

Fraudy

Our Cyber Fraud Protector

Meet Fraudy, The Cyber Fraud Protector

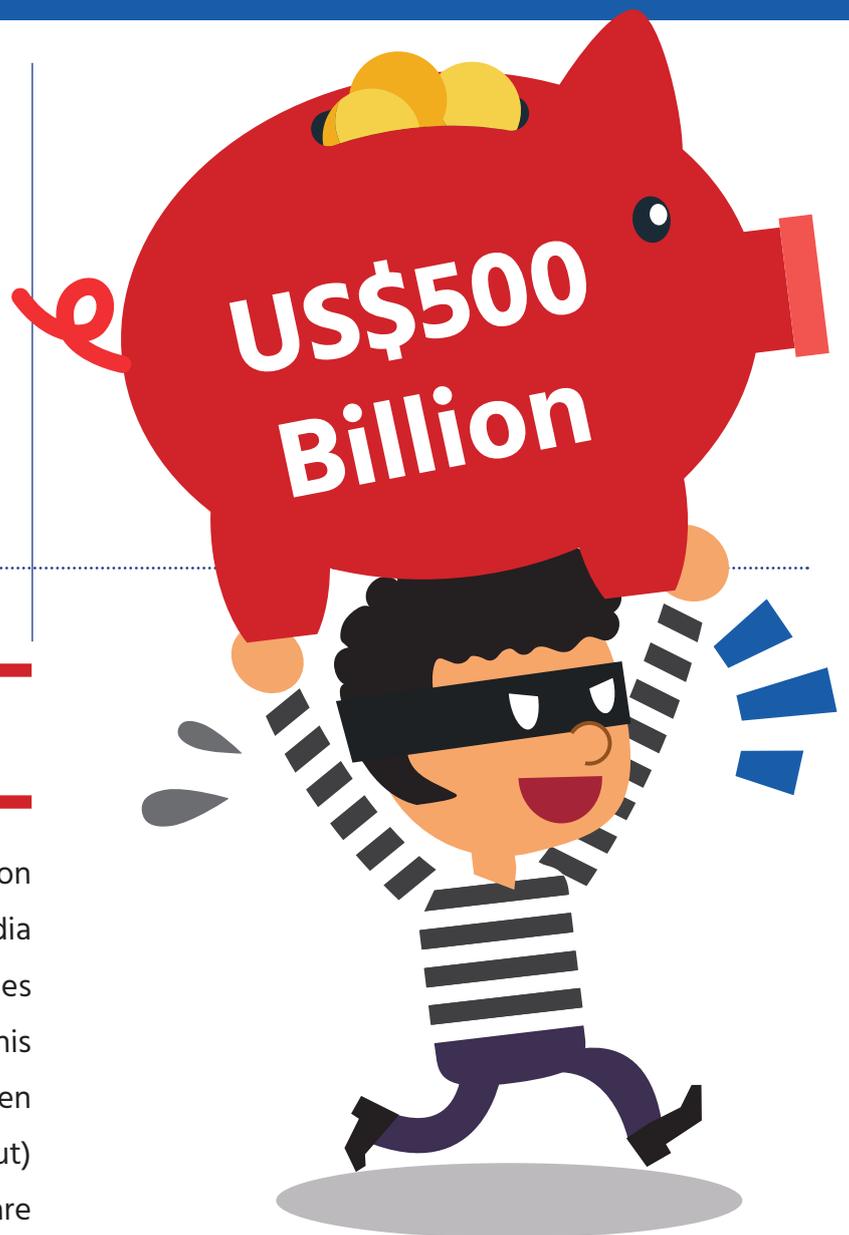
Fraudy grants companies ultimate visibility unto attempts at fraud activities; scanning the open, dark, and deep webs in real-time, for various types of fraudulent activities. Fraudy enables businesses to be proactive in their digital fraud detection; flagging incidents of fraud as they appear in the cyber space.



Fraudy's work is a critical asset to enterprises in our times, as stats show a continuous growth in cyber fraud. Threat actors and criminals use social media platforms and secondary markets (on the dark and open web) to carry out these fraudulent activities which include: scam campaigns, fake vouchers, Intellectual Property theft, account/ID take over and more.

Fraudy outsmarts these threat actors with new thinking that redefines your fraud prevention cybersecurity strategy.

According to Forbes magazine, cybercrime costs business as much as US\$500 billion a year.



How Fraudy Does it?

Fraudy's real-time intelligence collection on the Darkweb, monitoring of social media and tracking of secondary markets catches attackers in their tracks. Together with his team of specialists, Fraudy knows when criminals are attempting (or carrying out) to engage in fraudulent activities, or are acquiring tools or 'selling off' stolen data.

► The Technology Behind Fraudy

Fraudy uses CyberInt's Argos platform to build a level of protection that the hackers can't beat. Argos allows Fraudy to automate 90% of his work in tracking the bad guys. Working closely with his team of cyber analysts, the CyberOPS team, Fraudy can provide you with both indications and mitigations of fraud in real time.



◀ Threats Prevented by Fraudy

Every business is threatened by the risk of cyber fraud; a risk which is uniquely defined by each individual business's digital footprint and online interactions.

Fraudulent activities like scam campaigns, black markets, stolen credit cards and hijacked accounts are common in the thriving cyber fraud landscape.

In order to cut losses and protect customers, companies must take a proactive stance in detecting these fraudulent activities and mitigating them in real-time.