Kaspersky Enterprise Cybersecurity

KASPERSKY lab

A Buyer's Guide to Investing in Endpoint Detection & Response for Enterprise 2017-2018

www.kaspersky.com
#truecybersecurity

Proven.
Transparent.
Independent.

Contents

Introduction 1

All about Endpoint Detection and Response 2

Defining EDR 5

The Top 5 challenges when initiating an EDR project 8

1. Endpoint data: too much visibility 8
2. Responsibility for aggregated and stored data 9
3. Detection: manual hunting vs automated engines 10
4. Don't just React - Respond 12
5. Prevention – EDR or EPP? 13

The Future of Enterprise Endpoint Security 14

Immediate Recommendations 15

Introduction

One key business goal of any organisation is to maintain the constant availability of data and systems that can be trusted for decision-making purposes. The evolving threat landscape has resulting in an increased focus, right up to board level, on cybersecurity. IT operational and security teams should demonstrate a comprehensive, cohesive approach in their response to security incidents and data breaches.

Cybersecurity is now one of the 'Top-3' priorities recognised by senior management in their pursuit of business continuity leading to business success.

Business leaders today need an understanding of the cyberthreat landscape specific to their organisations. They should be asking questions like these:

- Does my organisation understand the main threats and security risks to our industry sector and to ourselves?
- Can we quickly detect and halt cyberattacks?
- How do we position the reduction of cyber-risk within our overall business development strategy?

Endpoints at the sharp end

Corporate endpoints – your servers, workstations, mobile phones etc – are where that synergy between data, users and corporate systems that generate and implement business processes takes place, and these myriad individual devices remain the key element in any network from both a business and a security point of view.

To protect these endpoints, and to prevent their use as illicit entry points into your infrastructure, you should expect your information security teams to be looking at adopting processes and technologies associated with advanced detection, threat hunting, IoC-scanning, malware analysis, incident forensics, global threat intelligence implementation and the establishment of a formal Incident Response process.

But where do you start? Jump on the advanced machine learning bandwagon? Improve your threat hunting? Focus on growing your monitoring and SOC? Better perhaps to cover these areas and more with one of the new Endpoint Detection and Response (EDR) solutions. But what exactly can you expect from EDR, and what type of solution should you go for?

This Document can help you to choose the EDR solution that will deliver for you. Our goal is to highlight the vital differences between various types of EDR capabilities available on the market, and to help you identify the technologies which will prove most valuable in securing business continuity and security in your organisation.

All about Endpoint Detection and Response

A new approach to endpoint security

To prevent attacks, protect your perimeter. It always sounded reasonable – if your IT perimeter is well defended, endpoint protection becomes just one more layer in your overall security strategy.

But this approach falls short in a world where, thanks to technologies like mobile devices, connected devices (IoT) and cloud computing, defining let alone defending your IT perimeter becomes a challenge, and where the evolution of threats has rendered a defensive perimeter-based approach obsolete.

Targeted attacks, a sharp increase in complex penetration techniques, fileless malware and the use of legitimate software, the stolen credentials of normal users, legitimate rights usage, exploitation of security policies issues and misconfigurations - all these have led organisations to recognise the importance of integrated security solutions and strategies. This in turn has led to the growth of SIEM implementation and Security Operational Centers (SOCs). Corporate cybersecurity has become proactive, multi-faceted and highly specialist – of necessity.

The world is changing, and is ready to embrace a new endpoint security paradigm. The focus has shifted back to the endpoint. There have always been far-sighted IT Departments who have treated every endpoint as requiring its own security perimeter. And, thanks in part to organisations who have **not** taken this approach, and whose poor visibility over individual devices has led to low overall security levels, endpoints have never ceased to be the main initial target for cybercriminals.

Becoming more proactive

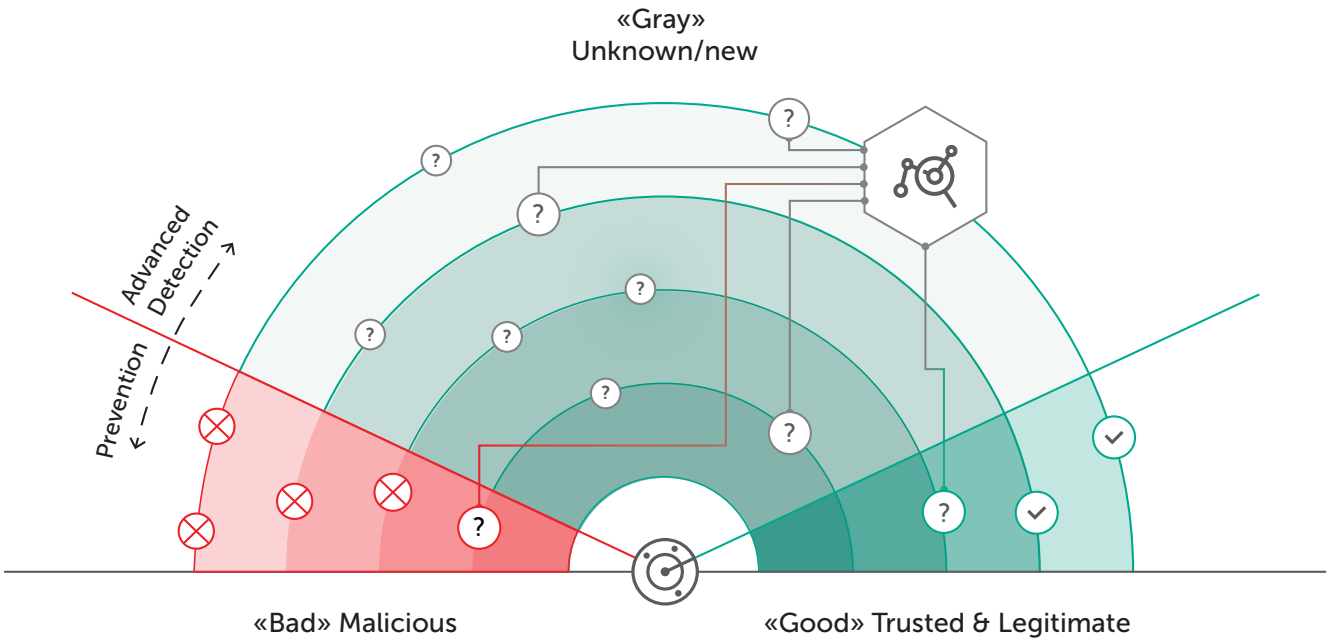
Meanwhile, regulators are introducing new requirements (GDPR, PCI DSS etc.) which may call for continuous monitoring and incident recording over every endpoint in the network. For most enterprises, the number of events/incidents recorded by their current security solution keeps escalating, so that verifying and analysing every event recorded becomes an issue in itself. It doesn't help that security experts with the necessary skills in Reverse Engineering, Malware Analysis, Digital Forensics and Incident Response to handle these tasks are now at a premium, and are not easy to come by.

At this point, most security processes concentrating on advanced threats, and most SOC monitoring approaches, are essentially alert-driven and reactive. Security officers wait for evidence of a breach before alerting the security analyst, after which the incident response team can take action. At best, incident responders identify the artifacts of an attack at the latest stage of the 'kill chain': at worst, they simply wait to tally the damage, sometimes months after systems were breached. This is clearly unsatisfactory. So organisations are reviewing their security processes, particularly in terms of proactive incident detection as well as response.

How does this affect endpoint solutions?

Threat Hunting - helping to uncover advanced threats hiding within the organisation, using proactive threat search capabilities and carried out by highly qualified and experienced security professionals.

The latest generation of endpoint solutions focuses on the effective detection of new threats coming into the organisation, patrolling and analysing events in the 'grey zone' where unknown, undefined threats may be lurking – we're talking about proactive 'threat hunting'.



Beyond endpoint protection

Effective threat hunting relates directly to the capabilities of a mature SOC. Upgrading bought-in security solutions is not enough. New requirements can't simply be imposed on traditional Endpoint Protection (EPP) solutions – they will not fit or function effectively.

Let's take look at some key issues effectively closed by traditional EPP, and the new challenges that endpoint security now faces:

Issues of control and protection, closed by traditional solutions EPP:	New advanced challenges for endpoint security:
How to automatically protect (both prevent and roll-back) against existing threats, including ransomware and crypto-lockers	How to proactively seek out intrusion evidence such as Indicators of Compromise over the entire network in real time
How to centrally manage and enforce security controls for web/apps/devices	How to detect and remediate an intrusion before the intruder has a chance to cause significant damage
How to centrally manage vulnerability assessment and patch management processes	How to correlate alerts from network security controls in order to understand what's happening on the endpoint in real time
How to protect corporate data and information on devices	How to validate alerts and potential incidents discovered by security solutions
How to deploy endpoint-level web and mail protection policies	How to rapidly investigate and centrally manage incidents across thousands of endpoints
How to provide endpoint users with specific sets of security domains tailored to their own needs	How to make the incident response process (manual work, level-3 skills, alerts overload etc.) less expensive by automating routine security team operations

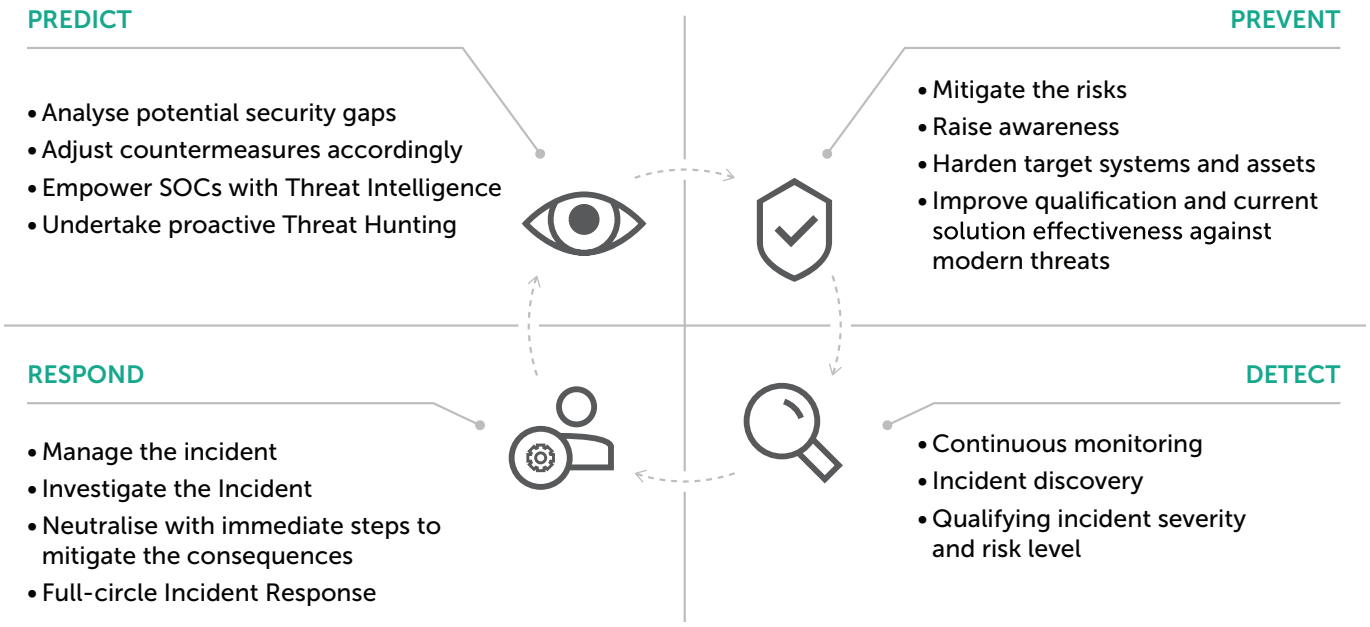
How can these new challenged be addressed?

Your endpoint cybersecurity strategy: adaptive, advanced, predictive

Harder to detect and - often - even harder to eliminate, targeted attacks and advanced threats call for a comprehensive, adaptive security strategy.

One of the most effective Adaptive Security Frameworks is founded on the viable security architecture described by Gartner. Its approach is to provide a cycle of activities in four key areas: Prevent, Detect, Respond, and Predict.

- **Prevent** – both blocking common threats and hardening the core systems to decrease the risk of advanced threats
- **Detect** – rapid discovery of activities that could signal a targeted attack or existing breach
- **Respond** – precisely contain the threat, perform investigations and respond appropriately to attacks
- **Predict** – know where and how new targeted attacks could appear



Adaptive Security Model

Essentially, this assumes that traditional prevention, especially for endpoints, should function in coordination with advanced detection technologies, threat analytics, response capabilities and predictive security techniques. The result is a cybersecurity system that continuously adapts and responds to emerging enterprise challenges.

Multi-layered, prevention-based technologies are still a key element in this new, proactive approach to guarding against targeted attacks. But if the attacker is sufficiently highly motivated, and perhaps even hired by a third party to conduct a successful attack, a prevention-only approach will not be enough. You must also be able to quickly identify threats, make decisions and anticipate the possibility of penetration, while simplifying current manual operations and automating response tools.

Defining EDR

Key features of an EDR-like solution

As we've seen, Gartner defines EDR solutions as having the following primary capabilities:

- detect security incidents
- contain the incident at the endpoint, such that network traffic or process execution can be remotely controlled
- investigate security incidents
- remediate endpoints to a pre-infection state

Endpoint Incident Detection

Detect security incidents by **monitoring of endpoint activities** and objects, policy violations or by validating externally fed indicators of compromise (IOCs)

Incident Investigation

Investigate security incidents. The investigate function should include a **historical timeline** of all primary endpoint events to determine both the technical changes that occurred and the business effect

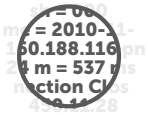
(privilege escalation, spread, exfiltration, geolocation of C&C and adversary attribution if possible)

Incident Containment & Response

Contain the Incident at the endpoint and **Remediate** endpoints to a pre-infection state.

Remove malicious files, roll back and repair other changes or - can create remediation instructions that can be made available for other tools to implement

Forensics Data Collection

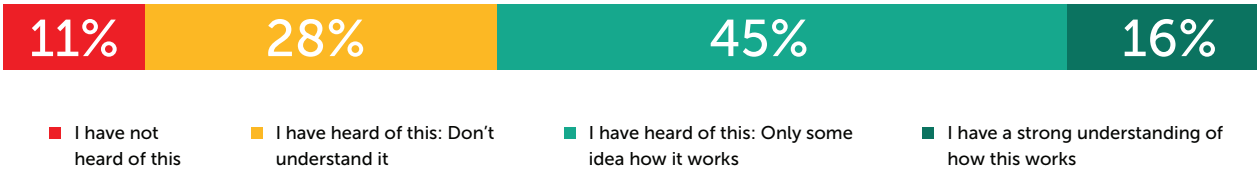


Collect datasets, RAM dumps, HDD snapshots etc. for further analysis

How well do organisations understand the workings of EDR, and how these technologies contribute to business continuity? A Kaspersky Lab survey among the enterprise organisations over 2016 produced some disturbing results.

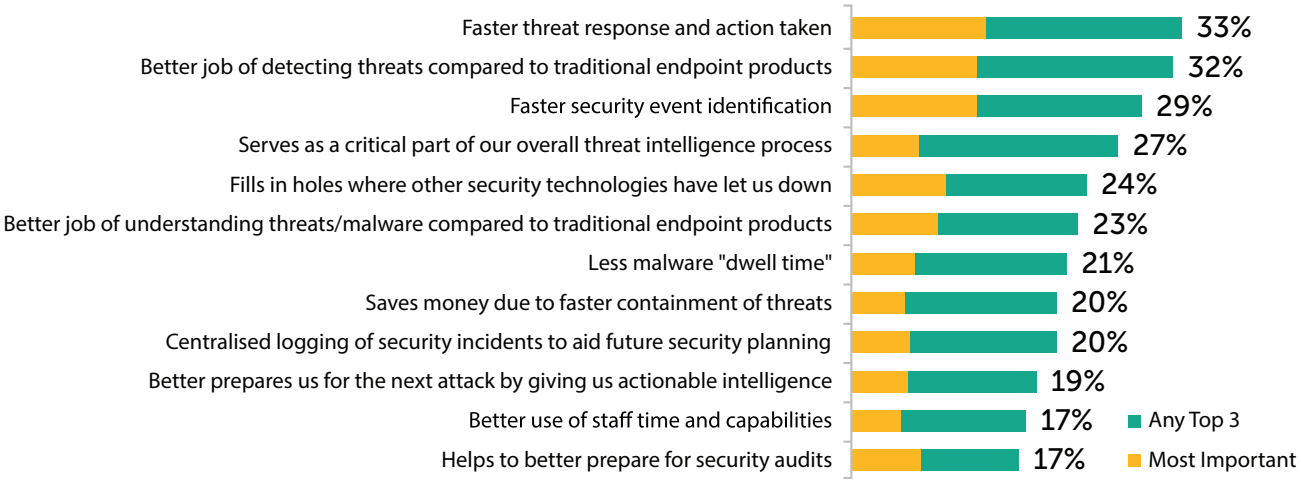
Survey question: 'How well do you know the EDR class of solutions?'

Response:



Source: IT Experts In Businesses With Over 250 Employees

At the same time, interviewed representatives of companies clearly formulated the basics of their expectations and the results that they would like to see from the use of EDR solutions in their organisations:



This combination of limited understanding and clear expectations is a concern. EDR solution providers are naturally keen to meet these expectations, developing 'kill-features' which promise much and look exciting at the pilot stage, but which often prove very much less practical and cost-effective when incorporated into the customer's new or already established processes of incident response, investigation or threat hunting.

As a result, EDR is already viewed in some quarters with suspicion.

The rise and fall of Endpoint Detection and Response solutions

Early-adopters of EDR solutions are not always, alas, the technologies' biggest fans. There were shortcomings with many of the very first EDR solutions, resulting in some customers facing disappointment and frustration.

Unfortunately, there's not as yet an established comparative analysis or independent report laying out all the key functionalities and possible variations of EDR technologies available in the market today. And many 'first generation' products in this still-immature market initially failed to deliver in practice what experts and organisations had expected.

Most solutions started with some 'kill features' instead of complex functionality. Instead of an integrated solution with the ability to unify and automate network security threat intelligence, threat hunting, anti-malware, incident response and forensics capabilities, EDR proved in practice to be a set of analytical and research tools. And this technology toolkit turned out to be both costly for what it was and extremely tough for the average security professional to master.

Some EDR solutions also failed to deliver on efficiency promises. When responding to a malware incident, an EDR solution will gather information from endpoints – signatures and malware behaviour – which can be used to identify future infections. But if the solution is not tightly integrated with detection technologies and security systems, there's a high risk of overlap and duplication, actually generating more manual processes and hampering workflow, instead of improving efficiency and effectiveness. The EDR simply becomes an additional storage silo of security-related data - data which can't in itself tell you how the event originated or how to stop it recurring. Without root case resolution built into the workflow, an organisation can't remediate conclusively and reduce the risk of a recurrence.

Another shortcoming has been that some solutions initially on the market were not really designed to discover or investigate APTs. To do this, EDR owners still needed to outsource activities to experts – possibly those belonging to the vendor – or to purchase expensive additional training. If an external incident response team must be brought in whenever a breach is identified, the cost-effectiveness of the original EDR solution may well come into question.

A growing trend has been the use of cloud versions of EDR, with certain logs and data being transferred to the vendor's cloud rather than held on installed agents or a centralised repository. But this has tended to result in the generation of more incidents, with slower reaction times (and occasionally none at all).

However, much of this is in the past, and those currently contemplating the EDR market should not judge the potential outcomes of their investment by the experiences of those early pioneers. Today the market has grown and become more mature.

So what should you be looking for in EDR today, and what should be taken into account? Let's look at 5 challenges that you need to consider when starting up your EDR project.

The Top 5 challenges when initiating an EDR project

There are inevitably going to be new challenges for organisations embracing any new technology or unfamiliar processes. And as EDR solutions are more expensive than their traditional EPP counterparts, justifying your investment in EDR in terms of added value, when weighed against the costs of a SIEM or forensic tools for example, can be a complicated business.

The core capability of an enterprise-grade EDR is **the ability to assist the security team with question-driven investigations:** hunting tips are iterative and start with questions or hypotheses – in order to achieve visibility. An initial question or hypothesis might be based on the steps of the cyber-kill chain and be something like "Is data exfiltration or malicious communication happening?" or "If there is suspicious connection to external domain happening it's most likely going on through this part of the network but from which endpoint and process?".

In order to deliver these capabilities, the EDR solution must have **investigation-assisting functionality** as well as **data collection** and **storage features**. And **incident discovery** should incorporate both automated and manual elements. Last but not least – as the initial incident is detected, the security team and threat responder should be equipped to **easily contain** the threat, **remediate** the endpoints and **prevent** the specific activity from happening again.

Let's take a look at 5 common challenges that organisations should take into account while choosing advanced EDR solutions, or generally improving their current Endpoint Security in terms of Detection and Response.

1

Endpoint data: too much visibility

Endpoint protection in any form begins with the collection of new data, its storage and analysis. Theoretically, the more data you can collect, the greater the benefit. The same theory also used to be applied to SIEM systems. But, to interpret large volumes of collected data, the EDR operator also needs relevant context. For example, the rapid discovery of a malicious connection to a bad domain is of considerably less value if you don't know from which endpoint this originated, how the process started, what the root cause was and which assets may have already been affected.

Immature EDR solutions on the market collect some data, but do not provide the right context. They may, for example, allow the operator to quickly discover which machines hold a file with a certain hash sum, without providing information about how the file appeared on these machines. A list of generated processes may be provided for the object and activities, but with no visualisation. Or complex alerts about atypical behaviour or deviations may be provided, but without basic scans and verdicts.

Some solutions collect all the data from the endpoints, then present it straight onto the interface - like a direct window into the database. Unless the operator is a data scientist or big data champion as well as a security expert, he or she won't be able to make an informed decision on the basis of this raw data.

Often such systems generate thousands of messages, and literally millions of alerts, all of which somebody has to validate. Even in the largest organisations, the monitoring and response team is unlikely to be able to handle more than 50-60 medium to highly critical incidents at any one time. As a result, we have a solution which finds everything, but little or nothing can actually be done about what's found – there's just too much, and not enough, to see.

One compromise here may be the sharing of alerts between your own security team and an external MSSP, but you'll need to find a provider with the right training and expertise. And without incident prioritisation, this could involve a huge investment and waste of resources on non-critical alerts. An additional concern, as with any MSSP, is the matter of trust, data privacy and compliance restrictions.

Recommendations:

- Look for solutions that don't just enable you to automatically expose risk through alerts, but which also allow for deep customisation - configuring different user roles, allocating VIP groups, quickly setting up whitelists. This will allow you to properly highlight what's important, reduce what's unnecessary, and check that only critical information is visible to any external MSSP.
- Think about the extent to which you're expecting to conduct data analysis within the organisation, and how much data you're expecting to store and process. Gearing up to handing terabytes of data in-house may well mean substantial additional hardware costs.

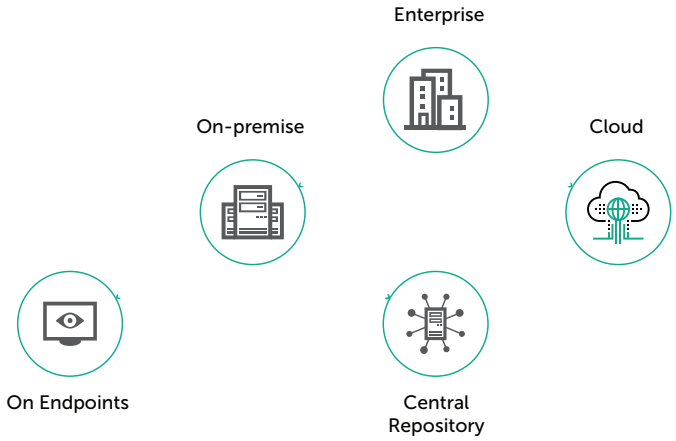
2

Responsibility for aggregated and stored data

Another important feature related to data is how it's collected and stored. Questions you need to ask an EDR vendor here are:

- How much data is stored, and why?
- What data is stored?
- Where is it stored?

There are several possible storage approaches:



Let's take a closer look at them.

Cloud

Many vendors offer cloud solutions to store data or even to manage EDR agents (so-called MDR). They're convenient, but limited by the amount of data they can upload at any one time. This also involves having an open conduit transmitting data outside the organisation, which can be an issue in some environments. When considering this option, questions to ask include:

- Are we ready to send security data into a public cloud? How much control will we have?
- Can the vendor or cloud provider (this may be a third party) who will be storing my data be trusted? How good are their own cybersecurity provisions?
- Could using this service violate compliance with internal security standards and/or regulatory requirements?
- If only small volumes of non-critical data are sent to the cloud, how effective can the solution be?

On-agent

A local cache on each device delivers a compromise between heavy storage and the cloud. This approach has less impact on the network, and large numbers of agents can be supported simultaneously. Important information is recorded into the endpoint cache itself, and all analysis takes place in real time through queries. But decentralised storage is not always the fastest and most effective way to analyse and respond to information. If, for example, a sub-segment of the network is unavailable, it will not be possible to incorporate data from the machines affected into the overall analysis.

Centralised on-premise repository

All essential information is accumulated and analysed by a dedicated server with a repository. A local database and analysis tools (for example, a sandbox) do all the work. This local approach has a number of advantages - data is not stored on potentially compromised devices, as can theoretically be the case with agent-based storage. There's no load on the resources of the computer, and you can conduct endpoints queries and 'fast search' over the database itself in real time. On-premise solutions like this are particularly useful where regulations or security standards require that no data is transferred outside the organisation.

Recommendations:

- For cloud storage, assess your cloud EDR provider in terms of data privacy and control
- For sensitive environments, and where regulatory compliance puts potential restrictions on external data transfer, your evaluation may include exploring options for on-premise, fully isolated implementation and the private delivery of threat intelligence.
- For agent-based data storage, check what will happen if an endpoint is unavailable, or has been compromised by your attacker (how the agent itself, the PC, and data are protected)
- For on-premise solutions, check internal data storage capacity and the amount of data sent from each device.

The number of agents will dictate hardware requirements – if an EDR solution requires only a small server to support hundreds of thousands of agents – there's something odd going on. On average, one endpoint generates around 10 megabytes of useful telemetry per day. So if you have 10,000 nodes, you're looking at 100 gigabytes of data per day – or 3TB for a one-month retrospective database.

3

Detection: manual hunting vs automated engines

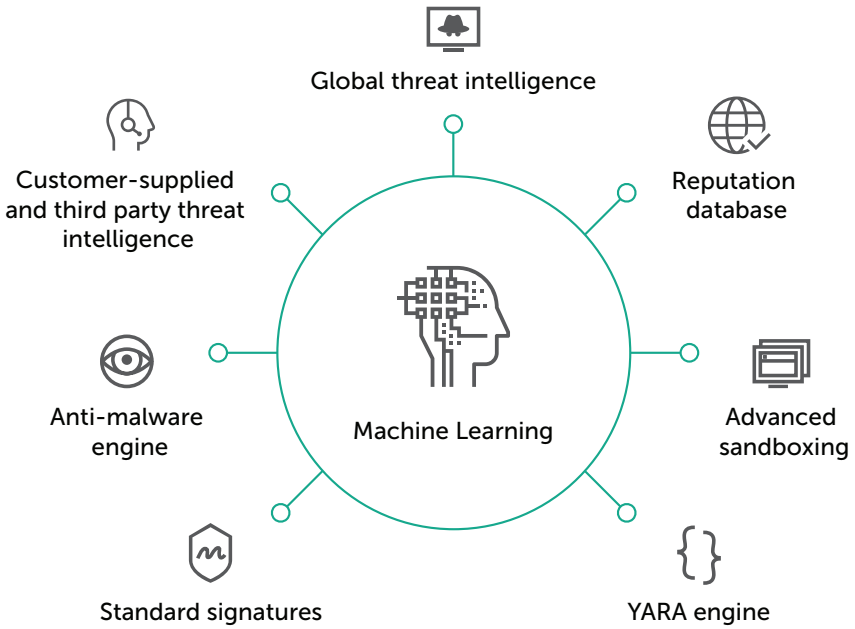
You've dealt with data and storage. Now we move to data analysis - threat hunting and monitoring conducted manually using your vendor's toolkits, databases and resources, and automatically through the EDR system itself. The earlier you detect an attack, the lower the financial impact and the less the disruption caused. So the speed and effectiveness of detection is paramount – and manual detection techniques alone are not generally the fastest or most efficient approach. Many vendors provide so-called 'advanced detection techniques'– IoC scanning of endpoints in real time or fast search over databases of centrally stored forensics data – adding an automated element to incident discovery capabilities.

To fully utilise your aggregated data, you will need powerful automated data analytics techniques that help your analysts reveal the risks and threats presenting over the network. Multi-dimensional and multi-layered analysis should continuously deliver not just new security incidents but also actionable intelligence, in order to help your security team make the right decisions and avoid spending unnecessary time on non-critical events.

Such advanced detection and threat discovery technologies shouldn't just uncover common malicious activities, but should go 'beyond malware' to detect more sophisticated breaches. We're now talking not about the filtering layers of prevention technologies that form the basis of most EPP solutions, but about advanced analytical systems.

Security solutions that use multiple detection technologies can greatly increase your chances of spotting attacks and intrusions more rapidly, before serious damage is done to the organisation. EDR solutions should include multiple detection engines - integrated to deliver Advanced Threat Detection that combines static, behaviour-based and dynamic analysis plus real-time access to global threat intelligence and machine learning technologies.

So the main goal here is to leverage as many different detection engines as possible to provide in-house 'virus analysis lab' capabilities, able to validate predictions, start new investigations or support those already in progress.



Depending on the vendor, detection techniques and engines used will almost certainly comprise a manual toolkit and automated systems in some combination:

Manual Detection Aids

- Indicators of Compromise upload and automated/manual search
- Fast search over the retrospective data
- Sandboxing (the ability to send a specific object to a dedicated or cloud-based sandbox)
- Access to the vendor's threat intelligence sources

Automated Detection

- Anti-malware
- YARA rules (customisable by vendor or/and your security team)
- Threat intelligence (delivered by vendor automatically)
- Reputation services (files or/and domains)
- Automated sandbox analysis of suspicious objects
- Machine learning
  - Deep learning (no signature – neural network)
  - Artificial intelligence (base-lining, behaviour analysis)

Recommendations:

- Ask your EDR vendor what detection technologies are available and in place
- Find out whether they are using in-house, OEM or open-source detection engines
- Explore the quality and immediacy of the threat intelligence that feeds these engines
- If there are several detection technologies in place – how are they integrated and correlated? (you don't want to end up with separate incidents logged in different engines for the same event)

4

Don't just React — Respond

Reacting to an incident is easy: responding effectively is what brings resolution. The response process is activated once a security incident has been validated through triage and initial investigation. Once it's confirmed that this is not a 'false positive', a swift, accurate response is required.

The Incident Response Management process will depend on the severity of the incident. Most incidents will have relatively little business impact (being detected directly upon entry). But there will be those which could lead to a serious situation - a major data breach, financially-related crime, espionage or even worse. These are the critical situations requiring an Emergency Response and Investigation process.

Once you've manually discovered or received a security alert about a potential threat, via a third party security solution or your EDR product, what happens next? Have you outlined the triage, investigation, and response processes for your organization? Without this in place, your security team can quickly become overwhelmed by the workflow surrounding any EDR solution.

Detecting an active threat is the vital first stage in repelling an attack. Having spotted the threat, you need to respond rapidly across potentially thousands of endpoints. An effective EDR solution will enable the centralised management of incidents across all endpoints on the corporate network – with a seamless workflow. In addition, a wide range of automated responses will help you avoid using traditional remediation processes – such as wiping and re-imaging – that can result in expensive downtime and loss of productivity.

Core response functionality depends on the vendor approach, but should focus on these common operations:

- Prohibiting the launch of PE files, office documents and scripts
- Ability to remotely delete the file on the workstation
- Move the file from the workstation to quarantine and recover it if necessary
- Obtain the file and perform an analysis during the investigation (for example forced Sandbox execution)
- Force the process to shut down
- Run the program/script on the workstation

Some vendors may provide additional scenarios for more precise responses. These could include network isolation, process isolation, user deactivation, roll-back, and remediation scenarios.

Recommendations:

Look for:

- Vendors with the ability to maintain powerful, comprehensive threat intelligence databases, and to provide you with expert support and consultancy as and when needed.
- EDR solutions backed by effective skills training courses, educating your security team so they can establish effective processes and make the most of your investment.
- A seamless workflow between detection, manual threat hunting, third party IOC and Incident Response processes, without the need to switch between different consoles or solutions.
- Agents that are silent for end-users even during investigations, that will not impact user behaviour and that will not contribute to downtime

5

Prevention – EDR or EPP?

EDR solutions are increasingly incorporating prevention elements in an attempt to offer an "all-in-one" solution. As prevention capabilities mature, it's possible that endpoint prevention, visibility, detection, and response capabilities will converge into a single endpoint product.

But we're not there yet. While it may be tempting to look for a solution that includes prevention alongside detection and response, we would not recommend that you give this aspect too much consideration at this point. Select your product first for its visibility, detection, and response capabilities. If the solution also includes prevention elements, that's an added bonus. But be cautious of 'next gen' EDR solutions with immature prevention capabilities. If you attempt to replace your traditional EPP with an EDR solution, you're unlikely to achieve the same levels of prevention functionality.

However, many EPP vendors are now buying in or developing their own EDR. If you're happy with your current EPP and your EPP vendor offers an EDR solution, it makes sense to evaluate how both interact and how they might work together for you – particularly if this means not having to install a second agent for EDR.

Recommendations:

- Look at the EDR product's roadmap and how it may evolve over time to deliver additional prevention capabilities.
- If the idea of integrated endpoint protection, detection and IR appeals, look at your current EPP vendor's EDR offering, and see what EPP capabilities other EDR vendors are offering
- Check out the EDR's architecture and in particular the ability to use a single agent for both EPP and EDR.

The Future of Enterprise Endpoint Security

Market leaders will try to adopt new technologies and leverage internal in-house development to increase their EDR capabilities.

For security experts right now, the endpoint security market feels seriously over-saturated with different vendors. It's becoming clear that this can't continue. Large vendors will eventually gobble up smaller businesses, using their products to fill portfolio gaps and to improve their brands. Market leaders will try to adopt new technologies and leverage internal in-house development to increase their EDR capabilities.

True 'Next Generation' endpoint security, offering both traditional methods of control and protection and advanced technologies, will evolve through the efforts of major players in the EPP market. The current generation of advanced endpoint security agents, like EDR, offer only elements of true EPP functionality – they're not aiming at this point to take on the mantle of a full-function endpoint protection suite.

Endpoint security has moved back up the corporate agenda, and will continue to attract ever more attention. Future customers will adapt and evolve their security strategies, revolving around advanced endpoint protection technologies combined with endpoint activity monitoring.

Technologically, such advanced solutions will form an adaptive approach to providing protection, while simultaneously providing systems hardening, malicious activity prevention and advanced detection. Cloud-based threat intelligence and on-premise machine learning, threat hunting including active response and rapid investigation and deep behavioural and threat intelligence analysis will also all play their part.

Immediate Recommendations

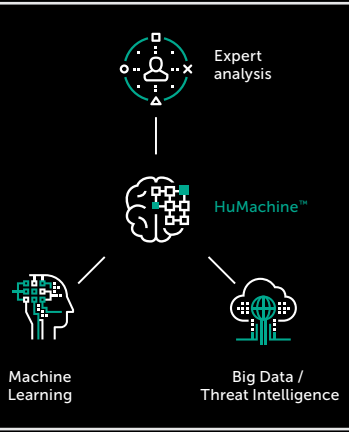
Recognising the growing need for deeper endpoint analysis and protection, security professionals inevitably find themselves with a long list of needs and a limited budget with which to address them all. But even without a budget, it makes sense to evaluate current technologies and possible future developments in terms of how they correspond with your business goals and internal capabilities. By fully investigating and testing the options, you can help focus your overall business decision-makers' attention on what new technologies can deliver, ensure more precise future security budget planning, and know that when the time comes to invest, you're ready to do so wisely.

Actions to take right away

1. Evaluate your overall security capabilities. How fast and how unified is your current Incident Response process? Are you currently running the right solutions for you, aside from EDR considerations? How do you stand on this in relation to your industry and your competitors?
2. Understand your current detection capabilities over endpoints. Perform analyses and look at trialling additional intelligence sources – for example, look at using Threat Data Feeds with your SIEM
3. Think about how you can start to grow IR expertise in-house. Evaluate your team's capabilities and investigate effective training options.
4. Start of formulate your actual requirements/upcoming demand and look at shortlisting EDR solutions in line with this.

Some useful links

1. Incident Response Guidelines: https://cdn.securelist.com/files/2017/08/Incident_Response_Guide_eng.pdf
2. Assess your security with this IT security calculator and download the Global Enterprise Report: https://calculator.kaspersky.com/en/



Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com

© 2017 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.