Unbelievable Tour Summary Report

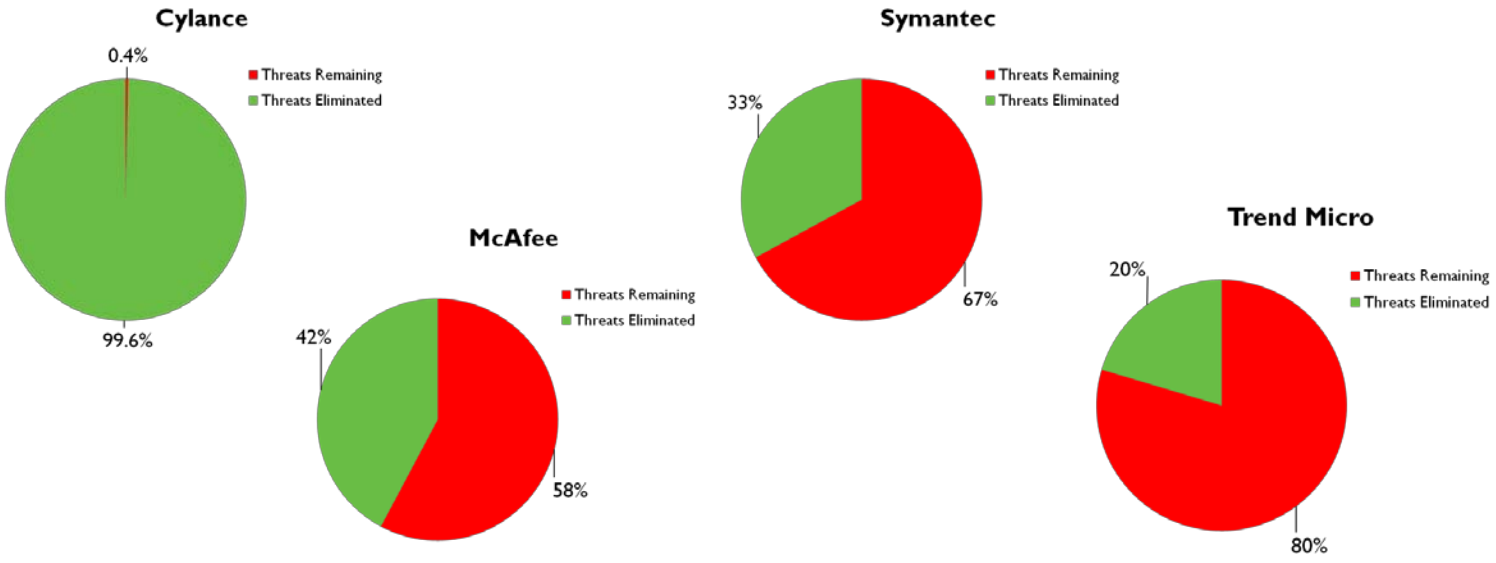
Threat Prevention is Possible | Insights from the Cylance Unbelievable Tour

The promise of threat prevention has been an increasingly elusive target for enterprises utilizing legacy antivirus (AV) and antimalware solutions. Zero-day exploits and polymorphic code have taken traditional threat protection to task, resulting in porous perimeters and costing industry leading brands hundreds of millions of dollars and senior level executives their jobs. The Unbelievable Tour, is not just a demonstration of the latest malware in live cyber-attacks versus legacy antimalware solutions and CylancePROTECT (an advanced artificial intelligence (AI) and machine learning endpoint protection solution), but also a demonstration that the promise of threat prevention is within reach. The Unbelievable Tour spanned 38 cities around the globe during the second half of 2015 and demonstrated that a new model of antimalware can restore confidence in the concept of threat prevention and reject the status quo that malware-facilitated data breaches are the norm.

Antimalware Performance Summary:

As the results of the Cylance Unbelievable Tour demonstrate, there was nothing static regarding the threat landscape in 2015. The growing sophistication and number of attacks, as well as the escalation of state sponsored attacks and availability of nation state malware variants, has quickly made legacy cyber defenses obsolete. Fortunately, CylancePROTECT's machine learning capability becomes more effective as the malware data set increases, resulting in 100% of threats eliminated in the final 16 events of the year and pushing Cylance's performance to near 100% effectiveness.

Total Threat Elimination Efficacy



The rapid and exponential rate of change in the threat landscape simply outpaces traditional defenses that are based on signatures, heuristics and network behavior analysis. In addition, polymorphic techniques are becoming more sophisticated and facilitate malware shape-shifting in order to escape detection. On more than one occasion during the tour, legacy anti-virus (AV) and antimalware solutions would thwart approximately 50% to 80% of malware one week, only to drop to less than 10% efficacy the following week. Cybercriminals are highly adept at identifying when their malware has been detected and then they make code modifications in order to obfuscate the malware from signature and hash matching methods utilized by traditional AV and antimalware solutions.

The Year of Ransomware

As The Unbelievable Tour progressed throughout the year, there was a significant increase in the number and frequency of cryptolocker variants, which brings credence to industry prognosticators that are predicting 2016 as the year of ransomware. Cryptolocker is a form of ransomware that encrypts a victim's files and holds them hostage while providing a short deadline to pay a ransom in exchange for a password to retrieve the files. Since the emergence of Cryptolocker, several other variants have spawned, including CryptoWall and CryptoBit that utilize alternative threat vectors to reach victims.

CylancePROTECT is particularly effective against ransomware because it identifies and eliminates the threat in advance of the malware executing.

Financially motivated attacks are a growing global phenomenon and the ease with which would-be hackers can enter the market, will likely accelerate this trend. Readily available tools and virus packages that are accessible on the black market have dramatically reduced the barrier to entry.

Emerging Threats with Increasing Sophistication

In addition, state sponsored malware is also on the rise with industrial control systems often being targeted. Once sophisticated malware is deployed by a nation state, it can become available to other parties that can alter the malware and utilize it for financially motivated attacks.

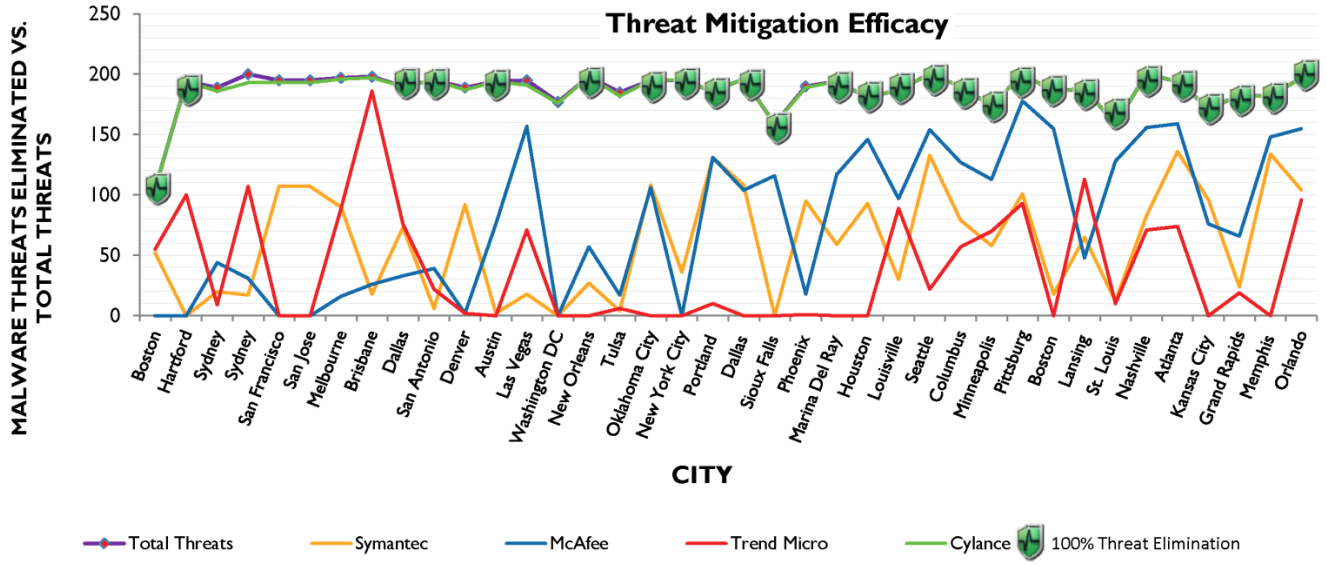
A Better Antimalware Solution

While the second half of The Unbelievable Tour was in full swing, cyber-attacks hit the hospitality industry particularly hard. Hyatt Hotels, Starwood Hotels and Resorts, Kalahari Resorts, Noble House Hotels and Resorts and Olympia Hotel Management, all experienced malware attacks resulting in data breaches. These attacks are evidence of the growing detection deficit of signature-based antimalware solutions.

Threat Prevention is Possible | Insights from the Cylance Unbelievable Tour

The growing malware detection deficit of traditional AV and antimalware solutions was the driving force behind the genesis of Cylance. Its innovative new method of threat detection, utilizing advanced AI and machine learning, has resulted in 99% of malware being detected and eliminated. In order to achieve this level of efficacy, CylancePROTECT analyzes and classifies hundreds of thousands of characteristics per file, breaking them down to an atomic level to discern whether an object is "good" or "bad," in real time.

The Unbelievable Tour Results by Market



Cylance is Simply a Better Solution

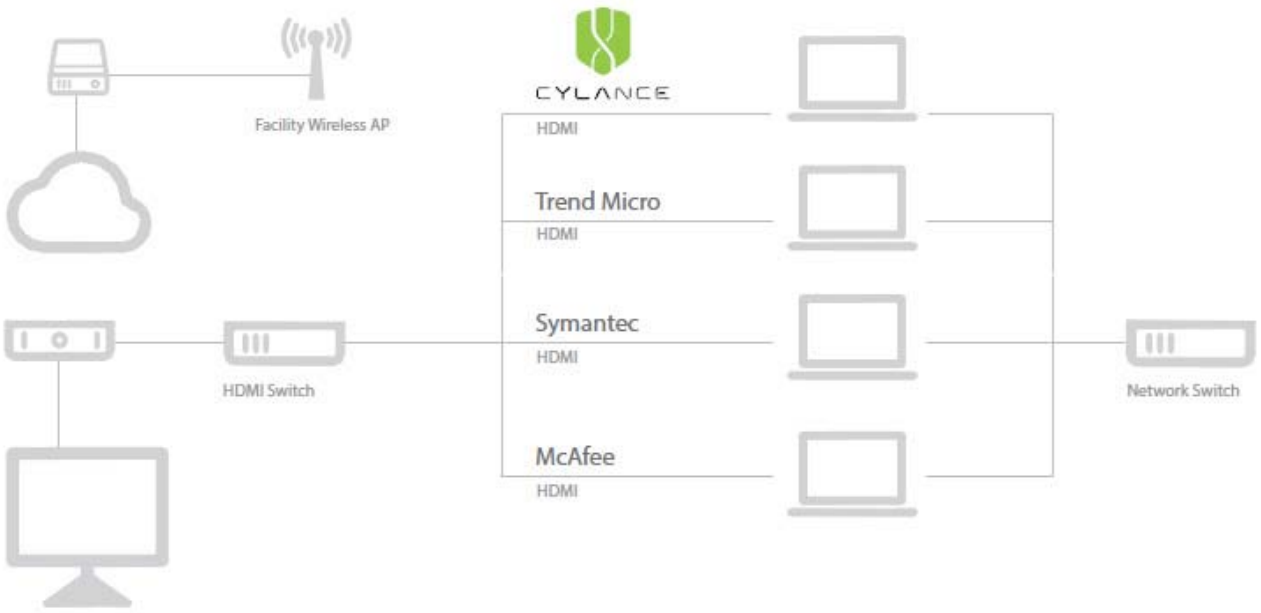
At its heart, is a massively scalable, cloud-based data processing system generating highly accurate mathematical models for data evaluation. Cylance automates the mathematical model processing with machine learning to create artificial intelligence decisions to solve the very difficult challenge of discerning which files are safe and which are threats. This new method of identifying and eliminating threats is highly accurate and delivers results in before the files can execute. The Cylance platform continuously captures code-level intelligence and utilized machine learning which improves the fidelity of the threat score in real-time. Cylance then applies the threat score to trigger policy-based protection decisions, including: ignore, alert, block or terminate file/process execution. CylancePROTECT operates 100% autonomously without a persistent Internet connection by classifying and taking action on threats using an entirely disconnected engine. The non-disruptive, low-impact agent is only 30 MB in size and typically uses less than 1% of CPU resources.

Threat Prevention is Possible | Insights from the Cylance Unbelievable Tour

Testing Methodology Overview:

The purpose of The Unbelievable Tour is to demonstrate the power of CylancePROTECT, and restore confidence in the concept of threat prevention. Cylance conducts a live cyber-attack and assesses the performance of CylancePROTECT as well as each of three legacy endpoint security products— McAfee, Symantec, and Trend Micro.

The following diagram depicts the test environment which was carefully designed to represent real-world scenarios. The test utilized an unbiased playing field in order for the four antimalware solutions to be tested accurately and fairly.



Each instance of the environment consisted of:

- Readily available, off-the-shelf hardware
- Four equally equipped laptops running Microsoft Windows 7 Pro
- Separate instances of VMware for each of the four endpoint security products involved in the bake-off: CylancePROTECT, McAfee, Symantec, and Trend Micro
- The latest downloaded version of each endpoint security product
- Wireless Internet access provided by the facility
- An HDMI switch so each screen can be displayed on a projector
- A server (not depicted in diagram) is also present to store original and mutated viruses used in the test

Testing Methodology:

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

Step 1: Download fresh virus samples. The Cylance representative connects to the Virus Total website (Google owned, 3rd party public malware repository) from a server console and downloads 100 virus samples published on the date of the event. The query used requests malware that is < 3mb, submitted to a third party virus repository in the past 24 hours, is a EXE, has been identified as 'bad' by more than 20 Anti-virus vendors, and does not include PUPs , Adware or corrupted files. This is Sample One called "Original."

Step 2: Create mutated virus samples. The representative then uses a generally available mutation packer tool and runs a command script on the server to create mutations of the 100 fresh virus samples and saves them into a separate folder on the server. This is Sample Two called "Mutated."

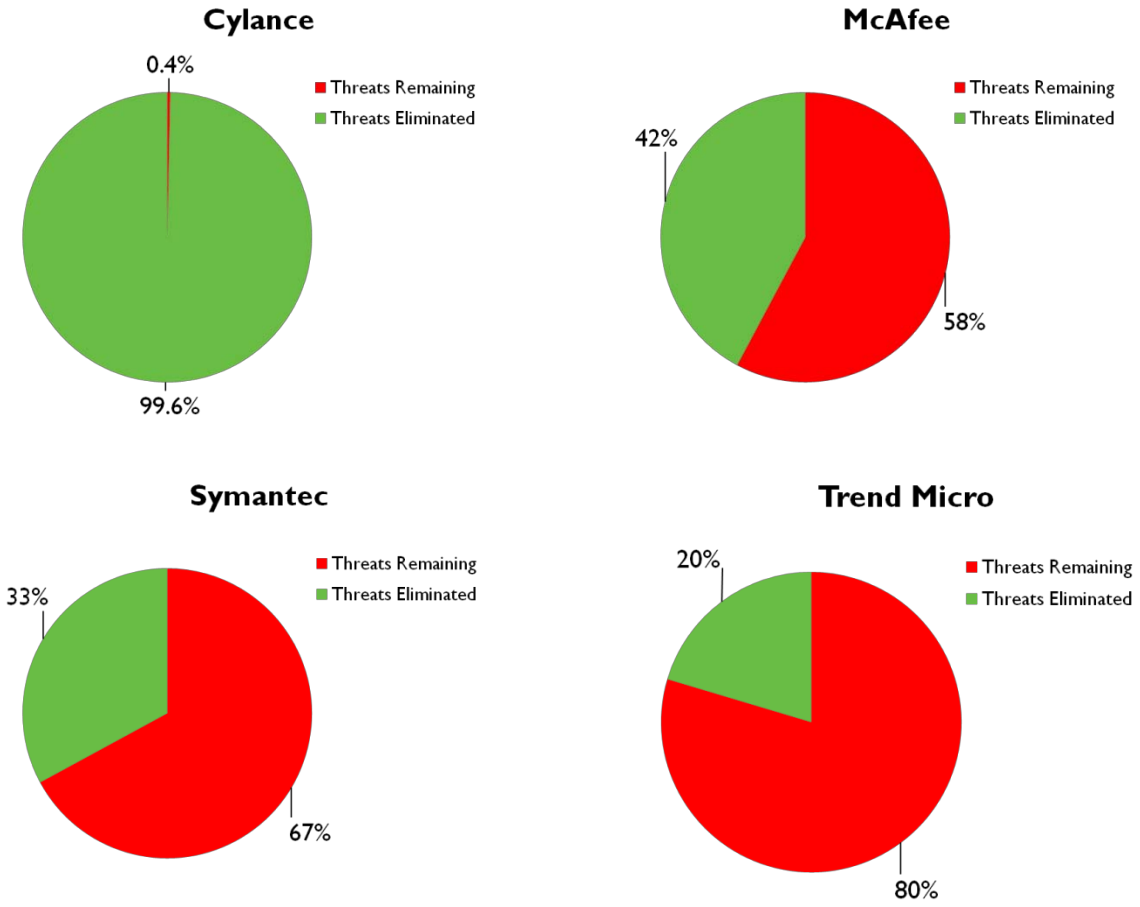
Step 3: Prepare each endpoint. The representative verifies to the audience that each laptop is working off a clean computer. The representative checks for any available Windows patches and endpoint protection virus signature file updates to prove the competitive products are completely up to date. Each vendor is also confirmed to have every conceivable security detection and prevention turned on.

Step 4: Import original and mutated virus samples. The representative copies the 100 original virus samples and 100 mutated samples from the server onto each laptop. Task Manager is displayed so the audience can monitor and compare CPU and memory utilization of each laptop.

Step 5: Document results. Each of the laptops is 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 is documented on a poster for the audience to track. This is also recorded on the Cylance web site: www.cylance.com.

Test Results

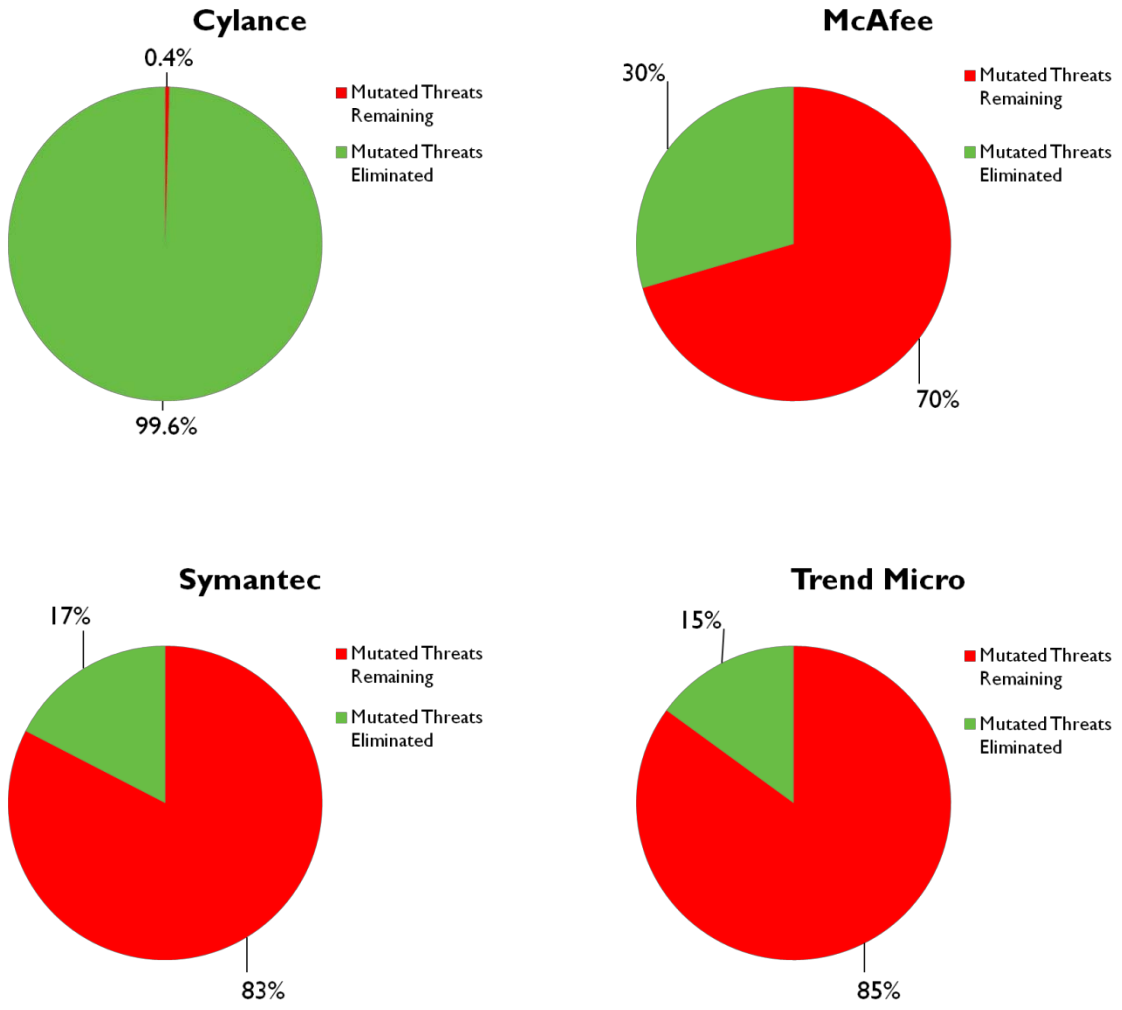
Over 10,000 malware and mutated samples were tested across 38 cities around the globe. The following results demonstrate the benefits of utilizing Cylance's new model of threat detection and elimination.



CylancePROTECT consistently outperformed the other endpoint protection solutions and achieved a near perfect performance by eliminating 99.6% of all threats.

Mutated Threat Elimination Efficacy

Metamorphic and polymorphic malware are malicious applications that mutate in order to evade detection. The speed of malware mutation is accelerating and therefore, the signature-based endpoint protection model is challenged to keep up and is often obsolete as soon as signature updates are deployed. During each test event a Cylance engineer utilizes a commonly available toolkit to create mutated variants of the downloaded malware. Here are the results of the threat elimination efficacy of the four antimalware solutions tested:



Mutated threats are particularly challenging for traditional antimalware solutions to identify and eliminate. CylancePROTECT was the only solution to sustain the same level of malware threat elimination across all types of malware.

Conclusion

In order to achieve a cyber-hardened enterprise threat profile and realize the promise of threat prevention, it requires a new approach to endpoint protection. Trends like bring-your-own-device (BYOD) and growth in metamorphic and polymorphic malware have facilitated the proliferation of compromised endpoints. Solutions based on signatures, heuristics and network traffic analysis simply fail to keep up with the dynamic nature of today's attacks.

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 a failure-based strategy that accepts succumbing to malware's presence in your enterprise.

Combating rapid threat evolution requires a new prevention paradigm. CylancePROTECT is the only endpoint threat prevention solution that leverages the power of algorithmic science and artificial intelligence to detect known and customized malware. Zero-day threats, polymorphic and next generation malware are eliminated without signatures and IP/URL blacklists. CylancePROTECT can be deployed as a secondary agent to detect and block threats missed by your current endpoint security or as a replacement for your current product altogether. Regardless of your preferred deployment strategy, you can rest assured that Cylance will help you realize the true promise of threat prevention.