THE STATE OF
Cloud-Based Security

Taking a Cloud-Based Approach to Security Can Improve Protection and Lower Costs

An Exclusive Research Report

By Erik Sherman

While media attention is often focused on cybercriminals' attacks on servers and networks, a far bigger problem for most companies is endpoint security. Traditional approaches to protecting users and their devices against an increasingly complex threat environment are becoming less effective. Cloud-based security may be an answer. While few companies currently take advantage of this technology, cloud-based security may be a big opportunity for IT to improve security while cutting cost. This exclusive UBM TechWeb and Webroot survey explores the state of cloud-based security.

Computer threats like malware, phishing attacks, and malicious web sites are a problem for businesses. They cost time and money and divert technical resources from other activities that could benefit a company, so they extract a double penalty.

Although news stories about computer vulnerabilities often focus on hacker attacks on servers and networks, a far bigger problem for most companies is endpoint security—protecting users and their devices against an increasingly complex threat environment. Experts have known for years about the need to protect client machines from attacks. There are many software and hardware packages available to help combat the problem, including typical solutions such as endpoint security, gateway-based Web security, email security, and virtual private networks (VPNs).

Sponsored by WEBROOT

UBM TechWeb

In 2009, the average cost of a data breach in the U.S. was almost $6.8 million.
— Ponemon Institute

However, these traditional solutions have weaknesses, such as difficulty of maintenance in an enterprise or the chance that a security approach simply doesn't work on a given threat, perhaps because a user may have unwittingly introduced malware into the company's network. Cloud-based security offers a solution to many of these problems, although relatively few companies take advantage of the technology. That means many IT departments have big opportunities to improve security while cutting administrative time and expense.

UBM TechWeb undertook a survey on the state of cloud-based security in August and September 2011. This paper examines the findings within the context of IT security and looks at whether similar companies could benefit from cloud-based security and how receptive they might be to using the technology.

Computer Security Today

At one time, computer security was a relatively simple issue. A company would install antivirus software on client computers, fortify its network with intrusion detection software and a firewall, and train employees on what they should and should not do. The IT department could reasonably claim to have addressed the issue.

Conversations about computer security often have a binary sense to them, as in either a company's systems are secure or they aren't. But a more realistic view might be that of a continuum on which a given company finds itself. There are no absolutes in computer security because of several factors:

- Attackers keep changing their tactics.
- Increasingly complex software creates ever more vulnerabilities.
- Budget constraints make it difficult for IT departments to apply all necessary software updates.
- Users often make mistakes.
- Mobility puts many endpoints of an extended corporate network beyond complete control.

The question becomes how relatively safe from computer threats a company is on any particular day, or even a given hour. The less predictable the threat, the less controllable the response can be. When it comes to unpredictability, employees are the largest threat factor. Even in the face of standard threats, they can forget to take precautions, unknowingly load something dangerous onto a machine, or intentionally go to a potentially dangerous site.

The result is painful, to say the least. In 2009, the average cost of a data breach in the U.S. was almost $6.8 million, with the maximum cost reaching nearly $31 million, according to the Ponemon Institute. The average cost across the U.S., U.K., German, France, and Australia was $3.4 million. The same study noted that in 64 percent of the U.S. cases, the cause was either a malicious or criminal attack or human negligence. The price climbed even higher in 2010.

How common are data breaches? Although getting accurate data on the topic is difficult, if Massachusetts is any example, the answer is very. According to Attorney General Martha Coakley, digital personal information on one third of residents has been compromised. The state gained the statistic from a new tough data breach reporting law.

In 2011 alone, the world saw high-profile computer break-ins of Sony's PlayStation Network, resulting in the loss of personal data on 77 million accounts. Someone stole a laptop out of a car with personal records of 4.9 million military personnel and families. Mobile security attacks

Methodology:

In August and September 2011, UBM TechWeb conducted the State of Cloud Security study on behalf of Webroot. Invitations with an embedded invitation to the online survey were emailed to UBM TechWeb's qualified database of technology decision makers. Those involved in evaluating, recommending, selecting, or setting/approving budget for endpoint or desktop security (software protection of computers and laptops from viruses, spyware and other malware) or Web security (protection from viruses, spyware and other malware when visiting any website via the browser) at companies with 100 to 4,999 PCs or laptops in their organization qualified to be included in the final data set. The greatest possible margin of error for the final data set of these 202 qualified respondents is +/-6.8 percentage points. These procedures were carried out in strict accordance with established market research practices.

Advantages of Cloud-Based Security

The current form of client deployment makes it difficult for IT departments to keep pace with the rapid development of new attacks, increased mobilization of the workforce, and the influx of new devices as parts of the computing infrastructure. Antivirus, anti-phishing, and desktop firewall applications have grown to large programs that make heavy demands on system resources. That impairs productivity, to which users can attest, based on systems being rendered practically inoperable any time an endpoint scan is run.

These programs can noticeably slow overall performance as every application and file must be checked before running or opening. In fact, a software scan can easily run hours, harming employee productivity. The endpoint security software itself often requires significant administrative time for installation as well as management of updates and patches.

The time lag in the process of identifying a problem and then updating endpoints can itself leave companies more open to vulnerabilities. Here is the process as it works today:

1. The security software provider identifies a new threat.
2. Researchers from the security software provider create a signature to that threat.
3. The security software company updates its threat database and makes this, and any other signatures, available to its customers.
4. Company management servers check in on some periodic schedule for signature or software updates.
5. Updates are downloaded and then distributed to each endpoints.

At the very best, this process takes hours. It can also take significantly longer—often multiple days. The greater the lag between threat identification and final installation of the updated database at the endpoints, the greater the chance that one of the endpoints could experience an attack.

Nevertheless, even with all the weaknesses of current security systems, it would be foolish to dismiss antivirus, Web filtering, and other technologies. Researchers constantly scour the landscape for the latest exploits and malware websites. Heuristic technologies look for behaviors that suggest software might be attempting to attack a system.

Companies can greatly benefit from a new approach to endpoint security, one that leverages a new form of delivery and does not require maintenance at every endpoint. That's the advantage that cloud-based security can offer. Not to be confused with securing the cloud, cloud-based security uses a cloud computing platform as the means for delivering security to protect endpoints without the usual large client footprint that is typical of traditional software based endpoint security solutions.

Instead, a small client is installed on an endpoint. This client is sometimes only a fraction of the size of a typical security client. Upon installation, the software undertakes a short initial scan of a few minutes to inventory files and applications on that endpoint, creating a baseline profile for subsequent scans. As new files are introduced into that endpoint environment, the client profiles each new file using a hash algorithm and then checks this profile against a large cloud-based database of known good and bad files. Based on file classification, the cloud determines whether or not to allow file to execute. In the event that a file has never before been seen, the file is allowed to execute within an endpoint sandbox type environment where file characteristics and behaviors can be analyzed to help understand file intent and whether it is malicious or not. Finally, because the cloud system has far more computing power than an endpoint device, it can examine file characteristics and behaviors and render a determination almost instantly, helping to eliminate the window of vulnerability between when an attack is introduced and a signature is created.

The cloud services also enjoy the advantage of always using the latest version of a threat database. Once the vendor adds a new threat, it is immediately available to all endpoints, helping to ensure real-time protection and greatly reduce the threat of zero-day threats.

Adding Web-based security solutions can create a layered approach to security, providing additional protection to traditional endpoint security solutions. Webroot, for example, protects endpoints against known threats and common behaviors of potentially malicious software to identify possible threats before they execute. Additional Web security layers enforce Internet use policy, clean Web traffic, and block Web-based threats in the cloud, before they reach a company's network.

More advanced security solutions also have a mechanism to protect endpoints when they lose their Internet connection. Webroot, for example, not only identifies threats by their behavior on a system, but can lock down various ports and USB connections and take other actions based on a set of pre-defined rules that govern how to handle the perceived threats, until a connection is reestablished.

Securing mobile and laptop users and protecting endpoints from malware were named as the most significant challenges.
—UBM TechWeb State of Cloud-based Security

are expected to double between 2010 and 2011. According to security vendor Webroot, an estimated 85 percent of all threats come via the Web, including such threats as surreptitious malware downloads or phishing sites that harvest sensitive data.

- Three out of 10 organizations reported their businesses' Web security was compromised by employees using personal Web mail accounts, visiting social network sites, and downloading videos.
- Only 15 percent of companies give their enforcement of Internet usage policies a grade of A.
- Web-based applications are extremely or very important for providing customer support at nearly half of the businesses surveyed.
- One out of four businesses reported a Web-based threat compromised confidential information, threatened online transactions or caused a Web server outage.

The rate of change is steep, and the administrative process to keep antivirus definitions and potentially malicious URLs timely would be significant. Unfortunately, budgets don't necessarily keep pace with increased demands. According to the Society for Information Management, 62 percent of companies will either keep IT spending flat or reduce it.

Even as attacks on client systems have taken ever more sophisticated approaches, the infrastructures and needs of IT departments become more complex. For example, mobile workers continue to be a rapidly growing category. According to market research firm Forrester, half of U.S. information workers split their time between office, home, and other locations. As the worker rises in rank, as well as the associated authority and system access rights, so does mobility. Among managers and supervisors, the percentage working from multiple locations jumps to 65 percent. About 90 percent of directors and executives are mobile.

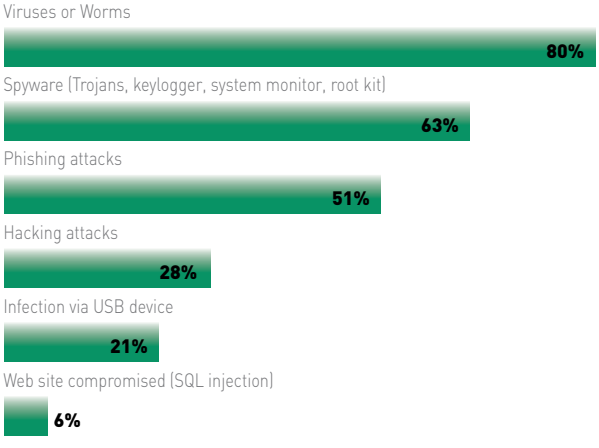
Furthermore, the use of tablets is exploding, with 11 percent of information workers already using the devices to do their jobs. That introduces new potential challenges in securing new endpoints and form factors.

The Pain on the Ground

Of all the emails with malware attached; booby-trapped Web sites; attempts at phishing; and direct attacks on Web sites, servers, and networks; how many actually hit home? To get a better sense of this, UBM TechWeb surveyed more than 200 IT professionals who are actively involved with computer security in businesses with between 100 and 4,999 PCs or laptops in their organizations. Their responses show just how prevalent that dealing with various types of digital attack has become.

One question was, "In the past 12 months, has your company experienced any of the following security problems?" Respondents had a list of common types of security problems and attacks, and could check all that were applicable. Figure 1 shows the data.

Figure 1. In the past 12 months, has your company experienced any of the following security problems?



Note: Multiple responses allowed
Data: UBM TechWeb Survey of 202 business technology decision makers at companies with 100 to 4,999 PCs or laptops in their organization, September 2011

Only 16.3 percent of the survey subjects said that they had experienced none of the security problems listed. The vast majority of companies had not only been hit with at least one type of attack, but the totals suggest that many faced more than one type in the previous year.

But consider the details a bit further. Of the answers, the second and third most frequently cited relate to attacks targeting company endpoints. Employees are subject to falling for phishing attacks, visiting malicious web sites, or opening an email or file that would deliver some sort of spyware. Even the largest answer, viruses or worms, is likely to include a large percentage of viruses originally targeted

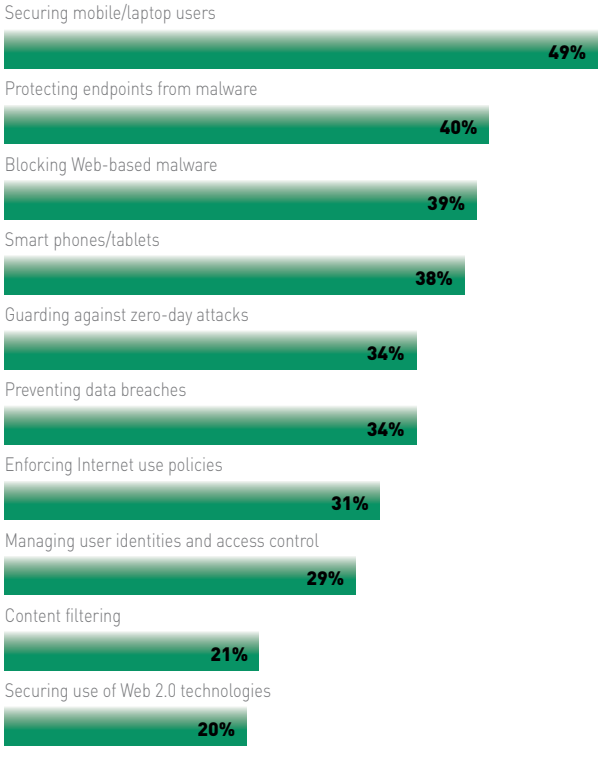
at an endpoint environment.

Now add the 21 percent—more than one in five—of companies that have seen an end user spread an infection by using a USB thumb drive. The logical conclusion is that employees that do what they should not—whether acting maliciously or, more likely, not aware of the risks of their actions—are the most heavily-targeted subjects for attacks and the most likely mechanisms for an attack to take hold in a company. Again, these are figures for a 12 month period.

Another question in the survey supports this finding. Participants were asked, "How challenging are the following security issues for you and your company? They answered using a scale of 5 to 1, where 5 is 'a major challenge,' and 1 is 'not a challenge.'" The possible answers were largely focused on endpoint security. What makes the response noteworthy is just how many companies found themselves challenged by basic security issues.

The critical data here is the combination of the 4 and 5 rankings (shown in Figure 2), which indicates either a challenge or a major challenge. Call the category a significant challenge, for short. The four highest significant challenges were for securing mobile and laptop users, protecting endpoints from malware, blocking Web-based malware, and smart phones and tablets. Although some of the later categories, such as preventing data breaches or managing user identities and access control, are more focused on data security and identity access management issues, each of the top-ranking categories was about endpoint security.

Figure 2. How challenging are the following security issues for you and your company? Answered on a scale of 5 (a major challenge) to 1 (not a challenge).



Note: Percentages reflect combined scores of 4 or 5 on the 5-point scale
Data: UBM TechWeb Survey of 202 business technology decision makers at companies with 100 to 4,999 PCs or laptops in their organization, September 2011

Even some of the lower ranked categories showed significant problems with some basic aspects of endpoint protection. More than 30 percent of the companies found a challenge in enforcing Internet use policies and a fifth had issues with securing use of Web 2.0 technologies.

The problems get harder as employees become more mobile in their work. As one respondent who is a compliance officer for a national organization said about securing laptops, "That's always tough."

Exploits Hit Hard

To realistically discuss security challenges, you have to know what impact they had on an organization. It is basic risk management, in which you compare the likelihood of an event with the damage it can do and the work required to avoid it in the first place.

The respondents answered the question, "In an average month, approximately how many IT employee-hours are spent doing the following for your on-site security software and/or appliances?" They estimated the number for each of the categories in Figure 3.

Again, grouping answers can prove informative. In this case, we'll combine the "1 to 9" and "10 to 19" responses, realizing that almost half of all the companies had fewer than 500 employees. About 71 percent of the companies spend from 1 to 20 hours a month on managing security-related patches. For managing definition file updates, the number was 69 percent. Nearly 60 percent spent that amount of time reimaging machines, while 66 percent did on managing software and/or hardware updates. False positives used 1 to 20 person hours a month for 66 percent, which was the same number for enforcing Internet or email policies.

Even in the worse case, no single category would take more than an eighth of a full-time person. But companies aren't dealing with only a single category. Look at the

Figure 3. In an average month, approximately how many IT employee-hours are spent doing the following for your on-site security software and/or appliances?

	IT EMPLOYEE HOURS						
	Zero	1 to 9	10 to 19	20 to 29	30 to 39	40 to 49	50 or more
Manage security-related patches	3%	48%	23%	9%	2%	3%	3%
Manage definition file updates	14%	54%	15%	7%	2%	1%	2%
Reimage machines	13%	38%	20%	9%	4%	3%	4%
Manage software and/or hardware updates	4%	41%	25%	10%	6%	5%	3%
Deal with false positives	15%	53%	13%	6%	1%	2%	2%
Enforce end user Internet and/or email policies	14%	48%	18%	5%	4%	2%	3%

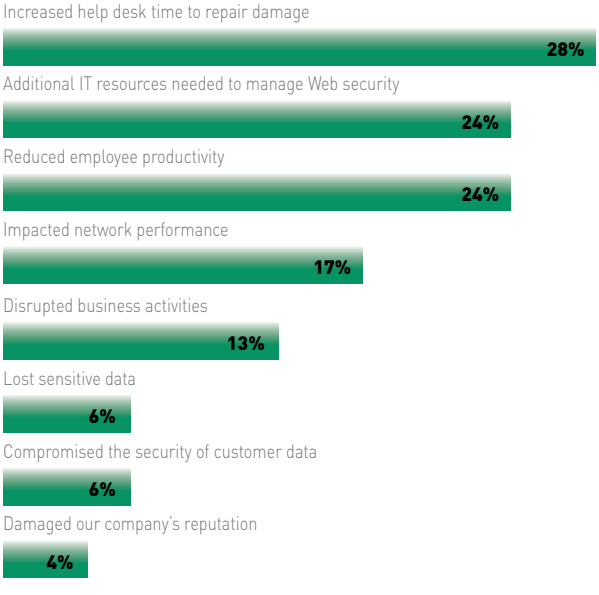
Data: UBM TechWeb Survey of 200 business technology decision makers at companies with 100 to 4,999 PCs or laptops in their organization, September 2011

percentage of companies that spent no time on the average with any given category of security chore. The highest figure is 15 percent, followed by 14 percent. When it came to managing security patches, the number dropped to 3 percent and it was 4 percent for managing updates.

In other words, 97 percent of the companies spent some time every month managing patches and 96 percent had to actively manage updates. Even if the two answer categories were completely exclusive of each other, well over 90 percent of all the companies have to spend between 2 and 40 hours a month managing those two items alone. Given that at most 15 percent spend no time on any one category ("deal with false positives"), chances are that the hours add up.

Now let's delve into the specific impacts that some of the security problems experienced in the previous 12 months had on the various companies. Again, we'll add the top two responses to get a significant impact.

Figure 4. How much of an impact did spyware have on your company?



Note: Percentages reflect combined scores of 4 or 5 on the 5-point scale
Base: 107 respondents who have experienced Spyware
Data: UBM TechWeb Survey of 202 business technology decision makers at companies with 100 to 4,999 PCs or laptops in their organization, September 2011

Spyware

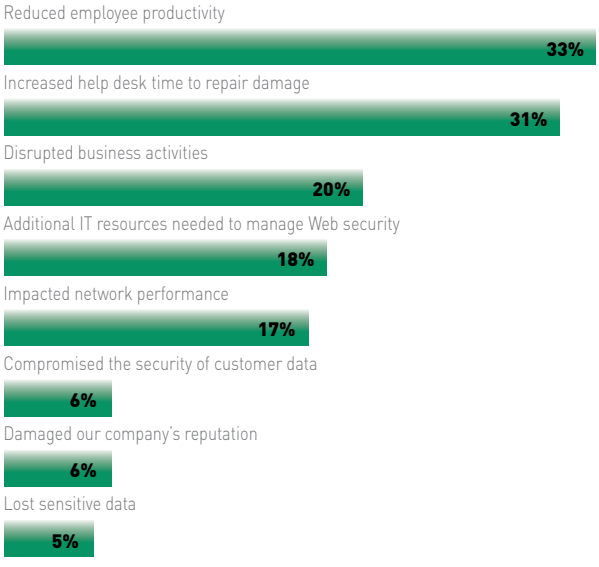
Of the companies that had a spyware attack, 28 percent had a significant impact through increased help desk time to help employees deal with the problem. Almost a quarter needed additional IT resources to manage Web security and the same percentage saw reduced employee productivity.

Viruses or Worms

Here, the impact is heavier. A third saw reduced employee productivity and 31 percent saw increased help desk time to repair damage. In a fifth of the companies, the virus or worm disrupted business activities.

Another way of looking at this data is that viruses, worms, and spyware—the top security problems for endpoints—take a significant toll on employee productivity in general and increase the workload for IT specifically to deal with the attacks. The result is ultimately increased business costs.

Figure 5. How much of an impact did Viruses or worms have on your company with regard to each of these areas? Answered on a scale of 5 (severe impact) to 1 (no impact).



Note: Percentages reflect combined scores of 4 or 5 on the 5-point scale
Base: 139 respondents who have experienced Viruses or worms
Data: UBM TechWeb Survey of 202 business technology decision makers at companies with 100 to 4,999 PCs or laptops in their organization, September 2011

USB Device

The impact of an infection that came from a USB device was smaller than the previous categories. Still, a quarter of the companies needed additional IT resources to manage Web security. Nearly as many (23 percent) saw increased help desk time. Only 17 percent saw reduced employee productivity.

Hacking and Website Compromise

We'll take both the hacking and website compromise issues together because they represent more of the network or infrastructure security breach rather than that of an endpoint.

Compared to some of the endpoint security examples above, hacking attempts to breach a company's systems had an even smaller reaction. Just 21 percent saw increased help desk time or the need for additional IT resources to manage Web security.

For direct compromises of a corporate website, the lowest scores went to disruptions, increased help desk time, and damaged company reputations. There are various reasons that answers for these two questions ranked as they did. Attacks on infrastructure are typically concentrated exploits. They seek to do damage at a central point. Endpoint attacks, however, are often more distributed. Treating one can mean working in more places to solve a problem, and that takes more time.

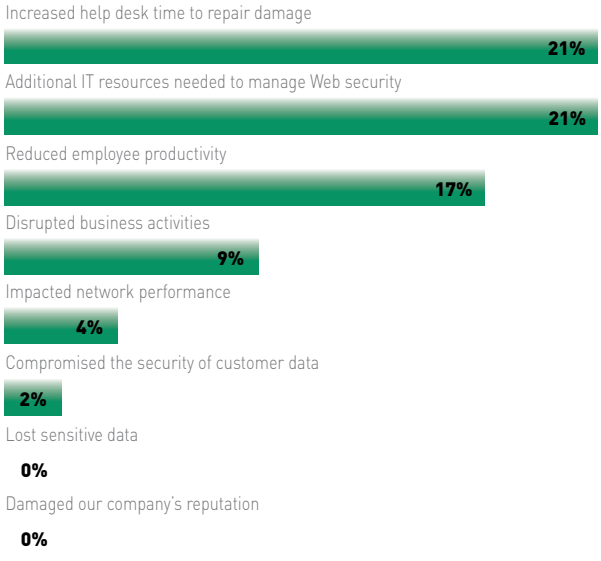
None of the figures indicate how many additional resources or time were necessary to clear up a problem. So a fair comparison between endpoint breaches and central infrastructure breaches is impossible to make. It could be that the resources necessary to fix a central problem are more than for an endpoint problem.

However, as became clear through other responses, endpoint breaches are far more common, and the resources they demand can be considerable. The national organization compliance officer we interviewed for this paper mentioned a problem his organization had a few years ago because antivirus definitions were not correctly updating. Correcting the error required spending an hour a machine to manually adjust the registry and replace software. "There were four or five of us doing that," he said. "It was a late Friday night

Figure 6. How much of an impact did an infection via USB device have on your company with regard to each of these areas? Answered on a scale of 5 (severe impact) to 1 (no impact).

Note: Percentages reflect combined scores of 4 or 5 on the 5-point scale
Base: 36 respondents who have experienced an infection via USB device
Data: UBM TechWeb Survey of 202 business technology decision makers at companies with 100 to 4,999 PCs or laptops in their organization, September 2011

Figure 7. How much of an impact did hacking attack(s) have on your company with regard to each of these areas? Answered on a scale of 5 (severe impact) to 1 (no impact).



Note: Percentages reflect combined scores of 4 or 5 on the 5-point scale
Base: 47 respondents who have experienced Hacking attack(s)
Data: UBM TechWeb Survey of 202 business technology decision makers at companies with 100 to 4,999 PCs or laptops in their organization, September 2011

and all day Saturday." That translated into 10 to 15 extra hours per person.

Sometimes what starts as an isolated endpoint attack can spread and do significant damage to a company network and other endpoints. The CTO of an accounting and IT consulting firm remembers a client in which someone in upper management received a phishing message that appeared to come from a partner but was actually from a competitor who had an accomplice inside the client. The partner logged into the site, which downloaded malware to his computer, which sent sensitive data to the competitor and then wiped the data from the company's computers.

Moving Forward with One Foot in the Past

The CTO of a home healthcare agency who was one of the survey respondents described how new technology was remolding the way his company did business. Roughly 80 percent of the company's employees work in the field providing services to clients. Three-quarters of them already use Apple iPads, with the remaining ones ready to switch. All their work is done through a Web-based system over a browser.

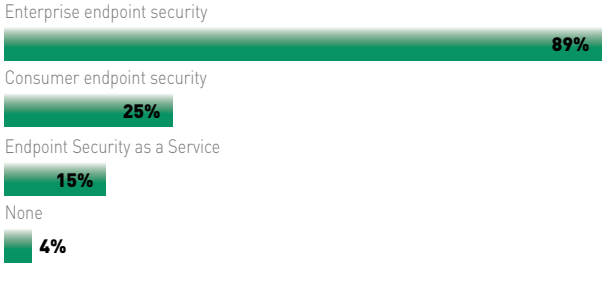
Currently, the CTO knows that viruses are uncommon for the new mobile devices. "If someone tells me there are things in the wild in terms of viruses that can harvest things on Apple iPad, then, yes, I'll have a concern, but until then I have other fish to fry," he says. However, the employees all own their tablets and have the right to download any apps they choose. "We felt that if we started to lock it down so it was iron-clad and secure, they wouldn't enjoy the novelty of it and would be less likely to use it for what we want them to use it for," he says. This approach potentially introduces new risks that the company's current security solution—a hardware firewall, email security software that acts as a front end to a Microsoft Exchange server, and server-delivered antivirus updates—were never designed to protect.

Even as the connected world becomes more intricate, the underlying nature of corporate response to potential threats has remained largely the same. IT departments install antivirus software on machines that then require regular virus definition updates. The update process can be automated, but as the compliance officer mentioned, it isn't a foolproof system.

Similarly, companies also typically run Web-filtering and other anti-phishing solutions that require regular updating. Because these solutions are mostly on-premise hardware or software, they also contain a fundamental weakness. Only endpoints that are actually connected to the corporate network are protected. Remote users outside the company firewall may go unprotected, increasing the risk of not only an infection to that user but also a broader infection to the company the next time that remote user connects to the network.

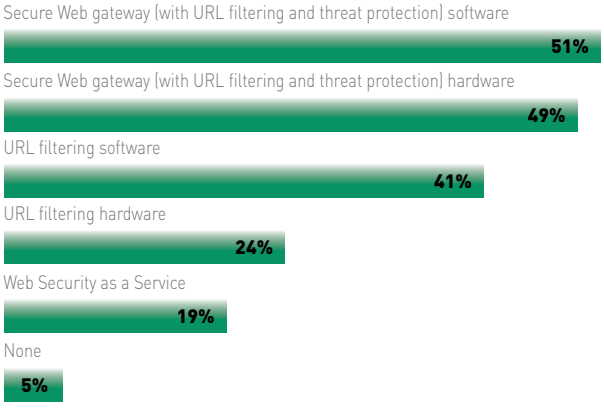
UBM TechWeb asked the subjects about how they currently implemented endpoint and Web security. One of the questions was, "Which of the following endpoint security

Figure 9. Which of the following endpoint security solutions are implemented at your company today?



Note: Multiple responses allowed
Data: UBM TechWeb Survey of 202 business technology decision makers at companies with 100 to 4,999 PCs or laptops in their organization, September 2011

Figure 10. What types of Web security solutions does your company use?



Note: Multiple responses allowed
Data: UBM TechWeb Survey of 202 business technology decision makers at companies with 100 to 4,999 PCs or laptops in their organization, September 2011

solutions are implemented at your company today?" Figure 9 shows the responses.

The vast majority of companies use traditional endpoint security software that resides on an endpoint device. Only 15 percent of the companies used a Software as a Service (SaaS) endpoint security solution. Although not as pronounced, a similar pattern appeared when respondents were asked, "Which of the following Web security solutions are implemented at your company today?"

Not even a fifth uses a SaaS offering, although that is not because the respondents were largely unaware of the option. When asked to rank their familiarity of security SaaS from 1 to 5, with 5 being "very familiar" and 1 being "not very familiar," 49 percent gave either a 4 or 5 rating. Only 24 percent said 1 or 2. Companies still rely heavily on hardware and software security solutions that reside on-premises. These solutions use an older security model that provides inadequate protection for workers at remote sites or who are traveling.

Why Companies Are Stuck

The reasons why IT departments have not adopted cloud-based security come down to 3 basic issues:

- "If it ain't broke" syndrome
- No time to change
- Concerns about cloud-based systems

It Ain't Broke

When companies have already invested in systems, they are reluctant to replace them for both budgetary and operational reasons. The home healthcare agency already has a set of security products and it has had no digital security problems in the last year. The only issue it faced was when someone broke into a vehicle and took a bag with information on a few patients.

Ironically, cloud-based security is something the company would consider if the server for the main office were nearing end of life. But the machine is only 18 months old and well-configured to handle expansion. The company already plans to run 90 percent of its patient-specific activity on a cloud-based software suite. Even at that, there are conditions under which the company would consider making a shift.

"If we started to increase our headcount tremendously here, if we had to double, I certainly would consider cloud a better solution than adding resources, human and physical," the healthcare agency CTO says. His only question would be about the learning curve his users would face for moving to "something like Google Docs for spreadsheets and word processing."

No Time to Change

The national association compliance officer has not even piloted a cloud-based security project because there are too many other demands on the IT department's time. "As we're expanding our portfolio of applications delivered through the public Web, we're focusing on the software implementation to deliver value to end users, as opposed to dramatically or wholesale redoing our security philosophy," he says. There are only 12 IT staff members, with three on operations and the remaining nine working on various projects and application development.

He does think that eventually the organization will reconsider how it does security, "but we just haven't gone down that road yet." That will likely happen in the future, but not for two to four years because there is not a perceived urgency to make the shift.

Cloud Concerns

The consulting firm CTO had the greatest reservations about cloud computing for three reasons. One is that vendors essentially turn what were once indefinite software licenses into annual payments that his budget must cover. "For instance, I will never recommend Microsoft Office 365

or one of the equivalents to anybody," he says. "If Microsoft ups the price, you're going to end up paying that for a long time until you can migrate everything to something else."

The second is the idea of passing responsibility for a business function to a third party makes a company vulnerable to either temporary or permanent disruption. "IT has become a critical part of the business infrastructure and I don't believe in leaving part of that in someone else's hands," he says.

The third concern is constant connectivity. Without an active connection to the Internet, a cloud service does a company little to no good. The consulting firm and its clients are in a part of a state served by a single communications link that over the last 18 months has seen outages lasting from a half hour to more than a day.

That said he sees cloud-based security as a different issue than other cloud services. "If I were in an area where I had a dependable Internet connection, I wouldn't have a problem using software as a service for my security," he says. "I would still be looking at issues like the total response time. I'd test to see if the time to open a file was longer." But his concerns about cloud delivery wouldn't apply because companies already pay for annual security software fees and using a cloud service doesn't transfer responsibility for security any more than installing software and hardware protection.

Only 15 percent of the companies surveyed used a SaaS endpoint security solution.
—UBM TechWeb State of Cloud-Based Security

Why Companies Should Consider a Shift Anyway

However, the gains that a company can make with a shift to cloud-based security likely overshadow the near-term costs. The cost of a U.S. data breach has reached $214 per compromised record. If a breach involves 10,000 records—and some breaches have reached the tens of millions—the price would hit six figures. In fact, the average cost of a U.S. data breach in 2010 was $7.2 million.

Once a breach happens, the price of changing the approach to security is trifling in comparison. But there are other reasons. UBM TechWeb asked the degree to which respondents agreed with the following statements, with 5 meaning strongly agree and 1 meaning strong disagree.

Figure 11. To what extent do you agree with the following statements? Answered on a scale of 5 (strongly agree) to 1 (strongly disagree).

Note: Percentages reflect combined scores of 4 or 5 on the 5-point scale
Data: UBM TechWeb Survey of 202 business technology decision makers at companies with 100 to 4,999 PCs or laptops in their organization, September 2011

Once again, consider the combined 4 and 5 answers (see Figure 11). The top answer was for the statement, "I want to enjoy my weekends and time off rather than deal with security problems." It seems humorous until you consider that there is weariness in the choice. Security problems easily turn into required overtime because they must occur over and above regular work.

An IT department can't choose between fixing the aftermath of an attack and implementing a new software system or undertaking normal network maintenance. Everything must get done. That puts additional stress on IT personnel at a time when technical employment markets are rebounding and the chance of losing key employees grows.

The other popular answers are revealing. Right now, about 45 percent, just shy of half, of the companies lose the opportunity to work on strategic initiatives because of the time that security solutions take. More than half of the companies find it difficult to keep up with emerging threats, which suggests that they are more at risk. And less than half found endpoint security solutions to have minimal conflicts with other applications, meaning that more than half spend time dealing with the clashes between software. Finally, as only 27 percent of the respondents found scans to be fast, the other 73 percent are losing productivity.

Perhaps it's time for your company to consider shifting

from traditional heavy footprint endpoint security to a cloud-based system for more current protection, better coverage for remote and mobile devices and improved IT capacity, allowing the IT department to focus on more strategic initiatives. ◆

About Webroot

Webroot is a leading provider of Internet security for consumers and businesses worldwide. Founded in 1997, privately held Webroot is headquartered in Colorado and employs approximately 450 people globally in operations across North America, Europe and the Asia Pacific region.

Consistently rated among the best home and enterprise internet security offerings available, Webroot's products include email, Web and archiving internet security services for businesses, and antimalware, privacy and identity protection for consumers. www.webroot.com

UBM TechWeb Marketing Services:

ubmtechweb.com/marketing-services

Ed Grossman:	*Executive Vice President, InformationWeek Business Technology Network*
Martha Schwartz:	*Vice President, Integrated Media*
Pamala McGlinchey:	*Vice President, Marketing Operations*
Elliot Kass:	*Vice President, Content Services*
Gene Fedele:	*Vice President, Corporate Creative Director*