HOW TO PICK A WINNER IN EDR

The endpoint security marketplace is crowded with vendors claiming to have superior capabilities. Cutting through all the marketing and sales pitches to understand how these products perform isn't easy. Luckily, The MITRE Corporation conducted an independent test of the detection and investigation capabilities of leading endpoint detection and response (EDR) products against real-world attack sequences. We'll break down MITRE's methodology, the results, and what it all means for your organization as you assess your current and future endpoint security toolkit.

Insights from the MITRE ATT&CK Evaluation

Independent research organization The MITRE Corporation released the final Round 1 results of its MITRE ATT&CK™ cybersecurity evaluations.[1] These evaluations put the detection capabilities of leading endpoint security tools to the test by emulating attack sequences of real-world adversaries, with the first round focusing on techniques used by the APT3 group.

In this evaluation, MITRE intentionally avoids directly comparing vendors, instead opting for a scientific approach that captures and categorizes each tool's detection and investigation capabilities for different real-world attack techniques.

To derive insight from the MITRE results, Josh Zelonis, senior analyst at Forrester Research, offers an objective third-party framework for scoring and evaluating the efficacy of tested products. His report[2] applied a public scoring methodology to the quantity and quality of detections to compare vendors and analyze the EDR marketplace.

Adding up all of the detections and applying Forrester's weightings, Forrester's framework shows Cortex XDR™ by Palo Alto Networks as providing the best visibility, by a significant margin, for detection and investigation in the EDR marketplace. Cortex XDR—along with Traps™ endpoint protection and response—outshined the competition in multiple areas, including the highest coverage, fewest misses, and best enrichment of any product tested.

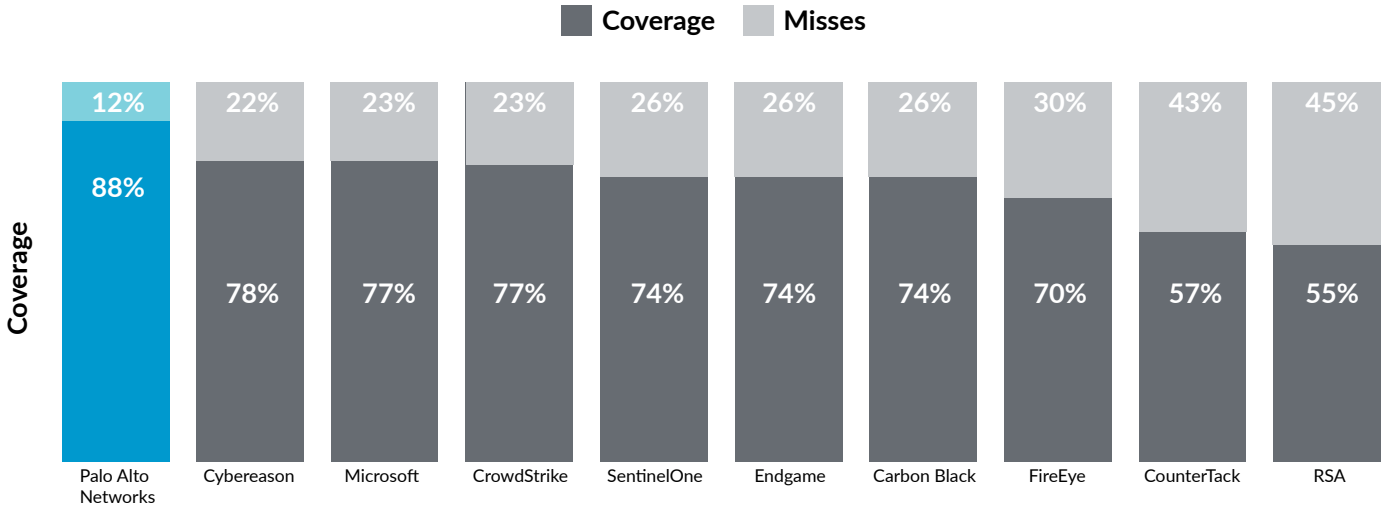

Figure 1: Coverage and misses across the marketplace

Evaluating new technology requires a tailored, comprehensive assessment. In this paper, we'll take a deep dive into the MITRE ATT&CK evaluation methodology and Forrester's analysis to assess which capabilities these independent firms deemed important. Then, we'll provide further analysis on the capabilities MITRE tested to help you evaluate which EDR tool is right for your needs.

Key Takeaways

- **MITRE and Forrester offer a starting template for security assessment.** It's just as difficult to keep up with the evolving threat landscape as it is to wade through contradictory vendor claims about why their products are the best. Although different organizations weigh various criteria differently, MITRE and Forrester have laid objective groundwork to help organizations understand the strengths and weaknesses of their current endpoint security as well as any potential investments.
- **SecOps teams require more than just endpoint data.** As if security teams weren't spread thin enough, they're also stuck with an incredibly fragmented set of tools. Consolidating capabilities into a robust platform means faster response, better security, and much less wasted time. Savvy SecOps teams will embrace tools that can correlate various sources of data to find threats that siloed tools may miss, including vulnerabilities in unmanaged endpoints.
- **Cortex XDR delivers unparalleled visibility.** Paired with Traps for endpoint protection (included), Cortex XDR delivers the greatest coverage across the attack life cycle, with the fewest missed techniques, high correlation, and zero delayed alerts. Furthermore, MITRE only tested EDR capabilities, but Cortex XDR delivers a number of additional critical capabilities, such as superior prevention and the ability to stitch together network, cloud, and endpoint data.

1. "MITRE ATT&CK Evaluations," The MITRE Corporation, accessed June 17, 2019, https://attackevals.mitre.org/evaluations.html.
2. "The Forrester MITRE ATT&CK Evaluation Guide," Josh Zelonis et al., May 21, 2019, https://www.forrester.com/report/The+Forrester+MITRE+ATTCK+Evaluation+Guide/-/E-RES147475.

Explaining Round 1 of the MITRE ATT&CK Evaluation

MITRE ATT&CK is a "globally-accessible knowledge base of adversary tactics and techniques based on real-world observations." The MITRE ATT&CK matrix encompasses hundreds of different techniques in 12 different categories (see figure 2). In a real attack scenario, an attacker ties together a logical sequence of techniques across these categories to gain access, run commands, extract information, and perform other actions. To emulate the real world, MITRE has broken its evaluations into rounds, each of which uses common strategies and techniques of a known real-world adversary.

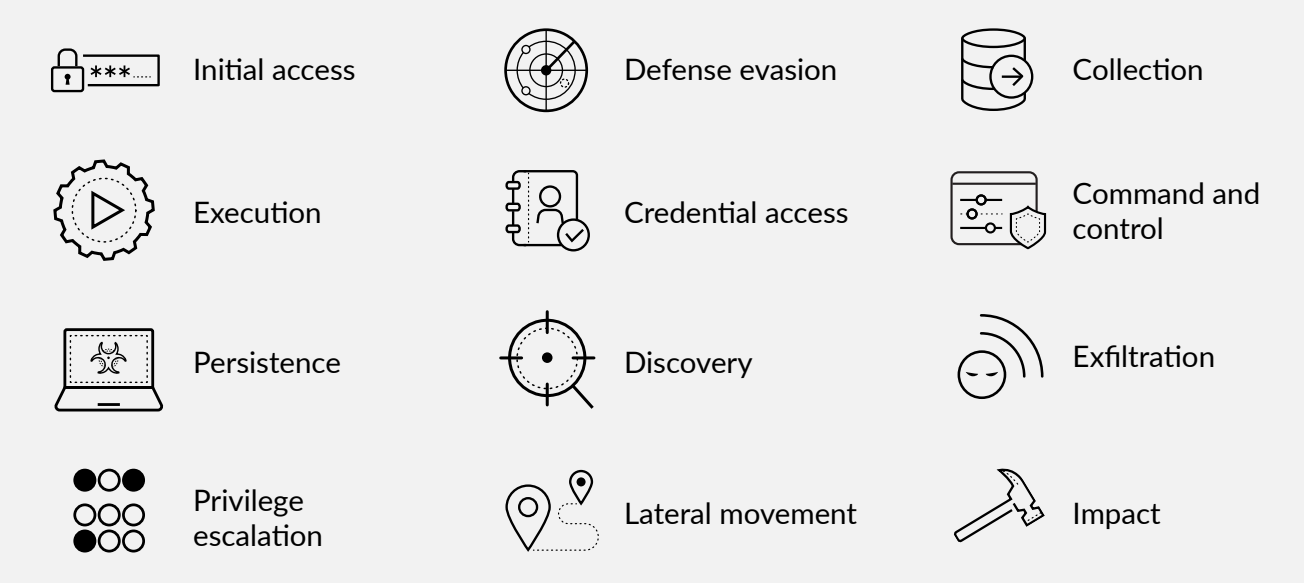

Figure 2: Categories of the MITRE ATT&CK Matrix

Round 1 was designed to emulate the APT3 group, a sophisticated adversary group associated with nation-state activity, which has a history of using browser-based exploits to harvest credentials. APT3 attacks frequently issue on-keyboard commands, take control of trusted programs, and move laterally to additional hosts. In this round, MITRE chose a series of 56 Enterprise ATT&CK techniques to represent several APT3 attack scenarios.

MITRE used publicly available threat emulation tools Cobalt Strike™ and Empire to orchestrate attacks against each vendor tested. For each technique, MITRE documented whether a detection occurred and, if so, the type of detection, on a scale from the lowest (no detection) to the highest (an alert with information about the specific threat). Tools that gathered telemetry data for threat hunting purposes but did not generate alerts scored in the middle of the scale (see figure 3).

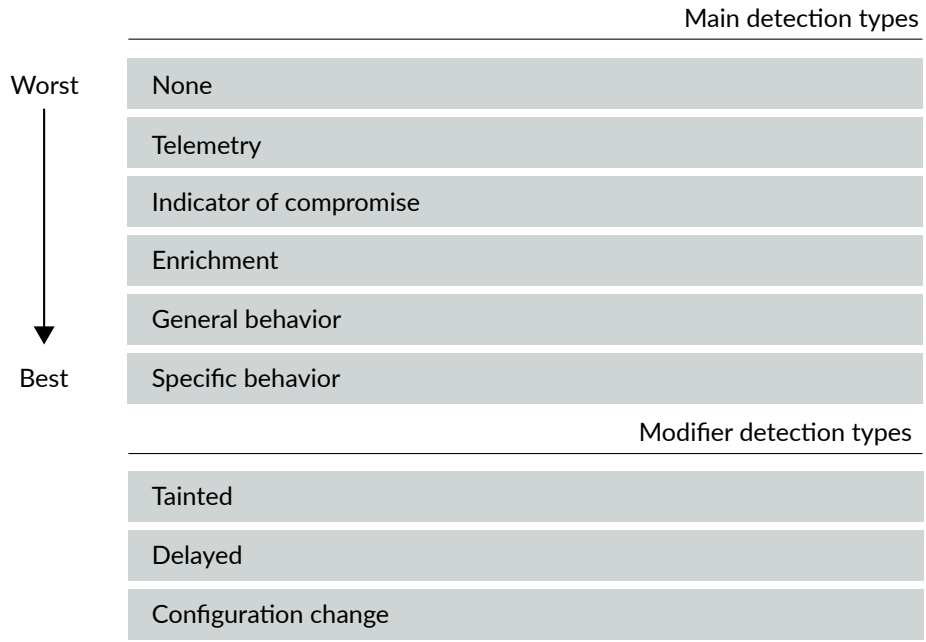

Figure 3: MITRE detection scale

On top of these categorizations, MITRE applied modifiers as necessary:

- **Tainted:** If a detection occurs immediately because of an association with a previously discovered malicious behavior, it's marked as "tainted." This is ideal.
- **Delayed:** The detection did not occur in real time, but it eventually got there.
- **Configuration change:** Any detection was made possible only because the vendor changed the initial configuration.

Layering on Forrester's Analysis

Based on the aforementioned criteria, Forrester has applied scores to each detection (see figure 4), also giving zero points for any detection that only came about via a configuration change.

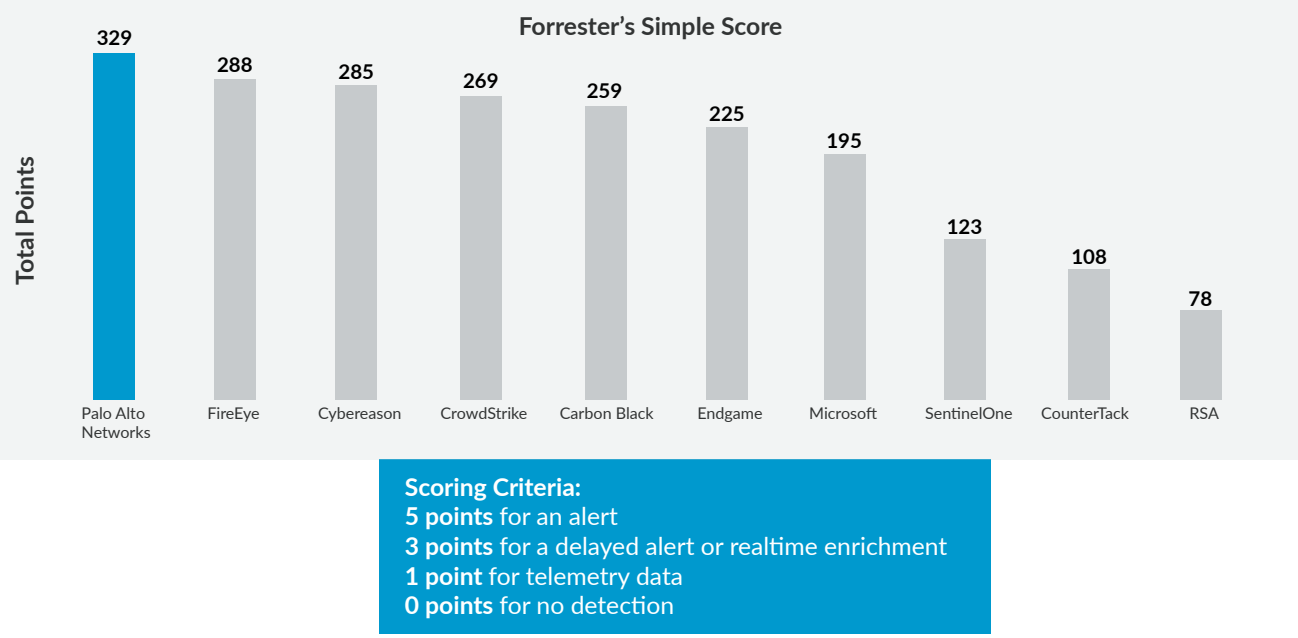

Figure 4: Scores by vendor

Forrester's evaluation goes into greater depth, assessing EDR tools and strategies based on three key metrics:

- **What percentage of techniques were detected?** Regardless of the type of detection, the bottom line is that a technique must be detected for an analyst to have any chance of investigating and remediating it.
- **What percentage of detections were tainted?** In the context of detection, the term "tainted" is a good thing. Data is deemed tainted if it is correlated to other malicious or suspicious events. Almost no action is inherently "bad" on its own—it's how techniques are tied together that indicates an adversary may be operating in the system.
- **How does the product perform across the kill chain?** The kill chain—which Palo Alto Networks calls the attack lifecycle—describes the full set of objectives an adversary must achieve over the course of a successful attack. Detecting and stopping an initial access technique is great, but if an adversary comes to a roadblock, chances are they'll look for an alternate route. Evaluating a product across the attack lifecycle shows its ability to provide defense in depth and indicates a more mature, comprehensive tool.

How Cortex XDR and Traps Performed

Cortex XDR discovered 88.9% of techniques (see figure 5), missing only 11.1% of 136 threats. The next-best vendor missed 21%, which equates to leaving security teams blind almost twice as often. Most techniques were correlated with and enriched by other data points, meaning that analysts received contextualized, actionable alerts rather than standalone data points that may not represent actual threats. Cortex XDR showcased its ability to detect across the entire attack life cycle without a single missed objective. Overall, the MITRE evaluation and Forrester analysis highlighted that Cortex XDR is elite among EDR tools, providing unrivaled detection.

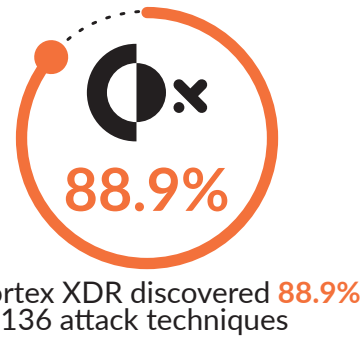

Figure 5: Cortex XDR coverage

Any Way You Spin It

Naturally, there are numerous other ways to analyze the data. It's important to take an in-depth look at how various tools may fit your organization's particular needs and strategies. Your security team may value certain types of detection over others or prioritize coverage in a certain part of the attack lifecycle. You may want to consider some additional analysis points.

Delayed vs. Realtime Alerts

Forrester's analysis combines delayed alerts and enrichments into one category. However, these detections are not the same, which may make a difference to your security operations team. In many instances, delayed alerts indicate the tool itself missed the alert, but a managed service monitored the telemetry data and manually generated an alert after the fact. The risk with delayed alerts is that, in the case of stopping a real adversary before they can do damage, the hours, minutes, and even seconds matter.

Vendors with no delayed alerts display a reliance on the technology, rather than an analyst, to make the detection. Cortex XDR had no delayed alerts, which highlights our strategic decision to develop tools that use robust threat intelligence, out-of-the-box rules, and machine learning to automate detection and correlation. As a result, Cortex XDR can reduce the mean time to respond (see figure 6).

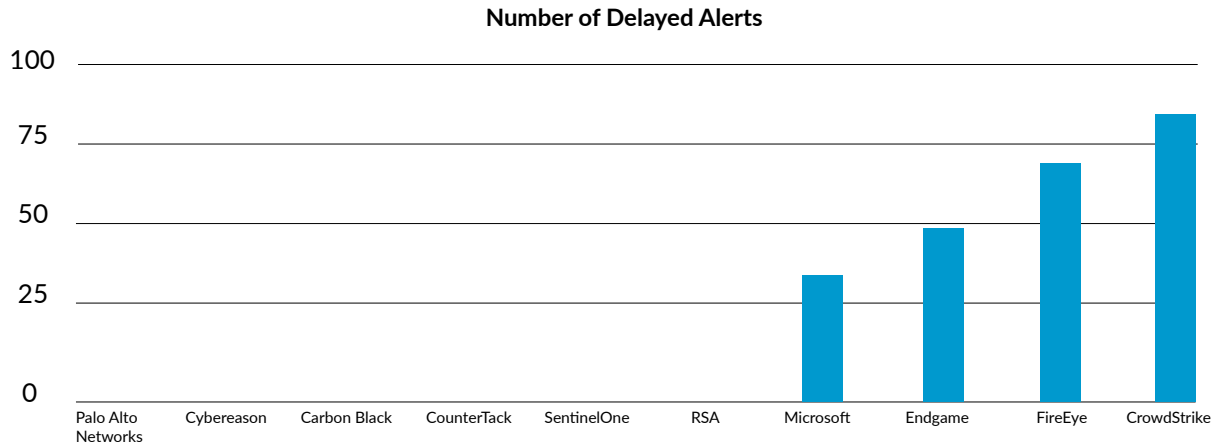

Figure 6: Number of delayed alerts by vendor

Alerts vs. Telemetry

Not all alerts are created equal. According to industry estimates, tools may generate more than 100 alerts for each actual threat—a false positive rate that can easily lead to real threats being overlooked or ignored (note that the MITRE ATT&CK evaluation did not test for false positives). At the same time, an EDR tool that generates no alerts is only useful for threat hunters who already have a good idea of what they're hunting.

There's a sweet spot somewhere in the middle. The ideal tool generates only high-quality, specific, prioritized alerts. For other potentially—but not likely—malicious behavior, your EDR tool should still capture and correlate telemetry data for investigation and threat hunting, but you may not want the tool to generate an alert that has a high likelihood of being a false positive. Further, you want your EDR tool to enrich telemetry data with additional context, making it quicker and easier for an analyst to derive meaning from it.

With its default configuration during the MITRE test, Cortex XDR generated 20 realtime, specific alerts and 82 enriched telemetry logs (see figure 7). In a real deployment, customers who connect additional network and cloud sensors into Cortex Data Lake give Cortex XDR even more visibility and context into the behavior of potential threat actors, further reducing false positives and improving identification of malicious behavior that may otherwise seem benign.

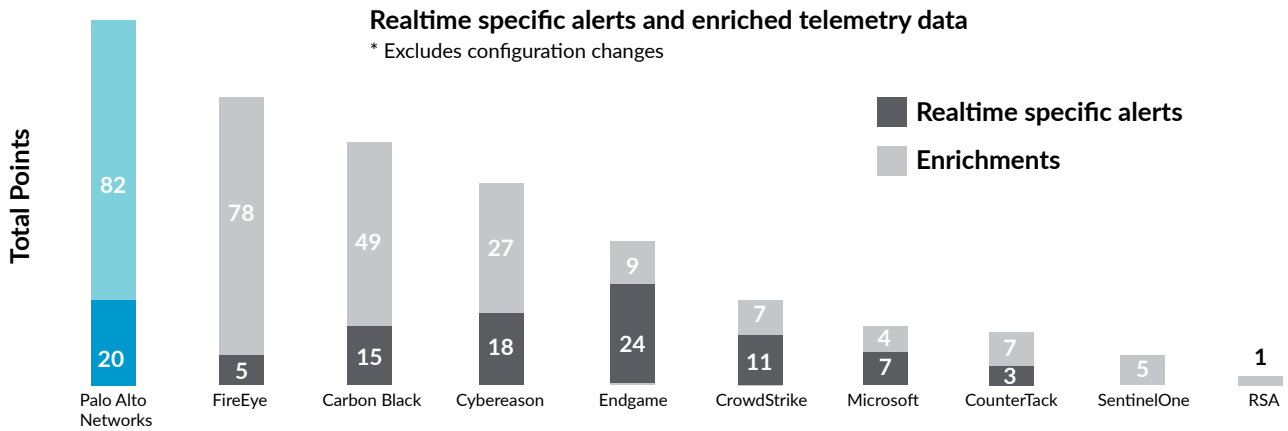

Figure 7: Realtime specific alerts and enriched telemetry data

EDR Is Not Enough

Security teams struggle with inefficiency, with a **mean time to identify (MTTI) of 197 days** and a **mean time to contain (MTTC) of 69 days.**[3] The Ponemon Institute has found that, since the advent of EDR, this inefficiency has only gotten worse. Adding more siloed tools is not the answer. Building EDR into an effective endpoint security program requires a more holistic and integrated approach.

First comes prevention with powerful endpoint protection—something Traps does exceptionally well (though prevention was turned off for the MITRE test). It's always better to prevent an adversary from entering your environment than to detect the adversary after the fact. The more you prevent up front, the fewer incidents your analysts will have to remediate.

Next comes broad visibility into your infrastructure, including the 10% to 20% of endpoints not under management, such as most internet of things (IoT) devices. This is where EDR, tightly integrated with user and entity behavior analytics (UEBA) and network traffic analysis (NTA) capabilities, is most useful. An integrated platform should detect threat actors who circumvent the first line of defense and follow their actions throughout the infrastructure. It should recognize when a string of behaviors is malicious or benign. Then, it should share those findings and coordinate response with endpoint and network protection technologies, ensuring all systems are updated and working together.

A simplified, integrated, and comprehensive platform is the right strategy to optimize your security today as well as build scalable security operations to handle the threats of the future. It should empower your security analysts—who are routinely overloaded with events, frequently forced to prioritize and ignore legitimate threats, and constantly waste time switching between tools—to focus on what matters.

Figure 8: EDR priority per ESG research[4]

The Cortex XDR Difference

Cortex XDR is the world's first cloud-based detection and response app that natively integrates network, endpoint, and cloud data to stop sophisticated attacks. We designed Cortex XDR from the ground up to help organizations secure their digital assets and users while simplifying operations. Machine learning and AI models uncover threats from any data source, including managed and unmanaged devices, with unrivaled accuracy.

Cortex XDR helps accelerate investigations by providing a complete picture of any alert or threat. It automatically stitches together different types of data and reveals the root cause, allowing analysts of all experience levels to perform alert triage and incident investigation in one console. Tight integration with enforcement points lets security teams respond to threats quickly and apply the knowledge gained from investigations to detect similar attacks in the future.

Some security teams need assistance managing tools like Cortex XDR. We have partnered with the best managed detection and response (MDR) providers to serve as or augment your security operations team. Each partner brings years of security operations experience, providing instant maturity with proactive, 24/7 coverage and market-leading detection and response times.

To learn more, visit our website or read the Cortex XDR datasheet.

3. "2018 Cost of a Data Breach Study: Global Overview," The Ponemon Institute, July 2018, https://veriphyr.com/the-2018-cost-of-data-breach-study-a-global-overview.
4. "A Promising New Chapter in Detection and Response Tools," Enterprise Strategy Group, May 28, 2019, https://www.esg-global.com/blog/a-promising-new-chapter-in-detection-and-response-tools.

CORTEX BY PALO ALTO NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

how-to-pick-a-winner-in-edr-wp-102819