MINERVA

THE STATE OF ENDPOINT SECURITY IN ADDRESSING MALWARE AND OTHER MODERN CYBER THREATS

MINERVA LABS SURVEY, 2018

About this Survey

The nature of cyberattacks is such that defenders and attackers are locked in an arms race. Each party has incentives to innovate in response to the other's advancements. Given Minerva Labs' objective to break the unending cat-and-mouse game dynamics in endpoint security, we surveyed 600 information security professionals about their concerns and opinions related to protecting systems from malicious software and related threats. Our hope is that the findings and our analysis, presented in this report, will educate enterprises regarding approaches to strengthening their endpoint security architecture.

Key Takeaways From the Survey

Despite using anti-malware software for endpoint protection

2/3 *of respondents believed their controls won't prevent a significant malware attack on the endpoints.*

3/4 *of respondents deemed their existing anti-malware solution to be able to prevent no more than 70% of infections.*

1/2 *of respondents were concerned about fileless or analysis evasion capabilities of malicious software as a way of getting past their existing security measures.*

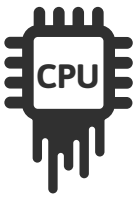
50% Days & Weeks

Respondents differed in their ability to swiftly recover from a malware attack: as many claimed being able to restore operations in hours as did in days or weeks.

50% Hours

75% *of respondents believed the rate of malware infections stayed the same or got worse in the past year, despite continued advancements in anti-malware technologies.*

of respondents preferred to strengthen security by adding an additional defensive layer on the endpoint, as opposed to completely replacing their existing solution.



40% *of respondents considered resource consumption to be of the highest operational priority for an anti-malware solution beyond its ability to safeguard the endpoint.*

Effectiveness of Baseline Anti-Malware Controls

Antivirus or full-fledged Endpoint Prevention Platform (EPP) solutions form the baseline for anti-malware controls. Not surprisingly, compliance frameworks and best practices require that such measures be deployed on endpoints. Yet, their presence alone is insufficient for safeguarding endpoints from modern threats.

To what extent do you think your antivirus or Endpoint Protection Platform (EPP) is preventing infections on your endpoints against modern malware threats?

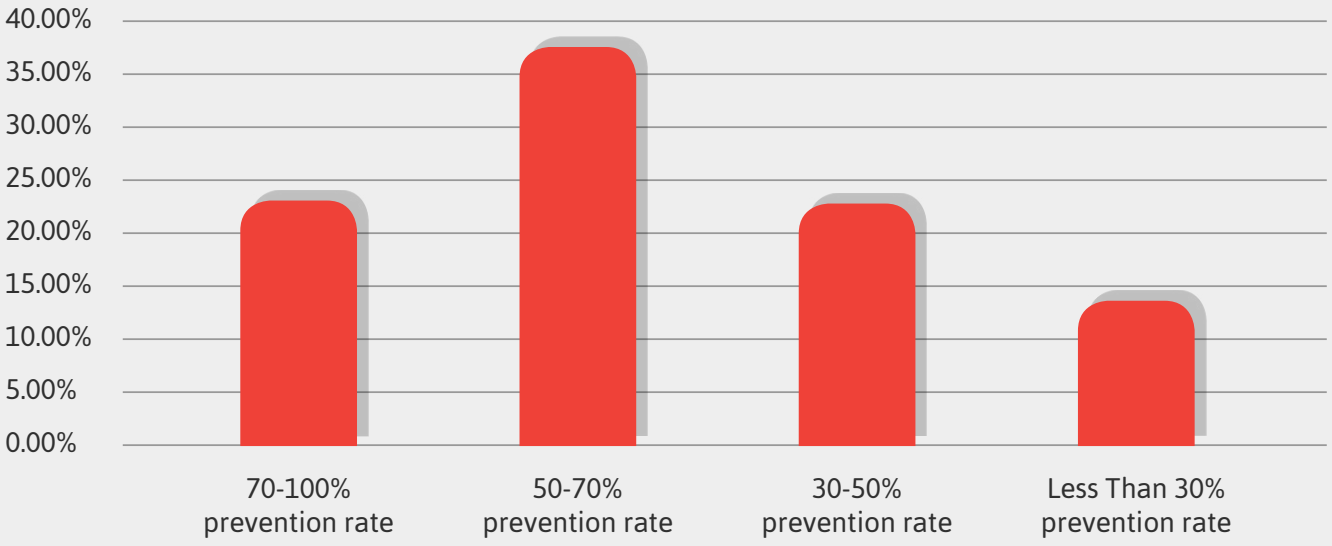


Figure 1: Efficacy of AV or EPP Solutions

***75%** of respondents think their current endpoint security solutions are preventing no more than **70%** of infections*

In a related question, the survey asked respondents how concerned they were with the ability of their existing endpoint security controls to prevent an attack. Two-thirds indicated high or moderate concern, with only 34% stating that their level of concern was slight or nonexistent, as shown in Figure 2. These findings indicate that enterprises continue to worry about their ability to prevent infections, despite their use of baseline anti-malware solutions.

How concerned are you that your existing security controls will not prevent a significant malware attack on your endpoints?

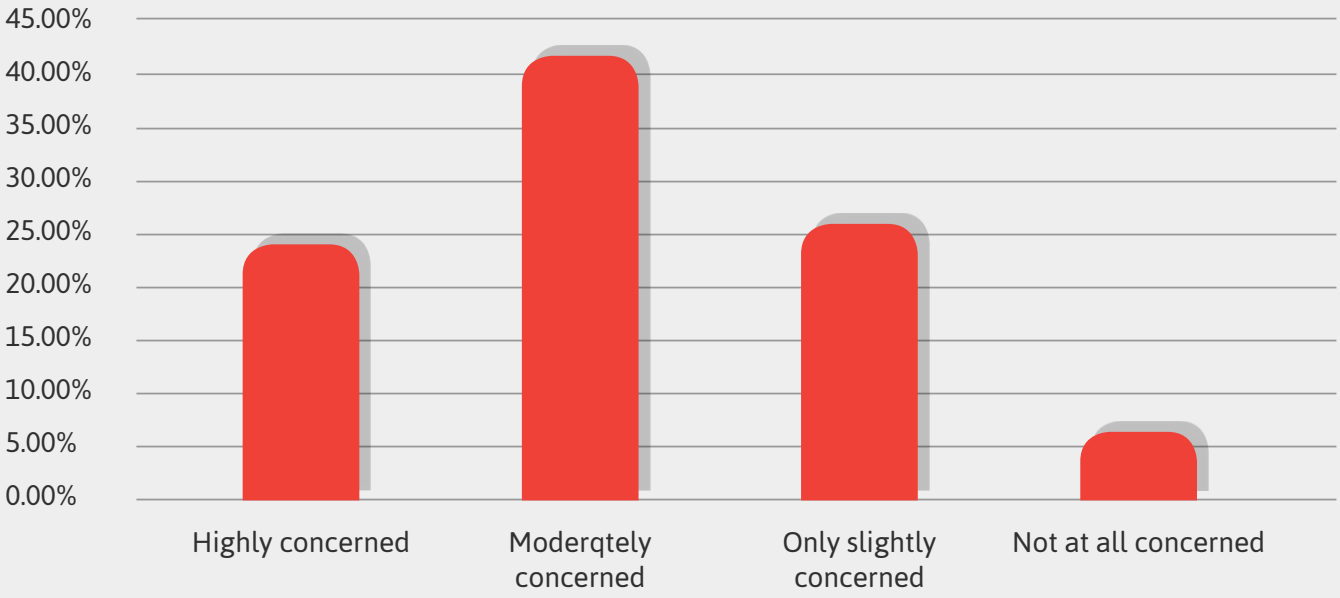
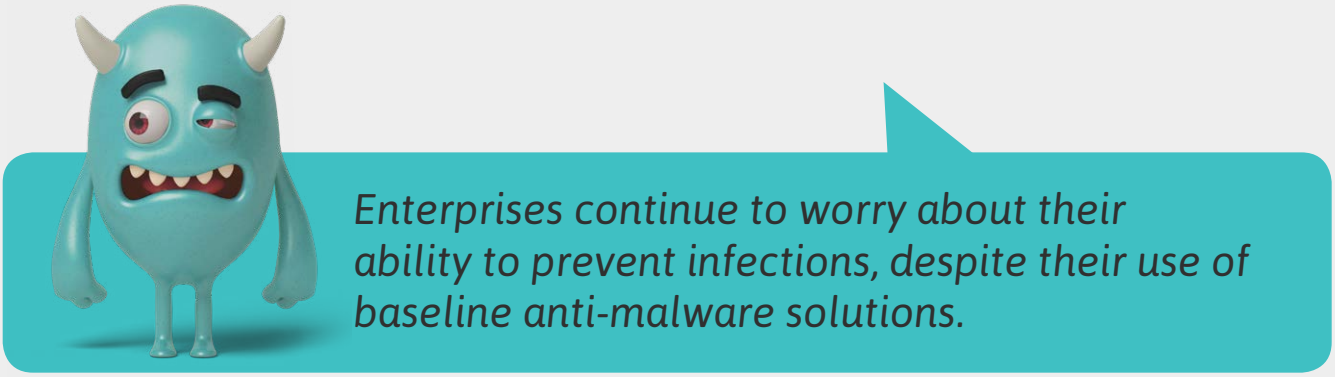


Figure 2: Concerns About Significant Malware Attacks



Enterprises continue to worry about their ability to prevent infections, despite their use of baseline anti-malware solutions.

Clearly, many enterprises continue to see and anticipate infections despite prior investments in security technologies such as Endpoint Prevention Platforms (EPP), Enterprise Detection and Response (EDR), application whitelisting and other malware countermeasures.

Though antivirus or EPP solutions differ in some aspects of their approaches to detecting threats, they all operate by attempting to identify malware based on the analysis of previously-seen malicious programs, as illustrated in Figure 3.

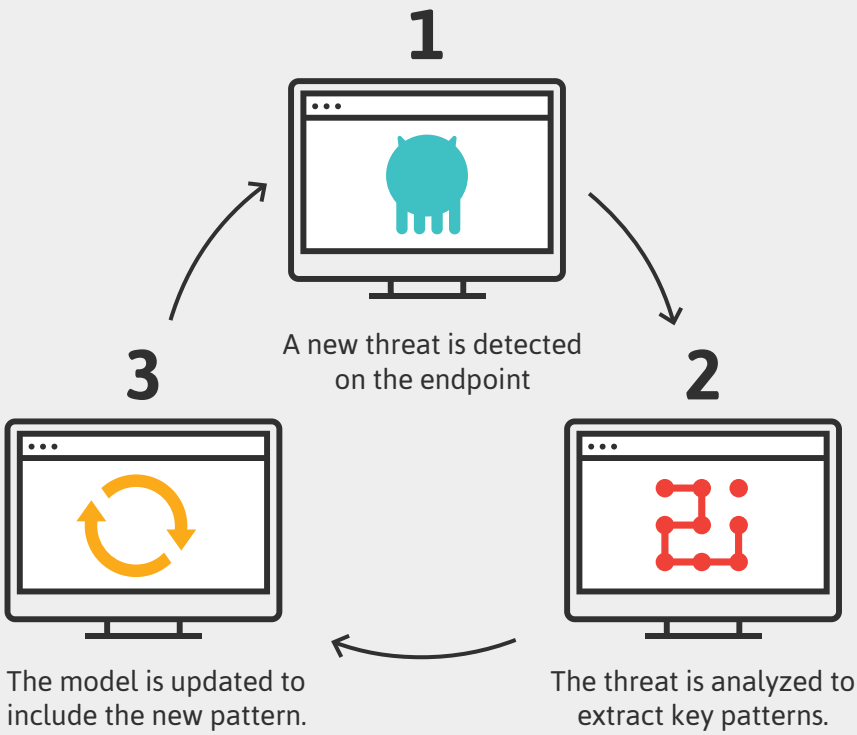


Figure 3: Relying on Prior Knowledge of Malicious Patterns for Detection

To address the gap that any baseline anti-malware solution will leave in its ability to prevent infections, defenders should look for approaches that work differently and are not detection-based, for instance by preventing malware from attempting to get around existing security measures.

Disrupting the Cycle of Reactive Security

Competitive industry dynamics, combined with the evolving threat landscape, brought significant innovation to the endpoint security industry in the recent years. Even the technologies that form the baseline of anti-malware protection now incorporate vast databases of known malware, employ artificial intelligence to spot new malware based on its similarities to previously-seen patterns and employ numerous other security mechanisms to protect systems from threats.

However, these improvements are insufficient for making progress at decreasing the number of infections, according to survey participants. As captured in Figure 4, over 75% of respondents believed the rate of malware infections stayed the same (48%) or got worse (32%) in the past year.

In the past year, to what extent have you seen your endpoints infected by malware?

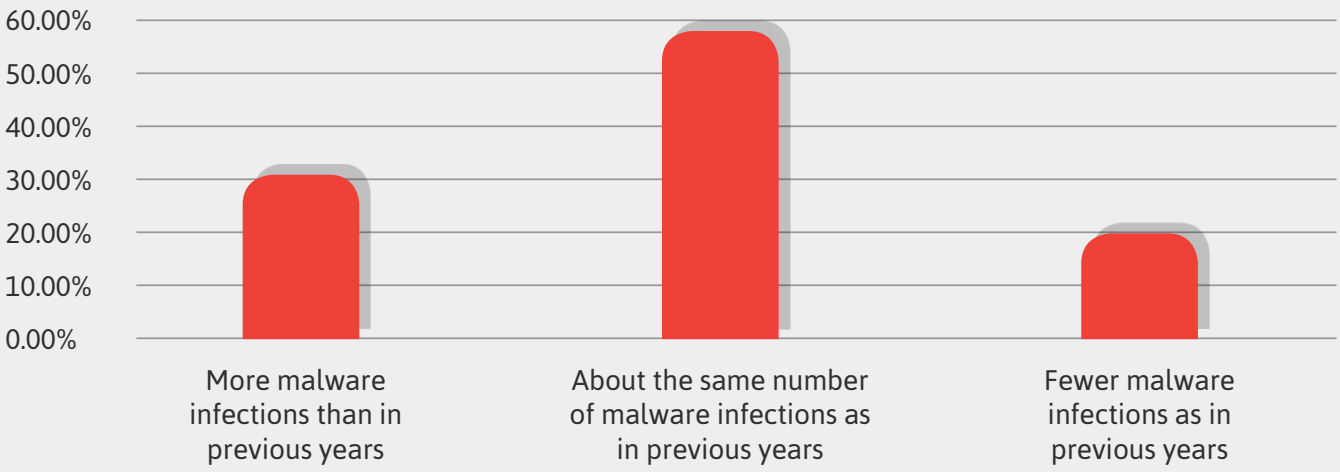


Figure 4: The Number of Infections in the Past Year

75% *of respondents believed the rate of malware infections stayed the same or got worse*

Why are our adversaries consistently able to evade detection? The very evolution of anti-malware solutions is driving the attackers to design malicious software that stays under the radar of security vendors and slips past existing defenses. Such evasive malware avoids detonating in sandboxes or forensic environments, resides in memory of legitimate applications, employs scripts and document files, and relies on other techniques that bypass traditional and "next-gen" security measures.

When asked about the nature of evasive threats that are most concerning to them, roughly half the respondents were worried about fileless (24%) or analysis evasion (42%) capabilities of malicious software as a way of getting past their existing security measures. A quarter of the respondents expressed concerns about the use of booby-trapped document files. This is captured in Figure 5.

Of the following malware evasion techniques, which concern you the most?

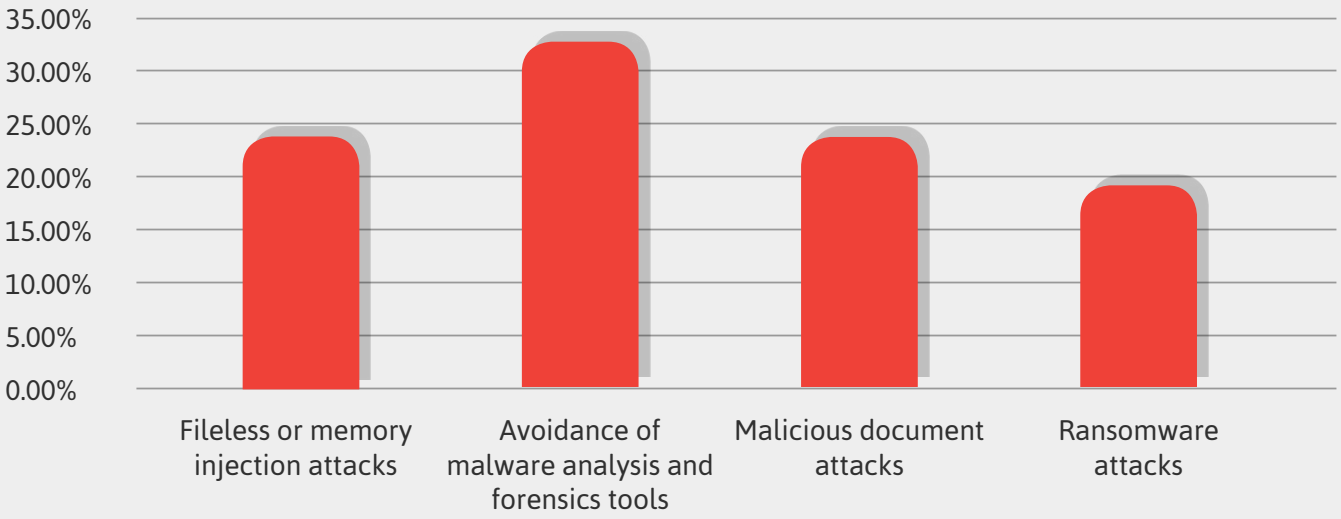


Figure 5: Concerns Over Evasive Threats

Endpoint breaches can cripple the business due to service disruption, data loss, staff utilization and other expenses. Many organizations have been improving their ability to detect and respond to security incidents. As the result, 17% of survey respondents stated that they were able to restore a compromised endpoint to a normal state within minutes. Unfortunately, this capability is relatively uncommon. 41% of responders are able to restore within hours, while over a quarter of responders take days or even weeks to accomplish this, as shown in Figure 6.

When faced with a compromised endpoint, how long does it take your organization to restore itself to a normal state?

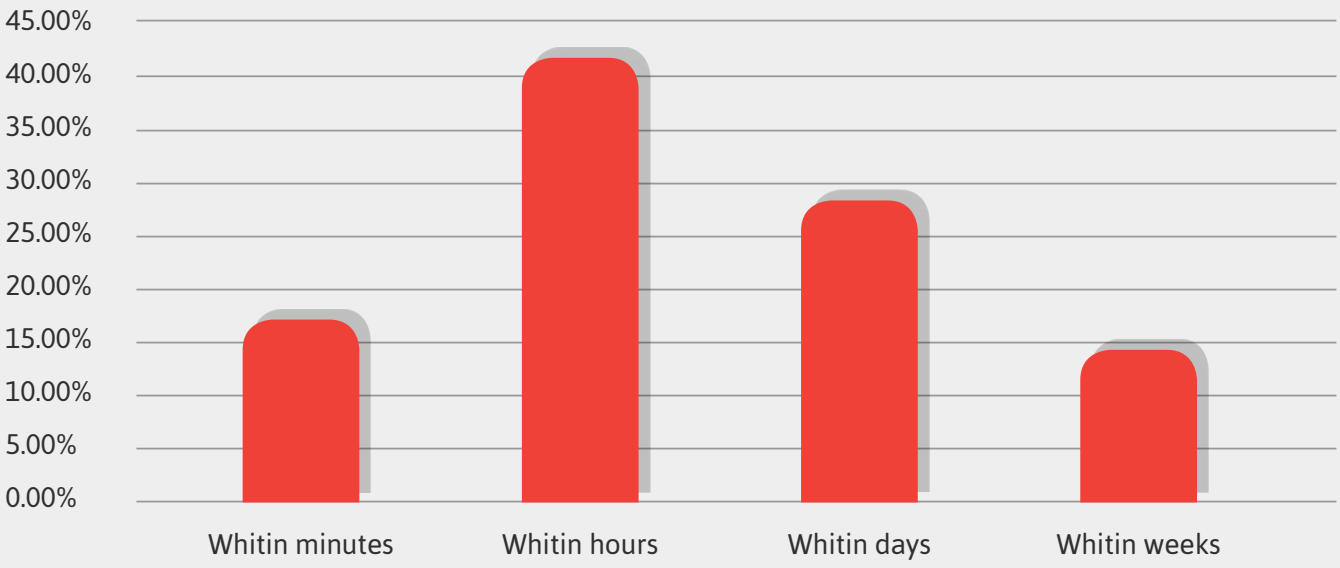


Figure 6: Time Taken to Restore a Compromised Endpoint to a Normal State

Given the effort required to react to a malware infection and return the system to a normal state, enterprises have the incentive to prevent as many compromises as possible. This entails practicing general security hygiene, such as asset and patch management, confirming that the right security capabilities are present in baseline anti-malware protection, and looking for ways to improve upon efficacy limitations of any foundational antivirus or EPP approaches.

Improving the Endpoint Security Posture

The survey asked about the measures the respondents would take to improve the performance of their antivirus or EPP tools in the face of modern threats. Some respondents were interested in relying solely on their existing solution (17%), and some wanted to entirely replace the solution with a competing product (31%).

If you were unhappy with the performance of your current antivirus or Endpoint Protection Platform (EPP) solution, please choose one of the following statements as your preferred approach.

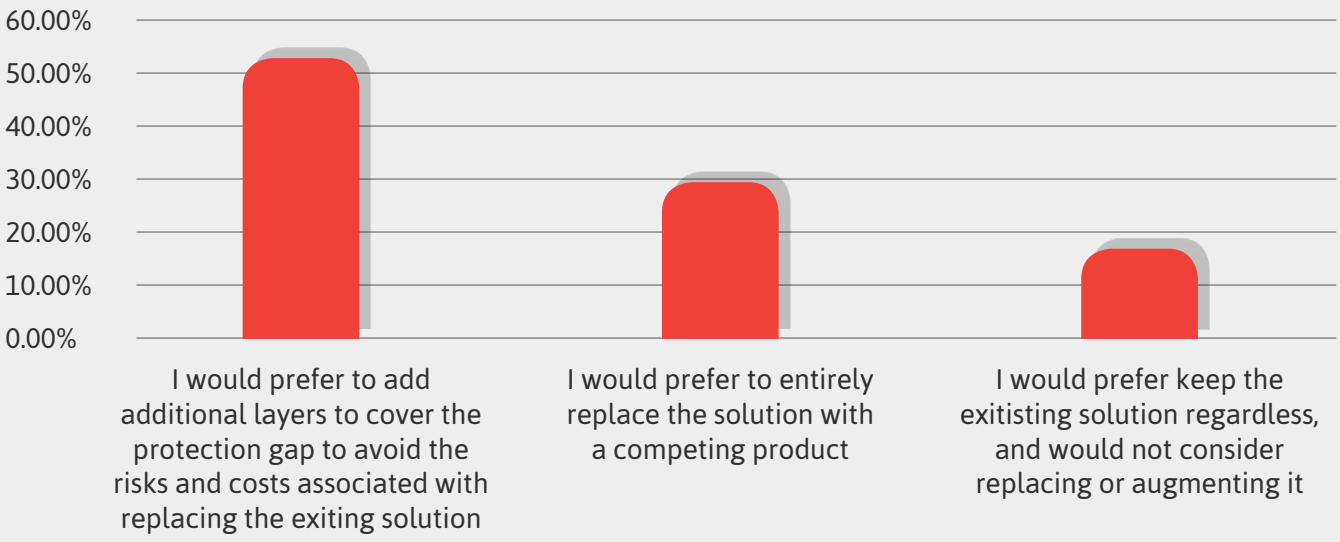


Figure 7: Improving Upon Baseline Anti-Malware Protection

We can assume that the respondents' preference for augmenting baseline anti-malware technology with a new layer was due to their desire to avoid the risks and costs associated with replacing the existing solution. After all, the "rip and replace" project is likely to involve a lengthy rollout, intense regression testing, and require reengineering of many IT processes. At the end the organization might only get incremental improvement on anti-malware effectiveness and may even lose functionality in the transition.

Over half the respondents preferred to add an additional layer to cover the protection gap rather than rip and replace their existing solution

We also asked respondents about the operational aspects of an endpoint security solution that were important to them. For instance, anti-malware technology can artificially inflate its level of effectiveness by flagging even slightly-suspicious files as bad, producing many false positives. This may result in an anti-malware product being effective at preventing infections but drain system performance (and human resources) in a way that interferes with normal business applications. Among the options that the survey presented, the respondents (39%) expressed a strong desire to ensure that the solution operates without consuming many resources on the endpoint. The next important property was the ease of deployment and upgrades (29%), followed by the need to maintain a low rate of false positives (17%) and operating without burdensome configuration requirements (15%). This is illustrated in Figure 8.

Besides security benefits, which of the following operational aspects of an endpoint security solution do you find most important?

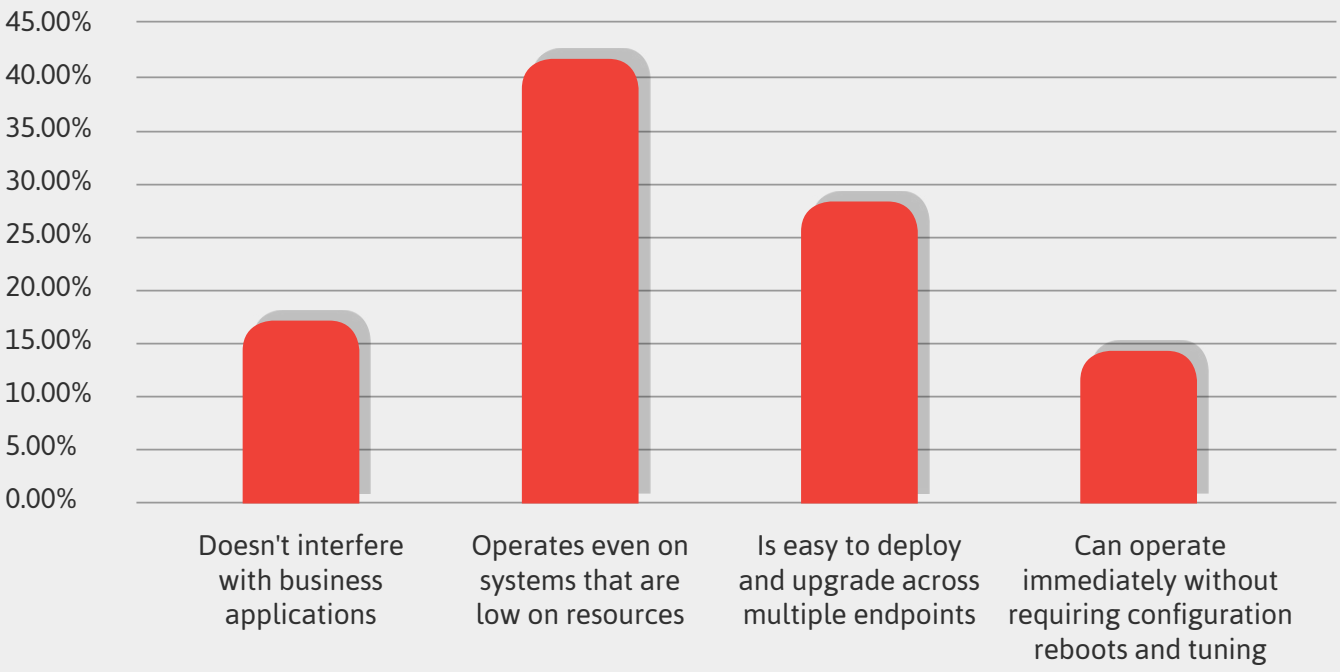


Figure 8: Solution's Operational Characteristics Beyond Security

Overall, organizations should question how they can improve their ability to strengthen endpoint security without interfering with business operations or overwhelming IT and security personnel. Furthermore, enterprises should assess their ability to go beyond blocking malware based on previously-observed patterns or by relying on detection and response tools to identify breaches after the fact. They should also look for ways to prevent infections from never-before-seen threats in a manner that differs from the approaches employed by antivirus or EPP technologies and leave the resource intense breach detection and analysis process to the few and far between incidents. This notion is illustrated in Figure 9.

Figure 9: Filling the Gap in Endpoint Security Architecture to Prevent Unknown Threats

The Need to Bridge the Endpoint Security Gap

Despite organizations' continued investments in cyber-security, malware continues to pose a serious threat to endpoints. Enterprises are starting to realize that antivirus technologies, even those that employ the latest and advanced approaches, are insufficient to disrupt the cat-and-mouse dynamics of the industry where adversaries continually adapt to evade defenses. The methods for bypassing such security measures are no longer limited to skilled attackers. They are also employed by unsophisticated threat actors with great effectiveness.

What's needed is a solution that approaches endpoint security from a different angle, one that doesn't look for previously seen patterns or suspicious behavior. Minerva's approach to accomplishing this involves stopping threats by deceiving them regarding the state of their environment, so that the malware breaks or disarms itself. As such, Minerva's Anti-Evasion Platform provides the ideal complement, or the "missing piece" to any endpoint security stack.

This survey demonstrated that beyond the security benefits an endpoint security solution delivers, its operational aspects are no less important. Enterprises value the ability for the technology to work in a heterogeneous environment where low resource, legacy systems need protecting alongside new systems. Furthermore, the solution should be easily deployed across large, distributed environments without impacting the end user's experience or productivity. Enterprises should seek solutions that thrive not only in security, but also in the area of operational performance.

Minerva Labs' approach to endpoint security turns the tables on attackers, giving defenders the edge traditionally enjoyed by our adversaries. We do this this by "attacking" attempts to get around security controls. This allows the existing security measures to function as designed and makes it impractical for attackers to take evasive actions. As the result, Minerva's Anti-Evasion Platform defends endpoints from threats that baseline anti-malware solutions don't stop, even preventing infections by unknown, previously-unseen malware. For every incident prevented, resource time is saved. Minerva forces attackers to make a choice: employ evasion and encounter Minerva's countermeasures, or avoid evasive tactics and get stopped by the target's other endpoint security solutions. All this is achieved with operational advantages built into the solution from the ground up.

ABOUT MINERVA

Minerva Labs is an innovative endpoint security solution provider that protects enterprises from today's stealthiest attacks without the need to detect threats first, all before any damage has been done. Minerva Anti-Evasion Platform blocks unknown threats which evade existing defenses by deceiving the malware and controlling how it perceives its environment. Without relying on signatures, models or behavioral patterns, Minerva's solution deceives the malware and causes it to disarm itself, thwarting it before the need to engage costly security resources.
Minerva boosts customers' existing defenses without the need to embark upon a costly and risky overhaul of their entire endpoint security architecture.

To learn more about Minerva Labs, visit ***www.minerva-labs.com.***