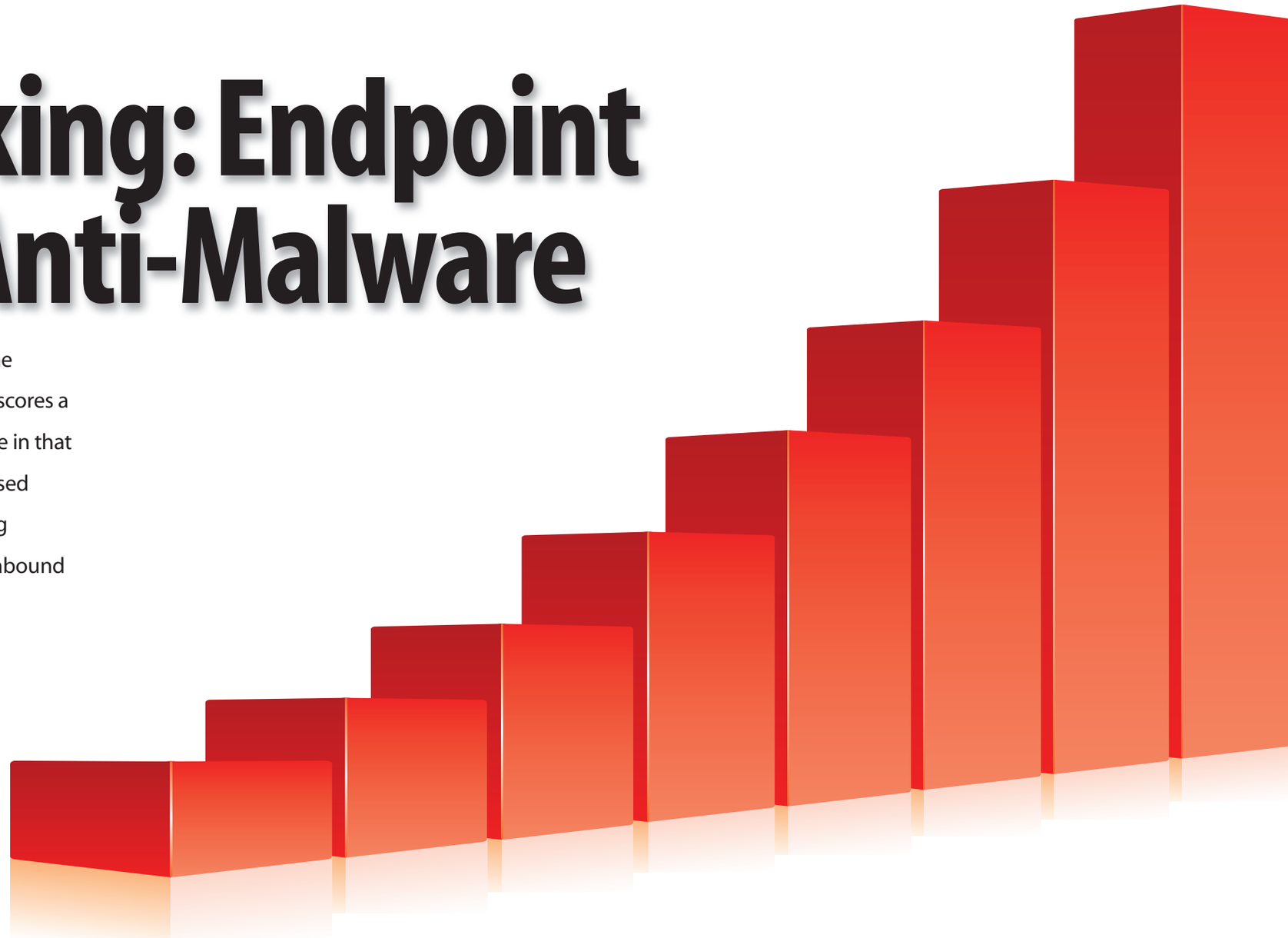
InformationWeek
reports

Reports.InformationWeek.com February 2012 $99

Next

IT Pro Ranking: Endpoint Antivirus/Anti-Malware



Kaspersky Lab and Sophos top our IT evaluations of nine antivirus/anti-malware vendors. Upstart Malwarebytes scores a **4.3** out of **5** for malware removal, the highest score in that category. Symantec and McAfee are the most widely used vendors, but **46%** of respondents are considering replacing or adding a vendor. Lucky for them, choices abound in this market.

By Kurt Marko

Report ID: R4130212

TABLE OF CONTENTS

Figures

EXECUTIVE SUMMARY

Our *InformationWeek* 2012 Antivirus and Anti-malware Vendor Evaluation Survey asked 386 IT professionals to gauge their impressions of AV/anti-malware vendors. We asked respondents to only rank vendors they've used or evaluated within the past 12 months. The core of our survey asked two sets of questions: one focused on overall vendor performance, including price, general performance and product reliability, and the other focused on product-specific features such as virus and malware detection and removal.

Our respondents rated nine vendors. Kaspersky Lab and Sophos earned the highest ranking for overall performance, closely followed by Avast Software and Malwarebytes. Note that only six percentage points separated the leaders from the last-place finisher, Trend Micro. Kaspersky and Sophos also took the top two spots for AV/anti-malware features. The spread was wider here, with 10 points separating first and last place.

While smaller players took top honors, brand name vendors still dominate IT's radar. When we asked respondents to select up to three vendors they use, or have used or evaluated in the past 12 months, 42% said Symantec and 36% said McAfee. Compare that to 10% of respondents who use or have used or evaluated Kaspersky. It's clear that brand names resonate with IT, but there's ample opportunity for smaller players to grab a bigger slice of the market.

This report analyzes the survey results, provides some product evaluation and purchase advice, and highlight changes in the threat landscape in the ongoing arms race between cyber vandals and anti-malware developers.

Note that our survey started with 20 antivirus/anti-malware vendors, but only nine received a sufficient number of responses to qualify for a full evaluation.

Protection From a Dirty Internet

The Internet is a cesspool awash in viruses and malware, and your users wade in it for hours and hours a day. Malware has multiple entry points onto a computing device, from spam to compromised Web sites to drive-by exploits that compromise browser plug-ins such as Flash and PDF viewers, to infected thumb drives that pass from user to user. And now mobile devices are becoming targets via malware wrapped inside seemingly innocuous apps.

Fortunately, anti-malware software options have never been more abundant. While client anti-malware isn't enough to defeat the barbarians at your corporate gate, it is a critical piece of a layered defense.

Kaspersky Lab and Sophos earned the highest scores for overall performance in our IT vendor evaluation of nine AV and anti-malware endpoint software providers. Both companies achieved 76% out of a possible score of 100% (see, Figure 1, right). Avast Software and Malwarebytes were close behind, each earning scores of 75%.

These performance ratings are almost the inverse of our chart on vendors being used or evaluated; here Symantec and McAfee dominate, with results up to four times as high as three of the four top performers (see Figure 2, page 5). However, as our results show, IT pros'

Figure 1

Antivirus and Anti-Malware Software Overall Vendor Performance

Weighted, aggregated score across all 10 evaluation criteria, with maximum possible score of 100%

Base: Varies
R4130212/5
Data: *InformationWeek* 2012 Antivirus and Anti-Malware Vendor Evaluation Survey of 386 business technology professionals, December 2011

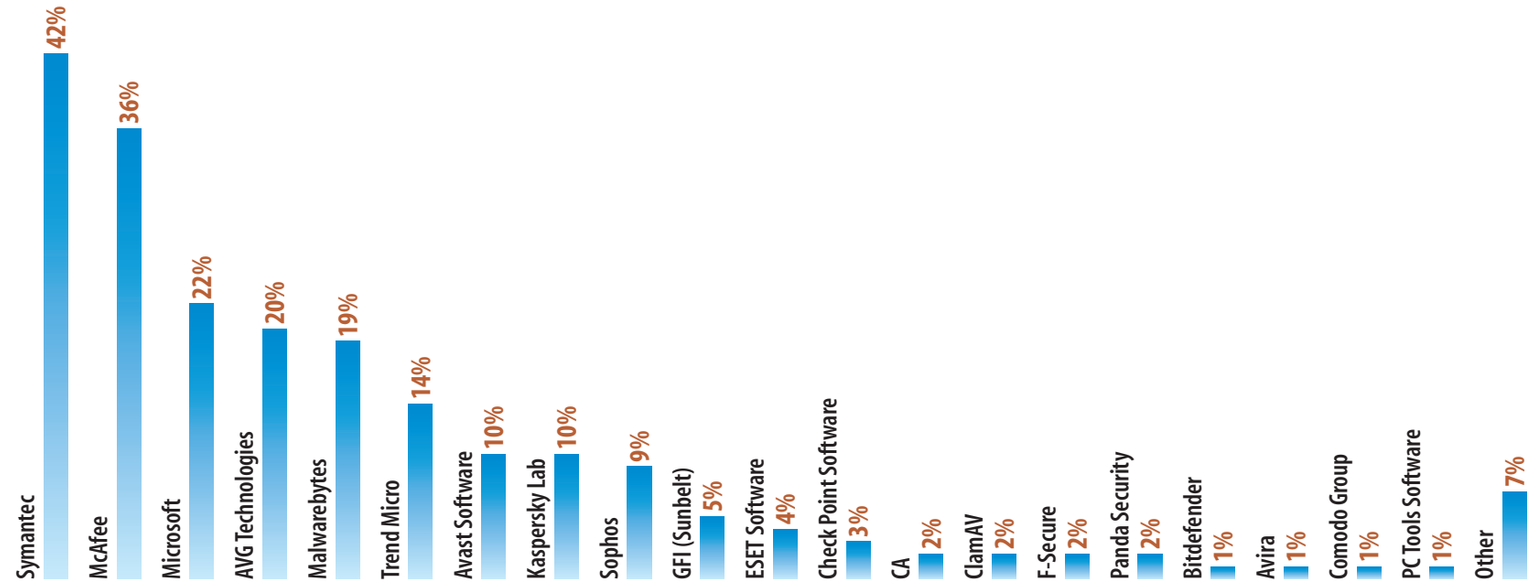
preferences aren't dictated by a vendor's size or brand name.

Our performance rating is based on a set of 10 evaluation criteria (see Figure 3, page 6). Product reliability and performance are clearly the most important attributes, while cost and adaptability occupy the next tier in our respondents' decision hierarchy. Service, support and innovation aren't high on product evaluation check lists: a fortuitous result for vendors, since almost all get mediocre scores in those areas. You can see how each vendor fares on the performance evaluation criteria in Figure 4, page 7.

Figure 2

Vendors in Use or Evaluated

Which of the following client-based antivirus or anti-malware software vendors are you currently using or evaluating, or have you used or evaluated within the past 12 months?



Note: Three responses allowed
Data: *InformationWeek* 2012 Antivirus and Anti-Malware Vendor Evaluation Survey of 386 business technology professionals, December 2011

R4130212/1

Diving into the details provides some insight on how IT arrived at the scores they assigned to vendors. Despite being the most prevalent products among our respondents, McAfee and Symantec are clearly not the value leaders, badly lagging their seven competitors on both acquisition and operational cost. However, size does have its advantages, as both lead, along with Sophos, in breadth of product line.

Product performance and reliability are the areas where smaller or foreign-based (and

FAST FACT

42%

Respondents who are using, evaluating or have used or evaluated Symantec antivirus/ anti-malware software.

consequently less popular among our predominantly domestic respondents) vendors really shine, with relative newcomer Malwarebytes a notable standout. The three-year-old company, whose origins trace to a lone developer writing code to rid his home PC from a malware infestation, passed 100 million downloads of its freemium product in July 2011 and is adding a million users a month, according to the company.

One area where all the vendors get a barely passing grade is sales support and service; all of them tightly bunched with ratings in the low 3's. This is a bit surprising, since one would think that the larger and more expensive vendors would use their big R&D budgets and legions of sales staff and support technicians to distinguish themselves from smaller competitors, but our survey doesn't support this.

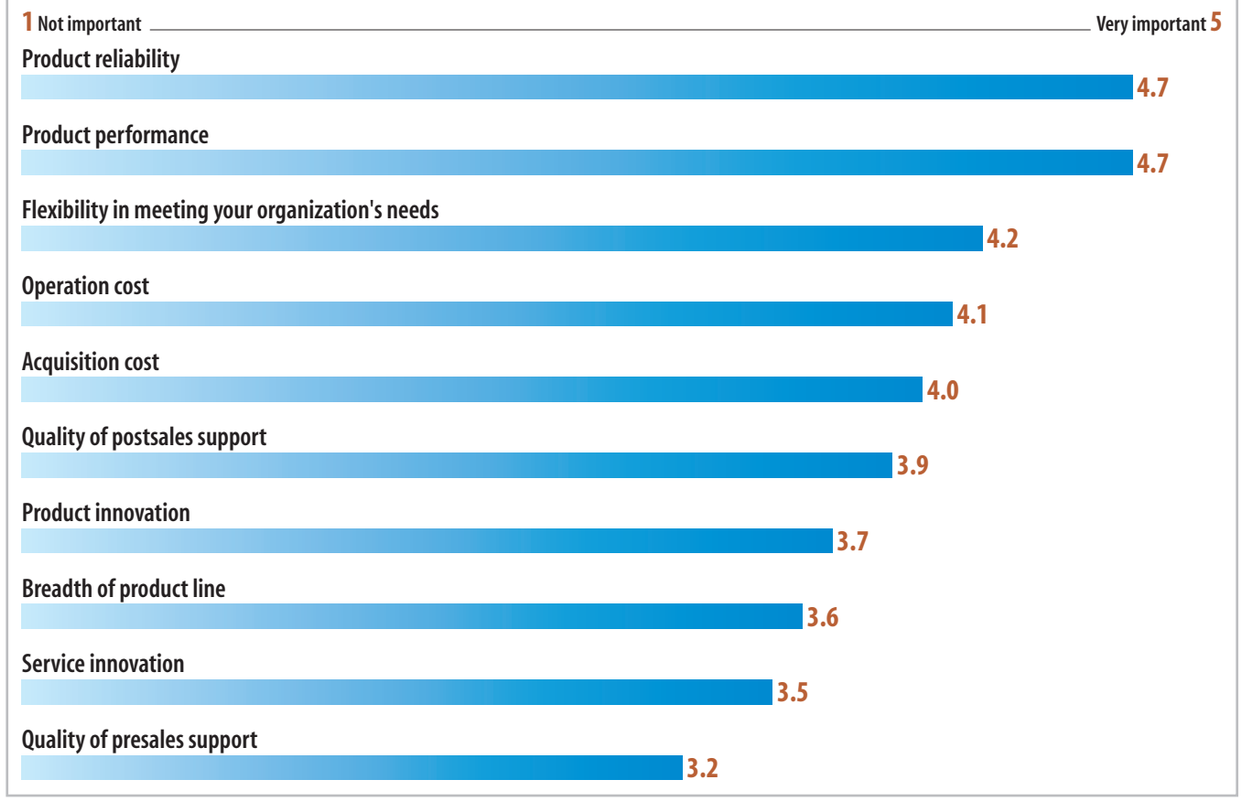
Rating the Malware Fighters

In addition to rating vendors on general performance criteria, we also asked IT to rate products they've used or evaluated based on 11 anti-malware and AV features. These fea-

Figure 3

Importance of Evaluation Criteria

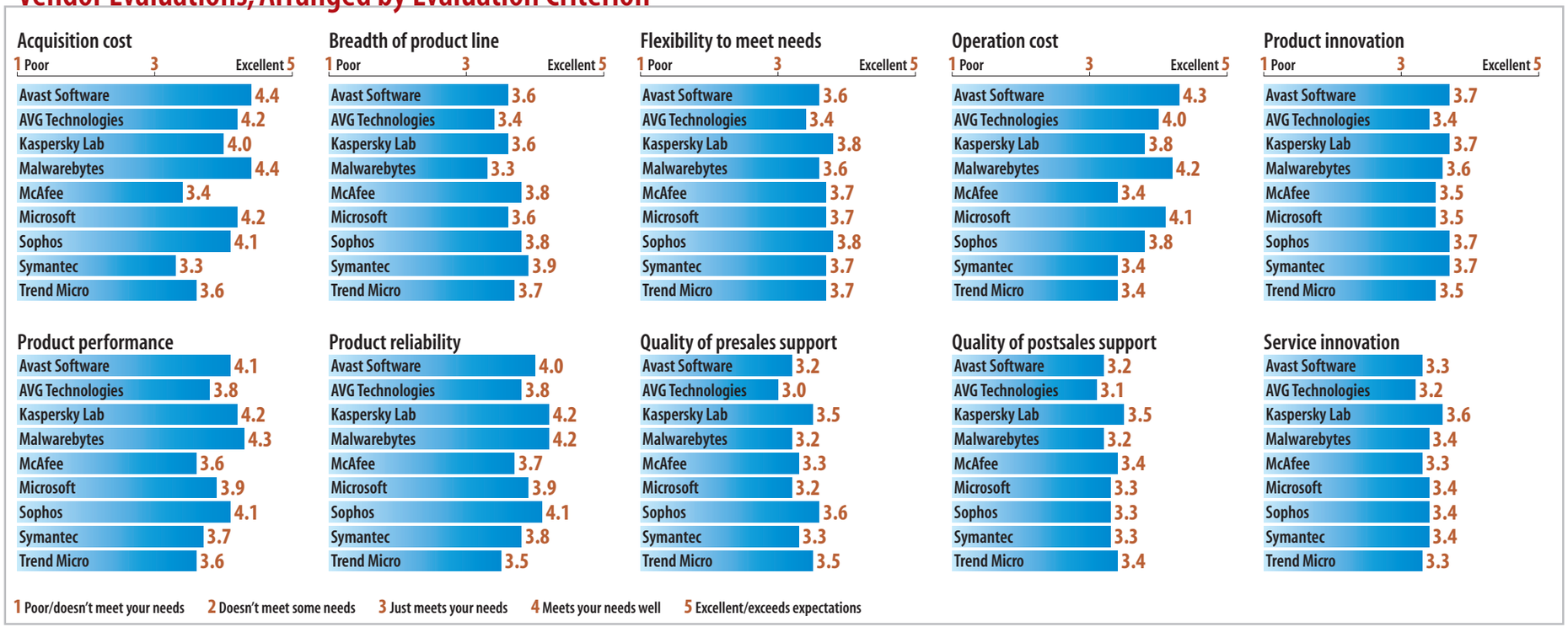
How important are the following criteria when evaluating solutions from client-based antivirus or anti-malware vendors? Please use a scale of 1 to 5, where 1 is "not important" and 5 is "very important."



Note: Mean average ratings R4130212/2
Data: *InformationWeek* 2012 Antivirus and Anti-Malware Vendor Evaluation Survey of 386 business technology professionals, December 2011

Figure 4

Vendor Evaluations, Arranged by Evaluation Criterion



Note: Mean average ratings
Base: Varies
Data: *InformationWeek* 2012 Antivirus and Anti-Malware Vendor Evaluation Survey of 386 business technology professionals, December 2011

R4130212/4

tures include malware and virus detection, malware and virus removal, and impact on device performance. IT rated the ability to detect malware before it executes, and accuracy of detection, as the most important criteria, with malware removal close behind (see Figure 5, page 8).

The overall feature ratings again finds Kaspersky at the top of the list at 83%, with Sophos in second with 81% (see Figure 6, page 9). Avast and Malwarebytes both earned a score of 79%. The four leaders excel

at all aspects of threat detection: accuracy and detection of viruses and malware either before or after installation or execution. For instance, Kaspersky, Malwarebytes and Sophos all score 4.4 out of 5 on detection accuracy. Kaspersky, Sophos and Avast all score highest on detecting malware before it installs or executes. This is a critical feature, given the potential difficulty of cleaning an infected system; it's far better to keep the malware off a device in the first place.

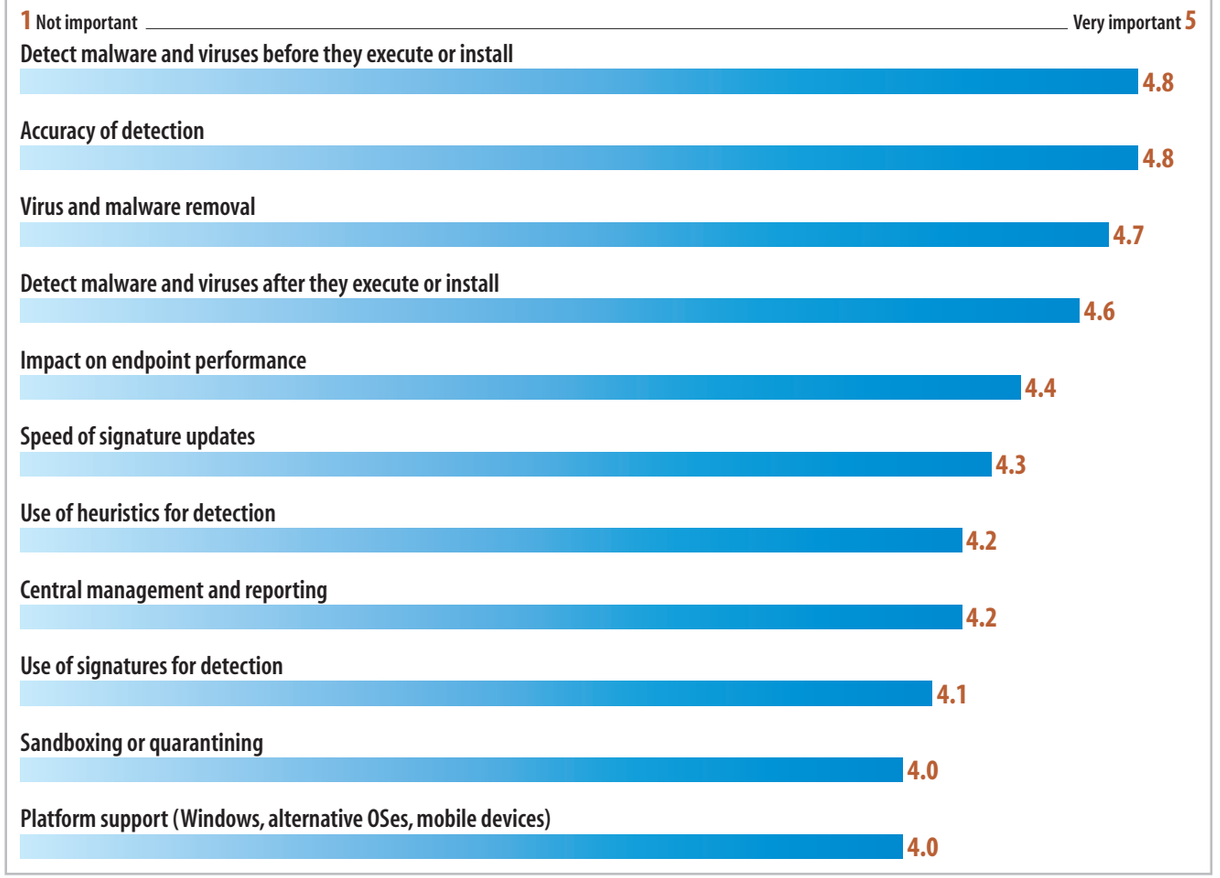
The top four vendors also lead the ratings for speed of signature updates, their signature and heuristic detection technology, and malware removal effectiveness. In fact, Malwarebytes bests all comers in this category, earning a 4.3 out of 5. You can see each vendor's average rating for each feature in Figure 7, page 10.

Symantec anchors the upper middle ground at 78% through good, but not outstanding scores across the board, with the notable exception of impact on system performance, where it lags badly. AVG Technologies falls to the bottom of the pile when it comes to AV/anti-malware features, scoring

Figure 5

Importance of Antivirus and Anti-Malware Software Features

Please rate the importance of these features in your client-based antivirus and/or anti-malware software using a scale of 1 to 5, where 1 is "not important" and 5 is "very important."



Note: Mean average ratings R4130212/10
Data: *InformationWeek* 2012 Antivirus and Anti-Malware Vendor Evaluation Survey of 386 business technology professionals, December 2011

just 73%, which is a 10-point spread between it and leader Kaspersky.

While Malwarebytes is the value and performance leader, it definitely isn't the product for those looking for a strong set of central management and reporting features, bringing up the rear in this category. By contrast, this was the only category in which McAfee stood out, earning the highest rating of 4.0. And despite Microsoft's good overall showing, it is still a parochial, Windows-only shop, as evidenced by its dismal showing, four-tenths of a point behind the rest of the pack, in platform support.

We also show the feature results broken out by vendor (see Figure 8, page 11). You can see that most of the vendors fared OK across most of the categories. No vendor scored below a 3, which in our survey means the vendor just meets your needs. In other words, IT may not be thrilled with the product, but it gets the job done.

In fact, the vast majority of our respondents are satisfied with their current endpoint AV/anti-malware products, with a mere 4% voicing outright dissatisfaction (see Figure 9, page 12). That's good news for larger vendors such as Symantec and McAfee.

However, that doesn't mean IT buyers are content to ignore alternatives. A full 29% are considering replacing their primary or sec-

FAST FACT

83%

Weighted aggregate score based on 11 features rated for Kaspersky Lab.

Figure 6

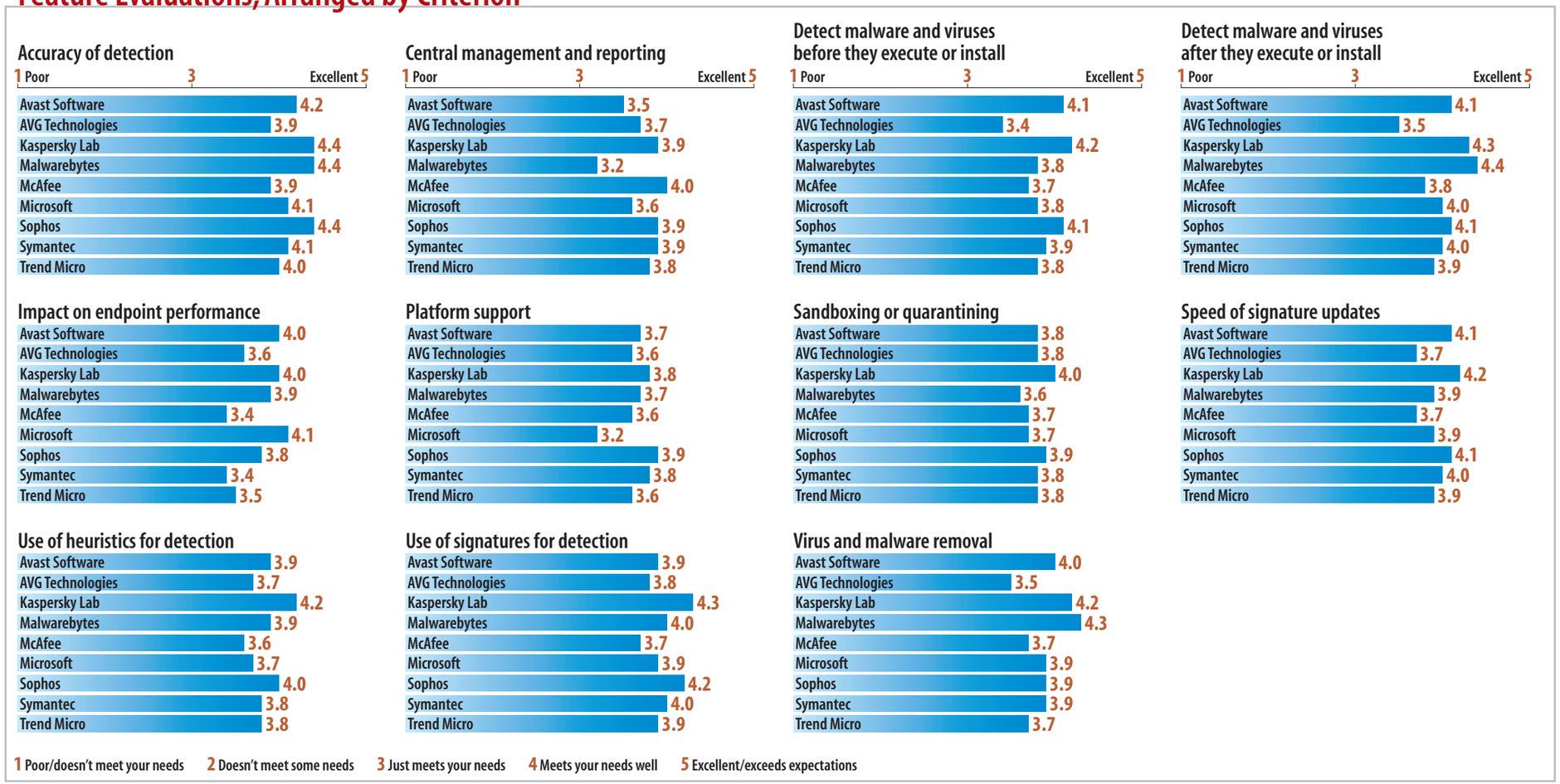
Antivirus and Anti-Malware Software Vendor Performance: Features

Weighted, aggregated score across all 11 features evaluated, with maximum possible score of 100%

Base: Varies R4130212/13
Data: *InformationWeek* 2012 Antivirus and Anti-Malware Vendor Evaluation Survey of 386 business technology professionals, December 2011

Figure 7

Feature Evaluations, Arranged by Criterion

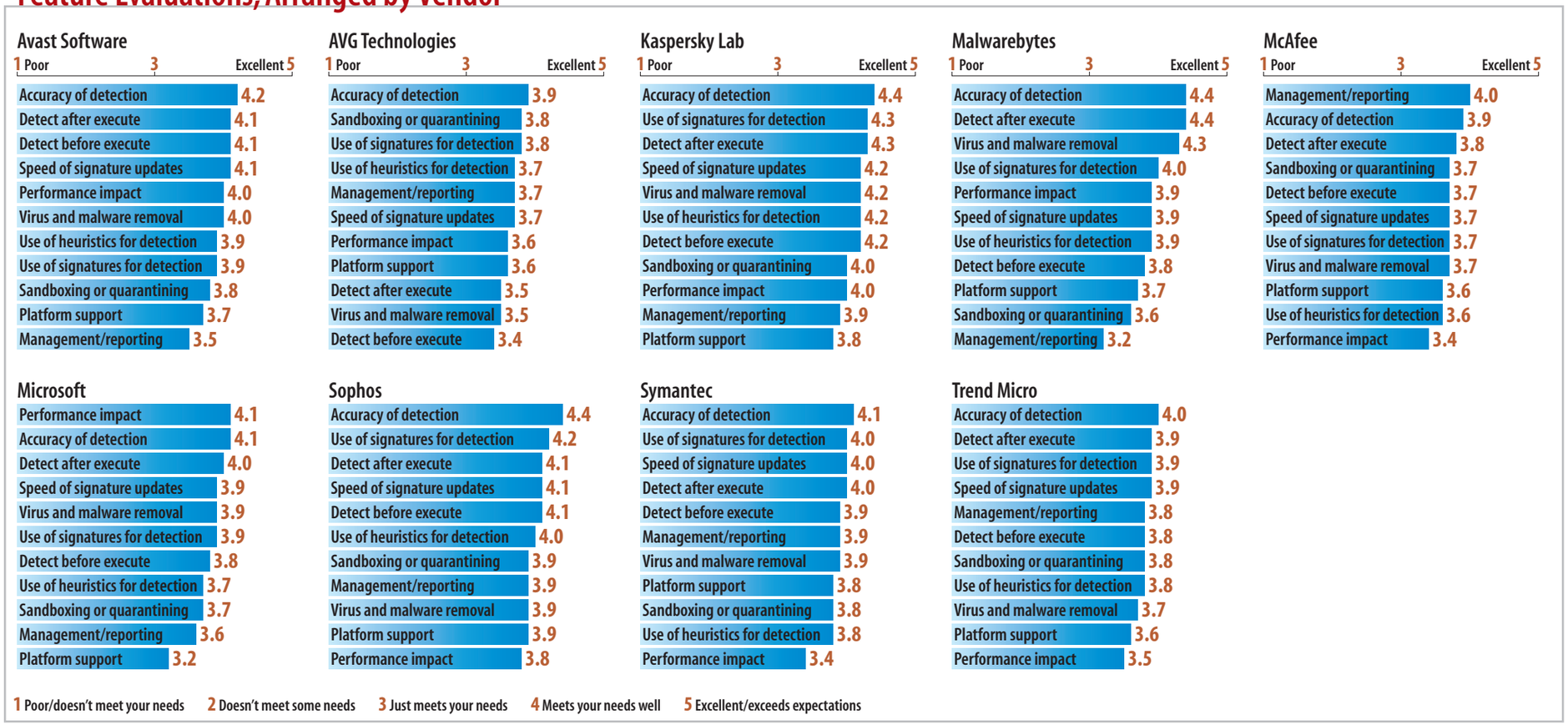


Note: Mean average ratings
Base: Varies
Data: *InformationWeek* 2012 Antivirus and Anti-Malware Vendor Evaluation Survey of 386 business technology professionals, December 2011

R4130212/12

Figure 8

Feature Evaluations, Arranged by Vendor



Note: Mean average ratings
Base: Varies
Data: *InformationWeek* 2012 Antivirus and Anti-Malware Vendor Evaluation Survey of 386 business technology professionals, December 2011

R4130212/11

ondary vendors, with another 17% thinking about adding a new one (see Figure 10, page 13). The reasons for such receptivity to change are almost entirely rooted in a desire to improve product performance and reduce capital and operational costs. Over 60% of our respondents that are considering replacing their current vendor or adding another cite performance as a key reason (see Figure 11, page 14). Similarly, for those not currently ready to pull the plug, price and performance are the deciding factors that could get them to change their minds (see Figure 12, page 15).

The rise in mobile devices complicates endpoint security because IT now has another platform to manage—assuming that IT has any control whatsoever over the device. In our survey, 12% are using a software suite to protect mobile devices, while 9% use standalone antivirus/anti-malware software (see Figure 13, page 16). The majority in our survey are still trying to get their arms around the issue: 40% of respondents are evaluating protection software for mobile devices.

FAST FACT

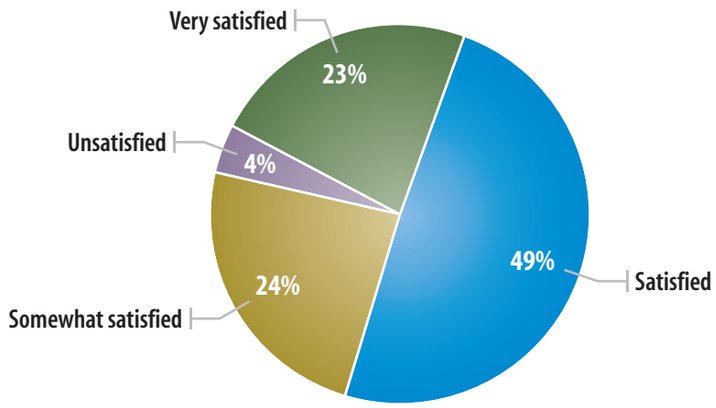
72%

Respondents very satisfied or satisfied with their current client-based antivirus or anti-malware products.

Figure 9

Satisfaction With Antivirus and Anti-Malware Products

What is your level of satisfaction with your current client-based antivirus and/or anti-malware product or products?



Data: *InformationWeek* 2012 Antivirus and Anti-Malware Vendor Evaluation Survey of 386 business technology professionals, December 2011 R4130212/6

The Evolution of AV

When evaluating client security software, the very term "antivirus software" is hopelessly inaccurate given the complexities of today's endpoint protection problem, the multiplicity of threat types and the consequent growth in endpoint security feature sets. Point products have almost entirely been subsumed into endpoint security suites whose mission is an all-encompassing security umbrella with a unified user and management interface. This market reality is manifest in our survey, with a majority of our respondents exclusively using software suites and another 17% a mix of suites and point products (see Figure 14, page 17).

The core endpoint security feature set for

PCs and laptops typically includes: antivirus, anti-spyware and malware removal, using both signature-based and heuristic algorithms. Also included are a client-side firewall, which often supports security controls for specific Web applications (like Facebook or Gmail), real-time system integrity checks, and a host-based network intrusion detection/protection system. Some endpoint suites now include other client security features like disk or file encryption, application control (for example, whitelisting/blacklisting), and data loss protection (DLP) software, including the ability to block the movement of content to local devices like USB drives.

Enterprise products typically add a central management and reporting console and (often) integrate with corporate directories and authentication systems (AD, LDAP) to facilitate building and enforcing user- and group-based security policies.

As the volume and dynamism of malware has increased, signature-based detection and heuristics have been augmented with network-layer safeguards and crowd-sourced, reputation-based signature databases. Reputation-based security is a relatively recent addition to the anti-malware arsenal in which endpoints report into and reference a continuously updated online threat database.

Seeking to counter signature-based scanning schemes, attackers now automatically generate millions of slightly mutated malware payloads, directing each one to a small number of victims. According to Symantec's collection data, each distinct threat typically shows up on only 20 or fewer machines worldwide. This makes the process of testing and creating traditional malware signatures impossible.

FAST FACT

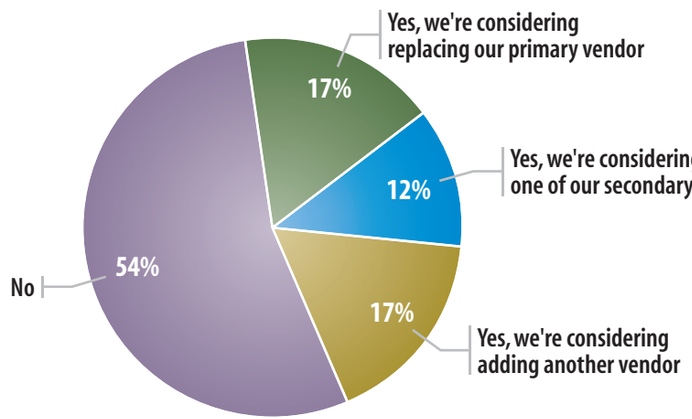
54%

Respondents who would not change their client-based antivirus or anti-malware vendor.

Figure 10

Replace or Add Vendors?

Would you consider replacing one of your current client-based antivirus or anti-malware vendors or adding another vendor?



Data: *InformationWeek* 2012 Antivirus and Anti-Malware Vendor Evaluation Survey of 386 business technology professionals, December 2011 R4130212/7

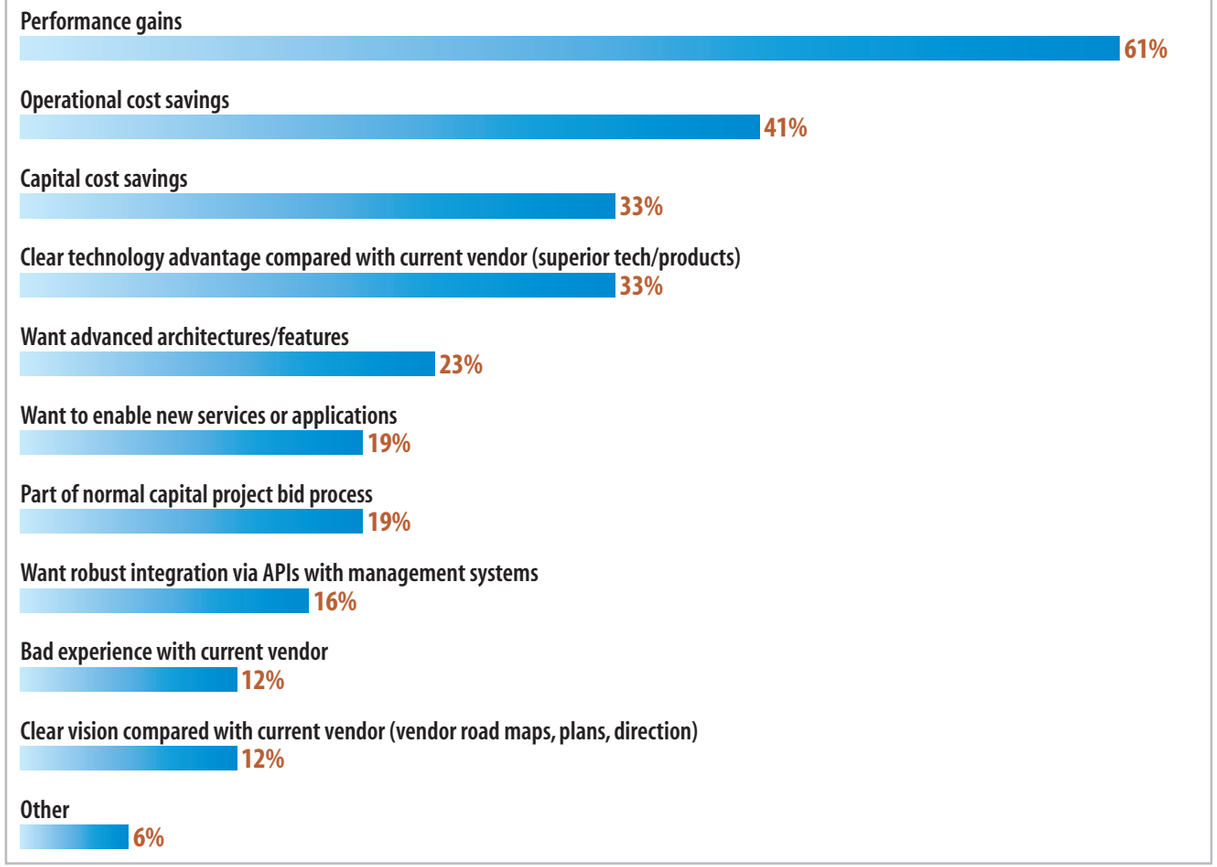
In response, Symantec and others have developed a reputation rating scheme that uses everything from heuristic scanning of the malware payload to the network addresses of any attempted connections or URL redirects to create a risk rating for every file —currently over 2.5 billion in Symantec's database. Users can set their risk tolerance by having the endpoint software block everything above a certain risk level. Although speed of signature updates isn't one of the most important product features among our respondents, expect this to change as the users come to realize how malware developers are circumventing traditional signature databases.

Another feature many organizations find useful is the ability to block Web-based ads, spyware or tracking cookies. One of our respondents plugs this gap with point products. "We use Symantec as out major antivirus server and client solution, but it is weak against spyware/adware. We supplement it with free software such as Spywareblaster, AdAware and Spybot S&D, however we're looking for something that will adequately handle it all."

Figure 11

Reasons for Replacing or Adding a Vendor

Why are you considering replacing your current client-based antivirus/anti-malware vendor or adding another vendor?



Note: Multiple responses allowed R4130212/8
Base: 177 respondents considering replacing or adding a vendor
Data: *InformationWeek* 2012 Antivirus and Anti-Malware Vendor Evaluation Survey of 386 business technology professionals, December 2011

Technical Evaluation Criteria

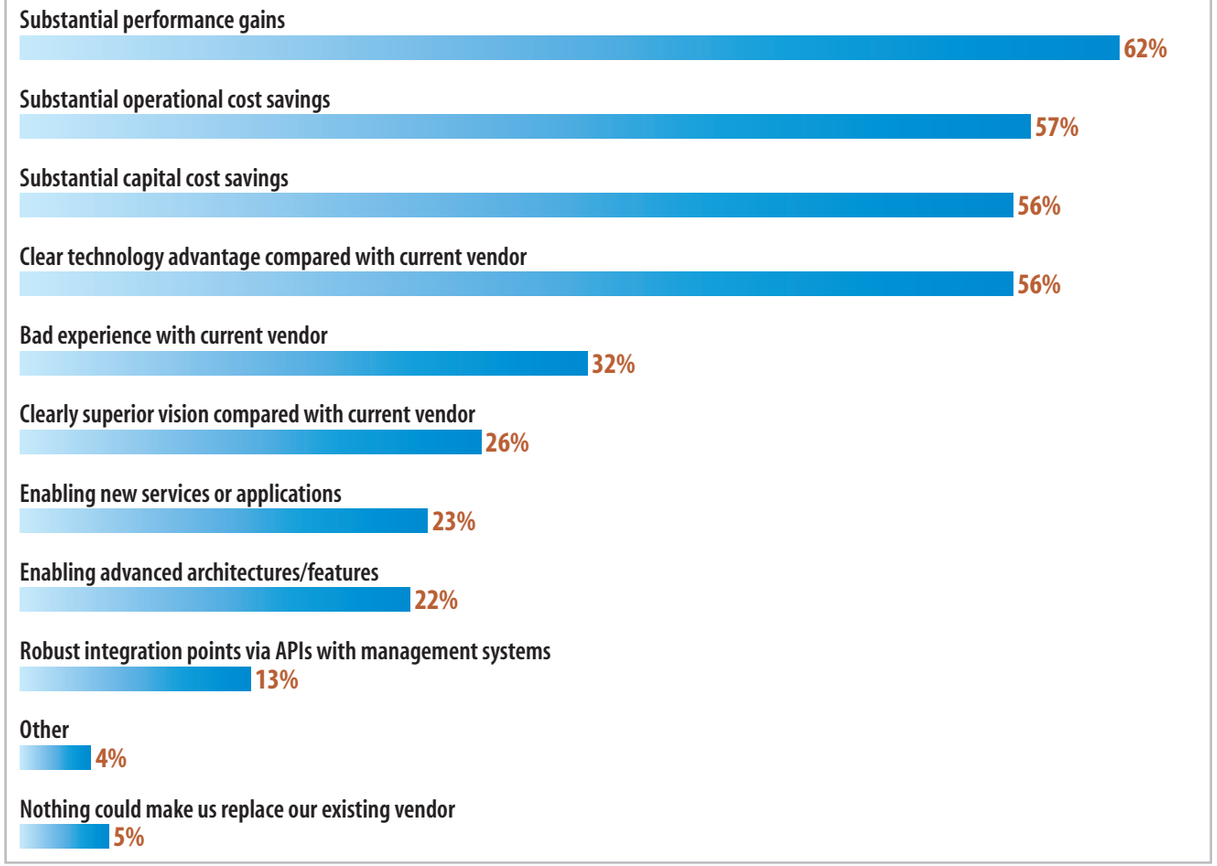
Rather than evaluating anti-malware products solely based on largely identical feature lists, buyers need to investigate how well these features are implemented, including the software's impact on system performance and the vendor's responsiveness to new threats. Unfortunately, performing such tests requires time and security expertise; resources in short supply in most IT shops. As one respondent puts it, "When shopping for anti-virus software, nobody really has the time to test and benchmark."

The basic metric for assessing anti-malware effectiveness is the software's coverage against the full spectrum of threats. Several independent groups, such as AV-TEST, NSS Labs and nCircle Network Security, conduct tests that measure antivirus and network intrusion detection coverage and threat remediation. For example, AV-TEST measures protection against zero-day attacks, a representative sample of recent malware and the most widespread and prevalent threats, grading products on a 0-to-100 scale.

Figure 12

Factors Resulting in a Change in Vendor

What would it take to replace your existing client-based antivirus or anti-malware vendor with another?



Note: Multiple responses allowed
Base: 209 respondents not considering replacing or adding a vendor
Data: *InformationWeek* 2012 Antivirus and Anti-Malware Vendor Evaluation Survey of 386 business technology professionals, December 2011

R4130212/9

Besides threat coverage, buyers should understand a product's deleterious effects on system performance. Here, Passmark Software provides a good benchmark that uses 13 different metrics; everything from boot time and scan speed to memory and CPU utilization and Web browsing speed.

The market for antivirus and endpoint protection software is bifurcated between corporate and consumer products; with the latter further segmented between free (or "freemium"—basic features for free or optional features in a deluxe edition at a charge) and commercial products. This means the market is, to coin a word, "trifurcated." This mix of business models means that it's difficult to get a comprehensive assessment of the endpoint security market because different surveys and market estimates measure different things. Some analysts track software revenue, others product usage. Some surveys look at the worldwide market, others just at the U.S.

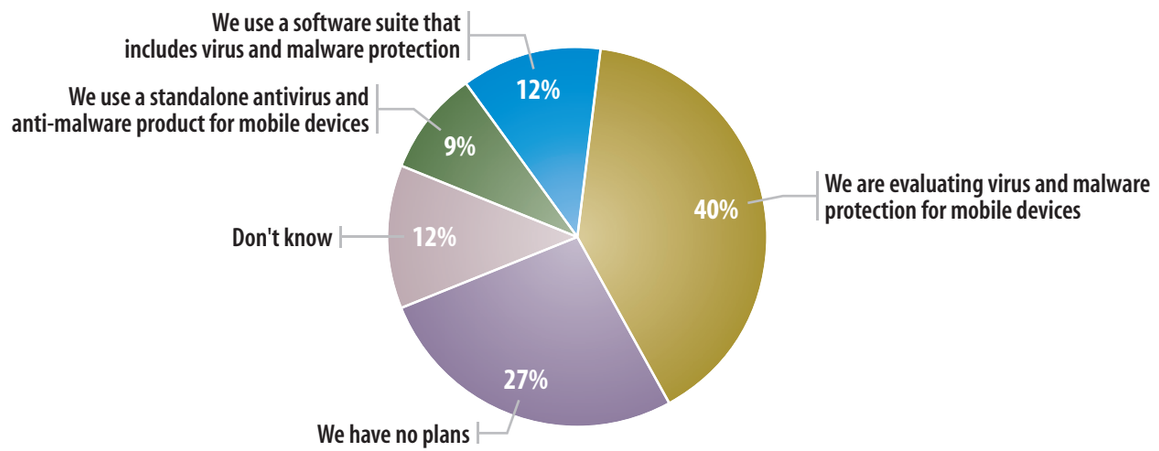
Yet for all but the smallest of mom-and-pop businesses, enterprise customers need some level of customer and product support; they may be disinclined to adopt one of the many free anti-malware products, even though independent testing shows some of them to be as effective as their commercial competitors. That said, some IT shops use both and enterprise product and free software, whether to address a perceived weakness in one product, or because a belt-and-suspenders approach to virus and malware detection may yield better overall protection.

As our survey found, among enterprises, two vendors dominate: Symantec and McAfee; a result that jibes with the latest estimates from IDC that show them with over 50% of the worldwide endpoint security revenue. What's notable however is that these two must con-

Figure 13

Mobile-Device Virus and Malware Protection

What are your plans for mobile-device virus and malware protection?



Data: *InformationWeek* 2012 Antivirus and Anti-Malware Vendor Evaluation Survey of 386 business technology professionals, December 2011

R4130212/16

tend with over 30 competitors, some of which, like Kaspersky, ESET and AVG, are growing revenue well in excess of 20% per year. Curiously, Malwarebytes and Microsoft, two of our top finishers, don't even appear in IDC's list, where Avast, Kaspersky and Trend Micro hold the 3 through 5 share positions.

Despite being among the oldest of third-party software utilities, the antivirus, cum endpoint security market is still growing at a healthy clip. IDC projects a compound annual growth rate of over 8% for the next five years.

Despite being among the oldest of third-party software utilities, the endpoint security market is still growing at a healthy clip.

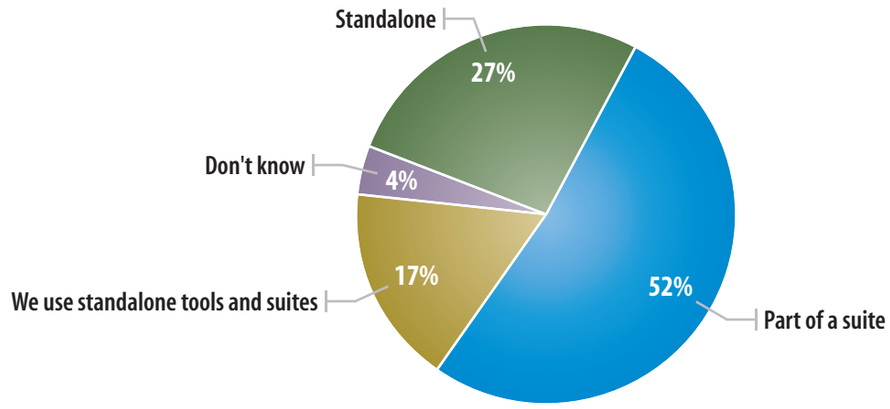
When looking at the endpoint security products actually in use, the picture gets much more muddled. According to the December 2011 OPSWAT Security Industry Market Share Analysis, which collects usage data on Windows systems, no fewer than four vendors split about 55% of the North American market. While Symantec again leads, spots two through four are occupied by free or freemium products from AVG, Microsoft and Avast, while McAfee drops to sixth place with a 6.8% share. Further illustrating the endpoint security market's fragmentation, OPSWAT detected 72 different antivirus vendors with 238 distinct products among North American users, with free versions again the most popular.

For enterprises, these market dynamics mean that there's not a strong correlation between product price and performance or effectiveness. For example, testing by NSS Labs found that Microsoft's product, which is free for small businesses and is often included in existing Microsoft volume license agreements for many enterprises, faired in the upper half of a group of 11 anti-malware products when tested for

Figure 14

Standalone Product vs. Suite

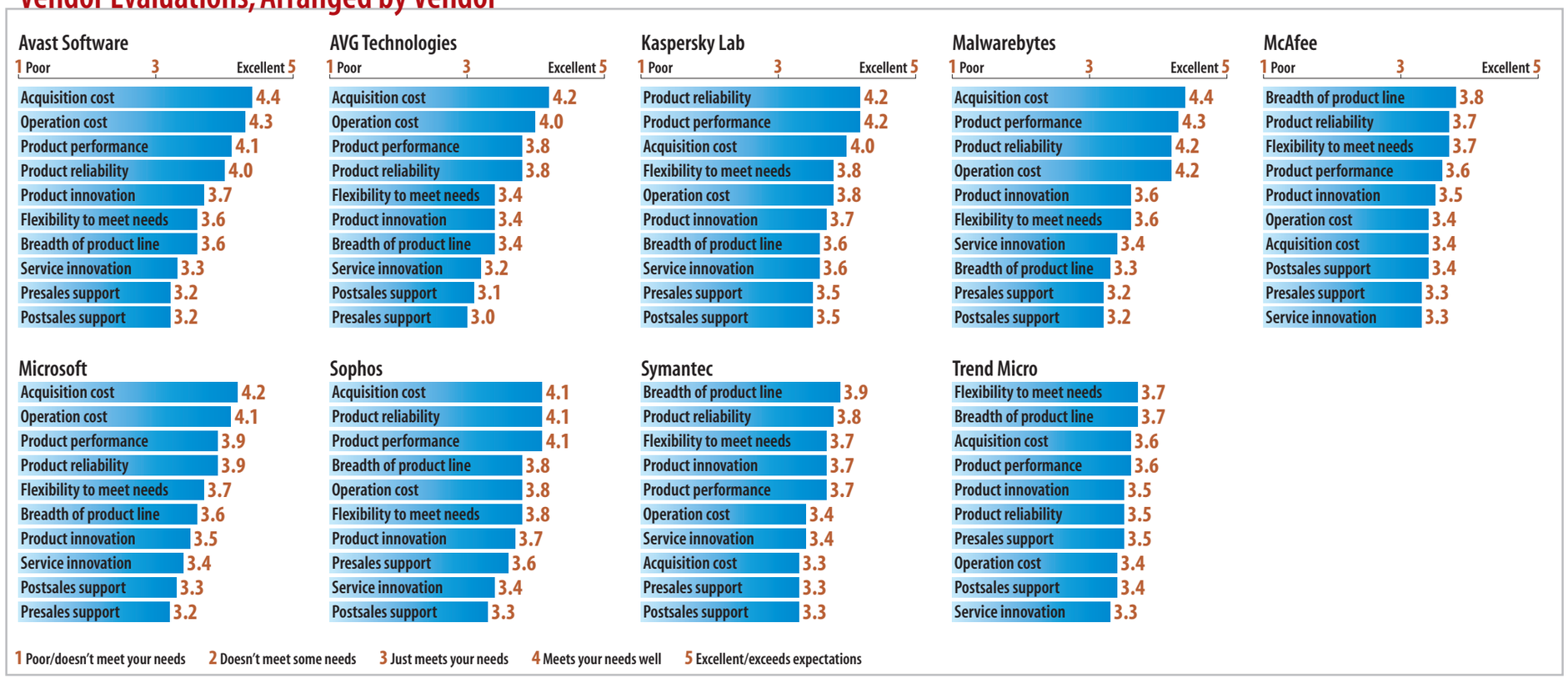
Is your client antivirus and/or anti-malware software a standalone product or part of a larger endpoint security suite?



Data: *InformationWeek* 2012 Antivirus and Anti-Malware Vendor Evaluation Survey of 386 business technology professionals, December 2011 R4130212/14

Figure 15

Vendor Evaluations, Arranged by Vendor



Note: Mean average ratings

Base: Varies

Data: *InformationWeek* 2012 Antivirus and Anti-Malware Vendor Evaluation Survey of 386 business technology professionals, December 2011

R4130212/3

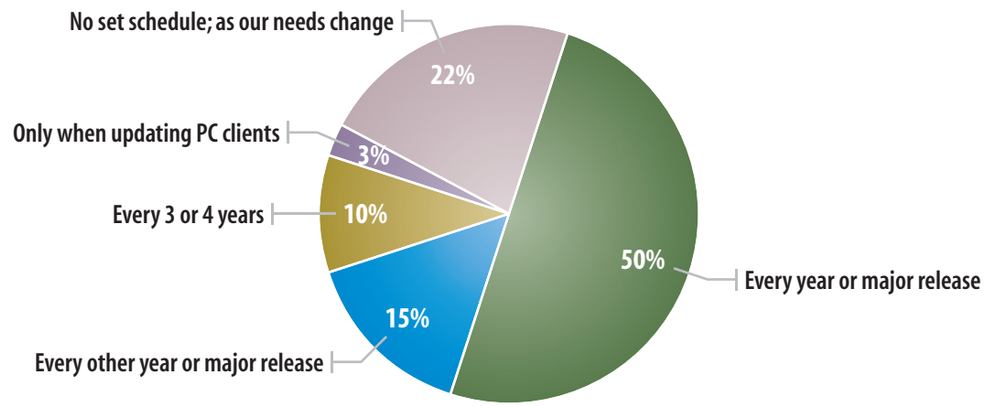
effectiveness at blocking malware and Web-based client-side exploits (attacks targeting browsers and plug-ins), while having the lowest negative affect on system performance.

As we saw, almost half of our respondents are considering replacing or adding endpoint anti-malware vendors, and fully half update products every year or major release (which typically happens annually). Such churn presents an opportunity for any vendor building a better mousetrap. Those that can significantly improve detection performance, reduce system overhead, lower costs and seamlessly integrate mobile devices into their product suite, could improve their market position in a hurry.

Figure 16

Frequency of Updates

How often do you update major versions of your antivirus and/or anti-malware software?



Data: *InformationWeek* 2012 Antivirus and Anti-Malware Vendor Evaluation Survey of 386 business technology professionals, December 2011

R4130212/15

The Burden of Choice

The endpoint anti-malware market is quite competitive: That's good and bad. While it fosters innovation and price erosion, it also makes product evaluation more tedious and confusing for IT. Although the feature overlap across products is extensive, here are a few items that should be on the shopping list of any organization thinking about switching vendors:

- Start with an endpoint suite, but consider augmenting with point products to counter Web-specific threats such adware and tracking cookies.
- A cloud-based, crowd-sourced reputation scanning database is an effective—nay, almost mandatory—feature to cope with the increasing volume of malware variants.
- Look for vendors with mobile modules and the ability to manage PCs and mobile devices from the same platform.
- Consider client anti-malware within a larger endpoint protection strategy that addresses control over applications (who can in-

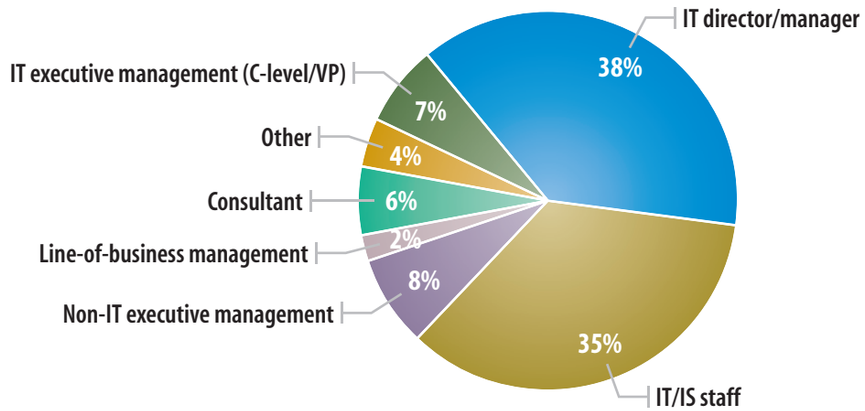
stall what), peripheral storage devices (USB sticks), and native Web applications (for example, Facebook apps). Make sure your endpoint product works well with other security layers like gateway content filters, network firewalls and UTM appliances.

Finally, remember that in a security environment where the threats change by the hour, any antivirus/anti-malware product is only as good as the vendor behind it. Due diligence is required before switching to the latest startup or open source project offering ostensibly better price/performance. When it comes to security, caveat emptor.

Figure 17

Job Title

Which of the following best describes your job title?



Data: *InformationWeek* 2012 Antivirus and Anti-Malware Vendor Evaluation Survey of 386 business technology professionals, December 2011

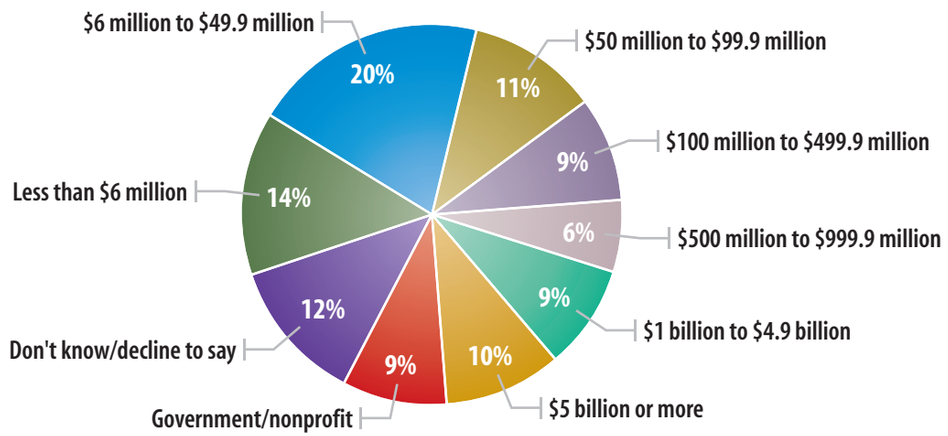
R4130212/17

APPENDIX

Figure 18

Company Revenue

Which of the following dollar ranges includes the annual revenue of your entire organization?



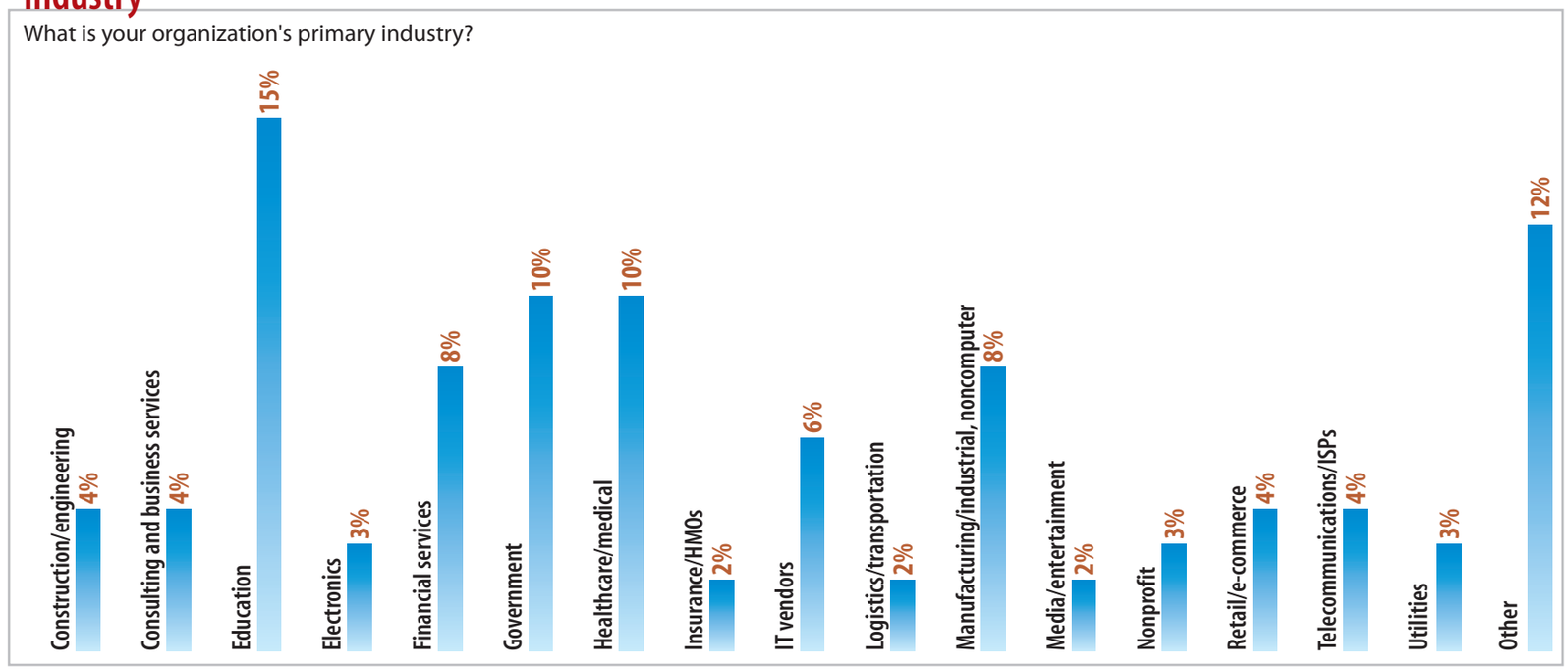
Data: *InformationWeek* 2012 Antivirus and Anti-Malware Vendor Evaluation Survey of 386 business technology professionals, December 2011

R4130212/18

Figure 19

Industry

What is your organization's primary industry?



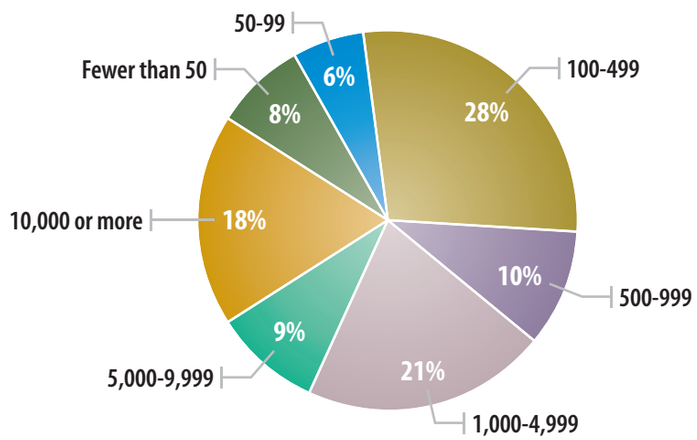
Data: *InformationWeek* 2012 Antivirus and Anti-Malware Vendor Evaluation Survey of 386 business technology professionals, December 2011

R4130212/19

Figure 20

Company Size

Approximately how many employees are in your organization?



Data: *InformationWeek* 2012 Antivirus and Anti-Malware Vendor Evaluation Survey of 386 business technology professionals, December 2011

R4130212/20

Kurt Marko
InformationWeek Reports

Kurt Marko is a technology writer and IT industry veteran, now focused on IT analysis and reporting after a varied career that has spanned virtually the entire high-tech food chain from chips to systems. Upon graduating from Stanford University with a BS and MS in Electrical Engineering, Kurt spent several years as a semiconductor device physicist, doing process design, modeling and testing. He then joined AT&T Bell Laboratories as a memory chip designer and CAD and simulation developer.

Moving to Hewlett-Packard, Kurt started in their laser printer R&D lab doing electrophotography research, for which he earned a patent, but his love of computers eventually led him to join their nascent technical IT group. He spent 15 years as an IT engineer and was a lead architect for several enterprise-wide infrastructure projects at HP, including its Windows domain infrastructure, remote access service, Exchange email infrastructure and managed Web services. For the past five years, Kurt has been a frequent contributor to several IT trade and consumer technology publications and industry conferences. He is now a regular contributor to *InformationWeek* and *Network Computing*.

ABOUT US

InformationWeek Reports' analysts arm business technology decision-makers with real-world perspective based on qualitative and quantitative research, business and technology assessment and planning tools, and adoption best practices gleaned from experience.

To contact us, write to managing director **Art Wittmann** at *awittmann@techweb.com,* content director **Lorna Garey** at *lgarey@techweb.com,* editor-at-large **Andrew Conry-Murray** at *acmurray@techweb.com,* and research managing editor **Heather Vallis** at *hvallis@techweb.com.*

Find all of our reports at *reports.informationweek.com*

SYNOPSIS

RESEARCH

Survey Name *InformationWeek Analytics* 2012 Antivirus and Anti-Malware Vendor Evaluation Survey

Survey Date December 2011

Region North America

Number of Respondents 386

Purpose To determine preference for vendors supplying endpoint antivirus and anti-malware software to enterprise IT organizations.

Methodology *InformationWeek* surveyed business technology decision-makers at North American companies. The survey was conducted online, and respondents were recruited via an email invitation containing an embedded link to the survey. The email invitation was sent to qualified *InformationWeek* subscribers. Individual evaluations were conducted for vendors whose products have been used or evaluated in the past 12 months by 30 or more respondents. Respondents were asked to evaluate only those vendors/products for which they reported recent use or evaluation.

MORE LIKE THIS

Want More Like This?

InformationWeek creates more than 150 reports like this each year, and they're all free to registered users. We'll help you sort through vendor claims, justify IT projects and implement new systems by providing analysis and advice from IT professionals. Right now on our site you'll find:

Informed CIO: Striking a Security/Usability Balance: How do you ensure that sensitive data isn't compromised and that vulnerabilities brought about by personal devices are mitigated?

Strategy: Database Defense: In tough economic times, desperate employees discover what enterprises and cybercriminals already know: Sensitive data can be sold for cash. For a data entry operator, call center employee, database administrator or salesperson with access to proprietary customer lists, the temptation to steal and sell sensitive data can be overpowering.

Research: Data Encryption: Ushering in a New Era: As we analyzed the encryption trends highlighted by the 506 respondents to our *InformationWeek* 2012 Data Encryption Survey, we realized that this old technology is proving invaluable to organizations looking to adopt a data-centric, rather than perimeter-based, security model.

PLUS: Find signature reports, such as the *InformationWeek* Salary Survey, *InformationWeek* 500 and the annual State of Security report; full issues; and much more.