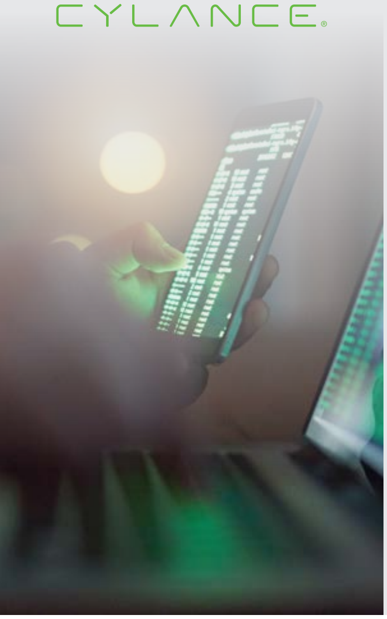
Sponsored by

BlackBerry CYLANCE



EXECUTIVE BRIEF

Why It's Time for Your Organization to Explore Next-Generation Antivirus

In this Paper:

- SMBs face the same security and compliance requirements as enterprises, without the same level of resources.
- Legacy AV has significant shortcomings, including a reliance on detect-respond instead of a prevent-first approach to security.
- BlackBerry Cylance is an AI platform that helps small businesses prevent, detect, and respond to threats

While much of the attention in information security focuses on massive breaches at large, valuable brands and public-sector agencies, there are many more small and medium-sized businesses (SMBs) relying on a combination of luck and technology they hope will keep their systems and data safe. The odds are against them.

According to the 2019 Threat Report from BlackBerry Cylance, overall malware attacks were up 10 percent in 2018. Among the report's observations about the threat landscape:

- Ransomware attacks declined slightly in 2018, but the sophistication of the attacks increased and the average industry response was 25 days.
- Existing threats continue to evolve and become more dangerous. Emotet, for example, was beefed up in 2018 to include capabilities like analysis awareness, multi-layered command-and-control (C2) encryption, brute-force credential attacks, and full-body email harvesting capabilities.
- Advanced persistent threat (APT) actors actively embraced tools and malware based on open source code like Mimikatz and HTran in 2018.

At large organizations, understanding these evolving threats, preventing attacks, and responding to incidents are the job of the security operations center (SOC). For SMBs, however, the first line of defense is often antivirus software, which is usually a legacy application that has not evolved as quickly as the threats it's asked to detect.

This is the information security dilemma of SMBs: They have the same security and compliance requirements as enterprises, but they are without the enterprise-level resources to detect and thwart attacks.

If your SMB's security strategy includes legacy antivirus products, it's time to think about a new approach. Legacy antivirus products are ineffective when it comes to preventing many of the threats that keep business executives and IT professionals awake at night, including ransomware, malware, and zero-day attacks.

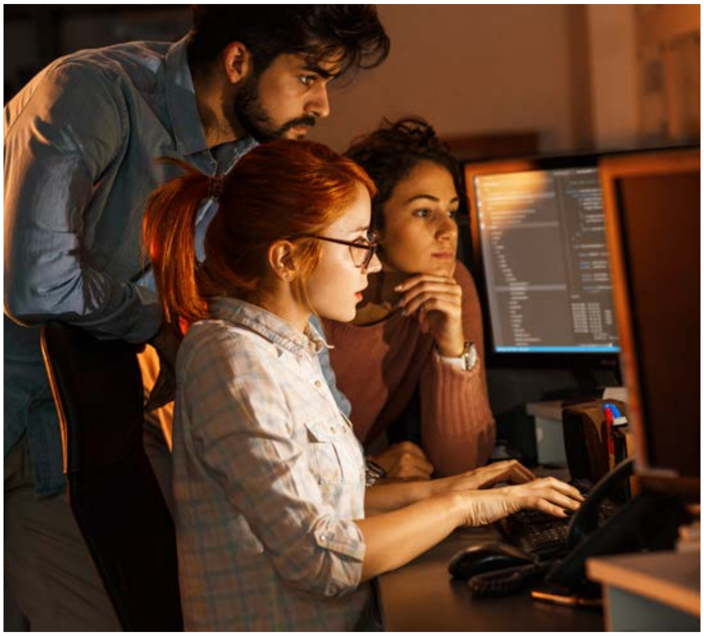
There are three major shortcomings of legacy antivirus solutions:

1. Reliance on signatures

Signatures slow the time it takes to secure your environment and often add unnecessary costs. When your antivirus relies on signatures, your organization is forced to accept a miss rate. In other words, a certain percentage of malware will get past your defenses. What is an acceptable miss rate for your business? Is it 12 percent? Or 18 percent? And which pieces of malware and malicious code are in that percentage of misses? If you're relying on signatures to protect your business, these are questions you need to consider.

Next Steps:

- Talk with Cylance about next-generation antivirus and get your questions answered. 844-295-2623 or sales@cylance.com
- For a free Cylance demo and ROI analysis, visit https://www.cylance.com/en-us/solutions/use-case/small-to-medium-business.html



2. Poor user and admin experience

Legacy antivirus has a well-earned reputation for degrading the computing experience for end users and creating headaches for administrators.

Users trying to focus on their daily tasks and projects find their machines slowed by legacy antivirus solutions and the steady stream of updates required to maintain some semblance of security. On the technical side, this slow performance is a problem of disk I/O. The procedure for merging and loading definitions is disk intensive, consuming processor power, and slowing the machine to a crawl.

Administrators working with legacy antivirus are devoting their valuable hours to a number of tasks that keep the system up and running, including investigating and remediating attacks, creating signatures, patching endpoints, and re-imaging systems.

3. Increased strain on resources

All of this daily management, remediation, patching, updating and more, quickly consumes the limited resources of SMBs. In a Forrester Total Economic Impact (TEI) report commissioned by BlackBerry Cylance, one administrator described their organization's legacy antivirus this way:

"We were spending most of our resources fixing things, rather than finding things or working proactively. So, the focus was on getting the (legacy) solution to work, instead of actually using it."[1]

Why Next-Generation Antivirus is Worth Exploring

The shortcomings of legacy antivirus solutions are leading security software vendors to explore new strategies and products known collectively as next-generation antivirus (NGAV). In an effort to improve security and ease the management burden, NGAV vendors tout their use of technologies like cloud computing, artificial intelligence, and machine learning.

Simply incorporating the cloud, however, does not make a next-generation antivirus solution; the cloud is an enabling technology throughout IT organizations of every size today. Even the legacy antivirus solutions are using cloud-based analytic security services to increase their visibility into events. But because of the delay in recognizing a piece of malware and creating and distributing a signature, this after-the-fact approach still often fails to stop zero-day attacks (and fails to update offline systems as well).

Get the Facts about Next-Generation Antivirus

All next-generation antivirus products leverage the cloud, but they don't all leverage it the same way. For example, many next-generation solutions are sending massive amounts of data to the cloud to analyze it and build threat intelligence. There are two problems with this approach:

- It's too late. Any benefit gained from analyzing data in the cloud is lost when it's derived after an attack and cannot minimize the damage.
- It can introduce more risk. When a large portion of your data is sent to the cloud, it's inevitable that sensitive information like customer data or PII will make the journey to the cloud. Your organization will also be on the hook for the cloud storage costs for all of that data.

> **"Legacy antivirus products are ineffective when it comes to preventing many of the threats that keep business executives and IT professionals awake at night."**

> **"If your SMB's security strategy includes legacy antivirus products, it's time to think about a new approach."**

As you explore next-generation antivirus products it's important to understand the extent to which they use technologies like the cloud and artificial intelligence, and whether or not they rely on signatures and humans to identify, block, and remediate threats.

And the most important question to ask as you evaluate next-generation antivirus solutions is the most obvious:

Would Next-Generation Antivirus Improve Your Security?

SMBs need an antivirus solution that combines effectiveness, affordability, and manageability.

BlackBerry Cylance brings a very different strategy to next-generation antivirus. BlackBerry Cylance focuses on a prevent-first approach to antivirus instead of the detect-respond approach used by many legacy and next-generation antivirus vendors. Prior to being acquired by BlackBerry, Cylance was the first vendor to deploy artificial intelligence in the antivirus market, and the company has since developed an AI platform that helps businesses prevent, detect, and respond to threats.

The BlackBerry Cylance models can catch and stop most attacks before they happen because they don't rely on signatures or humans. Instead, BlackBerry Cylance reduces its complex predictive model down to an algorithm that can run locally on an endpoint, independently of the cloud. This method of protection runs lighter than legacy and NGAV products, allowing users to maintain their productivity and security. It also helps BlackBerry Cylance protect offline devices and eliminates the need to send data to the cloud for analysis.

BlackBerry Cylance designed its platform to be easy to use and administer for IT professionals. Among the quantified benefits experienced by the Cylance customer in the aforementioned Forrester TEI study were:

- Savings of $8.4 million by decommissioning the legacy on-premises endpoint security solution
- A 10 percent improvement in cybersecurity team productivity
- A 25 percent reduction in the expected cost of a major security breach
- A 95 percent reduction in lost time thanks to faster investigation and remediation
- Reduced machine reimaging by 97 percent.

The financial analysis conducted by Forrester found the customer in its report experienced benefits of more than $14 million over three years, which led to an ROI of 99 percent on its BlackBerry Cylance investment.

BlackBerry Cylance offers SMBs the opportunity to fill in the IT security resources gap with a platform powered by artificial intelligence. By helping SMBs detect, prevent, and respond to known and unknown attacks, BlackBerry Cylance addresses the security shortcomings these organizations face today, from resources to costs to productivity – all with a focus on prevention first. It's enterprise-level protection for small and medium businesses.

Learn more at www.cylance.com.

Sources

[1] https://www.cylance.com/en-us/company/about-us/our-customers/2019-forrester-tei-report.html