Better Security. Fewer Resources.

Cylance Bolsters Endpoint Protection Without PC Performance Impact or Incremental Costs

CYLANCE™

Introduction

When you consider the number of headlines that appear on a regular basis about major data breaches — despite ongoing increases in security technology spending by organizations — you have to come to the conclusion that something isn't working.

The fact is, the traditional ways of protecting IT assets are no longer effective in today's increasingly complex threat environment. Many vendors tout the idea that having a collection of disparate technologies will provide better protection because each technology will stop some threats. But these products don't scale and they provide ever-weakening protection. Even using several of these traditional products is not sufficient for identifying and stopping the latest malware attacks.

Part of the problem with deploying more and more security technologies is that it costs far more money in resources and infrastructure, including servers, bandwidth, appliances, etc. Furthermore, many of these products negatively impact system and application performance, which can lead to decreased productivity among end-users and the organization as a whole. Older security tools can cost organizations far more time and money than they ever realized.

It's time for a new approach to security that addresses all the shortcomings of the old methods. Organizations today can deploy security solutions that are based on newer artificial intelligence and machine learning capabilities. These advanced methods are designed to stop the latest attacks without hurting performance and driving up costs. This white paper describes some of the main disadvantages of traditional endpoint security methods and explores how organizations of all sizes and in any industry can take advantage of advances in security technologies to protect their systems and data against threats in the most cost-effective way possible.

Traditional Security Hurts Performance, Drives Up Costs

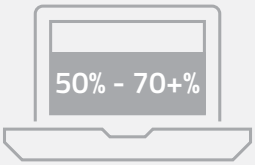
Among the biggest drawbacks of traditional security solutions is that they are a drain on performance as well as a source of added costs.

With traditional security tools, companies need to maintain huge databases of signatures of known malware or approved applications. They also must constantly deploy additional hardware and software, with minimal if any integration; download new file signatures in order to keep signatures databases current; and conduct daily scans and real-time scans of memory, emails, etc.

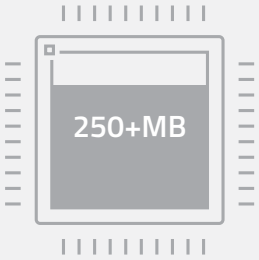
All of this takes up a lot of CPU cycles and degrades client device usage. On average, traditional endpoint security products use 50% to over 70% of CPU cycles during intensive scans.

Traditional Endpoint Security

CPU Utilization



Memory



TES – CPU Utilization: 50 -70+%; Memory: 250+MB

Next-Gen Endpoint Security (Cylance)

CPU Utilization

Memory

NGES (Cylance) – CPU Utilization: 1-3%; Memory: 40MB

Highly light weight and low impact

This leads to constant complaints among end-users at many organizations, who want to know why their systems are so slow or why it takes 15 minutes to boot up every workday morning. Furthermore, this also increases costs and reduces productivity, because users are making more calls to the helpdesk when problems arise.

The negative impact on performance goes directly against what so many enterprises strive to achieve today: enhanced systems and application performance that enables workers to complete tasks more quickly and efficiently. If systems are slow, so is the response to customer needs, or the development of a new product or service, or the launch of a marketing campaign.

The impact on the bottom line and on business operations can be dramatic. Clearly, security solutions need to be effective at stopping attacks, but not at the cost of diminishing performance to the point where employees and customers become disenchanted.

Recent industry research shows just how much of an impact security technology can have on user experience. For example, an online survey of 460 IT professionals and 301 business users in the U.S., U.K., and Germany, conducted in 2015 by Dimensional Research and commissioned by Dell, showed that 91% of business respondents said conventional security measures put in place by their employer negatively impact their productivity. A huge majority of the business respondents (92%) said they are negatively impacted when required to use additional security for remote work. When examining changes made to corporate security policies in the previous 18 months, more than half of the business respondents said security's negative impact on day-to-day work had increased.

The negative impact on performance and user experience can have other severe consequences for organizations. For instance, nearly 70% of IT professionals surveyed by Dimension Research said employee workarounds to avoid IT-imposed security measures pose the greatest risk to the organization. What makes the performance issue especially daunting for many organizations is that decision makers often do not consider the impact on systems and resources when they are evaluating security products.

In addition to the performance issues, another problem with signature-based security products is the added cost involved — both in terms of the greater expenditures in time and money when using these products, as well as the costs of security breaches that can result from inadequate security.

For example, because signature-based products are ineffective against malware, organizations often opt to deploy additional costly security technology, including endpoint detection and response solutions. Instead of focusing on stopping malware before it can execute on systems, these solutions hunt for indicators of compromise left behind by a piece of executed malware, and they require highly-skilled and highly-paid staffers to operate.

In many cases, this is done after malware has already propagated from system to system within the organization — at potentially great cost. In addition, solutions that collect and store most of the system events for detection and response might end up collecting more information than is necessary, leading to added resource costs.

From a time and cost standpoint, deep scans conducted on endpoints by signature-based anti-malware software mean work delays for users and a corresponding drop in productivity. When you consider 10-minute scans twice a day times the number of users on a network, that can quickly add up to big numbers that have a financial impact on the business.

Additional costs result from allowing more malware into the organization. These include malware issue resolution, machine re-imaging, declines in end-user productivity, extra IT security skills needed, and legal costs (if damage occurrs from an attack).

Signature-based products also require maintenance, primarily the distribution of the signatures. These generally take place daily but can be as frequent as hourly. Systems that are air-gapped require increased maintenance because they can't retrieve updates from the product vendor's Internet presence. Administrators may need to manually retrieve each update, place it onto removable media, check the media itself for malware, and physically transfer that media to a system on the air-gapped network for further distribution.

Traditional endpoint security vendors are forcing customers to deploy more and more layers of technology on the endpoint to try to improve protection efficacy. This additional technology, such as host intrusion prevention systems and reputation-based file lookups, requires additional installs, hardware, and management overhead. In many cases, users might see four to six different endpoint security processes being used within the organization.

Failure to Protect

Not only do signature-based security products impact performance and drive up costs, they also fail at their most important mission: to protect organizations against malicious content. None of the traditional endpoint security vendors can prevent malware from executing. By definition, signature-based antivirus always has a patient zero, as the malware must be discovered before the signature can be written. Many new evolved threats are zero-day attacks that use various techniques that must also be prevented from executing.

This is one of the disadvantages of post-execution monitoring. More often than not, a series of behaviors constitutes a malicious behavior. However, it might be too late to block the malware if that determination is not made in time and, more importantly, every time. Some solutions take minutes or even days and weeks to make such determinations.

A major drawback of using signature-based security methods is that organizations can wait up to 72 hours for a signature file to be created, depending on the level of risk. There are a number of steps that have to occur to develop a signature file. The more time that passes before protection, the more endpoints that get infected, which costs more money.

Ponemon Institute in its 2016 Cost of Data Breach Study noted that the average total cost of a data breach for the 383 companies participating in its research was $4 million. The average cost paid for each lost or stolen record containing sensitive and confidential information was $158.

Finally, there are indirect costs that result from attacks that get past signature-based tools. This includes the damage to brand reputation, the unknown cost of corporate information or state secrets lost or stolen, etc.

Security threats have evolved to become much more sophisticated over the years, and they can easily be mutated to take on new and unrecognizable forms. Today, nearly all malware is polymorphic, meaning it's highly customized and targeted. Traditional malware analysis techniques, such as file signatures, heuristics, or reputation cross-checking, are easily defeated by mutated malware. Also, because malware checks its environment for the use of dynamic analysis techniques such as sandboxing, these techniques are easily defeated.

Even though the cybersecurity landscape is characterized by constant change, the basic components of malware detection have stayed the same for more than three decades.

Decades-old signature-based antivirus technology is not effective against today's tidal waves of sophisticated attacks with countless variants of malware. For example, attackers can easily and effectively disguise (mutate) malware using ubiquitous packer software. This software modifies the malware attributes and changes the cryptographic hashes, allowing easy penetration past signature-based antivirus, just as easy as changing the license plate of a stolen car. In fact, analyses show that 99% of malware hashes are seen for only 58 seconds or less, and most malware was seen only once, reflecting how quickly hackers are modifying their code to avoid detection.

With the array of successful attacks making headlines in recent years, it's clear that the traditional approaches do not seem to be working. And it's not likely that the situation will get better for traditional security methods. These products will not improve because they still use reactive technology; they rely on a decades-old code base for reactive protection that increases the likelihood of damage from attacks; and they require customers to purchase and cobble together several technologies that cause an increase in operational and dedicated hardware costs.

Finally, traditional vendors sell add-on security technologies that incur more and more security bloat on the endpoint with additional agents, software to run, and management interfaces to operate, all driving up costs. To top that off, the software becomes more and more brittle as more layers are added on to existing code bases that cause software to crash and not optimally operate.

A Smarter Approach to Security

A new, modern approach to security that provides an alternative to legacy signature-based tools is available today. The technology focuses on proactive prediction and prevention versus after-the-fact reaction. Using artificial intelligence and machine learning, it immediately finds and blocks malware and zero-day threats from executing on a host machine, and enables organizations to protect against these attacks without the need for signatures. Real-time mathematical and machine learning models prevent threats from damaging systems.

Because this solution sits at each endpoint and proactively prevents malware from ever executing at those endpoints, organizations can more effectively defend themselves against the latest attacks.

Unlike traditional methods that are reactive and often fail to stop malware, this approach is proactive. As a result, it is capable of stopping 99% of the malware that attacks

endpoints, compared with the average 60% to 70% of traditional signature-based anti-malware products.

In addition to delivering a much higher level of security, this approach effectively addresses the performance issues related to traditional solutions. Because it does not involve the use of signatures and uses less technology, it is light on resource consumption, including CPU and memory. A protection architecture should be silent to users and easy to deploy and manage for administrators.

As discussed earlier, a main weakness of traditional security technologies is that they rely on huge databases of signatures of known malware or approved applications. Modern solutions can make decisions in real time on an endpoint by classifying an object's characteristics against artificial intelligence models that are updated a few times per year. This means there is no longer a need to constantly download new file signatures.

The newer security solution has a smaller footprint; it does not need to extensively examine an endpoint attempting to find malware like traditional signature-based products. As a result, its presence on the operating system and applications is transparent to both the end-user and the endpoint.

The solutions also enable organizations to avoid the high costs of using traditional methods of malware detection. With more effective defenses against malware in place, organizations do not need to deploy endpoint detection and response tools that require highly-skilled staffers. They replace antiquated methods that can only find malware after it has already executed and potentially damaged the organization.

The deep scans on endpoints required by signature-based software are eliminated, along with the long work delays for end-users. For enterprises with thousands of users on a network, that can lead to an enormous amount of cost avoidance. Also eliminated is the costly maintenance needed for signature-based products.

The stronger security posture made possible by modern solutions can help organizations protect themselves against attacks. Millions of dollars in data loss, legal fees, regulatory penalties and other costs are avoided. In addition, the intangible costs of damage to brand reputation that results from a security incident are precluded.

Finally, there's the added benefit of enabling security and IT staff to focus on more strategic, innovative endeavors. This is made possible by the time savings accrued from not having to employ signature-based tools.

Summary and Conclusion

Organizations that rely on signature-based security products have not done anything wrong; they've simply had no choice because there were no viable solutions available. The fact remains that these products are not adequately protecting against today's security threats, and they continue to become less effective every day.

While the attackers have grown in sophistication, the old ways of securing information assets have not evolved with the times. Malware mutation enables attackers to use the same attack vector and malware in a new undetectable attack. Thus, a more intelligent antivirus solution is required to prevent execution of the previously unknown and ebb the tide of zero-day malware.

On top of that, these legacy solutions are negatively impacting the performance of key business systems and applications, and driving up total security costs because of the multiple layers of defenses that are needed.

But now, there is an alternative. Proactive security solutions that prevent attacks, and identify threats before they strike, bring about a new level of security, performance, and cost savings. They are capable of keeping up with attackers and malware writers and stopping their attacks before they have any real impact.

This modern approach to security delivers in three key areas: providing maximum protection for data and systems; delivering this protection without inhibiting performance; and offering cost savings and other strategic benefits such as allowing IT and security staff to work on long-term projects instead of constantly responding to today's emergency.

Rather than taking any vendor's word, Cylance recommends that IT and security executives evaluate any traditional security product side-by-side and in a real-world environment. Cylance offers free proof of concept reviews, simplifying evaluation of its technology against a company's current security technologies. To access the company's testing resources, visit www.cylance.com/knowthetruth

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

20170223-2473