EDR とエンドポイントセキュリティ

EDR(Endpoint Detection and Response)

- インシデントデータの検索と調査
- アラートの優先順位付けや、疑わしいアクティビティの検証
- 不審なアクティビティの検出
- 脅威の捜索や、データ探索
- 悪意のある行動の停止

ハッキングの兆候を検知
アンチウィルスと共存、連携
インシデントに対して効果的な対処
検知、記録、攻撃遮断
マルウェアの侵入経路の調査支援

EDR（Endpoint Detection and Response）は、アンチウィルスなど従来のエンドポイントセキュリティ製品に加えて、新種のマルウェアなどのサイバー攻撃の脅威から守るセキュリティソリューションとして期待されています。
Gartner 社では、もともと 2013 年にベンダー、企業、アナリストから意見を集め、主にエンドポイントでの疑わしいアクティビティの検出と調査に焦点を当てたツールについて、Endpoint Threat Detection & Response（EDTR) という言葉を命名していました。その後、Gartner 社は、2015 年以降 EDR を EDTR の同義語として使用しています。EDR の Endpoint Detection and Response を直訳して「エンドポイントの検出と応答」という言葉では、エンドポイントの何を検出して応答するのか目的語が不明瞭でしたが、Threat（脅威）が隠れていたとわかると理解しやすくなります。
EDR が注目されてきている背景には、APT 攻撃のようにサイバー犯罪が巧妙化してきており、 従来のセキュリティツールの監視をすり抜け、知らないうちにマルウェアが侵入し静かな破壊や情報漏洩が進行していても、誰も気づかない場合さえ多くなってきたため、その脅威を可視化する必要がありました。そして、エンドユーザには、IT セキュリティの専門知識が少ないため、その対処方法の判断やアドバイスをしてくれる仕組みが望まれました。
たとえば、アンチウィルス製品を通り抜けてしまうような脅威についても、EDR は、そのアクティビティを検出し、マルウェアで感染した脅威がネットワーク移動をする前にそれらを封じ込めてしまいます。
イメージとしては、アンチウィルスソフトに代表されるエンドポイントセキュリティの製品である EPP（Endpoint Protection Platform）が、主に侵入したマルウェアを検知し、自動的に駆除したりして”マルウェアの感染防止”を目的にしているのに対し、EDR は、マルウェアが検知できず感染してしまった場合においても、攻撃が始まる前に脅威を検知し、その対処方法を提供したり、動きを遮断したり、ログの分析調査など”マルウェア感染後の対応を支援”する製品となります。よって、EPP をリプレースして導入するものではなく、むしろ EPP を補完するエンドポイントセキュリティの製品だといえます。
アプリケーションでもクラウドサービスの利用が多くなると、企業の PC もインターネットを使用する場面が多くなり脅威にさらされる機会も増えました。攻撃側の新種のマルウェアも日々増産されてきているため、従来のパターンマッチングのアンチウィルスの方式では対処しきれない現状があるため、今後 EDR の需要もますます増えていきそうです。