WhiteRook Cyber

22 Oct - 21 Nov

Security Business Review

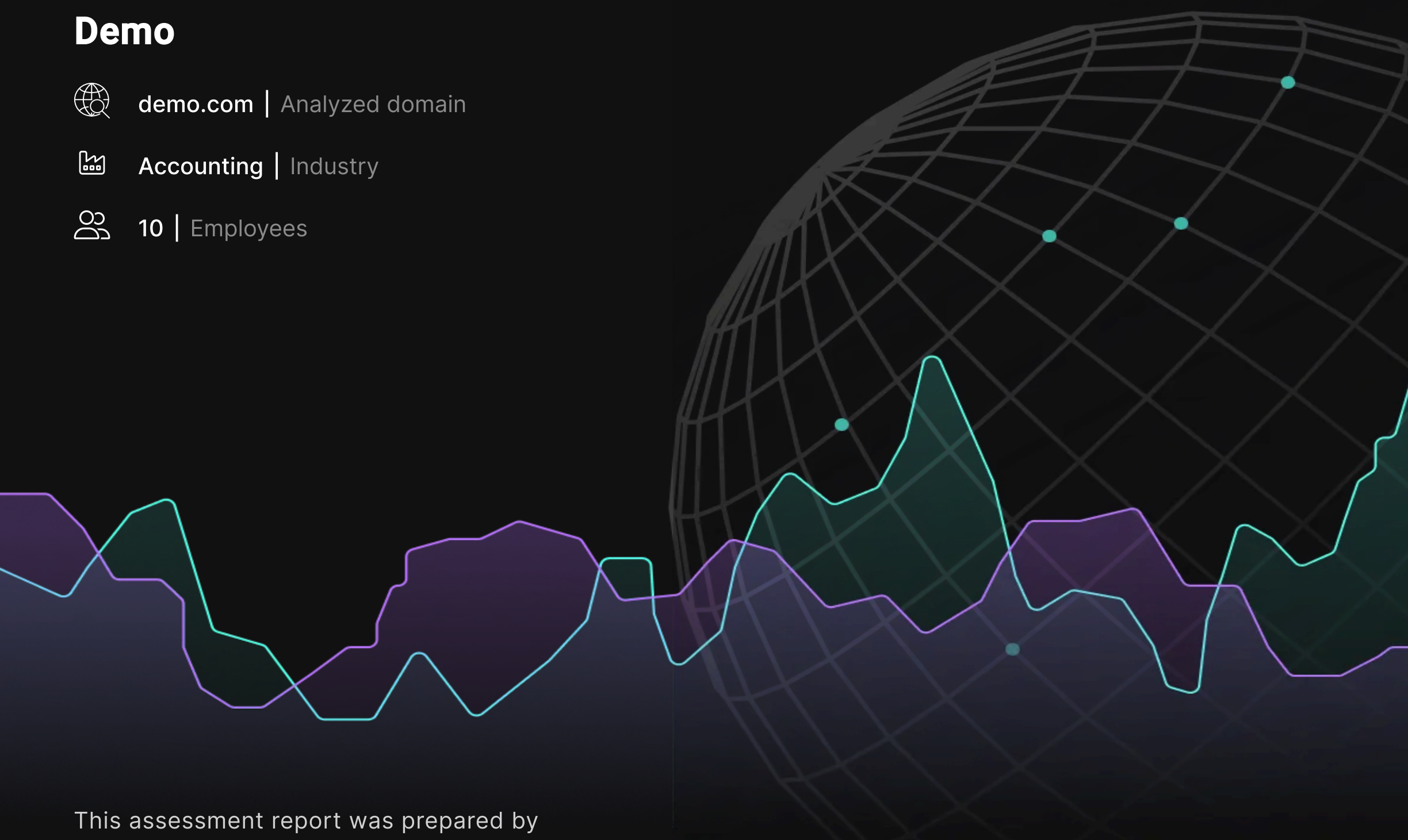
Generated For

Demo

demo.com | Analyzed domain

Accounting | Industry

10 | Employees



This assessment report was prepared by

White Rook Cyber

1300 794 777 whiterookcyber.com.au contact@whiterookcyber.com.au

WhiteRook Cyber

SECURED ASSETS

16 IPs & Domains — No Changes	10 Employees — No Changes	14 Devices — No Changes
13 Cloud Drives	10 Mailboxes	1 Browsers

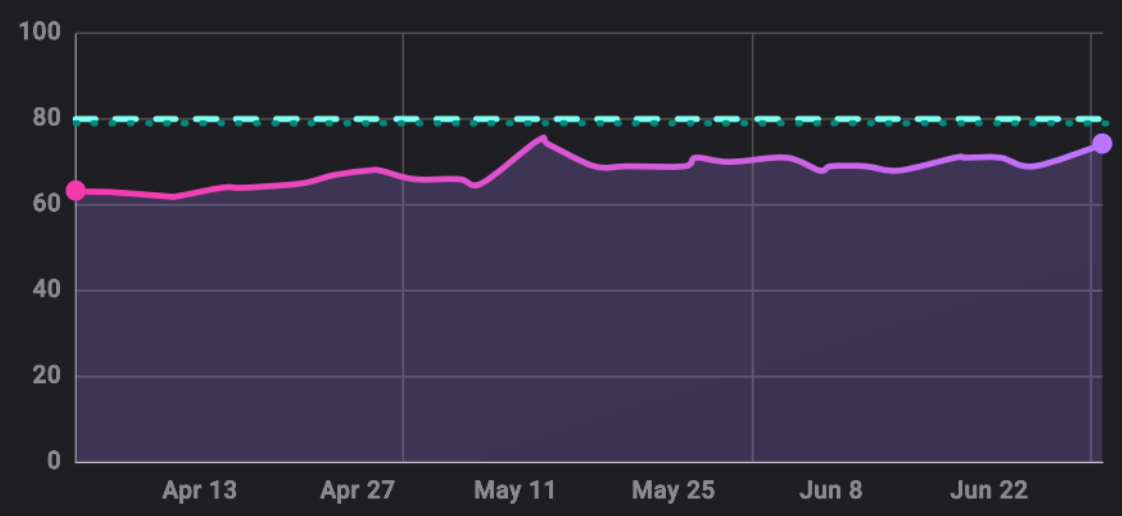
FINANCIAL EXPOSURE

~ $27,000
Possible Financial Loss

— 0% no changes from last period
$0

Possible Financial Loss - This data estimates potential financial losses based on internal and external scans, user risk, vulnerabilities and overall security posture, factoring in industry, company size, digital assets and attack surface.

SECURITY SCORE



74
Current Score
11 Increase

79
Industry benchmark

63
Starting Score

80
Insurance threshold

Security Score - The Security Score is based on coverage (activated security controls) and the volume and severity of issues within each control.

Financial loss due to cybersecurity incidents in Accounting

In the Accounting industry, where firms handle significant amounts of their clients' financial data, the specter of cyberattacks is a constant concern averaging around 3.86 million.

Accounting firms need to ensure stringent compliance with regulations like GDPR or GLBA, where non-compliance can result in severe penalties, up to **€20** million, or **4%** of the company's global turnover. A noted example is the cyber incident at prominent accounting firm Deloitte, which experienced a breach that exposed client and corporate private emails and information.

DETECTIONS & RESPONSES

282
Total Detections

- 123 Fixed
- 2 Ignored
- 105 Archived
- 0 In Progress
- 52 Open

Email Protection	32%	39
Cloud Data	7%	8
Endpoint Protection	2%	3
ITDR	1%	1
Phishing Simulations	0%	
Awareness	0%	
Dark Web Monitoring	0%	
External Footprint Scan	0%	
Secure Browsing	0%	

User Posture

SAFE VS RISKY USERS

10 Total

10% 1 safe users

90% 9 unsafe users

TOP RISKY USERS

emily.brown@demo.com	High
michael.johnson@demo.com	High
john.doe@demo.com	High
olivia.davis@demo.com	High
ava.wilson@demo.com	High
william.garcia@demo.com	High
sarah.lee@demo.com	High
daniel.martinez@demo.com	High

Risky Users - This score for each user is a combination of role, amount of detections and their type and severity.

IDENTITY THREAT DETECTION & RESPONSE

2 Total Detections

0% Open	0% In Progress	0% Ignored	0% Archived	100% Fixed
0	0	0	0	2

CLOUD DIRECTORY DETECTIONS BY TYPE

0 Multi Factor Authentication — 2 Decrease

0 Suspicious Mailbox Rules — 2 Decrease

0 Inactive User — 1 Decrease

0 Suspicious Login — 4 Decrease

TOP SUSPICIOUS LOGINS

Isfahan Iran
2 Logins | Open

Moscow Russia
1 Login | Open

Toronto (Old Toronto) Canada
1 Login | Open

Pyongyang North Korea
1 Login | Open

*The above is a subset of security detections, highlighted based on the severity and recency of the detections.

PHISHING SIMULATIONS

Passed Users | In progress | Failed Users

21 Oct
1 Assignee — 0% | 0% | 100%

AWARENESS CAMPAIGNS

21 Oct
2 Assignees — 0% Completed

21 Oct
1 Assignee — 100% Completed

USERS WITH MOST FAILED SIMULATIONS

	#
John Doe	1

USERS WITH MOST INCOMPLETE CAMPAIGNS

	#
Olivia Davis	1
Emily Brown	1

Email Protection

DETECTIONS & RESPONSES

57,492
Overall scanned emails

1,885
3% Detected emails
837 Increase

5
0% Quarantined emails
No Changes

0
0% Restored

0
0% Deleted

1,406
75% Caution banners
522 Increase

0
0% Marked as safe

0
0% Reported & removed

0
0% Ignored

246
17% Open

ATTACK TYPE BREAKDOWN

93 Spam	32 Phishing	42 Impersonation
0 Virus	0 Scam	156 Other

TOP TARGETED USERS

	# of detections
daniel.martinez@demo.com	1
david.williams@demo.com	1
ava.wilson@demo.com	1
jane.smith@demo.com	1
john.doe@demo.com	1

External Assets

TOP RISKY ASSETS

Asset	Type	Geo-Location	Issues
ldap.demopp.com	Subdomain	United States	2
demotech.com	Domain	United States	2
104.22.4.147	IP	United States	2
237.168.12.5	IP	United States	2

EXTERNAL FOOTPRINT DETECTIONS & RESPONSES

1
Total Detections

1	0	0	0	0
100% Open	0% In Progress	0% Ignored	0% Archived	0% Fixed

INTERNET ASSETS TYPES

16
External Assets

8	3	5
50% IP	19% Domain	31% Sub-domain
No Changes	No Changes	No Changes
Risk: 5 Unsafe	1 Unsafe	4 Unsafe
No Changes	No Changes	No Changes

Endpoint Protection

SECURED DEVICES

14

10 Unsafe Devices

OPERATING SYSTEM BREAKDOWN

6	6	2
43% Windows	43% MacOS	14% Win Server
6 Unsafe	2 Unsafe	2 Unsafe

DEVICE DETECTION BY TYPE

74
Total Attacks

73 Increase

73
Antivirus Threat
72 Increase

0
Antivirus Policy

1
Endpoint Posture

0
Endpoint Ransomware

TOP RISKY DEVICES

Identifier	Count	Status	OS
Work DESKTOP-PC 3	10	Risky	
WINSERVER-01	10	Risky	
Work DESKTOP-PC 5	9	Risky	

ENDPOINT DETECTIONS & RESPONSES

4
Total Detections

0	0	0	0	4
0% Open	0% In Progress	0% Ignored	0% Archived	100% Fixed

Cloud Data Protection

CLOUD DRIVES

13

EXPOSURE BY TYPE

0
External Share
2 Decrease

0
Public Link
2 Decrease

CLOUD DATA DETECTIONS & RESPONSES

26
Total Detections

16	0	2	0	8
62% Open	0% In Progress	8% Ignored	0% Archived	31% Fixed

TOP RISKIEST PATHS

Path	Issues	App
path/to/budget-folder	1	
path/to/Hidden_Crypto_Wallet.pdf	1	
path/to/investments	1	
path/to/results.doc	1	

Glossary

IP Address	An IP address is a distinct numerical label, unique to a device, server or website, serving as a specific online location. It's vital for all online activities, and should be protected as a valuable 'digital asset'.
Cyber Posture Rating	Based on the results of a non-intrusive external surface attack scan and dark web monitoring, a cyber posture rating is calculated from 0-100 which represents the level of risk allocated to a company's external digital footprint.
Security Findings	Security findings refer to identified vulnerabilities or weaknesses discovered during the risk assessment, highlighting security issues that organizations need to address. The findings in this report cover; Network & IT, Application, Human, and Compromised Credentials.
Dark Web	The Dark Web is a hidden part of the internet, commonly used by cybercriminals for illegal activities. A dark web scan identifies leaked credentials indicating the potential for unauthorized access of personal data, eventually leading to the risk of security breaches.
External Surface	The external surface refers to an organization's digital footprint that is visible and accessible to the public. This includes company websites, email systems, servers, protocols and other exposed services.
Assets	For the purposes of this report, a digital asset refers to company owned domains, subdomains, servers, and IP addresses. These assets often carry a lot of value, as they form a part of an organization's digital identity and operations which should be protected against cyberthreats.
Domain	A domain is a unique identifier that represents the web address or URL which is crucial for people to find and interact with a website. Domains are essential digital assets because of the traffic they attract, requiring protection to prevent misuse or unauthorized changes.
Web Server	A web server is a system that stores, processes, and delivers web pages to users. These servers require regular maintenance and if not updated can open up publicly accessible vulnerabilities.
TLS/SSL	TLS and SSL are protocols designed to provide secure communication by encrypting data between a browser and a website. It's crucial to ensure up-to-date versions of TLS or SSL to avoid vulnerabilities in the system.
Web Certificate	A web certificate authenticates a website's identity and enables an encrypted connection. When it is outdated, site traffic may be compromised.

Phishing

Hackers use phishing to trick people into giving away sensitive information, such as passwords, by posing as a trustworthy entity or person. Holistic protection against phishing combines email security, browsing, endpoint protection, perimeter posture, and awareness culture in one native solution.

Ransomware

This malware encrypts a victim's files or data and demands payment in exchange for the decryption key, causing damage to businesses.A managed anti-virus solution should detect and isolate infected systems in parallel with monitoring of vulnerable servers, email attachments, and abnormal activity.

Data Loss

Unauthorized loss of sensitive information, can have severe consequences, including financial losses, reputational damage, and legal implications. Data loss protection includes data in the cloud and secures several vectors of attack while exposing the risks of negligent and intentional data exfiltration.

User Risk

Users are the first line of defense against a cyber attack but are often also the weakest link, so in addition to ongoing security training, employees should be protected through monitoring for leaked credentials, spear-phishing prevention, as well as cloud and device posture analysis.

Common Threats FAQ

How can I identify a phishing email?

Looking for suspicious senders or sloppy formatting are quick indicators you can catch with your eye. But hackers are getting more sophisticated, and it is recommended by regulation and industry best practices to utilize email security with other detection tools.

How can I protect my computer or network from ransomware attacks?

To defend against ransomware, keep software updated, use reputable antivirus software, be cautious with email attachments/links, regularly back up important files offline/cloud, enable automatic backups/versioning, and educate about phishing and safe browsing. Bottom line employees need to be actively involved in security, and systems need to be in place to quickly detect and prevent ransomware attacks.

How to prevent data loss?

In a world where we are focused on collaboration, the same tools that allow us to be productive open up vectors of attack for external exposure of confidential data. It's about being diligent regarding cloud posture and sharing best practices to avoid accidental data leakage.

How to prevent user risk in cybersecurity?

To prevent user risk in cybersecurity, implement comprehensive user awareness and training programs to educate employees about common cyber threats, phishing attacks, and safe online practices as well as having the right tools in place to automate user access policies and mitigate common vectors of risk.

This assessment report was prepared by

White Rook Cyber

1300 794 777

whiterookcyber.com.au

contact@whiterookcyber.com.au

Generated For

Demo

demo.com | Analyzed domain

Accounting | Industry

10 | Employees

Secure Your Business Today

Powerful Cybersecurity in Action