Cyber-Resilience

The key to business security

CCS MEDIA

panda

Cyber-Resilience: The key to business security

Digital transformation affects daily life and the functioning of organisations in such magnitude that it has become a company's source of wealth and provides a competitive edge to countries. Appropriating this wealth is no longer a matter of armed wars, but of a "simple" digital transfer of that wealth, of the data assets that identify and differentiate the country in question. All it takes is a cyber-battle to attack key computers and obtain the information necessary to overthrow a government or to take away its competitive advantage.

In the context of security, cyber-resilience refers to the ability of an organisation to maintain its main goals and integrity against the latent threat of cybersecurity attacks.

A cyber-resilient company is one that can prevent, detect, contain and recover, minimising exposure to an attack and its impact on business, against countless threats to data, applications, and IT infrastructure. Especially against devices, where the organisation's most valuable assets reside, since reaching them also implies attacking the integrity of identities and users.

As hazards increase, traditional approaches to maintaining cyber-resilience are no longer enough. Many entities survive in a precarious equilibrium, and the slightest alteration, however small in relation to the size of the organisation or the importance of its activities, can precipitate a crisis. To avoid collapse, cybersecurity management will need a thorough revision and implementation of new protection models.

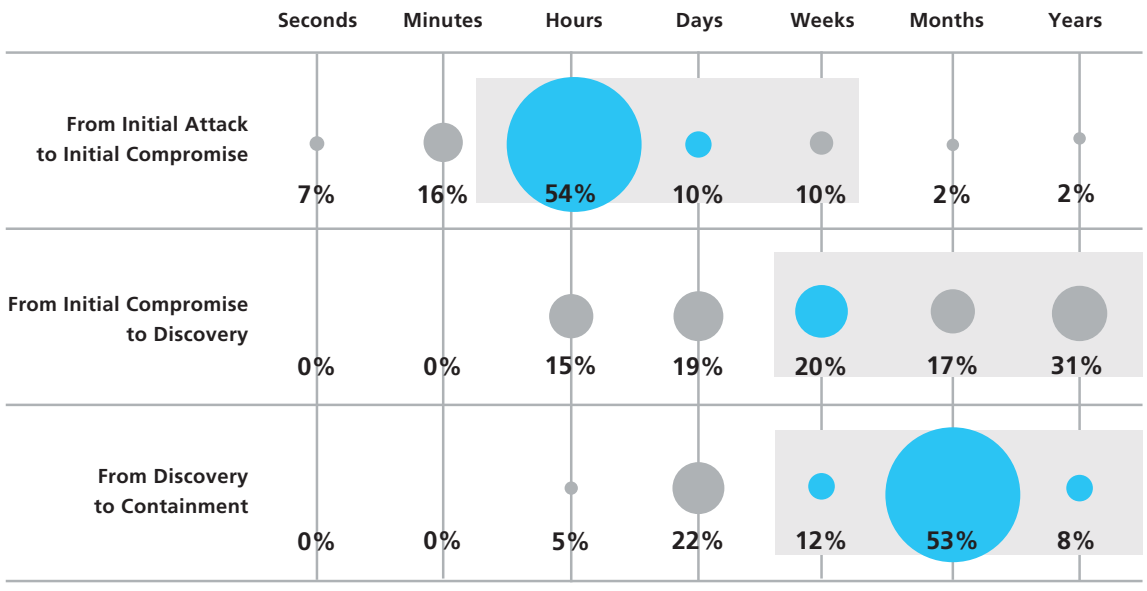
Until recently, financial entities and governments were the main targets of cyberattacks. Today, the development of businesses of any size and sector depends to a greater or lesser extent on the Internet and consequently, the threat has become universal. As these dangers increase, current approaches to maintaining cyber-resilience no longer work. Cybersecurity management is in need of a thorough revision with new and improved security models.

The paradigm shift toward a resilient company consists in avoiding the compromise of company assets and detecting attacks before there is damage with a limited response time. Now is the time for the materialisation of tendencies such as Threat Hunting, Forensic Investigation to identify the root cause of the attack, Endpoint Detection and Response (EDR), and constant endpoint monitoring. It is fundamental to generate forensic data in real time in order to thoroughly investigate incidents.

At the same time, a company that is mature in resilience will admit that failures and errors do occur and has the means to restore normal operations to secure assets and its own reputation. In short: the organisation is able to emerge strengthened from the incident, applying changes that improve its defence situation.

Let's Talk

Call 01 253 0180 to discuss the key to business security



Data from the 2016 DBIR

2018 Hiscox Cyber Readiness Report
https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf

Challenges for organisations to become cyber-resilient

Every entity, company, organisation is subject to tensions derived from events, changes, and incidents that occur in their environment. These situations are new challenges whose resolution will affect the functioning of the organisation until the situation can be managed through automation.

When it comes to the security of organisations, the situation in question requires a reaction that involves a new focus on the security program throughout the organisation. Companies must identify assets with the greatest value and establish a new model of security governance that centralises all cybersecurity efforts throughout the company. It is here that the head of this team gains visibility and participates in the decision making of the organisation, forming part of the executive team.

Moving towards cyber-resilience

The capacity to recover quickly from difficulties and end up stronger

7% — In 2018, global information security spending is projected to rise by just 7% to $93bn, while the surface area of attack is increasing exponentially.

Invest in cyber security
Without investment, the readiness gap will only intensify.

36% — Only 36% of cyber security professionals have a direct reporting line to the CEO.

Gain a seat at the table
Without greater visibility, cyber security needs will continue to be reprioritsed.

35% — By some estimates, only 35% of cyber security professionals vet ecosystem partners for cyber-integrity and preparedness.

Build a more robust ecosystem
Without greater visibility, cyber security needs will continue to be reprioritsed.

1.5m — The global cyber security workforce is expected to have over 1.5m unfilled positions by 2020.

Improve the talent pipeline
Hire and train more talent.

1/2 — Cyber security professionals estimated that over half of threat alerts are improperly reprioritsed by systems and must be manually reprioritised.

Make threat detection more accurate
Systems must be honed for an increasingly dangerous digital environment.

Figure 1. Technological progress is undoubtedly driving the growth of companies. Organisations and the world in general are more connected than ever and the pace of current technological development is the most advanced that has ever existed. This interconnectivity brings both opportunities and risks.

Complexity of IT infrastructure

Growing complexity is making companies more vulnerable. While cybercriminals perfect their skills, companies become increasingly digital, opening new doors to vulnerabilities and cyberattacks. Assets that range from new product designs to distribution networks and customer data are now at risk. Digital connectivity is also becoming increasingly complex, using a simple digital connection to unite thousands of people, applications, servers, workstations, and other devices. An organisation's assets are now more exposed than ever before.

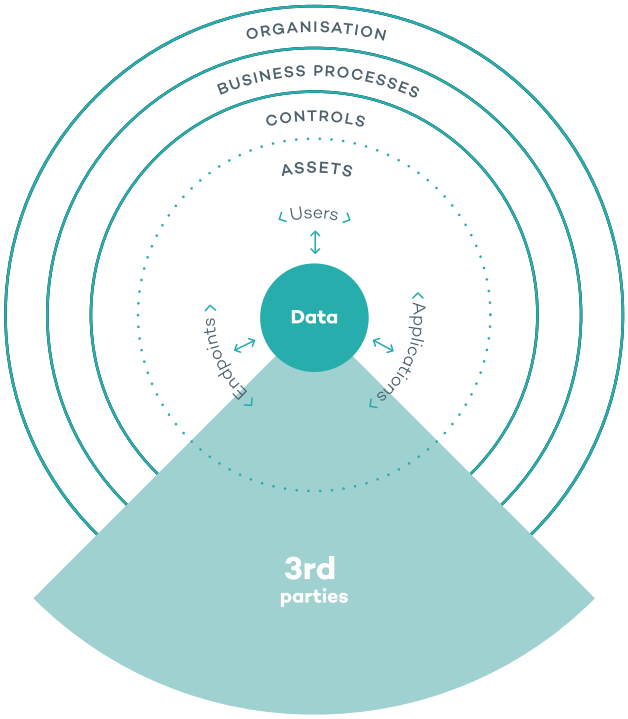
Adoption of Cyber-resilience

With this complex and real panorama in mind, how can companies intending to protect their assets in the most efficient way possible achieve this more adaptive, complex and collaborative approach in their struggle?

Cybersecurity should be treated as a problem of corporate risk management, not as a problem embedded in IT. The key elements of its management include

- Knowing and implementing the best defences against current and potential threats.
- Being prepared for a moment when adversaries can bypass all security technologies and detecting them, containing them and remedying their actions as soon as possible to minimise corporate damage.
- Adopting a crisis position which continuously and actively seeks threats and detecting vulnerable points.
- Managing at the corporate level any communication of a breach.
- Defining and constantly executing initiatives to minimise risk and reinitiate the cycle of continuous improvement in the management of corporate security.

The complete approach to cybersecurity management in companies



The complete approach to cybersecurity management in companies.

Adaptation is essential. The organisation's processes, technologies, tools and security services should be reviewed and adjusted as threats evolve in a process of continuous improvement based on wariness. Being resilient implies that this adaptation has to be carried out in the minimum time interval, at the maximum speed, even in real time.

Companies must seek out and mitigate their risk at all levels. Creating a complete record of all assets, from data to applications, and monitoring all actions that are carried out. Companies must take advantage of the tools and services that automate these tasks of profiling, cataloguing, and monitoring their assets (humans, data, infrastructure) for prevention and/or early detection of adversaries.

Assets	Threats	Control
 Data	Data breach Misuse or manipulation of information Corruption of data	Data protection (e.g. encryption) Data-recovery capability Boundary defense
 People	Identity theft "Man in the middle" Social engineering Abuse of authorisation	Controlled access Account monitoring Security skills and training Background screening Awareness and social control
 Endpoints	Malware	Control of privileged access Monitoring processes Malware execution prevention Network controls (configuration, ports) Inventory Secure configuration Continuous vulnerability assessment
 Applications	Manipulation of software Unauthorised installation of software Misuse of information system Denial of service	Email, web-browser protections Application-software security Inventory Secure configuration Continuous vulnerability assessment

Risks and controls to be implemented at all levels, from data and entities to endpoints and the applications that run on them.

Establishing a "resilience cycle".
Organisations need to understand and adopt the "resilience cycle" process, which will help security teams to continually build on the experience of blocked and/or detected threats.

This requires that they learn and adapt to the key phases of resilience:

- **In the pre-incident phase,** through the ability to better prevent and resist threats, including advanced technologies that detect known and unknown or zero-day malware.
- **During its execution**, by reacting quickly with detection, containment and response to sudden events that threaten the organisation to minimise its impact on business; taking advantage of the new paradigms that arise as a result of the monitoring and visibility capabilities that Endpoint Detection and Response (EDR) solutions provide.
- **In the post-incident phase**, by absorbing impacts while continuing to achieve strategic security objectives and reconstructing the operating environment in such a way that future sources of interruption are eliminated. This is what is called a "reduction of the attack surface".

Prevention, detection and response.
It's best to assume that sooner or later, every company will be compromised by a cyberattack. At that moment, the time of detection and response to the incident is critical. A balance must be found between responding and recovering the service level for the business as soon as possible and analysing the incident, the origin of the attack, and establishing measures to avoid it in the future.

As we said in the introduction, cyber-resilience refers to the ability of an organisation to maintain its main goals and integrity against the threat of cybersecurity attacks. A cyber-resilient company is one that can prevent, detect, contain, and recover, minimising the exposure time and the impact on business, of innumerable serious threats against data, applications, and IT infrastructure — and especially against the endpoint, where the organisation's most valuable assets reside, and against the integrity of user identity.

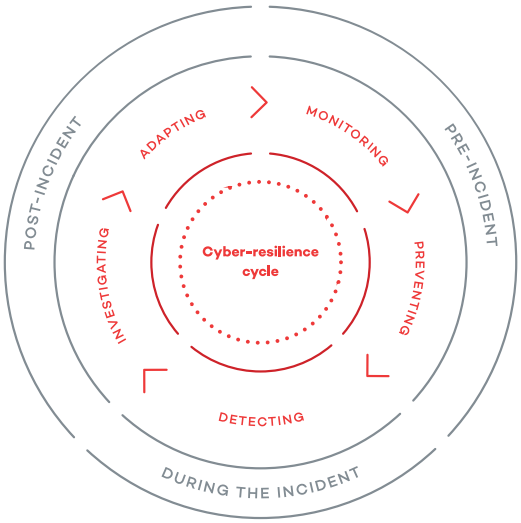
Although we are aware that total prevention is never guaranteed, companies should strive to minimise the cost of cyberattacks by strengthening prevention in pre-execution phases, preventing the attacker from executing malicious code on workstations and servers.

Equally important is complementing a cybersecurity strategy with quick detection and response in execution and post-execution phases to identify the damage, restore systems, and return operations to normal as soon as possible. Meanwhile, weaknesses and vulnerabilities can be newly detected in order to correct them and thus avoid the attack in the future.

Implementing continuous processes to detect anomalies in user, endpoint, and application behaviour.

When it comes to minimising the impact on business, the time that passes between a breach and its discovery, is the decisive factor in the overall cost of the incident.

Monitoring, visibility of the endpoint, and technologies that allow the automation of the detection and investigation can drastically reduce this amount of time. Detecting anomalous or malicious behaviour in the profiles of users, applications, and the devices, which are symptomatic of the presence of a hacker in the systems, is crucial.



The cycle of continuous improvement of the cyber-resilience that every organisation should develop and implement.

Let's Talk

Call 01 253 0180 and ask about a free trial

The management of cyber risk requires comprehensive and collaborative management.

Many companies distinguish between physical security and IT security, between IT and Operations, between business continuity management and data protection (e.g. encryption) and between internal and external security. In the digital age, these divisions are obsolete. Scattered responsibility can put the entire organisation at risk. Redundancies must be limited, and responses made quicker in order to increase resilience in general.

The following figure was taken from the Gartner report from January 28, 2018: **"Improve Operational Resilience Through to More Collaborative Incident Response Process"**. It illustrates the areas of the incident management and response cycle where collaboration and coordination is necessary — the boxes in grey functions where the specific capabilities of each department, operations and security apply - the box in red — with the aim of detecting and responding in the shortest time possible while identifying areas for improvement:

Companies that adhere to these principles tend to be much more resistant to attacks than ones that don't.

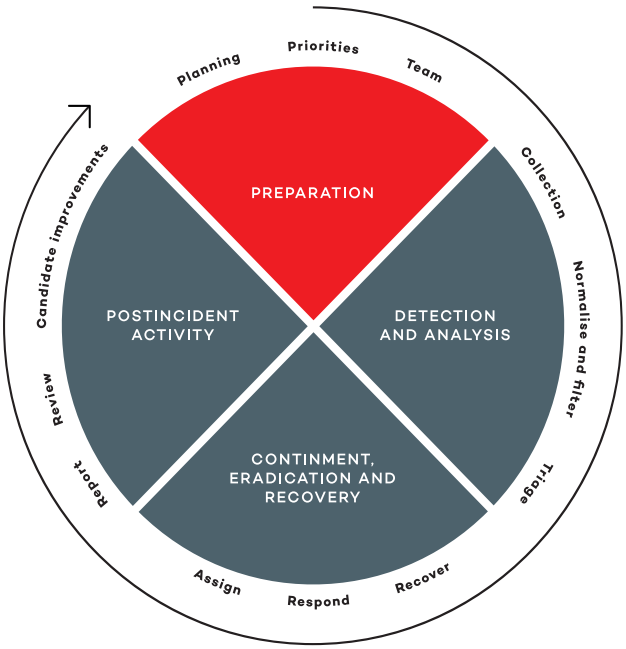
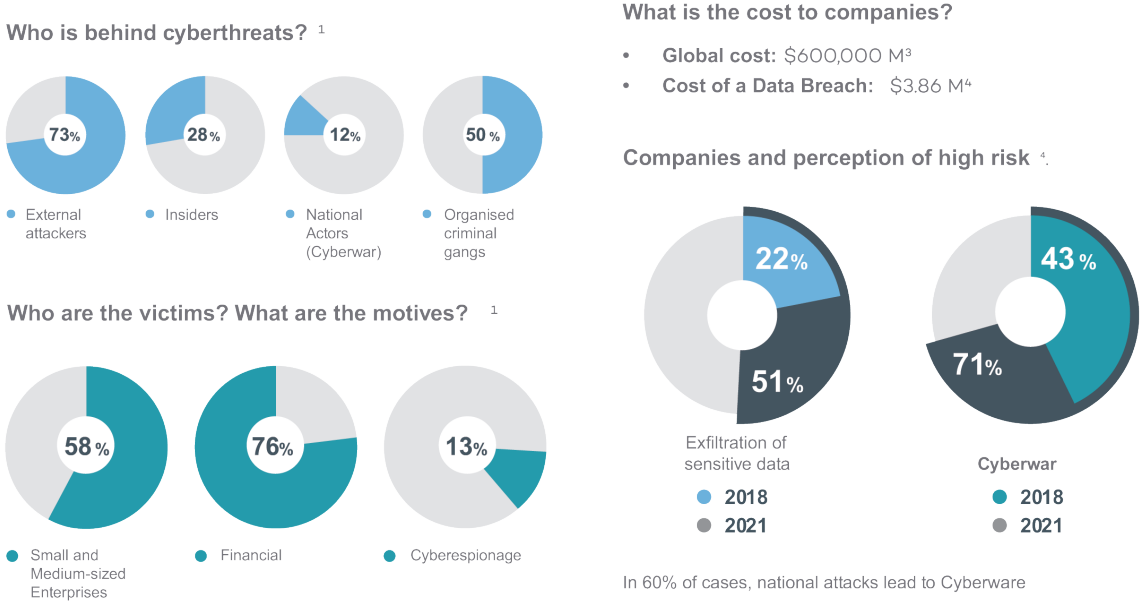


Figure 7. Coordination between Operations and Security teams when managing a security incident. Gartner: "Improve Operational Resilience Through to More Collaborative Incident Response Process". January 25, 2018. Analysts: Matthew T. Stamper, Kenneth Gonzalez

Corporate Cybersecurity



Endpoints are the new perimeter

Mobility, processing and cloud storage have revolutionised corporate environments. **Endpoints are the new perimeter.** Security solutions on endpoints must be **advanced, adaptive and automatic**, with the highest levels of prevention and detection of attackers, who will sooner or later manage to evade preventive measures. Such solutions must also offer agile tools to respond quickly, minimising damage and reducing the attack surface.

Professionalisation of hackers

Enemies are **increasingly sophisticated** and **growing in number,** the result of their professionalisation, the democratisation of technologies and the continuous leaks of cyberintelligence.

Next-generation cyberthreats are designed to slip past **traditional solutions** completely undetected.

Cyberdefense in organisations

Hackers are targeting computers and servers, where the most valuable assets of organisations reside, and **security teams have great difficulties in defending them**. **EDR** (Endpoint Detection and Response) applications, far from being the solution, **increase workloads**, as there is no automation of threat prevention, detection, containment and response. **Improving the security posture** of your company, **without increasing operating costs** inevitably means **automating the prevention, detection and response capabilities** in endpoints.

Endpoint Detection and Response Solutions (EDR)

EDR Solutions monitor, log and store the details of endpoint activity, such as user events, processes, changers to the registry, memory and network usage. This visibility uncovers threats that would otherwise go unnoticed.

What are the hidden problems with EDR solutions?

Multiple techniques and tools are used to search for security anomalies in events and confirm or reject alerts. All of this requires human intervention.

EDR solutions require 24/7 supervision, and rapid response from highly qualified personnel.

However, such resources are expensive and hard to find. Short-staffed organisations with low budgets are unprepared to take advantage of the benefits of EDR solutions on their own. Personnel find themselves with greater workloads deriving from the implementation and operation of these solutions, instead of supporting them in what matters: improving the security posture of their organisation.

Conclusion

The digital transformation that is taking place in almost all aspects of our lives has a special importance when looking at the evolution of organisations, interconnected devices, applications, tools, and productive processes.

From a competitive point of view, the search for optimisation using new and improved instruments, means, capacities, and processes, is the origin of almost all initiatives in both the private and public sectors.

However, there is another aspect that we cannot ignore on the road to digital transformation: the transformation must also be deeply invested in security and business risk management.

Even more so, given the evolution in number and sophistication of threats. Cybercrime is an attractive and very lucrative business. Attackers have increasingly more and better resources — both technical and economic — which allows them to develop increasingly sophisticated attacks. All this results in more complex and dynamic threats, in addition to a greater number of attacks.

Equifax, CCleaner, WPA2, Vault7, CIA, KRACK, NSA, WannaCry, Goldeneye/NotPetya, Meltdown/ Specter, the election hacks... These are some of the very recent protagonists of massive infections, theft, personal data leaks, ransomware attacks, hacked applications to launch attacks against an entire country or carry out attacks directed against large specific companies, and vulnerabilities that affect billions of devices.

With real cases like these, it is not surprising that 75% of companies (according to a recent survey by McKinsey15) consider that cybersecurity is a priority for the proper development of their activity. The "stress situation" described above requires a reaction that involves a company-wide focus on the security program, which develops and strengthens a business attitude of cyber-resilience.

Cyber-resilience is the ability of an organisation to maintain its primary goals and integrity in the face of the latent threat of cybersecurity attacks.

A cyber-resilient company is one that can prevent, detect, contain and recover, minimising the exposure time and the impact on the business of countless serious threats against data, information and applications and IT infrastructure. Especially against devices, where the company's most valuable assets reside. Reaching devices also means attacking the integrity of identities and users.

In order to become cyber-resilient, the new approach to security must cover at least the following points:

1. **Manage cybersecurity as a problem of corporate risk management,** not as an IT problem, **and adopt the stance of a "resilience cycle".** The key elements of the cyber-resilience cycle include:

   a. Prioritising the most valuable assets of the organisation.

   b. Prioritising, knowing and understanding the most relevant adversaries and threats for each organisation.

   c. Knowing and implementing the best defences against current and potential threats.

   d. Being prepared for a moment when adversaries can bypass all security technologies and detecting them, containing them and remedying their actions as soon as possible to minimise corporate damage.

   e. Adopting a crisis position which continuously and actively seeks threats, and detecting vulnerable points that can later be used by threat actors to reduce the attack surface.

   f. Managing at the corporate level any communication of a breach.

   g. Defining and constantly executing initiatives to minimise risk and reinitiate the cycle of continuous improvement in the management of corporate security.

2. **Strengthen the four key pillars: prevention, detection, Threat Hunting, and containment and response and reduction of the attack surface.**

3. **Adapt continuously to the new techniques and tactics of hackers and other attackers.** Being resilient implies that this adaptation must be carried out in the minimum time interval, at the maximum speed, even in real time.

4. **Prioritise and mitigate risks at all levels of the Organisation.** Companies must take advantage of managed tools, products, and services that automate these functions to profile, catalogue, monitor activity (human, data, and infrastructure), and learn from them so that security systems are predictive and accelerate the prevention and/or early detection of adversaries by reducing the level of organisational risk without incurring disproportionate costs, especially operational ones.

5. **Manage cyber risk through comprehensive and collaborative management**

Panda Adaptive Defense 360

Panda Adaptive Defense 360 is an innovative cybersecurity solution for desktops, laptops and servers, delivered from the cloud. It automates the prevention, detection, containment and response against any present or future advanced attacks, zero-day malware, ransomware, phishing, memory exploits and malware, less attacks, inside and outside the corporate network.
It differs from other solutions in that it combines the widest range of protection technologies (EPP) with automated EDR capabilities, thanks to two services managed by Panda Security experts, and delivered as features of the solution:

- **100% Attestation Service**
- **Threat Hunting and Investigation Service**

Thanks to its cloud architecture, the agent is light and does not impact the performance of endpoints, which are managed through a single cloud console, even when not connected to the Internet.

Panda Adaptive Defense 360 integrates Cloud Protection and Management Platforms (Aether), which maximise prevention, detection and automated response, minimising the effort required.

Let's Talk

Call 01 253 0180 and
ask about a free trial

Benefits

Simplifies and minimises the cost of advanced and adaptive security

- Its managed services reduce the cost of expert personnel. There are no false alarms, no responsibility is delegated.
- The managed services learn automatically from the threats. No time is wasted with manual settings.
- Maximum prevention on endpoints.
  Operating costs are reduced practically to zero.
- There is no management infrastructure to install, configure or maintain.
- Endpoint performance is not impacted as it is based on a lightweight agent and cloud architecture.

Automates and reduces detection and exposure time

- Prevents the running of threats, zero-day malware, ransomware and phishing.
- Detects and blocks malicious activity in memory (exploits), before it can cause damage.
- Detects malicious processes that slip past preventive measures.
- Detects and blocks hacking techniques and procedures.

Automates and reduces response and investigation time

- Automatic and transparent remediation.
- Recovery of endpoint activity – immediate recovery of normal activity.
- Actionable insights into attackers and their activity, speeding up forensic investigation.
- Helps reduce the attack surface.
  Supports improvement to security posture and maturity.

Gartner peerinsights customers' choice™

"Gartner Peer Insights Customers' Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates

Gartner Peer Insights Customers' Choice badge is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner Peer Insights Customers' Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates"

Best Endpoint Detection and Response Solutions of 2019 as Reviewed by Customers

Customers' Choice - Jan 2019

Panda Security is the leading European vendor of EDR systems, with European shareholders, headquarters, technology and cloud platform. The company, however, has a solid presence in more than 80 countries, including The US, and more than 7.5 million clients worldwide. Consistently maintaining a spirit of innovation, Panda has set a number of historical milestones in the security industry. Today, as a leader in advanced cybersecurity services, the company's aim is to prevent cybercrime and to eradicate advanced threats in all size organisations. Panda's Cyber-Intelligence Platform broke into the market as the first and only cybersecurity solution to combine the most effective advanced protection technology and the latest detection and response capabilities with the ability to automatically classify all running processes.

"A product that is great on visibility and proactive protection even against direct attack" — IT Assistant Manager in the Education Industry.

Let's Talk

Call 01 253 0180
and ask about a free trial
www.ccsmedia-ireland.com