White Paper

HardenStance

A New Era in Trusted Network Security Testing

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by

Spirent
Promise. Assured.

February 2020

Executive Summary

- The number of lawsuits between vendors and independent test firms in recent years points to how trust in third party security product testing is breaking down.
- At the heart of this break down is declining trust in the proprietary test methods that independent test companies use to test IT security products.
- A new industry association, NetSecOPEN, is driving a new model in trusted network security testing. It expects to release its first NGFW vendor test results in Q1 2020.
- Final IETF ratification of NetSecOPEN's NGFW testing model is expected in 2020.
- More accurate NetSecOPEN tests may yield lower numbers than proprietary tests. Vendors will be able to leverage NetSecOPEN datasheets internally and externally.
- Buyers must not stand on the side-lines and watch this play out. They should actively engage in demanding NetSecOPEN proof points from their NGFW vendors.

The credibility of network security testing as practised by incumbent independent testing companies is in decline.

Independent Network Security Testing Is Broken

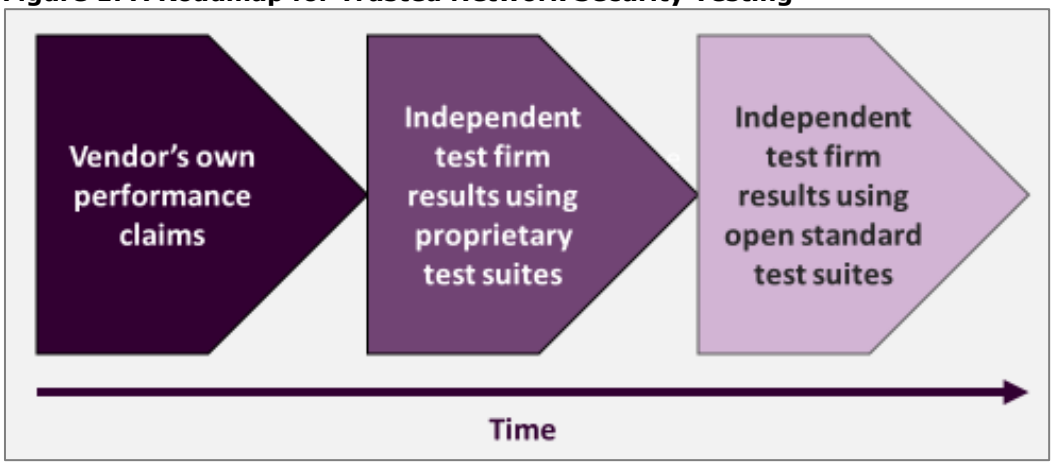
Vendors' own datasheets citing performance claims in their labs which then fail to materialize in real-world customer environments have inspired scepticism on the part of buyers of IT and network security products going back decades. It's this buyer scepticism that drove the rise of third party security testing businesses. Firms like ICSA Labs and NSS Labs created successful niches for themselves as independent test house intermediaries between buyers and vendors.

Most buyers have never entirely trusted independent test house results. On the whole, though, they have come to trust them a lot more than a vendor's own datasheets. Today, many buyers still depend to varying degrees on independent test results in choosing their security vendors. For that reason, vendors try and move heaven and earth to make sure that the results that independent testing firms publish for their products compare favourably with competitors.

Performance Testing is Never Simple

In IT and network security, the independent testing model has never been free of controversy. It still isn't. Even the most objective, best executed, most representative test suite need not, on its own, accurately predict the outcome that each user will see in their own unique network environment. That said, relative to the status it enjoyed in the cyber security ecosystem only a few years ago, the credibility of independent third party testing is in decline.

Figure 1: A Roadmap for Trusted Network Security Testing



Source: HardenStance

This paper argues that the legacy model of independent IT security testing is broken for three main reasons. These are summarized below and then explored in more detail:

- Enterprise networks, the cyber threat landscape itself, and the number of use cases to which some security products can be applied, have become infinitely more varied and complex. Depending on where a product is deployed, for which use case, and with which features switched on, the scope for a security product's performance to deviate from what's cited in an independent test lab report has increased greatly.
- The proprietary test suites that incumbent independent test companies use tend to lack the kind of industry consensus and transparency around their methodologies that are needed to build trust amongst buyers.
- There has been a marked decline in trust between independent test houses using proprietary test methods and security vendors themselves. Tensions and legal disputes over published test results have become increasingly common.

Enterprise IT and Networking has become Infinitely More Complex

The number of variables that can drive a security product's performance outcomes to deviate dramatically depending on where and how it is deployed has expanded dramatically in recent years. For example:

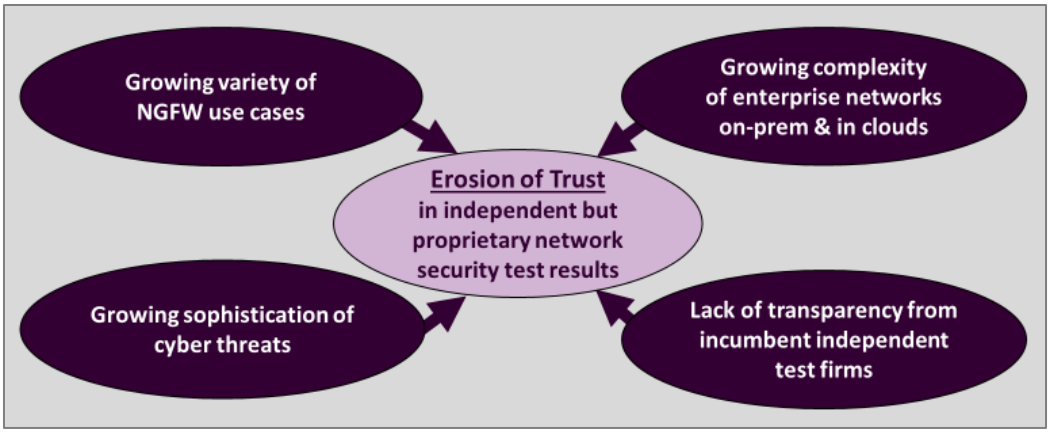
The number of variables that can drive a security product's performance to deviate from an independent test lab result has expanded dramatically in recent years.

- Enterprises are deploying security products on-premises, in private clouds, public clouds, hybrid and multi-cloud environments.
- Enterprises are mixing and matching dedicated security appliances as well as virtualized security software instances running on different types of open hardware.
- Some key security products have outgrown their original role and are now being deployed in many more use cases, leveraging a variety of different features.
- Cyber threats and attack vectors have become increasingly sophisticated in the way that they execute and the techniques used to obfuscate or disguise themselves.
- The characteristics of network traffic – and how that can impact the performance of security tools – have changed substantially. An example is the rise in application encryption, notably between an organization's own environment and public clouds.

Variations in the above factors result in wildly different demands being placed upon the hardware and software resources that different security instances run on. These factors heavily influence test performance outcomes, whether in terms of throughput or security efficacy. Some of the specific real-world examples that arise include the following:

- Whereas the role of firewalls arose as policy enforcement points at the perimeter of an enterprise network, today's Next Generation Firewalls (NGFWs) also sit behind the perimeter in network segmentation and micro segmentation use cases. NGFWs are now used in multiple threat detection use cases as well as for high performance SSL inspection as Secure Web Gateways.
- Endpoint Protection (EPP) and Endpoint Detection and Response (EDR) products have to protect endpoints that support multiple OSs, each available in different releases. They have to defend endpoints on-premise and in different clouds. Performance can be heavily impacted by the unique ways in which some EPP/EDR products interact with cloud-based elements in their solution architecture.
- The importance of representative traffic mixes to how accurately test outcomes are replicated in real-world environments is highlighted by one independent test house's recent findings. Testing a well-known NGFW product against a traffic mix that included a substantial percentage of encrypted https traffic, the test results came up with just 20% of the throughput cited in the vendor's own datasheet, which assumed no encryption at all.

Figure 2: The Erosion of Trust In Proprietary Test Suites



Source: HardenStance

The Problem with Proprietary Test Suites

As shown on the previous page, the modern IT environment makes it much more important – as well as much more difficult – to arrive at objective, real-world, performance test results that provide useful guidance to buyers. Relative to today's needs, that makes the traditional proprietary testing model fundamentally flawed.

Traditionally, test houses tend not to publish explicit details regarding the precise conditions under which their testing is carried out.

The problem with proprietary test models is three-fold:

- **They lack external scrutiny and inputs outside of the test house itself**. There is no consensus beyond the confines of that test house that its chosen test suite is indeed representative of market requirements or that it does not clearly favour one vendor's design, features and performance outcomes over another's. The independent model has always been inherently problematic in cases where vendors are paying for their products to be tested. Today's increasingly complex environment just makes it even more problematic.
- **They lack transparency**. Test houses using proprietary test methods tend not to publish explicit details regarding the precise conditions under which their tests were carried out. There is often no explicit, detailed, guarantee with proprietary test models that the highest standards of testing methodology have been rigorously adhered to. For example, there may not be an explicit guarantee that a vendor's product configuration has not been changed at one or more points during the testing rather than being locked down for the full duration of the test from start to finish.
- **Due to this lack of transparency, the proprietary test results of different independent test firms cannot be compared on an apples-to-apples basis.** It's therefore difficult for buyers to know how much trust they should place in these proprietary test results.

Litigation between Vendors and Test Houses is on the Rise

Disputes between vendors and test houses aren't new. They've been going on for years. However, there does seem to have been a marked uptick in high profile legal suits and countersuits between security vendors and independent test houses over the last three years. This has affected both the NGFW and EPP/EDR product spaces.

Among the IT security vendors that have engaged in very public spats with NSS Labs in recent years are FireEye, Palo Alto Networks and CrowdStrike. The dispute with CrowdStrike, which NSS Labs ended up settling, even led to the extraordinary case of NSS Labs filing an anti-trust suit against the 60-strong member Anti Malware Testing Standards Organization (AMTSO) and three vendor members of that organization. This was finally thrown out by the US District Court for the Northern District of California in August 2019. This particular dispute was extraordinary in the sense that a bona fide

industry standards group in the ICT sector was served with an anti-trust suit. The fear of litigation hangs heavily over the independent but proprietary security testing market nowadays. When it published its NGFW Security Value Map in July 2019, NSS Labs took the step of labelling two vendors that performed poorly "Vendor A" and "Vendor B" rather than calling them out by name.

This declining level of trust among industry players in the cyber security value chain is a direct consequence of today's more complex IT and networking environment and the openness and transparency failings of the proprietary testing model. There is no hard evidence in the public domain that demonstrates clearly that user trust in independent security testing is declining. However logic would suggest it is likely to be on a similar trajectory to that between independent test houses and many security vendors.

AMTSO and NetSecOPEN share a common approach to leveraging openness and transparency in specifying testing standards that buyers can have greater confidence in.

NetSecOpen's Membership and Mission

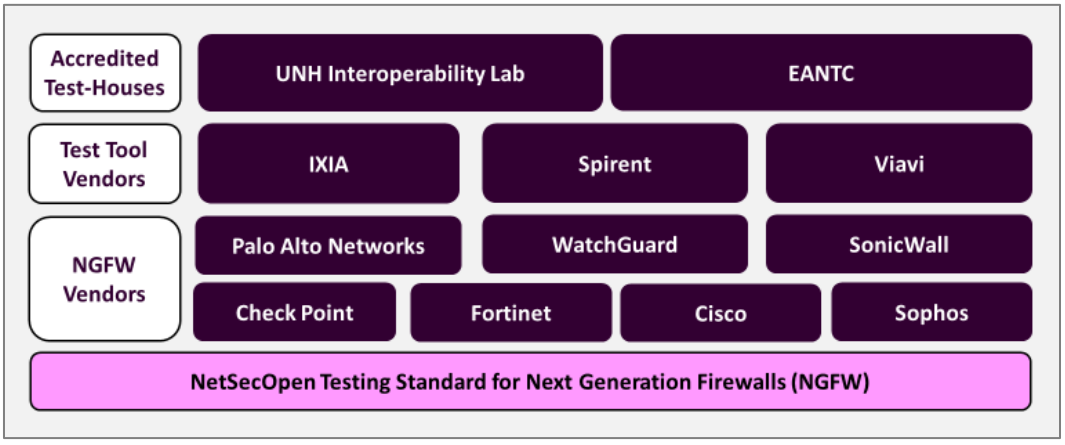
There are two industry associations that are currently dedicated to re-building trust in independent third party security testing through openness, transparency and consensus-driven standardization. One, AMTSO, is focused on malware testing in the Antivirus (AV) and EPP/EDR spaces. The other, NetSecOPEN, is focused on network security, initially on the testing of NGFW products.

The rest of this White Paper looks at the work of NetSecOPEN but it's important to recognize what these two organizations have in common. They share a common diagnosis of the problem of weak trust in today's independent but proprietary third party testing in IT security products; a common level of support from most of the leading vendors in the market space they are addressing; and a common approach to leveraging openness and transparency to specify testing standards that buyers can have greater confidence in.

All the Major Firewall Vendors are Members of NetSecOPEN

NetSecOPEN was founded in 2017. Its current members are shown below in **Figure 3.** NGFW vendors Check Point, Cisco, Fortinet, Palo Alto Networks, SonicWall, Sophos and WatchGuard are all members. Its own mission statement states that NetSecOPEN is "a membership-driven network security industry group, created in response to the need for more insightful, realistic, up to date and non-proprietary evaluation and certification practices. NetSecOPEN standards will provide guidelines and best practices for testing modern network security infrastructure including Firewall, IPS, NGFW and threat detection solutions."

Figure 3: The Membership of NetSecOPEN, January 2020



Source: HardenStance/NetSecOPEN

The first test specification NetSecOPEN has developed is for testing the impact of deploying a NGFW at the edge of an enterprise network on that network's performance in terms of throughput capacity. This is only the first of many test specifications NetSecOPEN expects to bring to market. This first one has been submitted to the IETF for ratification. This adds to the credibility of the approach and hence the confidence that buyers can have in NetSecOPEN standards.

As already alluded to, the evolution in NGFW functionality over the years has seen them enhanced to support a range of other capabilities that can also be supported in dedicated antivirus (AV), Intrusion Detection System (IDS) and Intrusion Protection Systems (IPS). As shown on page 7, NetSecOPEN's ongoing work items are developing NGFW test specifications for these and other threat detection use cases.

As well as openness and transparency, NetSecOPEN's competitive market in test equipment vendors, NGFW vendors and test-houses is designed to deliver benefits of scale and competition to buyers of NetSecOPEN-certified products.

NetSecOPEN's goal is to make vendor test reports freely available from the NetSecOPEN website.

Compared with the test results and deliverables they get from proprietary test suites, buyers of NGFW products stand to benefit directly from NetSecOPEN-certified test data in three main ways:

- **More realistic independent test results that provide better guidance on product performance in a buyer's own environment, thereby serving as a better guide to vendor selection**. A NetSecOPEN test certificate carries with it the guarantee that the traffic mix and test methodology is one that has been agreed and signed up to by NetSecOPEN's members (and is awaiting ratification as an IETF standard). The test methodology used is publicly available.
- **Free independent test reports.** NetSecOPEN's goal is to make vendor test reports freely available from the NetSecOPEN website. This contrasts with the independent but proprietary testing model which often requires that users pay for test reports.
- **Less time spent on initial testing prior to live deployment.** Greater confidence in NetSecOPEN test suites – derived either from detailed investigation into the test suites or merely because of their status as open industry standards – should make user organizations more willing to forego some initial rounds of the basic testing they undertake themselves prior to live commercial deployment. Users should be more willing to forego some of these basic tests compared with what they feel they have to do with products that are only certified against proprietary test suites.

Buyers also stand to benefit indirectly from the healthier, more efficient, vendor ecosystem that NetSecOPEN is fostering:

- **Continuous improvement in the performance of network security products resulting from vendors using independent NetSecOPEN test results for product engineering improvement, not just sales and marketing.** Unlike common practice with proprietary testing suites, vendors can test their products themselves against the NetSecOPEN test suite in their own labs any time they like. This should make for better, more agile, product improvement by allowing more frequent internal performance testing against NetSecOPEN standards.

  This can also reduce the cost to vendors of optimizing their product to perform well in independent NetSecOPEN tests. In the case of some proprietary test models, vendors sometimes pay a test house for an initial round of private testing to identify areas for improvement before submitting to a wider, public, multi-vendor, test whose outcomes are then published (and for which the vendor has to pay again).
- **Reduced variance in the test outcomes generated by different test equipment vendors when testing the same product.** NetSecOPEN is driving its test equipment vendor members to align aspects of their own product

characteristics. This is to minimize the variation in the test results their test tools generate when testing the exact same NGFW product against the exact same NetSecOPEN test suite. As well as further enhancing the credibility of NetSecOPEN test outcomes, this is intended to give NGFW vendors a more competitive market in test equipment. This should help NGFW vendors avoid the scenario of becoming dependent on any one test equipment vendor that consistently generates higher test scores for its products than another's.

NetSecOPEN Milestones 2017 - 2020

As shown in **Figure 4**, NetSecOPEN can point to a number of milestones it has achieved since its founding in 2017. As shown in **Figure 3**, it now boasts twelve industry members. Members have agreed on a representative traffic mix. The first draft NetSecOPEN standard for testing the throughput performance of NGFW products was submitted to the IETF in March 2018 and is now close to final ratification.

During 2019, working with test houses and NGFW vendors, leading test equipment vendors have made enough progress in reducing the variance in outcomes generated by their products to render NGFW vendors comfortable with investing in the first commercial NetSecOPEN certification testing.

The first vendors have submitted their NGFW products for formal NetSecOPEN certification.

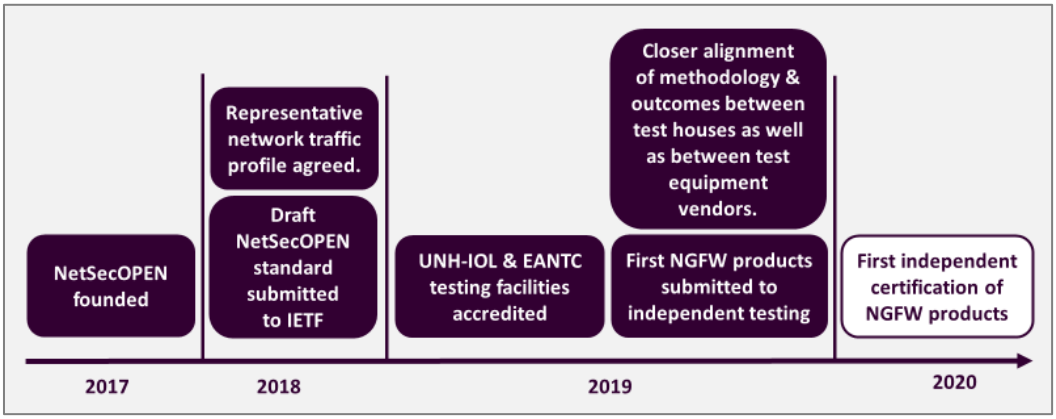
First Products Submitted for Certification Testing

The first NGFW vendors have submitted their products for formal NetSecOPEN certification testing under commercial contracts with the University of New Hampshire InterOperability Laboratory (UNH-IOL) and the European Advanced Networking Test Centre (EANTC). This is NetSecOPEN's most important commercial milestone to date. It should pave the way for the first NGFW vendors to go to market with NetSecOPEN-certified test results during the first quarter of 2020.

Ongoing work within NetSecOPEN over the next twelve months includes:

- Updating the set of Common Vulnerability and Exposures (CVEs) to be used in the test suite, with a view to updating them on an annual basis.
- Adding evasion techniques into the standard.
- Adding elements of malware testing.
- Development of standards for configuring devices for security effectiveness.
- Development of specifications for testing IDS/IPS systems (whether integrated into the current NGFW test suite, independent of it, or potentially both).

Figure 4: NetSecOPEN's Roadmap Milestones 2017 - 2020



Source: HardenStance

The Outlook for User Adoption of NetSecOPEN

The release of the first NetSecOPEN-certified NGFW products in 2020 promises to open up a new era in more trusted network security testing. NetSecOPEN isn't going to rapidly sweep the proprietary testing model aside, though. The organization is too new for that. Besides, the very strength of NetSecOPEN's consensus-driven and highly rigorous testing model also means that the organization cannot be as agile as test houses operating proprietary models in terms of how quickly they can bring new – albeit less trusted – test suites to market.

The most likely outcome, beginning from 2020, is that a new market opens up in standards-based NetSecOPEN certification which grows to co-exist with the established proprietary test model over a long period of time. Exactly what kind of commercial traction NetSecOPEN sees in the marketplace will then be determined by the preferences and behaviours of the two largest stakeholder groups. These are the NGFW vendors themselves and – above all - their end user customers.

As already discussed, NetSecOPEN's approach has potential to engage a vendor's product development team on a much deeper level. This should mean that vendor engagements with the NetSecOPEN testing ecosystem need not be driven almost entirely by their sales and marketing organizations, as they tend to be in today's proprietary testing environment.

The most likely outcome is that a new market opens up in standards-based NetSecOPEN certification which grows to co-exist with the established proprietary test model.

If NetSecOPEN yields lower numbers, Will Vendors Even Use Them?

That said, there is an obvious hurdle that NetSecOPEN potentially faces when it comes to gaining mindshare within an NGFW vendor's sales and marketing organization. This is that its' more realistic, real-world, test outcomes may generate performance numbers that are lower – perhaps a lot lower - than those generated by proprietary test suites. In this scenario, the obvious question then arises of how can an NGFW vendor justify promoting lower NetSecOPEN test results alongside – let alone instead of – higher proprietary test scores?

It's clear that in the first instance a vendor's sales and marketing team may hesitate to point customers to NetSecOPEN datasheets if their numbers are comparatively low. This will be a challenge but not an insurmountable one. Some of the following types of real-world sales engagements illustrate why the idea of using lower, more credible, numbers need not be as fanciful as it might appear:

- **Some buyers actually want more credible – lower – numbers.** On the ground, NGFW sales leaders know that some customers and customer prospects are so hostile to traditional sources of independent test data that they literally cannot be moved by serving them up their latest output. These customers are low hanging fruit for NetSecOPEN test results that can be shown to have been purged of proprietary excesses. If NetSecOPEN numbers are lower by comparison, this will actually be a more effective sales tool with these customers.
- **Any leadership position is always good.** NGFW vendors that emerge very well in NetSecOPEN tests compared with competitors will have a clear incentive to leverage those results in their sales and marketing.
- **Two different test certifications are better than one.** Consider an NGFW vendor whose numbers substantially outperform competitors in proprietary independent tests but are only on par with competitors in NetSecOPEN tests. Some buyers will consider a combination of the two independent proof-points – one standards-based, the other proprietary – more compelling than a pitch that revolves solely around the bigger proprietary test numbers. The same can be true of a vendor that rarely or never emerges in a leadership position or usually shows as being below par. Some buyers will trust two different test outcomes showing that vendor to be on a par with the market more than they would just one of them.

For an open ecosystem to take off and truly thrive will require buyers to step up, engage, and demand NetSecOPEN proof points from their vendors.

Ultimately, the rate of market adoption of NetSecOPEN test results is going to be driven by the expectations, assumptions and behaviours of buyers themselves. Buyers can no longer sit on the side-lines complaining about proprietary test outcomes. If they want better independent test results, they need to actively engage in demanding them.

For an open ecosystem to truly thrive will require buyers to step up, engage with NetSecOPEN, and demand NetSecOPEN proof points from their vendors. That's the only way a virtuous cycle can be created that drives NGFW vendors to invest further in the NetSecOPEN ecosystem and promote its test results.

Ultimately, user organizations also need to find ways of enabling some among their number to join NetSecOPEN, actively participate as members, and help drive the development of additional test requirements. A criticism that is often levelled at industry standards organization like NetSecOPEN is that they are dominated and driven by vendors with their own commercial agendas.

As this paper has shown, NetSecOPEN's members are doing a lot to create greater trust in independent network security testing. Users themselves now need to do more to play their part in increasing that trust still further. Users need to recognize that this effort can't succeed at scale without their support ■

About Spirent Communications

Spirent Communications plc. (LSE: SPT) offers test, measurement, analytics, and assurance solutions for next-generation devices and networks. The company provides products, services and information for high-speed Ethernet, positioning and mobile network infrastructure markets, with expanding focus on service assurance, cybersecurity and 5G. Spirent is accelerating the transition of connected devices, network equipment and applications from development labs to the operational network, as it continues to innovate toward fully-automated testing and autonomous service assurance solutions. For more information, please visit www.spirent.com and follow us on LinkedIn, Twitter and Facebook.

About NetSecOPEN

NetSecOPEN's mission is to work with industry and others to create well defined, open and transparent standards that reflect the security needs of the real world. Standards development efforts are open to all of those with a vested interest in the outcome. That includes enterprises in addition to security product vendors, tool vendors and labs. For more information visit www.netsecopen.org

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a well-known voice in telecom and enterprise security, a leader in custom cyber security research, and a leading publisher of cyber security reports and White Papers. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, ETSI and TM Forum. To learn more visit www.hardenstance.com