CENTRE FOR
CYBER SECURITY
BELGIUM

Recommendations for anti-virus, EDR and XDR security solutions

August 2022

Table of Contents

Executive Summary 2

Some Definitions 2

Level1, basic protection: Antivirus (also called Anti-malware) 2

- Problem they solve: 2
- Important minimum capabilities for antivirus software (1): 2
- Implementation strategy: 3
- Product assessment/comparison Organisations 3

Level 2: Substantial protection EDR (Endpoint Detection and Response) (4) (5) 4

- Problem they solve: 4
- Important minimum capabilities for EDR (4): 4
- Implementation strategy: 5
- Product assessment/comparison Organisations 6

Level3: Advanced Protection XDR - (eXtended) Endpoint Detection and Response 6

- Problem they solve (10) (5) 6
- Implementation strategy: 7
- Important capabilities for XDR (12) 7
- Product assessment/comparison Organisations (11) 7

Windows eco system 7

References 9

Contact 11

Executive Summary

Given the current context, a “defence in depth” strategy is important and organisations should prepare adequately. This includes many aspects like suitable policies and procedures, end-user training (awareness), vulnerability management processes, good configuration management, (local) firewalls, Web application protections, Security Information and Event Management (SIEM) systems, Intrusion Detection Systems (IDS), proper network segmentation, mobile device management…and all of those should be tailored to your organisation and take the architectural design into account such as cloud usage, “Bring your own device” strategy, etc.

Deploying and managing Antivirus, EDR (endpoint detect and respond) and even XDR (extended end-point detection and response) are part of the solution required to achieve this goal.

This document provides guidance on generic, pragmatic and generic technical criteria and some relevant references for **Antivirus**, EDR and XDR security solutions.

We have defined three levels within this approach: Level 1 (Basic) refers to antivirus protection, Level 2 (substantial) to EDR and Level 3 (advanced) to XDR.

If your organisation already has a basic security solution in place, additional licensing might allow you upgrade towards the advised capabilities of an EDR solution (see Level2).

Some Definitions

Antivirus (level 1, basic protection): Applications that scan (real-time/on access or scheduled at an interval) files, based on signatures or heuristics. They are ideal for detecting known malware.

EDR - Endpoint Detection and Response (Level 2, substantial protection): This is the next -generation solution that typically incorporates antivirus scanners but adds extra features based centralized management, correlation, and interpretation of events.

XDR - eXtended Detection and Response (Level 3, advanced protection): It increases the capabilities of an EDR solution(s) in a cross-domain environment by adding additional correlation sources but also additional functionalities.

Level1, basic protection: Antivirus (also called Anti-malware)

Problem they solve:

The traditional approach has always been the use of an antivirus as endpoint protection solution. Scanners were the most efficient tools, relying mainly on signatures and heuristics. Today, antivirus scanners are still the most used technical control for malware threat mitigation. See also the excellent publication from NIST.gov on malware tools (1)

Important minimum capabilities for antivirus software (1):

- Scan critical host components such as startup files and boot records;
- Perform real-time scans of each file as it is downloaded, opened, or executed (on-access scanning);
- Monitor common applications behaviour, such as email clients, web browsers, and instant messaging software;

- Antivirus software on hosts should be configured to scan all hard drives regularly to identify any file system infections. Scanning removable media inserted into the host before allowing its use is also recommended;
- Users should also be able to launch a scan manually as needed, which is known as on-demand scanning;
- Identify common types of malware as well as attacker tools;
- Disinfect files, which refers to removing malware from within a file, and quarantining files, which means that files containing malware are stored in isolated storage for future disinfection or examination.

Important criteria are:

- Administrative: Centrally managed, controlled and monitored regularly by antivirus administrators;
    - Tamper protection: User should not be able to disable or remove antivirus,
    - Regular updates of antivirus signatures and databases,
    - Visibility of infections and status of the deployments (reporting).
- Accuracy: Describes the tool's relative success rate and the types of errors it can make;
- System overhead: Impact on system performance.

Implementation strategy:

Organisations should deploy antivirus software on all hosts for which satisfactory antivirus software is available. Antivirus software should be installed as soon after OS installation as possible and then updated with the latest signatures and antivirus software patches (to eliminate any known vulnerabilities in the antivirus software itself) (1).

Product assessment/comparison Organisations

- **AV-Test** https://www.av-test.org/en/: German organisation acquired by the Swiss IT Security Group in 2021. Every other month, researchers publish their testing results, which includes a product list that have been awarded certification (2).

  Test methodology: AV-Test uses different modules for every operating system, based on 3 main criteria:
    - Protection reflects the results of tests involving protection against malware and other attacks,
    - Performance demonstrates the influence of tested products on the speed of the test systems,
    - Usability indicates disturbing influences of tested products due to false alarms and limitations in using the Internet.
- **AV-Comparatives** https://www.av-comparatives.org: Austrian independent organisation that tests and assesses antivirus software, regularly releasing charts and reports that are freely available. AV-Comparatives fundings are supported by several universities (3).

  Test methodology: Tests are run yearly.
    - Real-World Protection Test: online malware attacks that a typical business user might encounter when surfing the Internet (751 test cases in 2021).
    - Malware Protection Test: this is a scenario in which the malware pre-exists on the disk or enters the test system via e.g. the local area network or removable device, rather than directly from the Internet (30 tests in 2021).

- Performance tests: Impact on system performance.

Although antivirus software has become a necessity for malware incident prevention, it is not possible for antivirus software to stop all malware incidents. Antivirus software often do not excel at stopping unknown threats. Antivirus software products detect malware primarily by looking for certain characteristics of known instances of malware, which is highly effective for identifying known malware but is less at detecting highly customised, tailored malware (1).

Level 2: Substantial protection EDR (Endpoint Detection and Response) (4) (5)

Problem they solve:

Correlation and interpretation of events become increasingly important as to detect and respond to more advanced and custom malware, for example ransomware.

Antivirus software is not well suited to perform this task. Each separate event could be legitimate, but if an overload of events is happening in a brief period, this could be caused by a malicious incident.

To remediate this situation, a new generation of tools has been developed by different vendors. There is not a unique definition or standard about EDR, meaning that capabilities between vendors can vary a lot. Several vendors are packing the EDR features with other capabilities like antivirus, network security, …. All of this makes it difficult to compare.

Important minimum capabilities for EDR (4):

1) Detect security incidents;
2) Contain incidents at the endpoint;
3) Investigate security incidents ;
4) Provide remediation guidance.

The CCB recommends that an EDR solution should have as an absolute minimum the following capabilities:

- Endpoint monitoring and event recording;
- Data search, investigation, and threat hunting;
- Suspicious activity detection;
- Actionable intelligence to support response;
- Automated Remediation;
- Multiple OS Support;
- Central management component.

The CCB advises that the selected tool also has the following additional capabilities:

- Vulnerability reporting;
- Forensic capabilities / gathering data from systems;
- API for linking external systems.

<u>Capabilities more in detail:</u>

- Endpoint monitoring and event recording

We recommend that the tool selected has the possibility to record events, like processes that are running, users active on the machine, active network connections, services existing on the machine, ….

We also recommend that the tool can transfer alerts/events towards an external system like a SIEM or logging / storage solution.

- Data search, investigation, and threat hunting

  We recommend that the tool selected can run custom queries. Preferably, it also can run custom scripts towards a specified set of endpoints.

  Ideally, the tool supports live interaction with the endpoint system, to provide the security team with capabilities to investigate threats on the specific endpoint and exfiltrate samples for further analysis in a separate (sandboxed) environment.

- Actionable intelligence

  We recommend that the tool selected should have the possibility to ingest indicators of compromise (IOC). These could include network addresses (IP), file hashes, filenames, domain names, e-mails, ... The more indicators that can be ingested in an automated way, the better.

- Suspicious activity detection

  We recommend that the tool selected supports the creation of custom detection rules by the organisation itself. Signature-based detection and as well as rule-based detection (behavioural detection) are recommended.

- Multiple OS Support

  We recommend that the tool selected has agents that are available for multiple operating systems. Systems based upon Windows, Windows Server, Mac OS, and Linux distributions based on Debian or Redhat should be supported.

- Automated Remediation

  We recommend that the tool selected has the possibility to respond automatically to detected incidents and that the tool can quarantine an endpoint.

- Central management component

  We recommend that the tool selected can continually connect to its central management platform. Any (internet) network connection should be supported (even if this means that there is no direct VPN connection towards the organisation).

  If a cloud solution is used, we recommend that this solution is physically located in a European datacentre and a Data Protection Impact Assessment (DPIA) evaluation is made.

  Some integrated cloud solutions can offer some advantages like automated setup, maintenance of the management components, predefined integrated reporting, …

Implementation strategy:

We recommend onboarding as many devices as possible (on all supported operating systems). software should be installed as soon after OS installation as possible and then updated with the latest software patches. Updates are normally not as frequent as for antivirus software, but organisations should be able to deploy updates as soon as possible after a patch has been released.

Product assessment/comparison Organisations

We recommend to always assess the minimum capabilities of each solution with the recommendations from MITRE ATT&CK™ knowledge base (6).

The ATT&CK™ knowledge base provides a common foundation for describing both testing criteria and results. ATT&CK is a MITRE-developed, globally accessible knowledge base of adversary tactics and techniques based on real-world observations of adversaries' operations against computer networks (6).

MITRE performed an evaluation test of specific EDR tools in an interesting way. According to some vendors, MITRE is the first in the industry to assess EDR vendors. MITRE picked 2 specific threat actors (APT3 & APT29) and then executed the associated ATT&CK techniques in a cyber exercise.

The most recent evaluation was performed based on the tactics, techniques, and procedures (TTPs) of 2 groups:

- Wizard Spider (7) is a financially motivated criminal group that has been conducting ransomware campaigns since August 2018 against a variety of organisations, ranging from major corporations to hospitals.
- Sandworm Team (8) is a destructive Russian threat group that has been attributed to Russian GRU Unit 74455 by the U.S. Department of Justice and U.K. National Cyber Security Centre. Sandworm Team's most notable attacks include the 2015 and 2016 targeting of Ukrainian electrical companies and 2017's NotPetya attacks. Sandworm Team has been active since at least 2009.

The detailed results per vendor can be found on the Att&ck Evaluations (9).

It is important to note that MITRE does not rank the participants but when searching the internet, you will find summaries to make up your mind.

Level3: Advanced Protection XDR - (eXtended) Endpoint Detection and Response

Problem they solve (10) (5)

Most organisations do not have a unified, standard, and consolidated (endpoint) infrastructure. Security teams must be able to get an overview of all systems and alerts of the complete infrastructure. XDR streamlines security data ingestion, analysis, and workflows across an organisation's entire security stack, enhancing visibility around hidden and advanced security threats and unifying the response.

XDR is the evolution of EDR, Endpoint Detection and Response. While EDR collects and correlates activities across multiple endpoints, XDR broadens the scope of detection beyond endpoints to provide detection, analytics and response across endpoints, networks, servers, cloud workloads, SIEM, and much more.

This provides a unified, single pane of glass view across multiple tools and attack vectors. This improved visibility provides contextualisation of these threats to assist with triage, investigation and rapid remediation efforts.

Implementation strategy:

We recommend onboarding as many platforms as possible. Although, a phased rollout is recommended. An XDR platform must have sufficient time to baseline data flow behaviour to accurately detect security anomalies (11).

Important capabilities for XDR (12)

- Controls-agnostic

  XDR solution must integrate with multiple technologies and avoid vendor lock-in.

- Machine-based correlation and detection capabilities

  Enables faster analysis of much larger data sets and reduces the number of false positives.

- Pre-built data models

  Integrates threat intelligence and automates detection and response without the need for software engineers to do all the programming or create all the rules.
  We recommend that the XDR solution allows the creation of extra custom rules.

- Integration with SIEMs, SOARs and case management tools

  Rather than requiring the replacement of such products, XDR allows companies to maximize the value of their investments

  Note: It is important to quantify how much log and telemetry data will be collected and how long data must be stored. This will help determine the amount of storage space needed by the XDR platform, as well as the bandwidth that will be consumed across LANs, WANs, and cloud connections to send data to an XDR data collection agent.

Product assessment/comparison Organisations (11)

The CCB recommends assessing your organisation's infrastructure and tools first before deciding about the purchase of an XDR solution. There are some minor differences between XDR platforms.

- Detection level
  Some XDR applications will rely more heavily on endpoint detection data, others may rely more on data as it traverses the network. Having none or most homeworkers in your organisation, a large, diverse, and complex network, … can be a key factor in the decision process.

- Threat intelligence information
  It is important to consider how the vendor handles threat intelligence and hunting using external threat data and if they are proactive enough. Most enterprise-grade XDR platforms use their own in-house threat detection teams to identify new or emerging threats.
  Threat intelligence information gathered by these groups can be used to automatically create security policies that are then pushed to the organisation security tools. The ability for these teams to rapidly identify threats and create a policy is a critical factor for zero-day exploits.

Windows eco system

Every recent Windows operating system comes with a free windows defender (antivirus) client installed, out of the box. Organisations are, of course, free to install the antivirus product. If you install another antivirus product, the antivirus component in the defender client will simply be replaced. All other components in the defender client will still function (Windows Defender Firewall,…).

On the other hand, the free windows defender client can be configured and upgraded to an EDR client. (13) (14)

The defender for endpoint can also be deployed on Windows servers (15) or on your cloud infrastructure (16).

As an added value for the defender eco system, Defender for Identity might be an important feature. After installing a sensor on all Active Directory domain controllers (on premise) extra identity management options are available in the cloud platform. (17)

As for all cloud integrated products some changes might occur on your environment by default, changing your security exposure. This requires a continuous follow-up and evaluation of those changes applied by the vendor.

Special licensing terms may apply, please always check licensing terms with your supplier first.

We also recommend to install Sysmon which will enrich your logging and diagnostics capabilities. (18)

Other operating systems (Linux, Mac OS, …) or none-Microsoft devices might not always provide the same level of features and security scope within the Defender suite. Have a look at your non Microsoft systems, the version and/or distro being used and how it is supported by the vendor (19)

The use of Yara rules is not yet supported (June 2022) however there is Advanced query hunting available with a vendor specific implementation.

References

1. **NIST 800-83.** Guide to Malware Incident Prevention and Handling for Desktops and Laptops. *Nist.gov.* [Online] https://csrc.nist.gov/publications/detail/sp/800-83/rev-1/final.

2. **Wikipedia AV-test. *nl.wikipedia.org.* [Online] https://nl.wikipedia.org/wiki/AV-test.org.**

3. Wikipedia AV-Comparatives. *en.wikipedia.org.* [Online] https://en.wikipedia.org/wiki/AV-Comparatives.

4. Gartner. endpoint-detection-and-response-solutions. *gartner.com.* [Online] https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions.

5. Crowdstrike. edr vs mdr vs xdr. *crowdstrike.com.* [Online] https://www.crowdstrike.com/cybersecurity-101/endpoint-security/edr-vs-mdr-vs-xdr/.

6. Mittre Attck Product evaluations. attck based product evaluations. *Mittre.com.* [Online] https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/attck%E2%84%A2-based-product-evaluations.

7. Wizard Spider. [Online] https://attack.mitre.org/groups/G0102/.

8. Sandworm Team. [Online] https://attack.mitre.org/groups/G0034/.

9. mitre-engenuity.org. [Online] https://attackevals.mitre-engenuity.org/.

10. sentinelone.com. [Online] https://www.sentinelone.com/blog/understanding-the-difference-between-edr-siem-soar-and-xdr/.

11. Evaluate XDR. *techtarget.com.* [Online] https://www.techtarget.com/searchsecurity/tip/How-to-evaluate-and-deploy-an-XDR-platform.

12. *XDR according Mandiant.* [Online] mandiant.com. https://www.mandiant.com/resources/what-is-xdr.

13. What is Defender for Endpoint. *docs.microsoft.com.* [Online] https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide.

14. Configure Defender for Endpoint (client). *docs.microsoft.com.* [Online] https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints?view=o365-worldwide.

15. Configure Defender for Endpoint (server). *docs.microsoft.com.* [Online] https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-server-endpoints?view=o365-worldwide.

16. Configure Defender for Endpoint (cloud). *docs.microsoft.com.* [Online] https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-servers-introduction.

17. What is Defender for Identity. *docs.microsoft.com.* [Online] https://docs.microsoft.com/en-us/defender-for-identity/what-is.

18. Sysmon, Microsoft. [Online] https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon.

19. Configure Defender for Endpoint (other). ***docs.microsoft.com.*** **[Online] https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints-non-windows?view=o365-worldwide.**

Contact

Centre for Cyber security Belgium
Rue de la Loi, 16/ Wetstraat 16
1000 Bruxelles/ Brussel
info@ccb.belgium.be

Disclaimer

This document and its annexes have been prepared by the Centre for Cybersecurity Belgium (CCB), a federal administration created by the Royal Decree of 10 October 2014 and under the authority of the Prime Minister.

All texts, layouts, designs and other elements of any nature in this document are subject to copyright law. Reproduction of extracts from this document is authorised for non-commercial purposes only and provided the source is acknowledged.

The CCB accepts no responsibility for the content of this document.

The information provided:

- are exclusively of a general nature and do not intend to take into consideration all particular situations;

- are not necessarily exhaustive, precise or up to date on all points

Responsible editor

Centre for Cybersecurity Belgium
Mr. De Bruycker, Director
Rue de la Loi, 16
1000 Brussels