STRATADEFENSE

Network Security Focused. Customer Driven.

Executive Summary Report

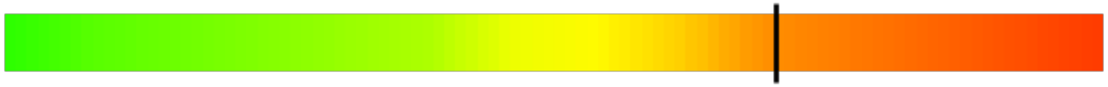
Prepared For

Your Organization Name

Executive Summary

Asset Summary	
No. of Assets discovered	29
Vulnerability Summary	
No. of Vulnerable Assets	14
Active Directory Summary	
Enabled Computers	24
Disabled Computers	28
Computers Not Logged In 30 Days	24
Total Computers	52
Enabled Users	39
Disabled Users	11
Users Not Logged In 30 Days	30
Users with Non-Expiring Password	26
Users with Expired Password	0
Locked Out Users	0
Users with Passwords Expiring Soon	1
Total Users	50
Linked GPO’s	3
Unlinked GPO’s	0
Total GPO’s	0
Empty Groups	47
Non-Empty Groups	24
Total Groups	71

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.

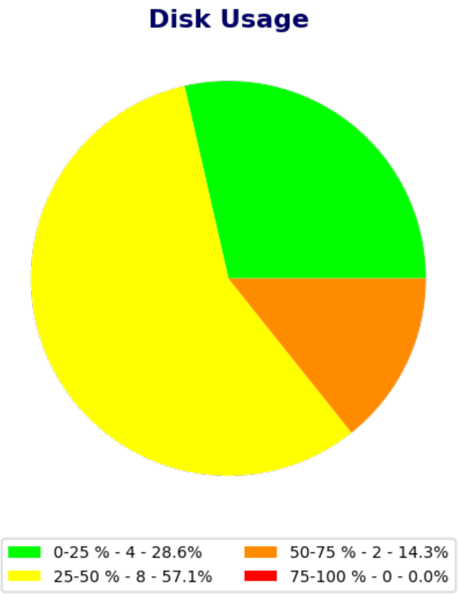
Asset Summary

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



Operating System Breakdown

Sl. No.	Operating System	Asset Count
1	Microsoft Windows 10 Pro	10
2	Microsoft Windows Server 2019 Standard	4

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	Hewlett Packard	7
2	Dell Inc.	6
3	Microsoft Corporation	6
4	Micro-Star INT'L CO., LTD	1

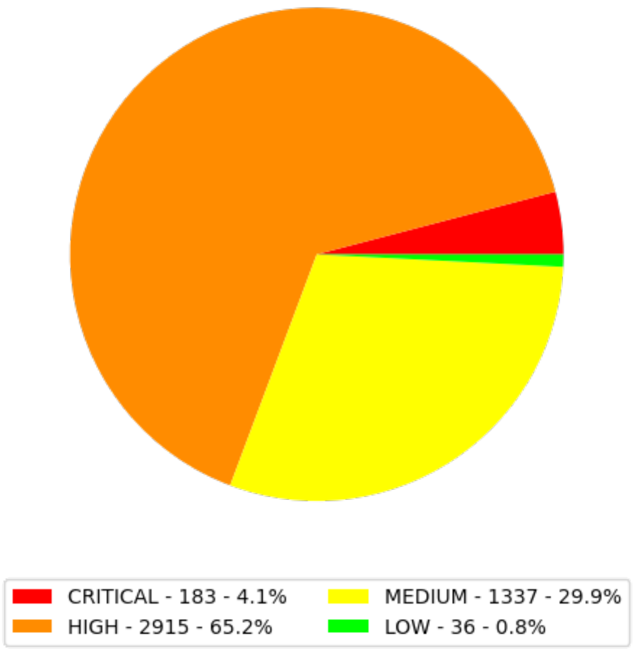
Endpoint Assessment

Network Scan Assessment

Sl. No.	Vulnerability	Count	Severity
1	Microsoft Office Visio Remote Code Execution Vulnerability	15	HIGH
2	Use after free in PDF in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: High)	12	HIGH
3	Use after free in PDF in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: High)	12	HIGH
4	Heap buffer overflow in WebUI in Google Chrome prior to 100.0.4896.60 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via specific input into DevTools.	8	HIGH
5	Out of bounds memory access in Service Worker API in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8	HIGH
6	Type Confusion in V8 in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8	HIGH
7	Type confusion in V8 in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8	HIGH
8	Type confusion in V8 in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8	HIGH
9	Use after free in ANGLE in Google Chrome prior to 99.0.4844.74 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8	HIGH
10	Use after free in Accessibility in Google Chrome prior to 98.0.4758.80 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via user interaction.	8	HIGH
11	Use after free in WebRTC in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8	HIGH
12	Use after free in WebSQL in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8	HIGH
13	Use after free in storage foundation in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8	HIGH
14	Type Confusion in V8 in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High)	6	HIGH
15	Type Confusion in V8 in Google Chrome prior to 91.0.4472.164 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	6	HIGH
16	Type confusion in V8 in Google Chrome prior to 92.0.4515.159 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	6	HIGH

Sl. No.	Vulnerability	Count	Severity
17	Use after free in DevTools in Google Chrome prior to 92.0.4515.107 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	6	HIGH
18	A user may be tricked into opening a malicious FBX file that may exploit a heap buffer overflow vulnerability in Autodesk® FBX® SDK 2020 or prior which may lead to code execution.	5	HIGH
19	Microsoft 365 Apps Vulnerability	5	HIGH
20	Microsoft Excel Remote Code Execution Vulnerability	5	HIGH
21	Microsoft Office Elevation of Privilege Vulnerability	5	CRITICAL
22	Microsoft Office Remote Code Execution Vulnerability	5	HIGH
23	Microsoft Outlook Information Disclosure Vulnerability	5	HIGH
24	Microsoft Outlook Remote Code Execution Vulnerability	5	HIGH
25	Microsoft Word Remote Code Execution Vulnerability	5	HIGH

Overall Vulnerability Summary



Vulnerability Summary

SL. NO.	Product	Critical	High	Medium	Low
1	Google Chrome	21	435	179	1
2	Windows Server 2019 Build 17763	25	407	145	4
3	Microsoft Edge	1	37	21	1
4	Windows 10 Build 19045	5	32	12	1
5	Windows 10 Build 19043	1	48	16	1
6	Cisco Webex Meetings	2	6	17	0
7	Zoom	3	13	7	0
8	Microsoft Office Home and Business 2019 - en-us	1	10	6	0
9	Microsoft 365 Apps for business - en-us	1	10	6	0
10	Java 8 Update 301	0	3	25	4
11	Java 8 Update 271	0	1	16	2
12	Microsoft .NET Host - 6.0.9 (x64)	0	17	1	0
13	Microsoft .NET Host FX Resolver - 6.0.9 (x64)	0	17	1	0
14	Microsoft .NET Runtime - 6.0.9 (x64)	0	17	1	0
15	Microsoft .NET Host - 6.0.14 (x64)	0	13	1	0
16	Microsoft .NET Host FX Resolver - 6.0.14 (x64)	0	13	1	0
17	Microsoft .NET Runtime - 6.0.14 (x64)	0	13	1	0
18	Intel(R) Rapid Storage Technology	0	4	0	0
19	Microsoft Teams	0	0	1	0
20	Microsoft .NET Host - 6.0.20 (x64)	0	4	1	0
21	Microsoft .NET Host FX Resolver - 6.0.20 (x64)	0	4	1	0
22	Microsoft .NET Runtime - 6.0.20 (x64)	0	4	1	0
23	Microsoft ODBC Driver 17 for SQL Server	0	2	0	0
24	Microsoft .NET Framework 4 Multi-Targeting Pack	0	1	0	0
25	Microsoft .NET Framework 4.5.1 Multi-Targeting Pack	0	1	0	0
26	Microsoft .NET Framework 4.5.1 Multi-Targeting Pack (ENU)	0	1	0	0
27	Microsoft .NET Framework 4.5.1 SDK	0	1	0	0

SL. NO.	Product	Critical	High	Medium	Low
28	Microsoft .NET Framework 4.5.2 Multi-Targeting Pack	0	1	0	0
29	Microsoft .NET Framework 4.5.2 Multi-Targeting Pack (ENU)	0	1	0	0
30	Microsoft SQL Server Management Studio - 17.9.1	0	0	1	0
31	Microsoft SQL Server Management Studio - 18.4	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:

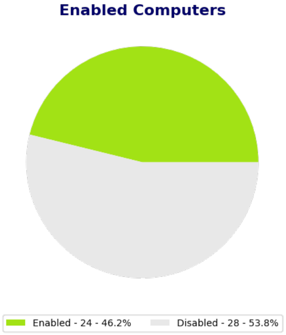
1. 28% of respondents reported that their endpoints had been breached.

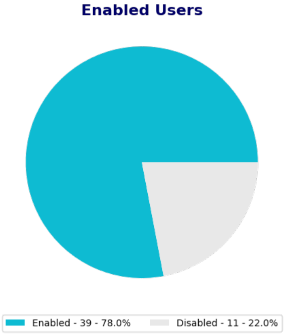
2. A variety of threat vectors were used, including web drive-by (52%), social engineering/phishing (58%), and/or credential theft/compromise (49%).

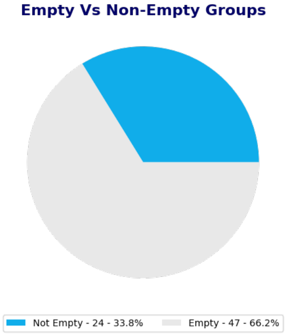
3. Only 39% of attacks were detected by traditional antivirus.

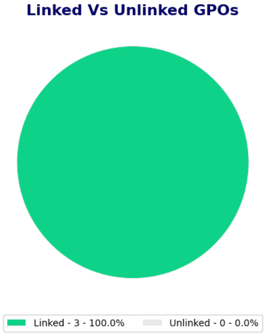
4. Another 39% of compromises were detected by SIEM alerts.

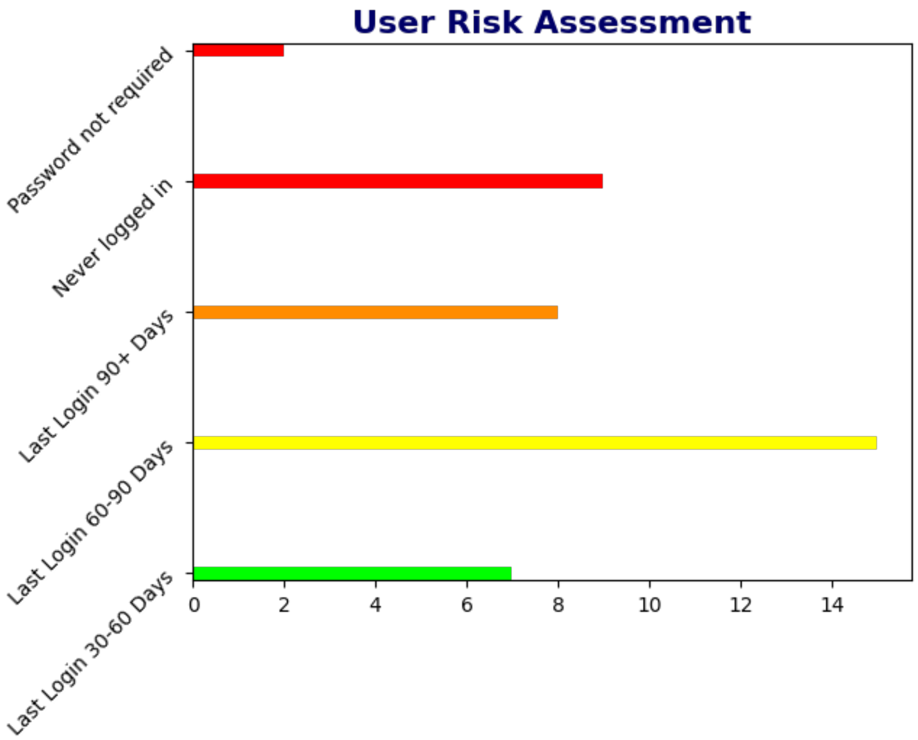
Active Directory Assessment


Enabled Computers

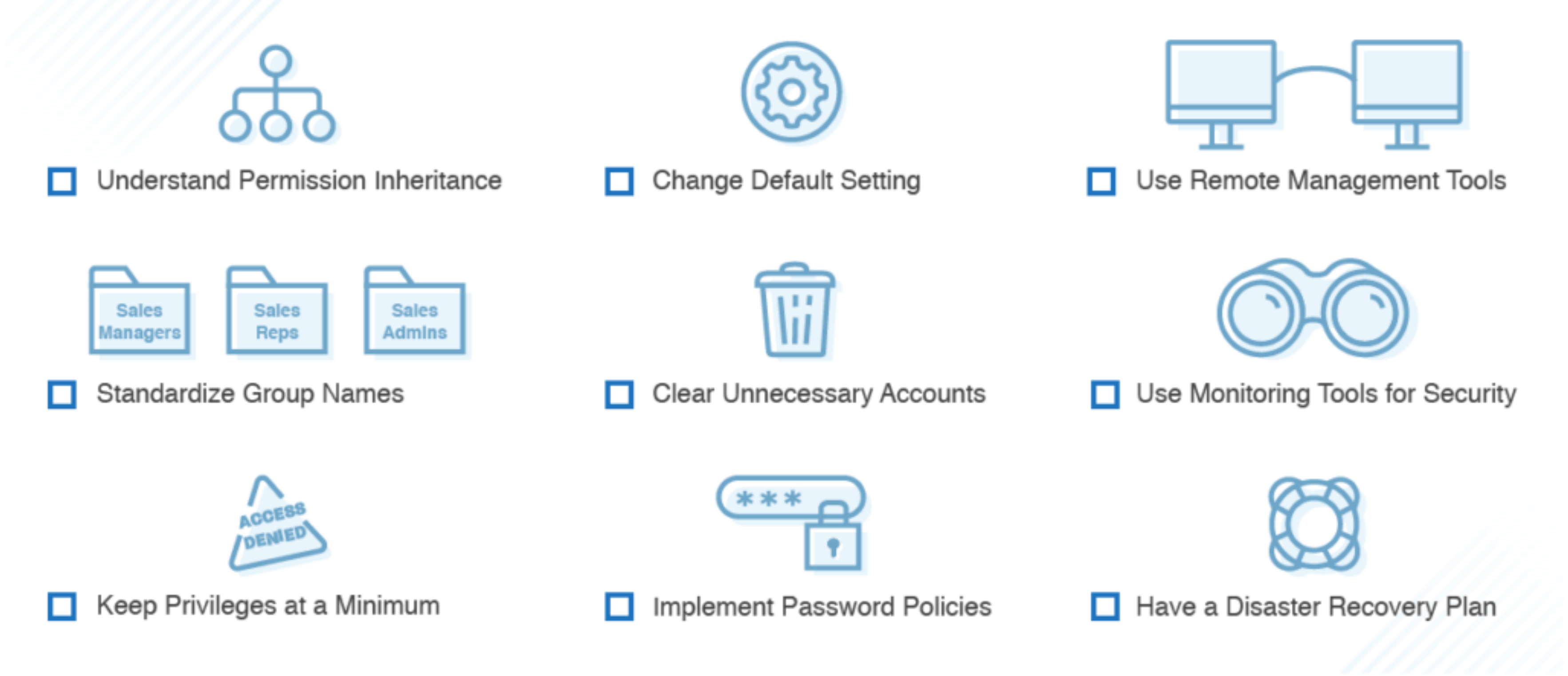

Enabled Users


Empty Vs Non-Empty Groups


Linked Vs Unlinked GPOs


User Risk Assessment

Active Directory Best Practices for User Accounts



□ Understand Permission Inheritance

□ Standardize Group Names

□ Keep Privileges at a Minimum

□ Change Default Setting

□ Clear Unnecessary Accounts

□ Implement Password Policies

□ Use Remote Management Tools

□ Use Monitoring Tools for Security

□ 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.

Your Microsoft Secure Score Summary

No Microsoft Secure Score