

Whitepaper:

Effective business bandwidth management

Contents

The problems.....	3
Malware.....	3
Copyrighted material.....	3
Unlicensed software.....	4
Questionable Content.....	4
Lost Productivity.....	4
The solution.....	5
How do you do it?.....	5
Free time.....	5
White and black lists.....	6
Downloads.....	6
Keeping bandwidth in check.....	6
Win the bandwidth battle.....	6
This is how GFI WebMonitor can help.....	7

There is some good news in the world of networking – maximum available bandwidth is increasing at a rapid rate and prices in general are falling. You would think that we should have all the bandwidth we need at a price we can well afford. Unfortunately this is not the case as bandwidth demands are increasing faster than the pipes are growing.

The problems

When available bandwidth starts to feel the squeeze, end-user applications slow to a crawl, as do critical systems and, finally, business operations. And while bandwidth is going down in price, the overall cost of Internet and WAN access can still be staggering. Bandwidth consumption is not the only problem businesses face.

Malware

Users are constantly at risk from malware. Whether they are trying to download the coolest screensaver, install a new tool, or they just happen to stumble across a compromised site, the risk is high that they will pull down some piece of malware that at best crushes productivity; at worst it could provide an attacker with a way into your network.

Copyrighted material

Some of your users may also be on the hunt for the latest musical hit from their favourite band, or that blockbuster smash that they missed in the theatre but which isn't on DVD yet. Either way, they may not even realize that downloading copyrighted material is wrong, let alone that it puts the business at risk.

Unlicensed software

Everyone has their favourite app, that does exactly what they need. If you don't have a license for that app, does that mean they won't just go out somewhere to download it, and perhaps a keygen as well? When your users have access to the Internet and lack an understanding of software licensing, they can put your business into a very sticky situation with software vendors.

Questionable Content

There's a time, and a place, for just about anything on the web, but during business hours is definitely not the time, and at work is definitely not the place, for a lot of what can be found online. Avoiding HR issues is not only good manners, it's also good business, and you don't want anyone to be offended or feel uncomfortable at work.

...Businesses
need to maximize
performance while
minimizing costs.

Lost Productivity

Has this ever happened to you? You go to check one thing on one social media or news site... it will only take a minute. The next thing you know, you're late to a meeting because you lost track of time. The Internet can be a black hole for productivity, and even the best of us will click on that link with the compelling headline, because it will only take a minute!

In short, businesses need to maximize performance while minimizing costs.

Some businesses use a combination of devices and software to maximize bandwidth such as bandwidth shapers and performance management tools. But these overlook the fundamental problem – end users run applications and exhibit web behaviors that hog bandwidth.

The solution

The easiest and perhaps most effective way to maximize bandwidth is to manage the demand side. Do users really need to watch YouTube videos all day, stream music in the background, or access their Netflix accounts? While some casual surfing is a boost to employee morale, too much squeezes your Internet and WAN connections, and brings productivity to a standstill.

How do you do it?

The first step is to have a clearly defined Internet usage policy that states what apps are permissible, which are off limits, and how much time can be spent on personal surfing.

TIP:

You can find a sample Internet Usage Policy on <http://www.gfi.com/pages/sample-internet-usage-policy>

A policy is nothing without the means to enforce it. Here you need to be able to manage what users can do on the web, such as:

What URLs can be accessed

What apps are allowed

What search settings should be enforced

How much time can be spent on particular apps as well as what users cannot do on the web, such as:

- What URLs are blocked
- What apps should not be used
- What content is prohibited by policy

Now that you've set policies and educated users, you need to turn to the specifics of the policy and how you'll manage each area.

Free time

You may decide that lunchtime is a free surf zone where users, on their break, can check the latest sports scores or look up the current news and weather reports. The advantage here is that there is less work demand on network bandwidth during the lunch break.

White and black lists

You can white and blacklist web sites based on acceptable use and your company's own culture. A music company would probably want to allow music downloads and streaming while a sports company will likely want open access to sporting web sites.

Downloads

Downloads are a major problem for network bandwidth and security. Even if the policy forbids all or most downloads, some are sure to try and break the rules. Whether malicious or based on size, you want the ability to block these downloads in real time based on IT intervention or by enforcing policies in an automated fashion. And instead of simply blocking downloads, you should be able to set quotas so a certain amount of downloads are allowed.

You can set download limits, or set time limits on bandwidth-intensive sites.

Keeping bandwidth in check

Bandwidth is a precious resource and demand for it is unrelenting. That means you want to make the most of the connections you have, and not waste them. With monitoring, you can determine which users consume the most bandwidth, and which types of content are most problematic. You can also take steps to limit bandwidth use, by blocking the download of large applications, video files and other large files.

At first, users may not be thrilled with a monitoring policy, but they may soon realize just how well it can protect the organization that gives them their paycheck and they don't have to worry about visiting a site that could get them (and the company) into hot water.

Win the bandwidth battle

URL, search and Web monitoring can cut the demand for bandwidth dramatically. Not only will your network be faster, you can put off major network upgrades and save money in the process. All three of these technologies, which are found in GFI WebMonitor, can easily block in real-time the downloading of applications and large files such as video or music.

These tools can also identify which employees are using the most bandwidth and then set controls on what they can do. Bandwidth controls can be based on amount of data, for example allowing no more than 100MB a day to be used, or by time spent browsing certain categories of sites.

Just knowing bandwidth and web management technology is in place in the organization can change user behavior. If users are aware of the company's internet usage policies, and know that everyone's web usage can be tracked, their browsing habits will change.

This is how GFI WebMonitor can help

Too many IT pros take a point solution approach to security with a firewall from one vendor, antivirus/antimalware from another, and perhaps other forms of protection from other providers. These tools are by definition not integrated and do not provide defense-in-depth style protection.

GFI WebMonitor offers an integrated suite of defense tools that includes strong antivirus protection with the inclusion of three of the world's top AV engines, state of the art phishing protection and malicious and vulnerable URL filtering.

Another great benefit involves application control. GFI WebMonitor can discover and control over 1,000 apps including those for online storage, file sharing, games and many more. This means IT can allow or block internet access to these apps. Through the product's advanced granular controls, for instance, IT can allow the use of social media in some departments, and block it for others. Time spent on social media and other apps can also be managed through policies.

GFI WebMonitor can stop malware in its tracks, prevent data leakage, put an end to phishing, keep your business in compliant, maximize bandwidth, and make sure employees are not wasting company time on non-productive web activities.



GFI WebMonitor™
Web security, monitoring
and internet access control
Download your
FREE 30-day trial
gfi.com/webmonitor
→



For a full list of GFI offices/contact details worldwide,
please visit: www.gfi.com/contact-us

Disclaimer. © 2016. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners. The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document. If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.