SentinelOne

Replacing Antivirus, and Doing it Right
A CISO Perspective

By Larry Whiteside, Jr.

OVERVIEW

As cyber threats grow in diversity and sophistication, AV-based protection offers less and less effective protection for organizations, creating a pressing need to replace existing signature-based endpoint protection software with a more advanced solution. Such a replacement project can be daunting, but with the right approach, you can get it done smoothly, and achieve a more robust security posture for your organization.

WHY AV IS NO LONGER EFFECTIVE

Antivirus (AV) technologies have not evolved much over the last fifteen years. Their detection model still relies on the core principals of a central repository with lists of virus "definitions" which contain the following information:

- known bad strings (typically cleartext) in the malicious file
- hashing part of or the full known bad malicious file

This signature-based approach has been called obsolete for at least a decade – Gartner dropped the AV magic quadrant in 2006, yet millions of organizations still spend billions of dollars on AV products annually. Most of these organizations also recognize that signature-based AV does not catch all the sophisticated malware present today.

Signature-based AV has a few fundamental problems that make it largely ineffective against today's complex threat environment, because:

- The number of recognized threats is growing exponentially. It is impractical to create new signatures for the volume of virus and malware strains that are created on a weekly basis today. AV-TEST registers over 75,000 new malicious programs every day.
- The volume of virus and malware variants being created require that endpoints need to be updated at a near constant rate to actually catch all the malicious files encountered by them
- It is impossible for endpoint AV products to compare suspicious files with all the signatures that exist today. If this was attempted on any device, it would consume all of the devices compute resources and bring performance to a grinding halt.
- AV products are particularly vulnerable to zero-day attacks where hackers create and distribute malware before the AV vendors have a chance to create and distribute the signature to detect it. This time lag is crucial since most attacks are executed within minutes.
- Hackers and cybercriminal are targeting specific organizations with spear phishing and typically custom create malware for their target. Very often, no signatures are ever created for such malware targeted specifically for a particular individual or organization.
- Hackers are using advanced techniques to evade signature based AV – polymorphic malware, packers, encryption and similar obfuscation mechanisms.

The main reason organizations continue to spend on AV products despite these obvious limitations is the lack of certified AV alternatives. Compliance mandates that were written during the early days prescribe AV in their requirements, and the organizations that manage these mandates are also slow to evolve to the new threat landscape. This has led to organizations adopting additional endpoint technologies to complement their AV deployments, but a complete rip and replace of embedded AV products is still a daunting proposition. However, there are a number of steps that can be taken to ease this transition.

HOW TO SUCCESSFULLY EXECUTE A COMPLETE AV REPLACEMENT

From a security standpoint, an organization-wide rip-and-replace of an AV-based endpoint security solution in favor of a next-generation solution is a sound decision. But—as is the case with practically every IT conceivable project—it is easier said than done.

I'll recount the details of one such project that I worked on, several years back. The goal was to replace one legacy endpoint protection solution with a new one from the other large, similarly established security vendor.

Number of Endpoint Devices:	**20,000 (primarily laptops)**
Initial Project Timeline:	**90 DAYS**
Actual Project Duration:	**180 DAYS**

It took 2 months of meetings just to get the initiative off the ground. There were many big questions that the team wasn't able to answer completely. For example:

- How will this project impact certain end-users?
- What are the specific logistics around deploying the new solution?
- What measurable benefits should be expected?

The team had to go back to the drawing board and then circle back with the details stakeholders were demanding.

Deployment of the new solution kicked off, but without having been fully tested with all business images. Some end-users were stalled and subsequently infuriated as they experienced intermittent device crashes. Since these failures weren't easily reproduced, no root cause could be identified. The issue spread to a wider group of endpoints, forcing the organization to exhaust budget prematurely to buy a whole set of new devices; it became far less complicated to deploy the new endpoint protection software on fresh hardware than to troubleshoot the problem on the existing affected devices. Though these issues were eventually resolved, the whole project was negatively perceived by a few key IT stakeholders, who became far less amenable to greenlighting subsequent security projects.

The way in which this particular project was planned and executed underscores the importance of the following best practices.

DO YOUR HOMEWORK... BEFORE DOING ANYTHING ELSE!

Before reaching out to key stakeholders, you have to prepare a plan for this project that addresses all major considerations across the organization, and be ready for any and all questions you'll get, and that requires a strong sense of what each key stakeholder cares about. If you've got allies or trusted advisors across different departments and management levels, get in touch with these folks and ask for their insights. These stakeholder-specific considerations are detailed in the following section.

GET COMPLETE BUY-IN FROM KEY STAKEHOLDERS

You can definitely make an airtight case for why static, signature-based endpoint protection needs replacing with a next-generation solution. The advantage from a pure security efficacy perspective is significant. However, the stakeholders you need to sell the project to care about very different things. Here's what you'll need to consider for each one:

EXECUTIVE MANAGEMENT

Having the best possible protection against cyber threats and lowering compliance risk are top of mind for C-level execs when it comes to security. Selling the project to upper management means clearly highlighting the deficiencies of the current endpoint protection solution, along with the overall value that the new solution will deliver. C-level stakeholders will also be very focused on business productivity and IT spending. Your pitch to them should address the end-user productivity impact of deploying and running the new solution. Address concerns related to potential deployment issues, and highlight any performance advantages the new solution brings. Furthermore, they'll want to know about any changes in IT resources required to deploy and manage the new solution. If you can present a solid ROI projection specific to your organization, then your chances of C-level approval are much improved.

IT STAKEHOLDERS

Your IT team will ultimately be responsible for the testing, coordination, and deployment of this new software. For these folks, the size of the installation, the time it takes to install, and the overall impact on endpoint devices as a whole will determine exactly how difficult a job ripping and replacing the existing endpoint security software will be. Also carefully consider that your existing endpoint protection software has integrations with the device OS, and other running applications, and uninstalling it may result in significant issues.

BUSINESS OWNERS AND END-USERS

Across the different functions of your organization, department leaders and end-users alike will be concerned primarily with productivity. Successfully pitching this group on your endpoint protection replacement project will involve a well-conceived deployment plan that minimizes both endpoint downtime and inconvenience to its user. Your plan should also address major contingencies, with details on what users should do in the event an issue arises that affects their device.

COMMUNICATE FREQUENTLY AND CLEARLY

Even with the best-conceived project plan, clear communication to all stakeholders at every step is imperative. This approach keeps everyone well-informed of your progress toward your end goal of better protecting the organization's valuable data, and in the best case, saves you the time and effort of answering a barrage of questions, since the information you share will pre-empt the majority of them.

CONCLUSION

With the increase in frequency of major data breaches perpetrated by highly advanced cyber attacks, we're clearly at a point where the traditional endpoint security technologies are no longer sufficient. For IT security leaders, implementing a next-generation endpoint protection solution is a highly likely, if not inevitable, project. Though a daunting effort at first glance, an organization-wide endpoint protection replacement is doable, and will be most successful with careful planning, stakeholder buy-in and clear, frequent communication.

For more information on SentinelOne, visit www.sentinelone.com.