



Cyber security audit as a service & more

Jozef Kačala
VP of Sales Engineering

Agenda

1. Cyber security audit
2. GFI LanGuard for MSPs
3. GFI ClearView
4. GFI AppManager



Cybersecurity is an arms race.
Hackers keep finding holes.

What is a Security Audit?

It's a process which allows organizations to test and assess their overall security posture, including cybersecurity. Result acts like a proof that defence is adequate and if the org meets compliance.

It covers :

- Infrastructure
- Deployed software
- Devices used by employees
- Data security
- Operational security
- Network security
- System security
- Physical security

What is a Security Audit?

It's a process which allows organizations to test and assess their overall security posture, including cybersecurity. Result acts like a proof that defence is adequate and if the org meets compliance.

It covers :

- Infrastructure
- Deployed software
- Devices used by employees
- Data security
- Operational security
- Network security
- System security
- Physical security

The first step to solving a problem is realizing it exists.

What are the Benefits

- Evaluation of data flow
- Vulnerability identification
- Issue identification
- Evaluation of internal/external processes
- Cost effective security approach
- Compliance

Best practices

- Include employees in the audit process
- Gather as much information as possible
- Track audit results over time
- Set clear timeline for mitigation of discovered issues
- Make results available for internal users
- Conduct regular audits
- Review your audit process to ensure it covers all aspects
- Update documentation
- Highlight discovered issues



Cyber security audit checklist

✓ Audit scope

✓ Identify sensitive data and its location

✓ Make sure users are accessing the internet safely

✓ Identify threats

✓ Ensure the safety of sensitive data

✓ Perform penetration testing

✓ Review and edit internal policies

✓ Inspect servers

✓ Assess your current backup strategies

✓ Reevaluate your password & access strategies

✓ Check the procedures of management system

✓ Reinforce firewalls

✓ Reevaluate security software

✓ Identify all OS present in the infrastructure

✓ Review logs or log monitoring system

✓ Ensure every workstation has an AV deployed and active firewall

✓ Ensure all OS and 3rd party SW is up to date

✓ Look for unauthorized access points

Cyber security audit checklist *with GFI LanGuard*

- ✓ Audit scope
- ✓ Identify threats
- ✓ Review and edit internal policies
- ✓ Reevaluate your password & access strategies
- ✓ Reevaluate security software
- ✓ Ensure every workstation has an AV deployed and active firewall
- ✓ Identify sensitive data and its location
- ✓ Ensure the safety of sensitive data
- ✓ Inspect servers
- ✓ Check the procedures of management system
- ✓ Identify all OS present in the infrastructure
- ✓ Ensure all OS and 3rd party SW is 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

Why service?

SMBs :

1. Low IT security budget
2. Low defense mechanisms and fewer policies in place
3. Simple structure makes reconnaissance easy
4. Small to no IT security team
5. Can be part of a supply chain

GFI LanGuard features



**All information is retrieved
by scanning**

Example 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
- „N“

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

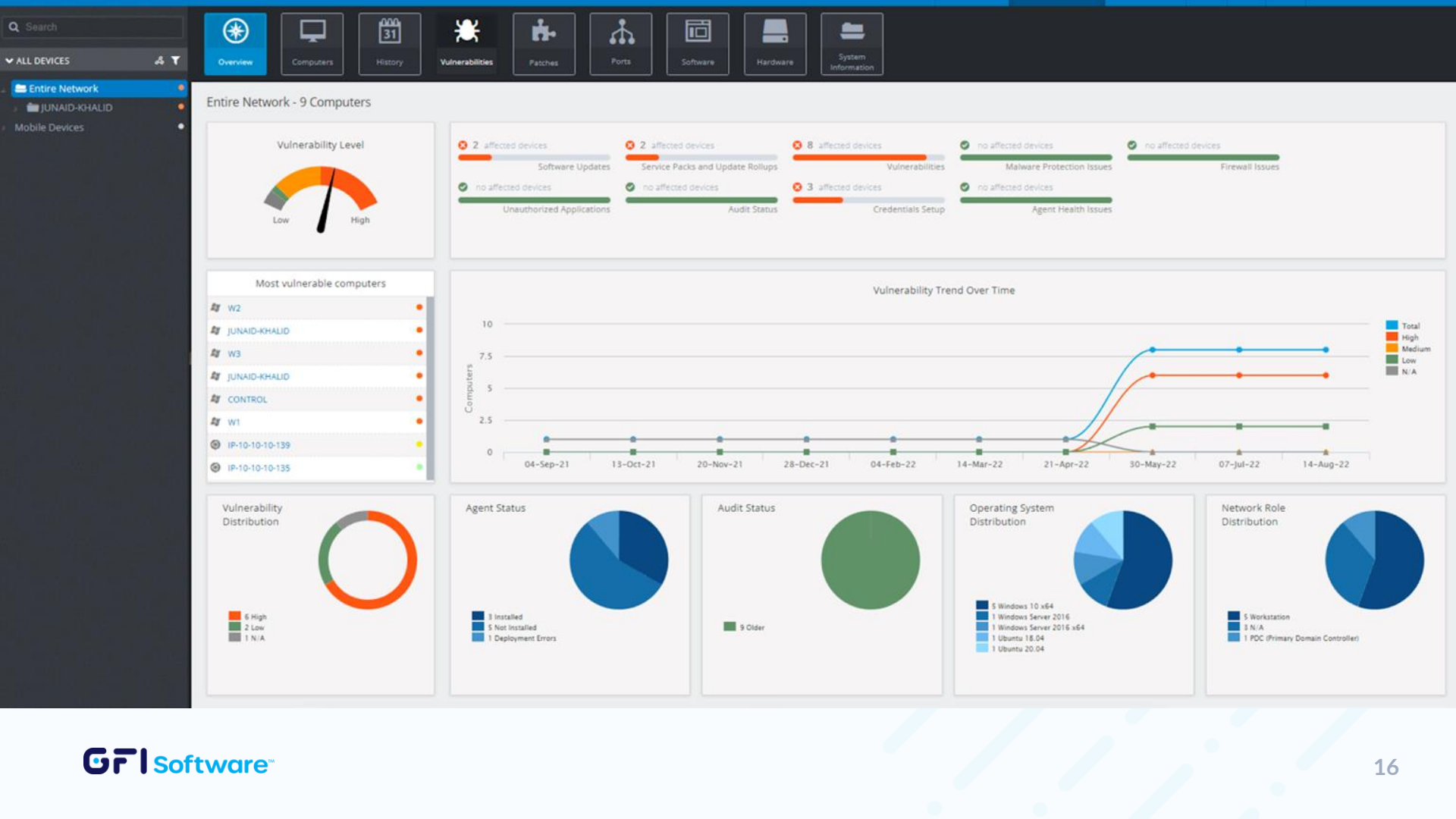
PS: Port Scanning

VA: Vulnerability Assessment

PM: Patch Management

SA: Software Audit

HA: Hardware Audit



Scanning capabilities



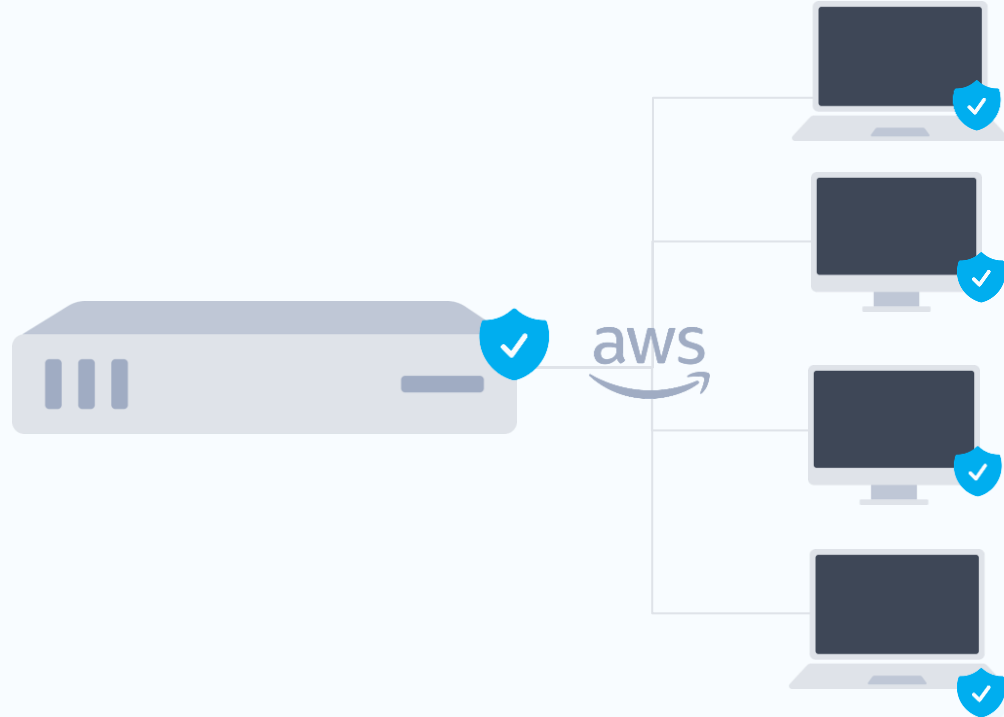
Server-based scan



Agent-based scan

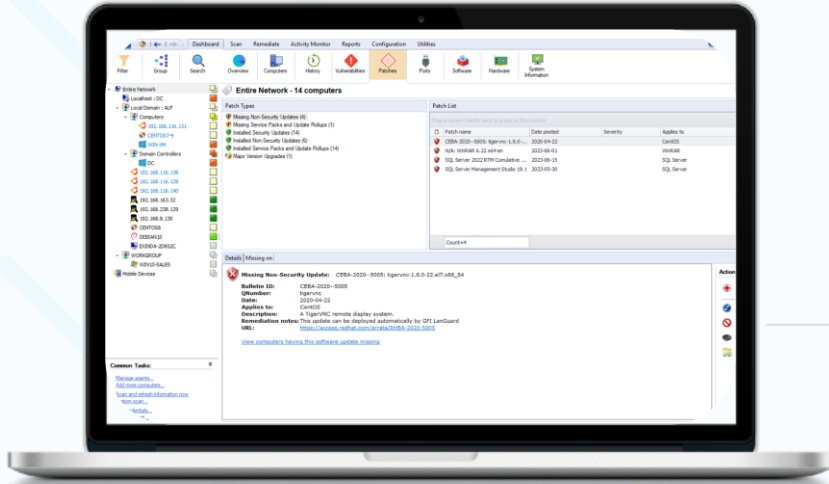
Traditional setup







MSP setup

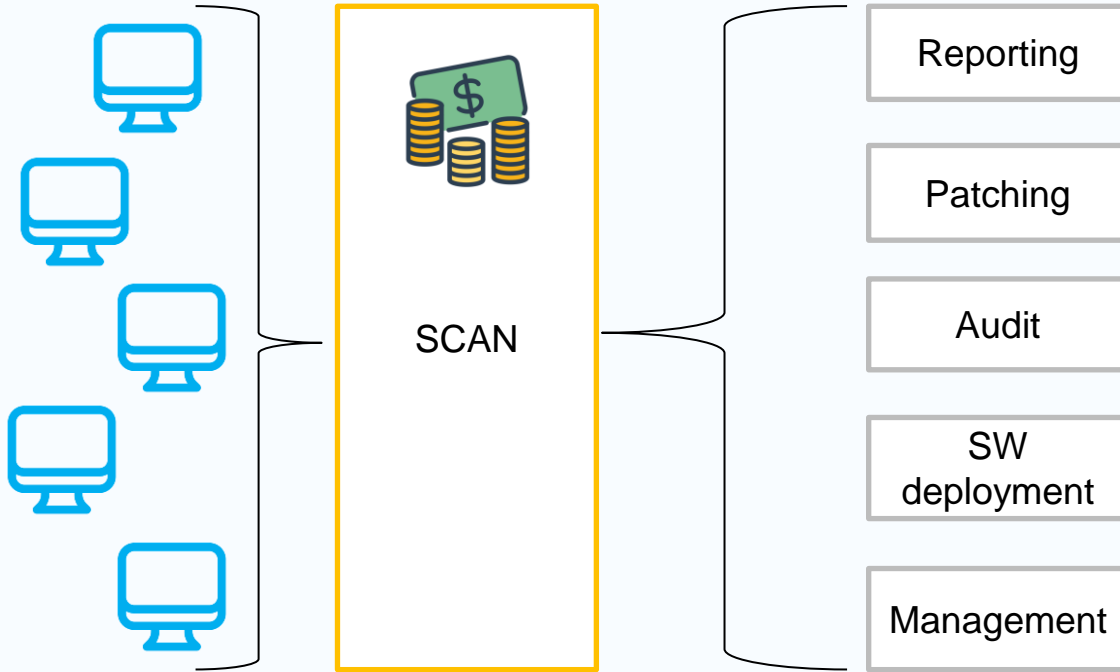




LanGuard




For MSPs

NEW!



**Its up to you
what service
you create**

Billing example *[MSP] Delta Solutions*

 Customer	A	B	C
 Nodes	<25 nodes <i>(20 scanned)</i>	<50 nodes <i>(45 scanned)</i>	< 100 nodes <i>(95 scanned)</i>
 Tier (USD)	Tier 1	Tier 2	Tier 3

175 nodes

Billing is for the scans only. Patch management and other operations can be performed for free (*no scan required*).

Example 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

MSPs need to go beyond just
the **product functionalities!**



Generic requirements of NIS2

The NIS2 directive sets new requirements for organisations' cyber and information security, as well as requirements regarding supervision and reporting.







ClearView Enterprise monitoring at an SMB price point

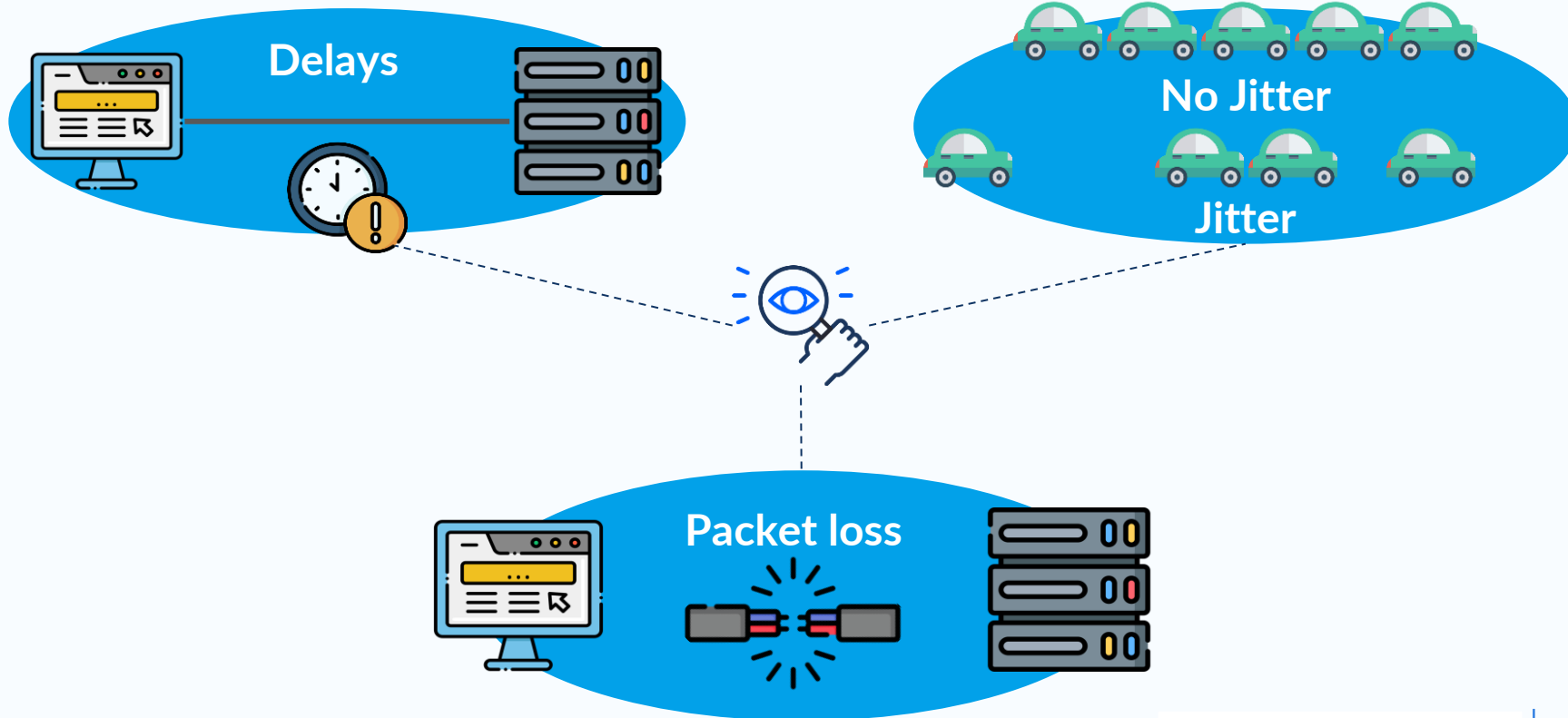


- Identify Bandwidth hogs
- Traffic usage (real-time & historic)
- Issues impacting application performance
- Recognizes thousands of applications
- Complements the firewall



ClearView

Troubleshooting network issues





Step by step

1. Deploy or Install ClearView Server on Network
2. Activate through the ClearView web UI
3. Mirror traffic from active ports to an unused port on switch
4. Enable Mirror option in ClearView Web UI
5. Start reporting



- Identify Bandwidth hoggers
- Traffic usage (real-time & historic)
- Issues impacting application performance
- Recognizes thousands of applications
- Complements the firewall



- Identify weak spots
- Central patch management
- Software & Hardware audit
- Built in reporting
- Asset tracking

Cyber security Audit



ClearView



LanGuard
For MSPs



**MSPs need simplified
management to increase
productivity and efficiency**



GFI AppManager™

*Paving the road for MSPs to
enhance their service offerings*

The screenshot displays the GFI AppManager web interface. The top navigation bar includes 'Home / GFI', 'Overview', 'Notifications', 'Configuration', 'Ip Address Groups', 'Url Groups', and 'Backups'. The left sidebar contains navigation icons for Home, Definitions, Alerts, Users, Products, and Radar. The main content area shows a 'Products' table with columns for Health, Product, and Appliance. Below the table is a filter for 'Last 3 hours' and an 'Instance Info' table. To the right of the instance info is a line chart titled 'Active Hosts'. At the bottom, there are two more charts: 'Active Connections by Protocol' and 'Active Archive Stores Size'.

Health	Product	Appliance
●	KerioControl	Appliance (7608)
●	Archiver	GFI Archiver
●	KerioConnect	GFI KerioConnect

Instance Info			
Product	Instance	Users	Version
kerio_connect	GFI KerioConnect	18	10.0.0 b
kerio_control	Appliance (7608)	3	9.4.2 pa
archiver	GFI Archiver	13	15.3
kerio_connect	s-kerio-connect	18	10.0.0 b

Active Hosts	
Time	Num hosts
09:00	2.5
09:30	2.45
10:00	2.4
10:30	2.7
11:00	2.9
11:30	3.0

Active Connections by Protocol	
Connections	Protocol
125	TCP
100	HTTP
75	HTTPS

Active Archive Stores Size	
Size (GB)	Store
1.08	Store 1
1.08	Store 2
1.07	Store 3

Go to application
for **everything**

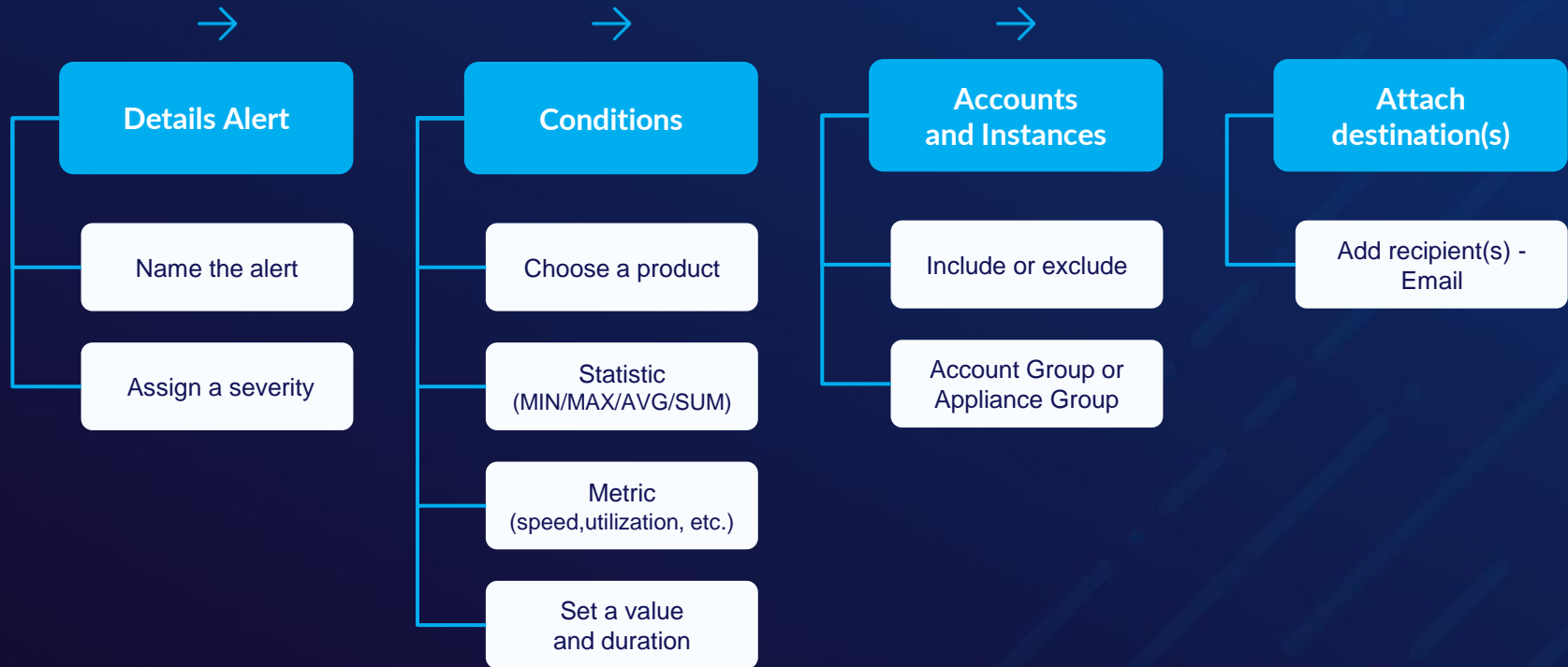




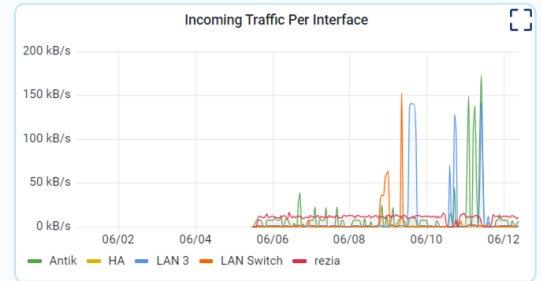
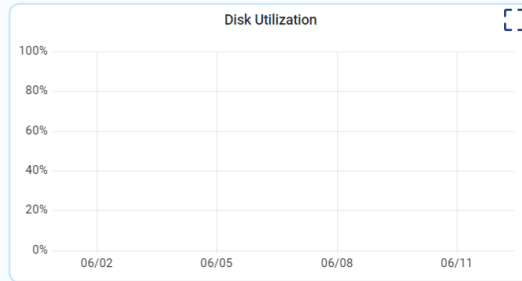
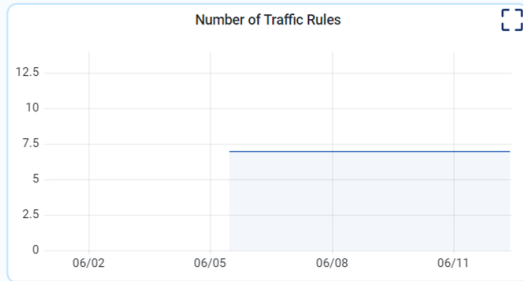
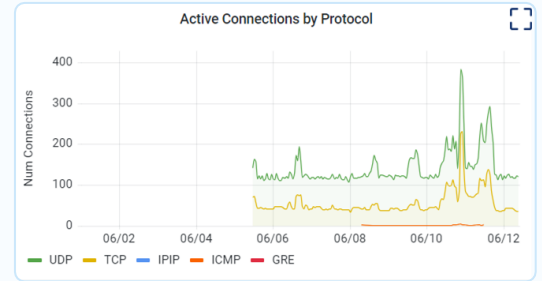
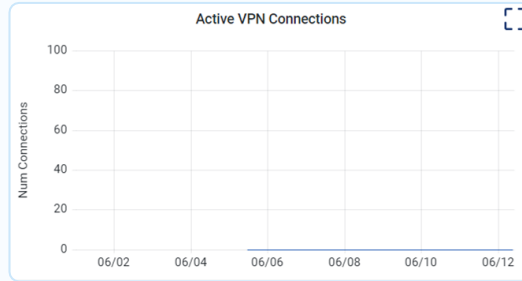
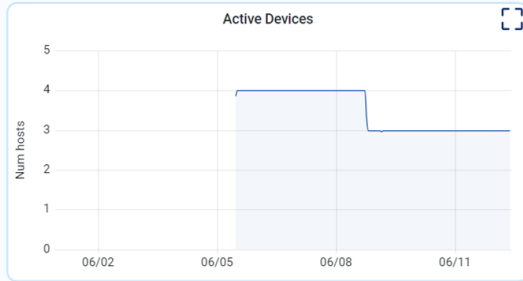
GFI AppManager™

*Innovation • Features • Ease of
use*

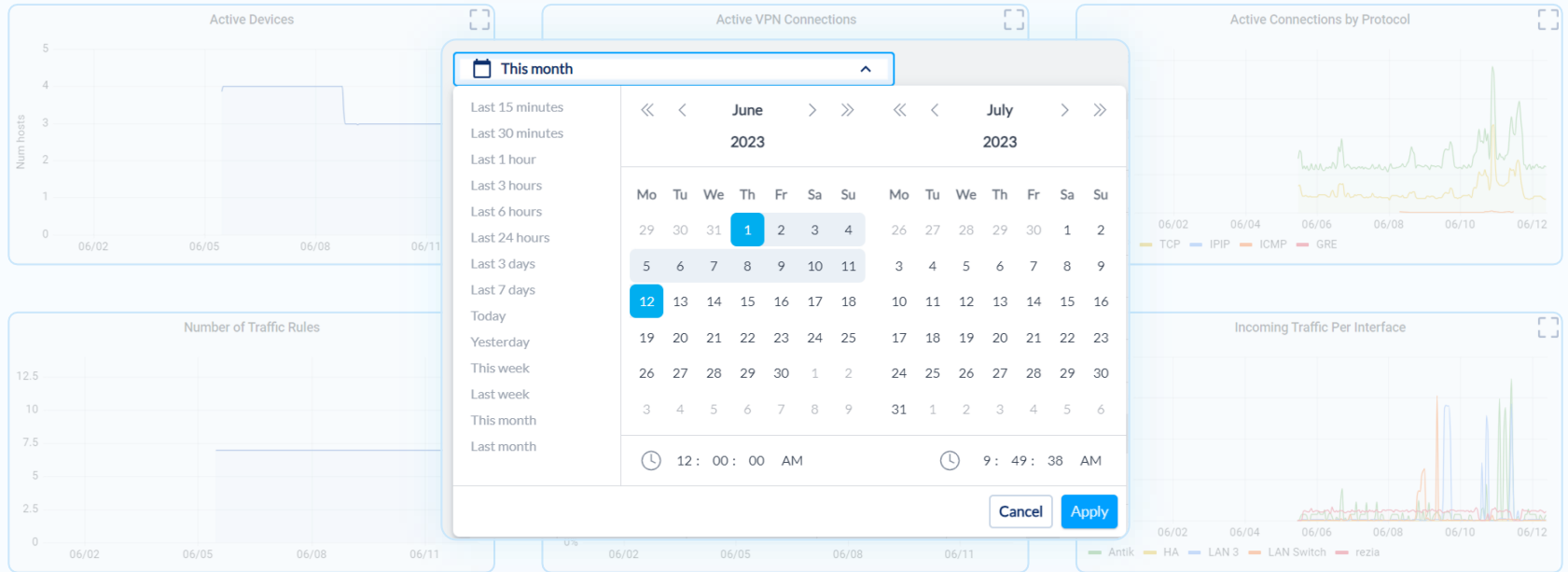
Alerts



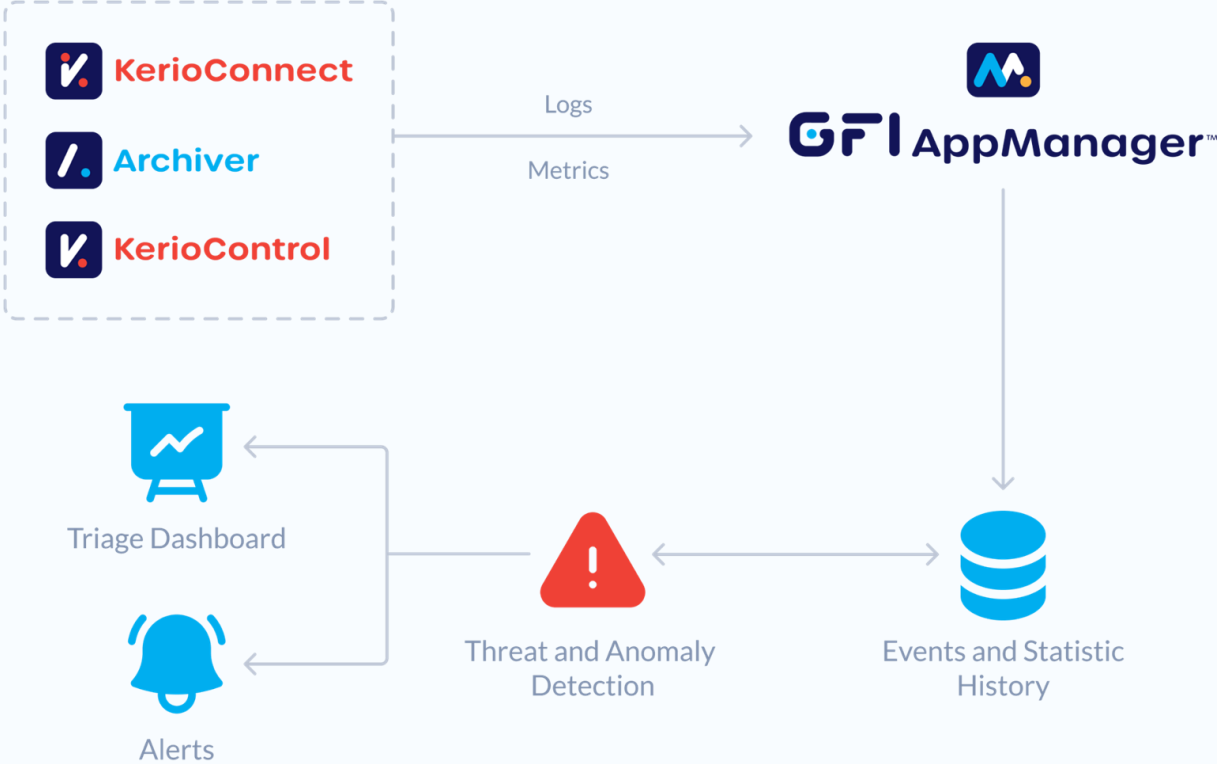
Monitoring



Monitoring



RADAR™



Thank you for listening!

Q & A

GFI Software™

gfi.com



Thank you!

GFI Software™

gfi.co
m

