#1 Choice of DIGITAL WORLD

eScan™
Enterprise Security

EPP vs EDR

EPP vs EDR

With a ton of products in the cybersecurity market, selecting the best product is difficult as there are many companies offering the same solution with just different wordings making it difficult to select the best product.

So, how do you select the best out of the rest?

Its simple. Below we've made a checklist for you:

- Learn about the product features
- Assess whether product meets your organization's requirements
- Gets the job done effortlessly
- Saves your precious time
- Fits the organization's budget

If the product meets all the above criteria, you are good to go with its purchase. So, let's begin by understanding the differences between EPP and EDR.

What is an EPP?

Endpoint Protection Platform (EPP) is a cybersecurity solution created to detect and stop threat on device/endpoint level. An EPP may be a Firewall, Antivirus, Intrusion Prevention System (IPS), Device Control, Data Loss Prevention (DLP), Data Encryption, and AntiMalware/AntiVirus, or a combination of all of these.

EPP products, normally, are prevention-based and detects only the signature-based threats i.e. it takes action on threats only if its signature is similar to the one in its database. While they do rely on signatures, some EPP products are quite developed and use modern detection techniques to catch threats. eScan EPP, for instance, is quite advanced and provides complete all-round protection using behaviorial patterns of binaries, in order to detect unknown malware.

What is an EDR?

Endpoint Detection and Response (EDR) is an advanced endpoint security solution that comprises of real-time activity monitoring, threat alerts, detailed analysis, and threat removal capabilities.

The EDR's real-time monitoring excels over EPP by maintaining detailed logs of registry changes, file execution and modification, configuration changes for network connection, and binary execution across all endpoints. EDR also provides administrator with Windows Events,

so that co-relation between Windows Events, eScan Events and end-point behavior can be analyzed & necessary action taken.

With all the above characteristics, the EDR

- Monitors and collects data activity data
- Assesses the behavior to identify potential threats
- Inititates a quick counter-response to contain/remediate threat
- Analyses the detected threats and searches for simillar suspicious activities across the network
- Closer integration with Enterprise SIEM for co-relation

Clearing the doubts

Now that you have gotten the idea of differences between EPP and EDR let's discuss more.

The EPP is your primary defence layer against the known cyberthreats and EDR is the secondary layer that continuously monitors for threats, assesses its intrusion, and gives a quick counterresponse to nullify it.

Now, the decision to select the perfect product became complicated when cybersecurity vendors decided to combine both products into one. While the target audience for EPP was single user, small and large businesses, and enterprises; the target audience for EDR was big enterprises with a facility specifically dedicated to cybersecurity operations. But, after understanding its importance and capabilities, oraganizations around the world are planning to get EDR product and implement it into their cybersecurity.

To strengthen the network security, organizations want a perfect product that combines capabilities of both active and passive endpoint protection. And to meet this market demand, many cybersecurity solution vendors started adding the EPP features into EDR solutions and EDR features into EPP solutions.

So, if you are an organization using EPP products that wants to strengthen your network security and threat response with EDR, then you should consult with your cybersecurity solution vendor for the new features/product. Furthermore, ensure that the EDR features are actually capable of mitigating an enterprise-level threat.

Getting the maximum of both EPP and EDR

To strengthen the network security, many small and large businesses are looking out for EDR solutions. But, the catch is, not all the solutions in the market are fully developed yet. But, eScan Enterprise EDR, gives best of both-the-world, providing detailed threat insights, current activity details, and advanced remediation techniques.

How can eScan Enterprise EDR meet your requirements?

At MicroWorld, the R&D team deep researched the market, understood the customers' problems, and grabbed all the requirements. This helped us design and deliver our most advanced product – eScan Enterprise EDR.

The eScan Enterprise EDR :

- Developed with a set of advanced cybersecurity technologies
- Detects even the most sneakiest threats
- Sends alerts to the administrator upon threat detection
- On-the-spot threat remediation at the endpoint level
- Exports detailed reports containing threat insights
- Reduces daily monitoring workloads and strengthens network security
- Does not slow down your network or endpoint performance

At MicroWorld, we believe that the eScan Enterprise EDR will help customers ensure their data belongs only to them. If you have any queries regarding eScan Enterprise EDR, send an email to Enterprise sales team at sales@escanav.com.