GFI Software™

LanGuard

GFI LanGuard

L 100 certification training

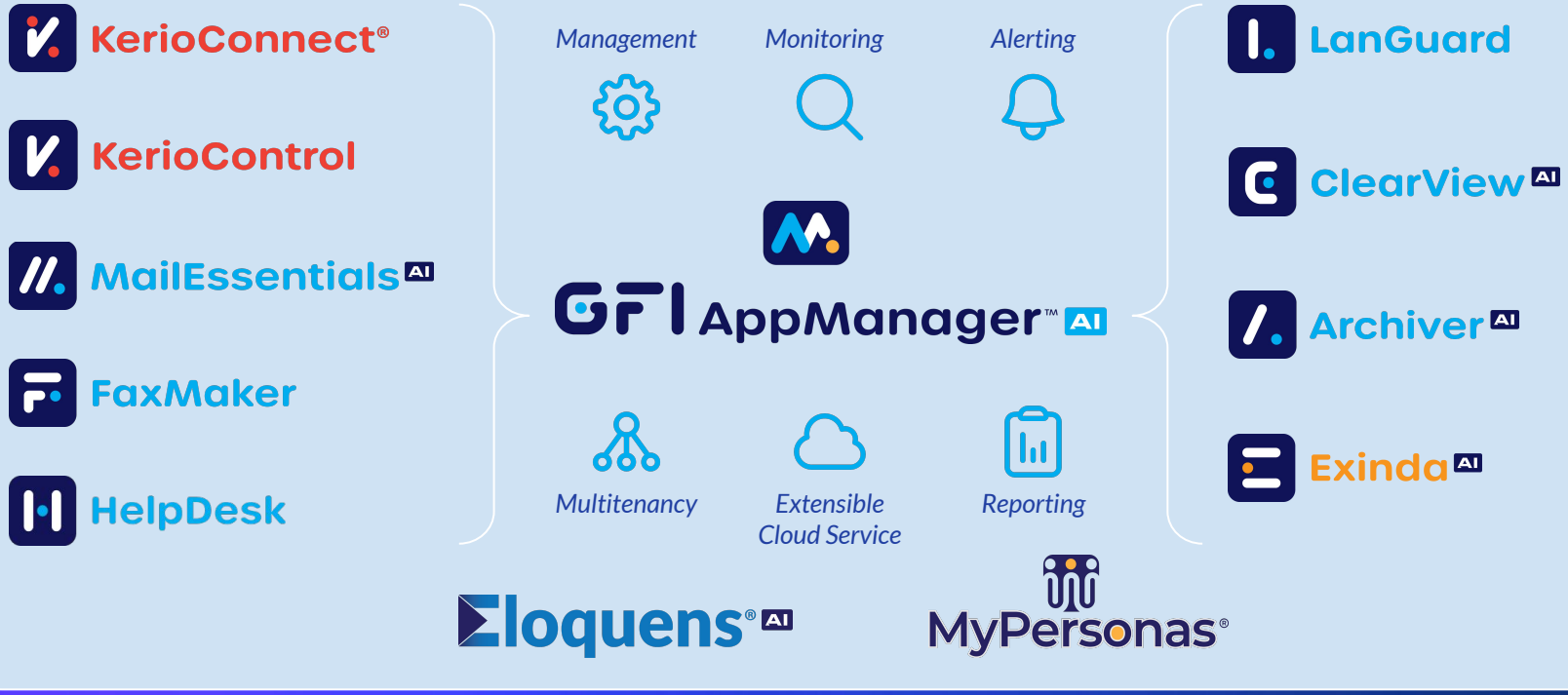


Agenda

1. GFI product family
2. GFI LanGuard product overview
3. Use cases
4. Deployment
5. Main features
6. Licensing

#1 GFI product family

GFI Product Portfolio



#2 GFI LanGuard:

product overview

GFI LanGuard features



Vulnerability assessment

Patch management

Software and hardware audit

Device identification

All information is retrieved by scanning

Variety of gathered information

1. Categorized OS vulnerabilities
2. Categorized 3rd party application vulnerabilities
3. Categorized already deployed patches
4. Deployed OS and version
5. Node vulnerability level
6. Network role
7. Model and SN
8. Installation date and language
9. Open TCP and UDP
10. Processes using TCP/UDP ports
11. Categorized SW deployed on target nodes
12. Categorized HW components deployed on target nodes
13. Present shares
14. Running services
15. Running processes
16. User groups
17. Logged on users
18. Open sessions
19. Microsoft SN
20. Password policies
21. Audit policies
22. Security audit policy
23. Time of the day
24. Present AV Software
25. State of Windows firewall
26. Organization units
27. Disk Encryption
28. And more...

Features per OS, app and device

Operating System	DI/PS	VA	PM	SA	HA
Windows Server	✓	✓	✓	✓	✓
Windows Client OS	✓	✓	✓	✓	✓
Linux Distributions *(Oracle, RHEL, CentOS, Ubuntu, Debian, SUSE, openSUSE, Fedora, Debian)*	✓	✓	✓	✓	✓
macOS 10.5 & above	✓	✓	✓	✓	✓
VM with supported OS	✓	✓	✓	✓	✓
Mobile & network devices	✓	✓			

DI: *Device Identification*

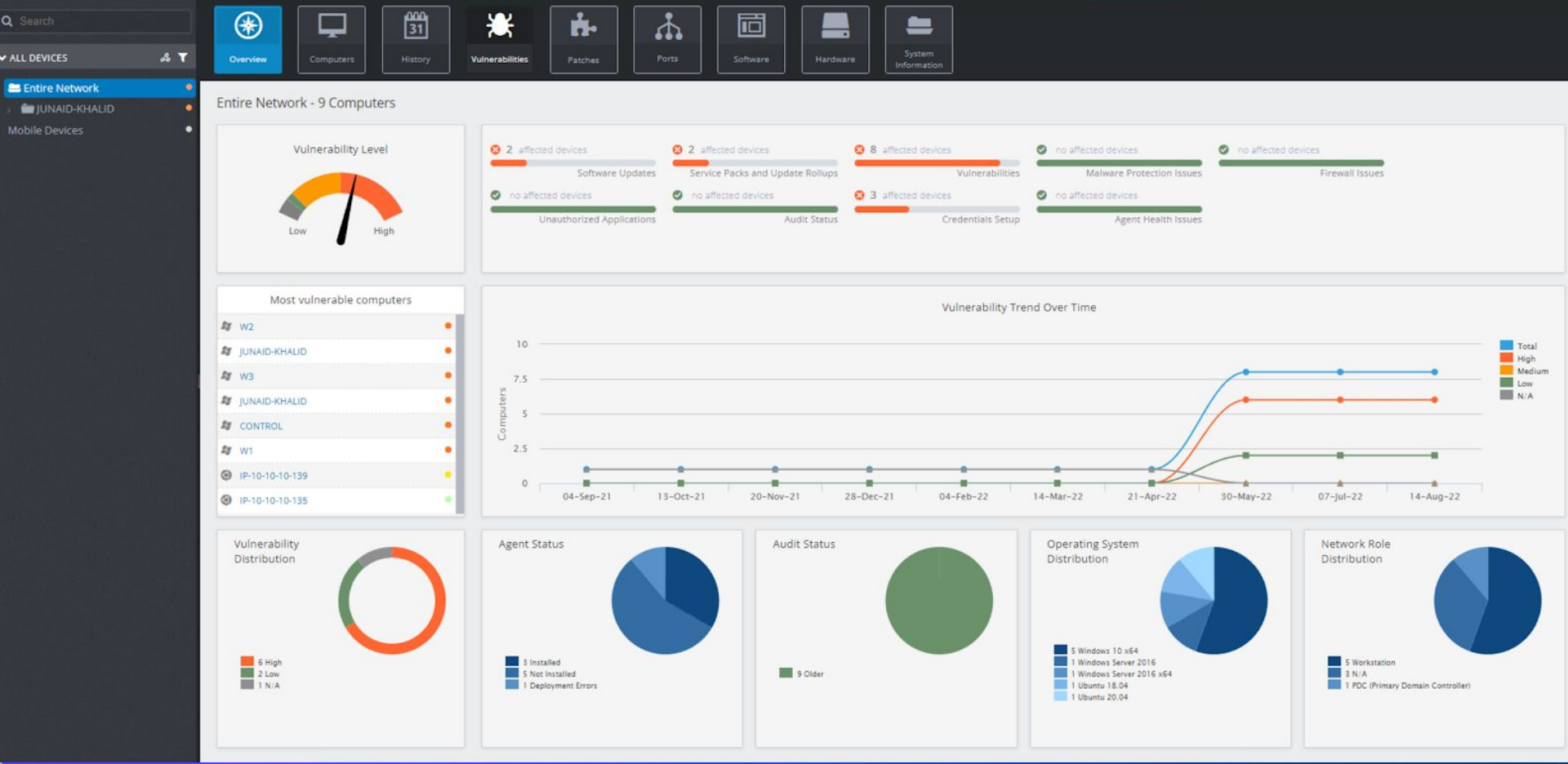
PS: *Port Scanning*

VA: *Vulnerability Assessment*

PM: *Patch Management*

SA: *Software Audit*

HA: *Hardware Audit*


Search
ALL DEVICES
Entire Network
JUNAID-KHALID
Mobile Devices
Overview
Computers
History
Vulnerabilities
Patches
Ports
Software
Hardware
System Information
Entire Network - 9 Computers
Vulnerability Level
Low
High
2 affected devices
Software Updates
2 affected devices
Service Packs and Update Rollups
8 affected devices
Vulnerabilities
no affected devices
Malware Protection Issues
no affected devices
Firewall Issues
no affected devices
Unauthorized Applications
no affected devices
Audit Status
3 affected devices
Credentials Setup
no affected devices
Agent Health Issues
Most vulnerable computers
W2
JUNAID-KHALID
W3
JUNAID-KHALID
CONTROL
W1
IP-10-10-10-139
IP-10-10-10-135
Vulnerability Trend Over Time
Computers
10
7.5
5
2.5
0
04-Sep-21
13-Oct-21
20-Nov-21
28-Dec-21
04-Feb-22
14-Mar-22
21-Apr-22
30-May-22
07-Jul-22
14-Aug-22
Total
High
Medium
Low
N/A
Vulnerability Distribution
6 High
2 Low
1 N/A
Agent Status
3 Installed
5 Not Installed
1 Deployment Errors
Audit Status
9 Older
Operating System Distribution
5 Windows 10 x64
1 Windows Server 2016
1 Windows Server 2016 x64
1 Ubuntu 18.04
1 Ubuntu 20.04
Network Role Distribution
5 Workstation
3 N/A
1 PDC (Primary Domain Controller)

#3 Use cases

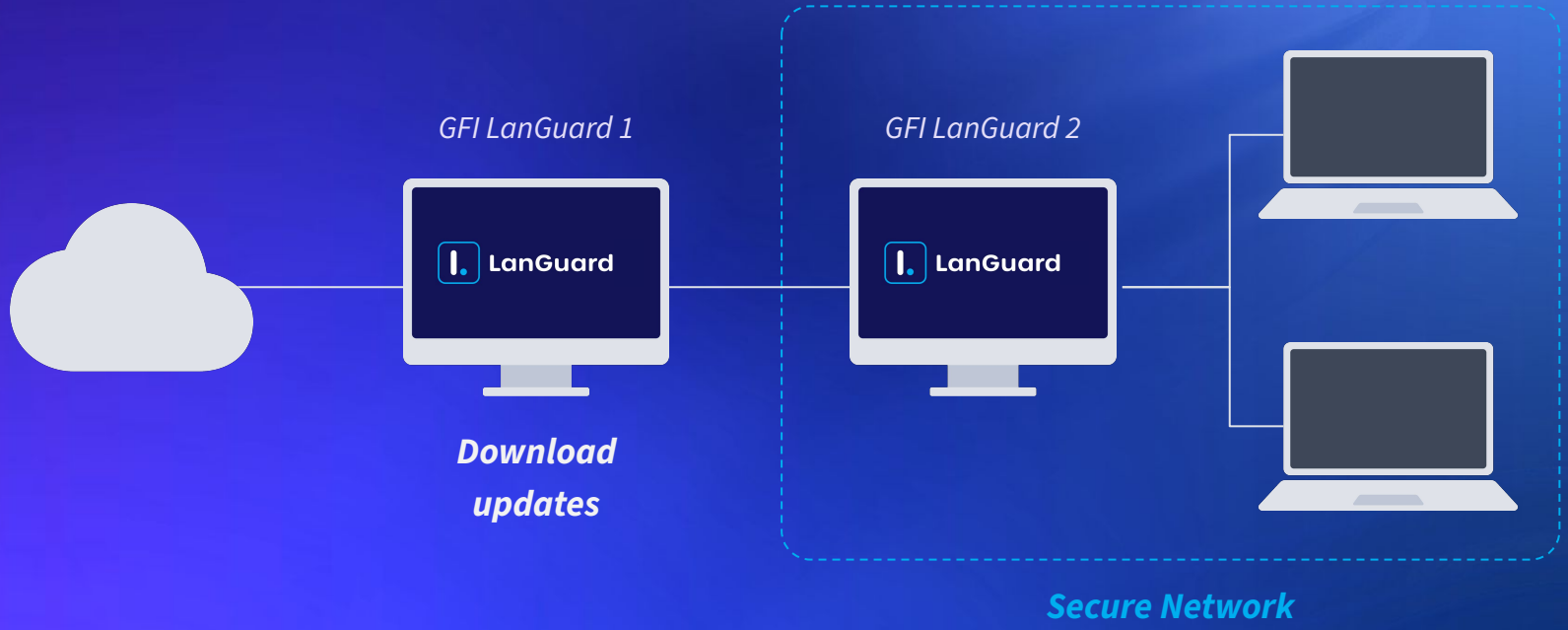
Patch automation is essential

for your cybersecurity hygiene

Common use cases

- Cybersecurity audit
- Vulnerability scanner
- Central patch management and patch automation
- Part of multi-layered security approach
- Compliance and SoC
- Deployment in secured environment

Updating in secured environments



#4 Deployment

Requirements



Supported OS (Windows) +
SQL or SQL Express database

Scanning capabilities

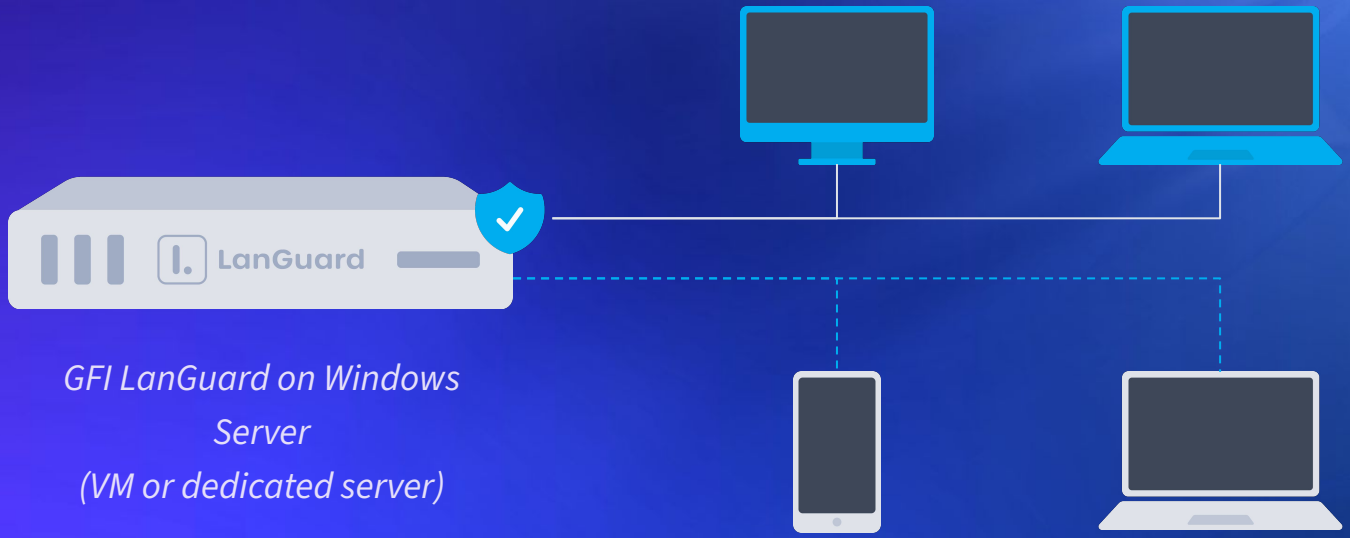


Server-based scan



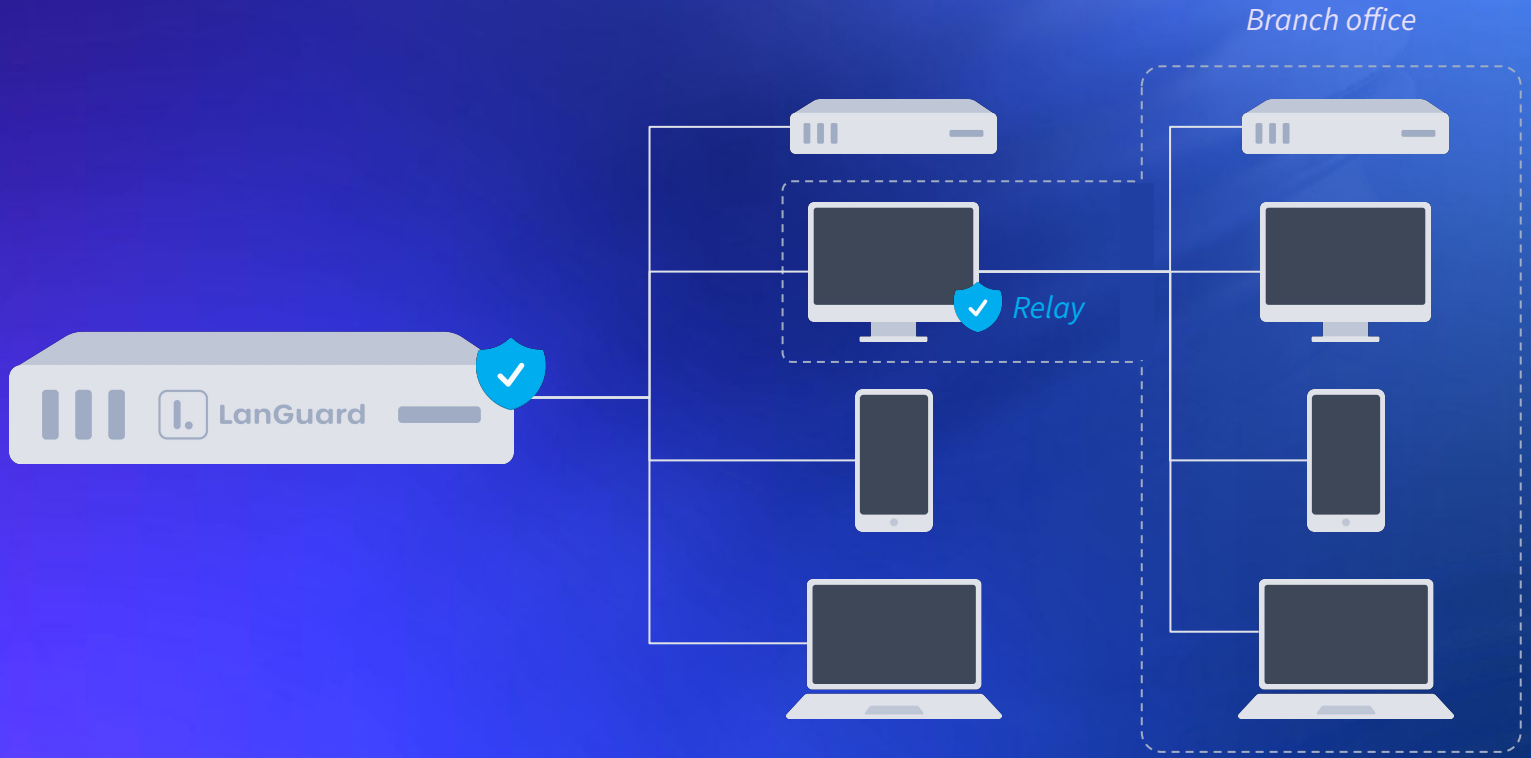
Agent-based scan

Sample deployment

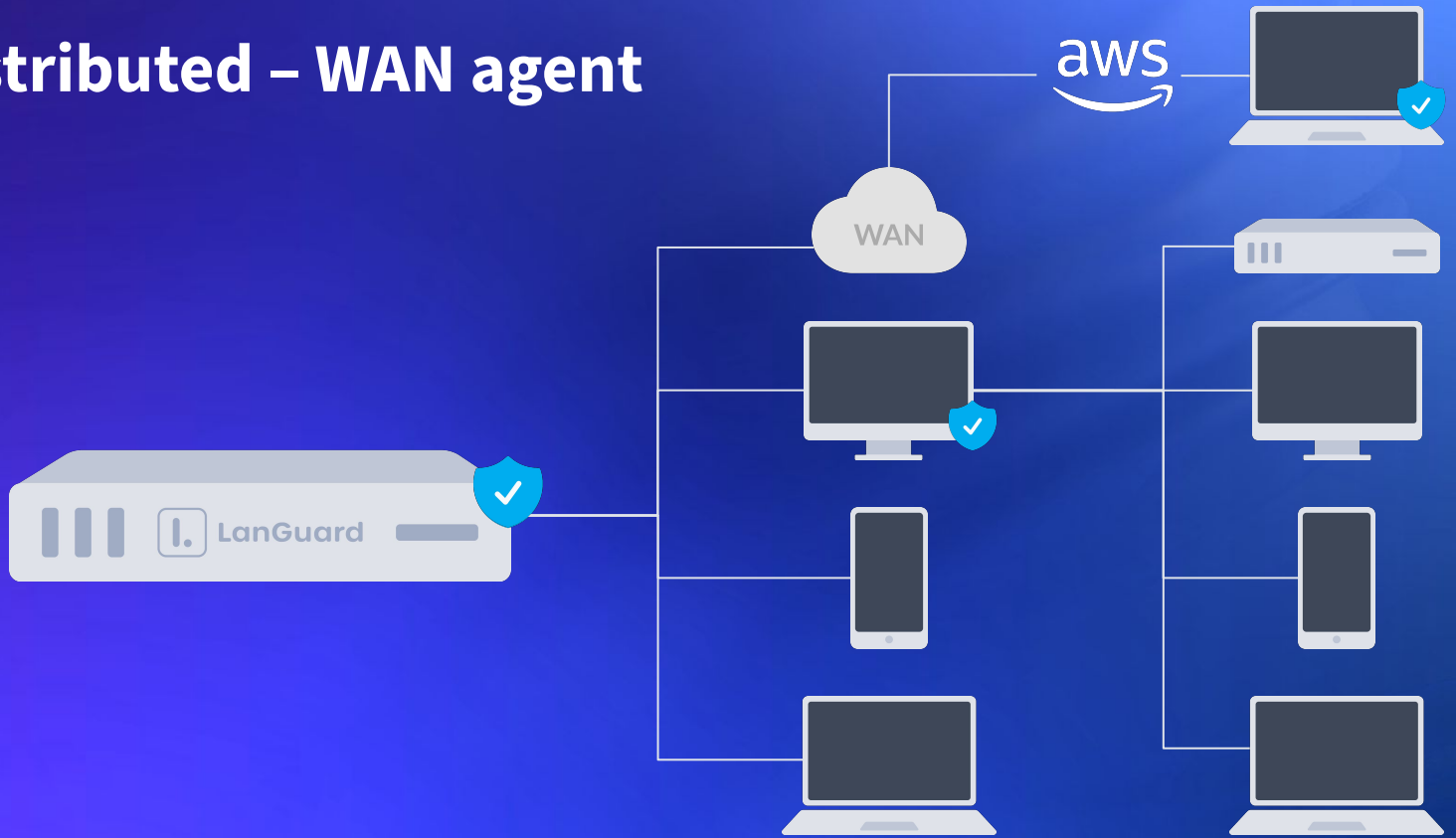


GFI LanGuard on Windows Server
(VM or dedicated server)

Distributed – Relay Agent



Distributed – WAN agent



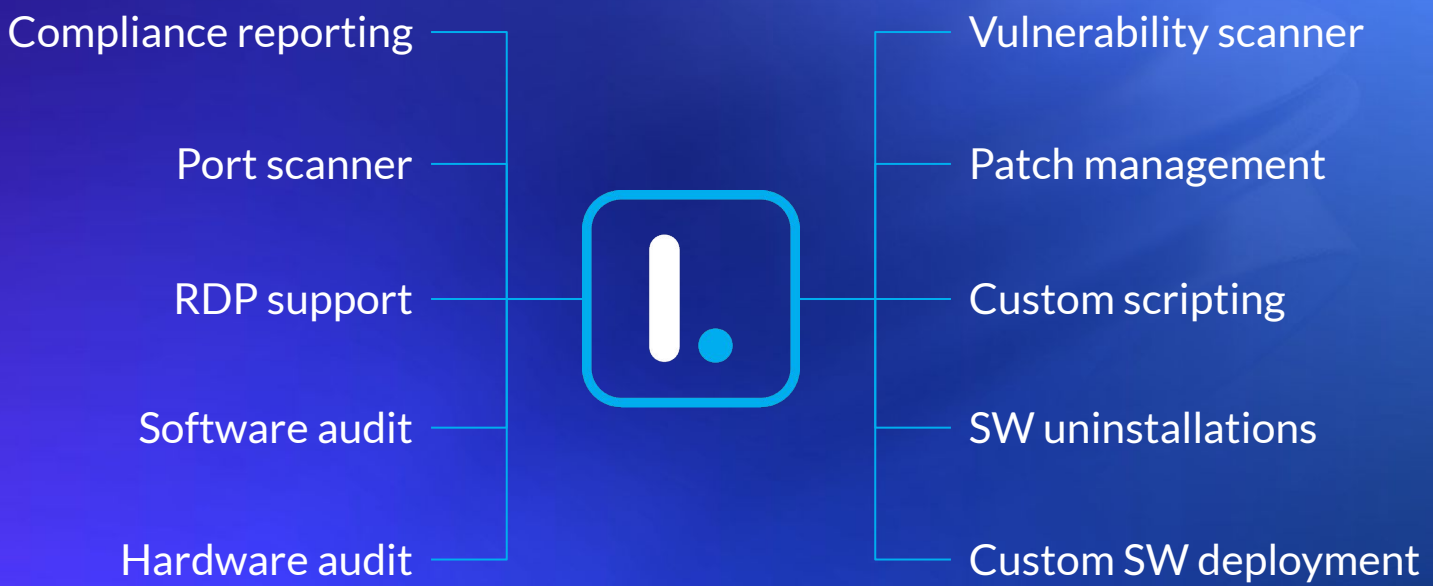
WAN Agent security

- Encryption
- SSL Communication
- AWS tenant isolated per customer
- No changes can be made to the tenant
- Connection to the tenant is always using certificates

Benefits

- Deploy anywhere
- Ensure complete coverage
- Deploy once, audit forever

#5 Main features


Compliance reporting
Port scanner
RDP support
Software audit
Hardware audit
Vulnerability scanner
Patch management
Custom scripting
SW uninstallations
Custom SW deployment

LanGuard

Compliance reporting

Port scanner RDP support Software

Automatically export reports covering well known regulations: PCI DSS, ISO 27001, SoX and others

LanGuard

Port scanner

RDP support

Software audit

Hardware audit

Evaluates availability of TCP and UDP ports on target nodes.

LanGuard

RDP support

Software audit Hardware audit Vulnerability

Within the same console, administrators can take advantage of embedded RDP.

LanGuard

Software audit

Hardware audit Vulnerability scanner Patch m

Detects and categorizes all applications deployed on the scanned nodes.

LanGuard

Hardware audit

Vulnerability scanner

Patch management

Detects and categorize all hardware components deployed/used on scanned nodes.

LanGuard

Vulnerability scanner

Patch management

Custom scripting

Detects vulnerabilities on supported devices and operating systems.

LanGuard

Patch management

Custom scripting SW uninstallations

Automatically or manually deploys desired patches on supported operating systems or over 60 third- party vendor applications.

LanGuard

Custom scripting

SW uninstallations

Custom SW deployment

Allows administrators to define custom vulnerabilities to be detected during scans.

LanGuard

SW uninstallations

Custom SW deployment

Uninstall unwanted 3rd party applications during remediation.

LanGuard

Custom SW deployment

Deploy 3rd party applications on target nodes.

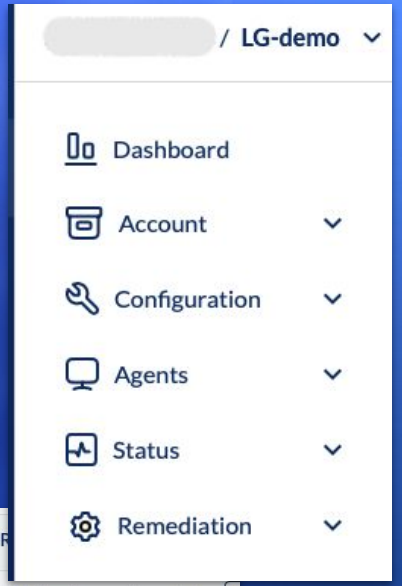
GFI AppManager AI integration

GFI LanGuard can be integrated with GFI AppManager AI for improved monitoring and management through GFI AppManager AI's cloud console, offering the following features:

- Role based access control
- User management
- Node allocation to specific accounts
- Enhanced alerting and notifications

LanGuard *in GFI AppManager AI*

- Customers can run scans, schedule scans, view configuration/status, and trigger remediation directly from AppManager



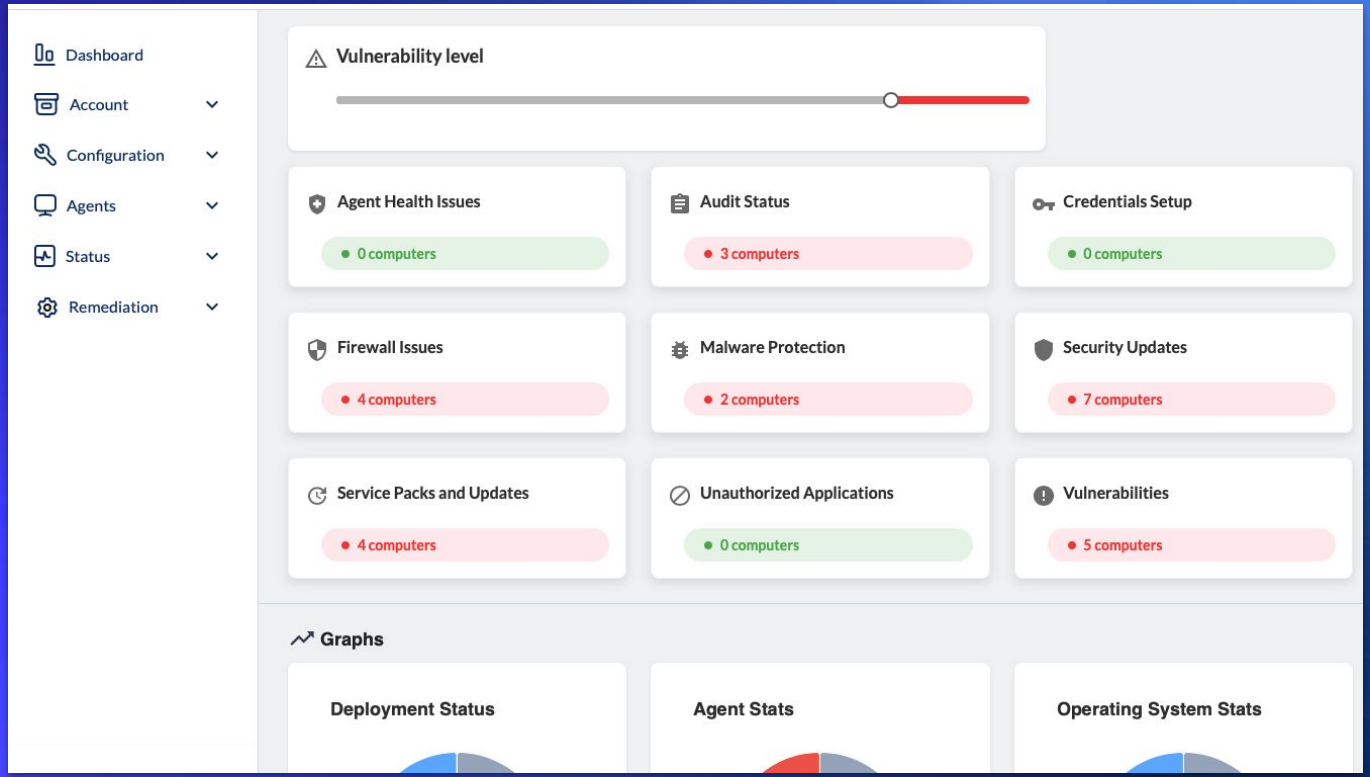
Overview | Shared Instances | Notifications | Configuration | IP Address Groups | UR

Search View

Appliance Status	Product	Appliance	Version	IP Address	Agent Version	Health Updated On	License Exp	High	Medium	Low
●	LanGuard GFI Official	LG-demo	12.15		1.2.133	1 minute ago	Jan 31, 2027	2	0	0

LanGuard *in GFI AppManager AI*

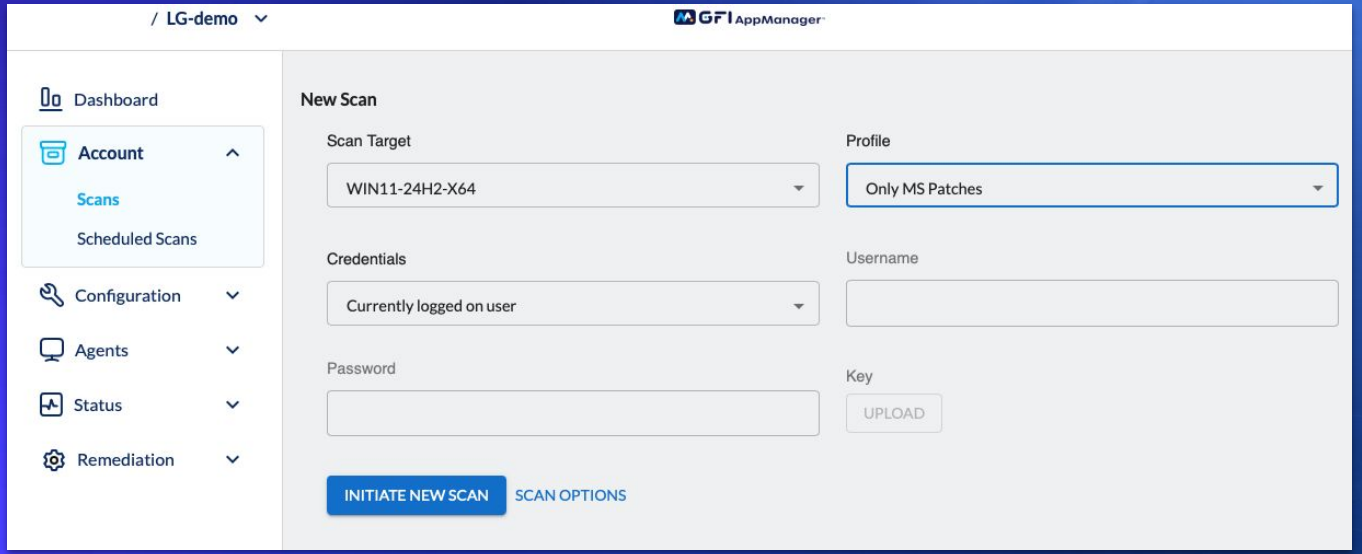
- Dashboard



GFI Software

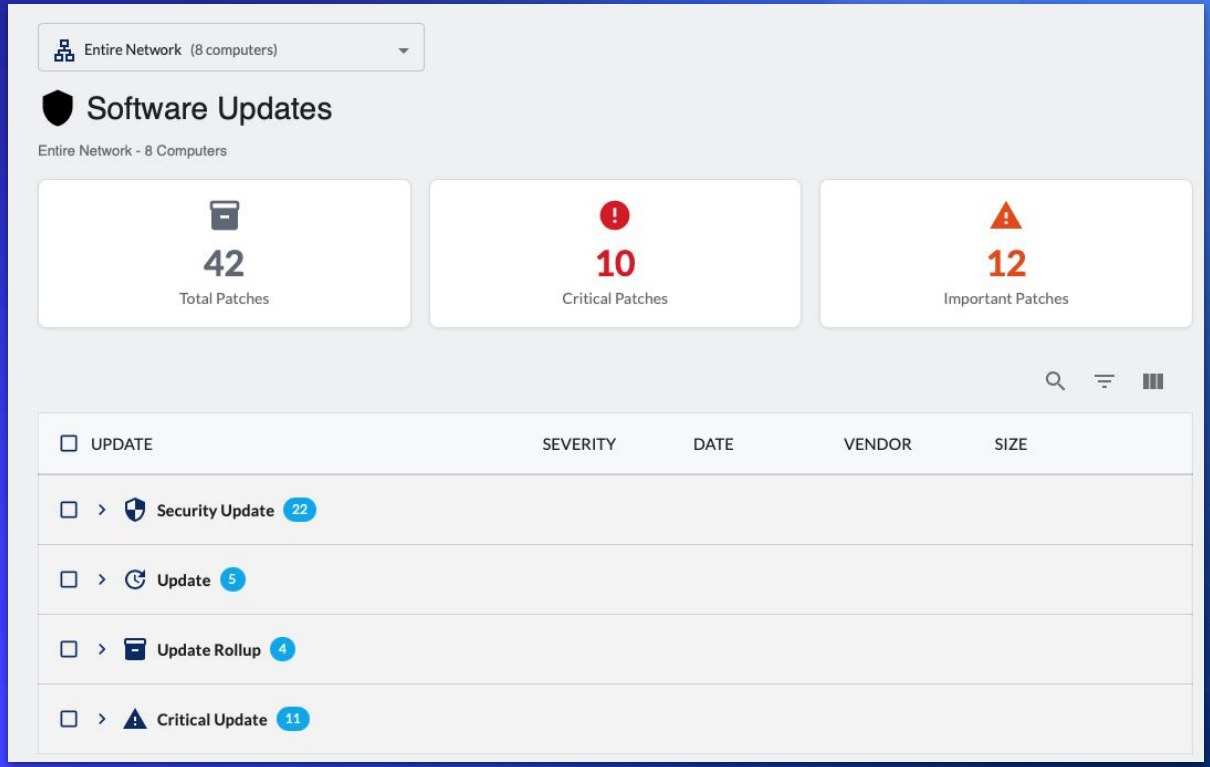
LanGuard *in GFI AppManager AI*

- Scans



LanGuard *in GFI AppManager AI*

- Patch management and Remediation



#6 Licensing

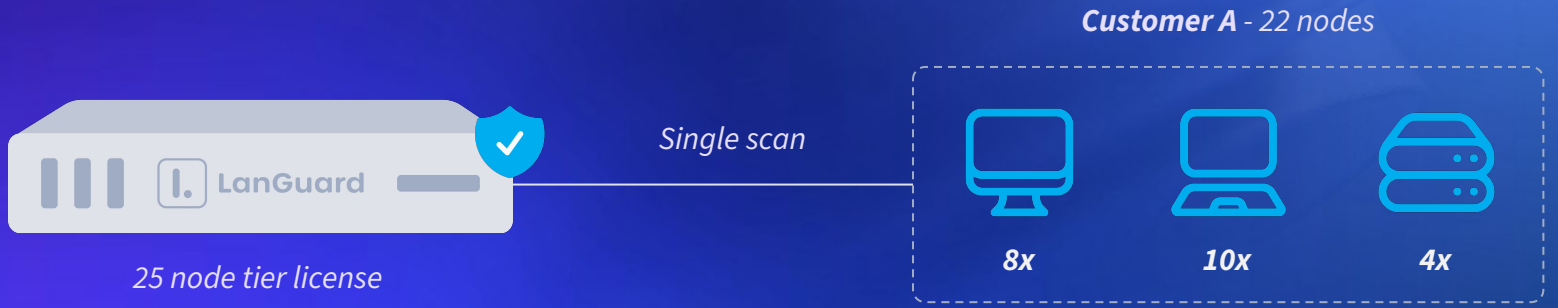
Licensing options

1. Yearly subscription based on the number of nodes.
2. “Pay per scan” monthly subscription based on number of nodes and number of scans. (GFI LanGuard MSP)

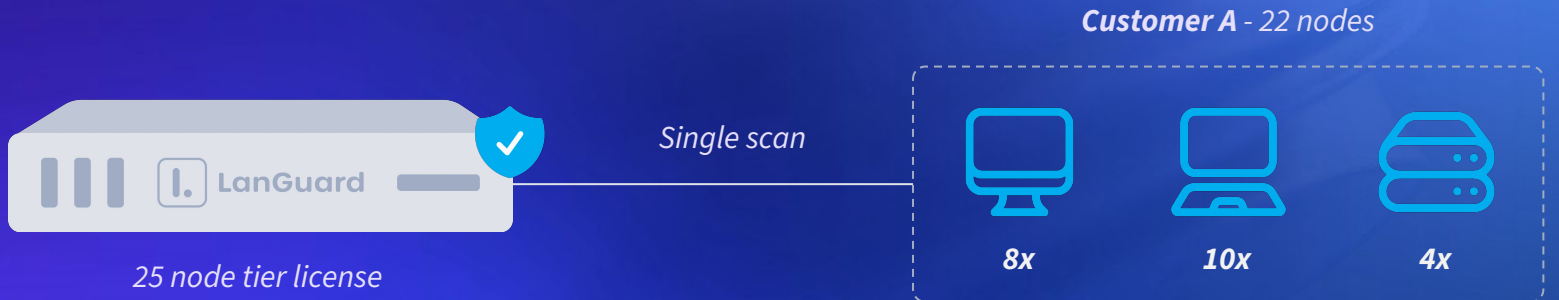


These are all nodes

GFI LanGuard MSP - “Pay per scan”



GFI LanGuard MSP - “Pay per scan”



Pay for single scan in 25 node tier

Single scan:

- Vulnerability level visibility
- Missing/deployed patches visibility
- Open ports
- SW and HW audit

+ Patch deployment
+ Reporting
+ SW uninstallation

GFI LanGuard MSP - “Pay per scan”



25 node tier license

Single scan

***Customer A** - 22 nodes*

8x ***10x*** ***4x***

***Customer B** - 20 nodes*

8x ***10x*** ***2x***

Pay for single scan in 25 node tier

Cybersecurity audit checklist *with GFI LanGuard*

- Audit scope
- Identify threats
- Review and edit internal policies
- Reevaluate your password and access strategies
- Reevaluate security software
- Ensure every workstation has an AV deployed and an active firewall
- Identify sensitive data and its location
- Ensure safety of sensitive data
- Inspect servers
- Check the procedures of management system
- Identify all OSs present in the infrastructure
- Ensure all OS and 3rd party SW are up to date
- Make sure users are accessing the internet safely
- Perform penetration testing
- Assess your current backup strategies
- Reinforce firewalls
- Review logs or log monitoring system
- Look for unauthorized access points

Thank you!

GFI Software™

gfi.com