WHITE PAPER

Stop the Cybersecurity Guessing Game

Continuous security validation ensures security infrastructure lives up to its promises and helps teams address the unmitigated risks created by today's threats

Table of Contents

Executive Summary

The great contradiction in cybersecurity today is that the more enterprises spend on their security and risk controls, the less sure they are that it will all work as advertised.

Year after year, organizations invest more and more into detection systems, response systems, event management systems, firewalls, secure web gateways, and more. According to Gartner, the cybersecurity industry will break another record in 2017 for spending—analysts predict organizations worldwide will shell out $90 billion.

Despite this increased spending, the cost of cybercrime continues to outpace investments in enterprise security and risk products; in 2016, cybercrime cost the worldwide economy $450 billion. Cybercrime is a dark industry, and it is making money hand over fist by probing for weaknesses in enterprise security infrastructure.

Meanwhile, new security vendors come out of the woodwork every day promising improved methods to fix old weaknesses and even more layers of protection to close gaps in new ones—all the while downplaying the added management overhead each new layer adds to risk management processes and architectures. As things stand today, the security market is awash with 1,500 or more vendors hawking their wares.

The Cybersecurity Guessing Game How Bad is It?

- Worldwide security spending will break $90B in 2017.
- Security spending keeps growing—it will increase by 26% in the next three years.[1]
- The average enterprise deploys and manages products from more than 54 security vendors.[2]
- Almost $3 of every $10 spent on security is wasted on shelfware.[3]
- 52% of security pros report they see no value-add from their deployed security products.[4]
- Only 30% of companies are rated as “experts” in cyber-readiness by a major insurer.[5]

THE BOTTOM LINE:

Enterprises are unsure of the effectiveness of their solutions once they're in place.

[1] “Gartner Says Detection and Response is Top Security Priority for Organizations in 2017.” Gartner. March 14, 2017. http://www.gartner.com/newsroom/id/3638017

[2] "Cisco: Overcrowded Security Market Needs More M&A.” Investor’s Business Daily. July 14, 2015. http://www.investors.com/news/technology/cisco-eyes-security-acquisitions-in-crowded-market/

[3] "Security on the Shelf: A New Report about Wasteful Spending.” Trustwave. Abby Ross. January 21, 2015. https://www.trustwave.com/Resources/Trustwave-Blog/Security-on-the-Shelf--A-New-Report-about-Wasteful-Spending/

[4] NSS Labs 2017 Enterprise Security Architecture Study

[5] “The Hiscox Cyber Readiness Report 2017.” Hiscox. https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html

Some vendors are selling innovative products that meet threats head-on and that can truly help organizations raise the bar for cybersecurity. For many other vendors, this is not the case.

The trouble is that differentiating between the innovators and the charlatans is hard, and understanding the subtleties of all the vendors in between is even harder. What's more, even the most effective solutions can be weakened by poor integration with the rest of an infrastructure, by inefficient configurations that spew out too many alerts and false positives, and by a lack of prioritized insight about the threats most relevant at any given minute. And attackers constantly work to neutralize effective solutions with new and more nefarious evasion techniques in the wild, so that yesterday's great solution is today's ineffective product.

The more layers of new security technology that are added, the harder it is to cut through the noise. CISOs and analysts on the ground struggle to answer basic questions such as:

- Which individual elements of our security risk ecosystem are working effectively, and which are not?
- Which threats to our enterprise systems remain unmitigated after passing through our security controls?
- Will we be throwing good money after bad if we pick up another shiny box promising protection against tomorrow's biggest threats?

The typical answer to these questions is, "Who knows?" Because as things stand, security is still largely a guessing game.

Too many organizations today govern risk management actions and investments by gut instinct and fear rather than by facts based on empirical evidence. That’s got to change.

Security Efficacy: A Moving Target

If there is one truth today in IT security and risk management, it's that what you don't know *can* hurt you.

The gaps in coverage between security products, the vulnerabilities created by ineffective configurations, the reduction of visibility caused by poor integration of tools, and endless new evasion techniques and exploits all leave behind residual risks. If unmitigated, these risks can lead to costly security incidents.

Unfortunately, not many of today's risk managers are equipped to quantify or track the residual risks within their organizations. One of the biggest challenges standing in the way of this kind of measurement is the dynamic nature of the risk factors. Things change day by day in three major areas:

Threats

Minute by minute, the crooks are coming up with new ways to circumvent existing security controls and are creating new exploits for common software flaws.

Security functionality

As new threats stream in, security vendors develop new methods to protect against them. Some are updates to existing products, while others are entirely new products or services that must be added to the mix.

Architectural composition and configuration

There are endless combinations of security controls, business applications, and configurations used by enterprises today. Each addition or change to the configuration of a technology stack impacts the risk equation.

With so many factors in the risk equation constantly fluctuating, it's daunting to find a repeatable method for continuously validating each unique environment's risk readiness at any given moment.

What IT Security & Risk Management Needs

So far, CISOs at major enterprises have gotten carte blanche to increase security spend in what one analyst at Piper Jaffray last year called "panic spending."[6] As boards of directors and CEOs heard the mounting horror stories of high-profile breaches, they were in a rush to green light any security initiative.

That spending is not going to last forever. Eventually, boards are going to demand a more scientific means of managing security portfolios and the risks they are built to minimize.

> At its most fundamental level, CAWS identifies critical gaps in security architectures and arms security teams with relevant information about the threats most likely to target their enterprise's systems.

If CISOs are going to deliver the discipline that the business requires out every other team, they've got to start looking for validation mechanisms that enable them to:

- Determine if their security architecture **provides the right protection**
- Ensure security configurations are **properly implemented**
- Make investment, operational, and personnel decisions **based on empirical evidence**
- Continuously assess vulnerabilities against active threats **to facilitate risk management**

Until now, there hasn't been an automated way to proactively ensure that a security architecture is truly effective against threats that are actively seeking to circumvent controls. But NSS Labs is changing the game with its CAWS Continuous Security Validation Platform.

At its most fundamental level, CAWS identifies critical gaps in security architectures and arms security teams with relevant information about the threats most likely to target their enterprise's systems. CAWS stands at the intersection of threat intelligence, security control assessment, and risk calculation to offer a complete and *relevant* view of unmitigated risks within an enterprise.

CAWS offers both macro-level visibility into strategic deficiencies that CISOs should address through further investments and reallocation of resources, as well as micro-level visibility

[6] "Cisco, IBM, Dell M&A Brawl May Whack Symantec, Palo Alto, Fortinet." Investor's Business Daily. February 8, 2016. http://www.investors.com/news/technology/cisco-ibm-dell-ma-brawl-whacks-symantec-palo-alto-fortinet/

into operational deficiencies that security analysts should address through configuration changes and system updates. This includes:

- Risk information to assess overall security posture
- Ability to monitor enterprise systems (i.e., applications and operating systems) and their impact against active threats
- Accurate metrics on the efficacy of security defenses
- Identification of security gaps by assessing the real-time status of the environment
- Ability to rationalize value from existing security investments and plan for future investments

How CAWS Delivers Continuous Validation

CAWS allows enterprises to make critical decisions based on real-time insights into the threats that impact their systems. The platform continuously assesses which systems are at risk by identifying active threats that are not mitigated by existing security controls.

The platform is powered by threats captured from NSS Labs' BaitNET™ live capture harness. This one-of-a-kind technology collects malicious URL and IP address information and uses it to run real exploits against virtual simulations of unique customer environments. Countless combinations of security controls and systems can be simulated to validate how threats operate within a given configuration and determine which risks remain unmitigated by that particular combination of controls. This information is then filtered according to which vulnerable applications and operating systems are deployed within a customer environment. Organizations can choose between public and private cloud offerings based on their requirements for granular control.

This is an evolution of threat intelligence capabilities, most of which provide a mountain of data without actionable insight into how to address the problems most relevant to an individual enterprise.

CAWS provides actionable information in the way of unmitigated threat specifics, which include threat sources, classification, number of days active, and chain of events. This provides a higher level of understanding and context for security teams to prioritize responses to current issues.

In the long term, it also provides strategic intelligence about how well the current architecture is performing against threats in real-time. This allows security organizations to make targeted purchases to fill specific gaps in architecture rather than buying based on fear, uncertainty and doubt.

The CAWS platform doesn't just help organizations meaningfully reduce risk, it also provides the reporting and structure necessary to adhere to the most rigorous governance standards, including those from the National Institute of Standards and Technology (NIST), Federal Financial Institutions Examination Council (FFIEC), and EU General Data Protection Regulation (GDPR).

What CAWS Allows You to Do

Clearly, there are too many security and risk management "solutions" in play and not enough problems actually being solved. CAWS helps security professionals at all levels gain the peace of mind they've been missing. The continuous assessment of security control efficacy and system vulnerabilities empowers each of these security stakeholders in different ways:

CISO

Unmitigated risk identification
Alignment to industry frameworks focused on continuous monitoring and validation

CSA

Technology evaluation and proof of concept for security controls
Risk posture identification through validation of security controls

Security Controls Team

Upgrade path and management for existing security controls
Effective patch management through evaluation of application and OS vulnerabilities

Threat Analyst

Identification of unmitigated risks impacting applications and OS in enterprise environment
Information to mitigate risk, namely indicators of attack (IoAs)

Why NSS is the Company to End the Guessing Game

NSS Labs has been the voice of the enterprise for more than a decade. Known best for our independent testing of security products, our mission has long been to arm enterprises with the objective, fact-based information they need to get secure and stay secure.

In the course of carrying out that mission, we increasingly heard from enterprises about their need for continuous feedback on the performance of their security controls and on the unmitigated risks affecting their systems. It's no longer enough to perform due diligence prior to purchase—boards of directors and executive management teams are demanding reassurance from their security teams that the controls they have in place are performing as they should be.

Our strong foundation of point-in-time security testing and expertise in enterprise research provide the basis for our CAWS Continuous Security Validation Platform, which validates the effectiveness of enterprise security controls and uncovers the unmitigated risks to enterprise systems.

Try CAWS free for 30 days by visiting www.nsslabs.com/cawstrial.

About NSS Labs

NSS Labs, Inc. is the global leader in operationalizing cybersecurity. Through continuous security validation and global threat discovery and automation, NSS Labs empowers enterprises to reduce the operational burden of cybersecurity and address crucial gaps in their cybersecurity efforts.

Informed by our experience and strong foundation of security product validation, NSS Labs offers CAWS, a cyber threat protection platform that provides businesses with visibility into the cyber kill chain and automated insights into active threats. With global visibility into active threats and vulnerabilities, CAWS delivers a unique cyber risk rating that makes cybersecurity measurable and helps enterprises focus their resources in the areas that make the most difference.

Combined, this information enables businesses to continuously monitor and respond to threats, strengthen their cybersecurity posture, and have confidence that they are appropriately securing the enterprise. CISOs, security operations teams, threat researchers, and information security professionals from many of the world's largest and most demanding enterprises rely on trusted insights from NSS Labs.

For more information, visit www.nsslabs.com.

NSS Labs
3711 South Mopac Expressway
Building 1, Suite 400
Austin, Texas 78746

+1 (844) NSS-LABS
www.nsslabs.com
advisor@nsslabs.com
@nsslabs