No.8
25th July 2018

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/UN-SPONSORED**

AMTSO's Malware Testing Standard: Some Progress in Endpoint Security

The Anti Malware Testing Standards Organization (AMTSO) adopted its first testing protocol standard at the end of May.

- AMTSO's new standard for transparency in advanced malware testing methods is a step forward in cleaning up the fiercely-contested endpoint security market.
- The new standard doesn't validate the efficacy of test methodologies, but this is next on AMTSO's agenda. One single, universal, standard for testing malware detection isn't on the cards.
- Enterprise users should work with peers, independent test frameworks and AMTSO standards to understand the real-world performance of endpoint security products.
- AMTSO and NetSecOPEN appear to be complementary standards bodies. Users, test houses and vendors should support both as drivers of more transparent testing.
- Until they have full confidence in their own testing capabilities, third party test results or peer recommendations, enterprise buyers may want to consider recent vendor choices by leading cyber-security players like Secureworks and IBM Security.

AMTSO's new standard is a step forward in cleaning up the endpoint security market.

Definitions and Acronyms

This Briefing focuses on endpoint security, the focal point of efforts to protect against advanced malware. The term 'endpoint security products' is the main one used throughout this Briefing. It is used as an umbrella term to embrace several commonly used product categories like Antivirus (AV); Next Generation AV (NGAV); Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR) products.

Exploring how these categories are converging (or have converged) is beyond the scope of this Briefing. Where any of the above four acronyms are used, it is only in the context of how a specific named vendor itself chooses to classify its own product.

The New Testing Standard from AMTSO

At the end of May the Anti Malware Testing Standards Organization (AMTSO) announced the adoption of what it's calling its first testing protocol standard. For the first time this standard prescribes in detail the ways in which test houses must disclose how their tests on anti-malware and related products were conducted in order to be AMTSO-approved.

AMTSO is made up of around sixty members. The largest part of the membership comprises a who's-who of endpoint security vendors. Many have roots in the traditional AV market. More recent members are new entrants in the NGAV, EPP or EDR space. The second largest constituency among AMTSO members are test houses. These range from niche AV-focused firms to larger security test companies like NSS Labs and ICSA Labs.

"This is big," said Dennis Batchelder, President of AMTSO, announcing the adoption of the standard. "AMTSO standard-based tests can remove biases and give enterprises and consumers information and context they need to choose their security providers".

This Briefing explores this new AMTSO standard and the endpoint security market more broadly. Specifically this Briefing asks:

- What is the outlook for adoption of the AMTSO standard?
- From an enterprise buyer's perspective, just how big a deal is this?
- What more needs to be done to level the playing field in endpoint security testing?
- What else can enterprise buyers rely on in evaluating endpoint security products?

Today's Market in Endpoint Protection Products

Palo Alto Networks Founder and CTO, Nir Zuk, has a nice way of explaining the development of the cyber-security product market in the context of three timeframes:

- 1995-2005 saw billions of dollars spent on around twenty security vendors trying to block known cyber-security attacks, which today comprise about 90% of all attacks.
- Since 2005, tens of billions of dollars have been spent across hundreds of security vendors trying to block an additional 9% of attacks that are unknown.
- The next ten years are set to feature hundreds of vendors chasing down the remaining 0.9% that remains very hard to detect.

There is increasing emphasis on around detection accuracy based on machine learning and AI.

You can argue with this perspective at the margins but the basics are sound. It's of course the endpoint security market which is the focal point of Zuk's last percentage point or two which is driven by advanced malware. And it's this which gives the endpoint security market its over-heated characteristics which can be summarized as follows:

- **A large variety of different products tailored to very different buyers.** These range from SMBs and consumers at one end to Fortune 500 companies at the other.
- **An expanding choice of vendors.** A variety of long-established endpoint security vendors with their origins in the AV market for enterprise and consumer (e.g. McAfee, Symantec, Kaspersky) have been joined by a lot of new entrants targeting the enterprise (e.g. CrowdStrike, SentinelOne, Cybereason).
- **Rapid evolution in the competitive landscape.** There is increasing emphasis - initially on the part of new entrants but increasingly now from established vendors - around malware detection accuracy based on machine learning and AI algorithms.
- **A highly complex testing challenge for enterprise security professionals.** The techniques used by adversaries and defenders in both designing and detecting advanced malware are getting increasingly diverse and sophisticated. Defenders have to protect endpoints that support multiple OSs, each available in different releases. They have to defend endpoints on-premise as well as in clouds. And they have to take full account of the unique ways in which many endpoint security products interact with the cloud-based elements of their solution architecture.
- **Some very high valuations among new entrants**. Just a year after achieving "Unicorn" status, CrowdStrike tripled its valuation to $3 billion with a new funding round just a few weeks ago.
- **An arms-race in marketing claims between vendors and high-profile disputes between vendors and test houses.** A high-profile battle broke out in September 2016 between Cylance, a vendor, and test houses AV Comparatives and MRG Effitas. Cylance accused the latter of a test methodology that amounts to nothing more than a "scam". In April this year, NSS Labs singled out CrowdStrike as a vendor whose effectiveness it was "unable to measure" and therefore cautioned "against their deployment without a comprehensive evaluation."

- **Absence of any industry standards for testing advanced malware**. Until AMTSO's announcement in May, there were no standards of any kind in this space.

From a buyer's perspective how big a deal is the AMTSO standard?

So how far does the new AMTSO standard help? The mere fact that AMTSO's large membership has signed up to a standard that embraces full disclosure of test methodologies is certainly an important step. Equally it's clear that it will be a while yet before buyers get to reap the benefit of the new standard and that it only solves one of the many challenges that buyers face.

The standard was only adopted in May so we're in the very early days of adoption. Two test houses, MRG Effitas and SE Labs, have public tests aiming to comply with the live standard by the end of September. The first product vendors that test with those companies won't start start using AMTSO-compliance in the way their products were tested as a marketing tool until the end of this year at the earliest. 2019 is more likely.

Not for the first time, though, some of the bigger beasts of the security testing jungle are dragging their feet. NSS Labs, for example, has yet to commit resources to gaining compliance to the AMTSO standard.

It looks like it will be 2020 before there will start to be a competitive market in AMTSO-compliant products.

There's a generous explanation for this foot-dragging. This speaks to the new task of aggregating aspects of the test reporting into a single document for the AMTSO standard. This creates an additional – or at least different – administrative burden. There's also the more familiar – less generous – explanation that the big test-houses aren't keen to level the playing field in testing so as to maintain their differentiation and market power.

In summary, it looks like it will be 2020 before there will be a competitive market in endpoint security products that have been tested according to AMTSO-compliant tests for buyers to choose from.

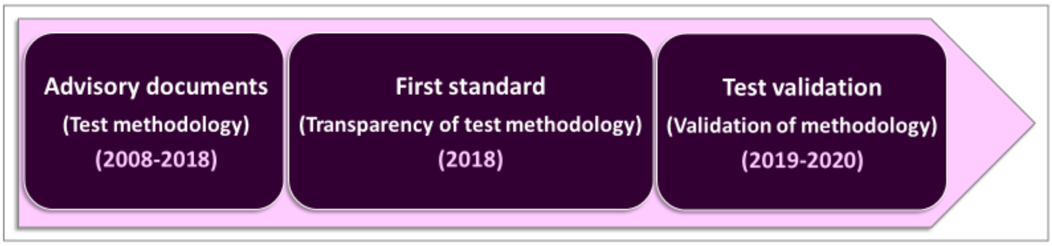
How much more needs to be done to level the playing field?

This first AMTSO standard should be seen as part of a continuum in the organization's work. Having been formed ten years ago, up until this year AMTSO has been known for publishing guidance to test houses that was no more than advisory in nature. These guidelines stretch all the way back to the days of static scan tests to today's far more dynamic test requirements.

The adoption of this first standard is a milestone because it represents the first time AMTSO gets to give or withhold formal recognition of compliance to a standard. The limitation of the new standard is that it only validates the transparency of a test methodology. It doesn't actually validate the efficacy of the test.

AMTSO does want to go further, though. The first conversations have already been had around ways in which AMTSO could do more than just recognize that a test methodology meets the new standard for transparency. The organization has started exploring options for providing some kind of next level independent stamp of test validation.

Figure 1: AMTSO's work: past, present and future



Source: HardenStance

This would state not just that a test is AMTSO-compliant in terms of the transparency of the test methodology but that that test methodology itself does in fact provide good value to the buyer. An analogy between this and the restaurant business would be extending from just validating the quality of a chef's ingredients to validating the quality of the meal that arises from those ingredients being combined.

A single AMTSO standard for testing product efficacy remains a very remote possibility. Agreeing a universal anti-malware testing standard applicable across such diverse environments and across such a diverse group of vendors is a very much bigger challenge. Not surprisingly, there's no commitment within AMTSO to that at all at this point. Even a best-case scenario would seem to point to it being at least five years away.

What else can buyers rely on?

A lot of organizations are vulnerable to smoke-and-mirror marketing from the less trustworthy security vendors.

From an enterprise perspective, nothing compares with testing candidate endpoint security products yourself before investing in one. The truth is, though, that the endpoint security space is fiendishly complex to test against. The smaller the organization, the less chance it has of reaching valid conclusions. That makes an awful lot of organizations vulnerable to smoke-and-mirror marketing from the less reputable vendors. In addition to AMTSO standards, enterprise buyers have other options to help them in evaluating different products:

- **Independent testing frameworks**. Buyers should look at the work of independent cyber security professionals. For example, the Independent Endpoint Testing Framework has been developed by independent researchers, Lidia Giuliano and Mike Spaulding. It provides excellent guidance to users on many critical 'do's and 'don't's of testing endpoint security products. Their summary presentation at BlackHat USA 2017 only saw the light of day after it cleared legal threats from some vendors alarmed at the rubbishing that some of their own marketing claims might be subjected to. Ingeniously titled "Lies and Damn Lies: Getting Past the Hype of Endpoint Security Solutions", the presentation was a stand-out highlight of BlackHat.

- **Informal peer networks**. Infosec professionals tend to be good at relying on their peers in other companies to get product referrals and recommendations. They may need to widen their circle for endpoint security procurement.

- **Evidence of recent vendor selections that market leaders in cyber-security have made.** Clearly, it doesn't necessarily follow that the vendor selections of the great and the good of the cyber-security market will be the right fit for any given enterprise buyer. But if a buyer is already leaning towards a given endpoint security vendor, then in a market that is currently so loaded with smoke and mirrors, validation from a top player can at least assure a buyer that they're not investing in the equivalent of cyber-security snake oil.

  One example that may be relevant to some buyers is the recent selection of Carbon Black by both IBM Security and Secureworks for the latest generation endpoint security products. There aren't many companies that can match these two companies for credibility in selecting third party security vendors (or in cyber-security more generally). The test regimes that any of their vendor partners have to get through are certainly proprietary but the calibre of these companies' testing credentials is beyond doubt.

  Secureworks offers a broad portfolio of endpoint security solutions, revolving largely around Red Cloak, its own internally-developed IP for EDR. The company may partner with other endpoint protection players in the future as sources for endpoint telemetry, but for now its only active commercial partnership is with Carbon Black. Carbon Black features in the Secureworks portfolio in conjunction with the company's Advanced Endpoint Threat Detection (AETD) offer. The

Secureworks managed Next Generation AV (NGAV) service, Advanced Endpoint Threat Prevention (AETP), also leverages Carbon Black's Cb Defense. Secureworks also monitors the AV and NGAV products of a wide range of vendors.

IBM Security has integrations with these endpoint security products: McAfee; Symantec; Sophos; Trend Micro and Microsoft Defender. IBM Security specifies that these vendor integrations only cover traditional AV solutions, not their next-gen or behaviour monitoring based solutions. For EDR, the only third-party product that IBM Security is actively reselling at this time is Carbon Black's Cb Defense.

Test houses should be investing in gaining formal recognition of compliance from both AMTSO and NetSecOPEN.

Doubtless some market actors will object that the buying patterns of market leaders shouldn't be pointed to as supporting factors aiding vendor selection. More likely, they'll object to a vendor (other than themselves) being singled out as above. All the more reason, then, for all endpoint security vendors to re-double their efforts to drive transparent and effective AMTSO standards that buyers can have genuine confidence in.

Greater Transparency with AMTSO & NetSecOPEN

In April, HardenStance published a report on NetSecOPEN. This is a new network security testing group whose first output is a new standard for the testing of Next Generation Firewall (NGFW) products.

The underlying rationales for both NetSecOPEN and AMTSO are very similar. Both want to drive transparency in security product testing. Both want to help buyers better understand the real-world performance of security products. In principle at least, the two organizations ought to be complementary.

At first glance, where the two differ today is in the product spaces they're currently focused on. But neither organization needs to stay confined to these initial focus areas. The more important differentiator between them is that NetSecOPEN's core focus is on the relationship between performance requirements and security efficacy whereas AMTSO's is more directly on the efficacy itself.

NetSecOPEN managed to submit its first draft standard to an SDO (the IETF) within a year of its launch. Ten years since it was founded – and largely because of the greater complexity of the endpoint security product space – AMTSO has yet to pursue SDO ratification. AMTSO has nevertheless previously published joint guidelines with the IEEE and could move towards SDO ratification in the future.

Test houses should be investing in gaining formal recognition of compliance from both AMTSO and NetSecOPEN. An enterprise security product tested in compliance with both AMTSO and NetSecOPEN standards: now wouldn't that be a thing to behold? ■

- HardenStance received no payment – direct or "in kind" – for publishing this Briefing.
- **Contact HardenStance's Principal Analyst:** patrick.donegan@hardenstance.com
- **Register here** for **free email notifications** whenever new IT and telecom security content is made available by HardenStance. www.hardenstance.com
- **See Disclaimer on the last page**

HardenStance Ltd Disclaimer of Warranty and Liability

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.