VIAVI Solutions

This Former Spirent Business is Now Part of VIAVI

Contact Us +1 844 GO VIAVI | (+1 844 468 4284)

To learn more about VIAVI, visit viavisolutions.com/en-us/spirent-acquisition

CASE STUDY

Ensuring Best Malware Detection Efficacy at a Major Financial Organization

Spirent™

CASE STUDY

Ensuring Best Malware Detection Efficacy at a Major Financial Organization

The Challenge

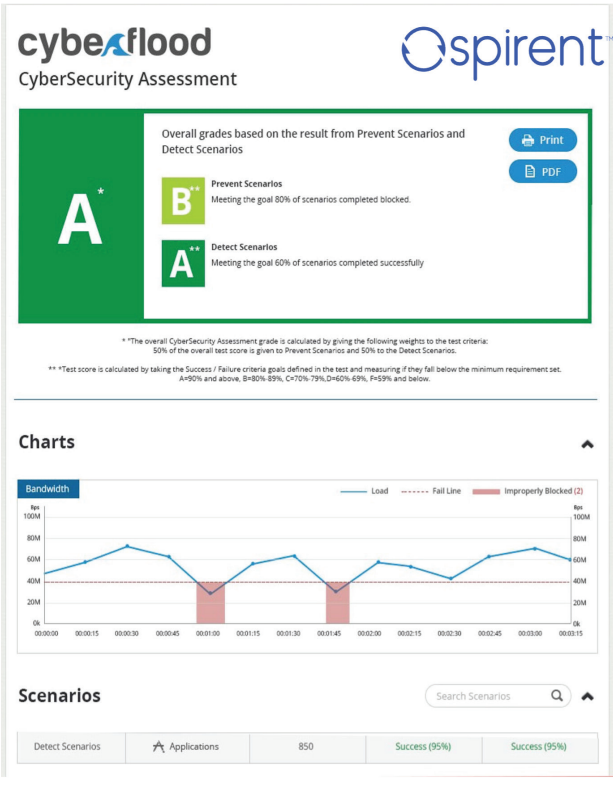
Deploying and managing next generation security solutions with anti-malware, deep packet inspection, and comprehensive security policies can be a daunting task. Customers are often stuck between the myriad of potential policies and configuration possibilities to determine how well they protect and perform. This situation presented some challenges:

Testing the catch rate of common, n-day and attack exploits:

To verify the catch, or block rate, of an in-line security solution, a validation test needs to have access to a database of thousands of n-day, current & legacy malware, attack signatures, as well as emulated application flows to provide accurate assessment results.

Assessing and validating security solutions under load:

In this use case the customer needed to ensure they could maintain 10Gbs of a specific mix of stateful user application traffic while honoring the security policies set in their security architecture. They also demanded low latency for common web applications servicing their end customers.



spirent

Customer Profile

A major financial organization had adopted new in-line security solutions that target malware and other specific traffic security policies for real-time protection of their network and application infrastructure from malware infection.

Internal and external customers of this organization demand high application availability while simultaneously ensuring that the systems and applications at this organization are protected with optimal security policies. Ultimately to maintain a delicate balance between high-performance, available, and robust security.

The Solution

This financial organization used Spirent's Professional Services to conduct specific assessments and tests with the results presented with high-level reports showcasing the fundamental malware and attack blocking capabilities of their security infrastructure. In addition, detailed analysis that could be utilized to help adjust policies to optimize both security efficacy and network performance were also presented by Spirent.

The Test Setup

The test utilized Spirent CyberFlood security and applications performance solution along with a C100-S3 multi 10Gbps testing appliance. The system was setup to have traffic and malware coming from the public facing interfaces of the security solution targeting an emulated application end point on the private side, which was also serviced by the C100-S3.

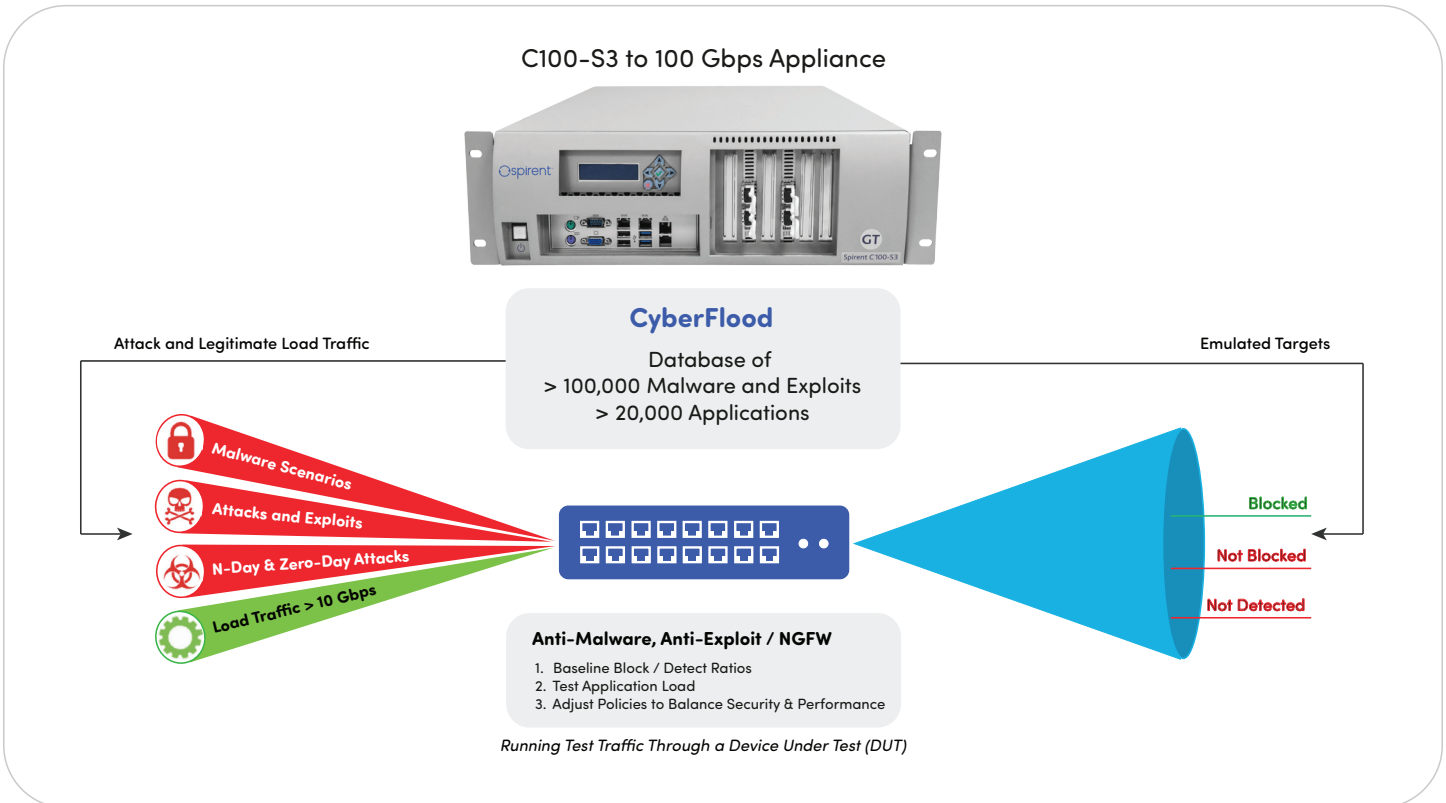
The Testing Process

We first conduced a test against the entire >100,000 malware and attack database through the 'inline security architecture' under test. This was done to verify which real threat samples were blocked, alerted but not blocked, and those that passed without detection. We then cross-referenced CyberFlood reports with those of the existing security solution logs to verify malware and attack vector coverage.

Baseline: Verify the catch rate of malware and attacks.

Rerun non-blocked: We re-ran all malware and attacks that were not blocked and adjusted network policies and signatures to ensure satisfactory block and alert ratios.

Inspection under load: We re-ran the same attacks through the security solution while running 10Gbs of industry specific application traffic. In order to verify security detection and analyze network performance, including application response latencies.



Running Test Traffic Through a Device Under Test (DUT)

The Results

This in-depth testing using real malware, attacks and application traffic showcases the true performance and security efficacy of the security solutions assessed. By adjusting security policies and ensuring the signature database on the security solutions were up-to-date, we improved the ratio of 'caught and alter events', while verifying the needed application performance this customer demanded.

Based on the initial negative traffic block ratios, we suggested to the customer that ongoing testing would be recommended to maintain system security and performance. As attacks and malware are continually changing, Spirent CyberFlood offers an up to date database of new signatures and threats for powerful validation methodologies.

Being able to comply with financial industry mandates and balancing performance with security was a key goal for this organization. The test results supplied by Spirent prove that this customer was able to achieve this balance.

Next Steps

Next generation firewalls with in-line malware and deep packet inspection policies continue to grow and evolve and have become more common in multipurpose infrastructure solutions, including migration to cloud based services. This growing complexity, including advanced cryptographic traffic and threat vectors, defines the need to ensure security and performance at the same time.

By employing advanced cybersecurity assessment validation is an effective means to verify you are deploying the right solutions, the right size and the right policies and ensuring they work in physical and cloud/virtual environments.

Contact us to learn more about cybersecurity assessment testing and how Spirent can help you get the most out of your security inventory.

Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com

Rev B | 12/23 | www.spirent.com