About the 2016 Advanced Malware Detection and Response Study

More than half of surveyed security leaders rate their organizations’ current anti-malware protection above average or superior. And yet ...

- 54 percent say their organizations have experienced ransomware in the past year;
- 25 percent say they struggle with threat detection;
- 51 percent say their current anti-virus tools have difficulty detecting APTs.

These are among the results of the 2016 Advanced Malware Detection and Response Study.

Aimed at determining how effective current anti-malware tools are at keeping organizations’ endpoints secure, the survey finds that reporting is the biggest failing of current tools. The clear message from respondents: “We don’t have a good dashboard to view all the data from our controls.”

There is good news in the survey results, too: 98 percent of respondents say they expect to receive the same or additional funding for anti-malware defense in the coming year. What are their top spending priorities? Read on to learn more. And pay special attention to our survey analysis at the end of this report, where we offer expert insight on how to best put these survey results to work for your organization.

Best,

Tom Field
Vice President, Editorial

Information Security Media Group
tfield@ismgcorp.com
This survey was conducted online in the summer of 2016, and it generated more than 200 responses from organizations across industrial sectors in the U.S.

### Table of Contents

- **Introduction** .......................................................... 2
- **By the Numbers** ..................................................... 4
- **Survey Results** ....................................................... 5
  - The Malware Baseline ........................................... 5
  - Anti-Malware Landscape ......................................... 9
  - Detection, Response ............................................. 12
  - Reporting and Analytics ........................................ 14
  - Software Deployment and Administration .................. 15
  - 2017 Agenda .......................................................... 16
- **Conclusions** ......................................................... 18
- **Survey Analysis** .................................................... 19
  - Justin Dolly of Malwarebytes ................................ 19

### About Malwarebytes:

Malwarebytes protects consumers and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional anti-virus solutions. Malwarebytes Anti-Malware, the company’s flagship product, has a highly advanced heuristic detection engine that has removed more than five billion malicious threats from computers worldwide. More than 10,000 SMBs and enterprise businesses worldwide trust Malwarebytes to protect their data. Founded in 2008, the company is headquartered in California with offices in Europe, and a global team of researchers and experts. Learn more about Malwarebytes at www.malwarebytes.com.
By the Numbers
Some statistics that jump out from this study:

54% of respondents have experienced ransomware in the past year.

48% rate the effectiveness of their current anti-malware protection at average or below.

82% say their top priority in 2017 is to improve malware detection.
The Malware Baseline

This quandary is at the heart of this survey report: 52 percent of respondents rate their organizations’ current anti-malware protection at above average and superior. Yet, 54 percent have been attacked by ransomware in the past year, and more than one third have been struck by infected Trojans and spyware.

The underlying question of this survey is: How effective are your current tools for keeping your endpoints secure?

The answer: Not as well as security leaders might initially believe.

Detailed results follow and shed light on the current baseline of malware challenges.

In the past year, what type of malware incidents has your organization experienced? (select all that apply)

No surprise. In a year when ransomware dominates the headlines – particularly for healthcare entities – more than half of respondents say they have experienced such attacks. Trojans and spyware also rate high. More significantly, only 16 percent of respondents claim no known malware incidents. "Known" may be the operative word.

In a year when ransomware dominates the headlines, more than half of respondents say they have experienced such attacks.
Survey Results

What consequences did your organization experience as a result of these incidents? (select all that apply)

Downtime: 49%
No consequences: 41%
Recovery costs: 23%

Downtime is always the big toll exacted by malware infection, as staff is suddenly redirected to investigate and mitigate. The other key impact: recovery costs, listed by 23 percent of respondents.

How long do you believe malware went undetected in your systems?

- Less than one day: 47%
- 1-5 days: 23%
- 1-4 weeks: 9%

Asked how long malware went undetected in their systems, 47 percent say less than one day – which is far better than the 200-plus days that researchers were discussing a few years ago. Twenty-three percent say malware went undetected for one to five days, while nine percent say it took one to four weeks.
How do you rate the effectiveness of your current anti-malware protection?

On one hand, it can be argued that the anti-malware glass is half full – 52 percent of respondents rate their current protection as above average or superior.

But 41 percent rate it only as average – and how good is “average” when you’re talking about protecting your systems from potentially crippling infections?

And when 48 percent of respondents say their current protection is average or worse, that makes a loud and compelling comment about “half empty.”

How good is “average” when you’re talking about protecting your systems from potentially crippling infections?
What do you perceive as the biggest failing of your current anti-malware solutions?

- Reporting—we don't have a good dashboard to view all the data from our controls (29%)
- Detection—we simply miss many of these threats (25%)
- Response—the damage is often done before we can eradicate malware (22%)
- Dwell time—malware sits in our system too long before it is finally detected (13%)
- Administration—we cannot keep our solutions and systems updated in line with the latest malware evolutions and variants (11%)

As for the most vulnerable devices, desktop computers (76 percent) and laptops (65 percent) remain the most ubiquitous, but mobile devices – corporate-owned as well as employee-owned – are creeping up the list.
Anti-Malware Landscape

Some standout statistics to introduce this section:

- 66 percent of respondents say efficacy is the top factor when evaluating an endpoint anti-malware solution.
- 51 percent say detecting APT is the biggest flaw not addressed by their current solutions.

Full results ahead.

When you're evaluating or purchasing an endpoint anti-malware solution, what's the most important factor?

<table>
<thead>
<tr>
<th>Factor</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Efficacy—ability to prevent, detect and remEDIATE malware</td>
<td>66%</td>
</tr>
<tr>
<td>Client performance—performance impact on the endpoint</td>
<td>16%</td>
</tr>
<tr>
<td>Management—ability to easily manage, configure, and get reporting on endpoints</td>
<td>15%</td>
</tr>
<tr>
<td>Deployment—easy to install</td>
<td>3%</td>
</tr>
</tbody>
</table>

Client performance, deployment, management – each of these factors is second by a longshot to efficacy when it comes to evaluating or purchasing an endpoint anti-malware solution. Sixty-six percent of respondents select “efficacy” as their top factor, saying they most value the “ability to prevent, detect and remediate malware.”

66 percent of respondents say efficacy is the top factor when evaluating an endpoint anti-malware solution.
Survey Results

Which of these vendors do you currently engage with for anti-malware/endpoint security protection? (select all that apply)

- Malwarebytes: 45%
- Symantec: 29%
- Trend Micro: 18%
- Kaspersky: 16%
- Intel Security (McAfee): 13%
- Cisco AMP for Endpoints/SourceFire: 11%

Asked which current vendors they engage for anti-malware/endpoint protection, 45 percent of respondents choose Malwarebytes. Twenty-nine percent name Symantec, while 18 claim Trend Micro.

Which of the following applies to your current anti-virus solution?

- We use an on-premise management console: 74%
- We use a cloud-based (vendor hosted) web management console: 15%
- Our endpoints are unmanaged: 7%

Asked to describe their current solutions, 74 percent of respondents say they use on-premise management consoles. Only 15 percent currently use a cloud-based, vendor-hosted solution.

Why the resistance to cloud?
**Survey Results**

What concerns (if any) do you have around cloud-based (vendor-hosted) web management consoles? (select all that apply)

- **The ability of my vendor to keep my data secure**: 48%
- **Compliance issues or regulatory concerns**: 38%
- **My endpoint data is not stored within my internal network**: 36%
- **No concerns**: 28%

Top concern, shared by 48 percent of respondents, is “the ability of my vendor to keep my data secure” – the recurrent complaint of those who question cloud security.

Other factors: compliance of regulatory concerns (38 percent) and because endpoint data is not stored within internal networks (36 percent).

Which problems are *not* being solved by your current anti-virus solution? (select all that apply)

- **Detecting advanced persistent threats**: 51%
- **Zero-day malware**: 37%
- **Zero-day exploits**: 35%
- **Mobile device vulnerabilities**: 34%
- **Cleaning infected endpoints**: 31%

Finally, when asked what problems are *not* being solved by current anti-malware solutions, 51 percent point to detecting advanced persistent threats. Thirty-seven percent say it is zero-day malware, while 34 percent cite mobile device vulnerabilities.

With the topic of detection fresh, the report next delves into results related to detection and response.
Detection, Response

One of the key numbers that jumps out from this section:

- 76 percent of respondents say they rely on a centralized anti-virus solution to detect malware incidents.

The following charts reveal other top responses related directly to detection and response.

How do you currently detect malware incidents within your organization? (select all that apply)

<table>
<thead>
<tr>
<th>Method</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>We rely on a centralized anti-virus solution</td>
<td>76%</td>
</tr>
<tr>
<td>We use an IDS or IPS</td>
<td>40%</td>
</tr>
<tr>
<td>We use a secondary anti-malware scanner on our endpoints</td>
<td>33%</td>
</tr>
<tr>
<td>We use an endpoint detection and response (EDR) solution</td>
<td>21%</td>
</tr>
<tr>
<td>We manually review endpoint anti-virus logs</td>
<td>19%</td>
</tr>
<tr>
<td>We use a SIEM to collect and correlate log data</td>
<td>16%</td>
</tr>
<tr>
<td>We use a network sandbox</td>
<td>10%</td>
</tr>
</tbody>
</table>

From the range of responses, one can conclude that detection is a mixed bag. While three-quarters of respondents rely on centralized anti-virus solutions, 40 percent use intrusion detection/prevention systems, and 33 percent say they have a secondary anti-malware scanner on their endpoints.

76 percent of respondents say they rely on a centralized anti-virus solution to detect malware incidents.
When malware is detected in your organization, how are you first notified about the incident?

When malware is detected, 45 percent of respondents say they are first notified via email. Twenty-five percent are alerted by their end users or the help desk.

But once detected, what happens next?

How do you primarily deal with malware infections once they are discovered? (select all that apply)

Seventy-three percent say they disconnect or isolate the infected system from the network. Sixty-one percent say they reimagine the compromised system, and 52 percent use a third-party malware cleanup tool.

The next section delves into one of the report’s hot topics: reporting and analytics.
Survey Results

**Reporting and Analytics**

**In terms of system dashboards, what data is the most important to have available at a glance?**

- **Summary of detections that require action**: 55%
- **Endpoints that have not checked into the management console recently**: 19%
- **Summary of top users who have been infected over the past x days**: 10%
- **I use my SIEM as a central system dashboard**: 9%

Asked to prioritize, 55 percent of respondents say that, for a system dashboard, the most important data for them is to see a summary of detections that require action.

**In terms of the ability to generate reports, which data is the most critical to you?**

- **Malware infections during a specific date interval**: 32%
- **Top users who have been infected**: 22%
- **Malware dwell time**: 14%
- **We use our SIEM for reporting**: 8%
- **Blocked malware**: 7%

For report generation, 32 percent say the most critical data is malware infections during a specific date interval, while 22 percent want to see the top users who have been infected.

Next: a brief look at software deployment and administration.
Software Deployment and Administration

How much time do you usually spend administering your anti-virus central management console?

- Less than 30 minutes daily: 64%
- Only when necessary: 21%
- 1-2 hours daily: 8%

The majority of respondents – 64 percent – spend less than 30 minutes daily administering their anti-virus central management console. Twenty-one percent have no set schedule at all, administering only when deemed necessary.

What is your ideal schedule for performing software updates?

- Weekly: 4%
- Monthly: 58%
- Quarterly: 18%
- Annually: 4%

As for software updates, 58 percent prefer to receive these monthly, while 18 percent would even settle for quarterly.

With these preferences in mind, prepare to review the 2017 anti-malware agenda.
2017 Agenda

Key points to consider upfront here:

• 98 percent of respondents expect the same or more budget for anti-malware in the year ahead.
• 82 percent say their top priority is to improve detection.

The following charts reveal other top responses related directly to detection and response.

What are your biggest anti-malware priorities over the next 12 months? (select all that apply)

No equivocation here. A resounding 82 percent of respondents say their 2017 goal is to improve detection of malware. Placing a distant second is improve reporting and analytics (48 percent), while improve response time is third (41 percent).

No equivocation here. A resounding 82 percent of respondents say their 2017 goal is to improve detection of malware.
How will your budget for endpoint protection/anti-malware change in the coming year?

- Increase greater than 10 percent: 8%
- Increase of 6-10 percent: 8%
- Increase of 1-5 percent: 25%
- No change: 57%
- Decrease: 2%

Resources are not a constraint. Fifty-seven percent of respondents expect no change to their current budgets for endpoint protection/anti-malware, while 41 percent expect some sort of an increase – some in excess of 10 percent. Only two percent expect a budget decrease.

What will leaders do with these funds?

Where specifically do you plan to invest new resources? (select all that apply)

- On-premise anti-malware tools: 54%
- User training: 51%
- Cloud-based anti-malware tools: 24%
- Managed/professional services: 20%
- Increased staffing: 8%

The top priority for 54 percent of respondents is to invest in on-premise anti-malware tools. Fifty-one percent want to focus more on user training, and nearly one-quarter (24 percent) are eyeing new cloud-based anti-malware tools.

What can we draw from the results? How can they inform 2017 anti-malware strategies?

Survey conclusions come next, followed by exclusive analysis of the results from Justin Dolly of Malwarebytes.
Conclusions

Before shifting to 2017, it’s important to reflect on the state of anti-malware in 2016. And the statistics from this report’s introduction are quite telling:

- 25 percent of respondents say their organizations struggle with threat detection.
- 51 percent say their current anti-virus tools have difficulty detecting APTs.
- 54 percent say their organizations have experienced ransomware in the past year.

The message could not be clearer: Despite the energy and resources organizations have poured into the fight against malware – the AV solutions, intelligence feeds, user training and detection tools – it isn’t enough.

To have any hope at all of achieving greater success against ransomware and advanced threats in 2017, security leaders need to be prepared to take on a whole new strategy. Toward that end, here are four points for consideration:

1. New Mindset Required

Malware defense was much simpler in the old days, when you just needed a current anti-virus solution to weed out the known threats as they lined up at your door. Today, the unknown threats are a bigger concern than the known, and they multiply at a rate at which no point solution can keep pace. Old tools and old skills just can’t be effective against threats such as ransomware, which evolve constantly to retain their edge.

2. Ransomware Can Be Your Friend

Sounds contradictory, but truly the outbreak of ransomware can be the security leader’s friend – if leveraged correctly. High-profile ransomware incidents have made board members and senior management keenly aware of the business and reputational risks of ransomware. Use their awareness to your advantage. Demonstrate where your organization is most vulnerable to ransomware and other emerging threats; show which security solutions are hopelessly outdated; and turn this into a means of building a stronger business case for the additional resources you need.

3. Think Beyond Detection

There is a strong sentiment from survey respondents that their organizations are particularly deficient in detection tools. But, frankly, in an environment where malware variants evolve quickly, detection is a more elusive target than response. Organizations need to be skilled and tooled to respond quickly and properly to malware threats. That means a strong emphasis on detection, of course, but also on threat intelligence (to be aware of the latest strains), on having secure, offline backups, and to have a team, tools and procedure in place to be able to isolate “patient zero” when there is an infection, and keep that infection from spreading.

4. Augment Your Team

That old political slogan is: It takes a village. When it comes to fighting ransomware and advanced threats, no one solution – no one individual – can do it alone. It takes an internal team armed with the latest intel and the most flexible solutions, and it likely also takes cloud-based solutions and third-party expertise to have your response at the high level of readiness required. Fighting malware is more than a full-time job. It’s now a mission, and your organization may need external tools and forces to support this mission.

Next, in Survey Analysis, Justin Dolly, CIO and CISO of survey sponsor Malwarebytes, offers his unique take on what these survey results mean and how your organization should respond to them.
How to Evolve Our Approach to Defending Against Malware

Survey Analysis by Justin Dolly, CIO and CISO at Malwarebytes

NOTE: In preparation of this report, ISMG VP Tom Field sat down with Justin Dolly, CIO and CISO at Malwarebytes, to analyze the results and discuss how security leaders can put these findings to work in their organizations. Following is an excerpt of that conversation.

The Big Picture

TOM FIELD: Overall, what's your gut reaction to our survey results?

JUSTIN DOLLY: I was surprised that companies seemed to be satisfied with the anti-malware tools they have when, at the same time, more than half say they have faced ransomware in the past year. In addition to that, more than 50 percent say they also have no way to see any form of an advanced persistent threat. Obviously, you look for those threats in different ways, but it does seem to be coming out of both sides of their mouths.

The CISO's lot in life may not necessarily be harder than everyone else's, but the bad guys get an incredibly wide target at which to aim. And there are so many areas where CISOs and security teams have to strengthen the security posture of an organization.

Ransomware is a relatively new attack tool. In a survey that we sponsored, nearly 50 percent of companies in the U.S. were victims of some form of a ransomware attack in the past year. So it's dramatically on the rise. And organizations have a hard enough time struggling with the existing tools they have while also trying to figure out the best ways to strengthen their posture against this type of attack. Companies need to find an answer for it.

Ransomware Readiness

FIELD: How do you assess what organizations have told us about their general readiness for ransomware?

DOLLY: More than half of them have experienced some form of ransomware attacks or events in the past year.

“I was surprised that companies seemed to be satisfied with the anti-malware tools they have when, at the same time, more than half say they have faced ransomware in the past year.”
“We've seen a 259 percent increase in ransomware delivered via exploit kits, in a five-month period, from December 2015 to May 2016.”

And other survey data out there says more than 40 percent of ransomware victims pay the ransom. And these ransoms range from $1,000 to $10,000 for a small business to hundreds of thousands of dollars for larger enterprises.

At the Malwarebytes' Labs, we’ve been laser-focused on the ransomware threat, and we've seen a 259 percent increase in ransomware delivered via exploit kits in a five-month period, from December 2015 to May 2016.

Ransomware is also evolving at a much faster rate, and has a more advanced code base than any code base we've ever seen. And none of this is surprising, because more than 40 percent of victims are paying the ransom. As long as it remains lucrative, ransomware attacks will keep going up.

It’s incumbent upon all of us to figure out how to combat ransomware. And some of those methods aren’t that technical. For example, if you keep very recent backups of your databases, endpoints and so on, particularly if those backups are cloud based, you likely won’t have to pay the ransom because the data is safe somewhere else. Then you can clean up your machine, remove all the malware from it, and invest in tools to ensure you avoid becoming a victim of the same type of attack in the future.

Beyond Ransomware

FIELD: How ready do you sense our respondents are to encountering other strains of malware beyond ransomware?

DOLLY: As we discussed, malware, including ransomware, is becoming more complex. Newer malware variants are coming out every hour or two, in some cases. It’s very difficult to keep up and a very hard thing to do part-time. Many companies have a makeshift security team, consisting of ops, forensics, risk management and compliance teams, among others. But few companies have security analysts who are 100 percent focused on emerging threats because more often than not, they can’t justify it financially. Instead, a majority of companies will focus on intelligence gathering, asking themselves:

- What tools are they currently using?
- What tools do their users use?
- What does their security posture look like?
- What types of threats and attacks are they vulnerable to?

Security Gaps

FIELD: Justin, what are some of the biggest gaps our respondents face in baseline detection and response capabilities?

DOLLY: While the industry has gotten a lot better at detection, response is another matter. The only metric that matters is how quickly you can intelligently respond to a malware outbreak or a breach. Do you have the telemetry to know exactly where patient zero is? How quickly can you get into that environment and do something about it? Have you deployed security technologies that will allow you to take action? It’s akin to a fire breaking out when you have hundreds or thousands of acres. If it breaks out in a certain area and is fairly contained, how quickly can you get to it before it spreads?

I tend to measure that metric in minutes. How many minutes does it take you to respond to a malware outbreak or a security breach within your environment? How do you even know something bad has occurred? Do you know what good behavior is in your environment, and can you determine bad behavior through anomaly detection? And then do you have the ability to take action? Do you have a device or some form of a filtering tool for those specific environments? And if you segmented those environments, can you quarantine that environment, so that it doesn’t impact the larger organization? I think most companies have a long way to go in those areas.
“While the industry has gotten a lot better in detection, response is another matter.”

Focusing Resources in 2017

FIELD: Ninety-eight percent of our respondents said they expect level funding or increased budgets in the coming year. So with those kind of resources, what’s your advice for how they should best invest them?

DOLLY: The security industry has shifted an awful lot over the last five years or so. We’re moving away from some of the traditional security technologies, which, for a lot of organizations, still solve a problem for them. But an awful lot of security technologies and capabilities today are delivered by cloud-based solutions. If I were to go back, say, 15 years to a meeting of CISOs and say, “Hey, let me tell you something. In the not too distant future, you’re going to adopt security technologies that live in the cloud, not inside your own network or even your own building. And a service provider will manage them,” there would be a lot of skeptics in the room. Similarly, if you told them their directories and credential management solutions would be in the cloud, they would probably recoil.

But more and more organizations are leveraging cloud solutions like Amazon, Azure, VMware and others for much of their production infrastructure, if not quality assurance and testing. Every quarter, we see the numbers go up. Increasingly we’re moving into this nimbler, more modern environment, and so we have a duty to secure those environments.

Organizations need to start focusing on locating the data that they need to secure and determine whether they still need those three layers of firewalls at the edge of their networks to protect it. Security programs should be 100 percent directed at securing high-value assets, because you can’t secure everything. So, they need to examine these newer technologies and more flexible solutions to see whether they make sense.

And they won’t make sense for every organization. Some companies will continue to run the way they did 25 years ago because their environment may be exactly the same. But for those of us in dynamic organizations, modern solutions to modern problems is the only way to go.

Malware in 2017

FIELD: Looking ahead, what are the overall malware trends that most concern you?

DOLLY: Ransomware is still very much on the rise, and also evolving very fast. The code base is becoming more advanced, and the techniques are getting more and more elegant, if you will. The bad guys are getting smarter, figuring out how to write these things better and how to hide them better. That makes it especially important for us to be able to identify these new techniques so that we have the capability to pivot and make sure we’re getting in front of the attack vectors they’re moving toward.
“This survey is so powerful because it casts a very wide net. You can say, 'These are what the outside trends look like, and we’re part of that trend.'”
“[U]se these survey results and our analysis to tell a story. ... [D]evelop your talking points, and don’t bludgeon them over the head with technology in trying to articulate your point.”

Put Study to Work

FIELD: How can our audience best use our analysis of the survey results and make a difference in their own organizations?

DOLLY: You’ve hit on something that I have spent a lot of time focusing on over the last few years. There seems to be a disconnect between security teams and the leadership at companies. It’s very important for security teams – whether they’re a CISO, manager of information security or whomever – to take the very technical day-to-day aspects of running a security program and translate that into a language that the board of directors and C-level executives can easily consume.

My advice is to use these survey results and our analysis to tell a story. There’s no sense in raising your voice or waving your hands over your head. Fear may be a great motivator, but because the board is already conditioned to focus on risks, they’re already a risk-aware body of professionals.

So don’t scare them. Use it to inform them. Give them little sound bites they can use, and don’t walk in there with a slide that has 14 bullets and lots and lots of acronyms, because they’re simply not going to be able to understand most of that. And if they seek to understand it, that’s going to be the longest presentation you’ll ever give.

So, when you get that opportunity, make sure that you understand your audience, develop your talking points, and don’t bludgeon them over the head with technology in trying to articulate your point. This survey is so powerful because it casts a very wide net. You can say, “These are what the outside trends look like, and we’re part of that trend. And so, these are the emerging threats, the technologies we should focus on, the problems we need to solve.” And then articulate that story by applying it to what’s happening within your own organization.

That’s where this survey becomes really valuable. I use them in those ways, and I hope others do too.
About ISMG

Information Security Media Group (ISMG) is the world’s largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from the North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401
sales@ismgcorp.com