

A Forrester Consulting Thought Leadership Paper Commissioned By Webroot

# The State Of Endpoint Protection

How Solid Is Your First Layer Of Defense Against Cyberthreats?

October 2011

**FORRESTER**

**Headquarters | Forrester Research, Inc.**  
400 Technology Square, Cambridge, MA 02139 USA  
Tel: +1 617.613.6000 | Fax: +1 617.613.5000 | [www.forrester.com](http://www.forrester.com)

Forrester Consulting  
Making Leaders Successful Every Day

## Table Of Contents

---

Executive Summary.....	2
Introduction And Survey Methodology.....	3
For Many, Protecting User Endpoints Is A Multifaceted Proposition.....	4
Defending Against Endpoint-Based Attacks Remains An IT Challenge.....	5
Current Desktop Av Products Left Much To Be Desired.....	7
Organizations Look To Cloud-Based Endpoint Security For Improved Protection And Reduced Costs.....	11
Key Recommendations.....	13
Appendix A: Methodology.....	14
Appendix B: Demographics.....	14
Appendix C: Endnotes.....	15

© 2011, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave®, RoleView®, TechRadar®, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to [www.forrester.com](http://www.forrester.com). [1-J2YO1B]

### About Forrester Consulting

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit [www.forrester.com/consulting](http://www.forrester.com/consulting).

## Executive Summary

---

In August 2011, Webroot commissioned Forrester Consulting to conduct a survey study of 161 North American and European IT security decision-makers. The purpose of the study is to understand the current state of endpoint security strategies across enterprises and SMBs, as well as identify key trends and market directions for endpoint security.

Our survey found that while almost everyone has some form of endpoint protection (the protection mechanisms do not always live on the endpoint—sometimes, it is a network-based capability that protects user endpoints), a majority of organizations have experienced endpoint attacks despite the presence of security defenses. Of these, almost 50% have resulted in financial loss greater than \$100,000 in the last 12 months alone. The security attacks, our respondents told us, also resulted in significantly increased IT help desk time, reduced productivity, and in some cases, disrupted business activity.

Most IT security professionals say their endpoint security products do not catch all threats.

This study took a detailed look at how organizations deploy endpoint security products, their common practices, pain points, and challenges. The study uncovered these key findings:

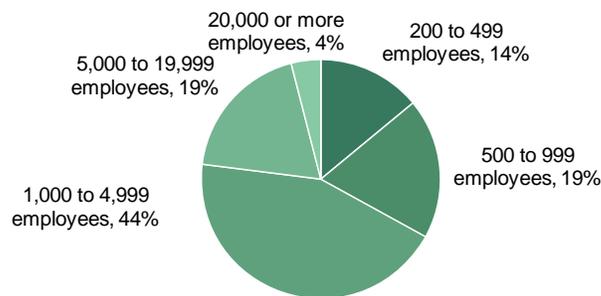
- **Endpoint security is a multifaceted IT task.** A typical IT shop deploys a plethora of endpoint security mechanisms to protect user endpoints against incoming threats. Our study found that almost two-thirds of the survey respondents use at least three different security measures. Very few organizations use only one endpoint security technology. Seventy-eight percent have endpoint antivirus, making it the most widely deployed endpoint security measure in this study.
- **Traditional endpoint security is not effective against modern threats.** Despite the widespread adoption of endpoint security products, organizations continue to experience penetrations via user endpoints. We found that 95% of all survey respondents suffered some form of endpoint-based attacks in the last 12 months. Some of the attacks resulted in significant financial damage.
- **Current on-premises endpoint AV technologies create unique operational challenges.** The study found that users of on-premises AV products are much more likely to experience performance slowdowns due to a scan. In addition, remote and roaming endpoints create a challenge for IT as many do not practice the timely delivery of virus definitions to these endpoints outside the corporate firewall.
- **Many look to cloud-based endpoint security for improved protection and lower costs.** Many respondents in our study expressed interest in cloud-based endpoint security. The main drivers in moving to the cloud are improved protection and lower cost. Manageability and better performance are also among the top benefits our respondents expect cloud to deliver. Interestingly, the enterprises in this study are just as interested in cloud as those small and medium businesses are.

## Introduction And Survey Methodology

In August 2011, Webroot commissioned Forrester Consulting to conduct a survey study of North American and European IT security decision-makers. We surveyed 161 respondents, with 73% from the US and the remaining 27% from the United Kingdom. The respondents come from companies with varying sizes, ranging from 200 employees to those with 20,000 plus (see Figure 1). They are from a wide range of industries, including business services, manufacturing, financial services, high tech, healthcare, the public sector, etc. All survey respondents are intimately familiar with endpoint security and web security technologies — many of them making buying decisions for their organizations and are screened for their familiarity with security-as-a-service (e.g., SaaS-delivered security capabilities). Readers who are interested in a more detailed description of respondent profiles should refer to Appendix A. We completed the online survey in September 2011 with 33 questions spanning many aspects of endpoint security, current pain points, and delivery methods.

**Figure 1**  
Respondent Profile — Size Of The Company

“Using your best estimate, how many employees work for your firm/organization worldwide?”

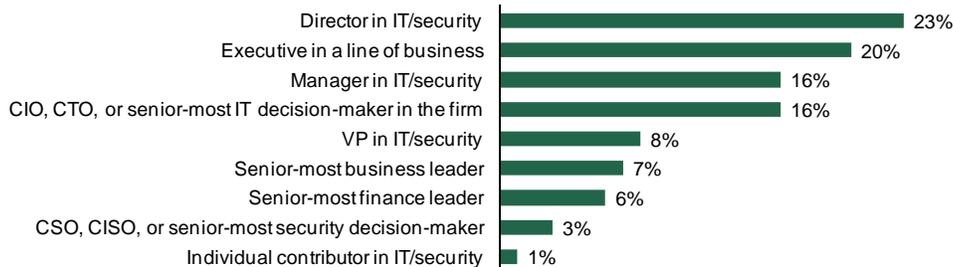


Base: 161 US and UK IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Webroot, September 2011

**Figure 2**  
Roles Of The Survey Respondents

“Which of the following most closely describes your job title?”



Base: 161 US and UK IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Webroot, September 2011

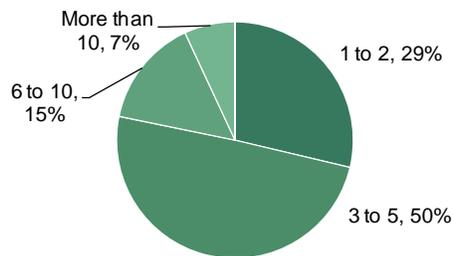
## For Many, Protecting User Endpoints Is A Multifaceted Proposition

The first goal of the study is to understand how IT organizations approach endpoint protection today. We asked our respondents what security technologies, either on device or in the network, they use to protect user endpoints. We found that almost everyone has multiple measures in place for endpoint protection (see Figure 3). Endpoint Antivirus (AV), web security gateways with AV, anti-spam gateways with AV are just a few examples of the technologies organizations employ to protect endpoints (and networks).

More specifically, 72% told us that they use at least three different technologies to protect users against threats, while 22% use more than six technologies. The respondents reported that endpoint antivirus (either desktop or via SaaS) is the most commonly deployed measure, followed by secure web gateways and anti-spam gateways, both with AV functions. Offline malware detection products and UTM with AV round out the selection (see Figure 4).

**Figure 3**  
Respondents That Use Multiple Endpoint Security Measures

“How many discrete endpoint security solutions do you currently use in your IT environment?”

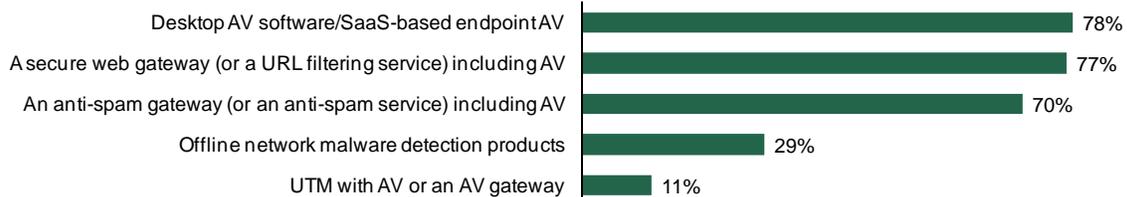


Base: 161 US and UK IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Webroot, September 2011

**Figure 4**  
Deployed Endpoint Technologies

“What are the security technologies that you use to secure your endpoints and protect users from security threats?”



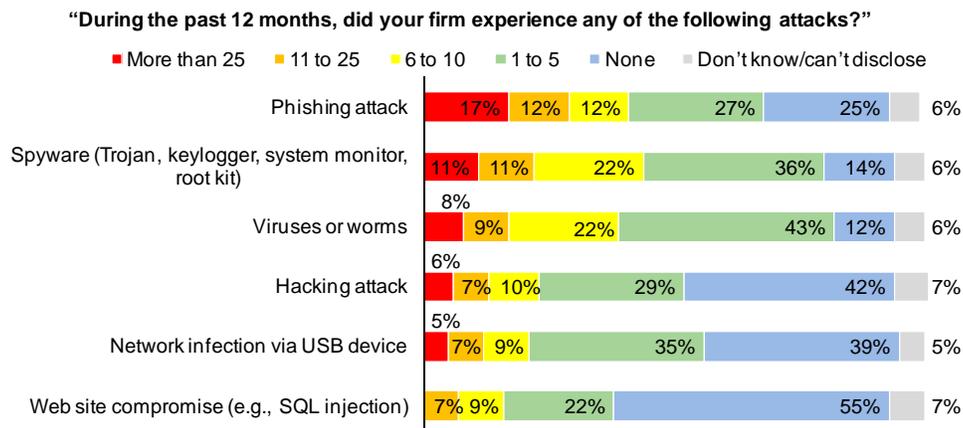
Base: 161 US and UK IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Webroot, September 2011

## Defending Against Endpoint-Based Attacks Remains An IT Challenge

We asked our respondents whether their organizations suffered security attacks in the last 12 months. Ninety-six percent of the 161 respondents say they have experienced some form of attacks, ranging from phishing, viruses, spyware, and hacking to website compromises (see Figure 5).

**Figure 5**  
Organizations Suffered Various Forms Of Attacks In The Last 12 Months



Base: 161 US and UK IT security decision-makers

Source: A commissioned conducted by Forrester Consulting on behalf of Webroot, September 2011

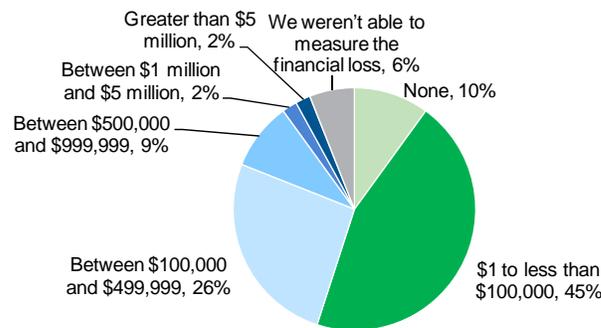
### Endpoint Attacks Are Widespread

Another look at the data shows that endpoint-based attacks, including viruses, spyware, phishing, or USB infection, were ubiquitous in the answers that we received. Out of the 154 respondents whose organizations have experienced attacks in the last 12 months, 100% have seen endpoint attacks.

Most of the respondents who experienced attacks also told us that they saw financial loss due to the attacks: 39% reported losses over \$100,000 in the last 12 months, 13% saw losses over \$500,000, and 4% — a total of 7 respondents — reported losses over \$1 million (see Figure 6).

**Figure 6**  
Financial Consequences Of Security Attacks In The Last 12 Months

“Using your best estimate, how much was the financial impact of these attacks to your firm?”



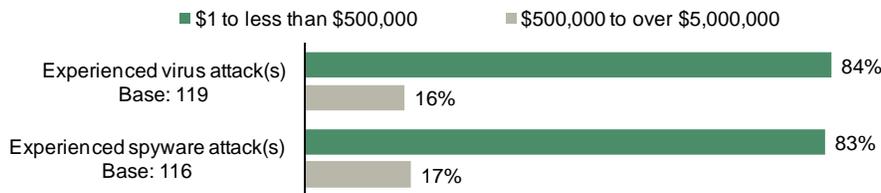
Base: 161 US and UK IT security decision-makers

Source: A commissioned conducted by Forrester Consulting on behalf of Webroot, September 2011

While it is not completely clear whether the endpoint attacks were directly responsible for the losses, a close look at the data suggests that the higher the financial loss, the more likely viruses and spyware are involved (see Figure 7). With the exception of the \$100,000 to \$499,999 loss category, the higher the financial loss, the more likely you'd see either a virus/Trojan or a spyware attack.

**Figure 7**  
Financial Loss For Those Who Experienced Virus Or Spyware Attacks

“Using your best estimate, how much was the financial impact to your firm of these attacks? by Those who experienced one or more attacks and were able to quantify financial impact”



Base: US and UK IT security decision-makers

Source: A commissioned conducted by Forrester Consulting on behalf of Webroot, September 2011

### Endpoint Attacks Negatively Impact Business And IT Productivity

Aside from direct financial consequences, the survey respondents also reported that the attacks they experienced reduced operational efficiency and productivity. Twenty-three percent says the attacks significantly increased IT help desk time, while 10% reported a significant reduction in employee productivity (see Figure 8). Disrupting business activities, compromising customer data, and increasing IT resources are other operational impact reported by the survey.

**Figure 8**  
Non-Financial Impact Of Security Attacks



Base: 161 US and UK IT security decision-makers

Source: A commissioned conducted by Forrester Consulting on behalf of Webroot, September 2011

It’s not surprising that survey respondents reported increased IT help desk time as the top impact of security attacks. Endpoint compromises often result in significant work on the part of IT in terms of troubleshooting, machine reimaging, and forensics. Endpoint attacks also directly affect employee productivity, as most users utilize their endpoint device for daily business tasks.

## Current Desktop Av Products Left Much To Be Desired

Desktop AV is one of the most commonly deployed endpoint protection measures. Many organizations use desktop AV without ever questioning its efficacy. Desktop AV was developed when viruses were relatively rare and signatures relatively static. Today, the APT-style of attack often has no signature to speak of, and the attack may morph quickly to evade old-fashioned signature detection.

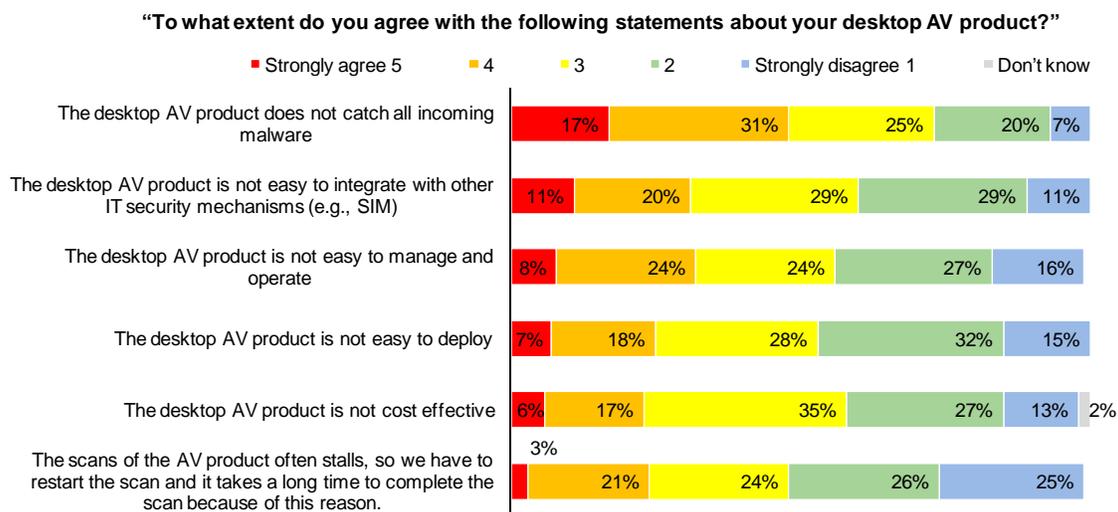
In order to understand the efficacy of desktop AV against modern threats and its operational burden on IT, we asked our respondents a series of questions spanning detection rate, performance, operational complexity, and manageability.

### Desktop AV Does Not Catch All Threats, And Consequences Are Elevated To Business Risks

For the 95 survey respondents who are using desktop AV products, we asked whether they agree with some of the common complaints about desktop AV, including AV not catching all threats, not easy to integrate, and not easy to manage, deploy, etc. The answers we got indicated an overall sentiment that desktop AV is not sufficient to catch all

incoming malware (see Figure 9). However, the respondents didn't quite render a consistent verdict for the other complaints — opinions were split between those who agreed and those who didn't.

**Figure 9**  
Respondents' Opinions On Their Desktop AV Products



Base: 95 senior decision-makers with desktop AV

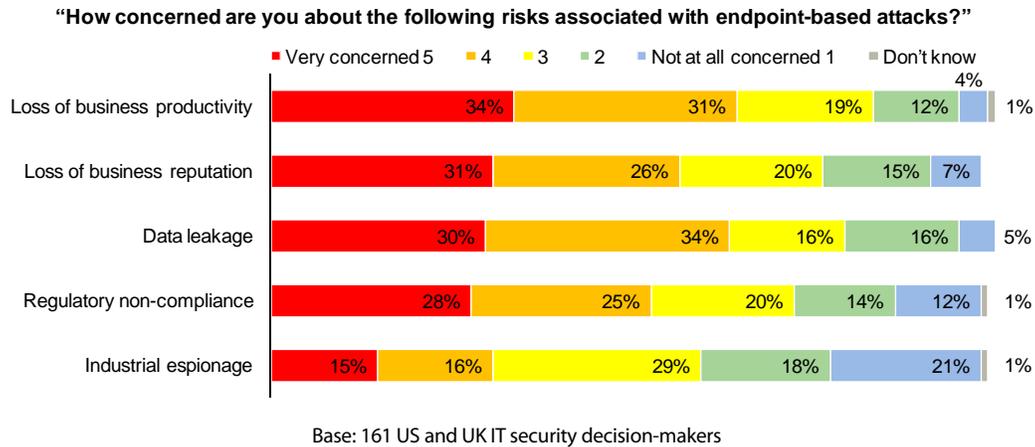
Source: A commissioned study conducted by Forrester Consulting on behalf of Webroot, September 2011

It's clear, with 17% strongly agree and 31% agree, our respondents consider detection rate a challenge for desktop AV products. This is not surprising as most of the desktop AV products are designed to tackle a virus problem that is more than 20 years old. With the number of new malware variants logged at hundreds of millions a year, organizations today do not have the luxury of accommodating false negatives, even at a low percentage point.

When asked which risks associated with endpoint based attacks are top of mind, our respondents chose loss of business productivity. Loss of business reputation and data leaks are close behind (see Figure 10). Because we surveyed primarily individuals with an IT background, operational metrics such as user productivity is typically more visible from their perspective. But even with this population of respondents, loss of business reputation and data leaks, two business metrics, still made the top three of the list of risks.

It is increasingly clear to security professionals, through a string of recent high profile attacks, that failure to properly protect your infrastructure and endpoints has a direct impact on business risks. This connection came out loud and clear in our respondents' answers.

**Figure 10**  
Concerns Associated With Endpoint-Based Attacks

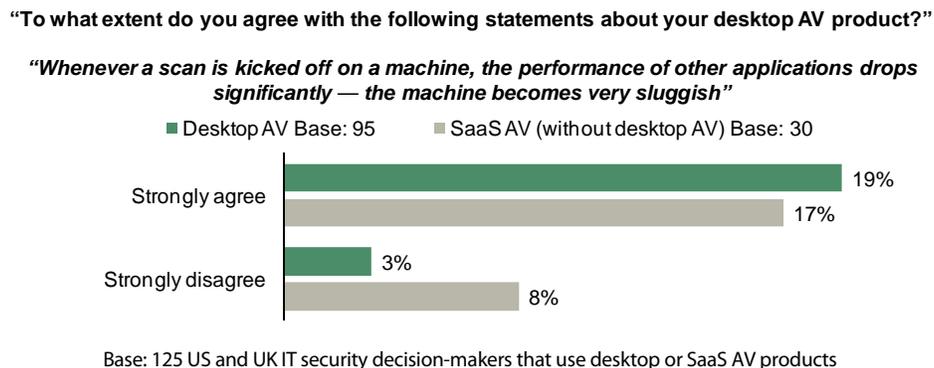


Source: A commissioned study conducted by Forrester Consulting on behalf of Webroot, September 2011

### On-Premises, Desktop AV Impact Endpoint Performance

When asked about the performance of their AV products, we see a clear division between those that have desktop AV and those that use SaaS AV. We asked whether the respondents agreed with the statement, “Whenever a scan is kicked off on a machine, the performance of other applications drops significantly — the machine becomes very sluggish,” 19% of those who use desktop AV chose “strongly agree.” In contrast, only 10% of those using SaaS AV (and no desktop AV) chose “strongly agree” (see Figure 11). There is no mistake that, in terms of performance impact on the endpoint, our respondents strongly favored cloud-based delivery over its on-premises counterpart.

**Figure 11**  
Perception Of Sluggish Performance Drops With SaaS AV



Source: A commissioned study conducted by Forrester Consulting on behalf of Webroot, September 2011

The performance impact also manifests in another dimension — scan time. Thirty-eight percent of the respondents said their desktop AV product took between one and two hours to finish scanning a typical user endpoint. Another 31% said the scan would take between 30 minutes to an hour. A scan that took more than 30 minutes to finish is considered slow by industry standards and may severely impact the usability of the endpoint.

## Remote And Mobile Endpoints Present Additional Challenges To IT Security

Many organizations have remote and mobile workers whose endpoints do not always live behind the company’s firewall consistently. For those corporate endpoints outside the firewall, updating AV definitions can be a difficult proposition. Many desktop AV products would download new definitions onto a management server; the server subsequently pushes the definitions onto endpoints. But this requires that the endpoints be in the same network as the management server, which means those corporate endpoints beyond the firewall will not get their virus definitions in a timely manner (e.g., the endpoints will only get updates when they are inside the corporate network or use VPN to access network resources).

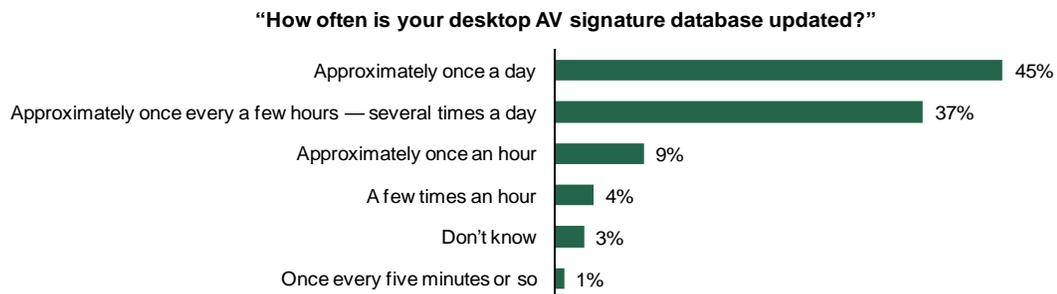
We asked the survey respondents how they update the desktop AV signatures for remote office and mobile workers; 61% said they only update the AV signature database only when the endpoint is behind the corporate firewall or connecting through VPN. Only 38% say they update the signature database directly from their vendor’s update server, regardless of the endpoint location.<sup>1</sup>

Since many organizations do not update the remote endpoints as soon as new virus definitions become available, it is no surprise that 45% reported that they only update the signature definitions once a day, and another 37% update only once every a few hours (see Fig 12). When an endpoint goes for an extended period of time without updating its virus signature definition, this endpoint is susceptible to new threats — the longer the update awaits, the larger the window of susceptibility. Recent industry numbers suggest that new threats emerge at the rate of over 200 million per year. That translates to over 500,000 new malware a day! If you update your endpoints once a day, you essentially have an open invitation for security incident to happen.

---

**Figure 12**  
Majority Of Respondents Update AV Signature Daily Or Several Times A Day

---



Base: 95 US and UK IT security decision-makers that use desktop AV products

Source: A commissioned study conducted by Forrester Consulting on behalf of Webroot, September 2011

---

## Organizations Look To Cloud-Based Endpoint Security For Improved Protection And Reduced Costs

---

Using cloud to deliver endpoint security functions is a recent industry trend. We define cloud-based endpoint security as security services/functions hosted at a third party, billed on a pay-per-use model, delivered via a multitenant architecture.

In our survey, 6% of respondents say they have already adopted cloud or SaaS-based endpoint AV. Though the deployment base is still small, 18% said they are “very interested in” procuring cloud-based AV in the next 12 months, while another 39% said they are “interested” in procuring (see Figure 13).

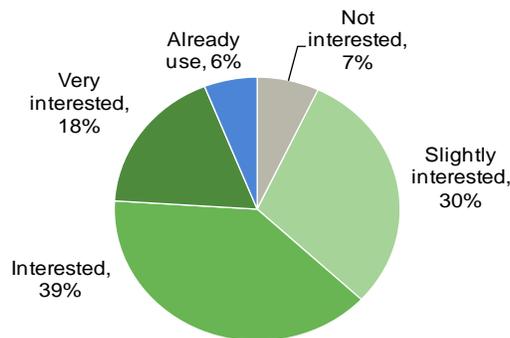
More interestingly, we found that enterprises are just as interested in cloud-based endpoint security as are SMBs (see Figure 14). In the study, companies with 500 to 999 employees expressed the strongest level of interest in cloud delivery, while small companies (with 200 to 499 employees) and enterprises (greater than 1,000 employees) expressed similar interest.

---

**Figure 13**  
Strong Interest Overall In SaaS-Based Endpoint AV

---

“How interested is your firm in procuring SaaS-based endpoint AV in the next 12 months?”

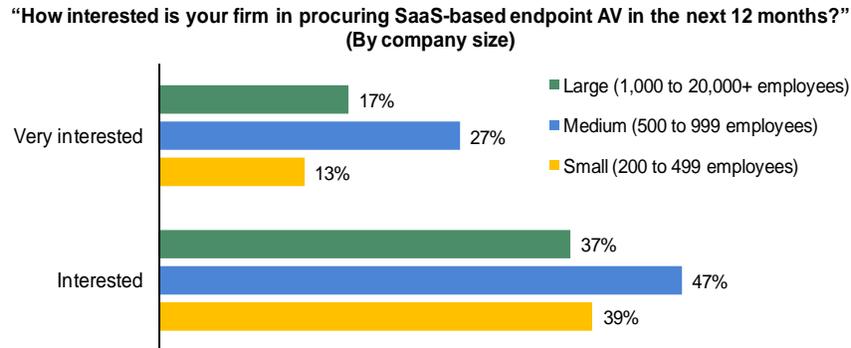


Base: 161 US and UK IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Webroot, September 2011

---

**Figure 14**  
Company Size Breakdown Of Interest In SaaS-Based Endpoint Security



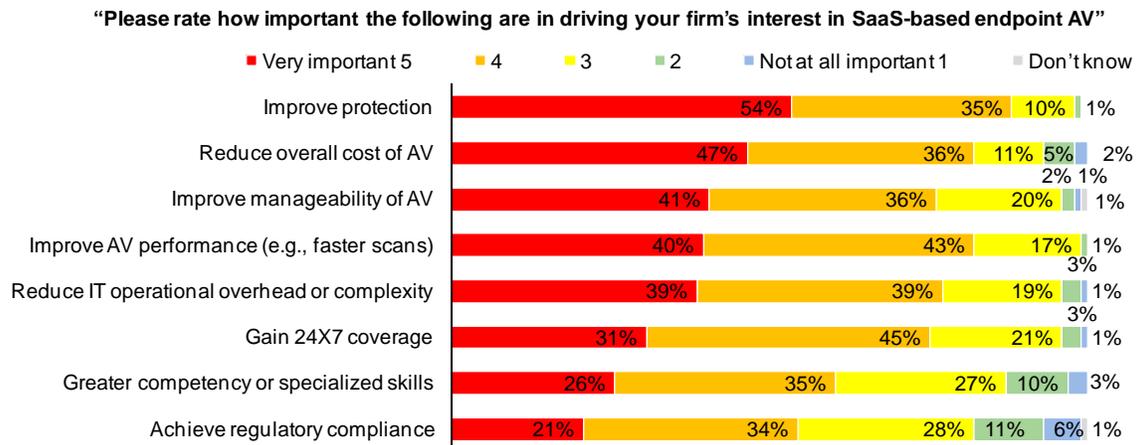
Base: 161 US and UK IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Webroot, September 2011

Organizations are interested in cloud-based endpoint security for a variety of reasons. Our respondents told us that the most common drivers are improved protection and reduced cost (see Figure 15). Improving manageability of AV, performance, and reducing IT operational overhead are also important drivers.

Manageability of IT solutions is a major challenge for organizations large and small. Many IT teams are inundated with too many point solutions that do not work well together. Moving to the cloud is a way to alleviate some of these challenges.

**Figure 15**  
Top Drivers For SaaS-Based Endpoint AV



Base: 101 US and UK IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Webroot, September 2011

## KEY RECOMMENDATIONS

Despite the widespread use of endpoint antivirus products, respondents continue to see attacks penetrating their organizations via user endpoints. Some have suffered significant financial loss due to endpoint attacks.

This study took a detailed look at how organizations deploy endpoint security products today, their common practices, pain points, and challenges. The detailed findings point to these high-level recommendations:

- **Rethink your AV strategy.** Antivirus is an essential component of IT's security strategy. However, as our survey respondents indicated, current desktop AV technologies are ill-equipped to deal with the kinds of fast-moving modern threats, such as zero-day exploits and malware tool kits. In addition, they visibly impact endpoint performance and user productivity. Instead of dutifully managing the AV technology you've got, security and risk professionals should take a critical look at your current AV strategy, take a step back, and assess its efficacy. In many cases, you may need more than a simple tune up for your desktop AV to deliver an effective return on investment.
- **Do not short-change your remote endpoints.** Today's cybercriminals target user endpoints as a way in to the corporate infrastructure. Remote endpoints are a weak link if their virus definitions are not updated as often. Failing to properly protect your endpoints, wherever they might be, can lead to breach of confidential information or intellectual properties, as we have seen in some of the recent attacks. Organizations must find a way to protect and treat remote endpoints in the same rigorous manner as they do with those that are behind the corporate firewall.
- **Leverage the cloud.** Cloud-delivered endpoint security has the advantage of coverage — it is capable of protecting endpoints regardless of their locations; performance — signature generation and storage in the cloud would not slow down the individual endpoints; lower operational cost — there is less of a client footprint (and versions) to manage; and ultimately improved protection, as more endpoints are protected in a more timely fashion, using more effective technologies. Cloud already delivers benefits for many other aspects of IT, and it is now time for cloud to provide benefits for your security initiatives.

## Appendix A: Methodology

---

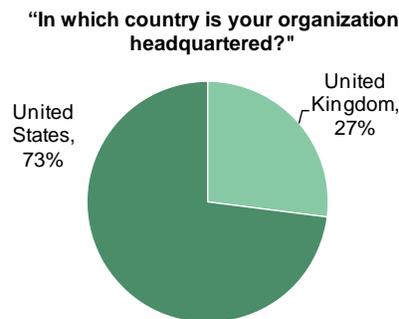
In this study, Forrester conducted an online survey of 161 North American and European IT security decision-makers. Survey participants included those intimately familiar with endpoint security and web security technologies — many of them making buying decisions for their organizations and are screened for their familiarity with security-as-a-service (e.g., SaaS-delivered security capabilities.) The study began in August 2011 and was completed in September 2011.

## Appendix B: Demographics

---

**Figure A**  
Country Breakdown

---



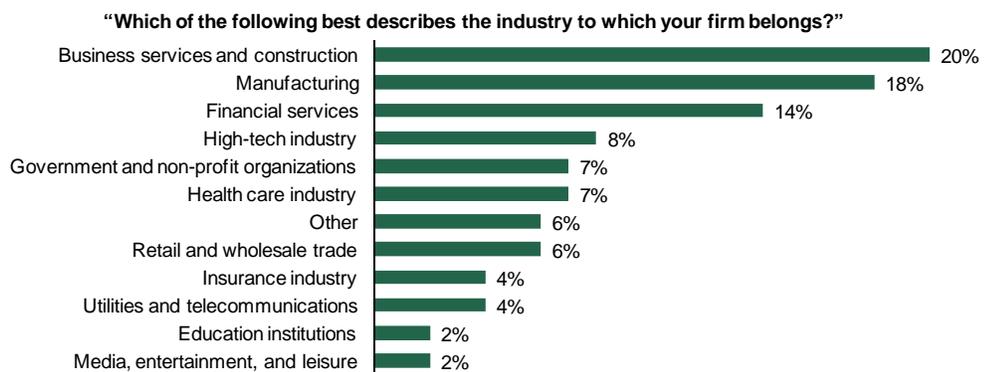
Base: 161 North American and European IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Webroot, September 2011

---

**Figure B**  
Industry

---



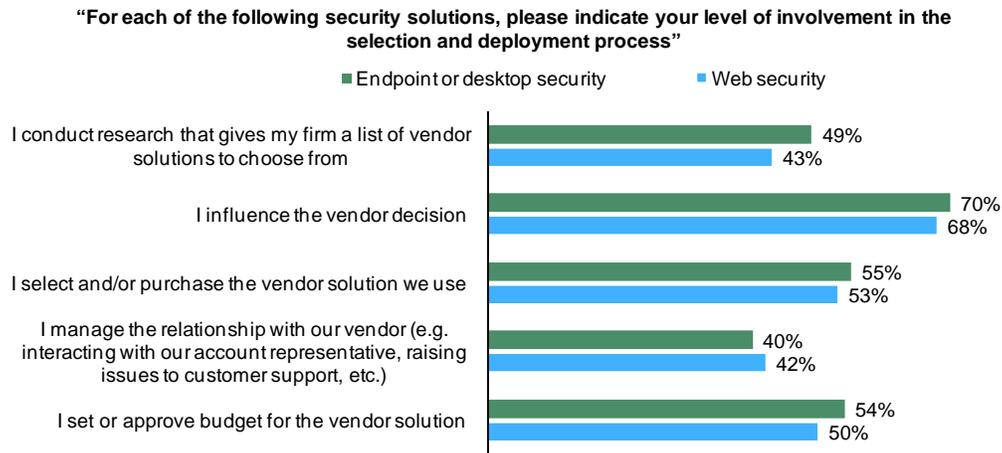
Base: 161 North American and European IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Webroot, September 2011

---

**Figure C**  
Respondent Involvement In Security Decisions

---



Base: 161 North American and European IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Webroot, September 2011

---

## Appendix C: Endnotes

---

<sup>1</sup> Due to space limitations, we omit the statistics graph here. We asked everyone who uses a desktop AV product how they update signature definitions for remote office and mobile workers. Twenty-seven percent said updates are only pushed to endpoints when they are behind the corporate firewall. Thirty-four percent said updates are pushed when the endpoints are either behind the firewall or connecting through a VPN. Thirty-eight percent said updates are pushed to the endpoints directly from vendor’s update server wherever the endpoints are.