EDR: The Future of Cybersecurity and Incident Response

By Securities Docket on May 8, 2015, 7:21 am

A data breach responder can be a lot like a high-tech plumber. Just like a plumber does when a house's basement floods, data breach responders toil to identify the cause of the breach; combine forces to contain its damage; and collaborate on remediation. But unfortunately, the basement-flood/data breach analogy stops there.

While a plumber can provide reasonable assurances that the basement will not flood again, a data breach responder cannot promise the same about a future data breach. In fact, another breach is not only possible, it's likely.

This is yet another reason why the field of incident response is an upside down one; because data breaches don't define victim companies, ***how they respond to them does***.

And this is also why installing a so-called "endpoint detection and response" or "EDR" tool, though not a silver bullet, will soon likely become a critical aspect of every company's cybersecurity defenses. A little history:

The term "EDR" actually originated as "ETDR," when it was first coined by Gartner's Anton Chuvakin in a July 2013 blog posting. Chavukan conceived of the fresh nomenclature to define the category of tools and solutions that focus on detecting and investigating suspicious activities and issues on hosts and endpoints. Chavukan wrote,

> *This name reflects the endpoint (as opposed to the network), threats (as opposed to just malware and officially declared incidents) and tools' primary usage for both detection and incident response. While some may argue that [the] "endpoint" label may be seen as applicable to workstations and not to servers, this minor loss of precision seems acceptable for the sake of brevity (others will say that four words is already too long).*

In a later November 2014 Report by Gartner Research entitled, "Competitive Landscape: Endpoint Detection and Response," the higher-ups at Gartner apparently shortened Chuvakin's term to *Endpoint Detection and Response* or "*EDR*." According to Gartner's report, EDR is:

> *[A]n emerging security technology market created to satisfy the need for continuous detection and response to advanced threats – most notably to significantly improve security monitoring, threat detection and incident response capabilities. These tools record many detailed endpoint and network events, and store this information in a centralized database for deep detection, analysis, investigation reporting and alerting. Analytic tools are used to continually search the database to identify the tasks*

that can improve the security state to deflect common attacks, to provide early identification of ongoing attacks (including insider threats), and to more rapidly respond to detected attacks.

Core delivered capabilities of EDR include collecting endpoint telemetry and data, centrally storing the information, and performing endpoint post-collection analysis of the data and telemetry information for threat enrichment, anomaly detection and correlation purposes. EDR tools also provide an interactive dashboard with search capabilities, which can generate alerts and mitigation responses based on specific threat indicators, patterns and behaviors.

Why Use EDR Tools?

EDR tools improve a company's ability to detect and respond to outsider and insider threats; enhance a company's speed and flexibility to contain any future attack or anomaly; and help a company manage data threats more effectively overall.

Not only can EDR tools gather and warehouse important data such as system events, network activities and indicators of compromise (IOCs) and then investigate that data in real-time with comprehensive forensic and analytic capabilities, EDR tools also serve a broad range of other more far-reaching purposes, such as:

1. *EDR tools act in concert with traditional signature-based antivirus solution, which are no longer enough to defend against data breaches*. EDR solutions can supplement traditional signature-based technologies for more fulsome behavior-based anomaly detection and more powerful visibility across endpoints. For example, *Advanced Persistent Threat* Attacks or "APTs" are stealthy, sophisticated, targeted and relentless (typically) state sponsored attacks, which use customized targeted malware that can bypass traditional signature based off-the-shelf antivirus products. An EDR tool fills this void by providing insights into an APT attack as well as internal lateral movement of attackers while concurrently performing system/application scans to, for instance, monitor and contain the use of stolen credentials (an oft used APT tactic) across an internal network.
2. *Installing an EDR tools helps mollify and soothe the multiple constituencies impacted by any data breach*. Should a cyber-attack occur, in addition to government-mandated notifications (such as state regulatory notifications), the need to make a host of other important notifications will also arise. Installing an EDR tool by an incident response team after a data breach (as a so-called "leave behind") is an effective and proven means of impressing these corporate constituencies. For example:
    I. Corporate Customers, Partners and Third Party Vendors. Corporate customers, partners and third party vendors will want to know all relevant facts relating to the cyber-attack, especially: if their data has potentially been compromised; if services will experience any disruption; the nature of remediation efforts; if there are any official or unofficial findings any investigation; or if there is any other information which can impact their operations, reputation, etc. These constituencies may ask for weekly or even daily briefings and may also have contractual language establishing their rights when a cyber-attack occurs, which can include: i) notification within a certain amount of time (as low as thirty minutes); ii) on-site inspections; and iii) even the option of an independent risk and security assessment of the victim company (at the victim company's, and not the customer's, expense). Installation of an EDR can help calm these constituencies and demonstrate the seriousness and professionalism of a victim company's response.
    II. Employees. Employees will undoubtedly become concerned and anxious about a cyber-attack, not only because their personal data may have been impacted but also because the future of the company (and their respective jobs) may be at risk. By installing an EDR, a victim company will impress its employees and employees will feel more secure (especially after an attack).
    III. Board of Directors. Increasingly, cybersecurity receives board level attention and scrutiny. After a data breach, a board of a victim company will require briefings, reports and may even hire its own independent investigator to review the findings of any digital forensic investigation. Installation of an EDR can demonstrate to a board the seriousness,

thoughtfulness and expertise of a victim company's response.

3. *EDR tools allow corporate IT departments to focus on running their business operations, as opposed to the exhausting and distracting imposition of staying current with data breach trends and developments*. Developing in-house incident response expertise is a Herculean task – not only because hiring in-house incident response experts is a tremendous challenge, but also because the data breach landscape remains in a constant state of flux. Becoming an expert on malware and the latest data breach techniques is simply not realistic for even the most technically-erudite company. The best EDR developers not only have an understanding of the latest malware exploits but they are also threat research and development organizations, solely dedicated to gathering the latest data breach intelligence.
4. *EDR solutions are not a substitute for, but can rather act in tandem with, other security measures*. EDR tools are complimentary to a variety of other security measures and solutions, including data loss prevention solutions, security information and event management (SIEM) products, network forensics tools and other enhanced security appliances. Just like adding cameras to a home security system does not jettison the need for powerful and reliable locks on all doors and windows, adding an EDR tool to an IT security system does not jettison the need for anti-virus protection, encryption, two-factor authentication and other more traditional security measures.

The Future of EDR

During the past few years, incident response professionals have witnessed the genesis of a brand new marketplace of dedicated incident response solutions known as EDR tools. A common complaint about traditional data breach protection toolsets is that they do not detect quickly or nimbly enough to counter the more sophisticated and clandestine data breaches that have begun to afflict public and private companies. EDR tools have emerged to pick up the slack.

Typically installed within an entire attack vector including domain controllers, database servers and user workstations, the innovative real-time "intelligence feeding" of EDR tools will become the standard for corporate cybersecurity.

In addition, EDR technologies provide a richer depth of behavior based anomaly detection and visibility into information relevant for detecting and mitigating advanced threats of all varieties. For example, regulated financial entities and SEC filing public companies must detect, identify, investigate and mitigate advanced forms of malware but they also must combat internal threats and malfeasance. By providing instant aggregate threat information and decreasing the so-called "dwell time" of targeted attacks, EDR solutions enhance enterprise visibility and can become a useful tool for countering insider threats, conducting internal investigations and improving regulatory responses.

For instance, most internal investigations kick off with manual data acquisition, file-system forensics and log file analysis on data aggregated and collected *after* the triggering event. By providing proactive *continuous* monitoring and recording of all activity on endpoints and servers, EDR tools reduce the need for such "after-the-fact" data collections. Thereby EDR tools can dramatically decrease the cost, complexity and time of traditional internal investigations and regulatory response while simultaneously accelerating the identification of not just the root causes and attack vectors of data breaches but also root causes of other types of unlawful behavior, such as theft perpetrated, or operational disruption caused, by a "bad leaver." An EDR tools can also impresses regulatory examiners by providing real-time and comprehensive responses to regulatory requests.

Unfortunately, like any other technology product marketplace, the EDR marketplace is not only complex but it is also replete with cybersecurity jargon and high-tech assurances. In the coming weeks, I will attempt to sift through all of the noise and offer guidance on EDR toolkit selections in plain English, from my perspective as a seasoned incident responder of over 20 years. My posts will help corporate executives identify the right EDR product for their company and offer a valuable resource for understanding current EDR solutions available in the marketplace.

Some of the more popular EDR systems include Carbon Black, FireEye MIR, Tanium, RSA ECAT, CounterTack, CrowdStrike, Cyberreason, Triumfant and several others. Clearly, the EDR marketplace is still

in its infancy while competition remains intense among current and future innovators.

Stayed tuned for some straight talk on the EDR market players — because I will be writing about them all.

Posted in Risk Mgmt, Stark on IR, Top | Tagged EDR, Endpoint detection

Securities Docket