Inside The Competitive Testing Battlefield of Endpoint Security

securityweek.com/inside-competitive-testing-battlefield-endpoint-security

By Kevin Townsend on July 19, 2016

Traditional AV Firms Battle "Next-Gen" Endpoint Security Vendors for Share of Anti-malware Market

There is bad feeling between what can be described as traditional antivirus (Trad AV) and next generation antivirus (Next-Gen Endpoint Security, or ES). It's not universal, but it does exist.

In May, VirusTotal applied new rules to the use of its services in a move that many interpreted as aimed at, or at least primarily affecting, Next-Gen vendors. In June, Sophos (Trad-AV) lambasted Cylance over comparative testing methods. Comparative and competitive testing has emerged as the primary battlefield.

It's a complex arena. Both technologies ultimately seek the same end: to protect systems from malware. Neither side is purely one nor the other: most Trad-AV companies have Next-Gen offerings or components; and many Next-Gen products include Trad-AV techniques. Nevertheless, most people will understand the difference.

Trad-AV includes, but is not limited to, companies such as ESET, F-Secure, Kaspersky Lab,

Panda, and Sophos. Next-Gen Endpoint Security includes, but is not limited to, Cylance, Fidelis, FireEye, Palo Alto Networks and SentinelOne. *SecurityWeek* approached all of these companies for their view on this 'bad feeling'.

For the sake of clarity we must stress that Next-Gen ES can usually claim to be more than just anti-malware; and that Trad AV today is far more than just a signature blacklist.

The prize is the anti-malware market. It's almost impossible to say which side has what percentage of this market because of the overlapping technologies. Nevertheless, EMA Research suggests that the total market is worth $9 billion per annum, and that Next-Gen currently accounts for around $1.25 billion. Trad-AV holds the ground; and for Next-Gen ES to truly succeed, it needs to dislodge its traditional competitors. There have been several recent claims that it is trying to do so with unfair comparative testing methods.

So this is our discussion: Are Next-Gen ES firms using unfair tactics; is Trad-AV wrongly calling 'foul'; and is it even possible to compare the two? Although customers could use both defenses side-by-side to defend corporate networks, there are few companies that will be able to justify the cost of both. Choice is, largely speaking, necessary.

The Arguments

Sophos prompted this discussion by calling out Cylance for unfair comparison practices. Dan Schiappa, a senior VP who wrote the Sophos blog, told *SecurityWeek*, "There are several reputable independent test labs who are very capable of benchmarking the effectiveness of all AV and endpoint security products, such as AV Comparatives, AV-TEST, MRG Effitas, NSS Labs, SE Labs to name a few. There’s even a collective effort called AMTSO that strives to advance the cause of high quality testing by these independent labs."

Trad-AV is rallying around AMTSO. AMTSO has done sterling work in developing standards that can eliminate unexpected bias from independent testing. Indeed, VirusTotal has made certified testing in accordance with AMTSO standards part of the requirements for using its full services. The majority of Trad-AV companies would like to see comparative testing performed by independent testers conforming to AMTSO standards.

Kaspersky Lab’s Michael Canavan is unequivocal: “Third-party testing plays a vitally important role for customers by providing an unbiased evaluation of the different types of available endpoint security. These independent organizations are able to test all types of solution capabilities while ensuring those products are configured properly to certify that the assessment is accurate, and it is the only method that will provide an impartial evaluation, proving which products are the most effective and reliable for protecting customers.” Not everyone agrees, as we shall see later.

There are problems with AMTSO. Its members are almost entirely Trad-AV companies and

independent testing bodies. It has no Next-Gen members. Perhaps this is a failing by the Next-Gen group; but the reality is that numbers would be stacked against them and they would have little ultimate sway over AMTSO policies.

"All testing is biased," suggests Carl Gottlieb, CTO of Cognition and a reseller of Cylance Next-Gen products. "Supposedly independent testing bodies are biased by their own experience, designing test methodologies that suit the majority of their tested products that represent their main source of funding." He clearly believes that it would be difficult to get unbiased tests via the preferred Trad-AV route; that is, AMTSO.

The Trad companies do not accept this. They point out that they have their own Next-Gen products and that AMTSO has developed methodologies to test these.

In fact, they tend not to even recognize a difference between the two sides. “Trad-AV and Next-Gen ES is purely a marketing concept invented by the ‘Next-Gen’ vendors,” suggests Andy Patel, security advisor at F-Secure. “Endpoint protection is endpoint protection. You either stop threats or you don’t. By and large, the technologies being used by both camps are similar. Companies that have been around longer just have a lot more of their own infrastructure and data.”

ESET senior research fellow David Harley takes a similar view. “It’s clear that the distinctions between ‘fossilized’ and ‘next-gen’ products are often terminological rather than technological. The basic approaches to defeating malware haven’t changed significantly since they were defined by Fred Cohen.”

Panda Security is one Trad-AV company with a product combining Trad and Next-Gen technology, called Adaptive Defense 360. Panda says they wanted to test their product against pure Next-Gens via an independent testing lab – and was willing to pay the costs for all those who entered. But, said Luis Corrons, technical director of PandaLabs, “when the testers started contacting Next-Gen ES vendors, none of them wanted to participate. And this is not like a regular antivirus you can download from the vendor’s website – they are pretty expensive and you have to go through them to obtain it.”

This is a common complaint from the Trad companies – while their own products are readily available for testing, the Next-Gen companies make it difficult to test theirs. “Despite our efforts, to date,” wrote Sophos VP Dan Schiappa in his blog post, “Cylance has been unwilling to allow us to license its products.”

There is a bigger concern voiced by the Trad companies – that Next-Gen abuses the facilities of VirusTotal (VT) in order to denigrate Trad AV capabilities. VT is a service, owned by Google, that allows anyone to submit a suspect file to be tested against the scanning engines of some 50+ Trad AV vendors. VT does not, was never intended to, and cannot test

the Trad AV product itself. New malware will always get a poor return from VT since it only uses the signature part of the whole product – but it does not mean that the product in situ will not detect the malware.

Next-Gen vendors have not been slow to suggest that while they can detect a new strain of malware, only one or two or even none of the Trad AV vendors can detect it according to VT. This, say the Trad companies, is misleading the market. Harley quotes from VT itself: "VirusTotal should not be used to generate comparative metrics between different antivirus products."

When *SecurityWeek* approached a number of Next-Gen ES vendors over the testing issue, only two, Cylance and SentinelOne, responded. Palo Alto, FireEye and Fidelis all replied with variations on 'no comment'. Note that Next-Gen differentiates itself from Trad AV by describing itself as 'advanced threat detection and prevention' (that is, detection of malware including zero-day malware). Trad AV describes itself as 'anti-malware, including zero-day malware'.

Chad Skipper, VP of Testing & Certifications at Cylance, suggested the following: "Research your vendor to determine if they are actually detecting advanced threats," he told *SecurityWeek*. "Here's an example – On June 3rd, 2016 the Cylance team published a blog, on how CylancePROTECT was detecting CryptXXX, another form of ransomware. In this blog there are several references to many hashes. When reviewing submissions to various multi-engine AV testing services one can see that hash fcf9347859f38088cbd41a69d660657baeec212125a1c647177262942c695873 called out in the referenced blog by Cylance was being detected by CylanceProtect a month prior to its submission to the multi-engine AV site. Is your vendor proactively detecting 'unknown/Zero-Day' malware like this or are they reactively creating signatures like those on these various multi-engine AV testing services?"

Cylance does not mention VirusTotal by name, but it is almost certain that VT is one of the 'multi-engine AV testing services' it used. This is, in itself, misleading.

David Harley suggests this is one of the primary problems with Next-Gen marketing: "By misusing VirusTotal (and/or similar services) as if they were 'multi-engine AV testing services' which VirusTotal certainly isn't." VT and similar are file checking services; they are not product testing services.

SecurityWeek asked a trusted Trad AV researcher to comment on Skipper's claims – which he did, but requested anonymity. "We detected this hash by 1 May 2016; that is, more than a month before the date of the Cylance blog. We suspect other companies did the same." The point is not that Cylance is *intentionally* misleading; but that it is unsafe and *actually* misleading to base arguments on VT assumptions.

Implying that VirusTotal results accurately measure Trad AV capabilities also helps to foster another frequent claim from the Next-Gen vendors: Trad AV is solely signature-based detection. When *SecurityWeek* asked SentinelOne (Next-Gen ES) how the user should choose between the two, Scott Gainey, Senior VP & CMO replied, "For decades antivirus software has relied on a signature-based model that compares a static list of previously identified threats, contained within a centralized database to local observations made on an endpoint as new inbound files come in…"

Gainey, who previously served as VP of Marketing at Palo Alto Networks, continued: "Today, most traditional antivirus solutions only protect against file-based malware attacks – any file-less (or memory only) attack will not be detected. This represents a large percentage of the malware population that's missed by traditional solutions, and even some 'next-gen' offerings."

However, Fraser Howard, a security researcher with Trad AV vendor Sophos, told this writer back in 2013, "We've been tackling RAM-only viruses since the late '80s. We already detect malware in memory. We scan bytes in processes in memory just as we scan bytes in files on disks."

SentinelOne did, however, continue with good advice: "Users should also be looking for solutions that provide the complete spectrum of detection, mitigation and remediation. It's not enough simply to alert someone to the presence of an attack – that detection capability must be closely integrated with mitigation tools so the attack's processes can be killed immediately, and the endpoint quarantined to prevent any potential for spread. This must happen in real-time, without the need for manual intervention. Finally, security can't come at the expense of performance."

The problem for the user, however, is that both sides can and do claim to do just this to one degree or another. None of it answers the basic question: how is the user to choose between Trad AV and Next-Gen ES (assuming that it is not realistic to have both)?

What End User Security Professionals Think

SecurityWeek approached a number of current and recent CISOs to see how they solve this problem. The bad news for both Trad AV and Next-Gen ES vendors is that their customers pay little attention to what they say about their own products.

Some argue that the two technologies simply cannot be compared. Brian Kelly, chief

information security leader at Quinnipiac University, says they are “two very different technologies. I see them like seat belts and airbags… you don't compare which technology saves more lives, but rather I agree that they both contribute to a safer automobile.” If the budget runs to both, then the solution may be to use both and get security in depth. Most organizations, however, will need to choose.

The difficulty for the buyer is that both technologies have strengths and weaknesses. Dan Swartwood, a senior fellow with the Ponemon Institute, said, “Companies like Cylance are seizing a market opportunity created by a fundamental truth: targeted attackers can get around traditional AV, always. A tool like Cylance can catch many threats that would bypass traditional AV. At the same time traditional AV will catch many threats that Cylance would never even inspect. This fundamentally explains the night and day differences in published testing (if you design your own test, you design your own result!). It also explains the confusion in the market, and the need to thoroughly test an agent against realistic threats to identify what is the best mix for your own organization.”

The reality is this: CISOs do not believe what the vendors tell them, even when it is based on a supposedly independent comparison. “To be honest, anyone who purchases a solution based on marketing fluff needs to seriously find a new industry to work in,” suggests John Masserini, CISO at MIAX Options. “I'd hate to be the CISO whose only excuse after a breach is 'Their marketing glossy said it would work…'”

Drew Koenig, security solutions architect at Magenic, points out that household consumers don’t expect a new car to achieve the mileage in real life as claimed on the sales sticker, nor detergents to remove stains as easily as demonstrated in the advert. Test results are used to promote ‘performance’. But, “if you can't solve your business problem the tool's performance is moot. Bring the top two or three selections into your environment and POC a performance test in the world the tool will live in.”

Martin Zinaich, information security officer for the city of Tampa, plans to do that by taking advantage of the ability to run both technologies side-by-side. “Next-Gen endpoint protections like Cylance claim they can be run in parallel with traditional signature/anomaly based products. So I plan to do that and see if the Next-Gen catches anything new. If it does, I’ll examine if these new things are just noise or real issues.”

Masserini explained his process in more detail. “We never purchase any solution without running a full 'release' version of the product in our environment for at least 90 days. We've had some vendors push back on that (wanting to limit to 30 or 60 days), but in the end, most choose to participate, otherwise, they get disqualified. By taking this approach, we've eliminated some 'quadrant leaders' from selection – not because their solutions didn't work, but because they didn't work ***for us***. You never know what you will find when coming out of a POC, but it will certainly add a level of credibility to the selection process.”

Dan Bowden, CISO at University of Utah Health Care and University of Utah, takes a similar view. He asks four primary questions: "Which tool helps us move forward most decisively? Which addresses our most serious gaps in threat prevention, detection, incident response, and forensics? And which tool helps us take more initiative in finding threats?

"These questions won't get answered clearly by listening to vendors rant about each other. And the answer may be different among different organizations. Each CISO must understand the organization's current, unique threat landscape, and which existing technologies are the 'keepers' to be combined with any new endpoint solution."

In general, CISOs believe that no test scenario could be the same as their own live environment – each one of which will be different. They want to see how the products work for them. "I believe that only way to choose would be to run a proof of concept with the two different A/Vs," says Thomas DeLaine, Director of information security at Comprehensive Health Services. "That way you can measure the effectiveness in a side by side comparison. The spec sheets may say one thing; however, the way the products react on your specific network and the reports/alerts provided will be different based on the size and scope of your user base."

"Users," adds Todd Borandi, a lead information security architect, "care about simplicity, then security. Security tools need to be easy to use and for AV they want it to be a 'fire and forget' application. Load it once and have it protect the system without need for interacting with it (maintenance, updates, etc.), having it interfere with their use of the computer during a scan, or guessing how to clean identified issues… We know nothing is perfect, but from a user perspective I would want to know two things. How close to perfect can you get me and how involved do I have to be to get there?"

Steve Lentz, chief security officer for Samsung Research, explained his own decision process. "The bottom line," he said, "is that testing is our responsibility, not vendors.

"We are currently evaluating several vendors for endpoint AV, DLP and APT," he continued." I created a Must-Wants matrix that I learned from my Six Sigma training. The matrix is based on our environment and what we are looking for in a solution. We have a number of Musts that are required to move forward. We then have Wants which we then grade by priority.

"For example we have five Musts the vendors have to meet. We are evaluating six vendors – five meet all the Musts; one does not. So we then move onto the Wants with the five that met the Musts. Say we have ten Wants; we grade 1-5 for each in priority. The vendor with the highest score is then the winner. All this is based on on-line webinars where we see the product in action. The team asks questions and of course our research into the solutions. You can even take further and take the 2 highest and conduct more stringent testing such as a POC to get more confidence in your final pick. This way the winner is not based on bias but actual performance, it does what it claims and it fits your environment. My company

environment is different from yours and the next person. Testing the way I just described makes sure it fits your requirements in Musts and Wants for your particular environment, without bias."

One CISO, who asked to remain anonymous, said, "We expect AV to only capture some of the bad stuff; we look to our other tools to catch the rest." That's why he has a SIEM and Next-Gen firewalls, spam/email gateway and cloud-based proxies and other threat detection tools. Only then, he added, do we feel "we've caught as much as we can.

"If we were evaluating AV," he continued, "we'd be doing a proof of concept of two or three providers. That's the only way to see how it works in our environment. We'd be looking at performance on the endpoint ***and*** effectiveness. We need tools that work well, without crippling our end users. We'd also be looking for how well the management console integrates reporting with our other tools. We tend to lean towards integrated solutions rather than stand-alone best of breed."

The Final Analysis

Our discussion hasn't looked at how SMBs might respond to test results. Smaller companies might not feel able to demand sixty-day try-before-you-buy options; nor could they realistically compare performances. Chris Bedel, an independent information security consultant concentrating in the financial sector, points out that many of his clients have Trad-AV and are likely to keep Trad AV because that is what they understand. "To make the switch, I think they would want to see an independent test; it's not something that they could perform themselves."

But in the final analysis it is clear that leading practitioners in major organizations take little notice of the vendor claims – they want to see how different products work for them and their own conditions in their own environments.

To some extent this discussion was prompted by the accusations of Sophos (Trad AV) against Cylance (Next-Gen ES). We also asked the CISOs what they thought about this. In general, they consider it typical of the arguments that always arise when a new technology appears. They don't take much notice.

However, Chris Kellogg, director of service reliability engineering at RelayHealth, said this: "Sophos' response was a little over-the-top given the context. They did, however, take a strong, aggressive position and invited challenge. As for Cylance, their disengagement blog was unfulfilling – passive-aggressive. They stirred the hornets' nest, and then said it was an unnecessary distraction. To me, they came off weak – conceding the table to Sophos. They need either better ethics or more conviction."

But that still doesn't say which is best.

Kevin Townsend is a Senior Contributor at SecurityWeek. He has been writing about high tech issues since before the birth of Microsoft. For the last 15 years he has specialized in information security; and has had many thousands of articles published in dozens of different magazines – from The Times and the Financial Times to current and long-gone computer magazines.

Tags:

- Endpoint Security
- NEWS & INDUSTRY