



Continuous audit and management with GFI



Jozef Kacala
VP of Sales Engineering

Datacenter challenges

Background:

Datacenters are housing numerous servers/hosts/VMs. This is the backbone infrastructure storing critical data or running business applications.

Common challenges:

- Application performance
- Track and fix vulnerabilities
- Certification/auditing
- Missing patches recognition and deployment

Why ?

Multiple applications with different priorities

Dynamic (snapshot revert, HW changes etc.)

Multiple OS & devices types

Limited bandwidth

Application performance strugle

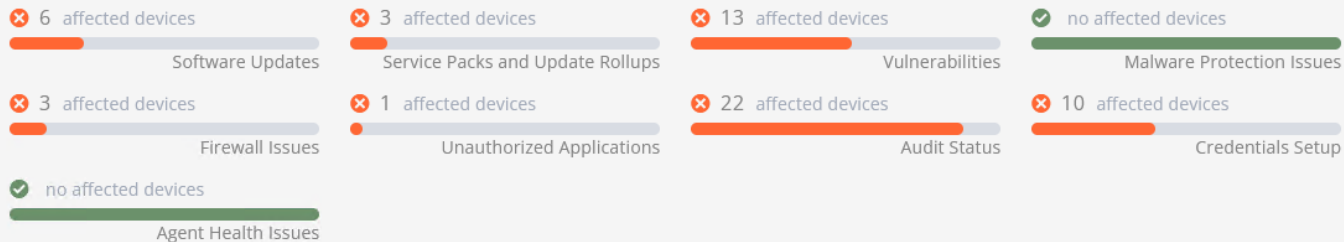
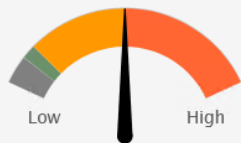


“ Regular scans done by GFI LanGuard is helping customers to track changes and recognize vulnerabilities and missing patches



LanGuard

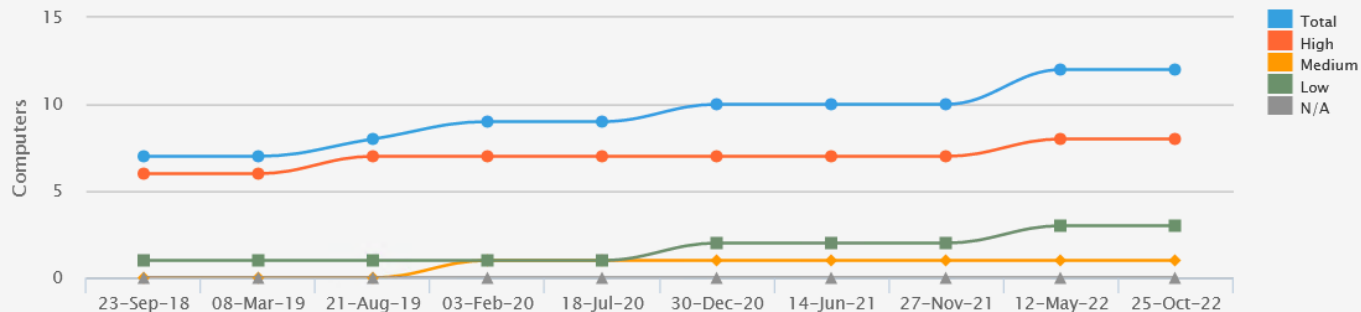
Vulnerability Level



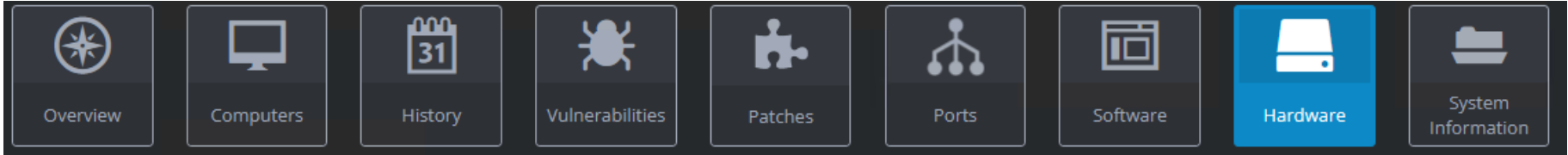
Most vulnerable computers










WIN-NQCL3B2QND7	High
KACALA-LAPTOP	High
ADMINISTRATOR-V	High
DARTHVADER-PC	High
JULINKA	High
HOST	High
MEDIASTATION-PC	Medium
10.10.10.16	Medium

Vulnerability Trend Over Time



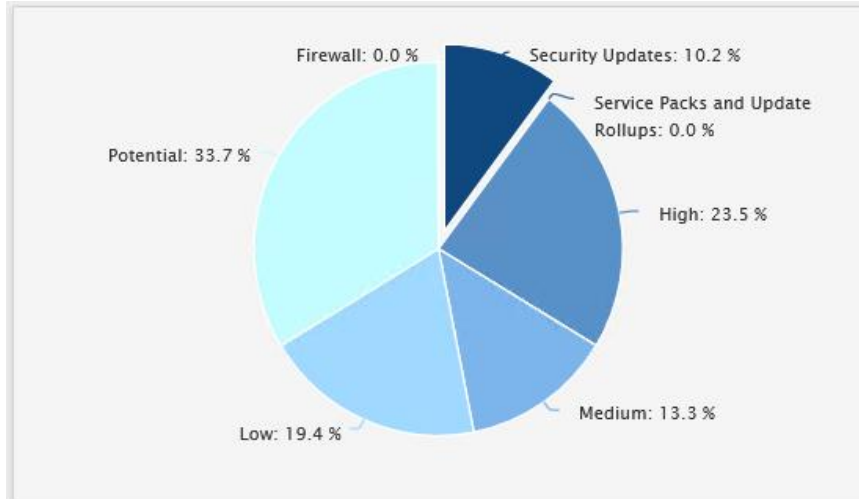
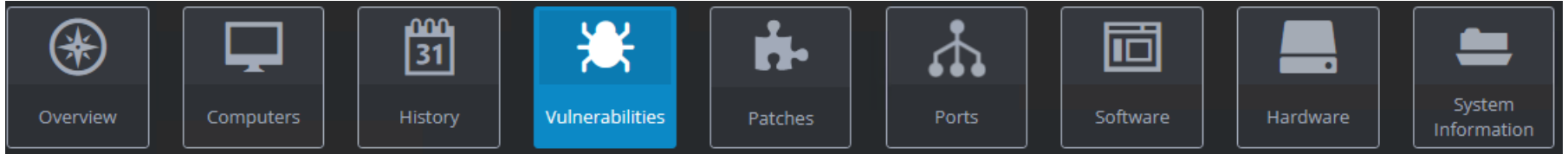
HW Changes



	Network Devices	54
	USB Devices	15
	Processors	4
	Storage Devices	15
	Display Adapters	7
	Motherboards	6
	Other Devices	91
	Local Drives	14
	Memory	5

- Discover
- Track
- Report
- Keep history

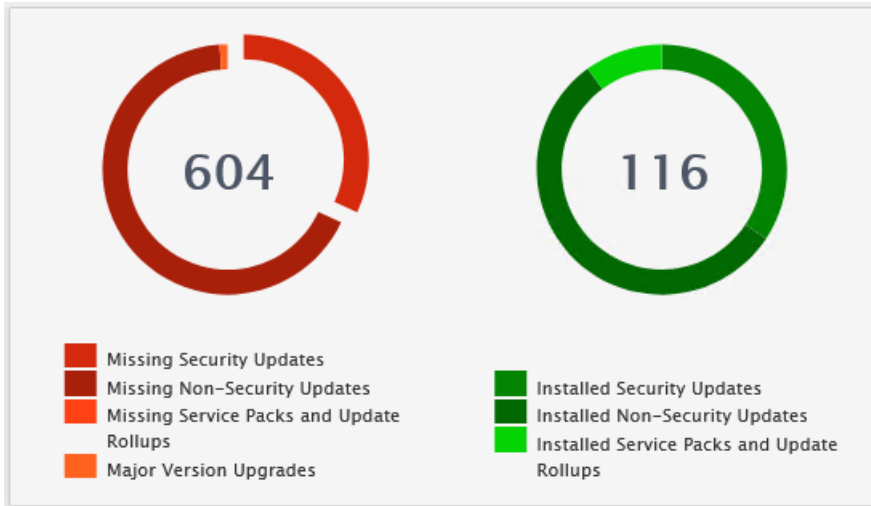
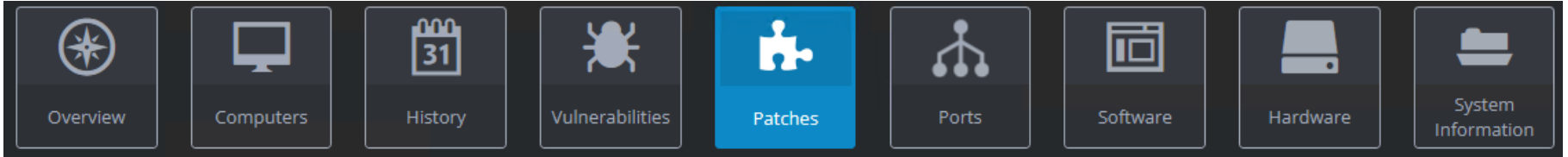
Vulnerabilities



Detects vulnerabilities of:

- Mac OS
- Linux
- Windows
- 3rd party apps
- Devices

Missing & deployed patches



Manage patches:

- Mac OS
- Linux
- Windows
- 3rd party apps



GENERAL REPORTS

View, print and schedule general reports



COMPLIANCE REPORTS

Run dedicated reports for different compliance regulations



PCI DSS



CIPA



HIPAA



ISO/IEC 27001 & 27002



SOX



FISMA



GLBA



CAG



PSNCoCo



NERC CIP



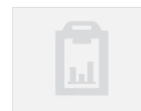
FERPA

Services



Lists all services found during an audit. The result is grouped by computer name.

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.

Vulnerability Status



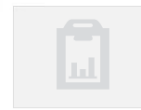
Shows statistical information related to the vulnerabilities detected on target computers. Vulnerabilities can be grouped by computer name, vulnerability severity, timestamp and category.

Baseline Comparison



Enables you to compare the results of all scanned machines to a base computer. The result is grouped by computer name and amongst others includes information on registry, installed service packs,...

Network Security History



Shows the changes done on target computers between audits. Amongst others, the report includes changes related to the vulnerability level, user accounts, groups, ports, shares and registry...

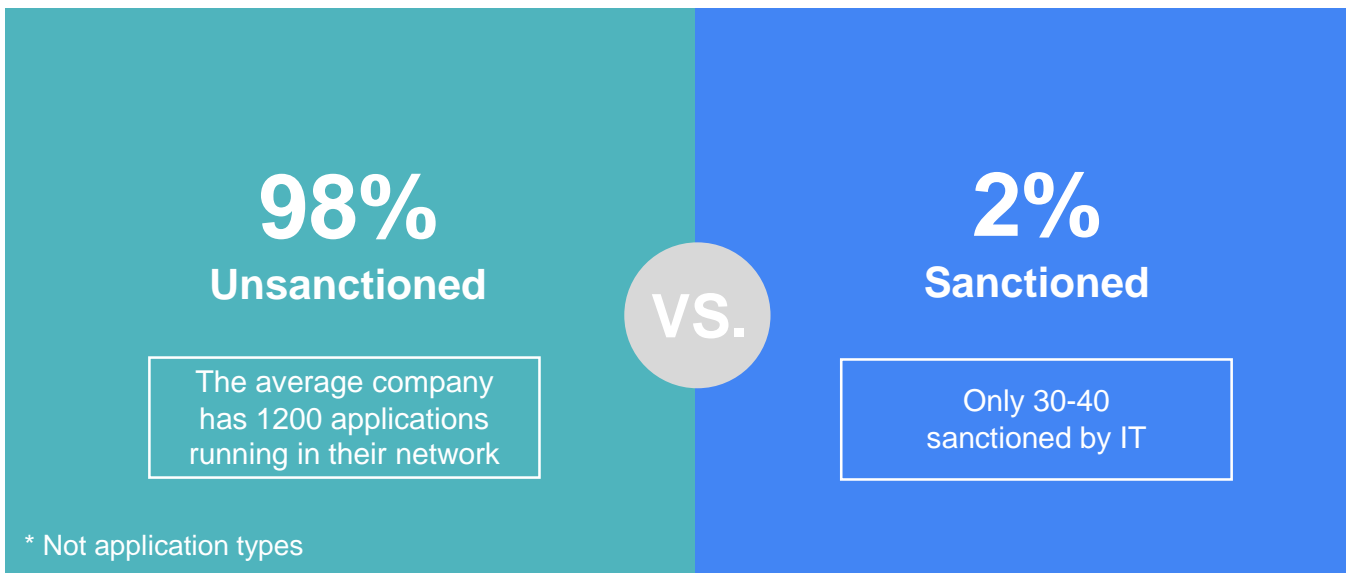


LOADING...

Bandwidth is not infinite



Exinda NetworkOrchestrator



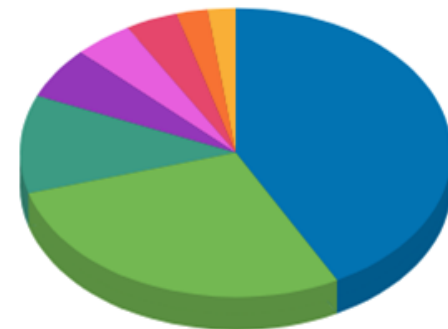
The evolution of applications



Full visibility and traffic control is the key to use all available resources to deliver peak performance of business critical assets.

Exinda helps recognizing the issue

Top 8 Outbound Application Groups



Recreational - How much recreational usage is there?

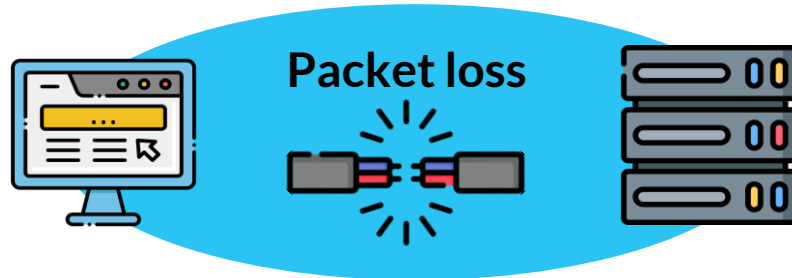
[More details](#) ? x

Application	Hosts	Time	Data
	452	7h 44m 30s	1616MB
Games	1	30s	0MB
Instant Messaging	0	0s	0MB
P2P	407	4h 49m 40s	291MB
Social Networking	38	1h 58m	1284MB
Streaming	9	56m 20s	40MB

APS Scores

Name	Score	Normalized Delays (ms/kb)		Transaction Delays (ms)		Jitter (ms)	Loss (%)		RTT (ms)
		Network	Server	Network	Server		Inbound	Outbound	
✓ SMTP Solution Center (235)	9.85	192.76	68.39	17385.98	179.12	3533.05	1.00	0.10	453.52
✓ Version One Solution Center (1000)	9.30	23.02	2.75	122.22	28.50	85.33	3.50	0.00	75.04
✓ HTTP Solution Center (201)	9.05	52.23	465.74	107.79	860.15	295.47	0.30	0.00	86.62
✓ SalesForce Solution Center (521)	8.34	66.64	27.69	161.45	113.59	67.24	0.00	0.00	88.06
✓ Apple Updates Solution Center (557)	7.93	8.89	158.74	6.74	133.72	0.00	0.00	0.00	10.79
✓ Spotify Solution Center (563)	7.71	73806.39	22178.18	6215.60	6627.60	1002.93	0.00	0.10	92.46
✓ SIP-SSL Solution Center (413)	7.15	40288.89	23918.97	92610.30	18426.43	46741.49	0.00	0.20	125.29
✓ Skype Solution Center (222)	6.83	114005.11	2014556.28	8604.32	21035.35	6742.88	0.00	0.00	104.08
✓ GMail Solution Center (618)	6.77	39376.86	209.09	49604.26	113.55	41094.88	0.60	0.00	134.52

Finding the root cause





Exinda NetworkOrchestrator



Available BW
100 Mb

VC #1

VC #2

VC #3

VC #,n"

10 Mb

Policy #1

Policy #2

Policy #3

Policy # „n"

Guaranteed

2 Mb

Burst

10 Mb

VLAN	Source	Direction	Destination	ToS/DSCP	Application
VLAN 2 ▾	Inside sales ▾	Both ▾	ALL ▾	ALL ▾	Skype Video ▾
VLAN 2 ▾	Inside sales ▾	Both ▾	ALL ▾	ALL ▾	Skype Voice ▾

Summary

Application performance.



Track and fix vulnerabilities.



Certification and auditing



Missing patches recognition and deployment



Exinda
Network Orchestrator



LanGuard

Thank you!

GFI Software™

www.gfi.com

Thank you for listening!

Q & A



GFI Software™

www.gfi.com