BYOD and multivendor networks raise the vulnerability ante:

10 ways to fight back!

GFI LanGuard™

Network security scanner and patch management

The problem: The security wars rage on. Attacks which were once performed manually, are now being fully automated, while hackers have more targets than ever to attack.

The adoption of Bring Your Own Device (BYOD) policies in small to medium businesses means that IT has to protect tablets and smartphones that they didn't even specify, procure or configure. In addition, most companies are now multi-platform, blending in Linux® and the Mac® with their mainstay Microsoft® Windows® client and server systems. And we mustn't forget the growing network infrastructure – all those switches, routers, access devices and printers which need their security continually assessed and tightened.

As an IT professional or service provider, you are responsible for helping to avert security disasters

Unless regularly audited, maintained and protected, these devices, applications, operating systems and assorted bits of hardware and software become increasingly vulnerable, and make easy targets for experienced cyber criminals.

Failure to commit adequate resources to identify vulnerabilities within your network, and take adequate security precautions to mitigate the risk they pose can easily lead to damaged computers, lost or stolen data, fraud, lawsuits, cyber-crime, and violation of compliance regulations. Your business can lose money, get taken to court, or even go out of business. Furthermore, business Directors/ Owners could even find themselves personally liable for events caused by negligence, and when reasonable security precautions were knowingly not put in place.

As an IT professional or service provider, you are responsible for helping to avert security disasters. Here are ten best practices for vulnerability assessment and security in a multi-vendor network. Implement all ten and the chances of a successful attack are nearly eliminated, - and if a hacker does break through, you'll know how to survive.

1.

Get executive support

2.

Define a policy

1. Get executive support

Vulnerability assessment to bolster network protection is a critical and on-going task. To make sure you are given the resources and budget to do it right, invest time in making sure that your leadership and managers understand just what is at stake: their very business. Budget and resources spent assessing and removing vulnerabilities before they can be exploited reduces business downtime/lost productivity, and protects against theft of data assets and damaged business reputation.

2. Define a policy

As well as being an essential part of many compliance requirements, time spent working on and defining a security policy for your business will pay dividends in the long run. Once in place, a detailed security policy will help define what a vulnerability scanning and assessment tool is and needs to do. The policy should provide rules that dictate the proper use of vulnerability tools, ensuring they will be used and also supported by IT and associated executives.

And what exactly are you trying to prevent? Cyber crime? Malware? Compromising data that falls under compliance regulations? By setting priorities you can give your most precious resources that extra attention. It is also a way to audit exactly how your IT staff are securing your infrastructure.

The policy is a living document. Treat it as a project, get key stakeholders to contribute, and make it clear and comprehensive. Then update it as your business evolves, infrastructure grows and the threats change.

A good vulnerability management tool helps continually improve your security posture and can even influence enhancements to the security policy itself. Over time, the experience built upon from regular network scanning will show which software is most risky and problematic. This will help IT to nip issues in the bud, eliminating problem software such as risky browsers or Java code, and guide IT to what areas of the network need additional focus and where security needs tightened up.

3.
Consider your entire network

4.
Think multiplatform

5.
Do a vulnerability deep-dive

3. Consider your entire network

The experience of BYOD has demonstrated that the devices IT may not even know about are those that can be the perfect attack vector. To reduce the risk, vulnerability assessment must discover and then fully analyse the entire network and all its components: this includes all your operating systems, applications, and devices, including remote and mobile employees.

Pay attention to the details, and the smallest devices connecting to your network: smart phones and tablets are just as large an attack vector as a full-size PC or laptop, if not more so.

All this is a function of a good asset management solution, one that regularly searches the network looking for new devices that need protection.

4. Think multiplatform

When considering your network, you must now not just think of scanning and securing devices running one operating system. You must consider many. Companies that used to be all Windows on the client and server sides are now decidedly mixed. Linux has made huge strides in servers, and a sizeable array of Linux distributions have now taken a large market share, each of which has to be analysed.

On the client side, nearly all companies have a least a small contingent of Mac users, especially in creative development teams. There may even be a group of Linux clients, particularly if you have a technical (some would say 'geeky') workforce.

Tablets and smartphones are likely a mix of Windows, iOS, Android® and Blackberry®. So, be prepared to scan multiple operating systems and identify vulnerabilities within all of them. If you protect only 90% of your systems and hackers creep through on the 10% that are left vulnerable, you are still in trouble. It only takes one exposed machine.

5. Do a vulnerability deep-dive

Some manual and even third party scans take little more than a cursory view of the devices and their states. You need to know their specific OS version as well as their patch and update status.

Software that is not up to date is all the more vulnerable: vendors spend significant resources updating published software to remove vulnerabilities within their products, and hence make them more secure. If you do not accept and deploy their updates, you are leaving a backdoor open for automated hacking software that scans networks for old, unpatched software, and then automatically exploits it.

And while you are digging deep into your network, looking for anything and everything that might need fixed, keep an eye out for open ports: if a port is open that should not be, shut it down. Regularly scanning for and identifying unauthorised open ports is a major step to mitigating your risk exposure.

6.
Avoid employee abuse

7.
Automate and repeat

6. Avoid employee abuse

Security is not just about hardware and software - you must also consider the people that use them: your employees. A security policy should consider the data and applications that network users have access to: do the right users have the correct access to the appropriate data and applications? Do they have the appropriate access and administration rights? Are any end users abusing access rights and misusing corporate data or resources?

And while you are considering these questions, you might also want to question if your employee passwords are too weak, too old, or already compromised? Are users accessing important data with no passwords at all? Have users left, but their accounts and therefore possible access remain in the form of ghost accounts?

7. Automate and repeat

Although it is still technically possible, the days of asking an IT administrator to manually assess the vulnerability of the key components on their network or rapidly disappearing. It is simply too time consuming and resource intensive. Which means that it is too expensive. Additionally, not only are manual processes fraught with human error, but networks are continuously changing, and what is secure today may be wide open tomorrow, unless you manually scan your network, again, and again, and again. Etc.

An automated and continuous approach to assessment is the only way to keep the network truly safe, and within budget.

In fact, the ideal vulnerability and security tool will be able to schedule and automate all of its important functions, from network scanning, to device and change discovery, to full security audits to remediation. Yet, just because it can, don't get carried away. Automated remediation should be carefully controlled by IT so it is done safely – so make sure the tool is easy to understand, easy to use, and easy to program.

With practice and as your confidence builds, perfect targets for automation include uninstalling unapproved software, rolling back problem patches, and activating turned-off firewalls.

Automation enables huge staff time savings. The software replaces the IT diagnostic leg work. So when a vulnerability is found, that is where you deploy your actual manpower - or for those lucky enough to have a capable security solution - remediate automatically.

8.

Report, understand and remediate

9.

Get behind a powerful security product with a good dashboard

8. Report, understand and remediate

A full, automated and near-continuous company-wide vulnerability scan means little if the results are not easy to understand: what's not understood, can't be acted upon.

Vulnerability scan tools need comprehensive reporting capability that is easy to use, but which produce results which are easy to interpret, with simple query functions for when questions arise.

The reporting tools shouldn't just show what vulnerabilities exist, but based on its own analysis and a rich database of vulnerabilities, it should rank the vulnerabilities in priority and risk level, so that you can address the most pressing ones first.

Reports produced by your vulnerability scanner should not just show what's vulnerable, but they should also inform as to what's fully and properly patched, updated and free of vulnerabilities. This can demonstrate to executives and upper IT management the efficacy of your vulnerability management tool and policy.

9. Get behind a powerful security product with a good dashboard.

For many overworked IT managers, there is always too much to do, and not enough resource to do it. So, when you look at a tool to help with vulnerability assessment within your business network, ensure that you choose one that makes your life easier: find one that has a rich and intuitive dashboard with a user friendly interface. Even better, try to find a security tool that not only performs vulnerability assessment, but also provides capability for a broader array of related security functions, such as patch management, asset and application management. And if you could have your dream come true? Then how about a tool where the dashboard links it all together, giving you a central location that doesn't just give you visibility on the vulnerabilities in your network, but also provides for their remediation.

10.

Create a baseline, scan regularly, track changes and act on them!

10. Create a baseline, scan regularly, track changes and act on them!
When vulnerabilities are discovered, they should be removed and fixed as soon as possible. What next? Scan your network again. Regularly. And ensure that new vulnerabilities don't sneak in under the radar.

The worry is that if you don't scan often enough, there could be long periods of time when IT administrators are not aware of new vulnerabilities that have appeared. On the other hand, if you scan too often, depending upon the tool you use, the performance of your network could be impacted.

The trick is to find the best compromise for your network size and assets. Scan the network once or twice, and establish a baseline for existing vulnerabilities within your network. After that, an advanced vulnerability tool will help identify changes to computers such as patching status and configuration. These are all reported to IT who can decide if any action is required.

Actions that IT may then decide to take might include uninstalling non-supported, non-licensed or otherwise unauthorized software, rolling back bad or untested updates or patches (or ones that simply interfere with existing software or your environment), or installing missing updates or patches. Silent uninstalls are also a hot feature to look for in your dream security tool, as it reduces end user complaints and helps minimize impact to end-users.

You may also want to update anti-malware definitions, kick off security scans, install custom scripts to remediate problems or improve operations, or activate security software such as firewalls. You may also wish to remove end-user applications, and replace them with alternative approved business software.

These actions should be automated as much as possible, so the system fixes problems quickly without IT intervention, before they can be exploited by hackers or automating hacking systems which are scanning your network, specifically hunting for these vulnerabilities.

Vulnerability product checklist: three must haves

- Does it integrate with third party security tools? GFI LanGuard works tightly with more than 2,500 security tools.

- Robust database. Whatever tool you use should have a solid, large and always up-to-date database of vulnerabilities. GFI LanGuard can do more than 50,000 vulnerability checks, and taps into leading dynamic vulnerability databases including SANS Top 20 and OVAL.

- Let's get virtual. It's rare these days that a company has an all-physical infrastructure. Nearly all companies have virtual servers and other virtual infrastructure. Your vulnerability solution has to work as well with virtual as physical systems.

GFI LanGuard : Your one-stop shop for automated network security management.

GFI LanGuard is a powerful, one-stop shop for automated network security management, that provides vulnerability assessment, patch management, asset audit and management and problem remediation, all from the same powerful console. To further enhance security for small to mid-sized businesses, it can integrate with anti-virus/malware, anti-spyware and personal firewall, as well as GFI EventsManager which provides log management, and GFI EndPointSecurity which provides device blocking.

About GFI®

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.

Download your free trial from **http://www.gfi.com/languard**

GFI 5042 dec13

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

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.