks thanks to the Zero-Trust Application Service.
- **Threat Hunting Service included in products**
- Detection of anomalous behaviors.
- Exploit-based attacks blocked.
- **Retrospective and real time IoC search.**
- **Advanced alerts are prioritized and mapped on the MITRE ATT&CK framework.**
- Tools for hunting, anomaly detection, triage and investigation with pre-created data scale data analytics.
- **Massive and remote containment and remediation**



## Lower TCO in cybersecurity

- **Single cloud-based platform. Single lightweight agent.**
- No servers or maintenance staff.
- Roll-out in seconds. Minimal implementation costs.
- Lower cost of cybercrime by increasing efficiency of prevention, detection, containment and recovery for incidents.
- Facilitates analysis of the root cause, and continuous improvement of security posture.



## Cooperation of SOC's technological stack

- **API-First architecture that enables:**
  - Integration into the SOC's stack
  - Automation of use cases to endpoint remediation
- **investigation in the SIEM or delegated to the Cytomic platform, specialized in scale endpoint analytics.**
- **Integral incident response from the SOC.** Endpoints are actionable from the Cytomic platform or from any element in the stack.



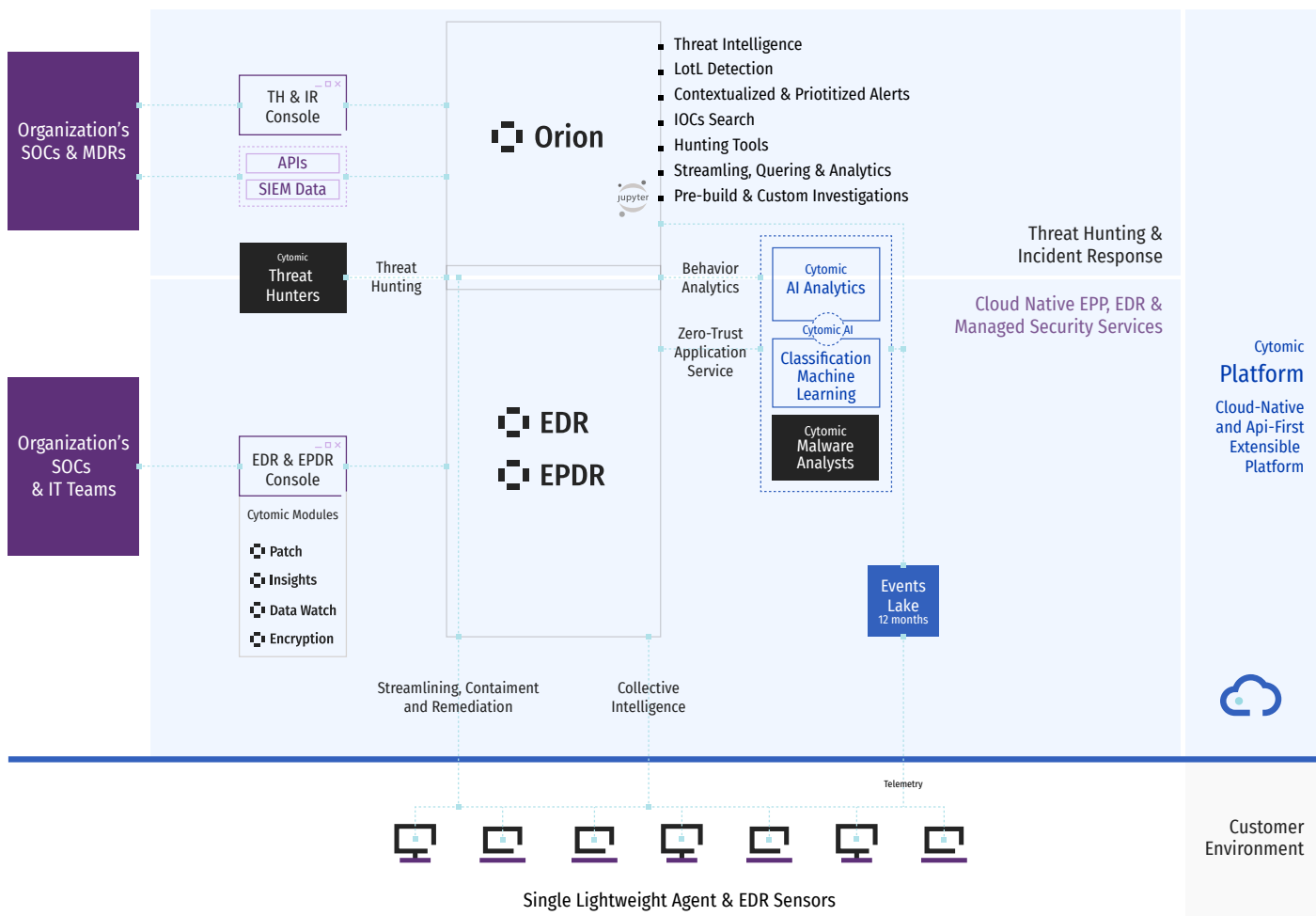
## Proactive detection. Threat hunting.

- **Services included in products by default:**
  - **Zero-Trust Application Service.**
  - **Threat Hunting Service.**
- Additionally, managed threat hunting services.
- **Telemetry service on the corporate SIEM.**

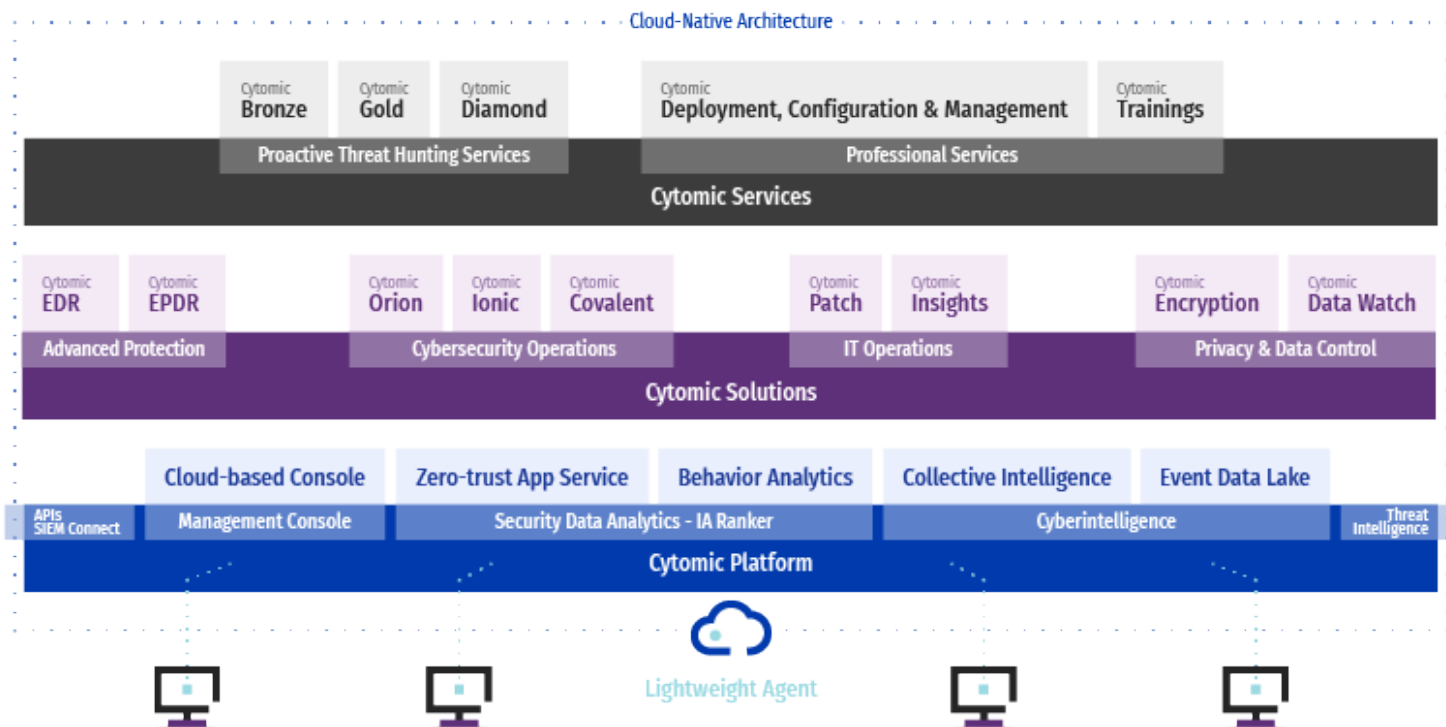
# Capacities of the Cytomic Platform\_



# Cyatomic Platform



# Cyatomic Portfolio



# Cytomic Zero-Trust Application Service

The **Zero-Trust Application Service** enables an unattended “deny-all” security model, with no alerts or delegation, and without affecting the organization’s operations. **In this model, malicious applications are no longer a successful attack vector for adversaries.**

In Cytomic’s advanced endpoint security solutions, all applications are stopped from running until they have been verified and certified by the service. Even if an application is approved, its activity is closely monitored to identify malicious behaviors.

This way, the service **definitively breaks the attack chain**, regardless of the nature of the malware. Trojans, worms, viruses, and of course, ransomware, are all eradicated.

The **Zero-Trust Application Service** combines different scalable technologies on the platform, stored on the Cytomic cloud.

These include **Collective Intelligence**, a repository of knowledge about legitimate and malicious applications, which is continuously fed with new internal and external knowledge from millions of protected endpoints. It also includes a **system based on scalable artificial intelligence in the cloud**, where different classification algorithms are run, from the simplest, such as similarity algorithms and decision trees, to the most complex, such as neural networks and deep learning models.

The system processes hundreds of static attributes, behaviors and contextals from each binary in real time.

All of this is supervised by a **human team of malware experts with years of experience in heterogeneous environments.**



**Malicious applications** are no longer a successful attack vector for adversaries after being inspected and classified by the Zero-Trust Application Service.

Organizations’ security teams benefit from this service, since it automatically filters malware-based attacks, and they can focus their efforts on malwareless attackers and scalable analysis of anomalous behaviors on the network.

**300,000** New application every day

 **4** hours Classification in under 4 hours

 **8x5** 8/5 CET Service Window



# The keys to **Living off the land** attack techniques

Attacks that employ Living-off-the-Land (LotL) techniques make use of what is already on the organization's devices and servers, with no need to download or install any other applications. This makes them extremely stealthy.

## There are five main types of LotL attacks:

- Double-use tools such as PowerShell or PsExec.
- Threats that run in memory.
- Fileless attacks, such as VBS code in the registry.
- Attacks in non-executable files, such as Office documents with macros and commands.
- Attacks that use Windows binaries (such as WMI) to run malicious activity—so called LOLBins.

## What advantages to these techniques offer to attackers?

- They can freely get onto systems via secure entry points.
- They don't arouse suspicions at any phase of the attack: entry, lateral movements, etc.
- They are difficult to identify, since they are confused with legitimate use.
- They require very few resources, and there are few impediments to carrying them out.
- They don't require the creation, purchase, and download of new malicious applications.

**Cytomic's advanced security solutions and managed services** monitor, supervise and process endpoint activity in a scalable manner, searching for anomalous patterns outside known profiles.

Along with **technologies**, the human element of **hunters and expert Cytomic analysts** is critical in order to be able to adapt to the evolution of adversaries and new technologies, both in malicious applications and in LotL techniques.

## How to avoid LotL attacks?

- Limit the use of scripting languages. If it's not possible to do without them, reinforce alerts.
- Constant, detailed monitoring. This way, anomalous activity can be discovered before it can endanger the organization.
- Having security operations teams (SOC/CSIRT) to run the organizations incident response program. The SOC filters alerts about anomalous activity, rapidly investigating critical alerts and responding to the attacker before they can cause any damage. What's more, once recovered from the crisis, the SOC can analyze the attacker in order to develop new ways to reduce the attack surface, thus improving the organization's security posture.
- Threat hunters that are free from the day-to-day processes of Security Operations can focus their efforts of detecting evidence of intruders that have managed to get around the organization's preventive controls. Hunters include these malicious behaviors in SOC processes for future detections.

**Cytomic's advanced security solutions and managed**

### **Avoid scripting language**

### **Monitoring and followup**

### **Threat Hunting services**

### **Cyber-resilience**

# Cytoomic

## El Servicio Threat Hunting

The threat hunting service included by default in all of Cytomic's endpoint solutions detects attackers using Living-off-the-Land techniques in any of the phases of the cyber kill chain.

Cytomic's team of cybersecurity experts manages and supervises the service with the technologies and capacities offered by Cytomic Orion.

The Cytomic Cybersecurity Team (CCST) investigates the indicators of attack generated in the platform by finding evasion and compromise techniques (TTPs) in the event stream.

On the other hand, and "always assuming compromise", the hunters in this team proactively search for patterns of anomalous behavior not previously identified on the network. To do this, they create advanced hunting rules, such as work hypotheses, which are evaluated against the telemetry gathered in real time and in the past 365 days.

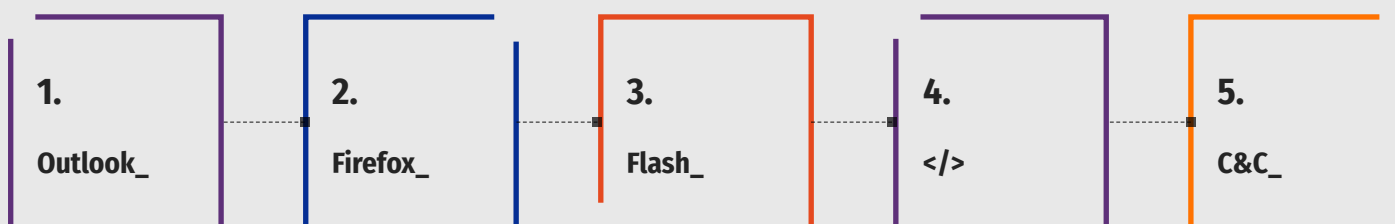
Should they come across an anomalous situation, the customer is proactively contacted by the team, providing forensic analysis of the affected systems, the origin of the attack, and the techniques used. They also provide recommendations on how to mitigate the attack and reduce the attack surface to avoid falling victim to future attacks.



Companies must assume that they have already been compromised. **There is no protection that covers 100% of attack techniques and anomalous behaviors, present or future.**



**Hundreds of TTPs and advanced hunting rules are continually evaluated on endpoints' event streaming.**



1. A user visits a website using Firefox from a phishing email.
2. This website loads with a vulnerable version of Flash.
3. Flash invokes PowerShell and introduces lines of command, operating from the memory.
4. PowerShell connects to a stealth command and control server, where a malicious Powershell script is downloaded that searches for sensitive information, which is sent to the attacker.
5. At no point does this attack download any malware, but it compromises the organization using Living-off-the-Land techniques.



# Cytomic Threat hunting service\_

## Security Data Science Unit\_

This unit is in charge of the Zero-Trust Application Service, where the scalable cloud-based machine learning system ensures that 100% of discovered binaries are classified.

They also maximize the results of the threat hunting process, applying machine learning and deep learning techniques to the more than 10 billion daily events processed by the platform, automating the analysis from the anomalies identified in the form of pre-constructed, flexible and reusable Jupyter Notebooks.

## Unit of threat specialists\_

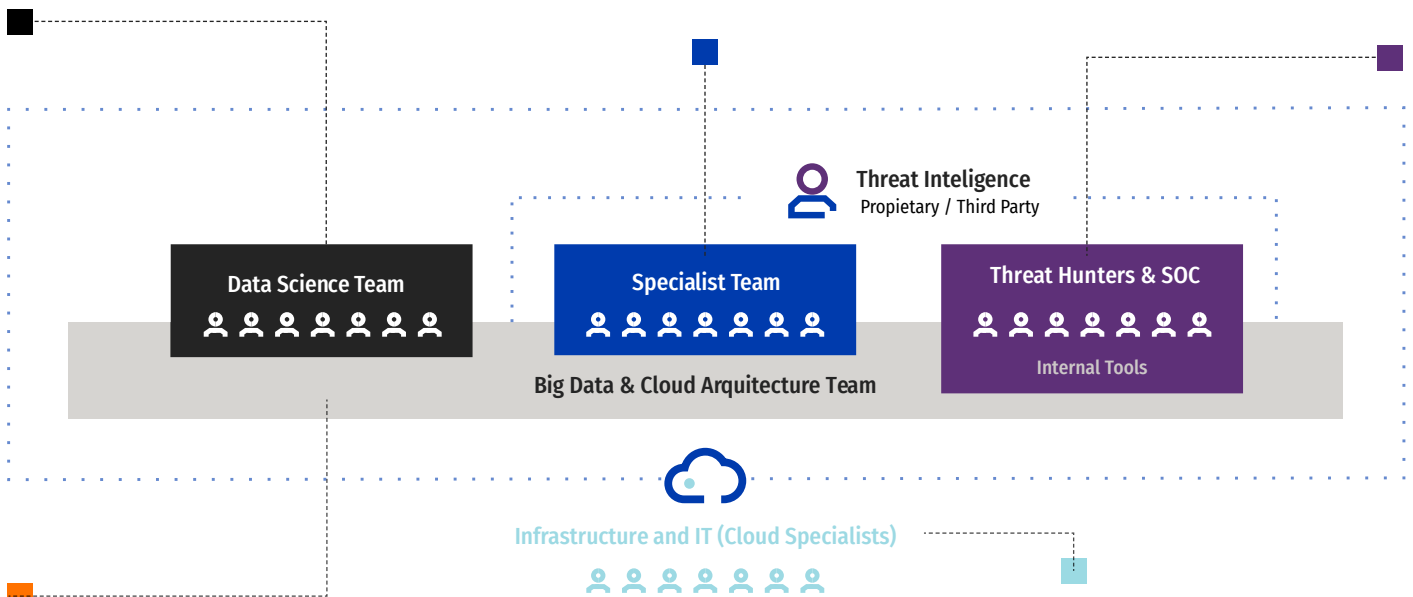
These specialists are key members that support the other units with their broad knowledge of threats and specific attack techniques. The team includes experts in:

- ■ **Reverse engineering.**
- ■ **Advanced artifact and TTP analysis.**
- ■ **Threat intelligence source analysis.**
- ■ **Specialists in vulnerability exploitation.**

## Hunters and operations team\_

They proactively search for anomalous behaviors, investigate and inform customers of any of the Cytomic threat hunting services.

Threat hunters are expert security analysts who detect new attacks or the beginnings of attacks on Cytomic customers by using Cytomic Orion, which allows them to investigate in the data lake of 365 days of events with a great level of depth and detail. The security operations team manages anomalies in behaviors (TTPs) indicators of attack (IoA).



## Application unit and specific Notebooks for other units\_

This unit serves the rest of the units, particularly the SOC and the threat hunters. For example, when a new sensor is needed on endpoints, or a new detection rule, or a new method in the threat hunting library to enable the detection of new evasion techniques.

## Big Data and Cloud specialists unit\_

The Cytomic platform can support immense volumes of events (70 billion per week), which must be processed in real time by complex machine learning algorithms, as well as being stored “warm” for 365 days in order to allow them to be processed massively and accessed at specific moments to allow investigations. The unit uses the latest cloud-based big data technologies so that the services fulfill preset levels.

# Cytomic Orion\_

**It is possible to get ahead of adversaries with real-time analytics and visibility.**

Achieving efficiency in the detection of advanced threats is directly related to the quantity and quality of the events monitored on endpoints and the capacity to enrich them with intelligence and analyze them at scale.

Hunting cyberattackers requires this structured data to be taken massively in order to apply behavioral analytics, including AI, and allowing the results to guide analysts in a complete investigation and in immediate action on endpoints. **This capacity is practically out of the reach of many organizations.**

Cytomic Orion **speeds up incident response and the search for malwareless** threats based on scalable behavioral analysis from the cloud.

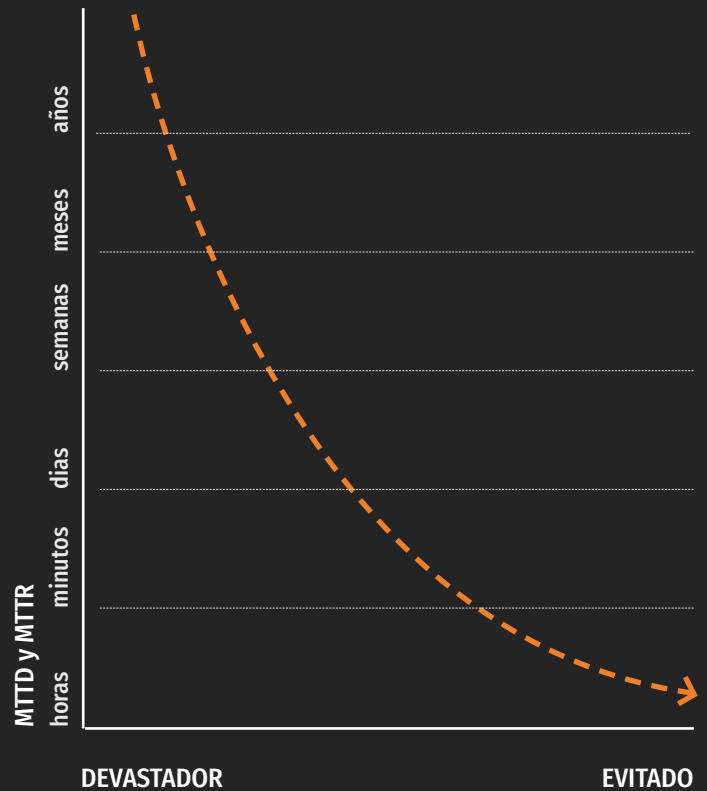
This is the analytic component of the Cytomic platform, where the gathering, enrichment and filtering of the millions of events monitored on endpoints and their context is all automated. Hundreds of algorithms and analytics rules are then applied to them, along with threat intelligence, in search of suspicious or malicious behaviors, in real time and retrospectively for 365 days.

Their tools, work consoles and pre-constructed analytics, such as the threat Hunting library and Jupyter Notebooks, allow an effective search for threats, accelerated investigations, and immediate actions on endpoints, from the very first day.

Pre-constructed investigations, Jupyter Notebooks, also favor a short learning curve for analysts and hunters, since they are self-explanatory, extensible and repeatable.

**Its APIs and connectors** allow for two-way integration with the SOC's technological stack, further speeding up discovery, investigation and action capabilities on the corporate network.

**The impact of an incident is directly proportional to the MTTD and MTTR.**



Cytomic Orion helps organizations to change their **security posture from defensive to offensive, and to reduce investigation time**, allowing analysts to swiftly correlate events and to test hypotheses.

**Mean time to detect (MTTD).** The average time needed to detect an attack. Requires additional investigation and response efforts.

**Mean time to respond (MTTR).** The average time to respond to and resolve the incident.

## What SOC capacities are amplified with Cytomic Orion?

- ■ Being prepared for an attack and running the Incident Response program.
- ■ Agile and continuous hunting, investigation process. Improvement of security posture.
- ■ Threat hunting with advanced consultations on the 365-day data lake.
- ■ Attribution and mapping with hundreds of TTPs from the MITRE ATTA&CK framework.
- ■ Real time and retrospective IoC search.
- ■ Threat intelligence from the Cytomic platform and external sources.
- ■ Expertise in in-depth investigations and investigations guided by tools on the investigation console.
- ■ Automation of investigations pre-fabricated with Jupyter Notebooks
- ■ Remote, scalable containment and remediation.
- ■ APIs to integrate with the technological stack in order to exchange information and processes.
- ■ Interoperability and automation of processes in the technological stack APIs and connectors on the platform encourage the exchange of information and



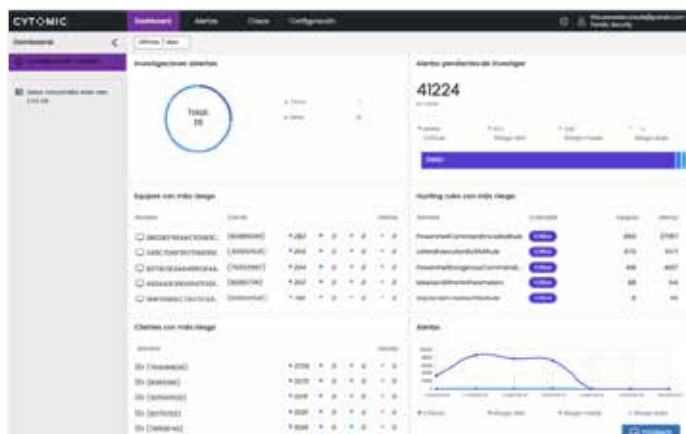
*“Given the complexity of attacks, security vendors have developed more flexible solutions with an ‘assume the attack’ mentality.*

*Focusing on the post-compromise stages of the cyber kill chain, with capacities to effectively detect and respond to advanced threats in a timely fashion.”*

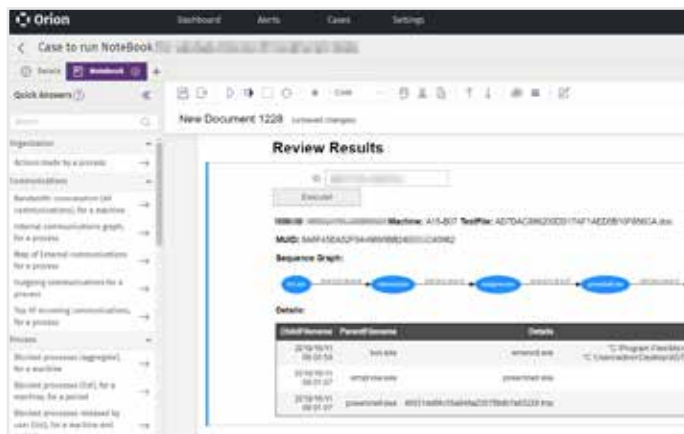


These solutions distinguish between expected actions and anomalous actions that may indicate the presence of a threat, a compromised device or attackers using techniques to hide their activity under the appearance of “regular” activity.

**Paul Webber, Patreek Bhajanka, Mark Harris, Brad LaPorte**  
Gartner analysts <sup>(11)</sup>



The investigation console allows analysts to carry out in-depth analysis on evidence. Events enriched with threat intelligence and patented security insights, visual event correlation tools, and trees of detailed processes include other capacities, and allow analysts to swiftly assign events to the sequences of an attack.



Our pre-constructed **Jupyter Notebooks**, the threat hunting library and the investigation console all provide data visualizations that speed up investigations.

Executions, network connections, and the correlation between processes, files and other events all allow SOC analysts to investigate and reproduce an attack, determining the impact and root cause in seconds.

(11) Market Guide for Endpoint Detection and Response Solutions, 23 de diciembre de 2019. Paul Webber, Patreek Bhajanka, Mark Harris, Brad LaPorte.

# Integration of the Cytomic platform in the SOC's technological stack

Integration with the SOC's technological stack, where the SOC already implements its incident response program, speeds up and enables processes to be automated by allowing platforms to access the capacities of other specialized and independent platforms.

The integration of the Cytomic platform is carried out via the SIEM connector and the integration APIs.

**365** days

By default  
"warm"

**IoCs and investigations are carried out on petabytes of historic events from up to 365 days ago**

## Benefits of integration with the SOC's technological stack.

### Unified visibility and cooperation

Allows for easy correlation and coordination between multiple products, as well as allowing more value to be extracted from organization's security investments. Enriches context information about incidents, and allows the petabytes of data needed for an investigation to be downloaded on the Cytomic platform, which is otherwise duplicated in other solutions such as SIEM.

### Rapid incident response

Provides analysts with synchronized tools to carry out actions on the whole infrastructure, from the perimeter to the network, and especially on the endpoints, which are the asset most often affected in a cyberattack.

### Coordination between security and IT operations teams

Security analysts and IT staff must coordinate to avoid and mitigate incidents, reducing the attack surface, and containing and remediating these incidents when they happen. The

The screenshot displays the Cytomic platform interface within a ServiceNow environment. The main area shows a table of 'Indicators of Attacks' with columns for Client, Username, Hunting rule, Indicator Date, Severity, Occurrences, and Last event. A context menu is open over one of the rows, showing options like 'Group by MITRE Technique', 'Pie Chart', and 'Graph'.

Client	Username	Hunting rule	Indicator Date	Severity	Occurrences	Last event	Tags
BRUNSWALTER_GUNGO	DESKTOP-NCEB8E1	Downdetected: Pooled in Event Stream	2020-05-09 20:08:24	High	1	2020-05-09 20:07:08:037923	Add Tag...
BRUNSWALTER_GUNGO	DESKTOP-NCEB8E1	Downdetected: Pooled in Event Stream	2020-05-09 20:22:17:28	High	1	2020-05-09 20:14:08:02901	Add Tag...
BRUNSWALTER_GUNGO	DESKTOP-NCEB8E1	Downdetected: Pooled in Event Stream	2020-05-09 06:39:12	High	1	2020-05-09 06:24:08:4285	Add Tag...
BRUNSWALTER_GUNGO	DESKTOP-NCEB8E1	Downdetected: Pooled in Event Stream	2020-05-09 23:53:52	High	1	2020-05-09 23:51:08:08117	Add Tag...
BRUNSWALTER_GUNGO	DESKTOP-NCEB8E1	Downdetected: Pooled in Event Stream	2020-05-09 05:05:11:13	High	2	2020-05-17 05:06:08:434812	Add Tag...
BRUNSWALTER_GUNGO	DESKTOP-NCEB8E1	Downdetected: Pooled in Event Stream	2020-05-10 11:53:23	High	5	2020-05-17 11:02:27:80948	Add Tag...
BRUNSWALTER_GUNGO	DESKTOP-NCEB8E1	Downdetected: Pooled in Event Stream	2020-05-10 04:49:24	High	6	2020-05-17 03:46:57:90835	Add Tag...
BRUNSWALTER_GUNGO	DESKTOP-NCEB8E1	Downdetected: Pooled in Event Stream	2020-05-10 12:53:18	High	1	2020-05-17 12:53:08:9054	Add Tag...
BRUNSWALTER_GUNGO	DESKTOP-NCEB8E1	Downdetected: Pooled in Event Stream	2020-05-10 12:53:18	High	2	2020-05-17 12:53:08:434812	Add Tag...
BRUNSWALTER_GUNGO	DESKTOP-NCEB8E1	Downdetected: Pooled in Event Stream	2020-05-09 18:58:54	High	1	2020-05-09 18:57:08:0613	Add Tag...
BRUNSWALTER_GUNGO	DESKTOP-NCEB8E1	Downdetected: Pooled in Event Stream	2020-05-09 12:09:14	High	1	2020-05-09 12:08:08:137384	Add Tag...
BRUNSWALTER_GUNGO	DESKTOP-NCEB8E1	Downdetected: Pooled in Event Stream	2020-05-09 18:28:45	High	4	2020-05-09 18:23:08:74282	Add Tag...

They proactively search for anomalous behaviors, investigate and inform customers of any of the Cytomic threat hunting services.

# CytoMIC EDR

CytoMIC EDR efficiently detects and responds to any kind of unknown malware and fileless and malwareless attacks, which traditional solutions can't detect.

It is based on the unique **CytoMIC Zero-Trust Application Service**, which simply stops any binary from running until it can be classified as trustworthy.

It also offers security teams:

- Total visibility of adversaries' actions.
- No impact on devices and servers, since the agent is lightweight and its architecture is cloud-based.
- Detection of anomalous behaviors on the endpoint (IoAs), blocking the attacker.
- Massive remote containment of endpoints from the console, such as isolating or restarting computers.

CytoMIC EDR coexists with and complements traditional security solutions.



# CytoMIC EPDR

Combines a full stack of preventive endpoint technologies in a single solution, with EDR capacities and the **Zero-Trust Application Service**.

CytoMIC EPDR prevents, detects and responds to any kind of malware, both known and unknown, fileless and malwareless attacks.

The Zero-Trust Application Service stops malware from running on computers, servers, virtual environments and mobile devices.

Extends CytoMIC EDR with a full range of endpoint protection capacities that are still necessary to stop threats from making their way onto devices and to stop threats from making their way onto devices and servers, reducing their attack surface.



	CytoMIC EDR	CytoMIC EPDR
Lightweight cloud-based agent	■	■
Real-time endpoint monitoring	■	■
Collective Intelligence lookups in real-time	■	■
Cloud-based big data Analytics	■	■
Zero-Trust App Service: Pre-execution, execution and post-execution	■	■
In-memory behavior anti-exploits	■	■
Behavioral IOA detection	■	■
Protection of systems when files are created		■
IDS, Firewall and Device Control		■
Web browsing and Email protection		■
Category-based URL filtering		■
Exchange server protection, antispam and content filtering		■

## Cytomic Ionic<sub>™</sub>

Coexists with and complements traditional endpoint security solutions, with a full set of EDR capacities, and with Cytomic Orion, which allows security teams (SOCs) to identify, investigate and contain bad actors using Living-off-the-Land techniques in the organization.

What's more, Cytomic Ionic increases the SOC's effectiveness and scalability, by using the Zero-Trust Application Service, which automatically blocks any attack that uses a malicious binary.

This means that, with Cytomic Ionic, the number of incidents for the SOC to manage is significantly lower compared to other EDR solutions that don't filter all unknown applications that display malicious activity.

## Cytomic Covalent<sub>™</sub>

Amplifies and extends the preventive detection capacities of Cytomic Ionic with a full range of endpoint protection technologies. EPP capacities are still necessary to stop threats from making their way onto endpoints and running there, as well as to reduce the attack surface.

With Cytomic Covalent, it therefore increases the efficiency and scalability of the SOC, by leveraging an integrated EPP and EDR architecture along with the Zero-Trust Application Service, which filters attacks based on malicious binaries.

This is the case even if they are unknown. It also leverages the tools and services of Cytomic Orion to speed up the search, investigation and containment of bad actors making use of Living-off-the-Land techniques.

The quantity of alerts and incidents to manage is significantly lower than when using any other EPP or EDR, which allow the attacker through when they deploy and use malicious tools and applications.



	Cytomic Orion	Cytomic Ionic	Cytomic Covalent
Threat Hunting Solution	■	■	■
Lightweight cloud-based agent		■	■
Real-time endpoint monitoring		■	■
Collective Intelligence lookups in real-time		■	■
Cloud-based big data Analytics		■	■
Zero-Trust App Service: Pre-execution, execution and post-execution		■	■
In-memory behavior anti-exploits			■
Behavioral IOA detection			■
Protection of systems when files are created			■
IDS, Firewall and Device Control			■
Web browsing and Email protection			■
Category-based URL filtering			■
Exchange server protection, antispam and content filtering			■



# Cytomic

## Managed threat hunting service\_

As well as endpoint protection solutions, Cytomic’s managed threat hunting services amplify the proactive security capacities of organizations that don’t have these roles in their teams.

These managed services are specialized in discovering suspicious behaviors that are typical in malwareless attacks, and proactively discovering unusual behaviors that could be indicators of attack.

When these indicators are uncovered by the Cytomic threat hunters, the customer is notified with context information and recommended actions. From that moment, the customer verifies and takes appropriate actions, both to contain the attack and to make the changes needed to reduce the attack surface against future compromise.

The managed threat hunting services extend organizations’ own capacities:

- Detecting cyberattacks in exploratory phases, lateral movements, etc., before malicious applications are deployed.
- Uncovering and applying data analytics to anomalous behaviors from users and computers.
- Discovering computers that have been compromised and the techniques used.
- Revealing bad practices or insecure

	Cytomic Bronze	Cytomic Gold	Cytomic Diamond
8/5 Offensive driven threat hunting	■	■	■
24/7 Offensive driven threat hunting		■	■
Cyber threats and living-off-the-land techniques email alerts	■	■	■
Monthly hunting reports	■	■	■
Telemetry agent assessment (weekly report)		■	■
Phone verification of critical malicious operations			■
Initial MDR assessment			■
Incident follow-up & advisory			■
Quarterly follow up & security recommendations			■

# Cytomic / Panda Security\_

## What differentiates the unit Cytomic from Panda Security?

Cytomic's stack shares technologies, platforms and services with Panda Security's solutions. However, Cytomic extends its portfolio of solutions with new capacities and services, such as Cytomic Orion and managed threat hunting services, to provide a flexible response to the needs of those organizations and service providers with a mature security program.

Below there is a brief outline of Cytomic's solutions and managed services compared to Panda Security's solutions, with an explanation of the differences between them:

Cytomic Solutions	Panda Security Solutions	Explanatory note
Cytomic EDR	Panda Adaptive Defense	<p>Cytomic EDR and EPDR include the following capacities not included in Panda Adaptive Defense and Panda Adaptive Defense 360:</p> <ul style="list-style-type: none"> <li>- The 100% Attestation Service is replaced with the <b>Zero-Trust Application Service</b>, which expands the former with a 4h 8/5 (CET) SLA.</li> <li>- The <b>Threat Hunting service</b>, integrated in the solution, includes up to 5 <b>notifications per year</b> in case of discovery of indicators of <b>malwareless attacks that haven't previously been blocked on endpoints</b>, with attack details: origin, computers affected, etc., and recommended actions.</li> <li>- On demand <b>uninstallers</b> for other solutions.</li> <li>- <b>Direct phone support with manufacturer 8/5 (CET)</b></li> <li>- <b>IoC search</b> <sup>1</sup>.</li> <li>- <b>Yara rule detection</b><sup>1</sup>.</li> <li>- Enforcement with advanced security policies to reduce attack surface on endpoints<sup>1</sup>.</li> <li>- Possibility of expanding the commercial offer with Cytomic Orion or with <b>Cytomic de Threat Hunting</b> <sup>2</sup>.</li> </ul>
Cytomic EPDR	Panda Adaptive Defense 360	<ul style="list-style-type: none"> <li>- Optionally, training and certification in: <ul style="list-style-type: none"> <li>• Advanced Administration (2 days).</li> <li>• Management console for partners.</li> <li>• Threat Hunting and Incident Response.</li> </ul> </li> </ul>
Cytomic Patch	Panda Patch Management	
Cytomic Insights	Panda Advanced Reporting Tool	
Cytomic Data Watch	Panda Data Control	
Cytomic Encryption	Panda Full Encryption	

<sup>1</sup> Available in Q2 2020

<sup>2</sup> Cytomic Threat Hunting Services Bronze, Gold and Diamond

Servicios Adicionales Cytomic	Servicios Panda Security	Nota Explicativa
<b>Cytomic Threat Hunting Service Bronze2</b>	-	<p>Only for customers with Cytomic Solutions/Services.</p> <p>The service differs from the default Threat hunting integrated in the endpoint solutions in the following ways:</p> <ul style="list-style-type: none"> <li>- <b>There is no limit on the number of notifications</b> about detected IoAs.</li> <li>- It includes <b>customized follow-up</b> of potential attacks previously detected and reported.</li> <li>- <b>Monthly report</b> on suspicious endpoint activity.</li> </ul>
<b>Cytomic Threat Hunting Service Gold2</b>	-	<p>Only for customers with Cytomic Solutions/Services.</p> <p>Expands the Bronze service with:</p> <ul style="list-style-type: none"> <li>- <b>Monitoring and weekly report</b> on the health of the endpoint protection.</li> <li>- <b>24/7 Availability</b></li> </ul>
<b>Cytomic Threat Hunting Service Diamond2</b>	-	<p>Only for customers with Cytomic Solutions/Services.</p> <p><b>Expands the Gold service</b>, available 24/7 with:</p> <ul style="list-style-type: none"> <li>- <b>Phone verification of suspicious activity.</b></li> <li>- <b>Initial analysis</b> of the organization's security and incident response program, and recommendations (MDR Assessment).</li> <li>- <b>Phone follow-up and recommendations for crisis situations.</b></li> <li>- Quarterly follow-up with recommendations to improve security posture.</li> </ul>
<b>Cytomic In-depth Incident Analysis</b>	-	<p>In case of compromise, <b>incident analysis and recommendations</b> to recover and reduce the attack surface.</p>
<b>Cytomic Threat Assessment On-Demand</b>	-	<p>In the event of suspected attackers on the organization's network, our team of cybersecurity experts <b>proactively searches for signs of malicious activity and prepares a detailed incident report.</b></p>
<b>Cytomic Training</b>	-	<p><b>Onsite or online training.</b></p>

(1) **Accenture:** <https://www.accenture.com/us-en/insights/security/cost-cybercrime-study>  
(2), (3) **University of Maryland:** <https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds>  
(4) **CSIS:** <https://www.csis.org/analysis/economic-impact-cybercrime>  
(5) **Verizon:** <https://enterprise.verizon.com/en-gb/resources/reports/dbir/>  
(6) **IDC:** <https://www.idc.com/getdoc.jsp?containerId=prUS44935119>  
(7) **Gartner:** <https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019>  
(8) **Cyber Security Ventures:** <https://cybersecurityventures.com/jobs/>  
(9) **Cisco 2018 Annual Cybersecurity Report**  
(10) **Ponemon Institute's cost of a data breach study 2019**  
(11) **Gartner: Market Guide for Endpoint Detection and Response Solutions, 23 de diciembre de 2019.**  
Paul Webber, Patreek Bhajanka, Mark Harris, Brad LaPorte.

# Awards and research\_



## Common Criteria “EAL2+”

Information Technology Security  
Evaluation



## High “ENS” Classification

ENS (National Security Framework)



## Qualified IT Security Product

Centro Criptológico Nacional  
(National Cryptology Center)



Panda Security regularly participates and wins awards for protection and performance from Virus Bulletin, AV-Comparatives, AV-Test, and NSS Labs. Cytomic's portfolio

shares technologies, platforms and services with Panda Security's solutions, extending its capacities with managed hunting services and Cytomic Orion.



[AV-Comparatives test Adaptive Defense 360 “This solutions classifies all processes executed and registers any kind of malware”](#)

# Your data belongs to you\_

## Your data resides in the European Union

Cytomic is committed to keeping your data safe.

We innovate to protect your devices, your users, your information and your privacy. And we use the most secure servers to manage your company's data.

Our servers are located in Europe, under its strictest security regulations and standards.

GDPR  
COMPLIANT



For more information\_  
[cytomicmodel.com](http://cytomicmodel.com)

Contact us\_  
[sales.hq@cytomicmodel.com](mailto:sales.hq@cytomicmodel.com)

