PRODUCT REVIEW

GFI LanGuard

Reviewed by Brien M. Posey

TechGenix

Introduction

I have always said that network security ultimately boils down to answering two really basic questions – where are the vulnerabilities on my network, and what can I do to address those vulnerabilities. As simple as these questions may be, they have historically been very difficult questions to answer.

Recently, I had a chance to review a product from GFI that may better equip security admins to answer these two questions. GFI LanGuard is designed to perform vulnerability assessments of the devices on your network, and then help you to remediate any vulnerabilities that are detected.

01 The Deployment Process

In preparation for writing this review, I downloaded the LanGuard free trial and installed it to a virtual machine within a dedicated Windows domain. In doing so, I found the installation process to be completely straightforward. LanGuard requires SQL Server, but since my lab environment contains fewer than 500 machines I was able to use the included copy of SQL Server Express, which was installed automatically as a part of the deployment.

02 Adding Computers

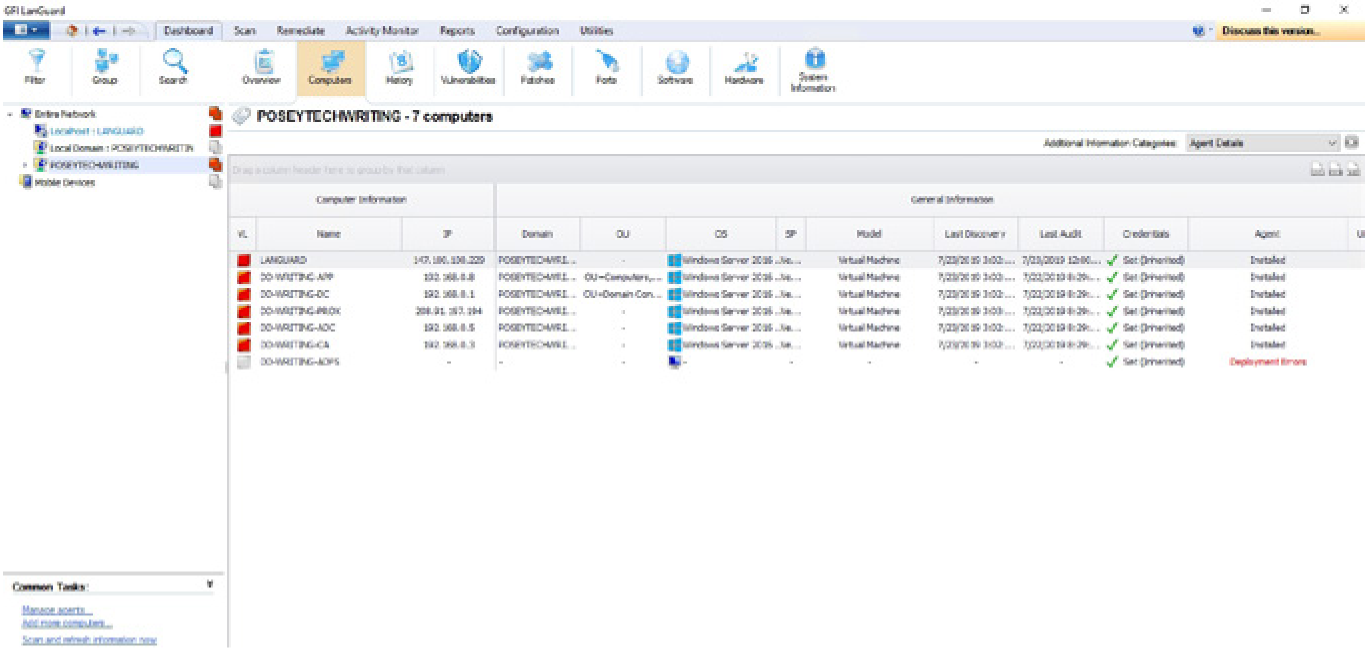
Once I had finished installing GFI LanGuard, the next thing that I attempted to do was to tell LanGuard which computers I wanted it to monitor. For the purposes of this review, I decided to monitor several domain joined virtual machines running Windows Server 2016. It is worth noting that although I am limiting my review to machines running Windows, GFI LanGuard is also designed to work with Linux and Apple OS X systems.

I found the process of adding the VMs to the LanGuard console to be relatively straightforward. Because my LanGuard server was domain joined, LanGuard already knew about my domain. I was therefore able to right click on the name of the domain and then use the Synchronize With Active Directory option to populate LanGuard with a list of the domain joined computers.

The next step in the process was to deploy an agent to the managed computers. The agent deployment process happens automatically, on a scheduled basis. However, there is a way to speed things up by forcing an immediate agent deployment.

Although the agents deployed without issue, it took some time for all of the agents to query their respective computers and populate the LanGuard console. I have been told that this process takes about a day to complete. In my case, I installed the agents just prior to leaving town for the weekend. By the time that I returned on Monday morning, the console had been fully populated.

You can see what the computer information looks like in the figure below. Incidentally, the reason why the last computer on the list shows a deployment error is because memory limitations prevented me from turning on that particular virtual machine. As such, the error is not an indication of a problem with LanGuard.



POSEYTECHWRITING - 7 computers

Additional Information Categories: Agent Details

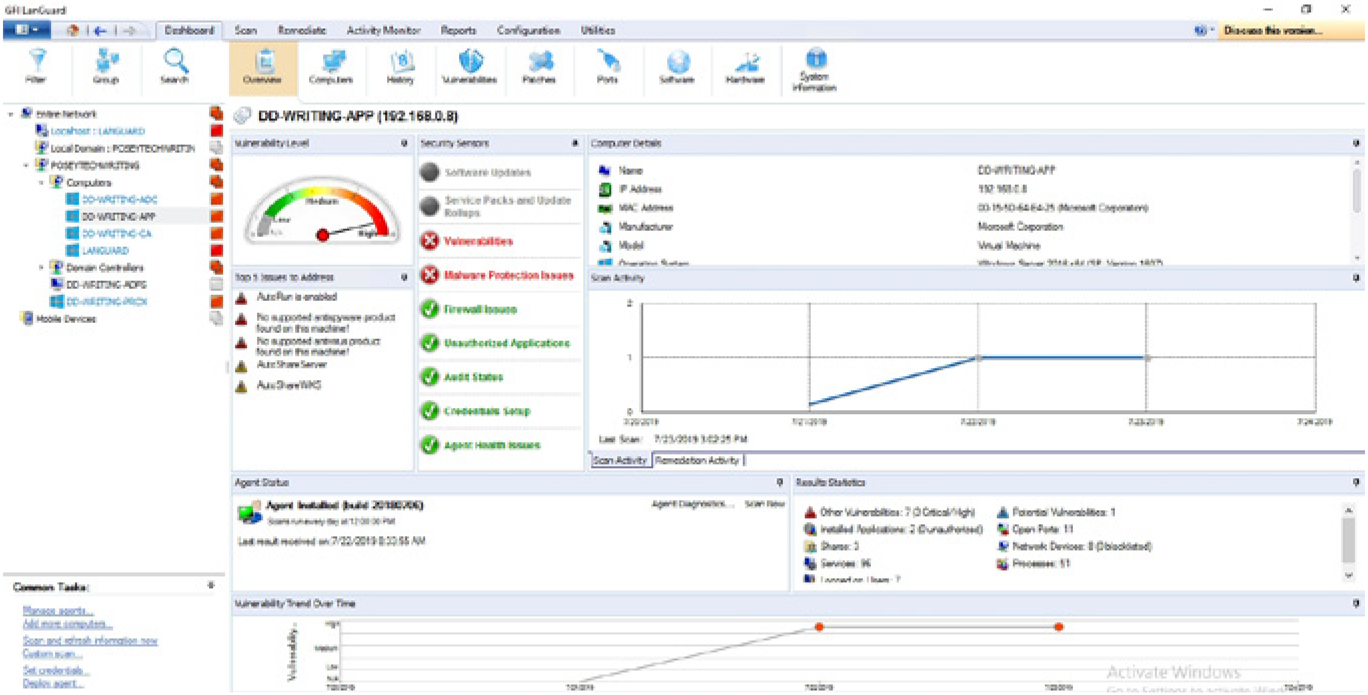
Computer Information			General Information								
VL	Name	IP	Domain	OU	OS	SP	Model	Last Discovery	Last Audit	Credentials	Agent
🟥	LANGUARD	147.100.100.229	POSEYTECHWRI...	-	Windows Server 2016 ...Ja...		Virtual Machine	7/23/2019 3:02:...	7/23/2019 12:00:...	✓ Set (Inherited)	Installed
🟥	DO-WRITING-APP	192.168.0.8	POSEYTECHWRI...	OU=Computers,...	Windows Server 2016 ...Ja...		Virtual Machine	7/23/2019 3:02:...	7/22/2019 8:29:...	✓ Set (Inherited)	Installed
🟥	DO-WRITING-DC	192.168.0.1	POSEYTECHWRI...	OU=Domain Con...	Windows Server 2016 ...Ja...		Virtual Machine	7/23/2019 3:02:...	7/22/2019 8:29:...	✓ Set (Inherited)	Installed
🟥	DO-WRITING-PROX	208.91.197.194	POSEYTECHWRI...	-	Windows Server 2016 ...Ja...		Virtual Machine	7/23/2019 3:03:...	7/22/2019 8:29:...	✓ Set (Inherited)	Installed
🟥	DO-WRITING-ADC	192.168.0.5	POSEYTECHWRI...	-	Windows Server 2016 ...Ja...		Virtual Machine	7/23/2019 3:02:...	7/22/2019 8:29:...	✓ Set (Inherited)	Installed
🟥	DO-WRITING-CA	192.168.0.3	POSEYTECHWRI...	-	Windows Server 2016 ...Ja...		Virtual Machine	7/23/2019 3:02:...	7/22/2019 8:29:...	✓ Set (Inherited)	Installed
	DO-WRITING-ADFS	-	-	-	-	-	-	-	-	✓ Set (Inherited)	Deployment Errors

LanGuard is monitoring the computers within a Windows domain.

03 Addressing Vulnerabilities

If you look at the previous figure, you will notice that the list of computers contains a column called VL. VL is short for Vulnerability Level. The VL column contains a color code that corresponds to the perceived level of vulnerability. In my case, each computer is considered to be highly vulnerable.

Clicking on an individual computer takes you to a dashboard that provides information about that specific system. If you look at the figure below, you can see that in addition to providing some basic computer details, LanGuard lists the top five issues that need to be addressed, as well as the vulnerability trend over time.



DD-WRITING-APP (192.168.0.8)

Top 5 Issues to Address
- AutoRun is enabled
- No supported antispyware product found on this machine!
- No supported antivirus product found on this machine!
- AutoShareServer
- AutoShareWKS

Name	DD-WRITING-APP
IP Address	192.168.0.8
MAC Address	00-15-5D-64-64-25 (Microsoft Corporation)
Manufacturer	Microsoft Corporation
Model	Virtual Machine
Operating System	Windows Server 2016 x64 (SP, Version 1607)

Last Scan: 7/23/2019 3:02:25 PM

Agent Installed (build 20180706)
Scans run every day at 12:00:00 PM
Last result received on: 7/22/2019 8:33:55 AM

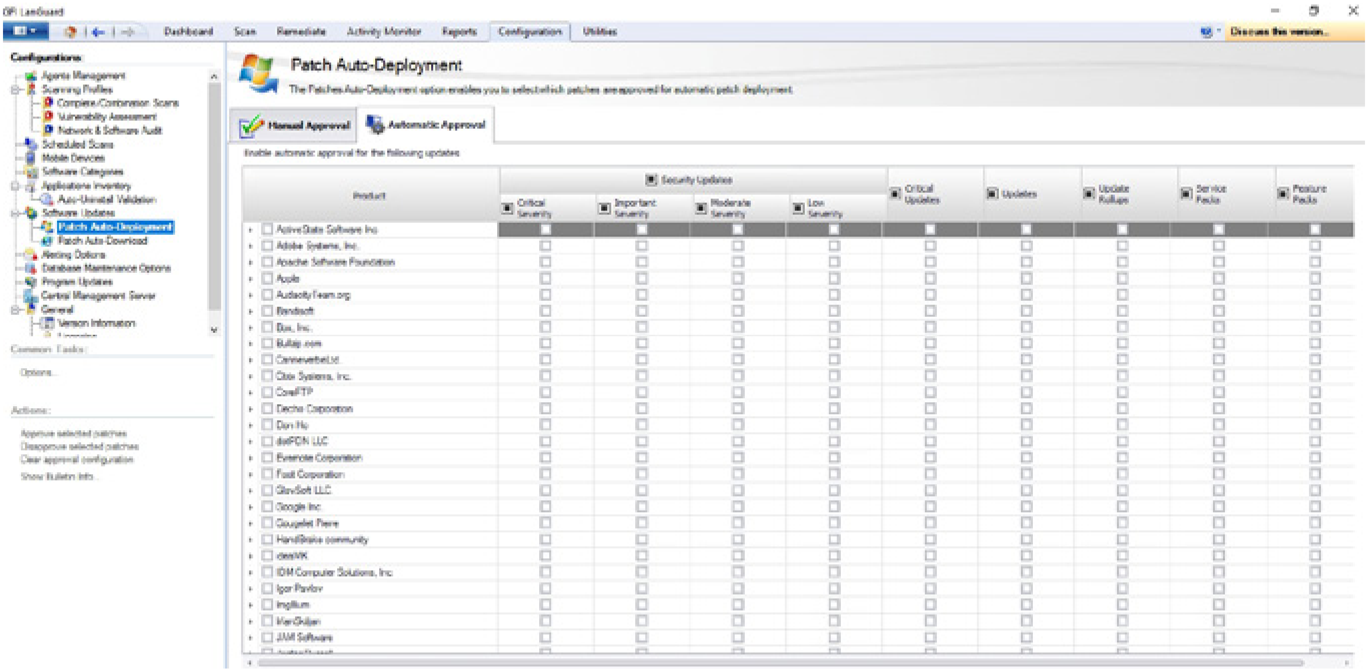
Other Vulnerabilities: 7 (3 Critical/High)	Potential Vulnerabilities: 1
Installed Applications: 2 (0 unauthorized)	Open Ports: 11
Shares: 3	Network Devices: 8 (0 blacklisted)
Services: 96	Processes: 51
Logged on Users: 7	

LanGuard allows you to examine an individual machine.

As helpful as it may be to learn what vulnerabilities may exist on a particular machine, it is much more important to remediate those vulnerabilities. Although you can of course, address vulnerabilities manually, LanGuard also gives you remediation capabilities. You can right click on a computer, a group of computers, or even an entire domain to be taken to the Remediation Center. The Remediation Center provides options for installing or uninstalling software updates, deploying custom software, uninstalling unauthorized applications, fixing problems with malware protection, and providing remote support via a RDP connection.

04 Patch Management

One of GFI LanGuard's key capabilities is that of detecting and applying missing patches. LanGuard is not limited to solely scanning for missing operating system patches. The software has built-in patch management capabilities for software from a huge number of vendors. You can see some of these vendors listed on the Automatic Approval screen, shown in the figure below.



Patch Auto-Deployment

The Patches Auto-Deployment option enables you to select which patches are approved for automatic patch deployment.

Enable automatic approval for the following updates

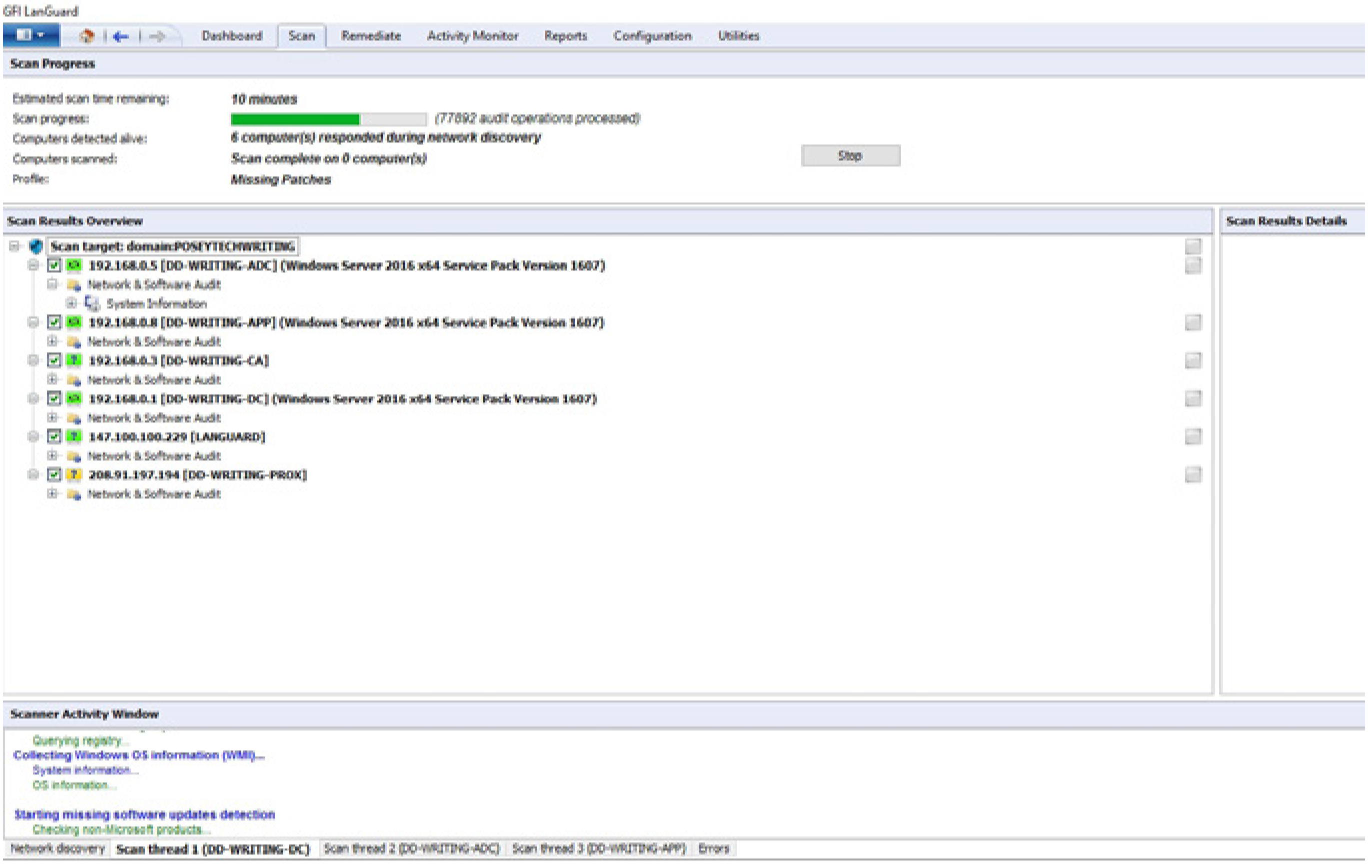
Product	☒ Security Updates				☒ Critical Updates	☒ Updates	☒ Update Rollups	☒ Service Packs	☒ Feature Packs
	☒ Critical Severity	☒ Important Severity	☒ Moderate Severity	☒ Low Severity					
☐ ActiveState Software Inc	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ Adobe Systems, Inc.	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ Apache Software Foundation	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ Apple	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ AudacityTeam.org	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ Bandisoft	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ Box, Inc.	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ Bullzip.com	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ CanneverbeLtd	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ Citrix Systems, Inc.	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ CoreFTP	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ Decho Corporation	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ Don Ho	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ dotPDN LLC	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ Evernote Corporation	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ Foxit Corporation	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ GlavSoft LLC	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ Google Inc	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ Gougelet Pierre	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ HandBrake community	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ ideaMK	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ IDM Computer Solutions, Inc	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ Igor Pavlov	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ ImgBurn	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ IrfanSkiljan	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐ JAM Software	☐	☐	☐	☐	☐	☐	☐	☐	☐

GFI LanGuard is able to scan for patches from numerous software vendors.

This brings up an important point. GFI LanGuard downloads patches automatically, but the administrator has quite a bit of control over the download process. For instance, an admin might opt to only download patches from specific vendors or for specific products. There are also ways of controlling the number of download threads used, and which patch languages are downloaded. Incidentally, if you have a WSUS server, then LanGuard can be configured to use it rather than performing redundant patch downloads.

05 Missing Patch Scans

Although GFI LanGuard allows you to perform a fully comprehensive scan of the computers on your network, the product also provides several different scan profiles. These profiles are handy if you want to check something specific without taking the time to scan everything. I decided to try out the scanning profile named Missing Patches to see how it worked. This of course meant running a manual scan, but scans can be configured to occur automatically. You can see what the scanning process looks like in the next figure.



Scan Progress

Estimated scan time remaining: 10 minutes
Scan progress: (77892 audit operations processed)
Computers detected alive: 6 computer(s) responded during network discovery
Computers scanned: Scan complete on 0 computer(s)
Profile: Missing Patches

Scan Results Overview

```
Scan target: domain:POSEYTECHWRITING
  ☑ 192.168.0.5 [DD-WRITING-ADC] (Windows Server 2016 x64 Service Pack Version 1607)
      Network & Software Audit
        System Information
  ☑ 192.168.0.8 [DD-WRITING-APP] (Windows Server 2016 x64 Service Pack Version 1607)
      Network & Software Audit
  ☑ 192.168.0.3 [DD-WRITING-CA]
      Network & Software Audit
  ☑ 192.168.0.1 [DD-WRITING-DC] (Windows Server 2016 x64 Service Pack Version 1607)
      Network & Software Audit
  ☑ 147.100.100.229 [LANGUARD]
      Network & Software Audit
  ☑ 208.91.197.194 [DD-WRITING-PROX]
      Network & Software Audit
```

Scanner Activity Window

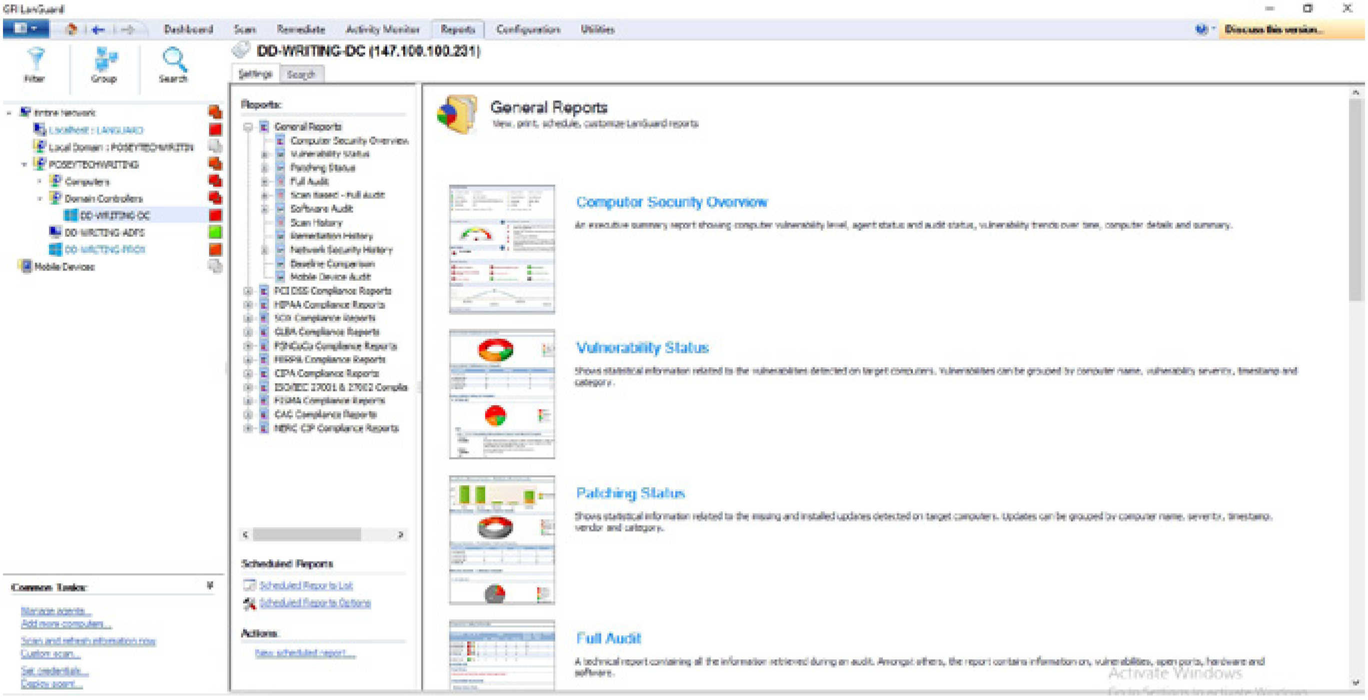
```
    Querying registry...
Collecting Windows OS information (WMI)...
    System information...
    OS information...

Starting missing software updates detection
    Checking non-Microsoft products...
```

Network discovery | Scan thread 1 (DD-WRITING-DC) | Scan thread 2 (DD-WRITING-ADC) | Scan thread 3 (DD-WRITING-APP) | Errors

I manually initiated a Missing Patches scan of the computers on my network.

The scanning process completed relatively quickly. It took roughly about fifteen or twenty minutes to scan my test VMs. In all fairness though, all of those VMs are on the same host, and the host server's resources were nearly depleted. I am guessing that a scan would probably complete more quickly in a production environment.

Once the scan has completed, you can easily perform a remediation that collectively deploys all of the missing patches. GFI LanGuard also includes a really nice reporting engine where you can find detailed information on the health of your systems. In addition to the general reports such as vulnerability status reports and patching status reports, the reporting engine includes a number of compliance reports that will be unquestionably useful to those who need to comply with regulations such as PCI DSS or HIPAA. You can see the reporting screen in the next figure.



General Reports

View, print, schedule, customize LanGuard reports

Computer Security Overview

An executive summary report showing computer vulnerability level, agent status and audit status, vulnerability trends over time, computer details and summary.

Vulnerability Status

Shows statistical information related to the vulnerabilities detected on target computers. Vulnerabilities can be grouped by computer name, vulnerability severity, timestamp and category.

Patching Status

Shows statistical information related to the missing and installed updates detected on target computers. Updates can be grouped by computer name, severity, timestamp, vendor and category.

Full Audit

A technical report containing all the information retrieved during an audit. Amongst others, the report contains information on, vulnerabilities, open ports, hardware and software.

These are some of the reports that are available.

06 The Verdict

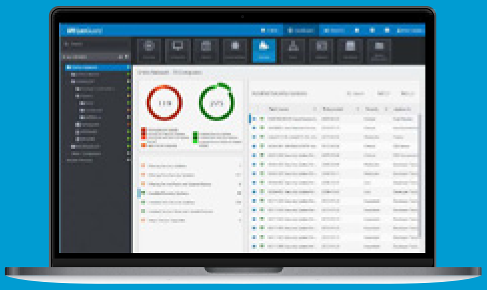
Whenever I write a review for this site, I like to conclude the process by giving the product a numerical score, ranging between zero and five stars, with five stars being the highest possible score. In the case of GFI LanGuard, I decided to go with a score of 4.7, which is a gold star review.

4.7/5

TechGenix ★ ★ ★ ★ ★ GOLD AWARD

Overall, I really liked the software. I found it to be mostly intuitive, and I think that it would do an excellent job of helping administrators to figure out which computers on their networks require attention.

In the process of writing this review, I did encounter some errors referencing insufficient memory. However, once I added a bit of memory, LanGuard worked exactly as expected. Incidentally, working through those memory issues gave me a chance to look at the product's documentation, which I found to be well written and easy to follow.



Get your FREE LanGuard trial

TechGenix

All product names and companies mentioned may be trademarks or registered trademarks of their respective owners. All information in this document was valid to the best of our knowledge at the time of its publication. The information contained in this document may be changed without prior notice.