WHITE PAPER:
WEB SECURITY

Bandwidth Bandits

Who should read this paper

Internet bandwidth is a finite and expensive resource; protect it from spammers, criminals, hackers, time-wasters and employee misuse.

A Symantec.cloud whitepaper

Symantec.cloud

Content

Introduction

Internet bandwidth is a finite and expensive resource; protect it from spammers, criminals, hackers, time-wasters and employee misuse.

Your company's internet link is precious. Not only is it expensive and limited but it is a vital business tool. Yet our analysis shows that companies can lose around a quarter of their internet bandwidth to employee web misuse, streaming media and spam. Imagine if you had to give up a quarter of your office space for non-work activities; it's inconceivable. But when it comes to internet bandwidth, most companies don't even know about the loss, let alone take steps to prevent it.

In the lead up to major sporting events, employees will want to watch real-time TV feeds from their desks. This may trigger internet brown-outs in companies that are unprepared.

Part of the problem is that the internet is designed to continue operating even if links are busy or damaged; indeed that's the whole point of it. This means you probably don't notice if your emails take longer to deliver, web pages take longer to load and internet phone and video conferences are lower quality. It all sort of works and you expect the occasional hiccup.

That doesn't mean bandwidth loss is irrelevant. In fact, there are serious consequences:

- You buy more expensive connectivity than you need
- Business-critical internet connections, such as remote users' VPN (virtual private network) connections or business-related web use, are slower than they should be, wasting people's time
- In some circumstances, such as spam spikes or when everyone in the office is watching the same World Cup match, you may experience service outages or serious delays
- Internet communications such as desktop video conferencing, VOIP (voice over IP or internet telephony) have lower quality
- As internet-delivered applications and services become more widespread, important business functions such as customer relationship management will depend on a fast, high-quality internet connection

Bits, Bytes and Megabytes

Employees are used to having fast internet connections at home and have come to expect that they can chat with their friends, browse photos, listen to music and watch TV over the internet. So when they come to work, they do the same there. If you have a hundred employees, the majority of them will have their own fast broadband connections at home. In the office, all of them have to share just one connection. So expectations are going up and the available bandwidth stays the same.

To make matters worse, the size of files and streams delivered over the internet has increased. When the internet first took off in the early 90s, most web pages were text-only. Today, it's perfectly normal to stream high-definition video over the internet. But a minute of HD video uses up massively more bandwidth than a page of text.

To understand the difference, consider that a King James Bible takes just 1.34 megabytes in text format[1]. If it were scanned in as a series of 1,200 black and white pictures, it would require 58 megabytes[2] – a huge increase. An unabridged voice recording of the same book runs to over 79 hours[3].

1- Project Gutenberg Literary Archive Foundation; King James Version Bible text: http://www.gutenberg.org/ebooks/10
2- Wikipedia, Tagged Image File Format, TIFF B&W file size at 300 DPI = 50 kB: http://en.wikipedia.org/wiki/Tagged_Image_File_Format
3- Audible, Inc; Unabridged Bible recording 79 hours and 42 minutes, http://www.audible.co.uk/

In MP3 format, this would require 4.3 gigabytes[4] – yet another huge increase. This is about the same as a single DVD's worth[5] of video information, for example, Monty Python's Life of Brian. In other words, each step from text to pictures to audio to video requires a huge increase in bandwidth.

Who Ate All The Bandwidth?

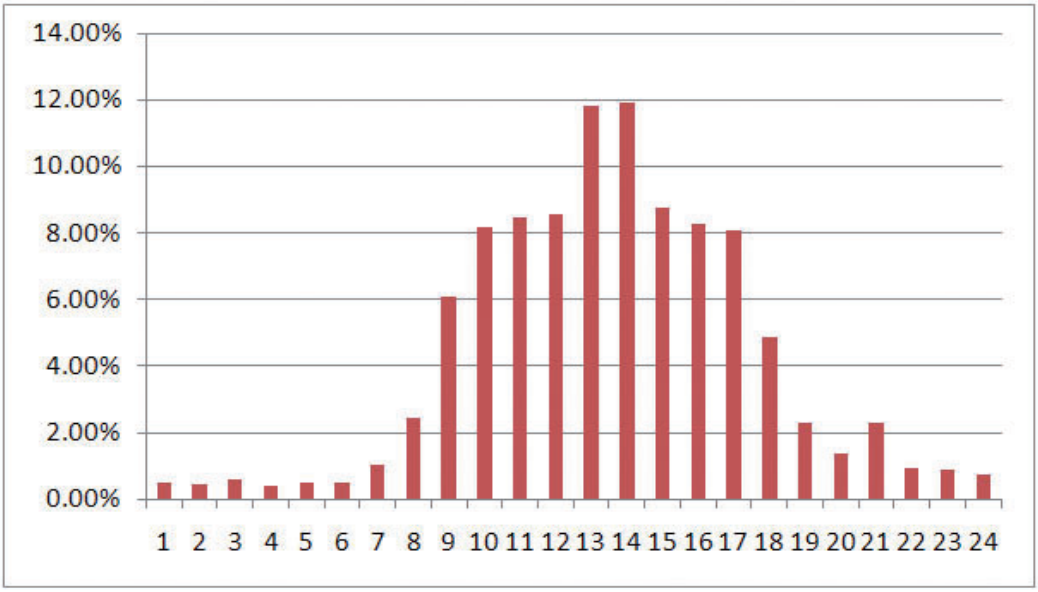
The Symantec Intelligence team at Symantec.cloud sees billions of web and email connections every day. As the market leader for cloud email and web security, they have a unique insight into the real state of the internet as a whole. In particular, they can see exactly what people do online. The top ten most-blocked website categories are:

CATEGORY	**% OF BLOCKS**
Advertisements & popups	**30.5%**
Social Networking	**28.6%**
Streaming Media	**7.2%**
Computing and Internet	**4.0%**
Peer-to-Peer	**3.5%**
Chat	**3.1%**
Hosting Sites	**2.8%**
Games	**2.0%**
News	**1.7%**
Entertainmet	**1.5%**

The majority of these blocked sites use lots of bandwidth. For example, social networking, audio streams and games and adverts all use lots of multimedia content which uses much more bandwidth than plain text or emails. Social networking and Streaming media are the worst culprit because video and audio need the most bandwidth. Almost 36% percent represents the very large drain on companies' internet connectivity.

The majority (87 percent) of non-work internet usage occurs between 8am and 6pm. The busiest time is over lunch but personal internet use is pretty constant during working hours.

4- Typical MP3 recorded at 128 kilobits per second
5- Wikipedia, DVD, http://en.wikipedia.org/wiki/DVD



Bar graph: Websites blocked by Symantec.cloud services over a 24-hour period

When it comes to bandwidth-intensive streaming media, the story is very similar; except that streaming media is more popular in the afternoon than the morning and there is another mini-peak around 5pm when people are getting ready to go home.

Spam Spikes and Blowback

Streaming media and web browsing represent a constant drain on your bandwidth but email poses a different kind of risk. It is less bandwidth-intensive because individual emails are relatively small in size. However, the sheer volume of spam and the constant stream of unwanted messages represent a constant drain.

It is completely possible, on a bad day, for a company with a hundred employees to receive 1,000 legitimate emails and 200,000 spam messages. Around 70.6 percent of all emails processed by Symantec.cloud services are spam messages[6].

The problem is made worse by spammers' use of random name generation to send emails to people at a given address even if they don't work there. For example, you might be joe@bloggs.com but spammers are also sending email to brian@, jane@, phil@ and uncle-tom-cobbley@bloggs.com too. It costs them nothing to send these messages because they use malware to turn thousands of unprotected PCs into spam factories.

Spam spikes and bounceback (also known as blowback or backscatter) spam can cause huge, short-term bandwidth problems. Spikes occur when spammers try new tactics, new botnets come online or when spammers use attachments in their spam messages. Spikes can produce a 25-fold increase in spam in a short period. Bounceback spam occurs when spammers use your email address as the 'reply-to' address in their messages. You end up dealing with all the 'message not delivered' and 'out of office' responses from recipients. This can produce another temporary burst in traffic and some companies see more than half of their spam load resulting from bounceback.

6- http://www.symanteccloud.com/en/au/globalthreats/charts/spam_monthly

Dealing with spam is a burden on companies with in-house spam filtering software. Every message has to be downloaded, whether it is wanted or not. It must then be processed to check if it is spam or if it contains malware. With nine spams for every real message, the result is that many companies have email systems that are ten times more capable (and expensive) than they actually need to be to process legitimate emails. When a spam tsunami hits, everything slows down. As a result, expensive bandwidth is wasted and legitimate business emails must wait their turn for processing, causing unnecessary delays.

A new trend, tracked by analysts in Symantec Intelligence, is that spammers are increasingly using the TLS protocol to send spam messages. TLS is an encryption system that ensures that messages sent from one mail server to another cannot be read by third parties. It's like putting post cards in envelopes. Spammers are using this protocol because it increases the chances of spam messages getting through defences, but it is also a bandwidth problem because each email now requires an extra two-way exchange of information to set up the encrypted link.

Rustock, one of the largest spamming botnets, sends 70 percent of its spam using TLS. Because Rustock spam accounts for a large proportion of global spam, this means that overall 20 percent of global spam is sent using TLS. This could increase rapidly if other botnets decide to follow Rustock's lead. If this trend becomes widespread, it could significantly increase the bandwidth drain caused by spam.

Protecting Roaming Users

Roaming and home-based workers present another bandwidth challenge. Mobile users typically have a slow wireless broadband connection via the mobile phone network. These links have a fraction of the capacity of landline connections. They can also be very expensive, with monthly costs per user running up to $186.341[7] and significant penalties for exceeding download limits.

Similarly, home workers with consumer broadband connections have limited bandwidth but may need most of it simply to maintain a VPN, VOIP or remote desktop link back to the company. If they start browsing the internet intensively or streaming video over a company-provided internet connection, it could affect their ability to do their job by slowing down their office links.

Both limitations – on mobile and home workers – mean that companies need to pay more attention to what they allow their employees to do online.

Calculating The Cost

What is the cost of all this waste? Taking a typical small to medium-sized firm as an example, with a leased line internet connection and around 100 employees, web misuse and email spam could waste around 23 percent of their internet bandwidth and cost thousands of dollars a year. Of course, your mileage may differ but our calculations and the research behind them may be a good starting point for estimating your own costs.

Let's take the direct costs first; that is the immediate cost of the bandwidth. A company might have a one megabit/second leased line that costs $645.00 a month[8] that provides a maximum capacity of 10,800 megabytes per day. With a hundred employees spending, on average, an hour a day browsing the web at 40 pages an hour[9] and an average page weight of 312 kilobytes[10], that would account for 1,218 megabytes a day or approximately 10 percent of the available bandwidth.

7- Typical data plans on Vodafone run from $17.20 - $186.34 per month depending on the cap: http://online.vodafone.co.uk/business/s/price-plans/
8- Zen Internet Ltd, Ethernet Line, http://www.zen.co.uk/LeasedLines/Products/ethernet.aspx
9- Useit.com, Jakob Nielsen, Alertbox, Typical time per page: http://www.useit.com/alertbox/percent-text-read.html
10- Website Optimization, Average Top 100 Weblog Performance Survey, Top 100 websites: http://www.websiteoptimization.com/speed/tweak/average-top-100-weblog/

Symantec Intelligence reveals that 7.3 percent of all blocked websites are multimedia streaming sites, so let's assume that they spend 7.2 percent of that hour a day (i.e. 4.3 minutes) online browsing video sites. One hour of low-resolution internet video is 128 megabytes of data[11] so 4.3 minutes requires 9.2 megabytes per employee per day – another 1,280 megabytes or 10 percent of the available bandwidth.

However, if they decide to leave a window open to watch a football match or listen to music while they work, the amount of downloaded data could increase dramatically. Also, higher-resolution or HD video requires significantly more bandwidth than standard resolution.

Email is a smaller burden, providing there are no spikes. If you assume 1,000 spam messages a day per employee at five kilobytes per message[12], that equates to 516 megabytes a day. However, if the majority of those spam messages arrive in the course of an hour, it could squeeze out legitimate traffic and overwhelm email servers.

All told, even with relatively modest levels of personal web use and plausible levels of spam, your company could be wasting 2,985 megabytes a day or 27 percent of its download bandwidth. That costs the company $2,090 a year.

The easiest way to do these calculations is to use Google calculator. For example, simply enter '4.3 minutes x 128 megabytes an hour' or '24 hours x 1 megabit per second' into the search box and press enter. Wikipedia has more information about the bandwidth required for different types of media: http://en.wikipedia.org/wiki/Bit_rate.

Beyond the raw cost of the connection, wasted bandwidth has a tremendous opportunity cost. It squeezes capacity for legitimate traffic, slowing down business web use and email. Dealing with spam in-house requires expensive servers and software. Employee time wasting has a real cost in terms of salary and missed opportunities. Even the disruption caused by one person watching a football game and disturbing his colleagues has a cost.

Reclaim Your Bandwidth

There are several measures you can take to reclaim your bandwidth:

MEASURES TO RECLAIM YOUR BANDWIDTH	WHY DO IT?	HOW SYMANTEC.CLOUD CAN HELP
Analyze your own usage	Use existing tools to get some insight into how your existing bandwidth is being used. E.g. some firewalls have the ability to report on the types of traffic passing through them, and anti-spam software or services can give you an idea of the volume of spam reaching your systems.	The Symantec.cloud dashboard provides flexible reports via a web browser that include web usage volumes, percentage of web requests blocked by AntiVirus, AntiSpyware and URL Filtering services, the top sites. You can also get information about bandwidth used and time spent on websites by individuals.
Quality of service	Some firewalls and routers allow you to give priority to certain types of traffic. E.g. you can give a higher priority to email traffic than web or make sure that VPN and VOIP traffic has the highest priority. This	You can use **Symantec Security Safeguard.cloud** to restrict access to nonessential sites, freeing up bandwidth for business critical services. E.g. you can restrict access to media streaming sites outside lunchtime.

11- Wikipedia, Streaming Media, http://en.wikipedia.org/wiki/Streaming_media
12- Symantec Intelligence estimate of average email size in Dec 2012

MEASURES TO RECLAIM YOUR BANDWIDTH	WHY DO IT?	HOW SYMANTEC.CLOUD CAN HELP
	won't reduce the wastage but it will help reduce the impact.	
Stop spam in the cloud	If you can stop nwanted email before it starts its journey through your internet connection to your servers, you free up all the bandwidth it uses and you don't need so much server capacity to process it. Cloud-based security and spam filtering services also block emails sent to non-existent addresses at your domain, further cutting the amount of spurious traffic you get.	***Security SafeGuard.cloud*** blocks 99 percent of spam before it ever reaches your network or your internet connection. With a false positive rate of 0.0003% and an easy to use quarantine system, you can be sure to get all the emails you do want and avoid nearly all the ones you don't.
Block inappropriate web use	Supported by acceptable use policies, employee awareness, training and enforcement, website filtering and blocking can be very effective at ensuring that business traffic gets through and non-essential usage is kept to a minimum.	***Security SafeGuard.cloud*** gives you control over who can access what online. You can set policies for the whole company, departments, types of employee or even on an individual basis. You can differentiate between websites that are absolutely offlimits, such as porn sites, and sites that you want to control but not ban altogether. For this reason, ***Security SafeGuard.cloud*** lets you set time limits on people's use of non-work websites.
Control remote users	Mobile and home workers have very limited and expensive bandwidth. If you can control the sites and services they use, you can keep costs down and ensure that their bandwidth is available for work purposes, such as internet phone systems and VPN connections to the office.	***Security SafeGuard.cloud*** extends web protection and filtering to remote users, including policy enforcement. It also ensures that remote users' online activities are tracked by the service's reporting tools.

Symantec Security Safeguard.cloud

Every week, ***Security Safeguard.cloud*** blocks millions of malicious, inappropriate or unapproved website requests for thousands of companies and billions of dangerous and unwanted emails. Whether it is email, websites or instant messaging, ***Security Safeguard.cloud*** will protect companies from more than malware and spam; it will help enforce acceptable use of IT systems to protect productivity, competitiveness and profitability.

About Symantec.cloud

Symantec.cloud, a division of Symantec Corporation, offers customers the ability to work more productively in a connected world. More than 55,000 organizations ranging from small businesses to the Fortune 500 across 100 countries use Symantec.cloud to administer, monitor, and protect their information resources more effectively. Organizations can choose from 18 pre-integrated applications to help secure and manage their business even as new technologies and devices are introduced and traditional boundaries of the workplace disappear. Services are delivered on a highly scalable, reliable and energy-efficient global infrastructure built on fourteen datacenters around the globe.

Symantec.cloud
Symantec Corp.
Level 14, 207 Kent Street,
Sydney NSW 2000 AUSTRALIA
Tel: +61 2 8220 7000
Fax: +61 2 8220 7075