

CONFIDENCE AMID CHAOS

Managing Fraud and Scams with Data and Analytics

AUSTRALIA

The LexisNexis® Risk Solutions Cybercrime Report

The global digital fraud attack rates continued climbing in 2023, increasing 19% year-over-year. Automated bot attacks remained stable after last year's surge in attack volume. Here's a snapshot of the cybercrime landscape in Australia.

Transaction and Attack Patterns in Australia

TRANSACTIONS ANALYZED

HUMAN-INITIATED ATTACKS



755M

5M

AUTOMATED BOT ATTACKS



19M

Transactions by Channel

DESKTOP / MOBILE



MOBILE BROWSER / MOBILE APP



Attacks by Channel

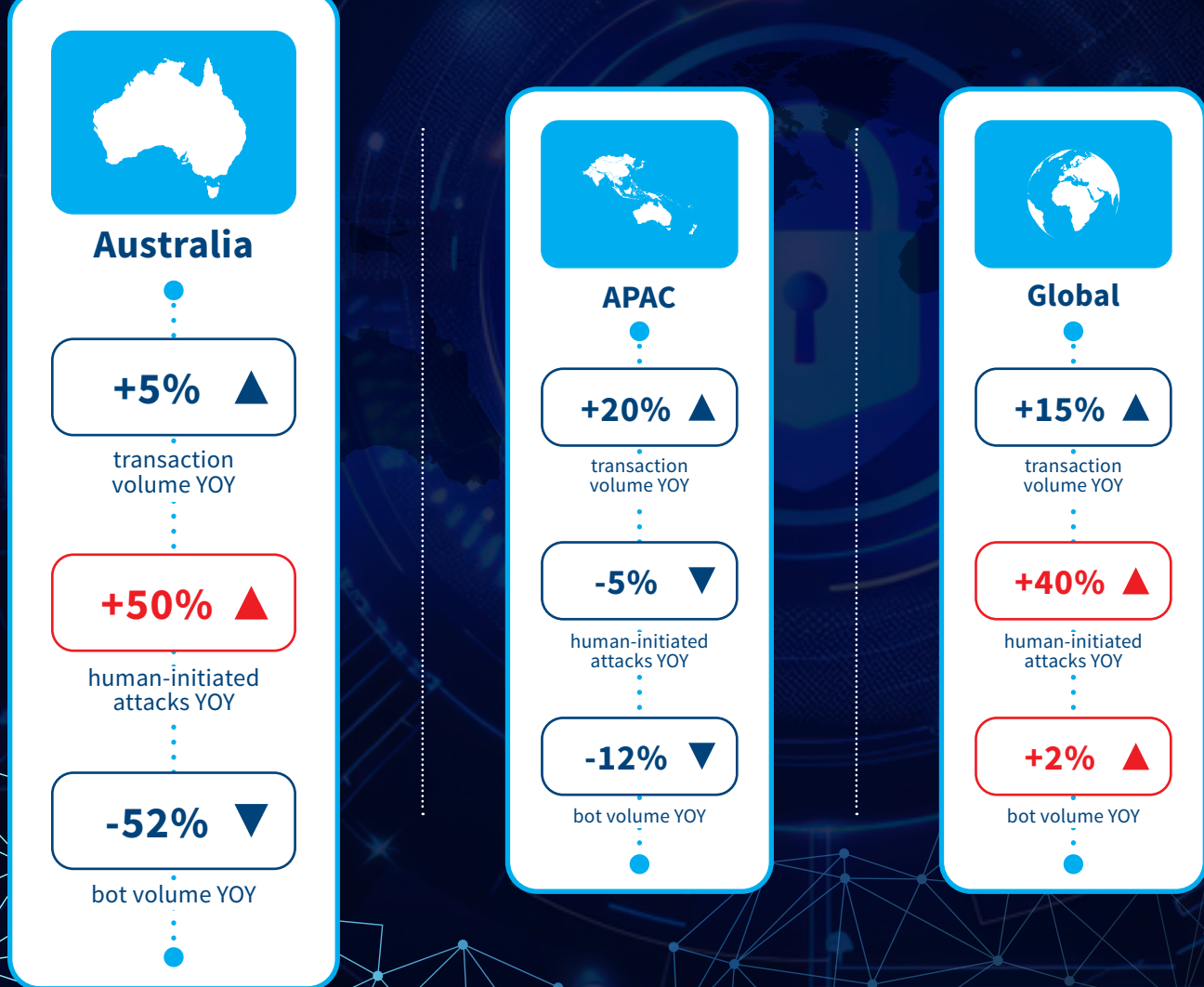
DESKTOP / MOBILE



Percentage of attacks coming from mobile devices has increased YOY
16% ▲

Spotlight: Australia vs. APAC vs. Global

Transaction volume in Australia has increased modestly compared to the rest of the world and APAC. While bot attack volume has decreased significantly, there has been an equally significant increase in human initiated attacks.

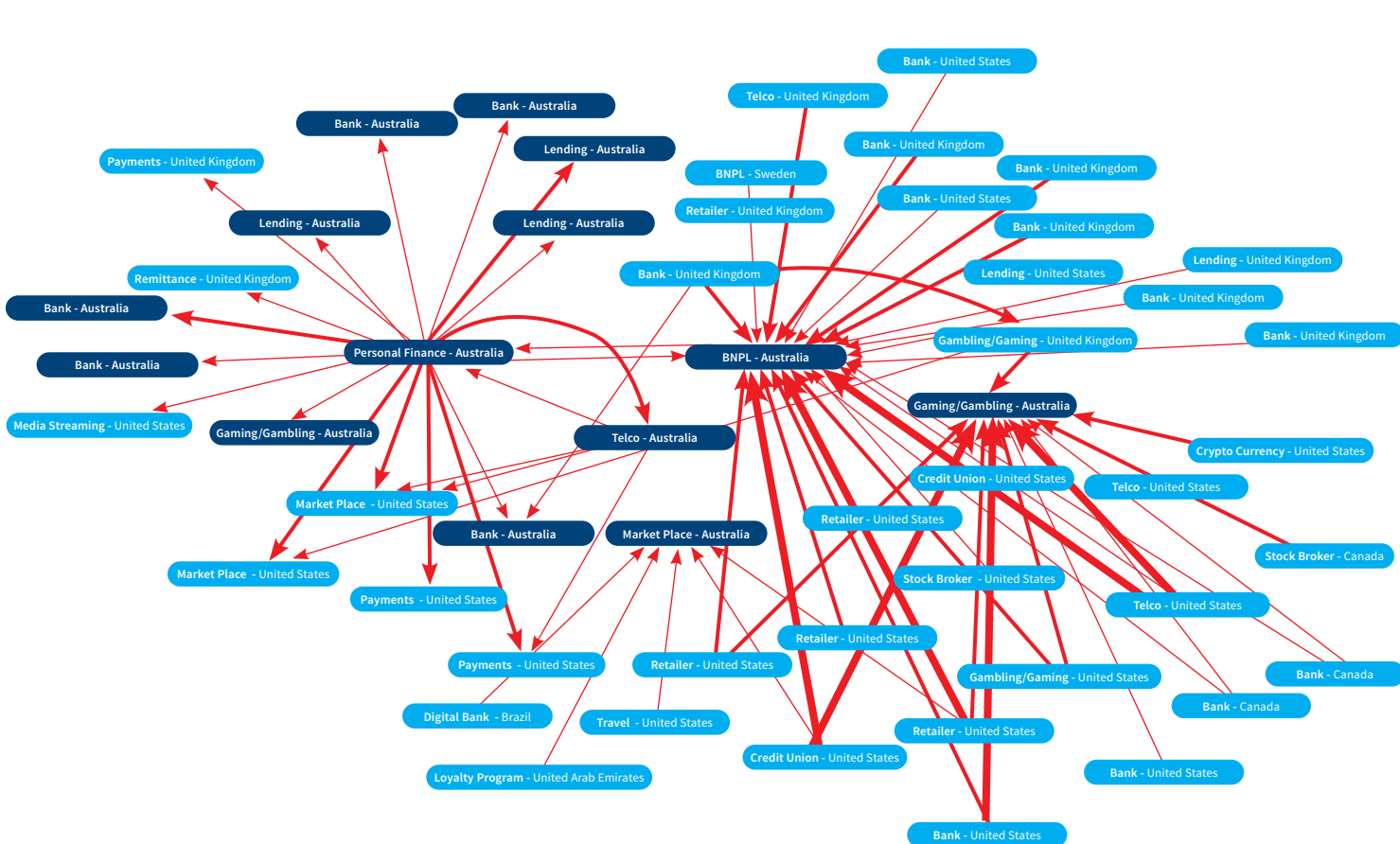


Networked Fraud Threats

This visualisation shows networked fraud (linked by digital identity) connected to organisations operating in Australia during the last quarter of 2023.

Each circle represents an individual organisation. Each arrow illustrates digital identities associated with confirmed fraud attempts at one organisation, crossing over to another organisation within the LexisNexis® Digital Identity Network®. A thicker line denotes a higher volume of attacks.

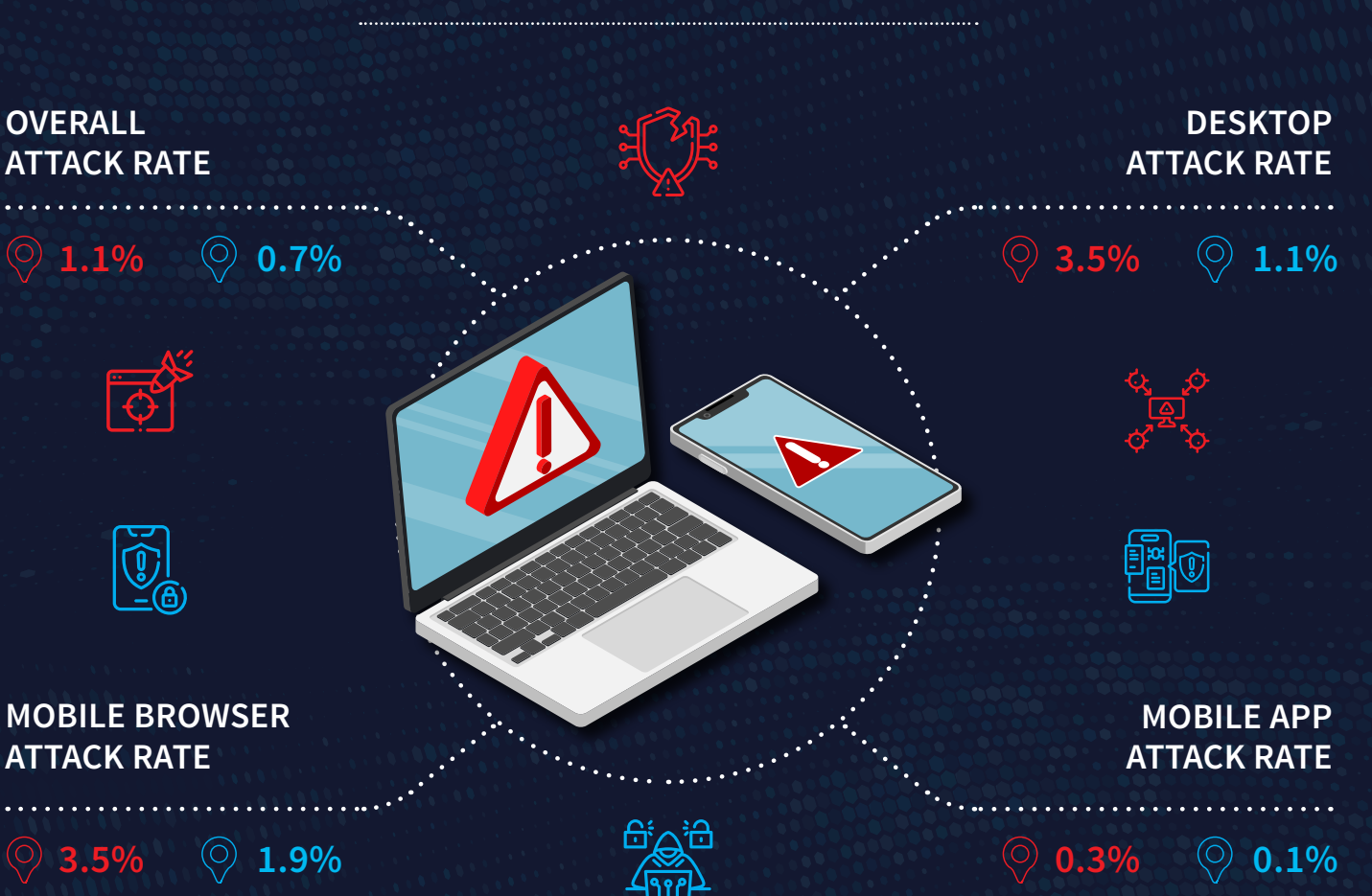
It shows that activity across organisations, sectors and borders has increased despite the relatively steady transaction volume.



A thicker line denotes a higher volume of attacks.

Australia's Fraud Patterns Compared to APAC

APAC AUSTRALIA



For further insights, download the LexisNexis Risk Solutions Cybercrime Report at risk.lexisnexis.com/global/en/insights-resources/research/cybercrime-report