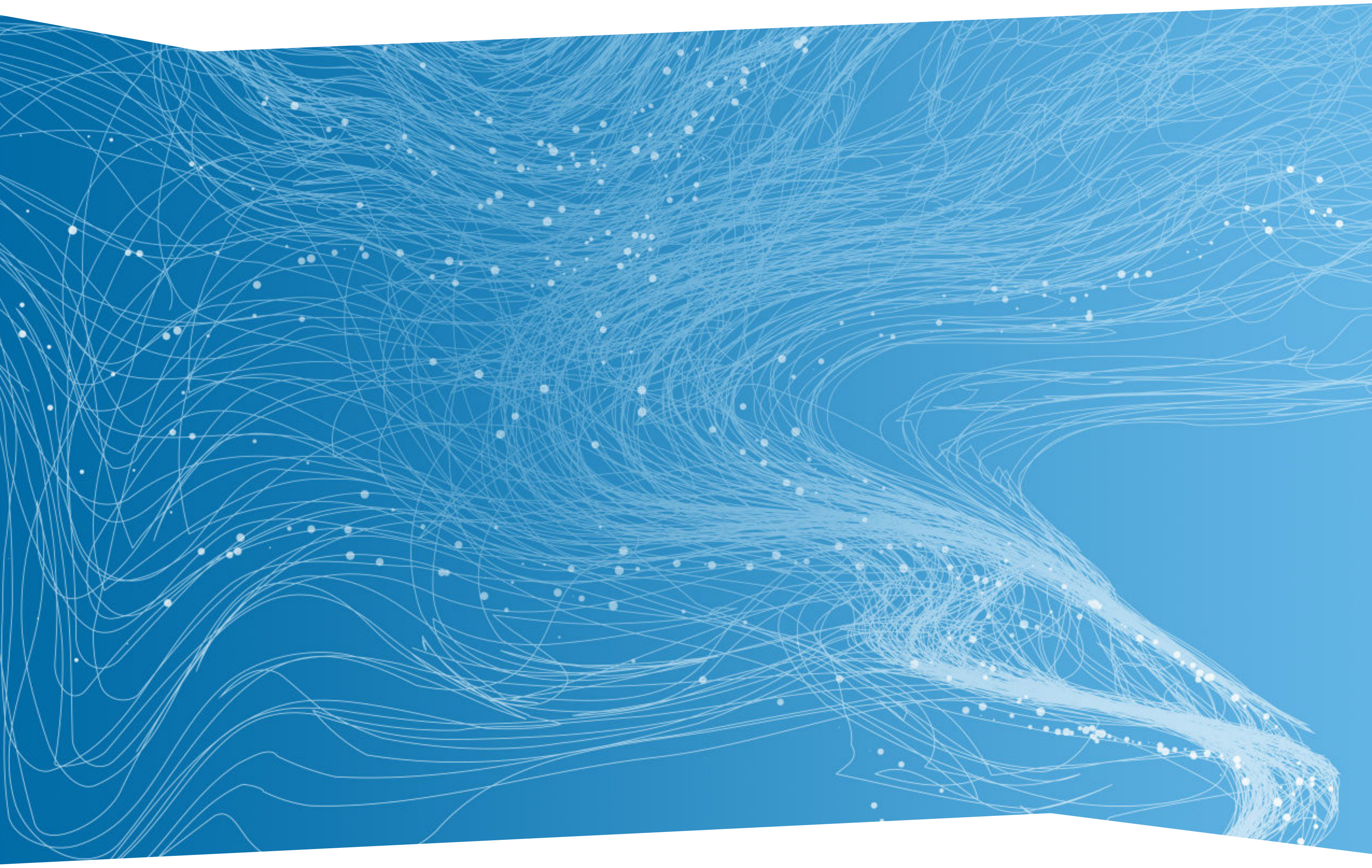

WHITEPAPER

BEYOND ANTIVIRUS

PROACTIVE THREAT HUNTING AT THE ENDPOINT

In 1986, the "Brain" boot sector virus caused the first widespread realization that bad actors could (and certainly will) exploit personal computers as attack vectors. In the intervening years, threats have become much more common, diverse, and sophisticated.

Viruses like Brain gave rise to a generation of signature-based antivirus (AV) tools that remains ubiquitous today. These tools are designed to receive the signatures of new viruses as they are discovered, and protect the endpoint from infection from them. Newer generations of AV have augmented signature-based approaches with heuristics and analytics that seek to identify and protect against even unknown threats. These "Next generation antivirus" (NGAV) vendors have continued to raise the bar on virus detection, seeking to match the increasingly sophisticated methods used by the virus creators. Thus, the once-simple AV market has evolved to a category known as an "Endpoint Protection Platform" (EPP).

Yet this game of cat-and-mouse is virtually unwinnable. That's because, even if an AV program can catch and neutralize the vast majority of threats, it only takes one miss to cause major problems. A virus operating undetected on a computer or network can steal user data, keystrokes, or intellectual property, or even take down an organization's IT infrastructure. Because of this dynamic, Gartner advises organizations that "systems are assumed to be compromised and require continuous monitoring and remediation."[1]

And, unfortunately, this is not a hypothetical risk. Threat actors target the well-known weaknesses of AV, and even next-gen AV, in their exploits. This is why 90% of malware samples are specific to the targeted organization[2], thus neutralizing tactics that look for exploits "in the wild." It's why a favorite delivery vector is highly-targeted "phishing" emails, which are responsible in 30% of breaches[3]. The principle of "dwell time" is central to today's threat actors, who realize that maximizing the interval between infection and remediation is the single biggest factor in a successful attack. This is why 93% of exploits take mere minutes to compromise an endpoint[4], while time to discovery continues to increase.

[1] Gartner, "Designing an Adaptive Security Architecture for Protection From Advanced Attacks," February 2016

[2] Verizon 2015 Data Breach Investigations Report

[3, 4] Verizon 2016 Data Breach Investigations Report

To successfully combat today's varied and sophisticated threats, a proactive approach is needed. EPP's essentially reactive approach to computer security is, to use the old canard, necessary but insufficient. While it's essential to take an AV-based preventive approach to eliminate as many threats as possible before they impact your business, it's simply no longer possible to catch them all.

The constantly evolving nature of threats has given rise to a new model of defense called "Endpoint Detection and Response" (EDR). This differs from the EPP protection model in subtle but fundamental ways, adding a more advanced layer of security that detects, identifies and addresses threats based on what they do, not necessarily how they present as malicious software.

EDR solutions are generally designed to record certain endpoint activities and events, which are stored either locally on an endpoint or centrally on a server. Then, these solutions search through these event databases to identify early indicators of a breach. This could be achieved in many different ways – for example, through the application of threat intelligence, which includes publicly-available research, community contributions, and vendor labs, through known indicators of compromise (IOCs), or through advanced analytics. It flags potentially risky activities, ranging from simpler concepts such as known bad IP addresses, URLs, and files, to more abstract concepts like commonality with methods attackers use to achieve their goals, e.g., lateral movement across machines in a network, or credential harvesting to gain privileged access to critical systems. Some EDR solutions apply other high-level techniques, such as behavioral analytics and machine learning, to further identify risks.

Therefore, one sees that a major difference between EPP solutions and EDR solutions is that while EPP solutions focus on static detection methods that can be automated to block threats on an endpoint, EDR solutions seek to identify more advanced attacks and threat actors by leveraging multiple IOCs that may be hiding among all the legitimate traffic, endpoint events, and user activities in an organization. Gathering information from many endpoints (including servers), an EDR solution applies analytics to help identify the likeliest potential threats. Fed to a central system via telemetry, these findings help reveal the full "scope of attack," in a way that an EPP running on a single endpoint is not designed to do.

Commonly, analysis is not done on the endpoint itself, but rather, the endpoint data are uploaded for further analysis on a server. The EDR solution then applies its own threat detection methodologies, which may include data science models and machine learning, in order to detect suspicious and potentially malicious endpoint activity with great accuracy. Generally, at this point, the EDR solution assigns a projected "risk score" to help security analysts (a.k.a. the "threat hunters") prioritize, investigate, and respond accordingly to these threats.

This extra layer of human attention – turbocharged by the ability of the EDR solution to identify potential threats, then to isolate and remediate them – empowers organizations to keep pace with threats both current and new. Basically, the bad guys cannot morph, obfuscate, or evolve their threats to defeat a static defense; because all exploits must eventually “do something,” these actions themselves become the signature by which their existence is revealed.

The chart below highlights some of the practical differences between EPP solutions and EDR solutions:

Attribute	Endpoint Protection Platform (EPP)	Endpoint Detection and Response (EDR)
Primary use cases	• Malware prevention • Automated blocking	• Threat detection • Root cause investigation and analysis • Incident response (IR) and threat hunting
Endpoint visibility	• Commonly, very little visibility	• A LOT of visibility
Defense posture	• Reactive (e.g., identify and block)	• Proactive (e.g., hunt for threats)
Operational Model	• Hands-off “Set and forget”	• Hands-on Ongoing process
Signatures and updates	• Continuous updates with new signatures	• No updates or signatures required
Endpoint Resource Utilization	• Heavier impact because everything runs locally	• Lighter impact because heavy work takes place on server

So what does this mean to the CISO tasked with securing an organization’s IT infrastructure? Nothing less than a complete re-thinking of endpoint security strategy. For while traditional EPP solutions will probably always have a place in preventing classic malware, it’s clear that advanced defense requires a higher order of solution, one that’s capable of evolving right along with the tactics, techniques, and procedures (TTPs) of exploit creators.

In fact, that may be the clearest differentiator between EPP solutions and EDR solutions: they belong to different security layers. An EPP solution falls into the base security layer, while an EDR solution occupies the security analytics layer. Both layers are necessary and complementary, but they do different things, and are therefore engineered from different design centers.

From this perspective, an EPP solution can be viewed like a firewall or spam filter, which are generally deployed, in great scale, as preventive security components. These are core tools deployed by all security-conscious organizations, and constitute a base level of preventative infrastructure that's quite effective in dealing with a large proportion of threats to an organization.

An EDR solution complements the value of EPP, which fulfills the role of endpoint security infrastructure. The EPP solution has a valuable role as the first line of defense, to block many exploits before they can infect an endpoint. EDR targets exploits that are able to get past the EPP defenses, and it does this by analyzing the behaviors of software and people.

RSA NetWitness Endpoint is an EDR solution that continuously monitors endpoints, to provide deep visibility into, and powerful analysis of, all behavior and processes on an organization's endpoints. RSA NetWitness Endpoint doesn't require signatures or rules. Instead, leveraging unique endpoint behavioral monitoring and advanced machine learning, RSA NetWitness Endpoint dives deeper into your endpoints to better analyze and identify zero-day, new, hidden, and even those "file-less", non-malware attacks that other endpoint security solutions miss entirely. As a result, incident responders and security teams gain unparalleled endpoint visibility allowing them to more quickly detect threats they couldn't see before, drastically reduce threat dwell time, and focus their response more effectively to protect their organizations.

Just as importantly, RSA NetWitness Endpoint is part of a full security analytics platform, RSA NetWitness® Platform. In this modular deployment model, the endpoint data can be seamlessly combined with information gleaned from system logs and network packets (using RSA NetWitness® Logs and Packets), and subjected to even deeper analysis (using RSA NetWitness® SecOps Manager). Behavioral analytics can be augmented by advanced threat research from multiple sources. With these rich forensic capabilities, SOC and IR teams gain insight into the full scope of an attack across both network and endpoint and receive actionable intelligence that streamlines threat analysis and response.

And detection is just part of the solution. Machine containment allows security teams to isolate an endpoint on the network, preventing attacker communication and threat lateral movement. This allows security teams to better understand the attack in a live environment with no fear of the threat spreading. With RSA NetWitness Endpoint, security teams can then blacklist malicious files as well as block and quarantine them with one action across all infected endpoints in the enterprise.

The use of traditional or even next-generation antivirus tools remains imperative in security-conscious organizations. They're often a cost-effective way to prevent attacks on an organization.

However, in today's fast-moving threat environment, it's no longer sufficient to deploy an EPP solution and expect to be fully protected. To achieve true protection, an organization needs more powerful tools that leverage higher-order analytics (including behavioral analytics) to fight back against the advanced, unknown threats and new non-malware attacks that easily evade a base endpoint security layer of EPP.

On the endpoint, that means implementing an EDR solution such as RSA NetWitness Endpoint. To enhance their overall security posture even more, an organization can then extend its threat detection and response capabilities through a fully integrated suite of tools like the RSA NetWitness Platform that combines network and endpoint telemetry with expert threat intelligence. This gives organizations, again to quote an old canard, both an ounce of prevention and a pound of cure.

04/18, White Paper, H15846.