



# Executive Summary Report

Scan Performed On  
05/16/2022

# Executive Summary

Asset Summary	
No. of Assets discovered	95
Vulnerability Summary	
No. of Vulnerable Assets	11
Active Directory Summary	
Enabled Computers	43
Disabled Computers	2
Computers Not Logged In 30 Days	39
Total Computers	45
Enabled Users	103
Disabled Users	28
Users Not Logged In 30 Days	36
Users with Non-Expiring Password	44
Users with Expired Password	57
Locked Out Users	1
Users with Passwords Expiring Soon	0
Total Users	131
Linked GPO's	3
Unlinked GPO's	1
Total GPO's	18
Empty Groups	112
Non-Empty Groups	58
Total Groups	170

## Company Grade



## What is a security risk assessment?

A security risk assessment identifies, assesses, and implements key security controls in applications. It also focuses on preventing application security defects and vulnerabilities.

Carrying out a risk assessment allows an organization to view the application portfolio holistically—from an attacker’s perspective. It supports managers in making informed resource allocation, tooling, and security control implementation decisions. Thus, conducting an assessment is an integral part of an organization’s risk management process.

## How does a security risk assessment work?

The 4 steps of a successful security risk assessment model:

1. **Identification:** Discovery of assets and diagnose sensitive data that is created, stored, or transmitted by these assets. Create a risk profile for each.
2. **Assessment:** Careful evaluation and assessment, determine how to effectively and efficiently allocate time and resources towards risk mitigation.
3. **Mitigation:** Define a mitigation approach and enforce security controls for each risk.
4. **Prevention:** Implement tools and processes to minimize threats and vulnerabilities from occurring in your firm’s resources.

## Asset Summary

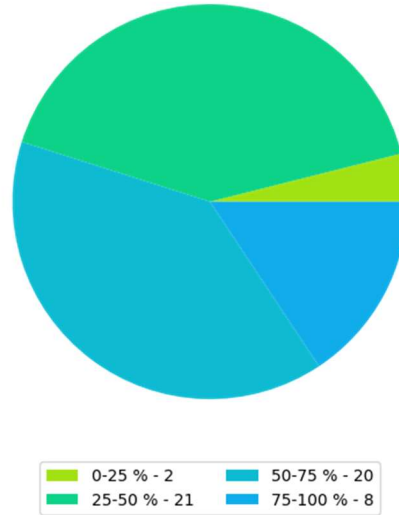
NIST requires as part of the cybersecurity framework that the system helps in identifying assets across the enterprise and keeping track of their status and configurations, including hardware and software. This comprises two large technical issues:

1. Tracking a diverse set of hardware and software. Examples of hardware include servers, workstations, and network devices. Examples of software include operating systems, applications, and files.

Lack of total control by the host organization. Financial services sector organizations can include subsidiaries, branches, third-party partners, contractors, temporary workers, and guests. It is impossible to regulate and mandate a single hardware and software baseline against such a diverse group.

# Your Asset Assessment

Disk Usage



# Operating System Breakdown

Sl. No.	Operating System	Asset Count
1	windows	14
2	linux based os	9
3	linux_kernel	8
4	mac_os_x	4
5	Mac OS X	2
6	Ubuntu	2
7	Windows Server 2012 R2	2
8	Brother NC-8200h	1

Sl. No.	Operating System	Asset Count
9	FortiGate	1
10	MacOS Big Sur	1
11	MacOS Catalina	1
12	MacOS High Sierra	1
13	Meraki	1
14	Windows Server 2012 R2 Standard Evaluation 9600	1
15	Windows Server 2016	1

Generic Operating Systems marked as Windows, linux\_kernel, etc. indicate that the OS was detected but the precise version was not found.

## The three dangers of unsupported operating systems:

### 1. No Security Patches:

This is the biggest problem when running an unsupported operating system. Once your software stops being supported, the updates and security patches stop, which means you've handed over the system's keys to an army of potential hackers.

### 2. Third-Party Software Outgrows Your Systems:

Part of a good vendor-management strategy is choosing the right software for your business. Most software vendors don't support outdated operating systems, since there is little profit in doing so. In addition, if you continue to use an outdated operating system, you risk losing the ability to run third-party software.

### 3. The Risk of Losing Customer Data:

Unsupported operating systems are giant holes in your security, which put not only your data at risk, but your customers' data too.



## Vendor Asset Count

Sl. No.	Vendor	Asset Count
1	Apple, Inc.	28
2	VMware, Inc.	17
3	Raspberry Pi Trading Ltd	2
4	Xiaomi Communications Co Ltd	2
5	AEWIN Technologies Co., Ltd.	1
6	Amazon Technologies Inc.	1
7	AzureWave Technology Inc.	1
8	Brother industries, LTD.	1
9	Dell Inc.	1
10	Tp-Link Technologies Co.,Ltd.	1
11	Ubiquiti Networks Inc.	1

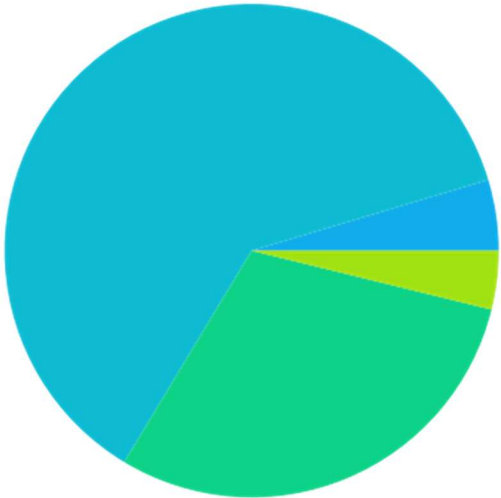
# Endpoint Assessment

## Network Scan Assessment

Sl. No.	Vulnerability	Count	Severity
1	MacOS Multiple Vulnerabilities (HT212011)	51	HIGH
2	MacOS Multiple Vulnerabilities (HT212147)	47	HIGH
3	MacOS Multiple Vulnerabilities (HT212530)	34	HIGH
4	MacOS Multiple Vulnerabilities (HT212981)	34	HIGH
5	MacOS Multiple Vulnerabilities (HT212871)	29	HIGH
6	MacOS Multiple Vulnerabilities (HT212326)	24	HIGH
7	MacOS Multiple Vulnerabilities (HT212600)	23	HIGH
8	MacOS Multiple Vulnerabilities (HT212805)	16	HIGH
9	MacOS Multiple Vulnerabilities (HT212872)	5	HIGH
10	Ubuntu Security Notification (USN-4013-1)	5	HIGH
11	CVE-2021-23017	4	CRITICAL
12	MacOS Multiple Vulnerabilities (HT212177)	3	HIGH
13	Ubuntu Security Notification (USN-4199-1)	2	HIGH
14	FortiClient (Windows) - privilege escalation in online installer due to incorrect working directory	1	HIGH
15	FortiClient Windows Service or Process Tampering	1	HIGH
16	FortiClient installer DLL Hijacking Vulnerability	1	HIGH
17	FortiClientEMS FortiClient - Telemetry protocol is vulnerable to a MitM Vulnerability	1	HIGH
18	FortiClientWindows FortiClient EMS - Privilege escalation via DLL Hijacking	1	HIGH
19	MacOS Multiple Vulnerabilities (HT210919)	1	HIGH
20	MacOS Multiple Vulnerabilities (HT211849)	1	HIGH
21	The VLC media player prior to 3.0.12 has Multiple vulnerabilities	1	HIGH
22	Ubuntu Security Notification (USN-3434-1)	1	CRITICAL
23	Ubuntu Security Notification (USN-4012-1)	1	CRITICAL
24	Ubuntu Security Notification (USN-4274-1)	1	HIGH
25	Ubuntu Security Notification (USN-4341-1)	1	HIGH



### Overall Vulnerability Summary



CRITICAL - 64	MEDIUM - 411
HIGH - 852	LOW - 53

## Vulnerability Summary By OS

SL. NO.	OS	Critical	High	Medium	Low
1	Windows Server 2012 R2	12	217	79	3
2	MacOS Catalina	9	223	102	5
3	Windows Server 2016	6	123	48	2
4	MacOS Big Sur	0	36	26	30
5	Microsoft Edge	0	15	8	0
6	Google Chrome	1	19	6	1
7	UltraVNC 1.0.5	15	7	1	0
8	Microsoft OneDrive	0	6	1	0
9	libsmbclient	1	10	10	0
10	libwbclient0	1	10	10	0
11	samba-libs	1	10	10	0
12	libsndfile1	1	5	5	0
13	krb5-locales	2	0	7	1
14	libelf1	1	0	9	0
15	libgssapi-krb5-2	2	0	7	1
16	libk5crypto3	2	0	7	1
17	libkrb5-3	2	0	7	1
18	libkrb5support0	2	0	7	1
19	libopenjp2-7	0	4	6	0
20	Go Programming Language amd64 go1.17.5	1	5	2	0
21	FortiClient	0	5	2	0
22	TeamViewer 11	1	3	0	1
23	VLC media player	0	5	0	0
24	WinSCP	1	1	3	0
25	libvpx6	0	3	2	0
26	klibc-utils	3	1	0	0
27	libklibc	3	1	0	0

SL. NO.	OS	Critical	High	Medium	Low
28	libncurses6	0	1	3	0
29	libncursesw6	0	1	3	0
30	libpcre3	0	2	2	0
31	ncurses-base	0	1	3	0
32	ncurses-bin	0	1	3	0
33	ncurses-term	0	1	3	0
34	AnyDesk	0	1	0	0
35	libcairo-gobject2	0	2	1	0
36	libcairo2	0	2	1	0
37	libtinfo6	0	0	3	0
38	libvorbis0a	0	3	0	0
39	libvorbisenc2	0	3	0	0
40	libvorbisfile3	0	3	0	0
41	Microsoft Teams - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com	0	2	0	0
42	Mozilla Firefox	0	0	1	0
43	libqt5core5a	0	1	1	0
44	libqt5dbus5	0	1	1	0
45	libqt5gui5	0	1	1	0
46	libqt5network5	0	1	1	0
47	libqt5printsupport5	0	1	1	0
48	libqt5widgets5	0	1	1	0
49	libtiff5	0	0	2	0
50	libxml2	0	2	0	0
51	python3-httplib2	0	1	1	0
52	python3-yaml	2	0	0	0
53	qt5-gtk-platformtheme	0	1	1	0
54	redis-server	0	1	1	0
55	redis-tools	0	1	1	0
56	tar	0	0	2	0
57	LibreOffice 6.4.7.2	0	0	1	0

SL. NO.	OS	Critical	High	Medium	Low
58	Mozilla Firefox ESR (x86 en-US)	0	0	1	0
59	PuTTY release 0.75 (64-bit)	0	1	0	0
60	Putty	0	1	0	0
61	bash	0	1	0	0
62	binutils	0	0	1	0
63	binutils-common	0	0	1	0
64	binutils-x86-64-linux-gnu	0	0	1	0
65	bluez	0	0	1	0
66	cracklib-runtime	0	1	0	0
67	dnsmasq-base	0	1	0	0
68	gdm3	0	0	1	0
69	gir1.2-gdm-1.0	0	0	1	0
70	gir1.2-polkit-1.0	0	0	0	1
71	gir1.2-rsvg-2.0	0	1	0	0
72	git	0	1	0	0
73	git-man	0	1	0	0
74	gnome-keyring	0	1	0	0
75	gnome-keyring-pkcs11	0	1	0	0
76	libbinutils	0	0	1	0
77	libcrack2	0	1	0	0
78	libcups2	0	0	1	0
79	libfl2	1	0	0	0
80	libgd3	0	0	1	0
81	libgdm1	0	0	1	0
82	libglib2.0-0	0	0	1	0
83	libglib2.0-bin	0	0	1	0
84	libglib2.0-data	0	0	1	0
85	libgraphite2-3	0	1	0	0
86	libidn11	1	0	0	0
87	libjpeg-turbo8	0	1	0	0

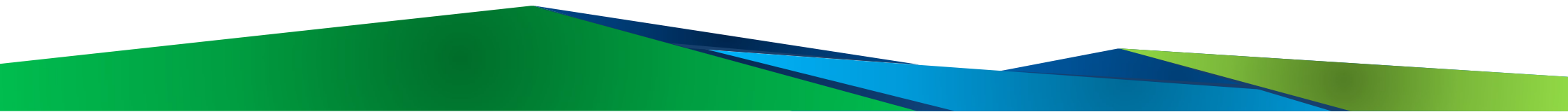
SL. NO.	OS	Critical	High	Medium	Low
88	liblz4-1	0	1	0	0
89	libmailutils6	0	1	0	0
90	libnss-systemd	0	0	1	0
91	libpam-gnome-keyring	0	1	0	0
92	libpam-systemd	0	0	1	0
93	libpolkit-agent-1-0	0	0	0	1
94	libpolkit-gobject-1-0	0	0	0	1
95	libprotobuf17	0	1	0	0
96	libpython3.9	0	0	1	0
97	libpython3.9-minimal	0	0	1	0
98	libpython3.9-stdlib	0	0	1	0
99	librsvg2-2	0	1	0	0
100	librsvg2-common	0	1	0	0
101	libsqlite3-0	0	1	0	0
102	libssl1.1	0	0	1	0
103	libsystemd0	0	0	1	0
104	libtag1v5	0	0	1	0
105	libtag1v5-vanilla	0	0	1	0
106	libudisks2-0	0	0	1	0
107	libwebp6	0	0	0	1
108	libwebpdemux2	0	0	0	1
109	libwebpmux3	0	0	0	1
110	libwmf0.2-7	0	0	1	0
111	lz4	0	1	0	0
112	mailutils	0	1	0	0
113	mailutils-common	0	1	0	0
114	openssl	0	0	1	0
115	policykit-1	0	0	0	1
116	python3-jinja2	0	0	1	0
117	python3-protobuf	0	1	0	0

SL. NO.	OS	Critical	High	Medium	Low
118	python3.9	0	0	1	0
119	python3.9-minimal	0	0	1	0
120	sudo	0	1	0	0
121	sysstat	0	0	1	0
122	systemd	0	0	1	0
123	systemd-sysv	0	0	1	0
124	systemd-timesyncd	0	0	1	0

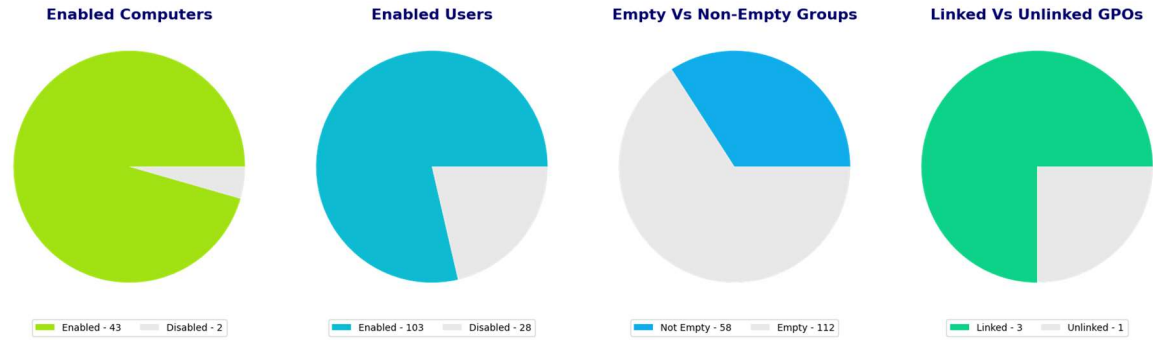




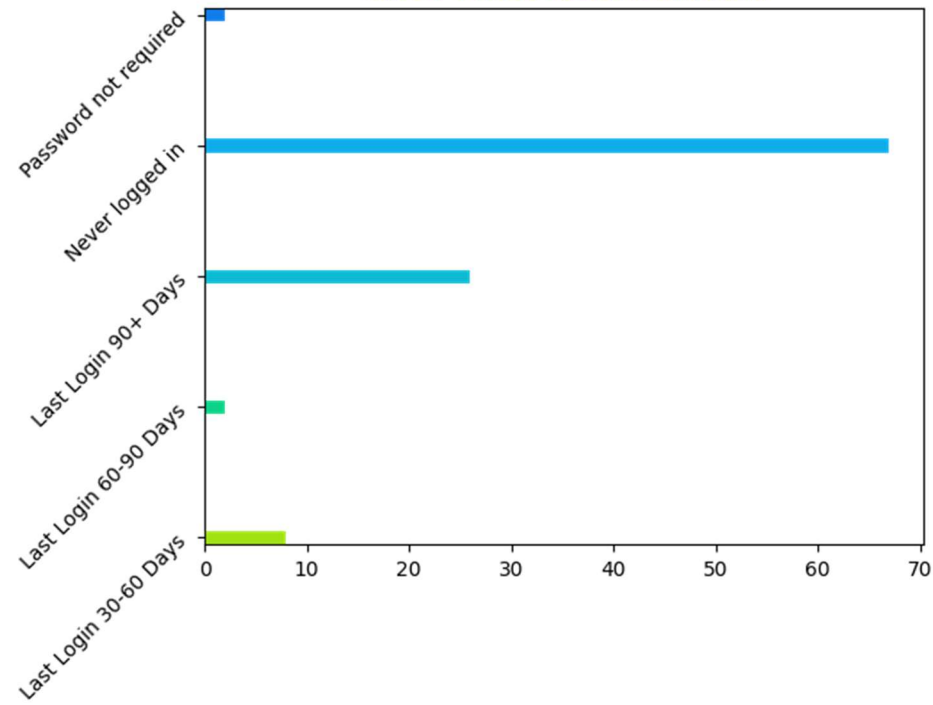
The latest SANS endpoint security survey highlights the importance of implementing a comprehensive endpoint protection solution. Some of the key findings from this survey include:

1. 28% of respondents reported that their endpoints had been breached.
  2. A variety of threat vectors were used, including web drive-by (52%), social engineering/phishing (58%), and/or credential theft/compromise (49%).
  3. Only 39% of attacks were detected by traditional antivirus.
  4. Another 39% of compromises were detected by SIEM alerts.
- 

# Active Directory Assessment



## User Risk Assessment



## Active Directory Best Practices for User Accounts



Understand Permission Inheritance



Change Default Setting



Use Remote Management Tools



Standardize Group Names



Clear Unnecessary Accounts



Use Monitoring Tools for Security



Keep Privileges at a Minimum



Implement Password Policies



Have a Disaster Recovery Plan

With thousands of user accounts to manage, it's easy to get overwhelmed. The best way to avoid headaches is to be proactive. If you can take steps to ensure a healthy Active Directory, your chances of a security breach drop significantly. Here are a few AD user management best practices to keep in mind:

- **Perform Housekeeping Duties:** Regularly deleting unnecessary user accounts from your Domain Admins group is critical. Why? Members of this group are granted access to a plethora of devices and servers. This makes them a prime target for attackers, who have become experts at breaking into user credentials. Keep the number of users within your Domain Admins group to a bare minimum to safeguard against this possibility.
- **Keep Track of Terminations:** When employees leave, so must their user accounts. Abandoned accounts leave room for former employees to gain access to information that is not rightfully theirs. They're also a target for hackers, who prey on inactive accounts as an easy way to enter a domain under cover. Do your due diligence and regularly sweep out abandoned accounts. You won't regret it.

- **Actively Monitor:** It's important to have an overview of your forests. This ensures you stay ahead of potential problems, like service outages, and quickly identify those that do pop up, such as syncing issues and user account lockouts. Practice monitoring for a spike in bad user account password attempts. This is often a red flag that you have attackers on your hands.
- **Implement Passwords Policies:** It would be great if AD were configured to require users to update passwords on a periodic basis. Unfortunately, that's not the case. But while it may involve some manual heavy lifting, it's important to set up processes that require regular password updates. This preventative measure is well worth the time. A few tips:
  - Long passwords are king. Think 12 characters at least.
  - Implement paraphrases, that is, two or more unrelated words strung together.
  - Allow just three login attempts before the user is locked out.