QUARTERLY PARTNER BRIEFING · JULY 2026

Independently validated. Formally closed.

This quarter youX was certified against three ISO standards and had both regulatory reviews of the recent cyber incident formally closed — with no further action required. Here is where we stand, and where we are headed.

3× ISO

CERTIFIED JUNE 2026
27001 · 27017 · 27018

2 reviews

REGULATORY REVIEWS CLOSED
OAIC & NOCS · NO FURTHER ACTION

0 findings

MATERIAL FINDINGS THIS QUARTER
FROM 3.9M EVENTS

01 INDEPENDENT ASSURANCE — CERTIFIED THIS QUARTER

Three ISO certifications, achieved in June 2026

Independent, internationally recognised validation of our information security, cloud controls and personal-data protection — assessed and confirmed by external auditors this quarter.

ISO 27001

RECERTIFIED

:2022 · JUNE 2026

Information Security, Cybersecurity & Privacy Protection

ISO 27017

CERTIFIED

:2015 · JUNE 2026

Cloud information security — controls for cloud service environments

ISO 27018

CERTIFIED

:2019 · JUNE 2026

Code of practice for protection of personally identifiable information (PII)

02 THE ROADMAP AHEAD — ACCREDITATION & ASSURANCE

A commitment to continuous improvement

Building on the three ISO certifications secured this quarter, our accreditation programme extends through FY27 to add privacy, AI and business-continuity assurance — with SOC 2 staged alongside.

NOV 2026

ISO 27701:2019

Privacy Information Management

DEC 2026

ISO 42001:2023

AI Management Systems

SOC 2 Type 1

Controls design assurance

JAN 2027

ISO 22301:2019

Business Continuity Management

OCT 2027

SOC 2 Type 2

Surveillance period begins · accreditation expected Oct 2027

MDR ADVANCED · YEAR 1 MATURITY PROGRAMME WITH TRISKELE LABS

Assess & govern

Cyber Maturity Assessment
SEP–OCT 2026

36-month Prioritisation Roadmap
OCT 2026

Cyber Health Check Scorecard
QUARTERLY · FROM JAN 2027

Test & assure

Annual Penetration Testing
APR 2027 · 5 DAYS

Purple teaming
QUARTERLY · FROM OCT 2026

Threat hunting
JAN 2027

MFA & M365 Essentials review
FROM OCT–NOV 2026

Prepare & respond

Incident Response Plan
JAN 2027

IR tabletop exercise
JAN 2027

Data & Privacy review
NOV 2026 · LEGAL / IT RISK

BY THE END OF YEAR 1: A MEASURED, TESTED SECURITY PROGRAM — BASELINE ESTABLISHED, DEFENCES PROVEN AGAINST REAL-WORLD ATTACKS, INCIDENT RESPONSE REHEARSED AND READY. AN IR RETAINER & DFIR TOOLING ARE ALREADY ACTIVE TODAY. TIMELINES ARE INDICATIVE.

REGULATORY OUTCOME — CLOSED. CONFIRMED. RESOLVED.

Both regulatory reviews of the recent cyber incident have been formally closed.

These outcomes reflect the strength of our response and the controls in place across the platform. We are now in a clear and stable position to move forward with confidence.

OAIC Investigation

CLOSED

The Office of the Australian Information Commissioner has confirmed the investigation is complete with no further action.

NOCS Review

CLOSED

The National Office of Cyber Security has finalised its review. No further action required.

HOW THE CONTROLLED INCIDENT WAS HANDLED — EXISTING CONTROLS PREVENTED BROADER COMPROMISE

01

Identified

Unauthorised system-level access identified within a legacy hosted application environment.

02

Contained

Immediate containment actions and credential rotation initiated.

03

Investigated

Independent CREST-accredited forensic specialists engaged.

04

Operational

No service interruption. Segmentation prevented lateral movement throughout.

03 MARKET OUTLOOK — ASSESSED BY TRISKELE LABS

The threat landscape right now

What is active across Australian organisations of a similar size and profile, as assessed by our SOC partner Triskele Labs. Activity reflects the broader landscape — not a measure of youX's own exposure.

THREAT CONDITION	WHAT IT IS	ACTIVITY	RECOMMENDED CONTROLS
Ransomware & extortion	Malware that encrypts data and extorts payment	HIGH	Patching, offline backups, EDR, MFA
Phishing & social engineering	Deceptive email, SMS or voice to steal access	HIGH	Awareness training, mail filtering, MFA
Business email compromise	Impersonation to redirect payments or data	HIGH	MFA, payment verification, mail controls
Credential & MFA–bypass	Stolen logins and hijacked sessions	ELEVATED	MFA review, conditional access, login monitoring
Cloud & third–party exposure	Misconfiguration or vendor access in cloud / SaaS	ELEVATED	Config review, least privilege, monitoring
Insider & data exposure	Authorised access misused or data leaked	NORMAL	Access controls, DLP, dark web monitoring

> **Fundamental monitoring is in place, supporting defence against the majority of common threats today. The roadmap ahead builds the fuller picture — assessing governance, assurance and a tested response, and maturing them where needed.**

TRISKELE LABS · YOUX MANAGED DETECTION & RESPONSE BOARD REVIEW · JULY 2026

The SOC narrows millions of signals down to a handful

Read left to right — the SOC absorbs the month's activity and escalates only what genuinely needs the youX team's attention.

SECURITY MONITORING · SIEM & EDR

3.9M
Logs ingested & analysed
MANAGED BY THE SOC

→

212
Alerts investigated
NO ESCALATION NEEDED

→

6
Security tickets raised to youX

DARK WEB MONITORING

Continuous
Credentials & exposure watched 24×7

→

57
Alerts cleared as benign

→

1
Ticket raised to youX

BOTTOM LINE

In June, the SOC filtered the month's activity down to just **7 items** needing our team's attention — a normal level for an environment of our size. **None were material.**

7
ITEMS ESCALATED · 0 MATERIAL

05 PROTECTION IN PLACE TODAY

The services actively defending youX right now

Six live services run continuously from Triskele Labs' Australian sovereign SOC — 24 hours a day, 365 days a year.

24×7×365 MONITORING

SIEM / monitoring platform

Threats detected and triaged around the clock — intrusions, lateral movement, suspicious logins.

MANAGED EDR

Endpoint detection & response

Laptops and servers defended against ransomware, malware and endpoint compromise.

INTERNAL & EXTERNAL SCANNING

Vulnerability scanning

Weaknesses surfaced before they can be exploited — unpatched software, misconfigurations.

SOC-LED · TIER 1

Response & automation

SOC-approved actions contain threats fast — host isolation, account lockdown, rapid containment.

DARK WEB MONITORING

Exposure monitoring

Exposed credentials and leaked data flagged early — leaked passwords, brand abuse.

25-HOUR RETAINER · DFIR

IR retainer & DFIR tooling

Ready to investigate and respond if something gets through — forensics and recovery.

ACCESS CONTROLS

Restricted admin pathways · least-privilege review · credential rotation & secrets management.

INFRASTRUCTURE

Private network architecture · segmented environments · bastion-controlled access · encryption in transit, at rest & at application level.

DATA LIFECYCLE

Collect → encrypt → retain → archive → delete, with retention mapped by category and board-level oversight.

Platform investment designed to reduce your risk

Speed with security

Platform improvements delivered quickly, without compromising the security posture that protects your business and your customers.

Continued investment

Ongoing investment in Australian-hosted infrastructure, layered encryption and advanced monitoring capability.

Transparency

We keep our partner network informed as improvements are implemented. You will not be left guessing.

Direct access

Our leadership team remains directly accessible and accountable. If you have questions, we want to hear them.

youX

These outcomes reflect the strength of our platform and the controls behind it. We are in a clear, stable position to move forward with confidence — and we will keep you informed every quarter.

Simon Penhaligon
CHIEF EXECUTIVE OFFICER

NEXT UPDATE

October 2026

ISSUED BY

Drive IQ Technology Pty Ltd T/A youX Powered
ABN 40 638 678 136 · Sydney, Australia