Essential Eight

An Implementation Journey

The Organisation.

Queanbeyan-Palerang Regional Council (QPRC) is one of the oldest regional councils in NSW, and the LGA shares its border with the Australian Capital Territory.

Amalgamated in 2016

Population 64,000+

AR Bluett Award 2020

Employees 450+

Essential Eight Controls

Prioritised mitigation strategies to help organisations protect themselves against various cyber threats

4 Top Controls	**8** Essential Controls
37 Strategies	**69** Assessment Points

E8: Overview and Scope

Essential Eight is a mandatory requirement for all Australian Non-corporate Commonwealth entities (NCEs) subject to the PGPA

1,2,3

Maturity Levels

ML 2

Baseline

2017

First Release

NOV 2023

Latest Version

The Power of 8

Patch applications

Patch operating systems

Multi-factor authentication

Restrict administrative privileges

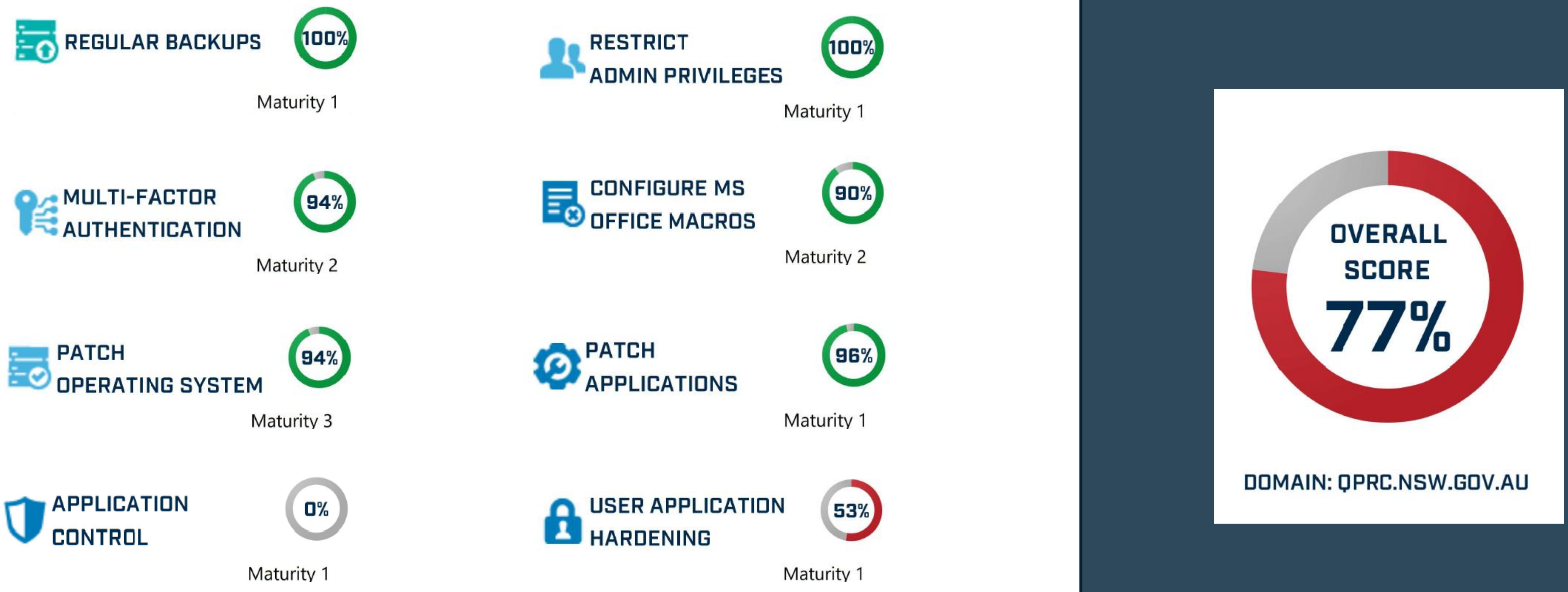
Application control

Restrict Microsoft Office macros

User application hardening

Regular backups

E8 Scorecard



REGULAR BACKUPS	100%	Maturity 1
MULTI-FACTOR AUTHENTICATION	94%	Maturity 2
PATCH OPERATING SYSTEM	94%	Maturity 3
APPLICATION CONTROL	0%	Maturity 1
RESTRICT ADMIN PRIVILEGES	100%	Maturity 1
CONFIGURE MS OFFICE MACROS	90%	Maturity 2
PATCH APPLICATIONS	96%	Maturity 1
USER APPLICATION HARDENING	53%	Maturity 1

OVERALL SCORE 77%

DOMAIN: QPRC.NSW.GOV.AU

Success Factors

Tone From The Top

Experienced Team

Resources

A Professional Team

12
ITSM

05
Change Mgmt

04
Project Mgmt

01
CISM

01
CISSP

ITIL® Prosci® PRINCE2® ISACA® ISC2™

Timeline

2019 Q4

Intro into Essential Eight

2020 Q3

Start of E8 implementation,
Auditor 8 software, etc.

2020 Q4

Regular backups: Maturity ML1

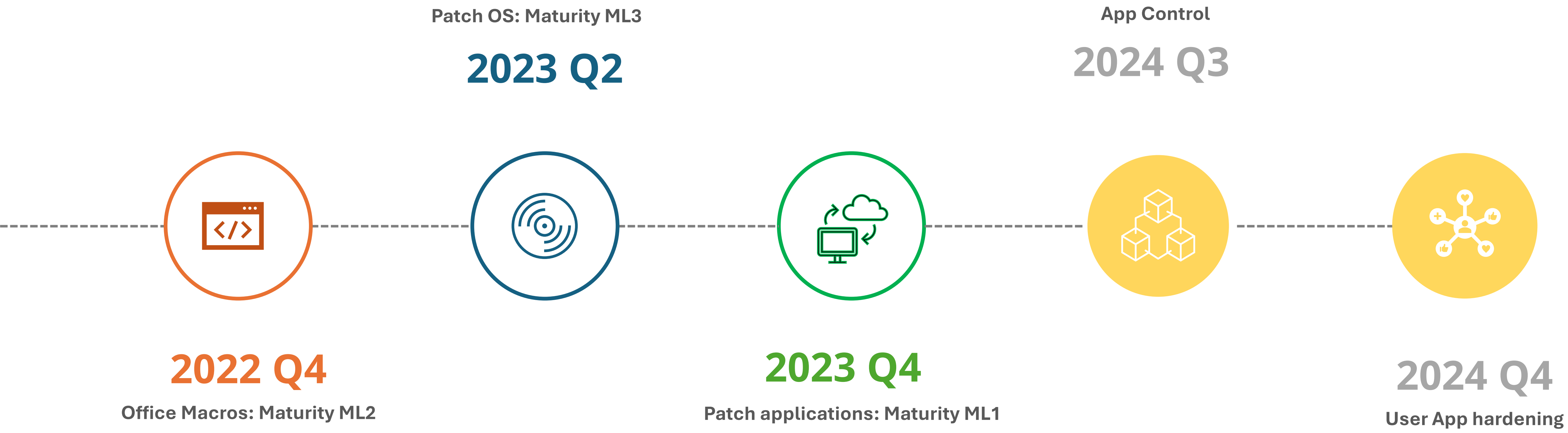
2021 Q2

Admin privileges: Maturity ML1

2022 Q1

Multifactor Auth: Maturity ML2

Timeline



2022 Q4

Office Macros: Maturity ML2

Patch OS: Maturity ML3

2023 Q2

2023 Q4

Patch applications: Maturity ML1

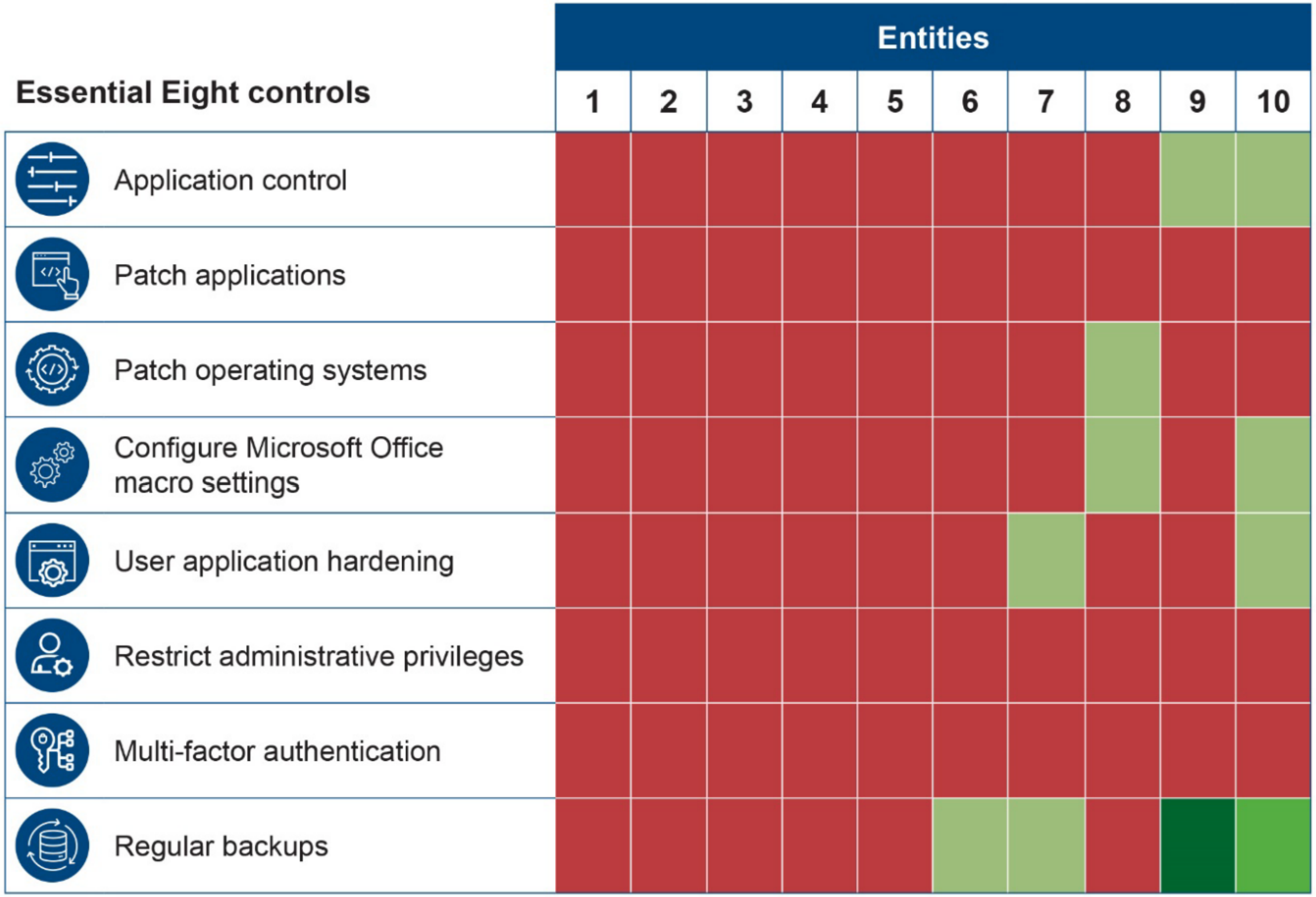
App Control

2024 Q3

2024 Q4

User App hardening

Benchmarking



Essential Eight controls	Entities									
	1	2	3	4	5	6	7	8	9	10
Application control	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩
Patch applications	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Patch operating systems	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟥
Configure Microsoft Office macro settings	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟩
User application hardening	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟥	🟩
Restrict administrative privileges	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Multi-factor authentication	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Regular backups	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟥	■	🟢

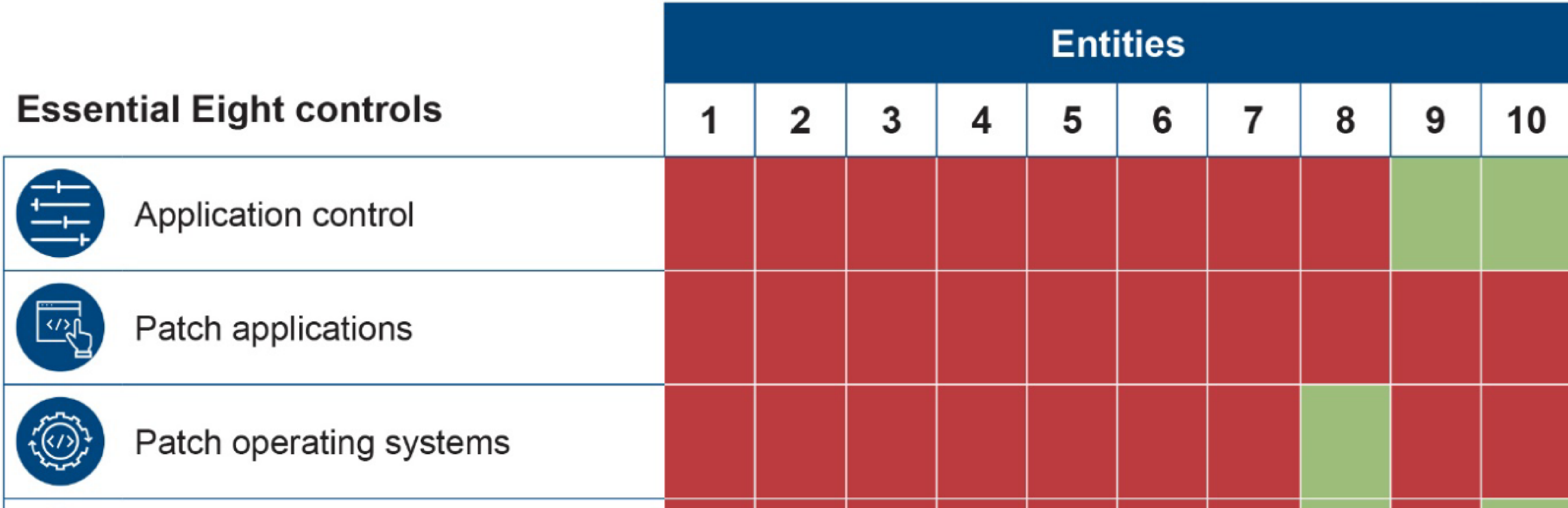
🟥 Maturity Level Zero 🟩 Maturity Level One 🟢 Maturity Level Two ■ Maturity Level Three

10 State Government Entities

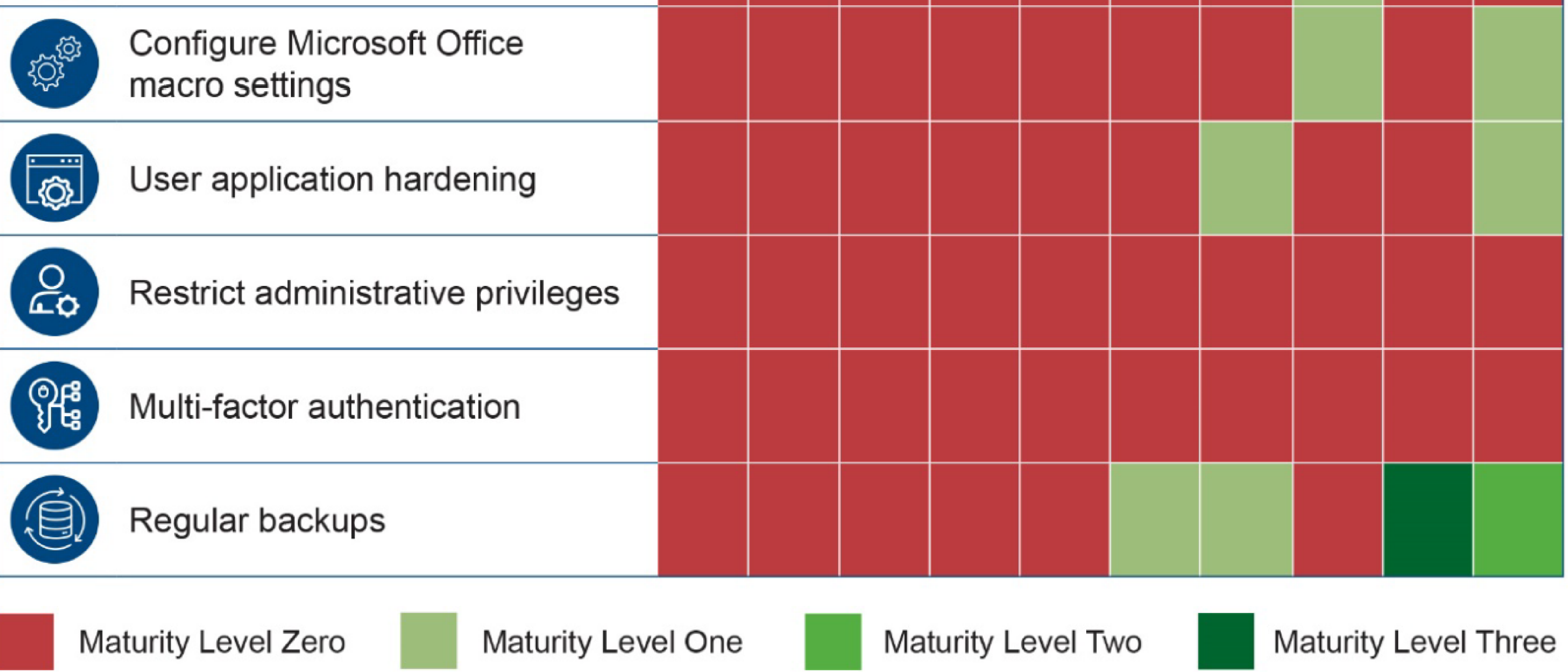
OAG's Report WA

December 2023

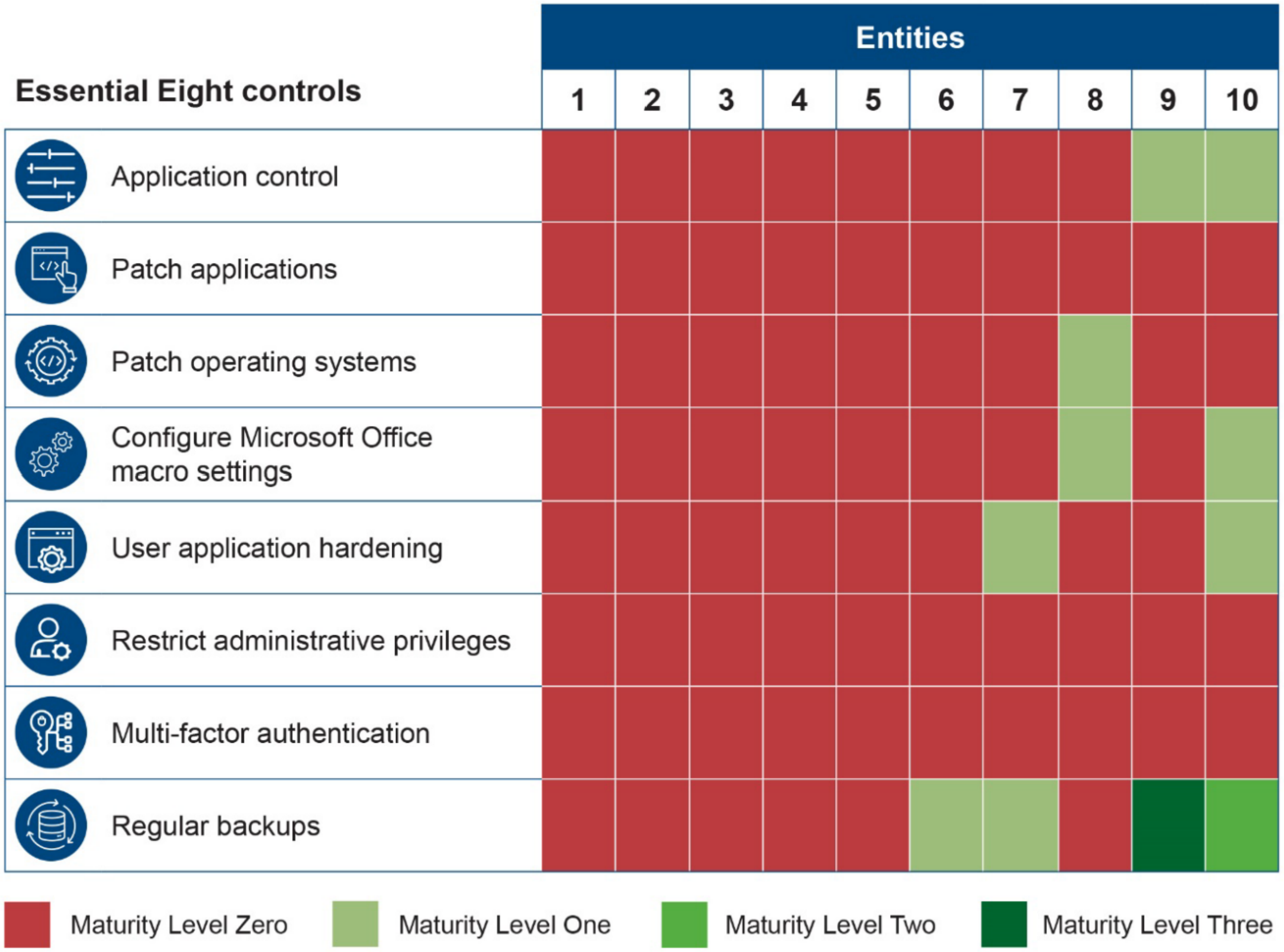
Benchmarking



Essential Eight controls	Entities									
	1	2	3	4	5	6	7	8	9	10
Application control	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩
Patch applications	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Patch operating systems	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟥


Configure Microsoft Office macro settings
User application hardening
Restrict administrative privileges
Multi-factor authentication
Regular backups
Maturity Level Zero
Maturity Level One
Maturity Level Two
Maturity Level Three

Benchmarking



Essential Eight controls	Entities 1	2	3	4	5	6	7	8	9	10
Application control	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩
Patch applications	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Patch operating systems	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟥
Configure Microsoft Office macro settings	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟩
User application hardening	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟥	🟩
Restrict administrative privileges	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Multi-factor authentication	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Regular backups	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟥	■	▩

🟥 Maturity Level Zero 🟩 Maturity Level One ▩ Maturity Level Two ■ Maturity Level Three

10 State government entities

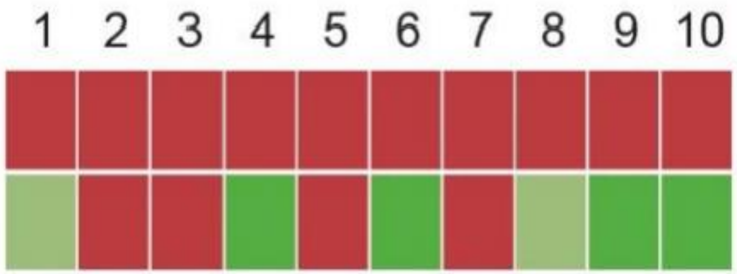
OAG’s Report WA

December 2023

Perils of Self-assessment

Restrict administrative privileges

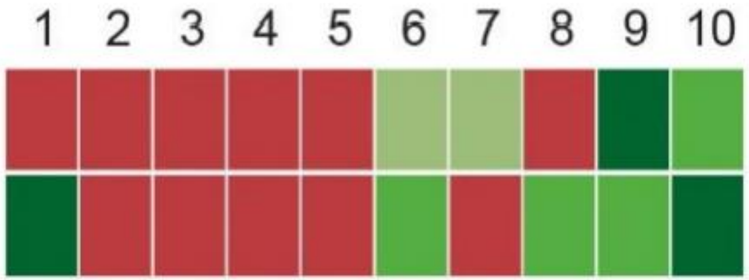
Entities



	1	2	3	4	5	6	7	8	9	10
OAG's assessment	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Entity's assessment	🟩	🟥	🟥	🟩	🟥	🟩	🟥	🟩	🟩	🟩

Regular backups

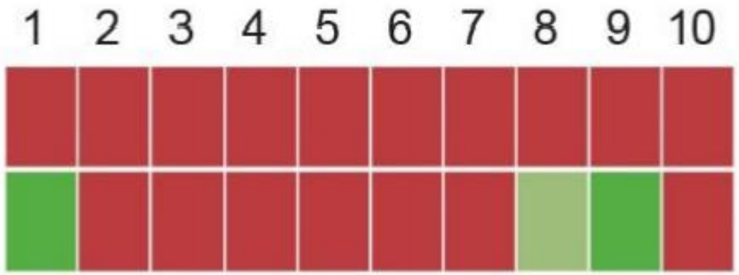
Entities



	1	2	3	4	5	6	7	8	9	10
OAG's assessment	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟥	🟩	🟩
Entity's assessment	🟩	🟥	🟥	🟥	🟥	🟩	🟥	🟩	🟩	🟩

Patch applications

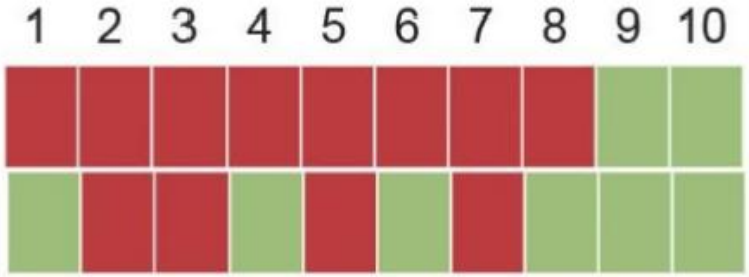
Entities



	1	2	3	4	5	6	7	8	9	10
OAG's assessment	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Entity's assessment	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟥

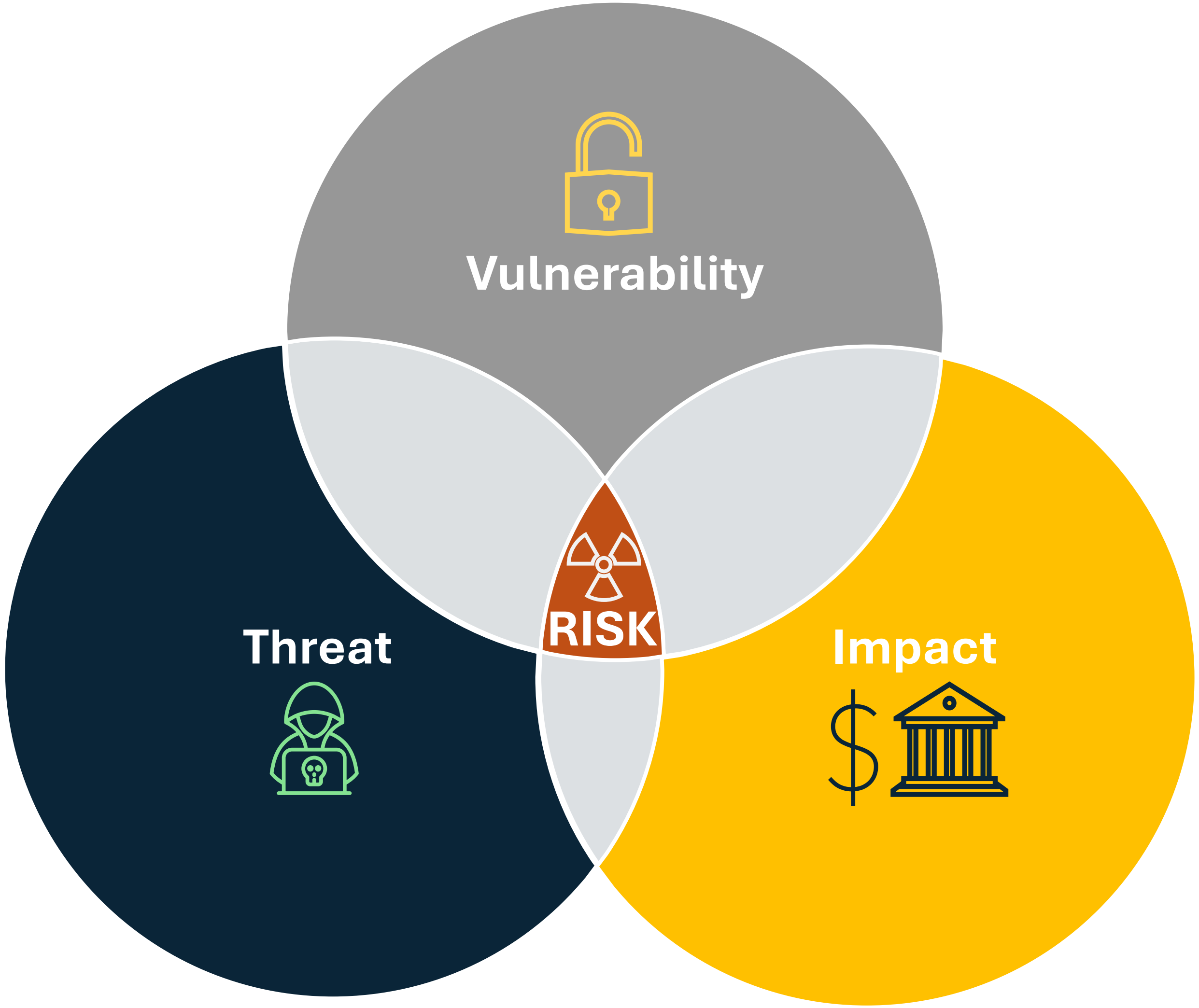
Application control

Entities

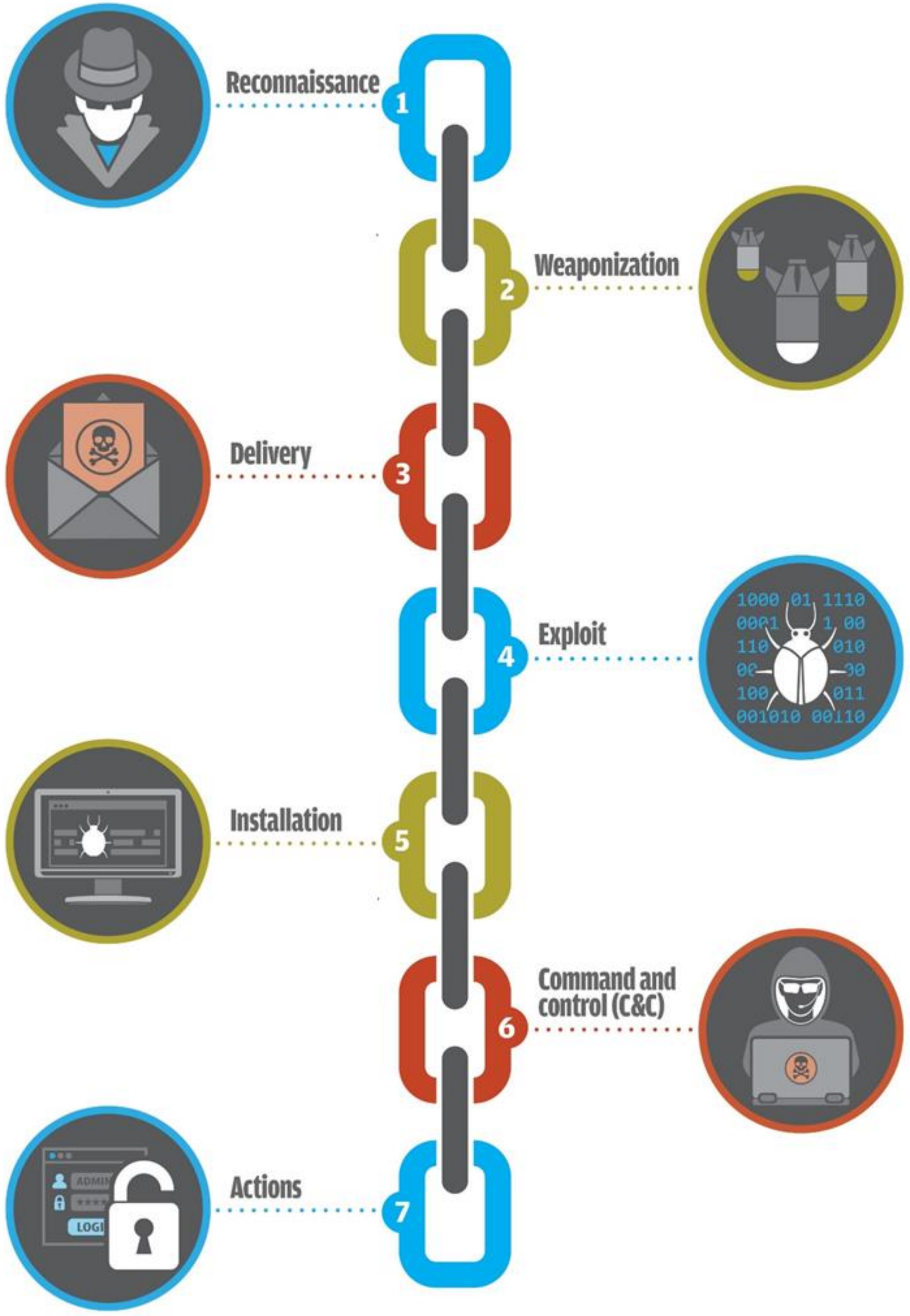


	1	2	3	4	5	6	7	8	9	10
OAG's assessment	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩
Entity's assessment	🟩	🟥	🟥	🟩	🟥	🟩	🟥	🟩	🟩	🟩

The Risk Equation

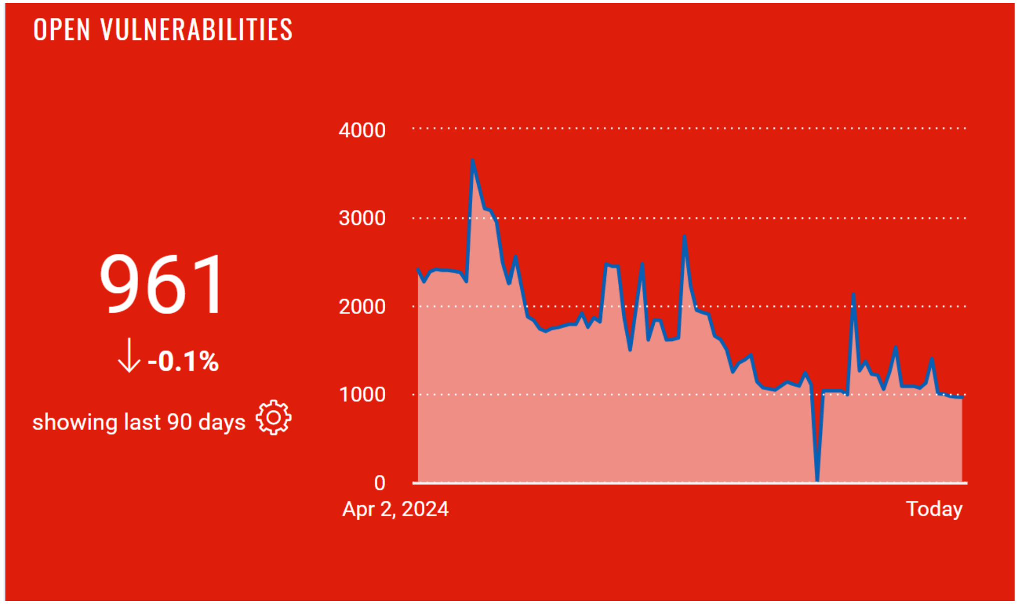


CYBER KILL CHAIN



SOURCE: LOCKHEED MARTIN

Software Tools: Qualys VMDR

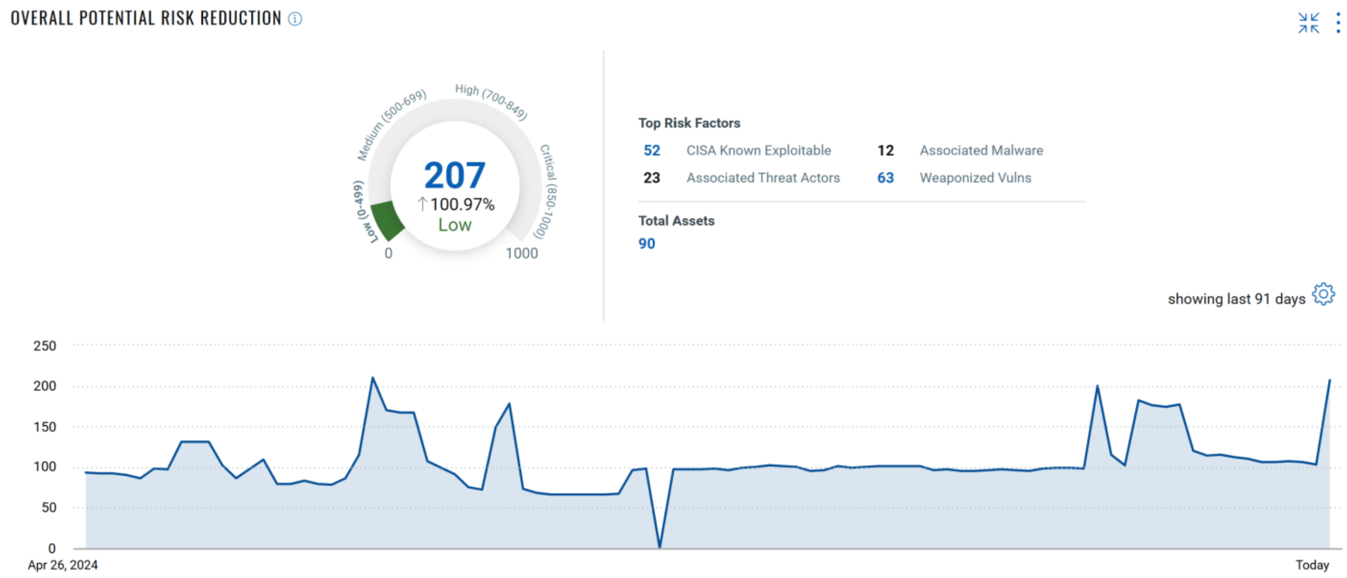


OPEN VULNERABILITIES

961

↓ -0.1%

showing last 90 days



OVERALL POTENTIAL RISK REDUCTION

207

↑ 100.97%

Low

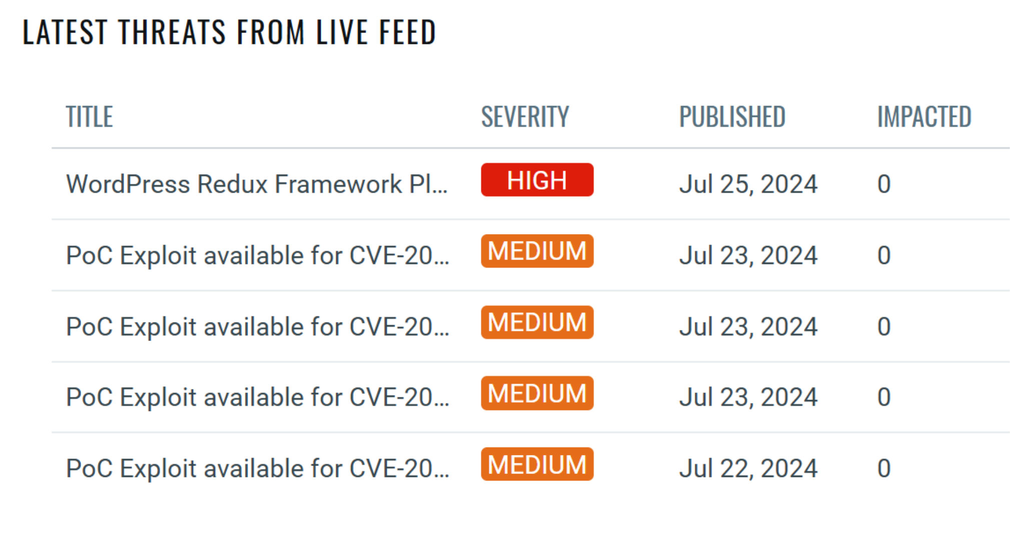
Top Risk Factors

52	CISA Known Exploitable	12	Associated Malware
23	Associated Threat Actors	63	Weaponized Vulns

Total Assets

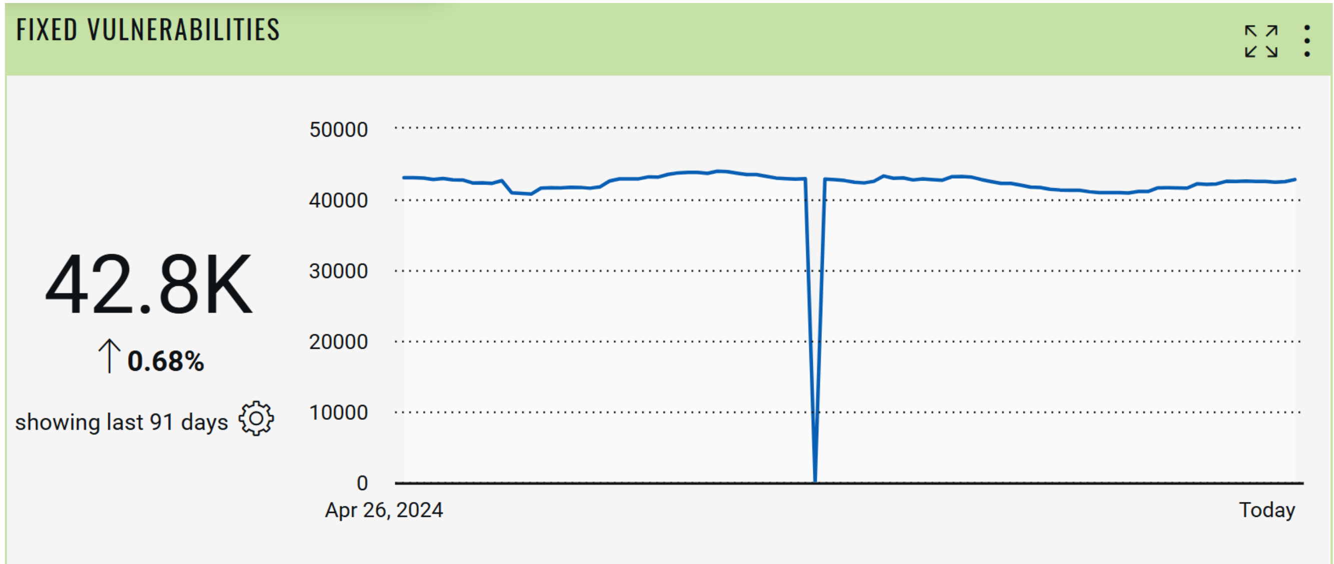
90

showing last 91 days



LATEST THREATS FROM LIVE FEED

TITLE	SEVERITY	PUBLISHED	IMPACTED
WordPress Redux Framework Pl...	HIGH	Jul 25, 2024	0
PoC Exploit available for CVE-20...	MEDIUM	Jul 23, 2024	0
PoC Exploit available for CVE-20...	MEDIUM	Jul 23, 2024	0
PoC Exploit available for CVE-20...	MEDIUM	Jul 23, 2024	0
PoC Exploit available for CVE-20...	MEDIUM	Jul 22, 2024	0



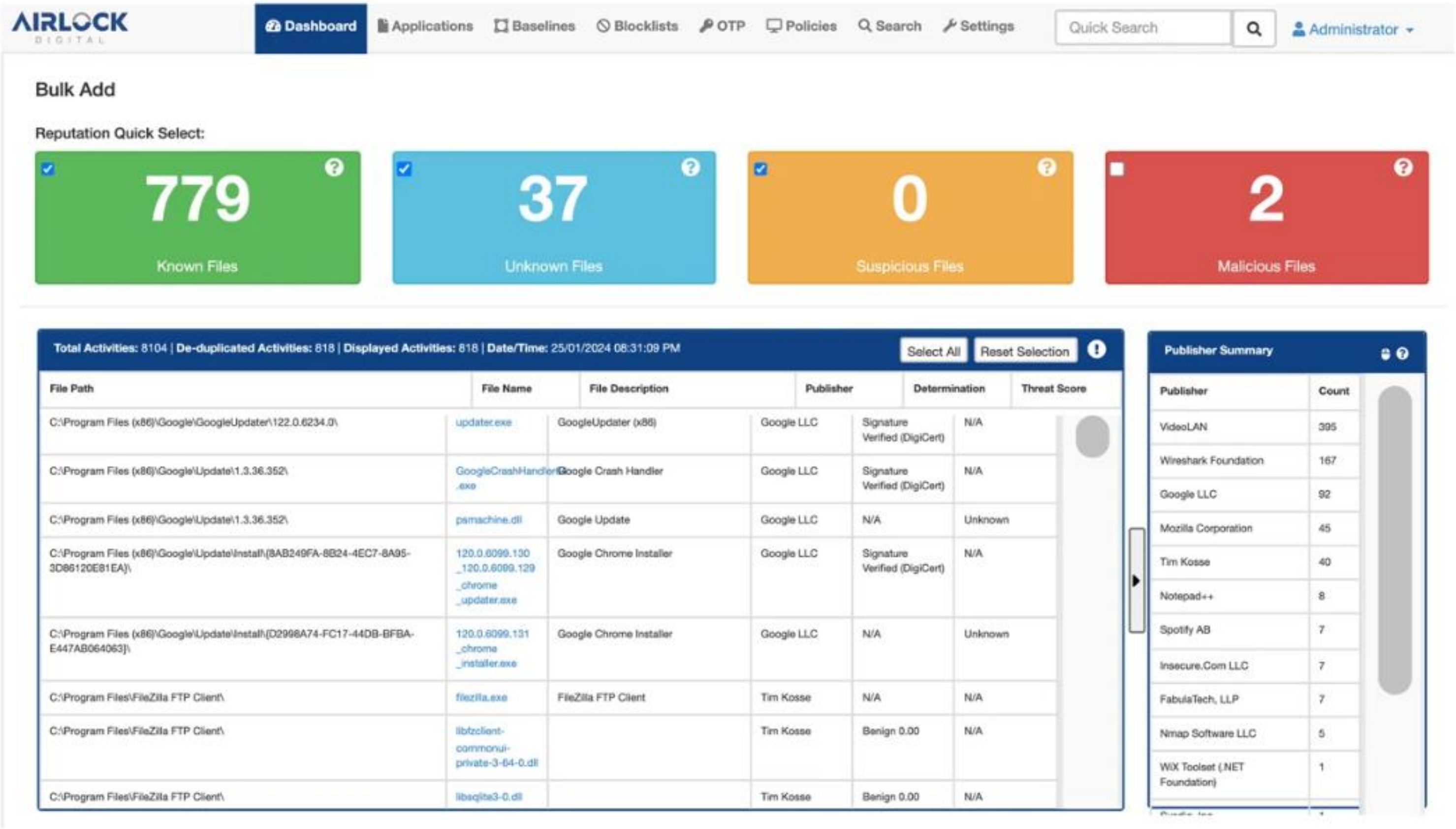
FIXED VULNERABILITIES

42.8K

↑ 0.68%

showing last 91 days

Software Tools: Airlock



Bulk Add

Reputation Quick Select:

☑ 779 Known Files

☑ 37 Unknown Files

☑ 0 Suspicious Files

□ 2 Malicious Files

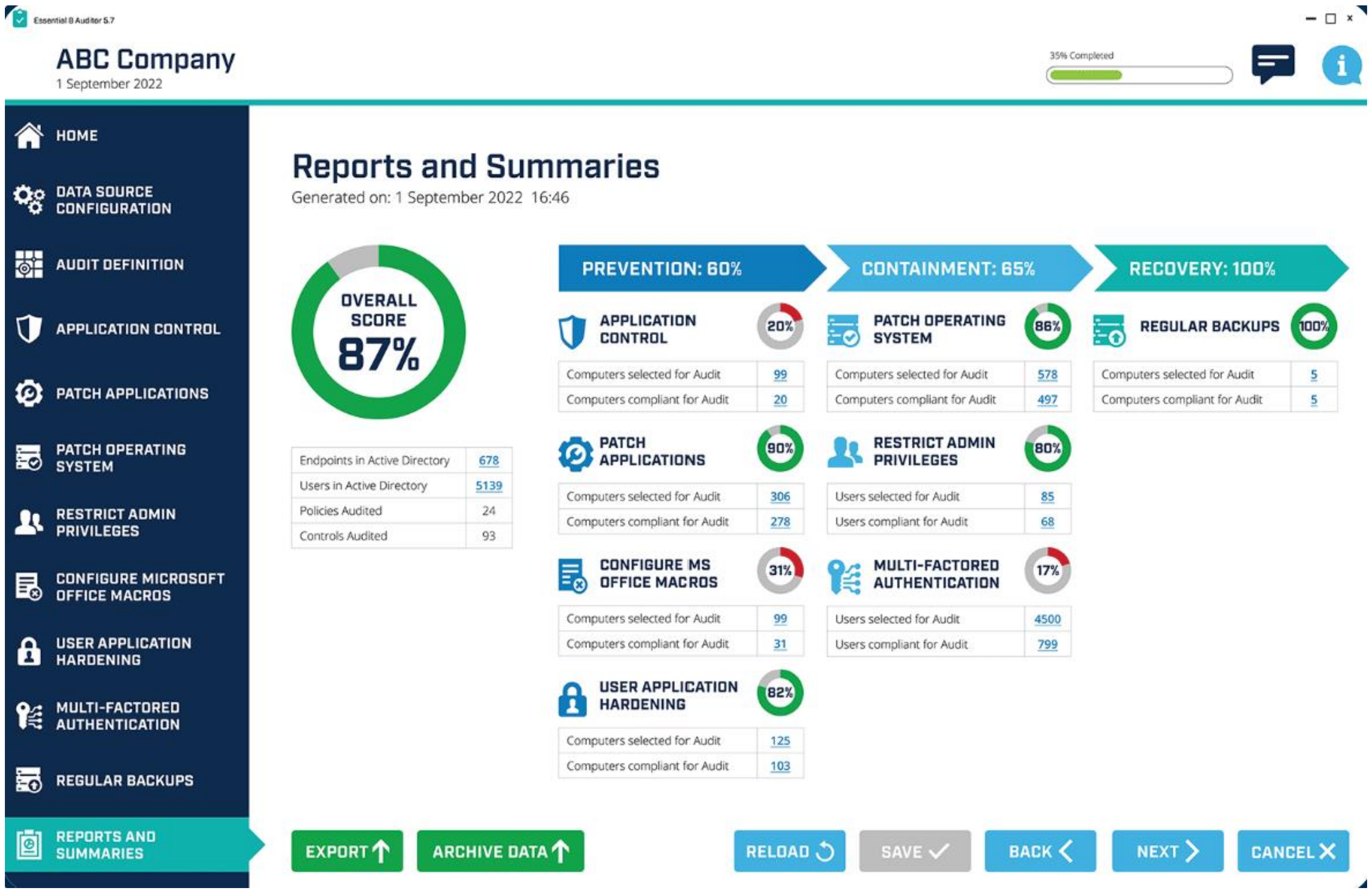
Total Activities: 8104 | **De-duplicated Activities:** 818 | **Displayed Activities:** 818 | **Date/Time:** 25/01/2024 08:31:09 PM

File Path	File Name	File Description	Publisher	Determination	Threat Score
C:\Program Files (x86)\Google\GoogleUpdater\122.0.6234.0\	updater.exe	GoogleUpdater (x86)	Google LLC	Signature Verified (DigiCert)	N/A
C:\Program Files (x86)\Google\Update\1.3.36.352\	GoogleCrashHandler.exe	Google Crash Handler	Google LLC	Signature Verified (DigiCert)	N/A
C:\Program Files (x86)\Google\Update\1.3.36.352\	psmachine.dll	Google Update	Google LLC	N/A	Unknown
C:\Program Files (x86)\Google\Update\Install\{8AB249FA-8B24-4EC7-8A95-3D86120E81EA}\	120.0.6099.130_120.0.6099.129_chrome_updater.exe	Google Chrome Installer	Google LLC	Signature Verified (DigiCert)	N/A
C:\Program Files (x86)\Google\Update\Install\{D2998A74-FC17-44DB-BFBA-E447AB064063}\	120.0.6099.131_chrome_installer.exe	Google Chrome Installer	Google LLC	N/A	Unknown
C:\Program Files\FileZilla FTP Client\	filezilla.exe	FileZilla FTP Client	Tim Kosse	N/A	N/A
C:\Program Files\FileZilla FTP Client\	libfzclient-commonui-private-3-64-0.dll		Tim Kosse	Benign 0.00	N/A
C:\Program Files\FileZilla FTP Client\	libsqlite3-0.dll		Tim Kosse	Benign 0.00	N/A

Publisher Summary

Publisher	Count
VideoLAN	395
Wireshark Foundation	167
Google LLC	92
Mozilla Corporation	45
Tim Kosse	40
Notepad++	8
Spotify AB	7
Insecure.Com LLC	7
FabulaTech, LLP	7
Nmap Software LLC	5
WiX Toolset (.NET Foundation)	1

Software Tools: Auditor 8



ABC Company

1 September 2022

Reports and Summaries

Generated on: 1 September 2022 16:46

OVERALL SCORE 87%

Endpoints in Active Directory	678
Users in Active Directory	5139
Policies Audited	24
Controls Audited	93

PREVENTION: 60%

APPLICATION CONTROL 20%

Computers selected for Audit	99
Computers compliant for Audit	20

PATCH APPLICATIONS 90%

Computers selected for Audit	306
Computers compliant for Audit	278

CONFIGURE MS OFFICE MACROS 31%

Computers selected for Audit	99
Computers compliant for Audit	31

USER APPLICATION HARDENING 82%

Computers selected for Audit	125
Computers compliant for Audit	103

CONTAINMENT: 65%

PATCH OPERATING SYSTEM 86%

Computers selected for Audit	578
Computers compliant for Audit	497

RESTRICT ADMIN PRIVILEGES 80%

Users selected for Audit	85
Users compliant for Audit	68

MULTI-FACTORED AUTHENTICATION 17%

Users selected for Audit	4500
Users compliant for Audit	799

RECOVERY: 100%

REGULAR BACKUPS 100%

Computers selected for Audit	5
Computers compliant for Audit	5

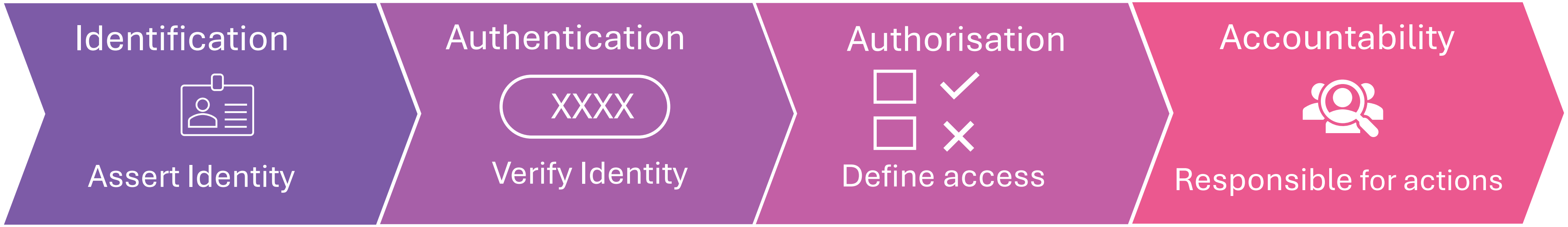
Re-assess your cyber maturity anytime

Full visibility

Easy-to-follow mitigation steps

Compliance reporting

Access Control



Identification

Assert Identity

Authentication

XXXX

Verify Identity

Authorisation

□ ✓

□ ✗

Define access

Accountability

Responsible for actions

Principle of Access Control

Knowledge

Ownership

Characteristic

Security Principles

- Asset inventory
- Principle of Least Privilege (PoLP)
- Principle of need-to-know
- Separation of Duties (SoD)
- Use complete controls wherever possible
- Logging and monitoring
- Don’t trust any network, including your own
- Choose services designed for zero trust

Thank You.

Essential Eight: An Implementation Journey.