BLACK ROCK TECHNOLOGIES®

Network Vulnerability and Assessment Report

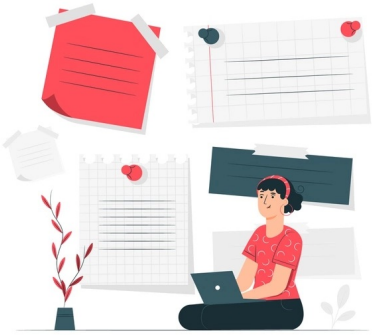
Prepared For

Scan Performed On: 01 Mar 2023

Executive Risk Summary

Asset Summary			
No. of Assets discovered	214	No. of Vulnerable Assets	49
Active Directory Summary			
Enabled Computers	462	Disabled Computers	2
Enabled Computers With Expired Passwords	0	Locked Out Enabled Computers	0
Enabled Computers - Never Logged In	2	Enabled Computers Not Logged in for 30 days	185
Enabled Computers - Password Never Expires	0	Enabled Computers - Password Expires	462
Enabled Computers - Password Not Required	3	Total Computers	464
Enabled Users	151	Disabled Users	48
Enabled Users With Expired Passwords	9	Locked Out Enabled Users	0
Enabled Users - Never Logged In	11	Enabled Users Not Logged in for 30 days	34
Enabled Users - Password Not Required	1	Total Users	199
Enabled Users - Password Never Expires	127	Enabled Users - Password Expires	24
Empty OUs	1	Non Empty OUs	23
Total OUs	46	Total GPOs	18
Empty Groups	152	Non Empty Groups	104
Privileged Access Groups	94	Total Groups	256

- 57 out of 214 assets with remote access enabled.
- 0 out of 214 assets missing advanced protection.
- 11 enabled users out of 199 users never logged in.
- 3 out of 53 storage devices with hard drive space utilized over 90% while 12 other storage devices with hard drive utilized over 75%
- 0 out of 214 assets with Antivirus not installed.



- 27 enabled users out of 199 users did not login for last 90 days.
- 41 out of 214 assets running end of life OS.
- 10 out of 53 storage devices with hard drive space utilized between 50-75%.
- 0 out of 214 assets with Antivirus installed but not up to date.

- 34 enabled users out of 199 users did not login for last 30 days.
- 16 out of 214 storage devices with hard drive space utilized between 25-50%.

- 49 out of 214 assets with basic Antivirus protection.
- 44 out of 214 assets with firewall protection.

Table of Content

Security Assessment

Assessment report for
provides visibility into specific weaknesses and deficiencies in the security controls employed within or inherited by the information system. Such weaknesses and deficiencies are potential vulnerabilities if exploitable by a threat source. The findings generated during the security control assessment provide important information that facilitates a disciplined and structured approach to mitigating risks in accordance with organizational priorities.

Risk Dashboard

The Consolidated Risk Report aggregates risk analysis from multiple assessments performed on the network, providing you with both a Consolidated Risk Score and a high-level overview of the health and security of the network. The report details the scan tasks undertaken to discover security issues. In addition to the overall Consolidated Risk Score, the report also presents separate impact scores for all area of assessments.

Vulnerability Assessment

A **vulnerability assessment** is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, and network infrastructures and providing the organization doing the assessment with the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately.

Critical

834 were unique critical severity vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems

834

High

12303 were unique high severity vulnerabilities. High severity vulnerabilities are easy to exploit and may provide access to affected systems.

12303

Medium

4469 were unique medium severity vulnerabilities. These vulnerabilities often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner but are not as urgent as the other vulnerabilities.

4469

Low

376 were unique low severity vulnerabilities. These should also be fixed in a timely manner but are not as urgent as the other vulnerabilities.

376

Risk Detected: High Risk Score

Top 5 Vulnerabilities

Vulnerability	Asset Count	Risk
Zoom clients before version 5.13.5 contain a STUN parsing vulnerability. A malicious actor could send specially crafted UDP traffic to a victim Zoom client to remotely cause the client to crash, causing a denial of service.	26	HIGH
Buffer Overflow vulnerability in tvnviewer.exe of TightVNC Viewer allows a remote attacker to execute arbitrary instructions via a crafted FramebufferUpdate packet from a VNC server.	17	CRITICAL
Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	8	HIGH
A background script invoking requestFullscreen and then blocking the main thread could force the browser into fullscreen mode indefinitely, resulting in potential user confusion or spoofing attacks.	7	HIGH
A lack of in app notification for entering fullscreen mode could have lead to a malicious website spoofing browser chrome.This bug only affects Firefox Focus. Other versions of Firefox are unaffected.	7	HIGH

Critical

Apply patches within 30 days of release

High

Apply patches within 30 - 60 days

Medium

Apply patches within 60 - 90 days

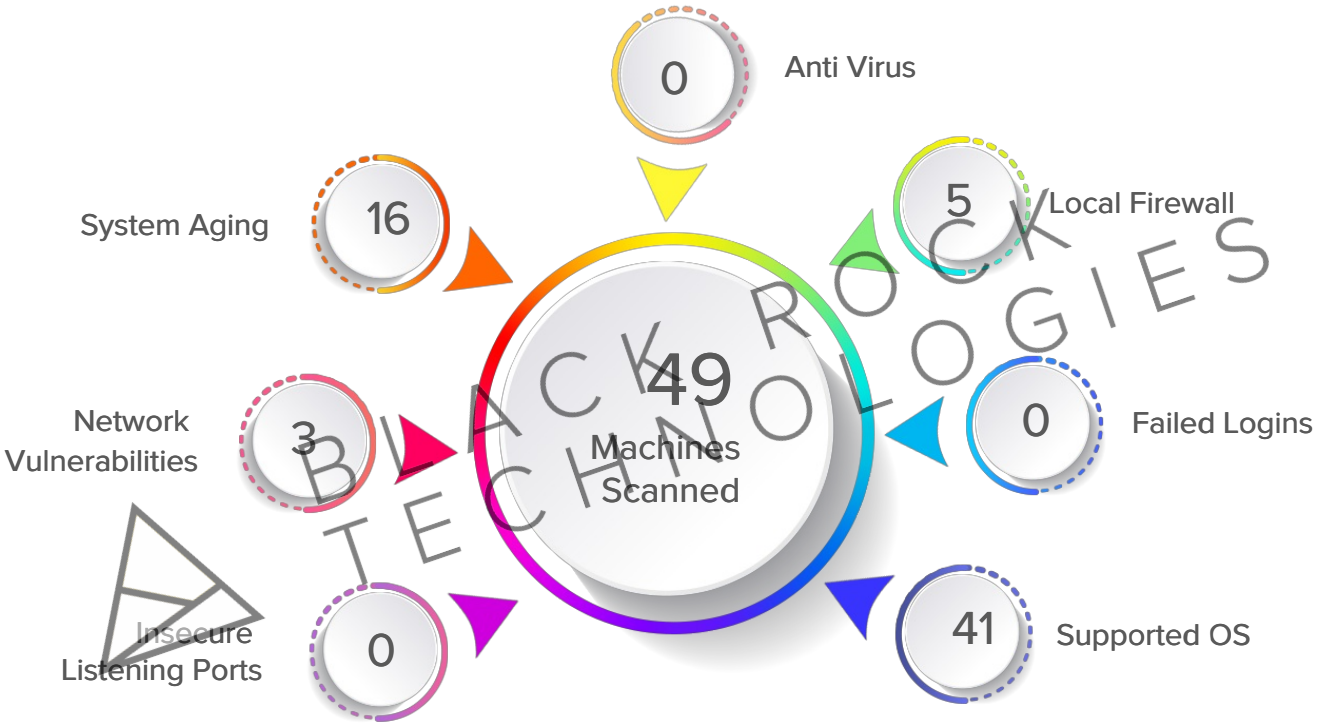
Low

Apply patches within 180 days

Endpoint Assessment

In today's time **end-users** have become a prime target for cyber criminals. But the real tangible target is the end-user's workstation, and organizations would be remiss not to regularly validate the security of their endpoints. To close the gap, we have developed an endpoint assessment methodology that accounts for each area of the attack. The identification of vulnerabilities and gaps in security controls that may have gone unnoticed will assist you in tuning detection or protective controls to handle user activities. Associated remediation efforts will enhance incident response capabilities and further strengthen your overall security posture.

Security Report Card



Anti Virus
0 assets with AntiVirus Not installed.

Local Firewall
5 assets with Local Firewall Disabled.

Supported OS
41 assets with Some OS not supported

Insecure Listening Ports
0 assets with More than one insecure listening port

Network Vulnerabilities
3 assets with CVSS greater than or equal to 9.0.

System Aging
16 Computers over 8 years old.

Failed Logins
0 or more failed logins in the last 7 days

Compliance Report Card

LLMNR
49 Assets with LLMNR Enabled.

NTLMV1
0 Assets with NTLMV1 Enabled.

NBTNS
49 Assets with NBTNS Enabled.

SMBV1 Server
0 Assets with SMBV1 Server Enabled.

SMBV1 Client
7 Assets with SMBV1 Client Enabled.

SMB Signing
47 Assets with SMB Signing Disabled.

Compliance Assessment

CIS

The Center for Internet Security (CIS) benchmarks are a set of best-practice cybersecurity standards for a range of IT systems and products. CIS Benchmarks provide the baseline configurations to ensure compliance with industry-agreed cybersecurity standards.

0	Compliant Assets
49	Non Compliant Assets
165	Not Applicable

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a security standard used to ensure the safe and secure transfer of credit card data.The regulations include security management provisions that cover policies, network architecture, software design and other critical safety measures.

0	Compliant Assets
49	Non Compliant Assets
165	Not Applicable

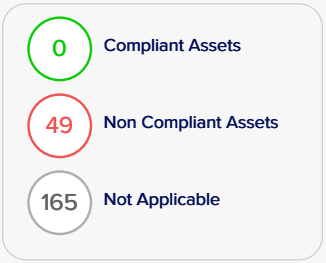
GDPR IV

General Data Protection Legislation(GDPR) is the legislative force established to protect the fundamental rights of data subjects whose personal information and sensitive data is stored in organisations.

0	Compliant Assets
49	Non Compliant Assets
165	Not Applicable

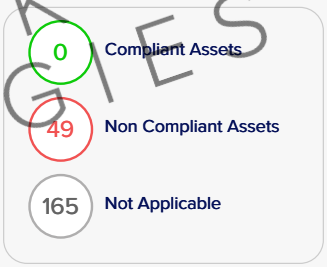
GPG 13

The Good Practice Guide 13 (GPG 13) is a protective monitoring framework. It provides a framework for treating risks to systems, collecting log information and configuring logs to provide an audit trail of security relevant events of interest.



NIST 800 53

National Institute of Standards and Technology (NIST) NIST SP 800-53 provides a list of controls that support the development of secure and resilient federal information systems. These controls are the operational, technical, and management standards and guidelines used by information systems to maintain confidentiality, integrity, and availability. The guidelines adopt a multi-tiered approach to risk management through control compliance.



HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.

0	Compliant Assets
49	Non Compliant Assets
165	Not Applicable

ISO 27002

International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) ISO/IEC 27002:gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

0	Compliant Assets
49	Non Compliant Assets
165	Not Applicable

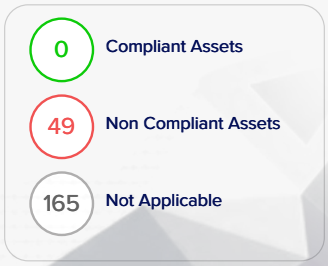
CIS 8 0

CIS Controls v8 has been enhanced to keep up with modern systems and software. Movement to cloud-based computing, virtualization, mobility, outsourcing, Work-from-Home, and changing attacker tactics prompted the update and supports an enterprise's security as they move to both fully cloud and hybrid environments.

0	Compliant Assets
49	Non Compliant Assets
165	Not Applicable

NIST 800 171

The National Institute of Standards and Technology (NIST) created Special Publication 800-171 to help protect Controlled Unclassified Information. NIST 800-171 standardizes how federal agencies define CUI: data that is private and sensitive but not classified per federal law.



Patch Assessment

Patch assessment is the process that helps acquire, test and install multiple patches on a computer, enabling systems to stay updated on existing patches and safeguards the IT environment from vulnerability and exploit.

Risk Detected

214 Assets Scanned

374 Patches Missing in 214 Assets

Impact Level High

Apply Patch to Stay Protected

229 Critical Missing Patches

Apply patches within 30 days of release

137 High Missing Patches

Apply patches within 30 - 60 day

137 Medium Missing Patches

Apply patches within 60 - 90 days

71 Low Missing Patches

Apply patches within 180 days

Top 5 Missing Patches

Vulnerability	CRITICAL	HIGH	Asset Count
Microsoft .NET Host - 5.0.17 (x64)	19	0	19
Microsoft .NET Host FX Resolver - 5.0.17 (x64)	19	0	19
Microsoft .NET Runtime - 5.0.17 (x64)	19	0	19
Microsoft Silverlight	0	19	19
Windows 10 Build 19043	6	257	18

Password Policy Summary

Policy	Setting	Domain
Enforce password history	3 passwords remembered	----.com
	3 passwords remembered	-----.com
Maximum Password Age	120 days	-------.com
	120 days	----------.com
Minimum Password Age	0 days	--------.com
	0 days	--------.com
Minimum Password Length	8 characters	-------.com
	8 characters	-------.com

Password history not remembered

Issue: Short password histories allow users to rotate through a known set of passwords, thus reducing the effectiveness of a good password management policy.

Recommendation: Increase password history to remember at least six passwords.

Maximum Password Age

Issue: Passwords that are not changed regularly are more vulnerable to attack and unauthorized use. Minimizing the allowed password age greatly reduces the window of time that a lost or stolen password poses a threat.

Recommendation: Modify the maximum password age to be 90 days or less.

Password length less than 8 characters

Issue: Passwords are not required to be 8 or more characters, allowing users to pick extremely short passwords which are vulnerable to brute force attacks.

Recommendation: Enable enforcement of password length to more than 8 characters.

Inconsistent password policy

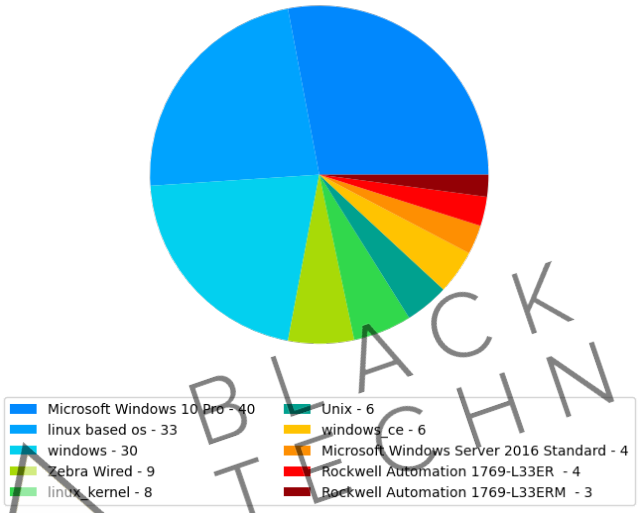
Issue: Password policies are not consistently applied from one computer to the next. A consistently applied password policy ensures adherence to password practices.

Recommendation: Eliminate inconsistencies and exceptions to the password policy.

IT Infrastructure Assessment

Asset discovery is simply the process of discovering and collecting data on the technology assets connected to a network for management and tracking purposes

Assets - Operating System



Risk Detected

214 Assets Scanned

3 STORAGE DEVICES WITH DISK SPACE UTILIZED OVER 90%

12 STORAGE DEVICES WITH DISK SPACE UTILIZED OVER 75%

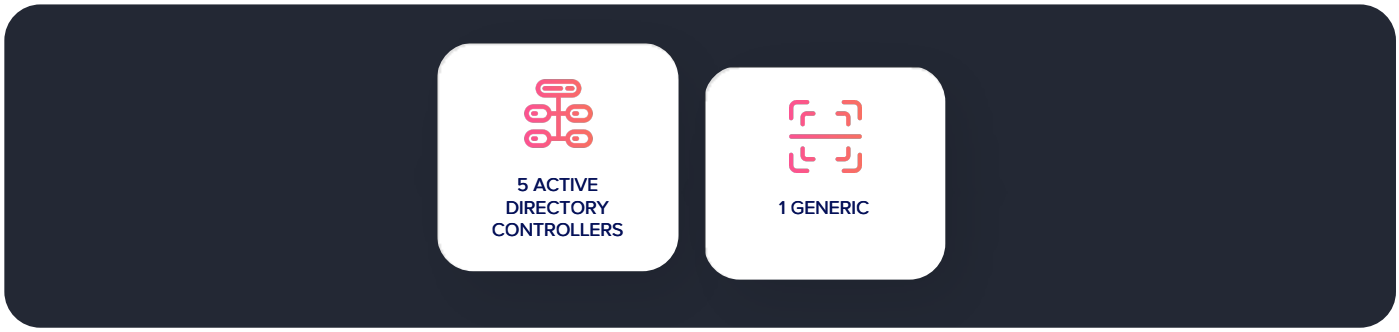
Storage Devices by Disk Space

Disc Space Utilized	Device Count
Up to 25%	15
25 – 50%	16
50 – 75%	10
75 – 90%	9
More than 90%	3

Storage Device Encryption Status

Status	Device Count
Encrypted	0
Not Encrypted	0
Unknown	53

Asset Breakdown



Assets by OS

OS Name	Asset Count
Microsoft Windows 10 Pro	40
linux based os	33
windows	30
Zebra Wired	9
linux_kernel	8
Unix	6
windows_ce	6
Microsoft Windows Server 2016 Standard	4
Rockwell Automation 1769-L33ER	4
Rockwell Automation 1769-L33ERM	3
Microsoft Windows 10 Enterprise 2016 LTSB	1
Microsoft Windows Server 2012 R2 Standard	1
Rockwell Automation 1768-ENBT	1
Rockwell Automation 1769-L35E	1
Rockwell Automation 1769-LxxE	1
Rockwell Automation 5069-AENTR/A	1
Windows 10 Pro	1
Zebra Technologies ZT230-300dpi / internal wired	1