The CISO's Guide to Ensuring IT Resiliency in the Face of Change

Using Actionable Security Intelligence to Assess and Defend Your Security Posture

BreakingPoint™

Find it before they do.™

Introduction

Without an ongoing security testing regimen in place, even the most sophisticated IT defense measures will not guard organizations against crippling attacks, data leaks or internal sabotage. And there's one enemy to blame: change.

Today, mutating advanced persistent threats (APTs) are being launched into the wild at an accelerated rate. New, highly dynamic social media applications that serve as carriers of vicious malware are exploding in parallel with the rampant "bring your own device" movement, impacting every organization. Torrents of converged network traffic are driving data, voice and video across and throughout IT infrastructures at an unprecedented clip. And these are just a handful of change agents challenging the efficacy of incumbent security systems that are being asked to adapt to environments scarcely resembling the IT world of just a few years ago.

As seasoned CISOs know better than anyone, the effectiveness of security measures and technologies cannot be judged in pristine lab settings. They are determined by the harsh realities of real-world operating conditions, where unknowns and constant change abound. And this raises important questions about how to protect existing investments in defense-in-depth security architectures and prevent the impact of change from eroding an organization's current security posture.

With so much at stake, this white paper will examine the role actionable security intelligence (ASI) plays in helping organizations:

- Monitor global threats and application trends and their impact on infrastructure resiliency
- Evaluate the efficacy of network, data center and security technologies under real-world, Internet-scale conditions
- Manage change and configuration drift through initial baseline measurement and ongoing testing and validation
- Gain better insight into how and where change impacts an organization's security posture
- Reduce the time to make informed and time-sensitive security decisions
- Transform processes enabling organizations to identify and maintain a resilient security posture

Combating Change Through Continuous Security Testing

Security is a moving target, which explains why so many organizations apply defensive measures on a reactive, trial-and-error basis. Against this backdrop is a dearth of truly qualified "cyber warriors" equipped with the expertise required to strategically combat the growing complexity of what amounts to a security battlefield. But without a way to bridge the "reality" gap between the static, unpolluted environments of preproduction test labs and live production networks contending with dynamic change, the majority of IT and security organizations often have no choice but to rely on the assurances of their vendors.

In many respects, this "strategy of hope" for avoiding attacks fosters a false sense of security and creates dangerous blind spots. It also makes evaluations of IT investments less reliable because canned performance benchmarks can belie how security systems — such as firewalls, UTMs, IPS/IDS, and more — actually perform in the volatile world of live networks. Adding to the mounting pressure on IT and security organizations are more aggressive legislative initiatives and policies mandating increasingly rigorous security enforcement and accountability. Failure to meet compliance requirements can incur stiff penalties. In short, enterprise IT and security organizations are at a breaking point.

Because of the severity, costs and increasing frequency of cyber attacks, organizations need new solutions for hardening IT infrastructures and security defenses. They need a way to understand how they will be affected by new security threats and high-stress conditions. ASI provides global visibility into emerging threats and applications, along with insight into the resiliency of an organization's IT infrastructure under operationally relevant conditions and malicious attack. From an implementation standpoint, BreakingPoint's ASI model is uniquely architected to combine global application and threat intelligence with the world's fastest simulation and testing platform to battle-test, optimize and harden IT infrastructures.

Using ASI, organizations are better equipped to predict the impact of attack, to perform in the midst of configuration and network changes, and to avoid or minimize fines and a damaged brand image. In addition, they are better positioned to contend with the considerable consequences of DDoS attacks, data leakage and other attempts at compromising security.

By implementing a continuous security-testing regimen, organizations can constantly measure and improve the resiliency of their IT infrastructures. That means selecting the right infrastructure devices and information security investments, ensuring these devices are configured and deployed according to rigorous standards, and measuring the resiliency of every aspect of the IT infrastructure to the latest attacks and changing network conditions — all without requiring an investment in a traditional test lab.

Using ASI to Continuously Maintain Infrastructure Resiliency

Using BreakingPoint ASI, CISOs transform security processes to continually validate and certify the resiliency of every element of their infrastructure over time. This provides an ongoing understanding of the efficacy and performance of existing defenses and their network and data center infrastructures as a whole, even in the face of change. Sophisticated "what if" testing in a risk-free yet entirely real-world environment can now be applied to predict the impact of the most current attacks and harden resiliency before those attacks are launched.

Equipped with this level of actionable insight, IT staff immediately understand the potential impact of an event and take steps to harden systems and troubleshoot problems faster than ever before. By instituting this systematic, rigorous process, companies identify critical risks — from unpatched vulnerabilities to uncontested gaps in security coverage — based on the unique composition of their networks, operating conditions, security processes and regulatory mandates.

As the industry's first complete ASI solution, BreakingPoint products and services enable organizations to continuously assess their network and data center infrastructure exposure by combining advanced Internet-scale application simulation with real-world security testing features. These are some of the reasons why the leading network infrastructure providers, Global 2000 enterprises, government defense and intelligence agencies, and other security-conscious organizations are using ASI as part of their IT resiliency best practices.

Ideally, to maintain security posture, a closed loop is needed among the discovery of new threats and applications, sophisticated test-bed simulation, security testing, analysis, and certified remediation. Historically, this has required specialized test labs with racks of disparate testing tools and dedicated and highly trained staff to manage the process and interpret results. For most organizations, this recommendation simply has been cost-prohibitive.

BreakingPoint enables IT staff to automate previously manual activities enterprise-wide, such as security testing to confirm full remediation of critical vulnerabilities. This is accomplished using documented, repeatable and scalable processes, all without adding expensive and scarce expertise or deploying an army of consultants.

BreakingPoint delivers "packaged" global threat intelligence and research on the current threat landscape that relieves organizations from having to spend weeks or months setting up tests to evaluate the severity of new attack schemes emerging in the wild. With BreakingPoint ASI, all organizations can rely on BreakingPoint for the specialized skills, contacts, experience and insight of elite security organizations. Armed with the BreakingPoint portfolio of exploits and attacks, application profiles, and massively scalable simulation and testing products, IT staff can focus their security efforts on hardening the resiliency of specific areas of the IT infrastructure determined to be most vulnerable.

With rigorous and continuous resiliency testing, IT staff now make informed choices about security with an accurate understanding of their IT risk posture, as well as:

- Transition from reactive to predictive/preemptive damage control from attacks
- Implement proactive and rigorous security assessment and remediation
- Bridge the gap between preproduction test labs, the live network and monitoring tools
- Optimize security budgets and operational efficiency
- Support procedures that streamline compliance
- Develop and hone IT staff skills

I. Baselining and Maintaining IT Resiliency and Security

You can't manage what you can't measure. That's why capturing a baseline is an essential first step in a well-run, continuous resiliency testing program. This means systematically evaluating the key elements of an IT infrastructure as well as those systems as a whole. It also means evaluating those elements in the context of real-world conditions throughout the selection, configuration, deployment and change-management life cycle to assess performance and security before and after change. It is critical to bridging the divide between preproduction test labs and production networks. This is provided through an agile and easy-to-use testing platform that is continuously updated by the BreakingPoint Application and Threat Intelligence (ATI) subscription service, which delivers the very latest attacks and applications. As a result, measurable improvements in areas such as troubleshooting, IT operations and performance engineering are achieved continually. Equally important, cost avoidance in areas such as compliance, liabilities, and brand and intellectual property protection will be realized.

Over time, tests must be revamped and adjusted to accommodate changes in the threat landscape, network traffic or IT infrastructure. With extensive automation and based on continuous research into the latest applications and attacks, BreakingPoint products make it easy to adjust test conditions to reflect current conditions. By outsourcing security research to BreakingPoint experts who have exclusive insight collected via network equipment vendor relationships, proprietary research and global service provider feeds, organizations can scale their security assessment and certification processes to cover the entire enterprise infrastructure with a continuous security assessment program.

II. Selecting and Deploying the Right Devices and Systems

It's a given that organizations need a layered security strategy to protect critical assets from sophisticated criminals, malicious insiders and even nation-state-sponsored hackers. Firewalls and intrusion-detection and -prevention systems are absolutes. Increasingly, security-conscious organizations are also focusing on data leak protection, DDoS mitigation systems, intelligent switches to prevent ARP spoofing and MAC flooding attacks, web application firewalls, DNS sinkholes, and more in response to the complexity of the constantly evolving security threatscape.

Given the deployment of additional layers of security, ASI is vital for system selection, capacity planning and configuration control purposes to mitigate the risks of deploying and managing every element within the IT infrastructure. ASI's role in this capacity helps maintain infrastructure resiliency and save money.

While it's easy to justify new infrastructure investments on the basis of vendor benchmark claims, it's much harder to determine if the vendors actually deliver on their promises. Regrettably, security vendor marketing claims are often exaggerated and frequently do not reflect performance results based on real-world or enterprise-specific conditions. The consequences of selecting the wrong network security product based on these claims can expose an enterprise to serious threats from inside and outside the network perimeter, which may remain undetected for long periods.

Untested network security devices can give the mistaken impression that an enterprise is fully protected against all current threats and leave critical servers and other key network assets dangerously exposed. This can seriously inhibit business or operational requirements. Network security device testing should not be limited to the purchasing cycle alone — it's imperative to make testing an integral part of the ongoing security maintenance regimen by implementing a solid, continuous testing initiative.

There are compelling reasons for doing so. Gartner Group has reported instances of a single poorly written signature crippling the performance of an IPS. And firmware updates can break previously stable inspection processes (anti-evasion techniques appear to be particularly successful in causing disruption between firmware updates). Once tool selection and initial deployment are complete, a full benchmark test should be performed to establish a baseline. Every time a new firmware upgrade, signature pack update or change in security policy is applied — however minor it may be — all devices should be retested and the results compared against the established baseline. This process of continual monitoring makes it possible to quickly and easily identify and correct adverse impacts on performance or security effectiveness.

Making an accurate determination, however, requires Internet-scale simulation of the most current real-world attacks and granular application control to test whether devices are in fact blocking actual breaches now and in the future. This is another powerful aspect of ASI that helps reduce vendor finger-pointing and accelerate highly accurate troubleshooting. In addition, as security controls and infrastructures evolve, BreakingPoint ASI products are architected to simulate the latest conditions for fast and accurate testing to meet both security effectiveness and network performance requirements.

III. Validating Next-Generation Security Measures

Emerging security measures are evolving to protect organizations from new threats by insiders and external agents. These measures rely heavily on deep packet inspection and analysis to prevent costly data breaches and service outages.

Content-aware data leak prevention (DLP) systems are one such measure crucial to enterprise security. However, their deployment presents serious challenges. These systems are designed to detect sensitive content in text files such as email and instant messages, and in nontext files such as images, video and audio recordings. But testing and validating their effectiveness and compliance requires highly complex and stateful test conditions.

BreakingPoint ASI solutions tax any DLP device by simulating an organization's unique real-world application traffic, sensitive data and user behavior. With more than 160 of the world's most popular applications, including all major social networks, email and other protocols, combined with the ability to auto-generate unique and readable communications with unlimited Social Security numbers, credit card data and other sensitive data in a variety of languages, security staff can simulate virtually any type of scenario needed to validate these systems. Creating these "needle in a haystack" scenarios at real-world scale is the only way to validate whether a DLP solution will identify and protect sensitive personal, financial, technical, IP and other critical company data.

ASI solutions also measure the ability of next-generation firewalls, IPS devices, anti-DDoS appliances and other equipment to recognize and block malicious traffic. By combining authentic DoS and DDoS traffic with a real-world mix of application, exploits and malformed traffic, BreakingPoint provides critical insight into the effect of DDoS attacks on applications, individual devices, networks and data centers. As a result, organizations now measure and report on the impact of a range of current DDoS attacks on selected IT targets, including network security devices, wide-area networks and data center infrastructures.

BreakingPoint ASI solutions deliver comprehensive DoS and DDoS simulation and assessment for fast, accurate answers to questions such as:

- Will target systems support a minimum threshold of users when under attack?
- How will application response time and user experience change when under a DDoS attack?
- How will a DDoS attack affect network-based services?
- Will certain devices or configurations amplify the effect of a DDoS attack?
- How will remote services perform?
- Are DDoS mitigation measures effective?

With the ability to derive immediate answers to these critical questions, organizations leveraging BreakingPoint gain essential insight into how particular DDoS attacks will affect network-based services and application response times. ASI also provides an understanding of how DDoS attacks impact user experiences and ensures continued application performance even when a network is under assault. Security teams now determine the limits to which their infrastructure defenses can scale.

IV. Reducing the Cost of Compliance

More stringent legislative measures and industry regulations such as HIPAA, SOX, FISMA/NIST and PCI DSS place additional accountability pressure on organizations. The need to produce documented results of IT infrastructure security testing with repeatable and consistent auditing practices has never been greater. The costs and penalties associated with falling out of compliance are steep. Consequently, organizations bound by such regulations require stronger data security measures, faster detection of security breaches and mandatory disclosure of leaked or stolen data.

BreakingPoint ASI enables organizations to conduct faster and more accurate security assessments to confirm the effectiveness of required defenses such as DLP, firewalls, intrusion-prevention and -detection systems, and other defenses. Because BreakingPoint ASI solutions provide definitive measurements of the efficacy of IT infrastructure and security measures under real-world conditions, customers can easily demonstrate compliance. It is also possible to quickly identify potential violations well ahead of auditors, thereby significantly reducing the cost of compliance verification. These automated processes relieve security teams from tedious and oftentimes manual testing to expedite compliance verification on an ongoing basis.

V. Honing IT Security Skills

All too often, a lack of effective training and IT staff skills is at the root of many high-profile data compromises. Once attackers have access to even a single endpoint within a network, they can move silently and laterally within an organization to gain control of critical assets and data, often after lying dormant for days, weeks or months. The ability to uncover insidious attacks that are increasingly the result of APT variants is vital, yet the pool of cyber experts experienced in intermediate to advanced forensics is small.

This is due to the fact that the majority of companies are hard-pressed to find skilled security experts and lack the budgetary and war-gaming resources to train their IT and security staff. Creating the current, large-scale and highly dynamic conditions required to immerse security staff in a cyber-battle is typically a "once and done" proposition conducted at far-flung intervals. Going forward, organizations in the public and private sector will benefit from ensuring their IT staff receive appropriate training and gain the necessary experience that can be provided only through immersion in the very conditions they contend with every day. Until now, the question plaguing CISOs has been "How can we afford to implement the same cyber security training grounds used by the military?"

The answer again lies in the BreakingPoint ASI solution, which is used to simulate attacks in the context of an organization's precise network and data center conditions through the generation of traffic that mimics the actual behaviors of users, applications and devices operating on the company's network. The leading military and intelligence organizations call this a "cyber range," in which live simulated events help to train cyber warriors and enable security staff to see the effects of the simulation in real time.

BreakingPoint simulation capabilities scale exponentially, are upgradable via biweekly updates, cost a fraction of the price of a military cyber range and are set up in hours, as opposed to the weeks or months required for a traditional cyber range. These sophisticated and automated simulations help develop IT skills to ensure companies are more resilient to the early stages of attacks. By delivering global application and threat intelligence, advanced simulation and testing, and new security analytics into the hands of IT staff, critical-incident analysis skills are transferred cost-effectively to educate and transform IT generalists into cyber warriors.

Summary

BreakingPoint and ASI solutions enable organizations to ensure IT resiliency in the face of constant change. From collapsing troubleshooting from weeks to hours to deploying the best-fit devices for their unique infrastructure, organizations are depending on ASI to harden and maintain their security posture. Through the exclusive ability to create authentic application traffic, malicious attacks and user behavior, BreakingPoint ASI solutions deliver value throughout an organization's security ecosystem.

The ability to provide accurate cyber-war simulations not only transforms infrastructure, but it helps to develop IT staff into an army working toward proactively remediating threats and implementing more effective security controls, and doing it without the need for additional resources and person hours.

By automating the process of identifying exposures and potential threats in IT environments, BreakingPoint increases the speed, reach and consistency of an organization's full array of enterprise security processes. By providing measurable and actionable insight into the security, performance and stability of every element operating throughout an IT infrastructure, only BreakingPoint enables IT to get ahead and stay ahead of change.

Fortune 100 Bank Transforms Network Security Certification Process

The most security-conscious organizations in the world are implementing rigorous security certification processes using BreakingPoint ASI. One Fortune 100 bank has shared its best practices for transforming its network security processes while boosting the effectiveness of performance and security testing. Before certifying equipment and systems as production-ready, the bank's security team needed to understand the actual breaking point of each piece of equipment and of the network as a whole. To accomplish this, they relied on BreakingPoint to re-create Internet-scale network conditions to:

- Measure the resiliency of all IT elements prior to purchase, prior to deployment and following configuration changes
- Stress infrastructures to assess capacity and confirm appropriate IT investments
- Validate functionality and defenses under high-stress load and attack

The team sustains the resiliency of the bank's systems by validating performance, security and stability with the constantly updated BreakingPoint ATI program. ATI pushes to subscribers newly discovered attacks, malware and other intelligence aggregated from proprietary research, strategic customer relationships and carrier feeds.

BreakingPoint has automated what was a manual process of researching threats and testing elements of the bank's IT infrastructure. Through ASI, the bank now maintains deep visibility into its end-to-end IT infrastructure, validates company-wide risk assessment to maintain resiliency, models application and threat impact, and provides predictive insight through proactive security and performance testing.

Another critical benefit afforded by BreakingPoint products is the repeatable certification of network and security products throughout their life cycles. Not only do BreakingPoint products accurately emulate the bank's unique network conditions, they do so in a standardized and repeatable manner that enables comparative results across vendor products and updates.

Notes

Notes

BreakingPoint™

Find it before they do.™

Headquarters
3900 N Capital of Texas Highway | Austin, TX 78746 USA
Phone 512.821.6000 | Toll Free 866.352.6691
www.breakingpoint.com

Learn more about BreakingPoint products and services by contacting a representative in your area.
www.breakingpoint.com/company/contact/