The New World of Endpoint Security: Traditional Signature-Based Malware and Virus Protection Can't Keep Up

CONTENTS

"Traditional anti-virus vendors are still using methodologies created 20 years ago. Our tools need to evolve with the times because, like it or not, the problem has evolved well beyond the capacity of those original methodologies."

—Josh King,
Technical Director, Security,
Carousel Industries

Overview: The King is Dead. Long Live the King.

Substitute "antivirus protection" for "the king," and you've pretty much described the current state of endpoint security. For all the marketing claims made by AV and malware protection vendors like Kaspersky, Symantec, MacAfee, and others data breaches occur often and account for the loss of millions of records every year. According to digital security company Gemalto, nearly six billion—yes, billion—data records have been lost or stolen since 2013. There were over 700 million records breached in 2015 alone. And it looks like once the numbers are in, 2016 will have been a banner year for data breaches. In the first half of 2016, there were more than 550 million records breached.

Many of these records contain personal information: credit card and social security numbers, account passwords, and medical data. Some also contain highly classified government data. Certainly, all the blame for this can't be laid at the feet of the AV industry. In 2015, only four percent of the data records breached in 2015 involved data that was fully or partially encrypted. But most companies and government agencies rely on AV and malware protection as one line of defense against data breaches. And their much-hyped success rates of virus and malware detection—in the high 90 percent range—don't stand up to scrutiny.

Why Traditional Malware Protection Doesn't and Can't Work

Ninety percent of all cyber security incidents occur through file-based malware. In 2015, the Symantec Internet Security Threat Report, noted there were 430 million new pieces of unique malware. New zero day vulnerabilities numbered 54—or about one a week.

The dat file that Symantec maintains to detect malware contains less than 10 million signatures. Ten million against 430 million. The math just doesn't add up. There's a huge disparity between how fast new malware is introduced and how quickly AV vendors can update their dat files.

In 2015, there were 430 million new pieces of unique malware.

Symantec Internet Security Threat Report

As Josh King, Director of Security Solutions forCarousel Industries puts it, "Traditional anti-virus vendors are still using methodologies created 20 years ago. Our tools need to evolve with the times because, like it or not, the problem has evolved well beyond the capacity of those original methodologies."

Likewise, Carousel's Security Solutions Architect Tim Ramsey explains, "Even if traditional AV could catch upwards of 98 percent, what about the 2 percent? What about malware that is mutated or unique to your organization? Signature-based technology can only protect against threats it has seen before." It's worth noting that two percent of 430 million is 8.6 million. That's a lot of undetected malware.

Another issue with the signature approach to detecting malware is performance. The bigger the dat file the more of a performance hit users experience when their AV software runs a scan. Organizations very often switch AV vendors for that reason: users complaining about slow performance. But among the 50 or so AV vendors, there's not much difference. You need a big dat file to catch more malware, and a big dat file eventually degrades performance.

Using Math to Catch Malware

Of course, there are technologies companies can use to augment their AV software, and some of these technologies can be added to their traditional AV suite as modules. Endpoint detection and response (EDR), isolation, sandboxing (cloud based and on premise), exploit protection, application control (also known as white listing), and behavior-based monitoring can all contribute to protecting the endpoint and by extension the organization. Nevertheless, adding all these modules would substantially degrade the performance of the endpoint.

A new approach to detecting malware based on machine learning holds the potential to finally shift the balance of power between "threat actors" and their targets. Wikipedia explains machine learning as follows:

> *Machine learning is the subfield of computer science that "gives computers the ability to learn without being explicitly programmed" (Arthur Samuel, 1959). Evolved from the study of pattern recognition and computational learning theory in artificial intelligence, machine learning explores the study and construction of algorithms that can learn from and make predictions on data…*

From this definition, it's easy to see how malware detection based on machine learning might differ from the signature-based approach.

With machine learning, after extracting and analyzing the attributes or features from millions of good and malicious files, computers can employ statistical models to identify and classify unknown files with a high degree of accuracy—all in milliseconds.

The benefits of using machine learning instead of signatures to detect malware include:

- High effectiveness—The catch rate of current solutions using machine learning hovers around the upper end of 99 percent.

- Off net coverage—Since there's no dat file to continuously update, AV protection based on machine learning does not depend on a constant online connection.
- Minimal performance impact—There's no dat file to reference against every file on a computer during a scan.
- Pre-execution protection—Traditional AV sometimes requires file execution to determine whether a file is malicious. Stopping malware before execution is more secure and requires fewer endpoint resources to stop infection.
- Greater OS support—Although endpoint security vendors may continue to write signatures for legacy systems, the absence of steady patches from software vendors limits the availability of signatures for those platforms. But, unshackled by signatures, machine learning solutions can identify malware in Windows XP as easily as in Windows 10.

More than 500 vendors compete in the security space today, many focused strictly on the endpoint. Of those, at least half offer only traditional, signature-based malware protection.

Navigating the Endpoint Security Marketplace

More than 500 vendors compete in the security space today, many focused strictly on the endpoint. Of those, at least half offer only traditional, signature-based malware protection. So, it can be a challenge to decipher which technologies offer the most complete and cost-effective protection.

The team at Carousel constantly researches and evaluates what vendors, or mix of vendors, offer the most security value for your business. If your organization has an open endpoint security project or needs some general guidance about the endpoint security marketplace, please visit carouselindustries.com.

About Carousel Industries

Carousel Industries is a recognized leader in helping organizations evolve the way they communicate and orchestrate the flow of information throughout their networks. Carousel enables clients to connect and collaborate the way modern IT users demand and advance from their current network infrastructure to meet tomorrow's standards. With deep expertise across a vast portfolio of communication, network, and security technologies, Carousel is able to design, implement, and support solutions tailored to meet the unique needs of each customer. By offering professional and managed services with flexible deployments in the cloud, Carousel ensures clients achieve agility and utilize technologies in the way most effective for their business.

Founded in 1992, Carousel serves more than 6,000 customers, including 35 of the Fortune 100. Carousel has been recognized by multiple publications and industry consortiums as a top technology integrator and managed services and cloud solutions provider–including the Inc. 500/5000, Healthcare Informatics 100, and CRN MSP Elite 150. Headquartered in Exeter, RI, Carousel has more than 1,400 employees based in 27 offices–with three Network Operating Centers nationwide.