MINISTRY OF SECURITY

DUMMIES GUIDE ON

# ENDPOINT SECURITY TECHNOLOGIES COMPARISON

# EDR VS EPP

# EDR VS XDR

# EPP vs EDR

| EPP (ENDPOINT PROTECTION PLATFORM) | EDR (ENDPOINT DETECTION & RESPONSE) |
|---|---|
| Prevents a wide variety of known and unknown threat | Used to respond to threat that have already affected the endpoint |
| First line of defense – scan, identify and block | Second line of defense – contain, investigate and respond |
| Passive – protect against known and easily identifiable against threat | Active – used to counter evasive threats that gets past security threats defenses or for proactive threat hunting |
| Protect endpoint but does not provide in-depth data about the threat on the endpoint | Aggregate data from multiple endpoints to enable forensic investigations |
| EPP is focused on prevention | EDR is focused on detection and response |
| EPP relies on signatures and heuristics | EDR uses behavioral analytics to detect threats |
| EPP only provides visibility into the activity that is related to malware | EDR can provide visibility into all activity on a device |
| EPP cannot investigate security incidents | EDR can be used to investigate and contain security incidents |
| Machine learning to support behavioural analysis | |
| Traditional threat monitoring | |
| Prevent unknown attacks, verifies indicators of compromise (IoC), memory consumption and vulnerabilities | |
| Antivirus is generally a single program that serves basic purposes like scanning, detecting and removing viruses and different types of malware | |

# EDR vs XDR

| EDR (ENDPOINT DETECTION & RESPONSE) | XDR (EXTENDED DETECTION & RESPONSE) |
|---|---|
| Limited to one security layer | Crosses multiple security layers – endpoints, networks traffics, identity management, cloud workloads, email, virtual containers, sensors (from operational technology, or OT) |
| Completed by NTA tools but not strongly integrated with them | Provides both endpoints and network security in one platform |
| Separate tools that needs to be managed alongside other security tools | Unified platform that provides a single point of reference for security analyst |
| EDR is a new generation of anti-malware | Provider improved detection and response to day-to-day security incidents |
| EDR no longer relying solely on signature systems to perform malicious behavior detection | Increased overall productivity of security personnel |
| EDR adds behavioral process analysis capabilities to determine deviance. | Lowered the total cost of ownership (TCO) of the security stack |
| EDR does support Forensic | Forensic - Investigate incidents swiftly with comprehensive forensics evidence |
| EDR does support Forensic | Host Insight - Find vulnerabilities and sweep across endpoints to eradicate threats |
| EDR does support Host base inventory | Host inventory |
| Pinpoint attacks identify behavioral deviations | Pinpoint attacks with AI-driven analytics and coordinate response |
| | File Search and Destroy |

# Introduction

From day of evolution of computer era, endpoint is the simplest route for the security threats which is rapidly evolving.

Though organizations have transitioned from simple antivirus software to full endpoint protection platforms (EPPs) that provide well-rounded, preventive security capabilities for endpoints to endpoint detection and response (EDR) solutions that complement EPP by adding the ability to actively respond to endpoint security breaches.

Today, all these security technologies are overshadowed by a new model called **XDR or Extended Detection and Response**. Since, endpoints have long been a major target for attackers. Whether located in a user's pocket, in the cloud, on IoT devices, or in an organization's server room, the data needs to be protected both inside and outside the traditional security perimeter.

## Antivirus Product Capability Support

| | |
|---|---|
| Platform Supports | Windows Operating System |
| | Linux - Ubuntu 16.04 to 22.4 and upcoming versions |
| | Cloud workloads, Containers, Kubernetes |
| | Android - All version |
| | MacOS - All version and upcoming versions |
| Hardware Platform | Desktop, Laptop, Server, Cloud, VM's, VDI |

## Antivirus Portfolio/Baseline

| Features | Description |
|---|---|
| NBA | Solution should have capability monitoring the network behavior analysis |
| UBA | Solution should have capability monitoring the user behavior analysis |
| Deception | Solution to stop attackers from breaching your system and causing damage |
| Web Security | Reliably protects your PC against viruses, spyware, trojans and other malware |
| Faster, More Complete Investigation & Response | MITRE ATT&CK Evaluation 100% threat prevention |
| Response Action | Live Terminal |
| | Endpoint isolation |
| | External Dymanic list (EDL) |
| | Script Execution |
| | Remediation analysis |
| | Incident Scoring Rules |
| | Featured Alert Fields |
| Application Control | Standard category wise application Allow/Block |
| | Custom extension-based application Allow/Block |
| Device Control (Should work on all OS windows, MacOS and Linux) | Mass storage allow/block, read only |
| | MTP/PTP- block/allow |
| | Bluetooth - allow / block |
| | Thunderbolt - allow / block |
| | Camera - allow / block |
| | Card reader - allow /block |
| | USB Printer- allow / block |
| | Wi-Fi printer - allow / block |
| Firewall | Host Firewall |

| | |
|---|---|
| | Host-based IDS and IPS |
| Email Protection | Antispam, Anti Phishing |
| File integrity monitoring | File integrity monitoring |
| EDR/XDR | Real time malware detection, protection and prevention |
| | Behavioural analysis |
| | Signature based analysis |
| | Real time threat analysis and advanced threat detection |
| | Malicious traffic detection |
| | Anti-Ransomware - Recognized & Unrecognized Ransomware Protection |
| | Detect suspicious activities and blocks them before any breach occurs |
| | Policy/ Rule based Host isolation |
| | Manual Host isolation |
| | isolated host accessibility and integration from management console without physical intervention with client machine |
| Managed Threat Response (MTR) | Deep Alert Analysis |
| | Threat Hunting, Suspicious Behavior Detection, Investigation and Remediation |
| Exploit Prevention | File-less Attacks |
| | Malware-Free Attacks |
| | Zero Day Attacks |
| | Exploit-based Attacks |
| | Toolkit blocking |
| Artificial Intelligence & Machine learning | Proactive techniques to detect malicious traffic as well as protect from attracters |
| | Malicious traffic detection and prevention |

| | |
|---|---|
| | Patch and Vulnerability Assessment, Real time monitoring and rapid mitigation of detected threats |
| Root Cause Analysis | Deep analytics on what, when, where and how incident happened. |
| Logs | Real time log synchronization between endpoint and server |
| | Log Retention period (Min 90 days) and policy |
| | Possibility of log retention period extension |
| Event alert and notification | Real time event alert and notification |
| Temper Protection | Should work on windows, MacOS and Linux |
| Central management with single console | Agent Deployment, Update (installer and bundled package) |
| | Asset Inventory |
| | Policy Configuration and Enforcement |
| | Dashboard |
| Report | Custom report |
| | Drill down analysis report |
| | Schedule report |
| | Management report with charts |
| Host Performance | Low CPU Utilization |
| | Low Hard Disk Utilization |
| | Low RAM Utilization |
| Integration | integration with security information and event management (SIEM )tools |
| Subject Matter Expert Availability | 24x7 technical support - on call, email, chat |
| Others | Data loss prevention |
| | Drive encryption |
| | No confliction with other antivirus installed in system |

| | |
|---|---|
| Deployment | Ability to be managed by central management on-cloud and on-prem |
| Password Exposure | The solution shall be able to prevent corporate password reuse |
| Browsing protection | Ability to prevent browser-based attacks by installing thin client on web browser to provide full SSL inspection |
| Document security | Ability to extract malicious content from document and deliver safe file to user immediately |
| Disk Encryption | Solution should support Bitlocker encryption |
| Web Control | Website browsing protection and content filtering |

## Evolution of Antivirus to Next-Gen AV

**Antivirus** - Antivirus (AV) protection is the most common type of endpoint security, especially among consumer electronics.

**Endpoint protection platform -** Endpoint protection platform (EPP) is advance antivirus tools with a key feature called machine learning to support behavioural analysis, extending traditional threat monitoring beyond known threats, prevent unknown attacks, verifies indicators of compromise (IoC), monitors a device's memory to identify irregular patterns in memory consumption.

EPP is advance than antivirus protection for widespread endpoint management and threat prevention in large companies, but some sophisticated attacks are still able to evade detection. EPP is useful for identifying vulnerabilities and preventing attacks.

**Endpoint Detection and Response -** Endpoint Detection and Response (EDR) represent the newest and most advanced layer of endpoint protection platform.

Typically, it expands EPP support for AI, machine learning, threat intelligence, and behavioral analysis to create a collation that neutralizes attacks.

For e.g.: EPP is a **shield**, EDR is a **sword**

An EDR system collects and analyzes data from endpoints across a network so it can stop an attack in its tracks. Once the threat has been removed, EDR can then be used to trace the exact source of the attack so similar events can be prevented in the future.

EDR functions as a centralized management hub for an organization's endpoints network-wide. It acts to stop an attack at the earliest signs of detection, even before a human administrator learns that a threat exists. Whereas EPP is a first line of defense that provides passive threat prevention, EDR actively works to mitigate network attacks before they can cause significant damage.

**Extended Detection and Response** - XDR solutions are a compelling alternative to EDR and traditional EPP. They provide improved threat intelligence, AI/ML analysis, applied to combined data from across the IT environment. They allow organizations to derive more value from existing investments in EDR, SIEM and security orchestration and automation (SOAR).

**Limitations of XDR -** XDR solutions are expected to provide a deeper understanding of the data generated by many other security technologies, but this can be a double-edged sword. While these solutions may have good knowledge of security technologies from the same vendor ecosystem, they may not have the same analytics capabilities for data generated from systems by other vendors.

Therefore, the deployment of XDR technology could lock you into a specific security technology ecosystem. If your organization is already pursuing a single vendor strategy, this may not be an issue. However, this can be an obstacle if you are taking a best-of-breed approach. Companies should consider whether the enhanced analytical value provided by the XDR solution is sufficient to justify a closer dependence on a specific security vendor.

## Antivirus Uses

| Advantages | Disadvantages |
|---|---|
| Signature similarity | Antivirus can't protect against everything |
| Heuristic analysis | It can slow down your computer |
| Integrity checking | It can be expensive to maintain. |
| Prevents a wide variety of known and unknown threat | It can generate false positives (warnings about threats that aren't present). |
| First line of defense – scan, identify and block | It can miss new threats that haven't been identified yet. |
| Passive – protect against known and easily identifiable against threat | It can be difficult to configure and manage. |
| Protect endpoint but does not provide in-depth data about the threat on the endpoint | It can create security holes if not properly configured. |
| Machine learning to support behavioural analysis | It requires regular updates to stay effective. |
| Traditional threat monitoring | It can be disabled or bypassed by malware. |
| Prevent unknown attacks, verifies indicators of compromise (IoC), memory consumption and vulnerabilities | It can give you a false sense of security. |
| Antivirus is generally a single program that serves basic purposes like scanning, detecting and removing viruses and different types of malware | antivirus will only catch known threats |
| | One limitation of antivirus programs is that they can often cause false positives. |
| | insufficient to protect such a large-scale and continuously expanding digital perimeter. |

## Conclusion

In this endpoint security article, we introduced multiple technologies like AV, EPP, EDR, and XDR solutions, and explained the basic differences between these solutions. In reality, these solution categories are not separate or alternative. Traditional AV, EPP and EDR is an essential component of modern security strategies. XDR is widely considered to be the future of endpoint security, but it does not replace AV/EPP/EDR. Rather, it leverages them and consolidates them with other parts of the security stack, to deliver improved security.

## Author

Vikas Vasant Upade

DID YOU LIKE OUR DOCUMENT
AND DO YOU NEED MORE

# CHECKLISTS | WHITEPAPERS
# TEMPLATES | VIDEOS

FOLLOW US ON

**MINISTRY OF SECURITY**

SECURITY & PRIVACY
MADE EASY