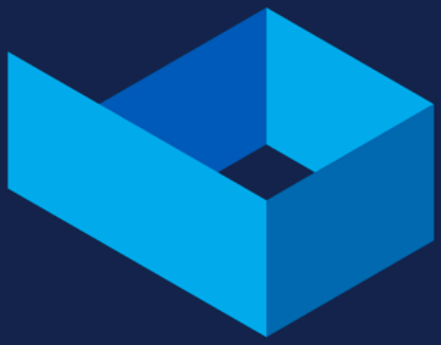


BLUEBOX IT

Cybersecurity Assessment Report

Executive Summary Risk

- 1 out of 1 endpoint(s) missing DNS protection
- 1 out of 1 endpoint(s) missing advanced protection
- 2 out of 2 user(s) never logged in.
- 2 out of 2 user(s) with possible password policy violations.

- 4 out of 21 user account(s) exposed on dark web in last 60 to 120 days.
- 1 out of 1 endpoint(s) missing basic anti-virus protection.
- 1 out of 1 endpoint(s) with incomplete/missing backup configurations.

- 1 out of 21 user account(s) exposed on dark web in last 120 to 365 days.

- 16 out of 21 user account(s) exposed on dark web for more than 365 days.

- All the domains fully compliant for anti-spam configuration.
- All the endpoints fully compliant for firewall protection. All
- the assets running on up-to-date operating system. All the
- endpoints with remote desktop access disabled All the
- assets with hard drive space utilized less than 25%. All the
- assets aged less than 3 years.

TABLE OF CONTENT

Security Assessment

This security assessment report 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 exploited 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 report details the steps taken to discover security issues. In addition to the overall Consolidated Risk Score, the report also presents separate impact scores for all areas of assessment.

Dark Web Assessment

The dark web is a massive and widely used marketplace by cyber criminals. Malicious actors use stolen email credentials to impersonate the owner to commit theft or other fraud. The stolen records including identity and credit card information are often sold on the dark web.

Risk Detected!

Top 3 Exposures

21 EMAIL ID(S) EXPOSED

MULTIPLE EXPOSURES DETECTED

HIGH RISK SCORE

Top Email Exposures	Exposure Count	Latest Exposure Date	Severity	Confidence	Risk Score
xxxxxxxxxx@company.co.uk	6	Aug 21, 2024	High	Low	HIGH
xxxxxxxxxx@company.co.uk	34	Jul 26, 2024	High	Low	HIGH
xxxxxxxxxx@company.co.uk	20	Jul 26, 2024	High	Low	HIGH

*Please refer to the detailed report to view all the records.

How to stay Protected

Keep your identity safe by keeping complex passwords.

Knowing in real-time which passwords and accounts have been posted on the Dark Web allows you to be proactive in preventing a data breach.

We scan the Dark Web and take action to protect your business from stolen credentials that have been posted for sale.

Anti-Spam Assessment

Today, forged and phishing emails are one of the biggest threats to business. Anti-spam assessment allows businesses to mitigate these gaps.

Complete anti-spam configurations require the configuration of DKIM. DKIM uses keys to verify that an email sender is who they say they are. Email domains can contain multiple DKIM cryptographic keys. If you are unsure that your domain has DKIM enabled, contact your email administrator for assistance.

Configured!

List of your email domains	*SPF	**DMARC	Risk Score
@xxxxxxxx.co.uk	✓	✓	NA*
@xxxxxxxx.co.uk	✓	✓	NA*

* SPF or Sender Policy Framework, is an open standard that specifies a method for preventing sender address forgery. It isn't about stopping spam; it's about controlling and stopping attempted sender forgeries.

**DMARC or Domain-based Message Authentication, Reporting, and Conformance, enables the message sender to indicate that their messages are protected with SPF and/or DKIM. A DMARC policy applies clear instructions for the message receiver to follow if an email does not pass SPF or DKIM authentication.

NA* : System is configured with best practices

How to get Protected

- Configuring SPF, DKIM and DMARC for your domains makes it significantly more difficult for a malicious actor to send emails impersonating your organization.
- Monitoring the anti-spam configurations at least once in every 6 months is recommended.

Vulnerability Assessment

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

Risk Detected: High Risk Score

0

Critical Severity Vulnerability

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

1

High Severity Vulnerability

1 unique high severity vulnerabilities were discovered. High severity vulnerabilities are ofter harder to exploit and may not provide the same access to affected systems.

0

Medium Severity Vulnerability

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

0

Low Severity Vulnerability

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

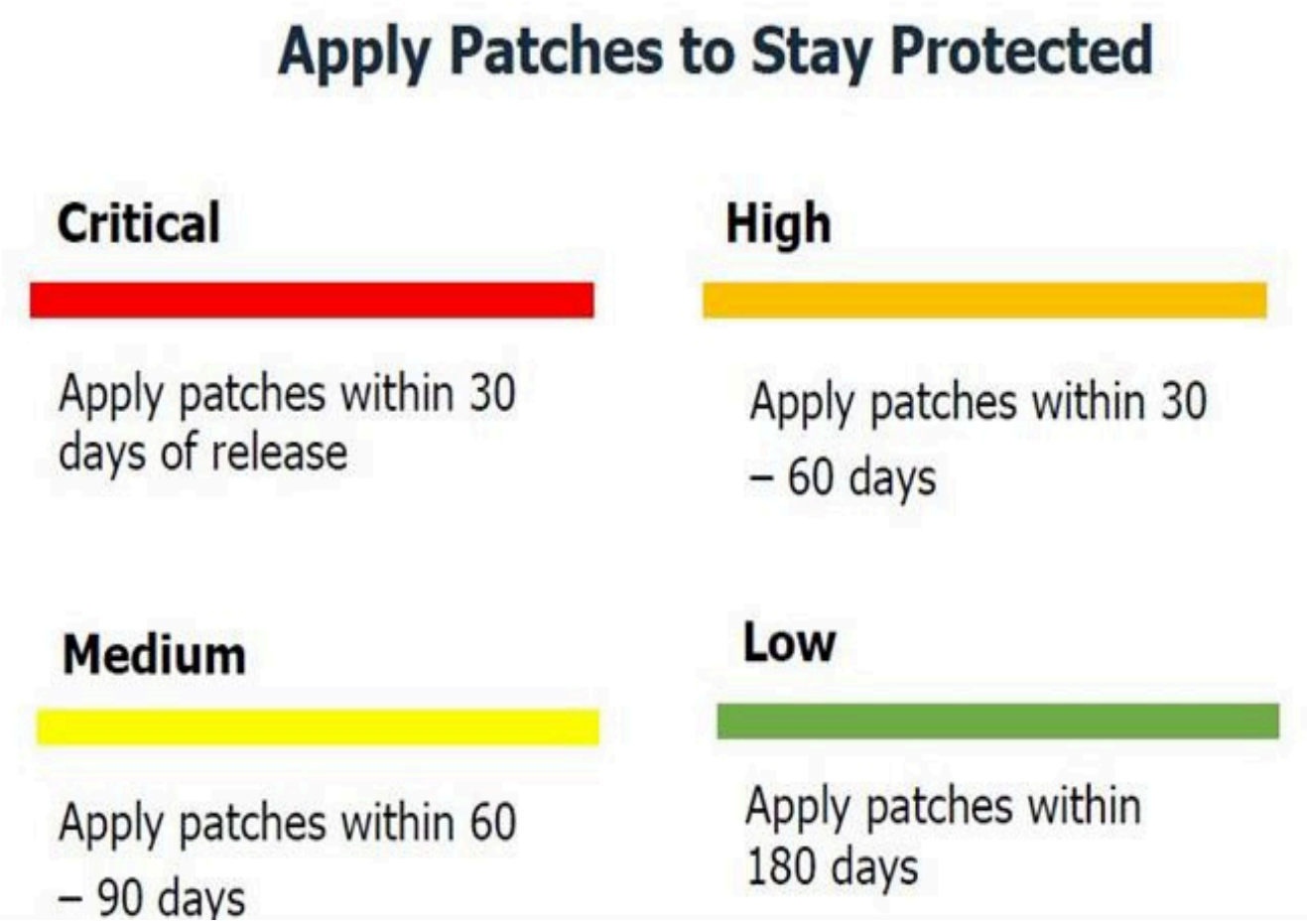
* Please refer to the detailed report to view all the records.

Top 3 Vulnerabilities

Vulnerability Detail	Desktop Count	Server Count	Other Count	Risk Score
Buffer overflow in a component of SQL-DMO for Microsoft Data Access Components...	**1**	**0**	**0**	**HIGH**

*Please refer to the detailed report to view all the records.

... For complete description of Vulnerability Detail , please refer to the detail report.

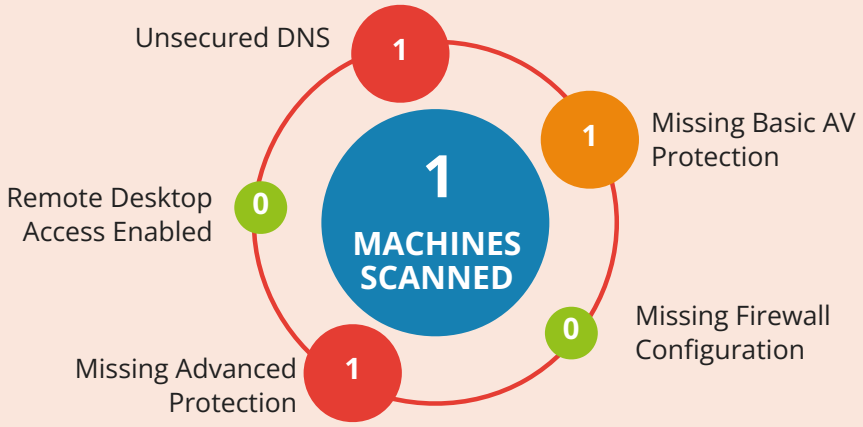


Endpoint Assessment

Today, 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, ConnectWise has 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.

Risk Detected:
High Risk Score



Unsecured DNS

1 out of 1 system(s) missing DNS system configurations.

is a kind of internet directory that delivers your device's name to the universe. Missing configuration leads to DNS attack like Hijacking, Phishing, Pharming etc.

Firewall Configuration

0 out of 1 system(s) missing firewall configuration.

Endpoint firewalls provide specific controls to safeguard endpoints from internal and external attacks.

Remote Desktop Access

0 out of 1 system(s) has remote access enable. Hackers can exploit and gain access to this/these system(s)

Basic AV Protection Missing

1 out of 1 system(s) missing Basic AV protection. AV protects endpoints from malware, viruses, phishing attacks, and other web threats and detects the upcoming threats before they enter the system.

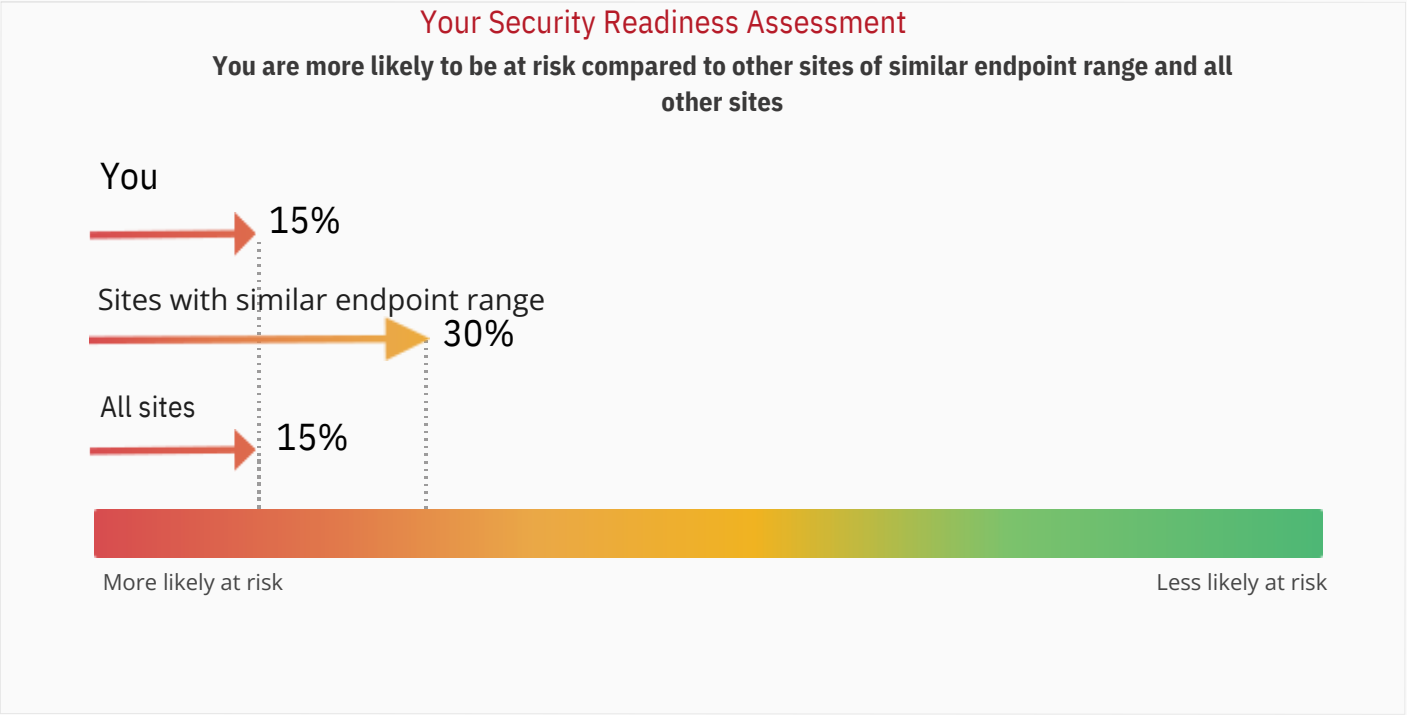
Advanced Protection

1 out of 1 system(s) missing advanced protection like SentinelOne. Advanced protection provide extra layer of security and protects endpoints from advanced attack like ransomware.

Top 3 Endpoints By Missing Controls

Host Name	Host Type	Control
xxxxxxxxxx	Desktop	Advanced Protection, Basic AV Protection, DNS

*Please refer to the detailed report to view all the records.



How to Stay Protected

- Upgrade your security strategies Shield your users from advanced phishing attacks by deploying DNS protection. Our analysis shows you may already have some security measures in place.
- However, your tools may not be enough to prevent and recover from advanced cyberattacks. While regular anti-virus software can prevent most attacks adding advanced protection solutions managed by a security operations centre can prevent most sophisticated attacks and can expedite recovery in the event an attack does occur.

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 vulnerabilities and exploits.

Risk Detected!

1 ASSET(S) SCANNED

3 PATCHE(S) MISSING IN 1 DESKTOP(S)

0 PATCHE(S) MISSING IN 0 SERVER(S)

HIGH RISK SCORE

Apply Patch to Stay Protected

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

Top 3 Missing Patches

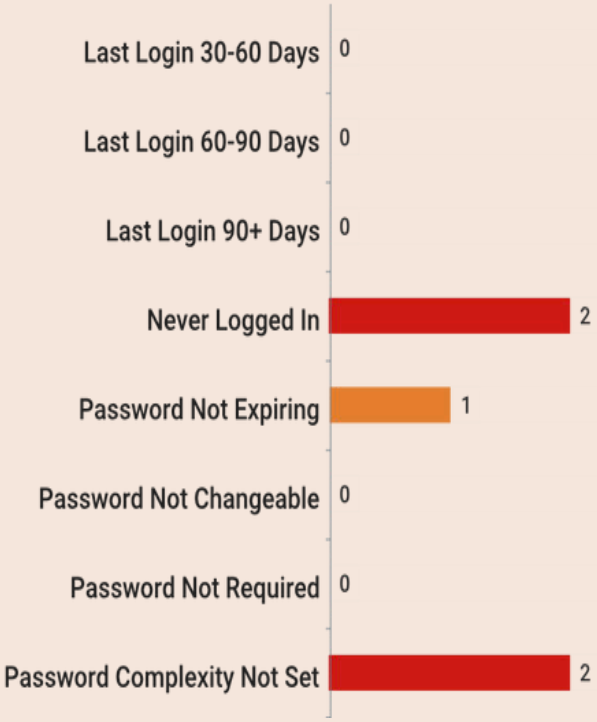
Patch Details	Desktop Count	Server Count	Other Count	Risk Score
2024-08 Cumulative Update for Windows 11 Version 23H2 for x64-based Systems (KB5041585)	1	0	0	HIGH
Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.417.247.0) - Current Channel (Broad)	1	0	0	MEDIUM
Google Chrome	1	0	0	LOW

*Please refer to the detailed report to view all the records.

User Risk Assessment

End-users have become a prime target for cyber criminals. User Risk assessment helps us in finding gaps and securing the IT environment.

Policy Compliance and Login History



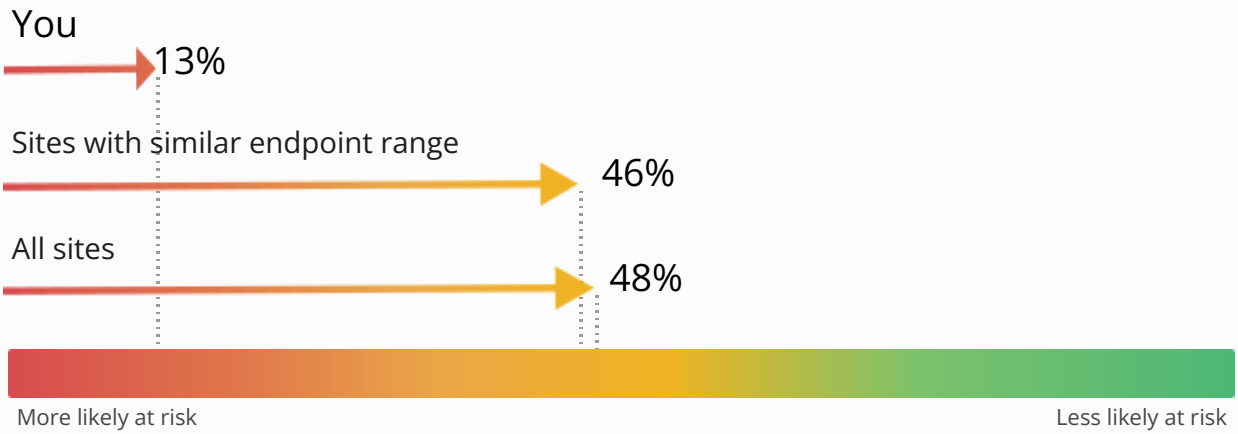
Top 3 Users by Failed Compliance

User	
XXXXXXXX	**Password Complexity Not Set**
XXXXXXXX	**Password Complexity Not Set, Never Logged In**

*Please refer to the detailed report to view all the records.

Your Security Readiness Assessment

You are more likely to be at risk compared to other sites of similar endpoint range and all other sites



How to Stay Protected

- Upgrade your security Strategies
- I mplement processes and tools to periodically review Use r Access Controls

IT Infrastructure Assessment

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

High Risk Detected!

Asset(s) by Disk Space

Disc Space Utilized	Asset Count
Up to 25%	1
25 - 50 %	0
50 - 75 %	0
75 - 90 %	0
More than 90 %	0

Asset(s) by Age

Asset Age (In Year)	Asset Count
0 - 3	1
3 - 5	0
5 +	0

Asset(s) by Backup & Recovery Configuration

Backup & Recovery provides visibility which helps organizations to prepare for any Data Loss. Backup copies allow data to be restored from an earlier point in time to help the business recover from an unplanned event.

Asset(s) by OS

Operating System	Asset Count	Unsupported OS
Microsoft Windows 11 Enterprise	**1**	**No**

How to stay Protected

Plan upgrades for End-of-Life Operating Systems.

Implement a backup and recovery tool. Backup copies allow data to be restored from an earlier point in time to help the business recover from an unplanned event.

Low disk space can impact business applications and prevent them from running properly. The organization should implement tools to monitor resources like disk space, memory, processor etc.