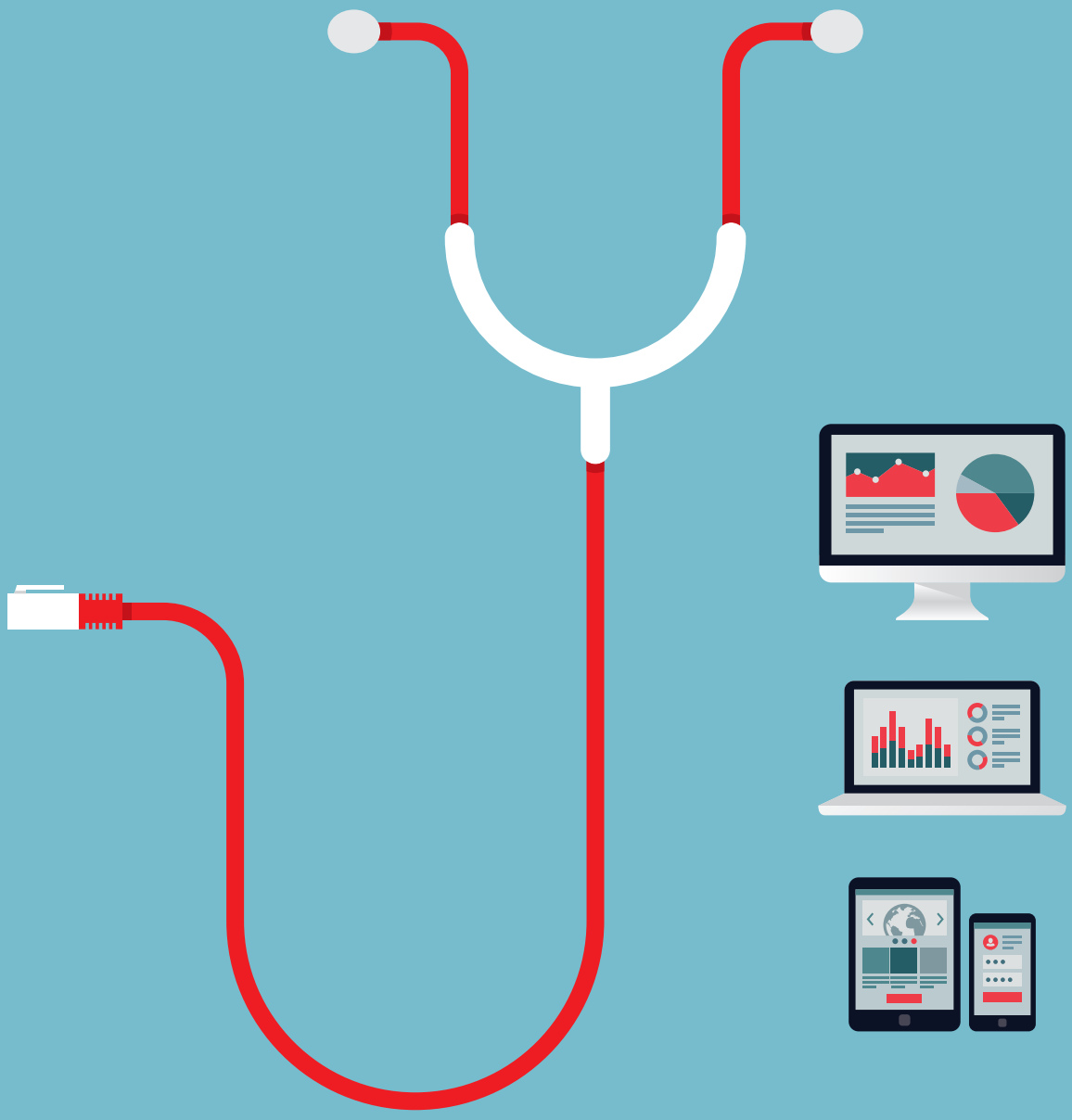


Five steps to improve your network's health

GFI LanGuard™

Network security scanner and patch management

On April 7, 2014, just when some people were beginning to feel more confident that their approach to network security was resulting in strong protection, an encryption vulnerability in OpenSSL known as "Heartbleed" hit – and it hit hard. Companies and customers worldwide scrambled to assess if and how the bug affected them – and, where necessary, take the required steps to recover.

Heartbleed was unprecedented in scale. Countless reports said it affected roughly two-thirds of websites. But the bug's reach also provided a powerful reminder that:

- Acting swiftly to patch a known vulnerability can mitigate threats to a network.
- IT administrators need to implement a methodical auditing and patching process.

Whenever a new virus or piece of malware hits the headlines, IT managers the world over quake in their shoes, worrying how exposed their network and business applications may be. It's challenging enough for the larger companies that enjoy well-staffed IT departments with sufficient resources.

But what happens if you are a small to mid-sized business (SMB), where IT resources and a budget for new security measures are often limited? Beyond the traditional antivirus, firewall and web security, what more should an IT admin be doing?

No network can be 100% secure. But diligently adhering to a simple plan can dramatically improve network security and enhance protection against new malware.

This white paper introduces five recommended steps for building a methodical network auditing and patching process.

1.
Know your network

Step 1: Discover: Know your network

The first step to protecting your network should be to understand what your network comprises:

- What software is being downloaded and used?
- What hardware devices are connected to your local area network (LAN)?
- Which individuals are trying to access your network resources?
- What wireless area network (WLAN) connections are active, and what mobile devices are your employees using on it?
- What websites are your employees visiting?

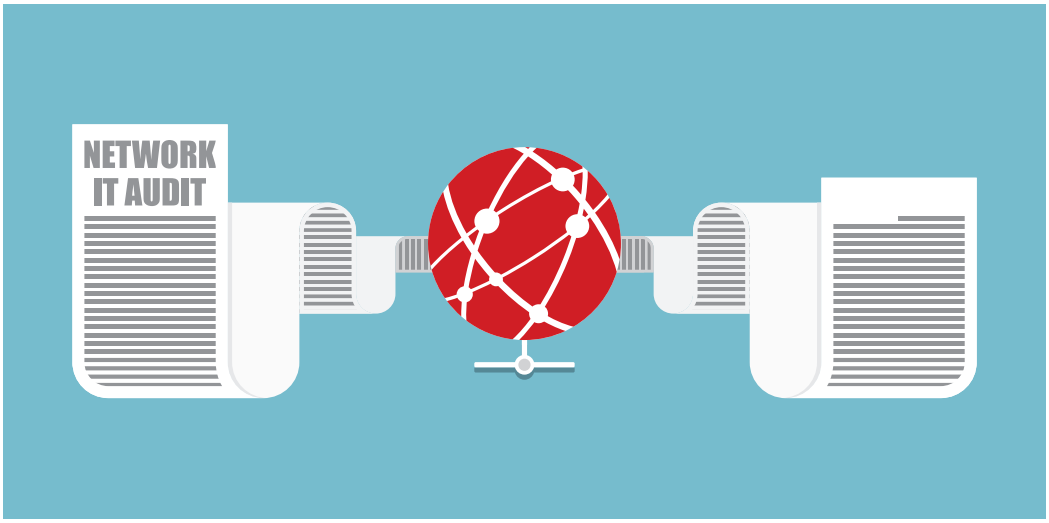
It sounds obvious, but with an increase in bring-your-own-device (BYOD) and work-from-home policies as well as the growth of wireless connectivity in businesses, it is critical to monitor who is connecting to your network, and regulate the devices and software applications connecting to your servers. It only takes one user connecting to your network with a device running old software for malware or a hacker to exploit a vulnerability and do some serious damage. Since networks are dynamic and the devices connecting to your business may always be changing, it is important to run regular audits of the software and devices that are physically connected.

In addition, an effective network audit will often reveal devices, applications and programs running on your network that are not supported by IT, and may not be authorized. In this case, the IT admin may choose to block network access, upgrade older machines or uninstall unsupported programs, thus mitigating unnecessary risk and reducing the opportunity for hackers/malware to exploit possible vulnerabilities within those devices and programs. In some cases, an IT admin may wish to replace an unsupported business or software application with an authorized alternative.

2.
Audit all elements on your network

Step 2: Assess: Audit all elements on your network

Conduct an assessment of the devices and software applications running within your network, with a focus on determining vulnerabilities that have already been identified and the vendor patches that have already been made available. Once this list is compiled, assess the severity and threat level of each known vulnerability. Prioritize the actions required to mitigate the risk exposure to your business applications and company reputation.



3.

Deploy patches to all the software/ devices on your network

Step 3: Patch: Deploy patches to all the software/devices on your network

For SMBs with limited resources and budget, the secret to maximizing security and minimizing risk lies in a simple, but very important fact: The majority of malware and hacker attacks are designed to exploit vulnerabilities in software which is deployed on your network; by identifying these vulnerabilities and removing them, you eliminate the vector by which an attack against your company can be successfully launched, stopping it before it starts. Can it be that simple? Yes, it can. But the good news does not stop there.

Each year, software vendors spend a considerable portion of their revenue testing the software they sell to you. They gather feedback from customers and strive to identify vulnerabilities that their products may contain. Almost all software vendors provide regular software updates to their customers. This enables IT admins to deploy patches to software on their network, and remove these known vulnerabilities.

Once these vulnerabilities have been identified and a fix has been provided by the vendor through a software update, it is important that the IT admin is able to roll out and deploy these patches as quickly as possible. Having conducted Step 2, the IT admin will know which patches are relevant to the network, and the priority in which they should be deployed.

It is at this stage of the process that many IT admins – often without realizing it – increase the risk to their network and help hackers target and disrupt their business. In short, they delay the rollout of available fixes to known vulnerabilities. This extends the window of time during which their network is vulnerable to attack, and gives hackers the time they need for their automated hacking attacks to pinpoint the vulnerability within a network and launch an exploit against it.

Often difficult to achieve without the proper tools, the regular rollout of available and relevant patches is critical to maintaining network health and mitigating risk.

4.

Check your network for open ports

Step 4: Scan: Check your network for open ports

The next step to improve network health is to scan your network to identify any open ports, enabling the IT admin to close any port that should not be open.

This is very important because hackers use automated tools to scan remote networks in the hope of identifying open ports through which they can then probe to see if the software services running behind each open port contain vulnerabilities they can exploit.

Whereas regular patching for known vulnerabilities significantly increases network protection, it is possible that a hacker is one step ahead of a vendor and identifies a vulnerability for which a patch has not yet been released. By probing networks for open ports, hackers may target specific IP-based services and software containing the vulnerability they wish to exploit.

It is common for all networks to have many more ports open than intended or necessary. An IT admin can reduce the risk of hackers/malware exploiting any unknown, unpatched vulnerabilities in services running behind these open ports by identifying them and closing any that are not needed.

5.
Review your work

Step 5: Check: Review your work

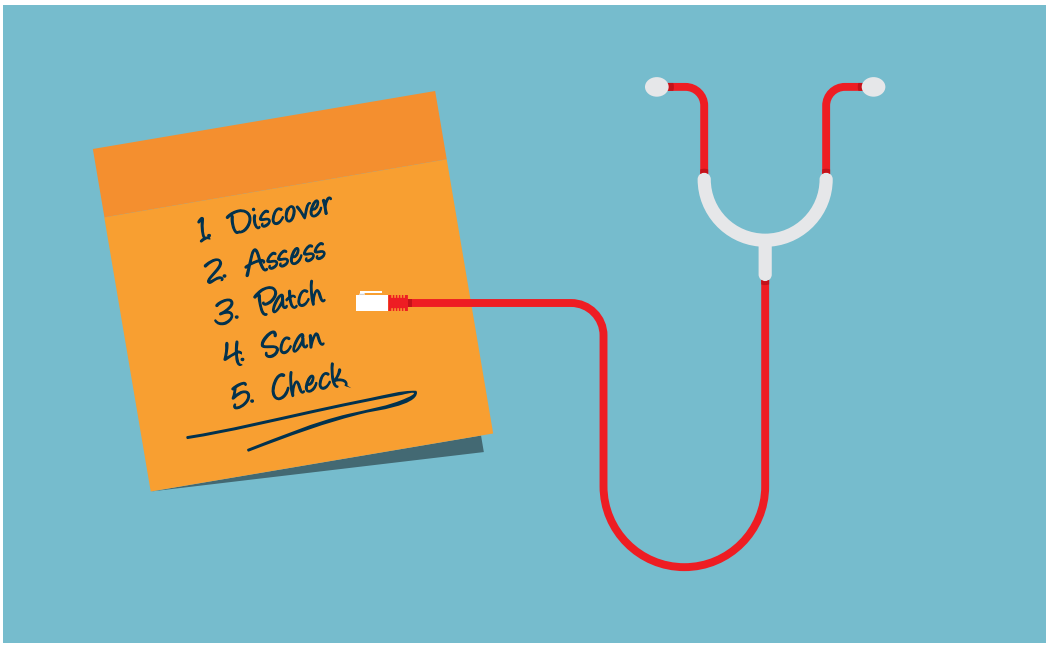
This step is arguably one of the most important: Go back and repeat Step 2. Check to see that the patches and remediation measures you carried out have been implemented correctly!

Unless a software patch has been implemented correctly, the vulnerability and network risk it poses will remain. Sometimes, network problems or other issues may prevent a patch from being implemented properly the first time round. This step of the process should therefore be conducted as soon as possible, to ensure that a patch has been completed and the vulnerability has been removed. In some cases it may be necessary to uninstall a patch and replace it.

"The five-step plan for achieving and maintaining computer security is a process, not an independent sequence of events."

How to implement the five-step plan for network health

IT admins reading this recipe for improved network health will understand the benefit the plan provides. But for SMBs without the proper tools and resources, this plan, no matter how sensible, could place an unachievable burden upon the IT admin.



The goal is to find effective tools that will enable the IT admin to automate as much of the process as possible. It is possible for IT admins to source software tools that specialize in offering services for each of the various steps. However, this would necessitate the IT admin to work with different tools for each step in the process. It also requires the IT admin to port data generated from one step in the process to the next software tool, so it can be used to complete the next stage. Obviously, this increases complexity and cost, and consumes another scarce commodity: time.

The key to mastering the five-step plan is finding a single, cost-efficient software tool that possesses the capability to perform all the processes outlined in the plan – and control, implement and monitor each of these steps from an intuitive management dashboard.

Using GFI LanGuard to implement the five-step plan

Designed with the SMBs in mind, GFI LanGuard® supports IT admins in each of these key steps from one management interface, as outlined below:

1.
Discover

Step 1: Discover

GFI LanGuard is a powerful network discovery tool that helps IT admins build a central inventory of network assets and generate automated reports detailing the devices, computers, software and applications installed on a network. This includes computers, laptops, servers and other network connected and USB devices. It can also detect mobile devices that connect to Exchange Servers, and other popular services like Office 365 and Google Apps.

It also provides valuable and essential insight into the state of other commercial security applications that have been installed in the network or on network devices (antivirus, anti-spam, firewalls, etc.) To do this, GFI LanGuard integrates with more than 4000 security applications such as antivirus, anti-spyware or firewalls, and reports on their status.

2.
Assess

Step 2: Assess

Having scanned the network and built an inventory of the network assets, operating systems, devices and software applications, GFI LanGuard will conduct more than 50,000 vulnerability assessments. It cross-references the inventory list against an extensive, industrial strength vulnerabilities database incorporating OVAL (8,000+ checks) and SANS Top 20 standards to identify all the vulnerabilities that exist within the network the IT admin is analyzing. This helps an IT admin build a complete and detailed overview of network security risks.

With GFI LanGuard, multi-platform (Windows®, Mac OS®, Linux®) vulnerability scans may be performed, with support for virtual machines. GFI LanGuard can also scan smartphones and tablets running iOS®, Android™ and Windows Phone®, and other devices such as printers, switches and routers from manufacturers like HP®, Cisco®,3Com®, Dell®, SonicWALL®, Juniper®, NETGEAR®, Nortel®, Alcatel®, IBM® and Linksys ®. Full flexibility is offered with the ability to set up custom vulnerability checks through wizard-assisted screens, to define custom groupings of computers and to create different types of scans and tests.

Once the vulnerability assessment has been conducted, a graphical threat-level indicator will provide IT admins with an intuitive, weighted assessment of the vulnerability status of any scanned computer, or group of computers, or the entire network.

The software will then assist in managing the next step in the five-step plan, enabling the IT admin to manage each vulnerability by selecting an appropriate action to conduct against it (marking each one with "remediate," "ignore," "acknowledge" or "re-categorize").

3. Patch

Step 3: Patch

Having identified the vulnerabilities in your discovered network, GFI LanGuard provides IT admins with access to the corresponding missing patches and service packs that should be deployed from the central server to update the software/devices in your network.

A powerful feature of the automation capability of GFI LanGuard is the ability to schedule patch updates to take place at times which provide minimal business impact to network users: The software's "Wake-on-LAN Support," can further minimize business impact by powering computers on and off when patches are deployed after business hours.

In addition, if unsupported programs/applications are identified during the network discovery phase of Step 1, GFI LanGuard can remotely uninstall these programs. Similarly, GFI LanGuard can remove and roll back any patches, post-deployment, should this be required.

GFI LanGuard automates patch deployment to Microsoft®, Mac OS X and Linux operating systems as well as Microsoft applications and more than 60 third-party applications – all in supported languages for both security and non-security patches. It is an essential and powerful patch management tool for SMB IT admins who struggle with the time-consuming and repetitive requirements of patch management.

Many popular third-party applications are supported, such as Apple QuickTime®, Adobe® Acrobat®, Adobe® Flash® Player, Adobe® Reader®, Shockwave® Player, Mozilla Firefox®, Mozilla Thunderbird®, Java™ Runtime and others.

GFI LanGuard also automates patching for all major web browsers running on Windows systems, including Microsoft Internet Explorer®, Mozilla Firefox®, Google Chrome™, Apple Safari® and Opera™ Browser.

4. Scan

Step 4: Scan

Having built the inventory list, conducted a vulnerability assessment and patched for missing updates and service packs, GFI LanGuard can then assist with scanning.

Several scanning profiles are available, providing the flexibility to scan for and enumerate all open TCP/UDP ports, or to narrow the scan down to those specific port ranges, including only those TCP/UDP ports commonly exploited by known Trojans. Once these open ports have been identified, the IT admin can use GFI LanGuard to close any ports that should not be open, further mitigating the threat to the network.

5.
Check

Step 5: Check

GFI LanGuard makes it easy for an IT admin to rescan the network and check that patches and missing service packs have been correctly deployed, and that previously identified vulnerabilities have been removed.

Conclusion

Many IT admins, particularly those working for SMBs with limited resources and budget, struggle to cope with the growing list of essential but repetitive, time-consuming tasks that they must address on a daily basis.
Yet, as Heartbleed proved, the need for building a methodical network auditing and patching process that improves and maintains network health has never been greater. Achieving this goal is possible by following five simple steps outlined in this white paper, which also introduced GFI LanGuard.

GFI LanGuard provides patch management, vulnerability assessment and network auditing, thereby reducing total cost of ownership of these essential security tools. It also assists in asset inventory, change management, risk analysis and proving compliance. Easy to set up and use, GFI LanGuard gives a complete picture of the network setup and helps to maintain a secure and compliant network state. It does this faster and more effectively through its automated patch management features, and with minimal administrative effort.

About GFI Software®

GFI Software develops quality IT solutions for small to mid-sized businesses with generally up to 1,000 users. GFI® offers two main technology solutions: GFI MAX™, which enables managed service providers (MSPs) to deliver superior services to their customers; and GFI Cloud™, which empowers companies with their own internal IT teams to manage and maintain their networks via the cloud. Serving an expanding customer base of more than 200,000 companies, GFI's product line also includes collaboration, network security, anti-spam, patch management, faxing, mail archiving and web monitoring. GFI is a channel-focused company with thousands of partners throughout the world. The company has received numerous awards and industry accolades, and is a longtime Microsoft® Gold ISV Partner.

More information about GFI can be found at http://www.gfi.com.

GFI 5042 jun14

GFI®

www.gfi.com

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

Other network security solutions from GFI

GFI EndPointSecurity™
Control of USB sticks, iPods and other endpoint devices

GFI EventsManager™
Log data analysis and IT management

GFI WebMonitor™
Web security, monitoring and Internet access control