Threat Insights Report 2020_

CYTOMIC

cytomic.ai

Panda Security Threat Insights Report 2020

Table of Contents_

1. Executive Overview
2. Key Insights
3. Introduction
4. Methodology
5. Findings
    - No Crystal Balls: Data Fuels Global Threat Intelligence
    - Global Hotspots: The Attackers or the Attacked?
    - The Proof is in the PDF: File-Based Attacks Persist
    - The Limits of Whitelisting
    - The New Threat: Fileless Attacks
    - One Solution, Many Layers
6. Conclusion
7. Contact Us

CYTOMIC

Executive Overview_

With cyberthreats continually evolving and proliferating, security professionals of all types, from CISOs to MSPs and other providers need to look beyond the reactive approaches to cybersecurity and embrace a more forward-thinking strategy.

Traditional endpoint protection, with a single layer of technology between you and the world, is no longer viable in and of itself. Considering the increasing costs of skilled cybersecurity professionals, today's threats are too varied and multiply too quickly for IT providers and the clients they serve to depend on manual, human management of these tools.

In 2020, protecting endpoints against known threats is no longer enough. IT environments must be protected against the unknown as well. After all, once a spotlight is thrown on a cyber threat, new ones will attempt to sneak by in the shadows. To that end, it's crucial that IT providers make a shift in their cybersecurity strategy. The latest threats demand a move from single-technology cybersecurity and towards multi-layered cybersecurity solutions that employ behavior-based monitoring (among other features) to root out advanced persistent threats, fileless attacks and other malicious activity.

Furthermore, networked endpoints of all kinds, from desktops and laptops to servers, require an approach that brings together advanced endpoint protection (EPP) and endpoint detection and response (EDR) capabilities, with a zero-trust security posture backed by artificial intelligence. It is a necessary shift in how the cybersecurity industry tackles the problem of cyber threats, by emphasizing the idea of goodware—known, logged and classified processes that are allowed to run on an endpoint—keeping unknown and malicious processes from ever getting a chance to launch. These layered technologies provide an unparalleled level of control, visibility and flexibility that's needed in the dynamic war against unknown attackers.

Data compiled by PandaLabs—the cybersecurity lab of Panda Security and Cytomic— has illuminated several emerging trends in cyber threats that require sophisticated, next-generation cybersecurity to combat them.

We built our 2020 Threat Insights Report on this foundation, to help guide you in protecting against what's to come. Because moving forward, the right combination of protections is not a difference between one cybersecurity solution or another; it's the difference between being protected against tomorrow's threats or becoming their prey.

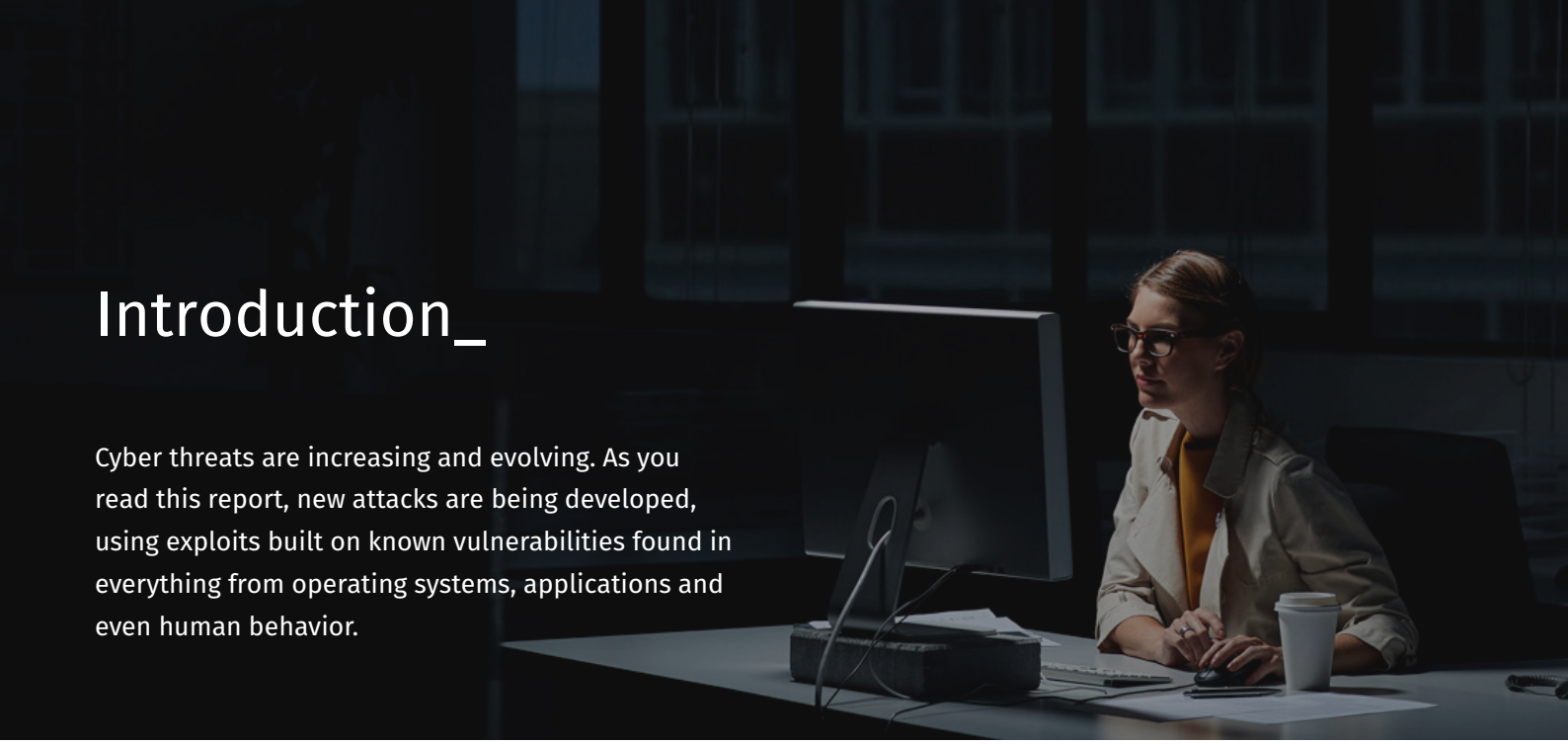
Key Insights_

Ransomware is still persistent and pervasive; one click can still bring down a network.

Fileless attacks are an increasing area of concern, as they are more difficult to detect and provide stealthy opportunities to corrupt an entire network.

Proactive threat hunting is now an essential solution for recognizing malicious behavior through otherwise trusted applications.

Cybersecurity defenses can no longer be based on a single technology; a layered technology approach, combined with a zero-trust security outlook ensures there are no gaps in a strong security posture.



Introduction_

Cyber threats are increasing and evolving. As you read this report, new attacks are being developed, using exploits built on known vulnerabilities found in everything from operating systems, applications and even human behavior.

Cybercriminals are ultimately after three things:

Financial gain, using ransomware to extort money.

Data, which can be sold on the dark web.

Control of infrastructure, networks or other important systems, so that access can be sold to power brokers such as nation states, political groups, paramilitary factions and more.

The frequency of attack in large enterprises is **2000 times higher** than in SMBs.

For small and medium-sized businesses, large enterprises, and local government and other critical organizations, the danger of cyber threats has never been more imminent. In just a few short years, the mindset has moved from “It won’t happen to me,” to “It’s only a matter of time.” It is now a simple matter of fact: there is inherent risk with operating a computer network, and a security incident could damage an organization irreparably.

Fortunately, as cyberthreats evolve, so too does cybersecurity technology. Long gone are the days of simple, slow and reactive antivirus applications. Today’s cybersecurity solutions employ a range of capabilities designed to keep networks free of infiltration, stop malicious behavior, and curb future intrusions. But not all cybersecurity solutions are created equal. Some are built on older architecture and cannot adapt as nimbly to new threats. Others are reactive—relying on detecting a breach before it can act. And others are just not feasible, letting far too many threats go undetected.

At a time where the cybersecurity market is flooded in a rush to provide CISOs, MSPs, IT service providers and large enterprises with the one solution that’s best for them all, how does one cut through the noise to find the right option?

As with most things, it starts with asking the right questions_

Why react to cyber threats?

What else is out there that the solution can't see—and will they attack next?

Why should a cybersecurity solution only detect threats that worked (i.e., infiltrated a network)?

Clearly, reactive security modalities are no longer viable. There are too many threats and too many attack vectors in any IT environment to risk a breach of any kind. Modern cybersecurity solutions must be predictive, proactive and prepared for anything that comes at it; they must be the sword as well as the shield.

This have given rise to a layered technology model, combined with a zero-trust security posture, which does not allow any unknown processes to execute on a network's endpoints.

The insights in this report will show why next generation endpoint protection solutions are using this support successfully, and why it's not only logical—it's mandatory.

Methodology_

This report is based on telemetry and detection data collected from our agents on endpoints running our technology during 2019. It was compiled and analyzed by the PandaLabs and our security operations center. PandaLabs serves as the nerve center for everything threat related and helps to shape our technology.

PandaLabs maintains a constant state of vigilance, following various threat and cyberattack trends and developments closely in order to formulate forecasts, tactics and strategies for future threats, and to alert the public to imminent dangers.

The cybersecurity professionals at PandaLabs provide real-time, uninterrupted countermeasures that protect our customers from all types of threats on a global scale. They also dig deep into threat forensics, performing detailed analyses of all types of threats to improve protection solutions and keep the general public informed.

Unique Telemetry Data_

Cytomic EPDR technology constantly monitors all the actions triggered by running processes on protected endpoints. Each event is cataloged based on more than 2,000 unique object characteristics. These telemetry events are not considered incidents, malicious objects or anomalies; instead, they represent information linked to a specific object, for example:

Processes: creation of a process, execution of a process, injection of a process in another event (child), etc.

File: creation of a new file by an event/process, editing of a file, deletion of a file, opening of a file and other operations.

Communications: opening of a communication socket, use of a communication protocol, communication direction, the origin of the communication, etc.

Registry: creation, edit and deletion of registry keys.

Administration: use of administrative credentials, login/logout events, installation of processes, service activity, among many others.

These actions are sent to our cloud platform, where they are analyzed using machine learning techniques to automatically extract advanced security intelligence. This information allows us to classify each and every process run, with near-zero false positives or false negatives.

Because Cytomic is committed to a zero-trust security posture, Cytomic EPDR repels virtually all malware-based threats, and any that do manage to claim a foothold on an endpoint, whether by deceptive measures or user error, are still not allowed to run. This is due to our 100% classification service, which prevents unknown and unclassified processes from executing, as well as our AI-backed threat hunting services that monitor app behavior to ensure that fileless attacks and other advanced threats are not proceeding unforeseen.

As such, the data you will find in this 2020 Threat Insight Report is—by mission and intent—unlike that of other industry reports. However, this should not be surprising. As leaders in cybersecurity, with more than 30 years at our backs and a collection of important firsts in the industry, Cytomic is committed to what's next, as we focus on protecting endpoints from ever being breached by threats of any kind.

Findings_

No Crystal Balls: Data Fuels Global Threat Intelligence

Next generation endpoint security requires the collection and analysis of a staggering amount of data, which fuels everything from artificial intelligence making context-based behavioral analyses and predictions to sophisticated threat hunting services that intercept threats before they strike.

If knowledge lights the way, then in the realm of cybersecurity, endpoint data provides the visibility that's integral in providing a best-in-class solution, and essential for administrative users who manage their networks day to day.

The data represented in this report shows not only how much information is processed in order to achieve optimal results from next-generation endpoint security, but also how essential that data is in seeing what is happening on each endpoint in order to detect changes, trends and anomalies in the global threat landscape. Without such a high level of visibility today and in the future, cyber criminals will assuredly drift through networks with ease.

Data-Driven Insight—Not Intuition

Our Telemetry Data, 2019. Figures are normalized to one million endpoints.

All telemetry data Collected for 2019

1.2
per million endpoints

Malware Detections

14.9M
malware alerts

Executables Identified

426M
executables identified

Applications executed

79.5M
child processes executed

(processes created or libraries loaded)

Dynamic library (dll) files identified

336M
files identified

Note: Actions taken by processes in general and the evolution of the malware detections in the network—whether actual malicious files were run or not—help administrators make decisions with regard to defining mitigation actions and adjusting security policies.

Detection and Remediation

Malware

14.9M
events

Exploits

76,000
alerts

Potentially Unwanted Programs (pup)

7.9M
alerts

Communications

Network Events

1.4T
events

Dns changes

2B
events
(failed DNS queries)

Download

1.6B
events

Note: Monitoring network connections established by processes is key in identifying suspicious or potentially risky destinations used to launch cyberattacks or steal data.

Entity (file) behavior

Processes

1.7T
events

Registry operations

735M
events

Scripts

1.9B
events

Applications executed

92B
events

Device operations

973M
events

Login/logout

133B
events

Note: Detailed information on entity behaviors enables administrators to focus their attention on the suspicious activities performed by new, yet-to-be-identified items, and compile data that can be leveraged to reach conclusions about their potential risk.

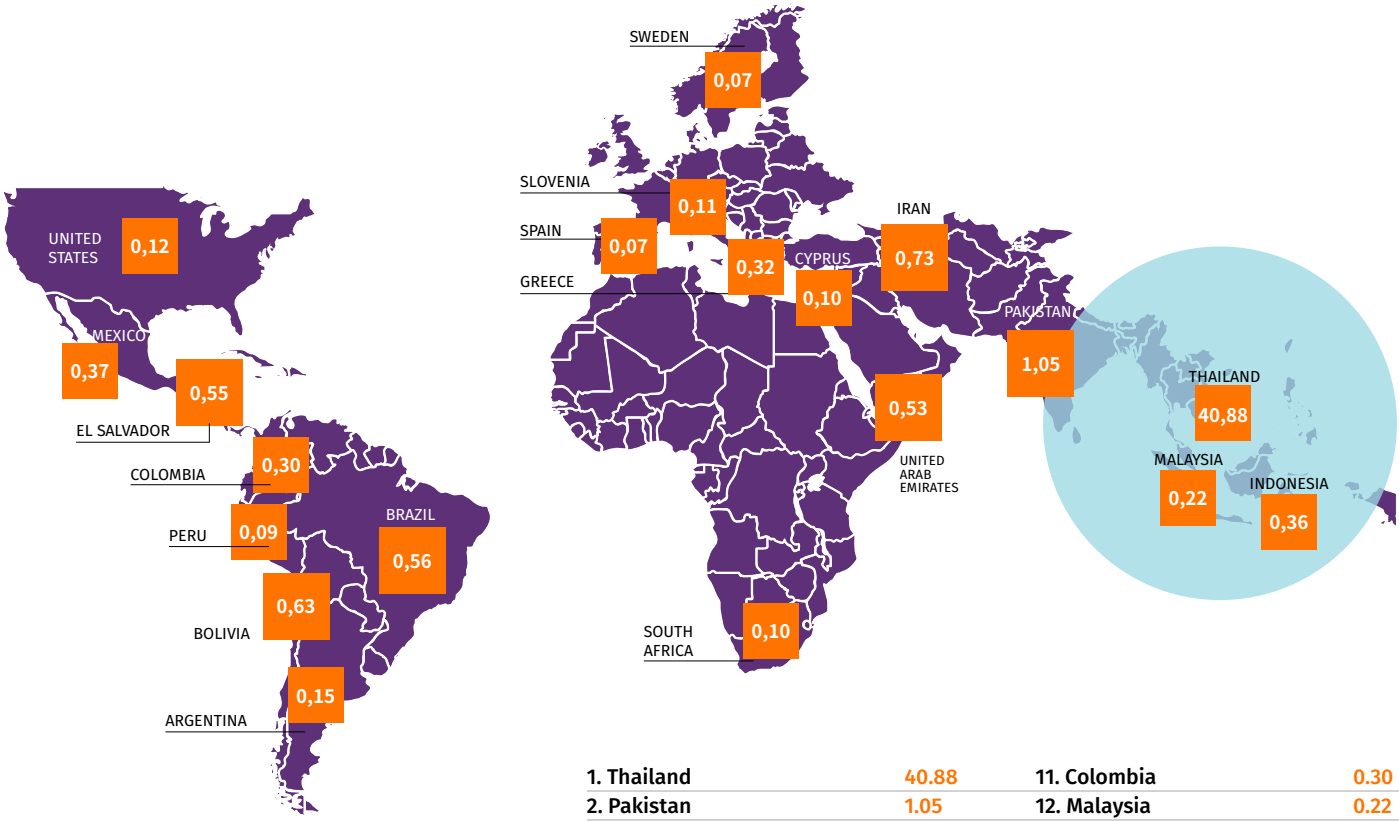
Global Hotspots:
The Attackers or the Attacked?_

From the data, there is a dramatic lead in targets in the Middle East and South America. However, Thailand leads the pack exponentially. This outcome may be expected, but the insight is double edged. These countries are good targets for a reason, as hackers have had success here in compromising systems, due to exposed, under-secured endpoints.

Conversely, these attacks that were repelled by our technology, which provides a strong barometer of the cadence that attacks are carried out within a region. It can be assumed that these targets are not the end goal; these targets are likely the source of other, even more sophisticated attacks on targets worldwide.

Top 20 Countries for Malware Attacks

A ranking of countries with at least 1,000 reporting machines, based on the ratio of malware alerts (not infections) to reporting machines.



1. Thailand	40.88	11. Colombia	0.30
2. Pakistan	1.05	12. Malaysia	0.22
3. Iran	0.73	13. Argentina	0.15
4. Bolivia	0.63	14. United States	0.12
5. Brazil	0.56	15. Slovenia	0.11
6. El Salvador	0.55	16. Cyprus	0.10
7. United Arab Emirates	0.53	17. South Africa	0.10
8. Mexico	0.37	18. Peru	0.09
9. Indonesia	0.36	19. Sweden	0.07
10. Greece	0.32	20. Spain	0.07

Access events to PDF files_

This data, compiled from endpoints running our technology, reveals the power behind certain file extensions—many of which are seen by users every day. And behind each of these extensions lies a vulnerability in the very nature of their file that can be exploited by bad actors to carry out attacks. The PDF, a ubiquitous file format used globally every day, tops the list—and with good reason: they have been notorious for decades in their ability to carry out malicious attacks and inject malicious code on application processes or used as a medium for phishing campaigns, with just one unsuspecting click by a user.

Top File Extensions for Data Access Events

A ranking of data file extensions accessed n 2019 and the number of unique access events logged.

#	Unique Events	Extension	Description
1	220,124,750	.pdf	Portable Document Format File
2	178,096,618	.odf	OpenDocument formula (associated with MS Office apps)
3	60,203,323	.job	Windows Task Scheduler task object
4	51,313,631	.pem	Privacy Enhanced Mail Certificate (involved in secure website authentication)
5	48,607,743	.mdb	Microsoft Access Database
6	28,006,668	.xls	Microsoft Excel spreadsheet (legacy 97–2003 format)
7	25,388,869	.doc	Microsoft Word document (legacy 97–2003 format)
8	17,199,902	.cer	Internet Security Certificate (involved in website authenticity validation)
9	16,896,788	.pst	MS Outlook Personal Information Store File (mailbox file)
10	10,927,605	.p12	Personal Information Exchange File (file containing a digital certificate)
11	10,576,428	.dwg	AutoCAD Drawing Database File
12	9,234,914	.odt	OpenDocument Text Document format
13	8,403,811	.ods	OpenDocument Spreadsheet format
14	6,175,198	.ini	Windows Initialization File (typically used to load application settings)
15	5,375,405	.ppt	MS PowerPoint Presentation
16	5,100,168	.dat	Generic data file format (generated by specific applications)
17	4,418,416	.txt	Plain text file

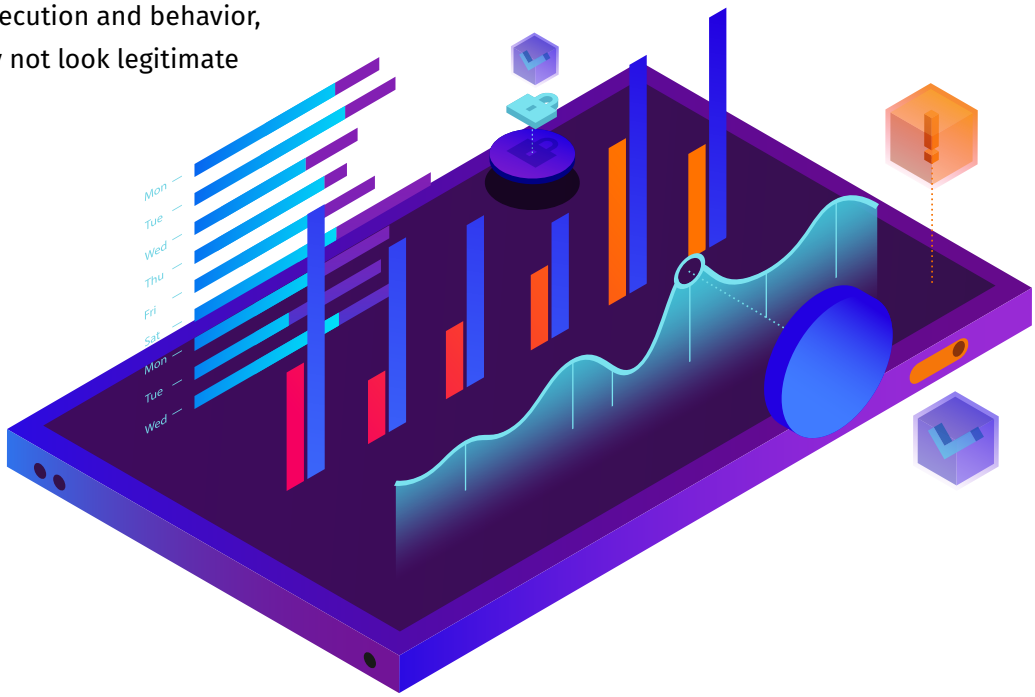
The limits of Whitelisting_

Blacklisting is practically as old as antivirus technology itself, and while blacklisting certainly blocks many simple threats, its limits are well known and easy to bypass. These days, with the rise of zero-trust security, many cybersecurity professionals take some comfort in seeing whitelisted apps, because that is one less application off their plate that they don't need to worry about. Therefore, many solutions simply skip over (even base their methodology around) whitelisted applications, trusting that when they run, they are not executing malicious behaviors or processes.

But it's cold comfort; whitelisting, just like blacklisting, has its limits, and modern threats can not only bypass whitelisting applications, they can exploit those apps in particular. The rise of fileless attacks have made goodware monitoring more essential than ever, as they abuse known, trusted applications to deploy attacks and spread to other machines unnoticed. And, because one application can trigger many events, it's necessary to monitor all application and process execution and behavior, seeking out anything that may not look legitimate in the hunt for attacks.

Luckily, there is a solution that moves beyond the limits of whitelisting, and it's active monitoring of all applications and processes. When endpoint activity is totally monitored, malware will always be identified and will never run, and goodware will not be misused for illegitimate goals.

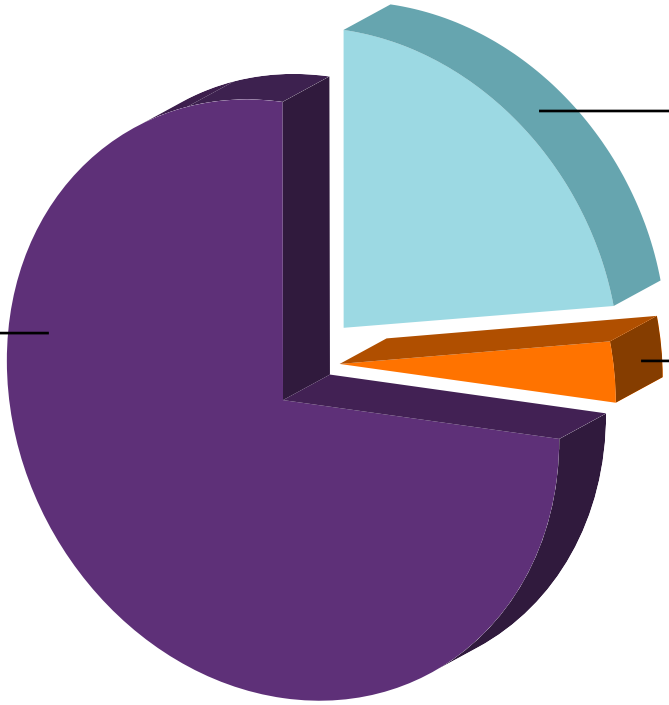
Any time an application attempts to run, or a library is loaded in Cytomic EPDR protected endpoints, the protection checks if it is trusted, locally or through a cloud-based reputation system, or generic signature—first in the local cache, then in the cloud-based knowledge (it also feeds the local cache for future queries). The cloud-based knowledge is continually being fed by the classification service (machine learning and PandaLabs analysts), with file hashes and their classifications as goodware, malware or potentially unwanted.



At the same time, machine learning is continually processing new evidence gathered from processes running at millions of endpoints being protected. However, as unknown files can be blocked until their classification is known, they are also run in a farm of physical (not VM) endpoints hosted in the cloud. It allows the machine learning system to learn from observing their real behavior over time. This new evidence is evaluated in order to classify them with maximum confidence and in the shortest time frame. Endpoint activity is also continuously monitored, in real-time, for all goodware executions and their context (events taking place while on execution, users executing each command or application, network traffic generated, data files being accessed, events before and after operations, etc.). All this evidence helps identify high confidence IoAs (Indicators of Attack), without false positives.

Application Monitoring and Execution

Distinct applications that run in the install base, on a monthly basis, per million machines, 2019 (approx.)



Applications Executed: **5 million**

18% of applications were newly identified by PandaLabs

0.6%–1.2% were classified as completely unknown malware that evaded any other layer of technology

The New Threat: Fileless Attacks_

This data confirms the global position on live hacking through the exploit and use of commonly whitelisted productivity tools, browsers, and OS components that are ubiquitous on the vast majority of endpoints worldwide. No application or executable on this list would ever be classified as suspicious, let alone malware, which make them perfect vectors for fileless attacks, live hacking, living-off-the-land (LotL) attacks, and more.

This list exposes the absolute necessity for anti-exploit technology. Note that there is no one common denominator for why each of these applications are chosen by attackers. For example, Microsoft IIS is exploited for its ability to spin up countless websites, while Microsoft Office macros open up the ability for screen and key logging, which is why context-based behavioral analysis is necessary to detect these attacks.

Top 10 Exploited Applications

The top-10 applications in which our technology detected exploit-based attacks.

#	Name	Executable	New Vulnerabilities, 2019 (CVE)	Vendor	Application Type
1	**Firefox**	firefox.exe	**105**	Mozilla	Internet Browser
2	**Microsoft Outlook**	outlook.exe	**7**	Microsoft	Email Client
3	**Internet Explorer**	iexplore.exe	**53**	Microsoft	Internet Browser
4	**Microsoft word**	winword.exe	**5**	Microsoft	Word Processor
5	**Internet Information Services (IIS) Manager**	w3wp.exe	**N/A**	Microsoft	Web Server
6	**Microsoft Excel**	excel.exe	**7**	Microsoft	Spreadsheet
7	**Adobe Reader**	acroRd32.exe	**N/A**	Adobe Systems	Proprietary File Reader
8	**Winamp**	winamp.exe	**N/A**	Nullsoft	Music Player
9	**Microsoft Access**	msaccess.exe	**N/A**	Microsoft	Database Management
10	**Google Chrome**	chrome.exe	**177**	Google	Internet Browser

Note: N/A means no new documented vulnerabilities in 2019. Older, but more recent or unknown vulnerabilities, may have been exploited. Source: https://www.cvedetails.com

One Solution, Many Layers_

Cyber threats are not alike, and where a technology stops one, it can let others through. It takes a combination of local signature-based technologies, cloud based-technologies and context-based behavioral analysis to detect and respond to cyber threats in 2020.

However, the numbers do not tell the whole story. While local signature-based technology may lead the pack in detections, in part it is because most attacks are known, and signatures are cost-effective, it is not stopping the same threats that context-based behavioral analysis is looking for, which are typically more sophisticated and potentially more dangerous. Therefore, applying multiple layers to combat a range of threats is the optimal approach for 2020, ensuring all threats are stopped as efficiently as possible.

Why Layered Security Matters

A look at where threats are stopped, and why using layered cybersecurity is essential. Data is based on a 30-day period from endpoints protected by our advanced solutions.

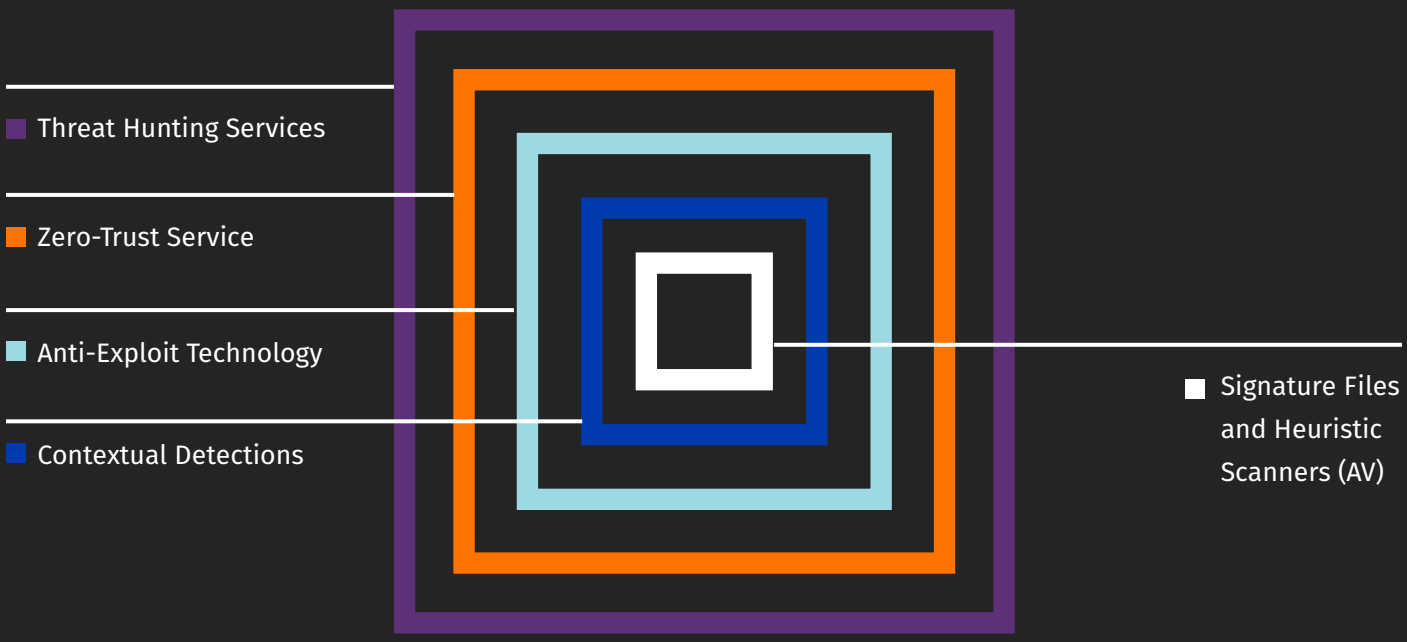
	Detection Technology Used	Description
Endpoints 47,648 **Incidents Detected** 598,952	Local signature	Checks for file hashes in a cache of known malicious elements hosted locally in the endpoint.
Endpoints 49,228 **Incidents Detected** 500,534	Cloud-based detection	Checks the cloud-based knowledge in real-time for malicious elements and feeds the local cache for future queries. The cloud knowledge is continuously fed by the 100% classification service.
Endpoints 7,828 **Incidents Detected** 250,733	Context-based behavioral analysis	Analysis of context of execution to identify indicators of attack at the endpoint. Denies execution of child processes and can block/kill parent processes. This technology also allows blocking attacks using administrative tools/scripts and detects in-memory attacks, e.g., detections of in-memory shellcode injection not mapped in the file present on disk.

Conclusion_

Cyber threats have never been more varied than they are in 2020. On any given day, an endpoint may encounter a phishing scam with link to a malicious file, acquire ransomware from a spoofed website, fall prey to an insidious fileless attack that keeps itself hidden in memory for weeks or months, or more.

At a time where the number of threats is growing and evolving constantly, IT professionals must deploy all the tools available to them to keep their networks' safe.

Cytomic EPDR:
The Market and Analysts-Recognized Solution to Threats in 2020 and Beyond



Cytomic EPDR is comprised of multiple layers of cybersecurity technology working concurrently to defend from and remediate cyberattacks. These layers can be grouped into **Endpoint Protection (EPP)** technologies and **Endpoint Detection and Response (EDR)** technologies.

Endpoint Protection Technology Layers_

Signature Files and Heuristic Scanners

Commonly known as traditional antivirus (AV) technology, this layer is proven effective against many common, low-level threats. It's optimized technology to detect known attacks, based on specific signatures, generic and heuristic detection and malicious URL blocking.

Behavioral Analysis

Tuned to notice abnormal, unusual resource and application utilization, this layer is essential for detecting malware-less and fileless attacks. It' s effective against script-based attacks, attacks using goodware tools (e.g., PowerShell, WMI, etc.), web browser vulnerabilities and other commonly targeted applications such as Java, Adobe Reader, Adobe Flash, Microsoft Office and more. Our contextual detection technology is continually improved and adapted to new threats, thanks to the complete visibility of Cytomic EPDR.

Anti-Exploit Technology

This technology specifically detects fileless attacks that are designed to exploit vulnerabilities. Complementing our contextual detection technology, it searches for and detects anomalous behavior, a surefire signal of exploited processes. The technology is important on all endpoints, but crucial on unpatched/waiting-to-be-patched endpoints and on endpoints with operating systems that are no longer supported.

+ 10.000

Events per day

3 Trillions

Events in the Data Lake

2 Millions

New binaries classified every week

Endpoint Protection Technology Layers_

100% Classification Service

Traditional EDR solutions identify malware, but nothing else, which introduces risk. Using our 100% Classification Service, Cytomic EPDR monitors not only all applications as such, but all running processes in the system. With this mature EDR technology (more than five years in operation), there are no suspicious items to investigate; it only allows those processes that are known and classified as trusted by Panda to run. This unique managed service is a core component of Cytomic EPDR and provides maximum protection without having to delegate important cybersecurity decisions to end users. In addition, this service provides superior protection should a previous layer be breached by stopping attacks on already-infected computers and lateral-movement attacks inside a network. It's AI-based approach ensures 99.98% of applications are automatically classified, while the remaining 0.02% are reviewed and classified by experts from Panda's laboratory. It is the only technology of its kind available on the market today.

Threat Hunting & Investigation Service

The only of its kind to be included standard in an EDR solution, Cytomic's Threat Hunting & Investigation Service (THIS) is an advanced, proactive service that detects compromised machines, early-stage attacks, and suspicious activities. When all else fails against extremely sophisticated attacks, which often can go undetected for months, Threat Hunting can root them out using a set of proactive procedures. Managed by Experts at Panda's Global Cybersecurity Team, THIS can find even the slightest of traces left by hackers in their attempt to take control of endpoints through living-off-the-land (LOTL) techniques.

The future of cybersecurity lies not in a single method of protection, but instead in a combination of effective, proven layers of security technology and advanced, forward-thinking solutions. This approach is the most efficient and effective way to proactively secure endpoints against threats known and unknown. And, as threats become increasingly complex in 2020, IT providers of all sizes need a cybersecurity solution that's consistently one step ahead of the hackers.

CYTOMIC

More info at_
cytomic.ai

Let's talk_
+34 900 84 04 07