Unbelievable Tour Summary Report: Seeing Is Believing

Global Tour Pits Cylance® Against Three Biggest Names In AV

CYLANCE™

Introduction

They say, "Seeing is believing." Well, that's never been truer for those IT security professionals who attended a stop along the global Cylance Unbelievable Tour — a live malware download and cyberattack demonstration of CylancePROTECT® and the three largest antivirus (AV) vendors to illustrate the efficacy of signatures versus artificial intelligence. Cylance's ground-breaking, machine learning based approach to detecting and blocking cyberthreats is leading next-generation malware protection — without signatures, heuristics, network behavior analysis, or sandboxing. This new approach to cybersecurity has been featured on CBS's '60 Minutes' television program and has spawned numerous industry accolades, including the prestigious SC Media Award for Best Emerging Technology.

For those unfamiliar with Cylance, it's understandably difficult to believe an emerging Southern California startup can achieve superior threat-detection and prevention efficacy when put up against security industry giants such as McAfee (Intel Security), Symantec, and Trend Micro, but as you'll discover, the results show ingenuity and focus can defeat seemingly daunting odds.

The purpose of this white paper is to educate you about the testing environment, methodology, and results from Cylance's global Unbelievable Tour. First, let's quickly recap why legacy endpoint security defenses are failing and gain insight into why CylancePROTECT is succeeding where others have failed.

Why Are Current Security Solutions Failing?

Legacy signature-based endpoint security solutions are failing to protect enterprises from today's advanced threats. Cyber adversaries are sophisticated, well-funded, and highly motivated. Rather than re-using the same recycled threats to target servers of interest, they're developing custom-crafted or modified malware to deliver targeted threats to vulnerable endpoints and susceptible users. They're using those infected endpoints as beachheads for compromising systems and exfiltrating stolen data. By simply changing a few bytes of code using an off-the-shelf toolkit, these hand-crafted threats sail past traditional signature-based defenses as if they're not even there.

Legacy security offerings fall short of enterprises' expectations because:

- Anomaly-, behavior-, and heuristics-based offerings operate post-malware execution and often yield high false-positive/negative rates, rather than true pre-execution threat prevention
- Most are dependent on having an Internet connection to detect threats either with cloud resident signatures or post-attack behavior analysis
- So-called micro-virtualization and containerization offerings cause sluggish endpoint performance in CPU and memory, suffer from usability concerns, and support a subset of the operating systems and applications used by enterprises

On a related note, advancements in network-based sandboxing technology are helping organizations find many of the advanced threats plaguing enterprises, but threats do not typically originate from the network. Rather, the network is the 'fall-back' position for detection past the perimeter defenses. Most malware is transmitted over https or handcarried into the office on compromised endpoints — laptops, tablets and other mobile devices used outside the office walls and corporate protection. An increasing percentage of web traffic is encrypted. Network detection and prevention are seldom configured to inspect https/SSL traffic due to the overhead it causes, which leaves a big door open for threats hosted on secure sites. And, of course, network security products are not foolproof, as cybercriminals have found clever ways to evade them through a variety of techniques, such as suppressing a malware payload until a future date or until the user performs an action with his or her mouse.

It's evident security professionals are fed up with legacy endpoint security. In its recent Cyberthreat Defense Report, information security researcher CyberEdge Group surveyed more than 800 enterprise security professionals in North America and Europe about plans for evaluating new endpoint security products. Two-thirds of the respondents said they intended to evaluate new solutions to either augment or replace their existing endpoint security platforms. Simply put, generating new signatures and updating IP/URL blacklists every time a new threat is discovered is not scalable and doesn't help organizations targeted by custom threats and zero-day attacks. There is a better way. We, at Cylance, have found it.

Cylance: Next-Generation Endpoint Anti-Malware

Cylance's patented artificial intelligence and machine learning based platform is changing the way enterprises defend their endpoints against common and advanced threats. At its heart is a massively scalable, cloud-based data processing system capable of generating highly accurate mathematical models for data evaluation.

Cylance automates the mathematical model processing with machine learning to create artificial intelligence decisions to solve the extremely challenging security problem of determining which files are safe and which are a threat. It provides highly accurate results at exceptionally rapid rates.

To achieve this, the cloud platform first continuously collects vast amounts of data from every conceivable source. Then, it extracts DNA-level features that the machine learning platform itself has determined to be unique characteristics of good and bad files. Most of these are so microscopic that human malware researchers and reverse engineers themselves don't understand the value and importance of examining these code-level characteristics. This automates and amplifies the job of what a human threat researcher can do to discover if a file is a threat. Next, the platform constantly adjusts to the real-time threatscape and trains the machine learning system for higher-fidelity decisions. Finally, for each file, Cylance assigns a 'threat score' that is used to automate policy-based protection decisions — ignore, alert, block, or terminate file/process execution. The application of this artificial intelligence is manifested by extracting a powerful math model approximately every six months to become Cylance's flagship endpoint security product, CylancePROTECT, the local endpoint agent. The following are key elements of the solution:

Automated code 'DNA' analysis

Analyzes every file on your endpoints to find executable elements, then extracts the core DNA of those files to find malware using our patent-pending artificial intelligence engine.

Memory protection

Detects memory-based exploits that prevent privilege escalations in addition to system attacks, enabling protection from both direct and 'drive by' attacks.

Execution control

Provides policy-based, real-time controls to take a variety of response actions – ignore, alert, block, and terminate – when objects are classified as suspicious.

No signature updates

Operates 100% autonomously without a persistent Internet connection, classifying and taking action on threats using an entirely disconnected engine.

Non-disruptive, low-impact agent

The agent is small and typically uses less than 1% of CPU. It is easy to deploy with common software distribution tools.

Centralized management with contextual visibility

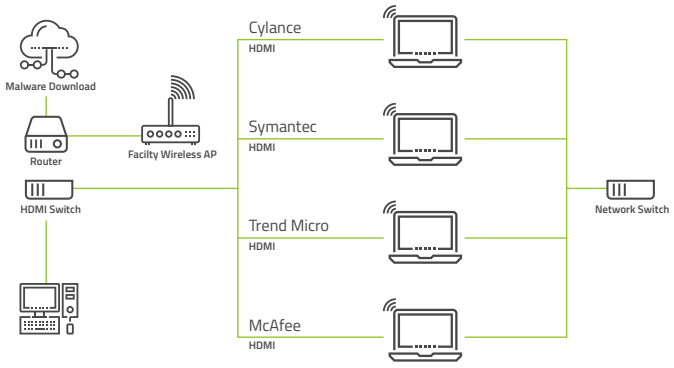
Our management console provides pre-execution insight and threat intelligence for dynamic analysis. MSI packages and open APIs enable easy deployment and integration into existing infrastructure management.

The Unbelievable Tour

Cylance conducted a road show in 75 cities across the globe called the Unbelievable Tour. The purpose of this tour was to demonstrate the power of CylancePROTECT by conducting a live cyberattack bake-off between Cylance and three of the most well-known legacy endpoint security products — McAfee, Symantec, and Trend Micro. The following three sections describe the test environment and methodology, as well as provide a summary of the test results.

Test Environment

The following diagram depicts the test environment that was used — four equally equipped laptops running Microsoft Windows 7 Pro and separate VMWare for each of the four endpoint security products involved in the bake-off: CylancePROTECT, McAfee, Symantec, and Trend Micro.



Test Methodology

The following five steps were performed by Cylance representatives in front of a live audience at each Unbelievable Tour stop:

Step 1: Download fresh virus samples. The Cylance representative downloaded 100 virus samples published on the date of the event. The query used requested malware that was smaller than 3 MB, had been submitted in the past 24 hours, was an .exe file, had been identified as 'bad' by more than 20 AV vendors, and did not include potentially unwanted programs, adware, or corrupted files. This sample was called "Original."

Step 2: Create mutated virus samples. The representative then used a generally available mutation packer tool and ran a command script on the server to create mutations of the 100 fresh virus samples and saved them into a separate folder on the server. This sample was called "Mutated."

Step 3: Prepare each endpoint. The representative verified to the audience that each laptop was clean. The representative checked for any available Windows patches and endpoint protection virus signature file updates to prove the competitive products were completely up-to-date. Each vendor was also confirmed to have every conceivable security detection and prevention turned on.

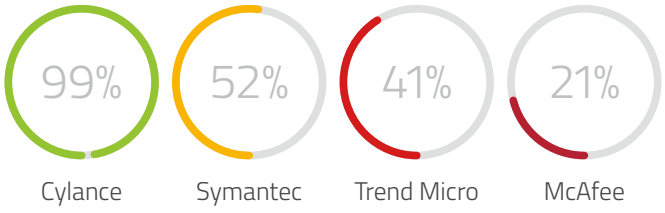
Step 4: Import "Original" and "Mutated" virus samples. The representative copied the 100 "Original" virus samples and 100 "Mutated" samples from the server onto each laptop. Task Manager was displayed so the audience could monitor and compare CPU and memory utilization of each laptop.

Step 5: Document results. Each of the laptops was inspected to determine the number of original and mutated viruses detected by each of the four endpoint security products. The number and percentage of viruses detected was documented on a poster for the audience to track.

Test Results

Recent results from the tests performed along the Unbelievable Tour can be found on Cylance's Unbelievable Tour web page. The chart below depicts the average test results achieved in the 75 cities we visited.

15,000 malware and mutated samples were tested around the globe. Over 2,100 people personally attended these



demonstrations and saw the unbiased testing approach and results with their own eyes.

Cylance significantly outperformed the three leading signature-based endpoint protection products. Cylance was able to detect and block more than 99% of all malware samples tested, including modified versions that vexed Symantec, Trend Micro, and McAfee. Symantec identified 52%, Trend Micro 41%, and McAfee just 21%. Cylance did not collect statistics related to CPU and memory utilization due to its variability, yet in many tests the competitive CPU and memory became overrun and corrupted by malware that executed on those machines, rendering them unusable. Unbelievable Tour audiences could see through each laptop's Task Manager utility that CylancePROTECT utilized a fraction of the computing resources needed by the three legacy endpoint protection platforms.

CylancePROTECT effortlessly blocked virtually every piece of malware, yet the laptops running the three legacy AV solutions struggled to keep running. In some cases machines became disabled as they were overwhelmed by malware that downloaded more malicious files, visited Chinese websites and showed pornography. CryptoLocker and its variants locked up the competitor machines every time it was part of the random sample during the Tour.

Conclusion

With over 100,000 new threat signatures published daily, mitigating targeted attacks with legacy signature-based defenses is an exercise in futility. Using technologies that permit malware to execute in order to detect and respond is an unnecessary approach. New threats require new thinking.

CylancePROTECT is the only endpoint threat prevention solution on the market that leverages the power of artificial intelligence and machine learning to detect known and customized malware plus zero-day threats — all without signatures and IP/URL blacklists.

Cylance products can be deployed as a secondary agent to detect and block threats missed by current endpoint security or as a replacement for the current product altogether. In either case, enterprises can rest assured Cylance never sleeps. CylancePROTECT is a highly-reliable last layer of defense against today's advanced threats and targeted attacks.

The Next Step Is Yours

Don't take our word for it. Sign up for the Cylance Test For Yourself framework, which provides a safe testing environment for malware protection products, by visiting www.cylance.com/tfy. You can examine CylancePROTECT using fresh malware samples in a safe but realistic scenario tailored to your environment. Or perform your own in-house testing by requesting an on-site evaluation of CylancePROTECT from a Cylance representative at +1-877-973-3336.

+1-877-973-3336
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

CYLANCE™

20170227-2629