DOCKET MEDIA LLC
PHONE: (424) 2-DOCKET
WWW.CYBERSECURITYDOCKET.COM
EDITOR@CYBERSECURITYDOCKET.COM

CYBERSECURITY DOCKET
GLOBAL CYBERSECURITY AND INCIDENT RESPONSE REPORT

STARK ON IR OCTOBER 16TH EDR Tool Review: Carbon Black

Recently, a wave of dedicated incident response solutions known as "endpoint detection and response" or "EDR" tools have come into being. I wrote about this phenomenon a few months back, and promised to report back on the various companies that sell EDR tools and solutions.

Today I am presenting the first of my reports, a neutral and objective discussion of Carbon Black, which from where I sit, is an EDR powerhouse. A few research notes: 1) I actually deployed Carbon Black in the context of a large data breach response engagement; and 2) Last week, I spoke at length with Ben Johnson, one of the Founders of Carbon Black (with whom I had never met or spoken before).

Some Background on EDRs.

Typically installed within a swath of IT equipment including domain controllers, database servers and workstations, EDR technologies provide an ongoing rich and in-depth of behavior-based anomaly recognition and acute visibility into threats of all varieties, not just malware. By providing instant aggregate threat information and decreasing the "dwell time" of targeted attacks, EDR solutions enhance enterprise discernibility and help counter internal threats and malfeasance.

For instance, suppose a corporate network scan reveals an indicator of compromise or some other anomaly or form of malware in its systems. Of course, many immediate questions arise such as: How did the file get there? How long was it there? Where has that file been before being detected? What other computers has it been opened on? If it executed, what did it do?

For most organizations, the requisite information required to answer these questions is not being actively captured. This is why most internal data breach investigations kick off with manual data preservation and acquisition, file-system forensics and log file analysis on all of the data amassed and collected after the suspected breach – which is too often a time consuming, costly and tedious IR drill. By providing continuous monitoring and recording of activity on endpoints and servers, EDR tools tackle this challenge head-on.
EDR tools reduce the need for such after-the-fact costly and wearisome data collections while also: 1) accelerating the identification of root causes and attack vectors of data breaches; and 2) decreasing the cost, complexity and time of internal investigations and regulatory response.

The New EDR Paradigm.

EDR tools have quietly ushered in a new generation of cybersecurity, geared more towards the cybersecurity paradigm of *response* rather than *prevention and detection*, which is far more realistic and effective. Every company can experience a data breach – and probably already has. That is why companies need to shift cybersecurity practices away from prevention and detection and recalibrate cybersecurity into a more effective archetype of response.

When companies trying to prevent data breaches rely too much upon customary protections of intrusion detection and firewalls, they are just as misguided as parents trying to prevent their kids from catching colds by relying upon hand washing and multiple clothing layers. The smarter method for combating data breaches (like colds) is to focus efforts and preparation on how to contain, treat, and cure the problem, as fast and as painlessly as possible. Company executives should preach this realism, rather than the fantasy of ironclad security.

EDRs are the foundation of the new paradigm of cybersecurity: where technological infrastructure has expanded dramatically; where data-points reside on multiple platforms (including employee devices, vendor networks, and the cloud); and where data breaches don't define victim companies; how they respond to them does. Carbon Black embraces this new paradigm.

Carbon Black: What Does it Do?

Through continuous endpoint recording, customized detection, live response, remediation, and threat banning, Carbon Black makes advanced threats easier to see and faster to contain. The Carbon Black solution provides continuous, real-time visibility into what's happening on every computer, real-time threat detection and alerts and a proactive and customizable lens into the "kill chain" of an attack.

Carbon Black abandons traditional signature detection, which has failed so many companies in so many ways. As famed cybersecurity blogger Brian Krebs has written, "In short, as I've noted time and again, if you are counting on your antivirus to save you or your co-workers from the latest threats, you may be in for a rude awakening down the road."

Carbon Black's data gathering is forensically sound and does not alter any of the inherent characteristics of the data it collects or copies. Carbon Black is also attentive of privacy concerns by "anonimizing" the data it collects (rendering it essentially as metadata).

Specifically, Carbon Black boasts five core capabilities: visibility, detection, response, protection and integration.

Carbon Black: Visibility.

Rather than scanning reactively, Carbon Black continuously records the critical data necessary to utilize multiple forms of threat prevention, builds customized threat detection and responds at the moment of compromise. This means that Carbon Black gathers the relationships of every file execution, file modification, registry modification, network connection and cross-process event while maintaining a copy of every executed binary for all major operating systems (Windows, Mac OS X, and Linux).

Rather than requiring remote connections, Carbon Black stores historical data in a central facility, deployed onsite or in the cloud as a hosted service for rapid one-stop-shopping remote access. From one console, one investigator can analyze an entire enterprise. This dramatically reduces the initial (and very costly) phase of incident response where preservation of data and access to data can take weeks.

By replacing reactive "after-the-fact" manual data acquisition with proactive continuous monitoring and recording of all activity on endpoints and servers, Carbon Black offers IR teams the ability to "roll back the tape" to identify the root cause of an attack, which is one of the most critical aspects of any IR investigation. This retrospection is what makes EDR tools so different – and so powerful. Through Carbon Black's gapless recorded history and visualization of the entire attack kill chain, IR teams, whether internal or external, can respond and recover at the moment of discovery.

So many times, an IR team arrives on site and historical data is lost, piecemeal or otherwise incomplete, which can trigger criticism, not just from customers, vendors and partners but also from regulators and law enforcement. By maintaining a data repository of relevant breach information, companies can avoid the inevitable bevy of faultfinders who come forward after a breach (and who can exert extraordinary drag upon an otherwise blameless and hard working management team).

A central data repository also curtails the typical legal fees incurred from custodian interviews. By maintaining a centralized data repository of a methodically stored historical data-set, there is less of a need to interview custodians about what data resides on their machines.

In fact, Carbon Black's consistent and technologically supported methodology for data collection is probably more trustworthy, more convincing and more reliable than information gained from custodian interviews. Interviews about the data stored on a custodian's workstation have always been problematic; no matter how technically savvy or experienced, users (and even administrators) rarely understand precisely what data resides on their own machines and are seldom in a position to testify competently along those lines.

Carbon Black: Detection and Response.

Carbon Black's threat feeds enable security teams to monitor and examine threat vectors across systems such as files executing from the recycle bin, suspicious process names or extensions, backdoor installations, ransomware, host file modifications, firewall tampering, malformed documents, suspicious attack processes, geolocation, spear phishing attacks and more.

Purchasing a Carbon Black license includes threat intelligence Carbon Black has aggregated from millions of endpoints to design and publish actionable indicators of malicious attack behaviors and compromise. Many IR firms maintain their own libraries of indicators of compromise but given Carbon Black's continuous data gathering, their research teams deliver a handy intelligence library, perhaps even more comprehensive and current than the best IR consulting firm.

Carbon Black also offers their own *Threat Intelligence Cloud's Attack Classification Service,* which provides wide-ranging attack context and attribution to assist enterprises in identifying the type of attacker, country of origin, related attacks, and their tactics, techniques and procedures.

I am always skeptical of attacker profiles. In my experience, attacker profiles are often wrong and identifying them can become too much of a distraction from the important tasks at hand, such as containment and remediation. However, the multiple constituencies impacted by a data breach want to know the identity of the attacker, especially if the culprit is a foreign government. Moreover, when a company investigating a data breach cannot ascertain at least some of the identifying traits of the attackers, the company risks appearing weak, clumsy or even inept.

Along those lines, Carbon Black's Classification Service could be useful in assuaging the concerns of the many impacted constituencies of a data breach, especially customers, partners, vendors, regulators, law enforcement and even employees – all of whom expect a breach victim to discover some intelligence relating to the attackers.

Carbon Black: Protection.

When network security or malware detonation solutions detect malware on the network, Carbon Black records where the malware landed, if it executed and what other files or processes were spawned as a result. Carbon Black looks for any sort of anomaly, such as file registry changes; unfamiliar executables; driver activations; file system changes; unusual network logging; and other variances.

Similarly, Carbon Black need not be implemented into an entire network. Carbon Black can be loaded only on to key servers and core infrastructure systems, and user groups that require much tighter control of their systems, thereby providing an easy way of keeping administrators from adding unnecessary and/or dangerous tools to key servers.

Carbon Black: Integration.

A big concern about every cybersecurity solution is whether it can successfully integrate into an IT environment and become a reliable, and not disruptive, component of a company's security stack. CISO's, CIO's and CTO's also worry about so-called "agent fatigue," where IT administrators must monitor: agents relating to antivirus; host based agent intrusion detection systems; compliance agents to track software; and the list goes on. Moreover, different agents serve different purposes, communicate to different control servers, and may even be managed by different IT groups, inadvertently creating a disjointed cybersecurity hierarchy.

Carbon Black reduces agent fatigue in two ways. First, by combining into one function what many discrete agents may already be doing, Carbon Black reduces the number of agents required in a system. Second, Carbon Black was engineered and designed to be light weight, minimally invasive and easily integrated. Carbon Black's activities have no impact on the endpoint and are "low impact" overall; its work is carried out by the server (e.g. looking for: patterns not looking for specific hash; IP or domain information; unusual files; or strange behavior).

In other words, given that Carbon Black maintains real-time, always on communication, its activities remove the stress off of the endpoint by leveraging back end servers. No scans, no need to wait for off hours for results, and Carbon Black's agent reportedly sits at less than 1% CPU, a very light weight.

I have worked a data breach response where Carbon Black was installed quickly (within days) and, with a little help from Carbon Black's technicians, we were able to report to customers, to regulators and to

partners, that Carbon Black was up and running. This gave senior executives within the company, as well as skeptical constituencies outside the company, some immediate confidence that the data breach response was vigorous, thoughtful and on track.

Though any system's assimilation into network security, analytics and SIEM can present challenges for any IT environment, the light weight genetics of Carbon Black's tool together with their now experienced integration team, foretells a quick and easy implementation process. Like beefing up a home security system, there may be a need to punch a few dry wall holes, but in the end, the disruption is relatively minor.

Carbon Black Alliances.

Over 60 IR firms have already made Carbon Black a core component of their detection and response services, including for example, Kroll, who are part of the Carbon Black Alliance Program. According to Kroll, combining an IR firm with a tool like Carbon Black strengthens overall security posture, speeds up deployment times, and leverages the integration for a cheaper overall cost. "Equipping our expert teams with Carbon Black streamlines the response and recovery process more than ever before," notes Tim Ryan, Kroll's managing director and head of the cyber investigations practice (and a former FBI Supervisory Special Agent who investigated cyber attacks). "By joining [the Carbon Black Alliance] program, we are combining the best people and best technology on the market to battle against advanced attacks and targeted malware."

Carbon Black Clients and Costs.

Carbon Black has grown dramatically in the past few years, and now has over 450 employees and 800 existing clients (2000 clients if you includes their Bit9 product, which is a related product offering), with licenses attributed to companies with as many as hundreds of thousands of endpoints to as few as 50. Subscription costs for a license are typically for one to three years, with a rack rate of $30 an endpoint for a year (an endpoint can be as simple as a computer or laptop or as dynamic as a high-powered Linux server – and anything in-between). Carbon Black provides a 30-day evaluation period for its clients as well as training and onsite technical assistance.

Carbon Black also allows clients to "throttle" the data it collects and aggregates, and build a customized data repository uniquely suited for a client's capabilities and requirements, either in one data set or individual subsets (and if desired, each with different lifespans).

Carbon Black's cost may be more than the licensing fee because clients will have to add headcount to handle the influx of more intelligent and richer information. But the cost savings will also be exponential over time, given the tool's rapid response capabilities and the reduction of the typical preservation and "lather rinse and repeat" digital forensics of most data breach response workflow. Carbon Black specifically asserts that after installing Carbon Black, customers do more with less so while it is perceived to require more headcount, that is usually not the case. Having said that, Carbon Black seeks a more long term relationship with its customers, because Carbon Black's customers are looking at Carbon Black "to really help them revamp their program and become cyber security rock stars."

Conclusion.

Traditional cybersecurity technology controls such as signature based technology and antivirus are being purposely bypassed by customized targeted malware attack toolkits and advanced, organized, persistent attackers. Along those lines, many organizations have already conceded that their traditional anti-malware defenses have failed and that an endpoint detection strategy is the best solution.

Some have even conceded that the real-time "intelligence feeding" of EDR tools will soon become a corporate cybersecurity standard, surpassing antivirus as the cornerstone of the typical cybersecurity security stack; I am firmly in their camp. In my view, EDR will be adopted into security mandates such as PCI and other regulation-based security requirements (which are already vague and are constantly evolving).

In short, Carbon Black is a strong solution. It is a powerful IR tool, not just skillfully and elegantly engineered, but also serviced by a proven, experienced, motivated and talented corporate team.

After a data breach, impacted constituencies (such as customers, partners, vendors, regulators and the rest) clamor for innovative solutions to aid attack detection and to strengthen incident response. I have witnessed first hand how Carbon Black can impress these victim constituencies, and though not a panacea or silver bullet, can evidence robust IR competence and wherewithal.

I suggest considering Carbon Black for any corporate enterprise. Ask for a demo -- as I learned long ago during my first year in law school: *res ipsa loquitur* (the circumstances speak for themselves).

Stay tuned for more reviews . . . next up: Tanium.

John Reed Stark is President of John Reed Stark Consulting LLC, a data breach response and digital compliance firm. See www.johnreedstark.com. Formerly, Mr. Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, the last 11of which as Chief of its Office of Internet Enforcement. He has also served for 15 years as an Adjunct Professor of Law at the Georgetown University Law Center, where he has taught several courses on the juxtaposition of law, technology and crime. He also served for five years as managing director of a global data breach response firm, including three heading its Washington, D.C. office.

DOCKET MEDIA LLC
PHONE: (424) 2-DOCKET
WWW.CYBERSECURITYDOCKET.COM
EDITOR@CYBERSECURITYDOCKET.COM