WHITEPAPER

How to Perform a Network Security Audit

GFI Software™

Network Security Audits Made Easy

Organizations large and small often go to great lengths to keep cybercriminals, ransomware, and other threats at bay. In spite of their best efforts though, IT pros are often left wondering if they have missed anything. It can be difficult to know whether or not your network is safe.

Good network security is best achieved through a defense in depth strategy revolving around a collection of best of breed security products, and an adherence to established IT security best practices. At the same time though, you also need a tool that can help you to audit the security of your network endpoints so that you can find and address any vulnerabilities that might exist.

GFI LanGuard is easily one of the best tools that a small to medium sized business can use to evaluate its network security. Although network security auditing tools are notorious for being difficult to use, GFI LanGuard makes the security auditing process almost effortless. Within a couple of hours' time, you can scan a sample of network endpoints, and discover the types of vulnerabilities that exist on your network. In fact, this paper will even show you how.

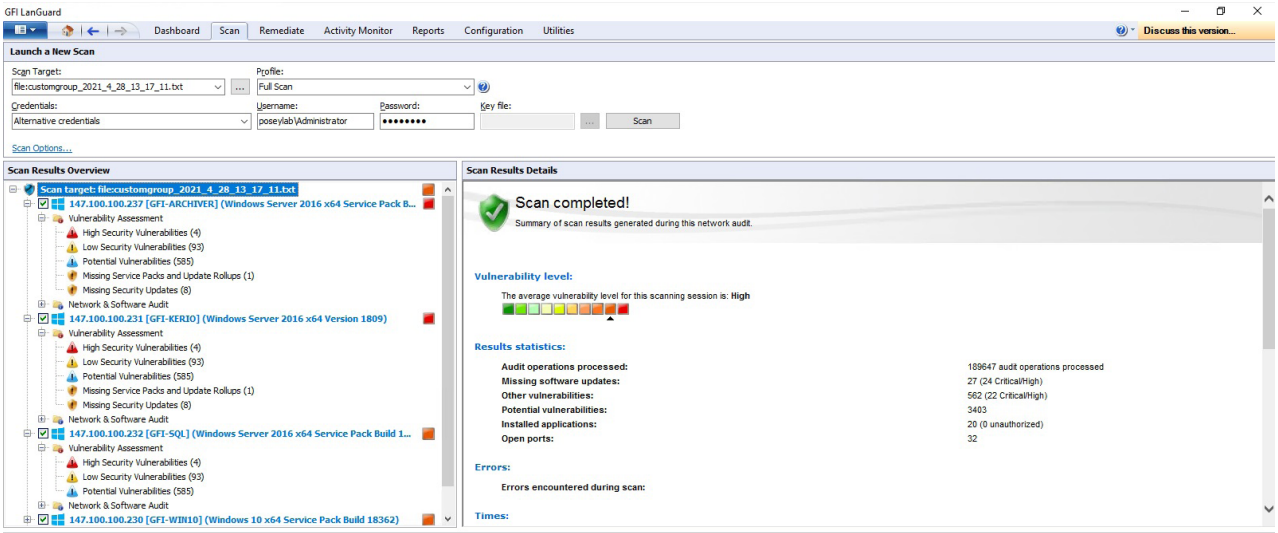
Performing a Quick health check

Initially, your goal should be to figure out where you stand with regard to the security of your network. At this point in the process, taking the time to set up a full-blown network audit is probably overkill. It's better to just perform a quick and easy network security scan to get a general sense of what your most pressing security issues may be. Once you have taken steps to correct critical security issues, you can go back and perform a more detailed audit to figure out what else you should be doing to better secure your network.

GFI LanGuard makes it easy to perform a high-level security scan. You don't have to worry about installing agents, configuring firewall rules, or any of the other tedious tasks that are so often associated with security audits. Instead, all you have to do is to open the GFI LanGuard console and click on the Launch a Scan link. Once you have done that, you need only to select the machines that you want to scan and the scanning profile that you want to use and click the Scan button. It's that easy.

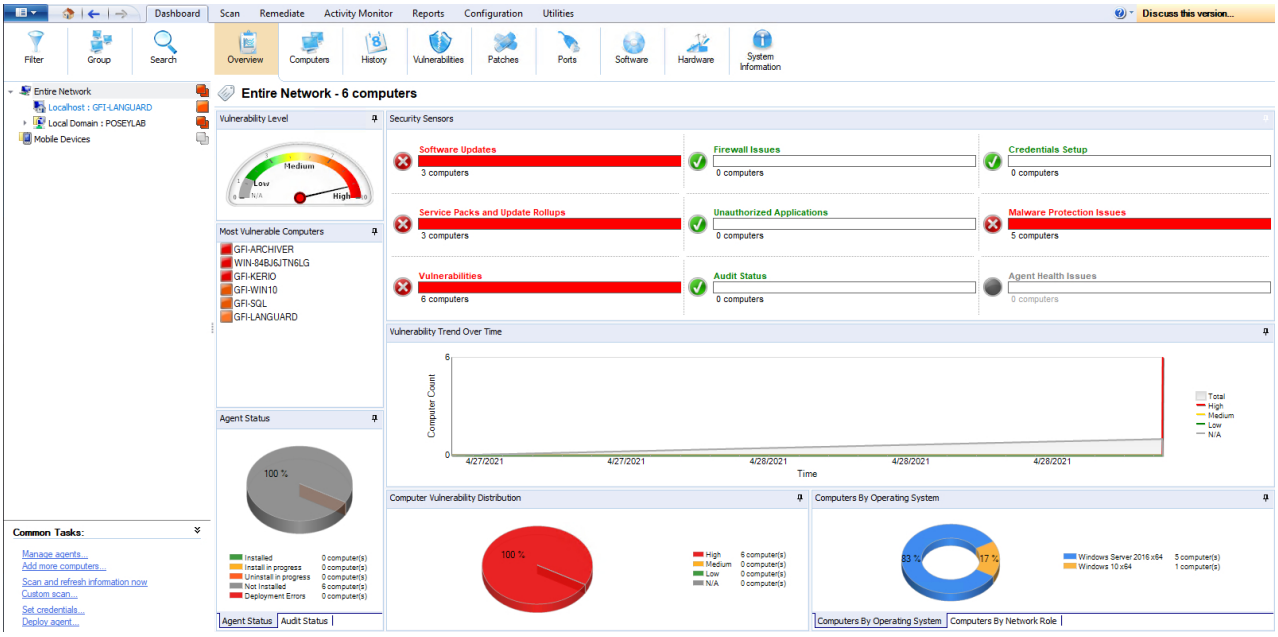
It's worth noting that at this stage in the process, you don't have to scan your entire network. If your goal is just to get a better idea of the types of security issues that currently exist on your network, then you can scan a representative sampling of the machines on your network rather than scanning them all. That will help the scan to complete more quickly and will make the results easier to digest.

When this initial scan completes, you will be taken to a screen that is similar to the one that is shown in the figure below. As you can see in the figure, the vulnerabilities that are detected for each machine are color coded and categorized by severity. In addition, a pane on the right side of the screen gives you a quick summary of the scanning session as a whole. In this case for example, the average vulnerability level across all of the machines was High. You can also see the number of software updates that are reportedly missing, how many firewall ports are open, the total number of applications that are installed (as well as how many of those applications are unauthorized), and more.



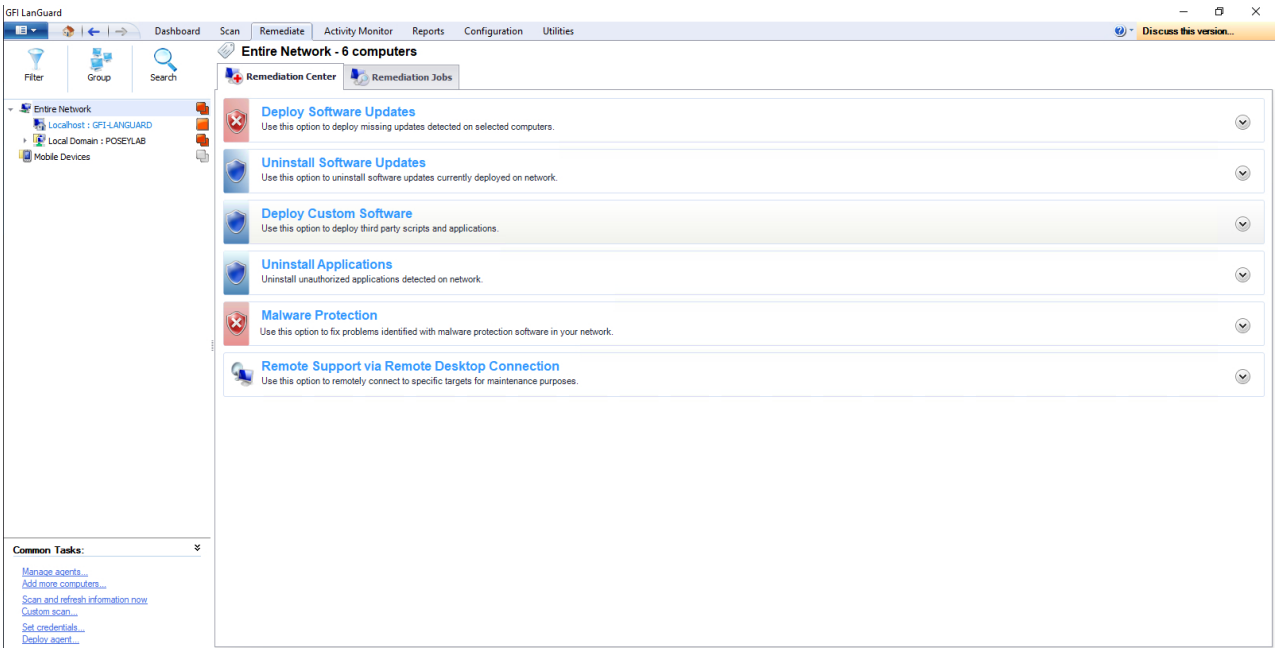
The initial scan revealed that numerous vulnerabilities exist.

You can see a graphical view of the scan results by going to the Dashboard tab. This tab shows you which of your scanned computers are the most vulnerable and how many of the computers on your network have vulnerabilities related to things like software updates, firewall issues, or malware protection issues.



The Dashboard tab provides a summary of the vulnerabilities that have been discovered.

If the initial scan detects serious vulnerabilities on your network, you can use the Remediate tab to correct some of the problems. As you can see in the next screen capture, the Remediation Center allows you to deploy missing software updates automatically, enable malware protection, or take other corrective action.

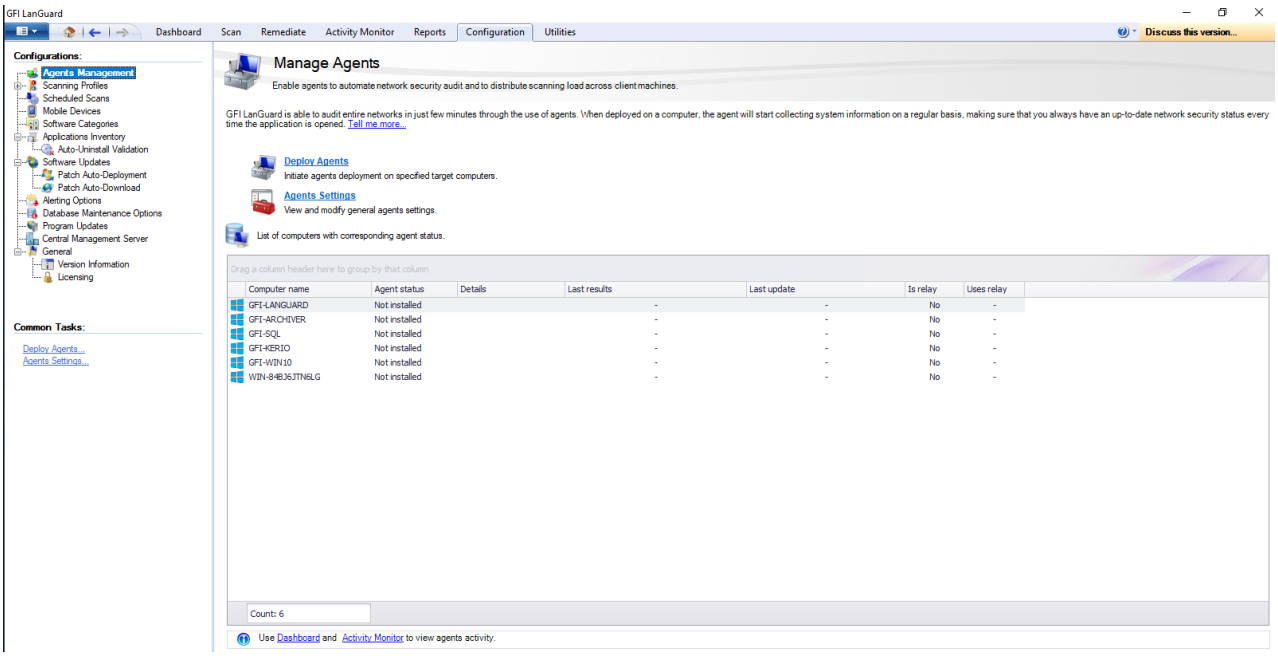


The Remediation Center makes it easy to correct some of the issues found during the initial scan.

The type of scan that was described earlier in this paper is quick and does a great job of finding the more significant vulnerabilities. This quick scan is often a prelude to a full-blown audit. Performing the full audit is more time consuming.

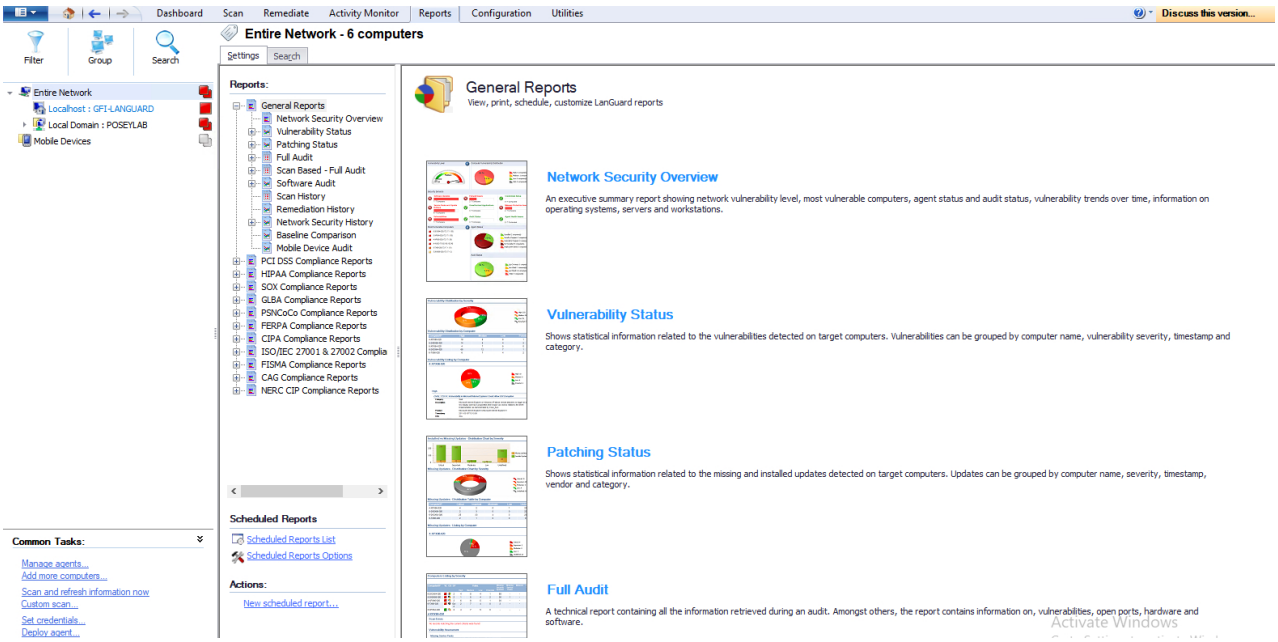
The quick scan lets you identify and correct your most pressing issues before taking the time to perform a security audit.

The first step in running an audit is to deploy agents to the machines on your network. These agents allow LanGuard to collect more security information than it would otherwise have access to. You can deploy the agents by going to the Home screen and clicking Manage Agents, followed by the Deploy Agents link that is shown in the figure below. Now, just follow the prompts to deploy the agents. Once the agents are installed, go back and run the scan again.



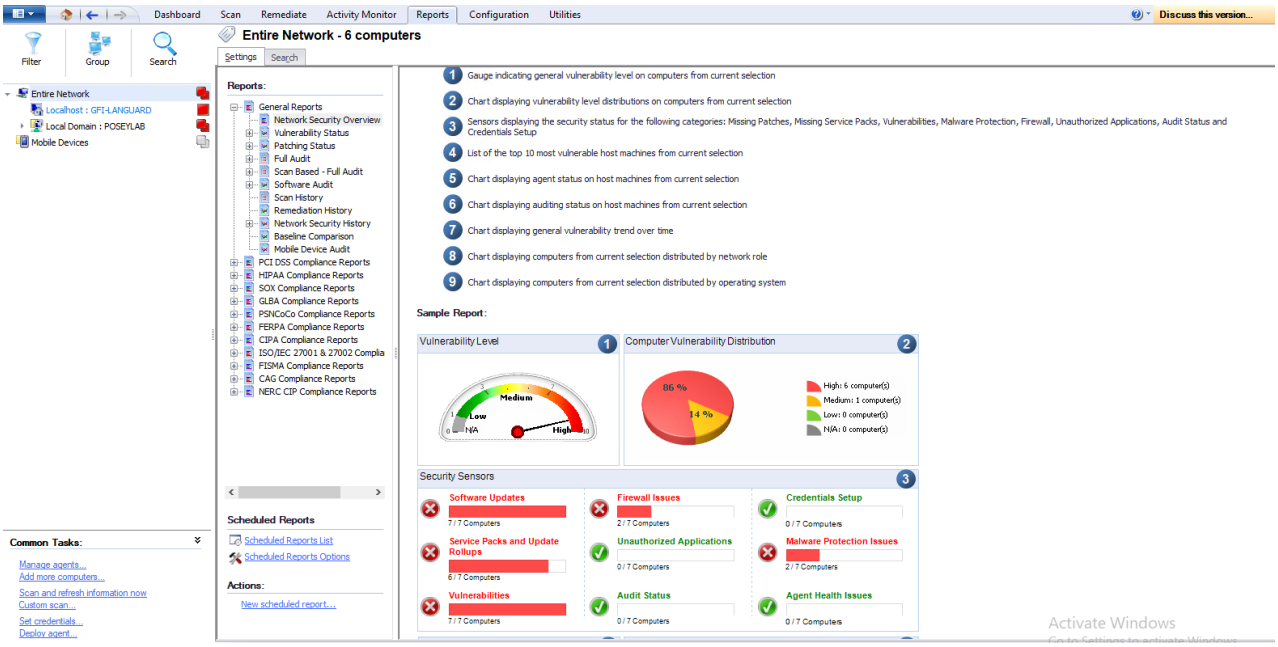
The Configuration tab makes it easy to deploy agents to the machines that you want to audit.

Once the scan completes, you can use the GFI LanGuard collection of reports to assess the security state of your network endpoints in depth. You can see some of the available reports in the next figure.



GFI LanGuard includes numerous built-in reports.

When you click on a report, GFI LanGuard provides you with a list of the items that are included within the report, and also shows you a sample of what the report will look like. That way, you can get a feel for whether a particular report is of interest before you take the time to run the report. For example, the Network Security Overview report is intended to give you a brief synopsis of the most significant security issues that exist on your network. This report, which you can see in the next figure, is a good place to start if you are not yet familiar with your network's overall security health.

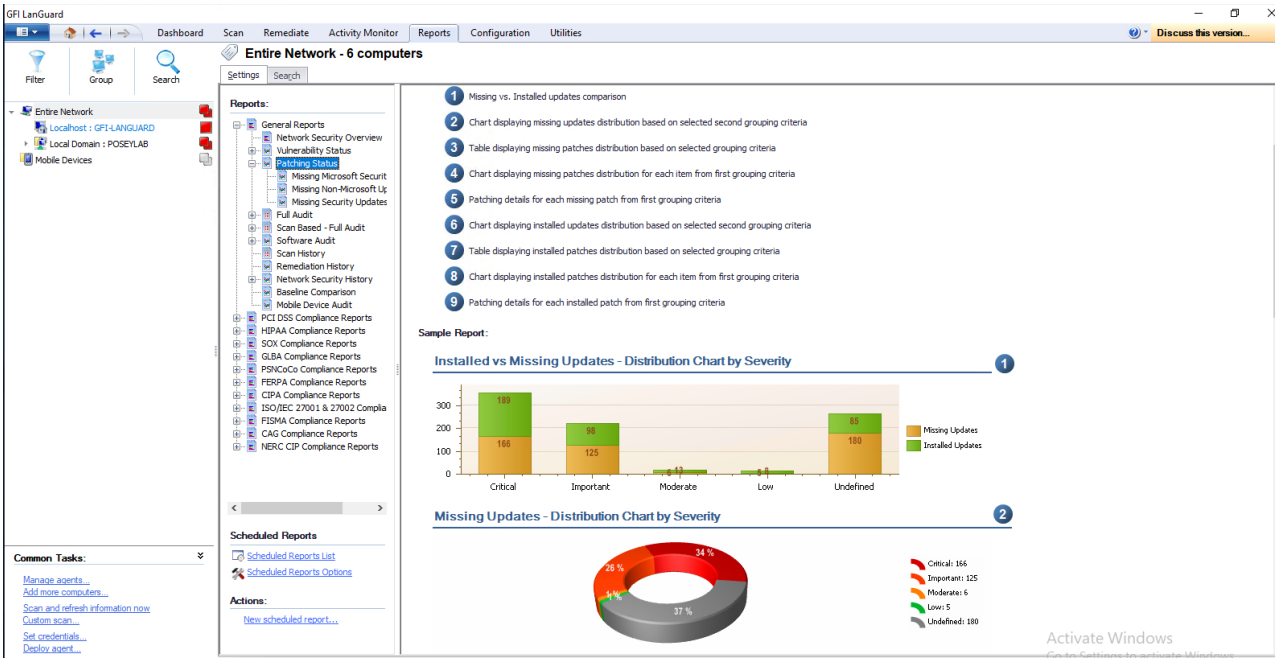


The Network Security Overview report acts as a general network security status report.

If you do decide to generate a Network Security Overview report, then there are two things you should look for. First, pay attention to any reported agent health issues. The agents normally work well, but if there are issues with the agents then you will probably want to address those issues before moving forward with creating other reports. Otherwise, your report might lack information on the hosts whose agents are having problems.

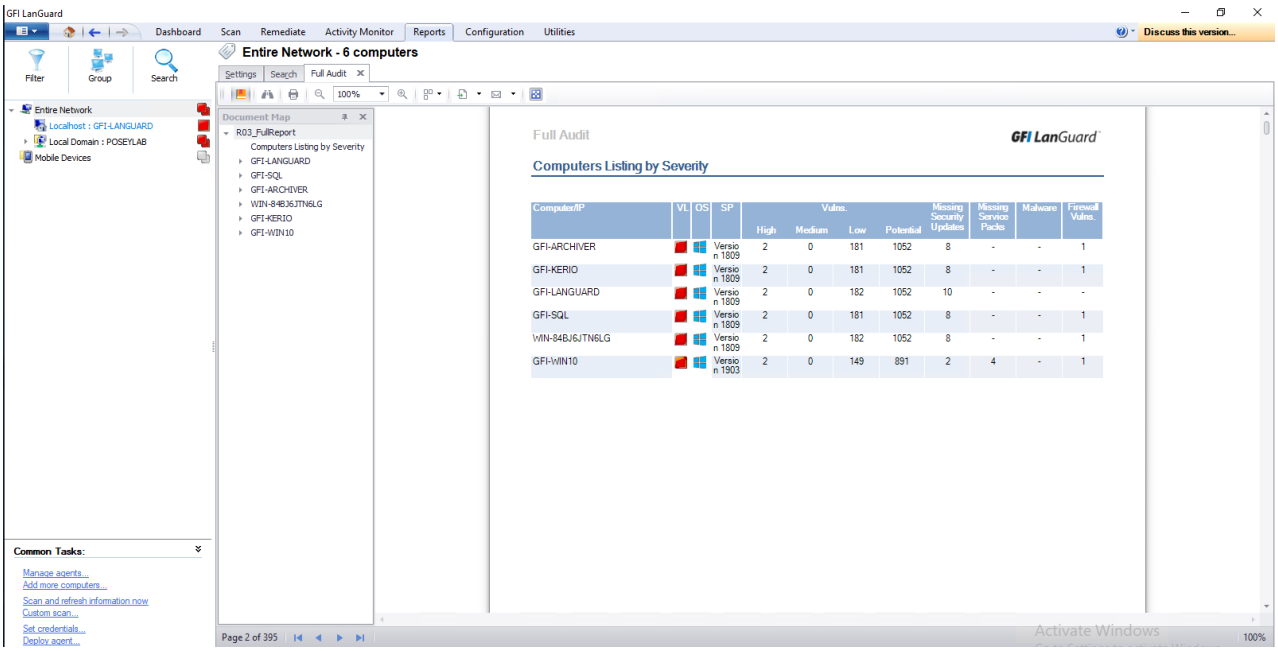
The other thing to look for is areas with a lot of red. In the sample report shown above, for example, most of the computers that were scanned have issues with software updates, service packs and update rollups, and other vulnerabilities. There are also some machines with firewall and malware protection issues, but those issues affect a relatively small percentage of the machines. As such, it would be best to address the update and vulnerability related issues first since they affect so many machines.

If you look at the list of general reports shown in the previous figure, you can see that there are individual reports for each of the issues that are shown on the sample report. These reports provide more granular detail on the issues appearing on the sample report. If, for example, you wanted to know which software updates were missing, you could run the Patching Status report, which is shown in the next figure.



The Patching Status report gives you information about the patches that are missing from your network endpoints.

The individual reports can be helpful if you are trying to address a specific security issue. If your goal is to document all of the known security issues, then you are better off performing either a full audit or a scan-based audit. These audit reports, which are fully customizable, provide you with detailed information about any issues that were found while scanning the computers on your network. Whereas the overview reports tend to be high level, audit reports are far more granular. If you look at the figure below, for instance, you can see that the audit report is nearly 400 pages in length even though only six computers are covered in the report.



The audit report spans hundreds of pages.

The audit reports can be extremely helpful for identifying the security issues that exist on your network. Once you have identified these issues, you should immediately begin working on addressing those issues. This might mean installing patches, closing firewall ports, or taking other corrective actions. In many cases, the previously mentioned Remediate tab can address the issues for you so that you do not have to deal with them manually.

The most important thing to remember about this process is that securing your network is not a onetime task. Once you have addressed any reported security issues, it is extremely important to rescan your network endpoints and run fresh audit reports on a regular basis. Otherwise, security issues will tend to gradually reappear over time.

The GFI LanGuard security reports identify security threats and can also help quantify how an organization's IT staff's hard work has made the network more secure over time. Being able to quantify your network's improved security can make it easier to adhere to compliance regulations. These types of security trend reports are also something IT pros can show their bosses as a way of demonstrating their value to the organization.