WHITE PAPER

ixia

Maximizing Security Resilience: The 4-Letter Word That Can Save You Millions

Table of Contents

Executive Overview

If you are in any way responsible for "security" for your organization, you are definitely living in challenging times. Everyday, your network and applications are caught in the crosshairs of attackers intent on finding any vulnerability or weakness they can exploit. It is no longer sufficient to just choose and deploy the products designed to address your security needs; you now need to prioritize gaining deeper insight into your overall security resilience.

"Resilience" is defined as the ability to bounce back, and when it comes to security, every second needed to defend and recover from attacks can mean millions of dollars lost. Most enterprises are now spending heavily to deflect crippling cyber attacks that impact their revenues and reputation, but without a viable means of testing before they invest, and validating future changes.

Why read this paper?

"Resilience" is defined as the ability to bounce back, and when it comes to security, every second needed to defend and recover from attacks can mean millions.

If your job involves addressing and responding to the security challenges your organization faces, this paper can help you. We'll explore traditional approaches to assessing security investments, look at the financial benefits of testing, and debunk the excuses that keep IT organizations from validating their security infrastructure and deployment processes.

And last but not least, we'll introduce new solutions and best practices for staying a step ahead of the evolving threat landscape. Ignoring security resilience testing is a "head-in-the-sand" approach that can cost organizations millions, and individuals their jobs.

We'll look at solutions and technologies that can cost-effectively model and apply the realism found in your company's one-of-a-kind network, right down to your applications and even a single user behavior. Creating and applying the realism of your unique network traffic and application activity includes modeling user behavior that involves both legitimate enterprise users and malicious attackers. Using this approach and economical new techniques, IT managers can quickly evaluate how specific technologies such as NGFWs, or a layered security architecture, will perform and safeguard application performance in their own unique environments.

Along with opportunities for cost-reduction, this paper will discuss other powerful benefits of security resilience testing such as knowing for certain that:

- You're selecting the most optimized and cost-effective security for your one-of-a-kind network
- You have right-sized investments to meet your company's business AND security needs
- Your network has the high level of security resilience needed to defend against attacks
- Company personnel and the enterprise network will be ready when inevitable attacks occur

Let's start with a look why traditional means of making decisions aren't sufficient for ensuring security resilience in today's fast-changing threat environment.

Chapter 1: Does Buying the "Industry Best" Mean Anything Anymore?

Ask any IT manager how they make new security investment decisions and most will answer, "We buy from the industry's leaders," or "We buy the best solutions in the industry." But in a world of one-of-a-kind application-driven networks, does "industry-best" mean anything anymore?

For example, according to the 2014 Gartner Magic Quadrant for Enterprise Network Firewalls,[1] NGFWs are finally becoming mainstream, representing a forecasted 70% of new edge purchases in 2015. This prediction means many equipment manufacturers will be beefing up their marketing to capture a share of the sales growth, while enterprises toil over their next major IT purchasing decision.

The reality is that all vendor technologies are engineered with biases and objectives, with the hope of mass adoption. For example, most NGFWs include support for AppID, IPS, AV, and even APT sandboxing. These are compute-intensive applications that respond differently based on the applications and user behavior they see, as well as the biases that go into their engineering. These are not cookie-cutter functions and won't necessarily perform well in your network using only the default configuration.

Figure 1. Magic Quadrant for Unified Threat Management

Source: Gartner (August 2014)

So while the information captured in quadrant-type reports may be suitable for vendor marketing purposes, the product comparisons they contain may not be as relevant as you'd like them to be in planning your network. Vendors may slice and dice information to tout themselves as market leaders recognized by industry analysts, but the findings are largely based on an analyst's review of data sheets, conversations, and other anecdotal information.

While the information captured in quadrant-type reports may be suitable for vendor marketing purposes, the product comparisons they contain may not be as relevant as you'd like them to be in planning your network.

While it's not directly stated, the implication of high rankings in these reports is an "industry-best" label, but there's an inherent conflict between what the analyst report portrays and the nature of how well devices meet a company's one-of-a-kind network needs. There is no "one-size-fits-all solution;" the promise of a magic box for the masses just doesn't exist.

1 https://www.gartner.com/doc/2329815/magic-quadrant-enterprise-network-firewalls

Analyst and sponsored third-party reports may define a “best” based on a single, generalized synthetic criteria, but so what? Their findings don’t reflect the needs for your unique network and business objectives, so why should they impact your important buying decisions?

Instead, the challenge is determining what “industry-best” means for your particular network. Like it or not, the decision—along with the justification behind it—may fall squarely on you, and there’s only one proven way to protect yourself, and your network, from ever-growing risk.

You Don’t Have to Like It, but You Now Need to Do It

Since you can’t rely on the “magic” in the quadrants, what can you do? Although it’s a forbidden word in many IT organizations, the answer is: TEST. In some enterprises, ‘testing” is somewhat of an unspoken 4-letter word, often linked with two other 4-letter words: "Cost" and "wait."

Testing validates or debunks what you think you know, and uncovers what you don't (but need to) know. Relying on anything else, including sponsored lab reports and vendor data sheets, amounts to guessing.

Even here at Ixia, we’ve resorted to skirting the “T” word with terminology such as “access, validate, and verify.” But the harsh reality is that the issue can’t be skirted any longer.

Enterprise IT managers are realizing that the same fundamentals they learned at school about good design practices – including testing (or verification/validation) – remain essential amidst the realities of today’s threat landscape and hectic IT lifecycle management. Testing validates or debunks what you think you know, and uncovers what you don’t (but need to) know.

Relying on anything else, including sponsored lab reports and vendor data sheets, amounts to guessing. And that’s dangerous.

So let’s debunk some of the popular myths surrounding testing.

Chapter 2: Debunking Myths about Enterprise Testing

Technical schooling teaches that testing is an integral and essential part of good design practice; that it proves or disproves our assumptions, and validates design objectives. More importantly, testing uncovers unknowns we may not have considered as inputs in designing complex systems.

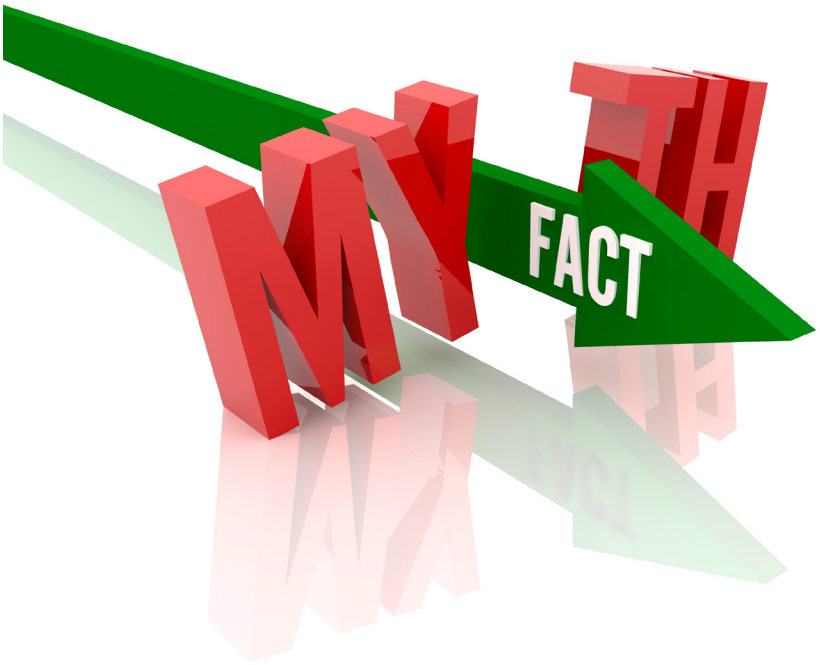
This proves especially vital for security, where failures to protect an organization may have financial, legal, and job-retention ramifications. Rigorous high-fidelity security resilience testing conducted in a safe environment is a must prior to rolling out new technologies and architectures, before the stakes become too high.

To date, some IT and security professionals have chosen, or had no choice but to have their live production networks serve as the test bed, and to use support line ticketing to gauge the success or failure of the implementation. In rolling out a NGFW using the vendor’s default configuration, or a new patch to existing technology, such an approach might easily result in IT being forced to do a costly rollback when the help desk ticket logs go beyond what can be ignored. Worse yet, the company’s name may be splashed throughout the media in yet another headline about failed security.

We can all see that this logic is deeply flawed, yet those with clear intentions for building and running secure, resilient networks continue to work this way, often for one of the following reasons:

- "Vendors test, so I don't need to"
- "We contract a Pen tester every year to stay compliant, so we don't need to test"
- "We don't have time to test"
- "We don't have budget to test"
- "Management doesn't understand why we have to delay rollout to conduct testing"
- "We tested the network when we initially rolled it out years ago"

In the past, there was no getting over some of these hurdles. Today there is. So let's take a closer look at these persistent and costly fallacies, then at how cost-effective new evaluation strategies help IT overcome resistance to making sure their networks perform as expected.



No vendor can reproduce every potential customer environment.

Vendors test, so I don't need to."

While it's definitely true that vendors conduct exhaustive testing of new technologies, we need to consider their objectives and how they relate to your real-world, one-of-a-kind network and application implementations. Ixia's core business arose from network equipment manufacturers (NEMs) who purchase high-end test equipment and services to help in creating innovative, world-class technologies. But even with these investments, no vendor can reproduce every potential customer environment, nor do they advertise having done so.

The object of vendor testing is to verify the functions and performance advertised on data sheets in the context of a reproducible, fixed use-case. Test methodologies are largely driven by marketing with the objective of substantiating the biggest, most eye-catching parameters.

For example, vendors may use industry standards like RFC2544 (UDP/TCP) or RFC3511 (HTTP) to validate performance. Both of these standards are more than 10 years old and use synthetic transport streams with artificial data in the payload. In contrast, modern networks are content-aware and driven by applications. The real performance of a content-aware next-generation technology will behave radically differently when passing a string of "AAAA" to a pair of IP address and ports, versus application traffic from thousands of users setting up and tearing down multiple sessions. Understanding application and user behavior using deep packet inspection (DPI) is compute-intensive and cache-inefficient versus synthetic traffic that is easily hardware-accelerated and cache-efficient.

Second, when it comes to security effectiveness, the parameters are captured while no real workloads are active. This is not a valid use-case for your network. Detecting threats is like finding a needle in a haystack; without a haystack, it's easy to find the needle. Pile on the hay, and it's a different story.

Only realistic testing of security technologies or the whole network using valid workloads and attacks—at scale – lets you be sure the network will bounce back during and after an attack, stay resilient, and determine which devices are best as you build out your system.

For example, do attacks come on Saturday at 2 AM when there is little activity on your network, or it is more likely that you'll experience a distributed denial of service (DDoS) attack or exfiltration at the most precarious time – when there are thousands of critical transactions that need to be defended? Vendors can't give you these performance numbers on a data sheet.

What about interworking? How can any vendor give assurance that their technology will seamlessly interoperate in your complex environment?

Only by testing against the variables of real-world traffic mixes and conditions can you can answer these critical questions for yourself in your one-of-a-kind network.

"We contract a Pen tester every year to keep compliant."

Wrong again. Pen testing and vulnerability assessments are critical steps used as evidence of compliance with requirements for securing a network. But "in compliance" doesn't necessarily equal "secure." Pen testing has many benefits, but does not cover all critical elements of security resilience.

What about knowing how a security technology or the network will behave under real-user workload while under attack? How about the ability of your network and security/IT personnel to defend against DDoS during peak customer hours? What about determining the best technologies to bring into your network and right-size your investment?

Only realistic testing of security technologies or the whole network using valid workloads and attacks—at scale – lets you be sure the network will bounce back during and after an attack, stay resilient, and determine which devices are best as you build out your system.

"We don't have time to test."

The plain truth is: you don't have time not to. For sure, security professionals are under tremendous pressure and are often under-staffed. Time is fixed, and needs to be managed. But in the end, effective use of time is best explained in the simple time-proven adage: "Measure twice, cut once."

Following best practices means carefully planning, designing, implementing, and testing up front. Validating results ahead of time will dramatically reduce the huge time-sink of daily firefighting. Intuitively we all know this is true, but often emphasize urgent reactive firefighting over vital proactive steps that will minimize future firefighting.

"We don't have budget to test."

In the past, building robust testing platforms like those used by vendors has been difficult and cost-prohibitive for the enterprise, in terms of both implementing test technologies and allocating the manpower needed to conduct tests. Massive racks of servers were typically required to model user behavior and create realistic traffic loads, and introducing realistic security attacks into the test bed was nearly impossible.

Simulate a DDoS attack at scale? Good luck.

The only options were to conduct functionality testing at small scale, or resort to low-level brute-force packet-generation tools to flood ports. Fortunately, the ecosystem and best practices for testing has advanced quite a bit.

Today, technologies are available from providers such as Ixia to enable testing at enterprise-wide scale by generating realistic traffic that effectively models your unique network as well as attacker behavior. And was we'll see in Chapter 5, comprehensive testing can now be conducted using low-cost appliances or virtualized software that can be loaded onto servers or reside in the cloud and be shared by users at multiple locations.

"Management doesn't understand why we have to delay rollout to test."

Dealing with CxO demands can be challenging since they too are under pressure and often lack technological backgrounds. CxOs are primarily focused on business where it's not always about doing the right and smart thing, but rather the things that make money, save money, or that someone requires us to do (compliance).

Even so, they must ultimately answer the same important question from stakeholders, "How do you know it will work?"

They, like you, should consider the possible answers:

1. "Because we only buy the best technology."

2. "Because it worked yesterday, it should work tomorrow."

3. "Because we tested it."

Obviously, Number 3 is the only safe and acceptable answer. In the next chapters, we'll look at calculating and demonstrating to management how testing equals (many) dollars saved.

There's only one acceptable answer to the question, "How do you know it'll work," and that's, "Because we tested it."

"We tested when we rolled out years ago."

Great. But networks, services, applications, and attacks change constantly. Looking back on your network two years ago—its size, the average bandwidth consumed by users, the applications and services used—what percentage remains the same today? In today's world of ever-changing threats, perpetual patch rollouts, virtualization, and other challenges, a two-year statement on change may be as narrow as one hour ago.

Hopefully by this point you're convinced that you can't rely on data sheets, analyst reports, outmoded data, or other anecdotal information to select the right security gear for your particular network. Testing is now the only way to ensure your network is secure and resilient to attack. "Knowing," versus "guessing," is the only safe way to decide which technologies will result in secure and resilient networks that pay off in the near term as well as the long run.

Let's do the math...

"Knowing," versus "guessing," is the only safe way to decide which technologies will result in secure and resilient networks that pay off in the near term as well as the long run.

Chapter 3: The Value of Testing

What if you could show management quantifiable savings of 20%, 30% or even 50% of the budget allocated for your next security investment spend (and unequivocally know you made the right decision)? You can.

Here's how:

Maximize Security Investment with an Onsite PoC

Acquiring new security technologies is an important and highly visible stage during which real-world testing can dramatically impact the bottom line. Consider a recent Infonetics Research report[2] reinforcing the company's 2013 forecast for enterprise data center spending on security. The report projected average spending on security products would reach $17M. This number might vary according to how a network scales, and the functions being secured.

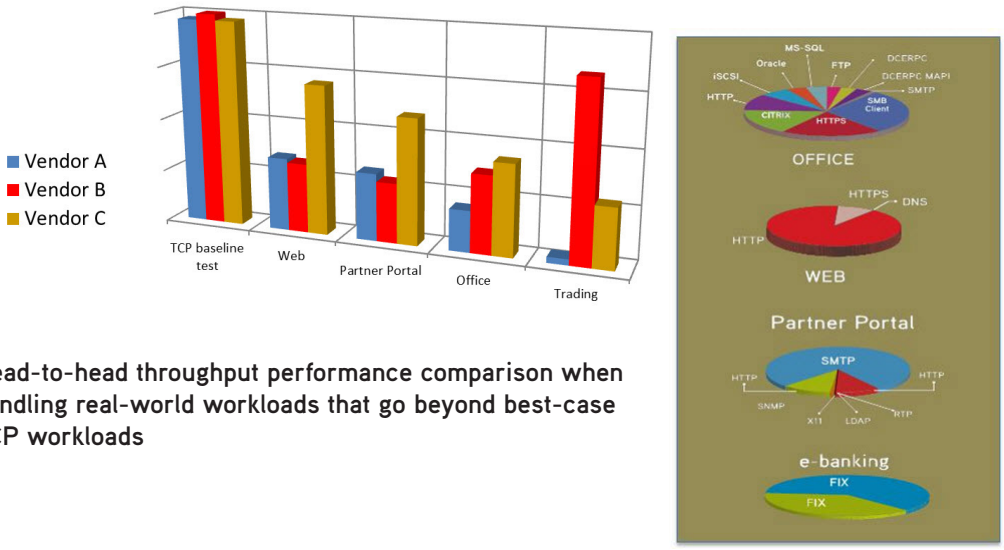
Now consider the selection process for procuring those security products. Typically, IT organizations will research available products and send out a request for information (RFI) with the goal of narrowing the search to two or three vendor solutions. At this point, some level of more detailed research and evaluation of each solution typically begins.

But as we discussed earlier, vendor data sheet performance numbers are not a good estimation of how devices will perform on your particular network, running your particular network traffic. To get meaningful performance numbers that lead not only to the purchase of the best gear for your implementation, but also to significant cost-savings, enterprises must conduct onsite head-to-head bakeoffs. [Learn more about why and how to do data-driven proof of concepts in the Ixia white paper, "How to Maximize IT Investments with Data-Driven Proof of Concept (PoC)"[3].]

2 http://www.infonetics.com/pr/2013/Enterprise-Data-Center-Security-Survey-Highlights.asp

3 http://info.ixiacom.com/Enterprise_IT_6_Steps_Data_Driven_Proof_of_Concept.html

The following diagram portrays a real PoC that Ixia helped conduct which showed the deviation in performance of a set of industry-leading NGFW products when real-world simulated workloads were applied. As the diagram illustrates, the synthetic TCP workload doesn't tell much other than to validate the best-case data sheet numbers provided by the vendors. However, once the real-world workloads were applied with the target features enabled on the security product, a great deal of light is shed on how each technology and its compute-intensive algorithms will behave in a real network. An interesting note is that it took just three days to get to this level of quantifiable data using Ixia's BreakingPoint test solution.



Head-to-head throughput performance comparison when handling real-world workloads that go beyond best-case TCP workloads

As we've seen, device vendors develop their technologies with specific problems in mind that they're aiming to prove they help solve. Then they take these products to market as general solutions with the hope of reaching a wide customer base. The reality is that performance and security effectiveness will never be the same in any two networks. Selecting the right technology that best matches your network needs, and then right-sizing that investment, will add quantifiable dollars to the bottom line.

Selecting the right technology that best matches your network needs, and then right-sizing that investment, will add quantifiable dollars to the bottom line.

The price variance among NGFWs is evidence that selecting the right device can have a profound impact on investment costs. By way of example, let's choose four competing NGFW solutions that enterprises commonly evaluate today (evidenced by their inclusion in the NSS Labs NGFW Security Value Map[4]). Pricing is publically published by a common reseller.

These devices all have different functionality, performance, and capacity, so this is by no means a scientific apples-to-apples comparison, but it does show widely varying costs for solutions advertising similar benefits.

4 https://www.nsslabs.com/next-generation-firewall-security-value-map-download

Randomly chosen models from NSS report and price available on www.CDW.com	CDW advertised price (www.cdw.com,Jan 2015)	% to highest advertised price
Cisco ASA 5585-X Security Plus Firewall Edition SSP-20 bundle	$50,061.99	100%
McAfee Next Generation Firewall 1402-C1	$34,707.99	69%
Fortinet FortiGate 1500D	$43,658.99	87%
Palo Alto Networks PA-3020	$15,573.99	31%

Using simple math based on the $17M average data center security spend mentioned above, it works out that there would be a huge cost variance if all the products satisfied an IT department's need; however, it is not very likely that all products will satisfy your particular needs.

If you could spend $5M annually rather than $17M to satisfy your security needs, surely that kind of savings offsets the cost of conducting your own PoC.

Generalizing that all security product categories have similar price variance, and doing simple calculations, reveal that knowing which solution satisfy your needs at the lowest cost could result in significant cost-savings.

Average data center security spend (Infonetics estimate for 2015)	$17M
Highest cost solution	$17M
Lowest cost solution	$17M x 31% = $5M
Cost range	$5M - $17M

If you could spend $5M annually—rather than $17M—to satisfy your security needs, surely that kind of savings would offset the cost of conducting your own PoC. But the financial benefits of testing don't end there:

The ABC of Negotiating

Whether for a personal or work purchase, everyone wants a good deal. Many companies have entire purchasing departments that are graded on deviations to standard price, otherwise called discounts. Negotiating is an art-form whose roots lie in information.

PoCs reveal quantifiable data on performance, security effectiveness, and actual feature viability. Getting the right data to your purchasing department provides a decided but fair advantage in negotiating, and removes the need to be heavy-handed or come from a weak position making unjustifiable demands.

With the stakes approaching $17M in annual security spend, a 15%, 10%, 5%, or even 3% discount has very significant impact to the bottom line. Testing strengthens IT's negotiating position, resulting in another significant financial gain.

Discount %	Discounted $ from $17M budget
15%	$2.6M
10%	$1.7M
5%	$850K
3%	$510K

Helping your company reduce capital outlay is good for all the stake-holders, and for your career.

Right-Sizing Investments

Without knowing exactly how a security solution will perform in your network, the only option is to guess and work off of a de-rating factor. By nature, de-rating is conservative and forces you to buy up, rather than down. Depending on the technology and historic experience with a vendor, you may choose 30% or even 70% de-rating from the data sheet.

Let's take one of the above vendor solutions as an example of sizing. Without confidence in top-end performance scaling, you would need to scale out by adding another product, or scale up by upgrading to the next higher SKU. Either way, the cost impact is significant. Performance and cost do not scale linearly, so scaling up may be more expensive than scaling out.

Sample solution from above table	Price advertised by distributor (www.cdw.com, Jan 2015)	Variance to the lowest advertised price
Fortinet FortiGate 1500D	$43,658.99	100%
2x Fortinet FortiGate 1500D	$87,317.98	200%
Fortinet FortiGate 3600C	$157,844.99	362%

As we've seen, de-rating and guessing is a costly strategy. Testing your technologies and network with real-world workloads while under attack will give you the data needed to more efficiently right-size investments.

As all networks are unique, we'll leave the tallying of your company's potential savings to you. The net, however, is that you can't afford not to do it.

Chapter 4: The Not-so-Hidden Costs of Failing to Test

The real world, as we know, can be harsh. The media is littered with companies, all with good intentions of securing their networks, who quickly succumb to attack.

Afterwards, the organization, customers, and other stakeholders consider what went wrong, and how to keep it from happening again. What's surprising is that many front-page incidents are based on well-understood attack strategies that have not changed much over the years, other than to become more targeted and persistent. In DDoS attacks, for example, strategies from the '90s are still used today, intensified by the ease of creating massive and long-duration campaigns.

Post-mortems conducted recently after major breaches at Target and Sony did not reveal any new exotic attack vectors, but the impact was clearly costly and far-reaching. And while the cost of having customers be afraid to do business with you may not be quantifiable, other costs are:

Attack timing and duration is most problematic as DDoS attacks are conducted at critical times in the targeted organization's business window and, if successful, cause the equivalent of unplanned downtime.

The Cost of Downtime

The cost of security incidents can be partially quantified for enterprises in the form of lost productivity due to unplanned downtime. A July 2014 Gartner blog[5] reported that network downtime typically costs enterprises $5,600 per minute.

Downtime (mins)	Downtime $ impact
1 minute	$5,600
10 minute	$56K
1 hour	$336K
8 hours	$2.7M

Attacks and network incidents are inevitable in today's application and threat-driven environment. The time it takes to defend and restore to full operation is critical, and the dollar-impact math simple.

DDoS attacks in particular take the cost of downtime to the extreme. The volume of DDoS attacks is on the rise, and they continue to grow in size and complexity using application-layer strategies. Attack timing and duration is most problematic as these attacks are conducted at critical times in the targeted organization's business window and, if successful, cause the equivalent of unplanned downtime.

5 http://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/

The Prolexic Q1 2014 Global DDoS Attack Report[6] revealed that DDoS attacks average 17 hours. This amount of time is staggering in and of itself, and the cost of resulting downtime even more onerous:

17 hours =	1,020 minutes
1,020 minutes x $5,600/min. =	$5,712,000

Once again, security resilience –and in turn security resilience testing – can make the difference between timely recovery and going out of business.

Rollbacks = Setbacks

Patching and upgrading technologies is a common occurrence in modern networks, and critical to securing networks, devices, and applications. Unfortunately, most of us have experienced a fair number of patch, feature, and even equipment rollbacks.

Rollbacks are embarrassing first, and second, they add substantial cost to your operations. No one intends for firmware updates to be brought back to a previous state, so personnel time has to be diverted from what was planned to deal with the unplanned.

Additionally, equipment and security effectiveness is compromised for the periods of time during which technologies are inaccessible. These issues can be mitigated if the patch or upgrade is tested against the previous baseline in the staging phase of the rollout, all with the same due-diligence as when the technology is first brought into the organization.

The impact of rollbacks is not easily quantified in dollars as most of the costs have extreme variability: labor ($75-$150/hour); travel, if required; support ticket management from complaining users; troubleshooting hours for tier 1-3 support; taking products out of service during the unplanned rollback; and the like. We'll leave it to you to estimate in your own context whether these events should be seen as inefficiencies or catastrophic events that can rip apart a business' bottom line.

In any case, these are just some of the costly occurrences that real-world testing can help eliminate or substantially reduce. Assuming you agree by now testing makes infinitely more sense than not testing, let's look at how evolving solutions make it exponentially easier and more efficient to do so.

6 http://www.prolexic.com/kcresources/attack-report/prolexic-quarterly-global-ddos-attack-report-q114/A4-Q12014-Global-Attack-Report.pdf

Chapter 5: Virtualizing Industry-best Techniques

In recent years, platforms used to validate security resilience and device performance have scaled to fit the needs of the enterprise. Smaller, lower cost chassis, testing as a service (TaaS), and subscription-based services for keeping threat databases updated have made it easier for companies that don't maintain pre-deployment labs to avail themselves of the industry's more powerful performance validation.

Ixia BreakingPoint, the leading choice of security infrastructure manufacturers and service providers worldwide, can now deliver powerful PoC capabilities on the compact PerfectStorm One platform. For ongoing protection, Ixia's Application and Threat Intelligence (ATI) Subscription Service delivers:

- 6,000+ live security attacks
- 35,000+ pieces of live malware
- 180+ evasion classes
- DDoS and botnet simulation
- Real-world applications
- 250+ application protocols
- Social, P2P, voice, video, Web, enterprise business applications, gaming, mobile, storage workloads
- Bi-weekly software updates and enhancements
- Research into emerging vulnerabilities

In recent years, platforms used to validate security resilience and device performance have scaled to fit the needs of the enterprise.

More recently, Ixia announced BreakingPoint Virtual Edition (VE) to make it even easier for companies of all sizes to validate their technology choices and identify problems before costly incidents occur. This software- and subscription-based approach allows enterprise IT departments to leverage the same powerful capabilities as BreakingPoint on PerfectStorm using a highly scalable deployment model.

BreakingPoint VE delivers:

- ***Lower cost of entry*** based on annual subscriptions that fit well within IT project budgets for initiatives such as deploying NGFWs
- ***Virtualized test capabilities*** that are easily shared by multiple users across multiple locations
- ***Shareable licenses*** that begin at just 1G and scale by 1Gbps increments

This efficient, pay-as-you-grow model allows IT to quickly and easily replace guesswork with facts, and uncertainty with confidence. With virtualization, the two most formidable objections to testing – "We don't have time," and "It's not in the budget" – can easily be overcome, and the missing piece of ensuring security resilience put in play.

BreakingPoint VE
Low cost of entry
Scalable in 1G increments
No lab required
Easily shared by multiple locations

Conclusion: Do You Know How Your Network (and Personnel) Will Fare?

Attacks are a foregone conclusion. Attackers are persistent, technologies fail, humans err, and the landscape moves constantly.

No technology, network architecture, or even rigorous disciplined testing can provide a 100% guarantee that issues will not arise in production. However, it is a fact that real-world security testing helps you find problems, validate knowns, and discover unknowns in advance of costly security incidents.

A network resilient to attacks, misconfiguration, bottlenecks caused by integration, and changes from user behavior and patching can be the difference between an inconvenient incident and going out of business for many organizations. Testing technologies, networks, and the reactions of security personnel with simulated real work-loads, at scale, provides advanced knowledge on how your organization and its technology will fare under attack, and define its breaking points. With this knowledge in hand, you can adjust configurations, architectures, and policies to ensure defenses are working properly and will bounce back within a reasonable timeframe.

With virtualization, two of the most formidable objections to testing – "We don't have time," and "It's not in the budget" – can easily be overcome, and the missing piece of ensuring security resilience put in play.

As we've seen, there is a high price to pay for a network that is not resilient – not only to attacks, but inefficient lifecycle and change management processes. Testing is a critical component of every organization's battle to ensure network security resilience that can handle the worst global attackers dish out.

We challenge you to use the information in the previous chapters to calculate what your organization can save in dollars, and brand reputation, by making cost-effective security resilience testing a focal point in evaluating new technologies. From there, it's a matter of what approach to testing best fits your organization's needs.

But make no mistake, big, small, or geographically dispersed, your company can no longer afford not to its infrastructure to the test before investing in defenses, and as threats evolve into the future.

We challenge you to use the information in the previous chapters to calculate what your organization can save in dollars, and brand reputation, by making cost-effective security resilience testing a focal point in evaluating new technologies.

Ixia Worldwide Headquarters
26601 Agoura Rd.
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800
(Fax) 818.871.1805
www.ixiacom.com

Ixia European Headquarters
Ixia Technologies Europe Ltd
Clarion House, Norreys Drive
Maidenhead SL6 4FL
United Kingdom

Sales +44 1628 408750
(Fax) +44 1628 639916

Ixia Asia Pacific Headquarters
21 Serangoon North Avenue 5
#04-01
Singapore 554864

Sales +65.6332.0125
Fax +65.6332.0127

915-6784-01 Rev. A, February 2015