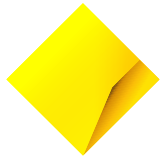
MIKE LAYTHAM

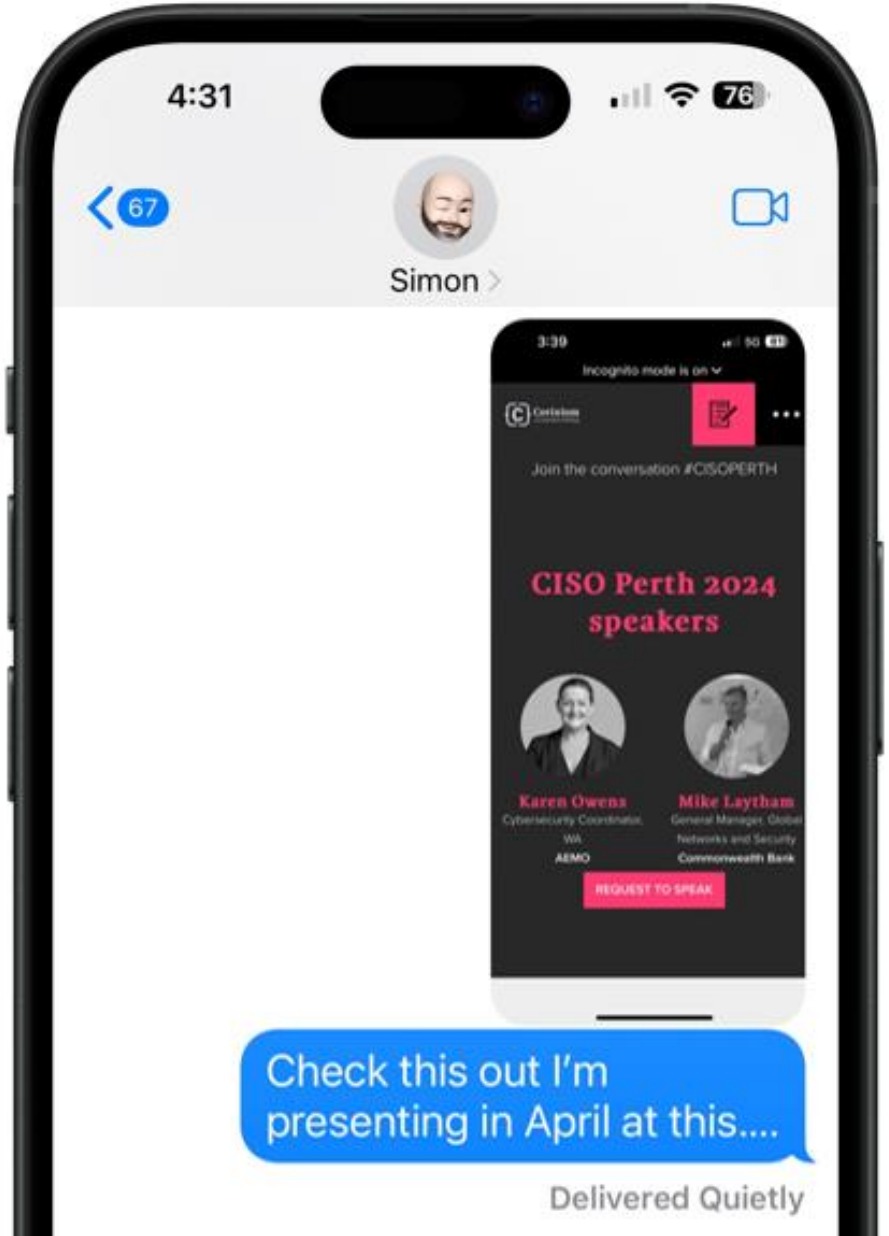
Engineering General Manager

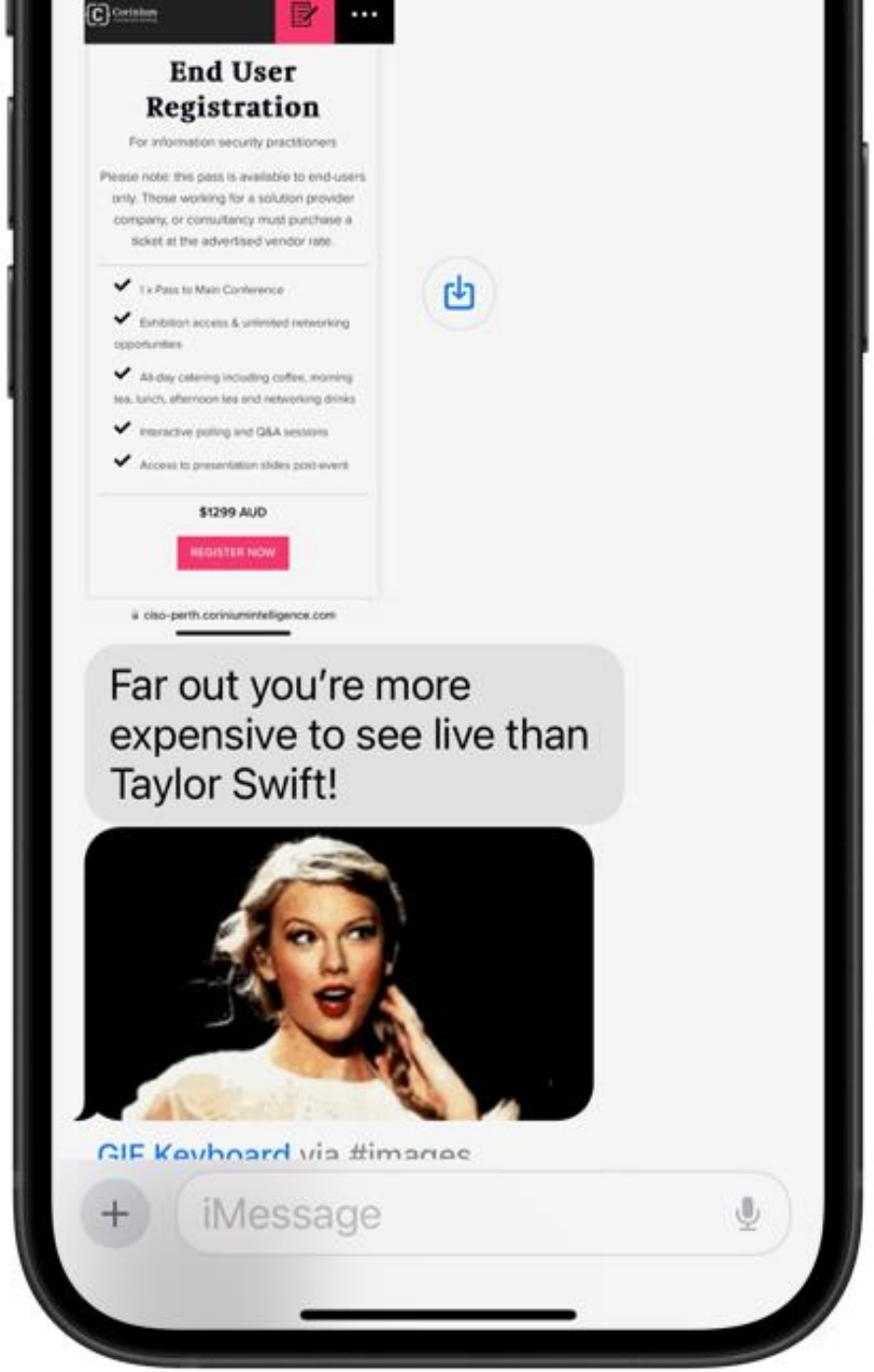
CBA Global Networks/Security & Bankwest Technology



Commonwealth Bank

Blank Space


4:31
67
Simon
Join the conversation #CISOPERTH
CISO Perth 2024 speakers
Karen Owens
Mike Laytham
REQUEST TO SPEAK
Check this out I'm presenting in April at this....
Delivered Quietly


End User Registration
For information security practitioners
$1299 AUD
REGISTER NOW
Far out you're more expensive to see live than Taylor Swift!
iMessage

About me

Military Aircraft Engineer

Flight Simulations On Linux

Banks Across The Globe

Astrazeneca Global Tech Platforms

Start Ups & IT Businesses

Go To Oz

BANKWEST
General Manager of Technology Platforms
Networks & Security
Cloud/hosting
Mainframe
Digital Workplace
Service Management

COMMONWEALTH BANK
Engineering General Manager for Commonwealth Bank Global Networks and Security
Reporting into the Group CTO
Cyber Leadership Team

Availability and security go hand in hand

> You have the most dangerous job in the bank

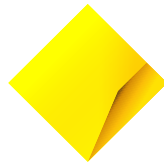
Bob Bigman

Former CIA - Chief Information Security Officer (CISO)

They want Mach 10?
Let’s give them Mach 10

Size of the Prize

42



Size of the Prize

EVERY DAY !!!

42%

of the Australian economy goes through CBA

$16,000,000,000,000.00

($16 Trillion Dollars)

1.8 **billion** transactions just mobile app

22 **million** customers

Cyber

108,682,056,364

Signals analysed

210,000,000

DDoS Blocks

EVERY MONTH

Biggest deltas on DoS requests last month

Don’t think, just do.

Can’t see the wood for the trees

paloalto NETWORKS

CISCO

Symantec

Microsoft

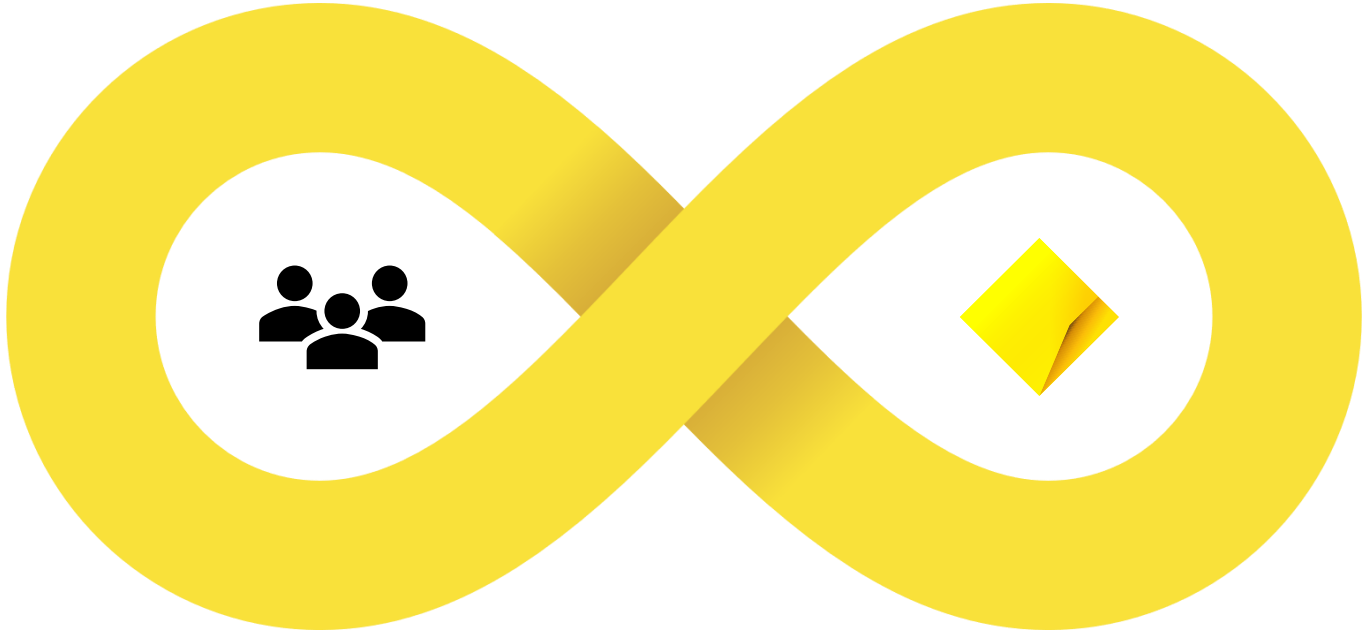
FIREEYE™

McAfee™

AIRLOCK DIGITAL

JUNIPER NETWORKS

Partners that play well together



People over dramatize

Get the basics right

72 minutes

Average time from click to being in the system

99% **99%** Basic security hygiene still protects **99%** of attacks

The Basics

- Enable multifactor authentication (MFA)
- Apply Zero Trust principles
- Use extended detection and response (XDR) and antimalware
- Keep up to date
- Protect data

*Microsoft Digital Defence Report - October 2023

Tech Lifecycle Management

Asset identification – can’t fix what you don’t know

Can’t leave it until the last minute – Decision process

Otherwise struggle to patch

3 Year view - End of Life & End of Support

3 MONTHS — Architectural design decisions

3 MONTHS — Contract negotiations

18 MONTHS — Swap key capabilities

<30 days Patching

unless zero day

Move to fully automated

at a business service level not a server

Traditional thinking

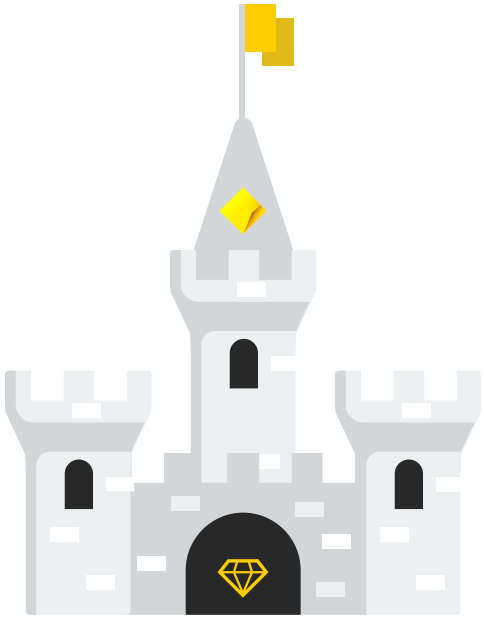
Datacentre

Traditional security tools

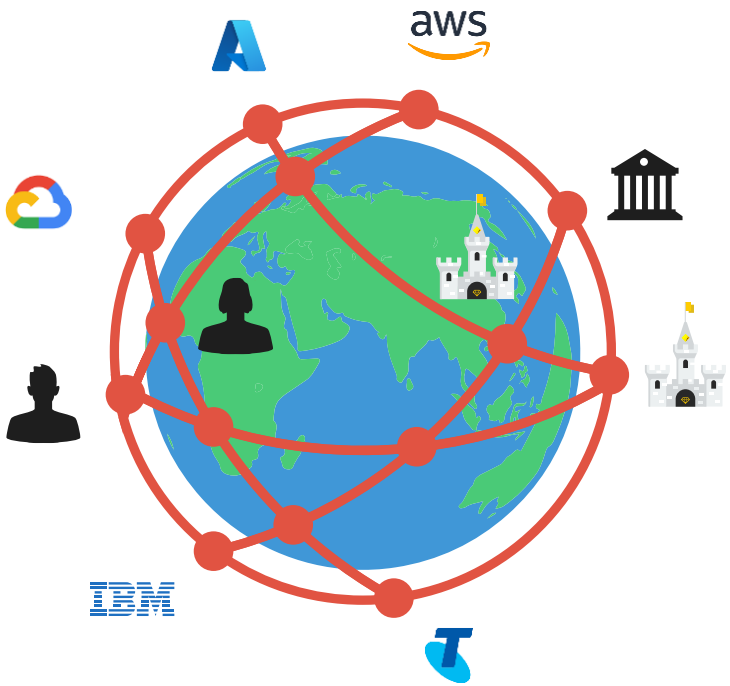
- Keep unauthorised out
- Not track and protect data
- OK as data didn’t go anywhere

No longer a Datacentre

In 2023 **47%** of all data breaches in organisations originated in the cloud



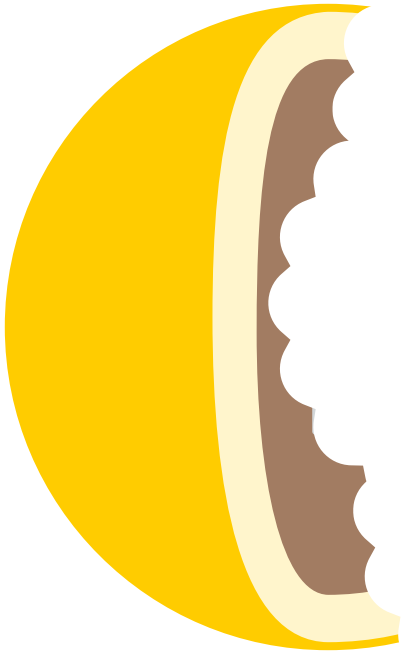
Datacentre



Data estate

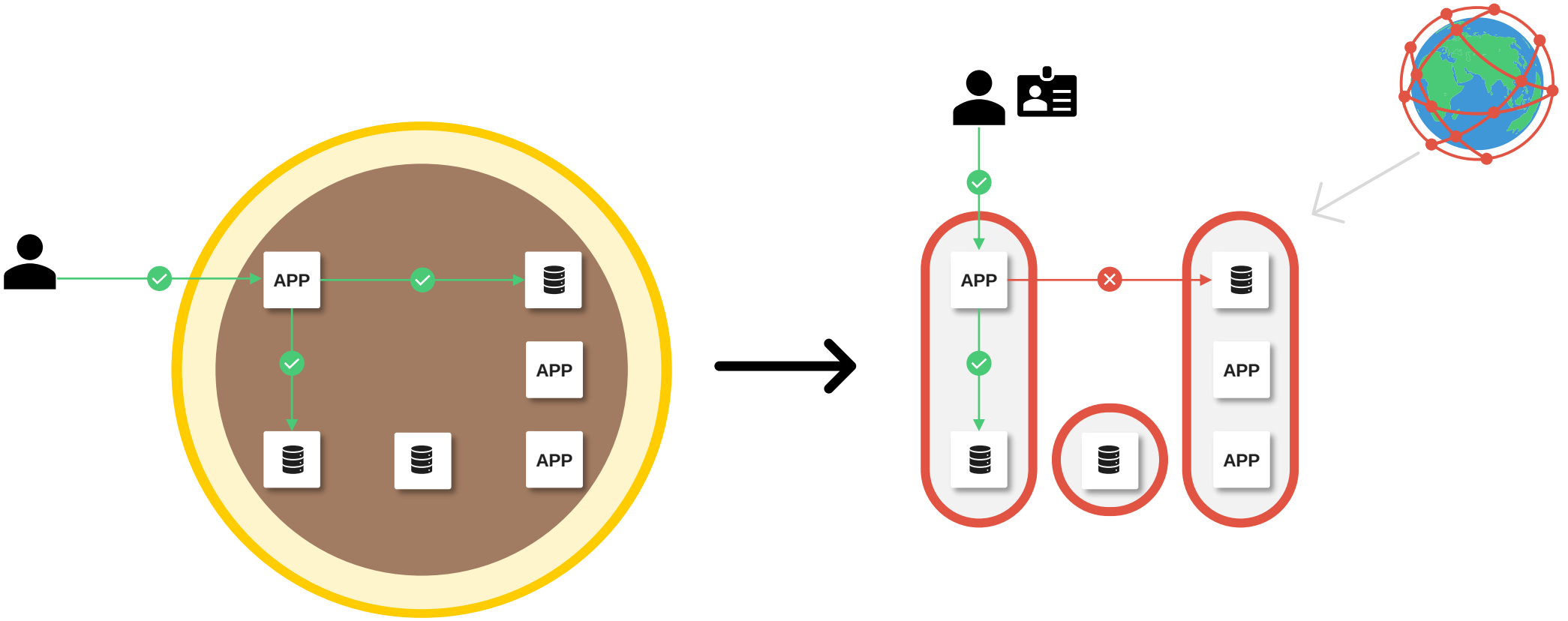
Crunchy M&M – Nom Nom Nom

Nice secure exterior wrapped around all the nice goodness



...but once you get through it you've got the lot

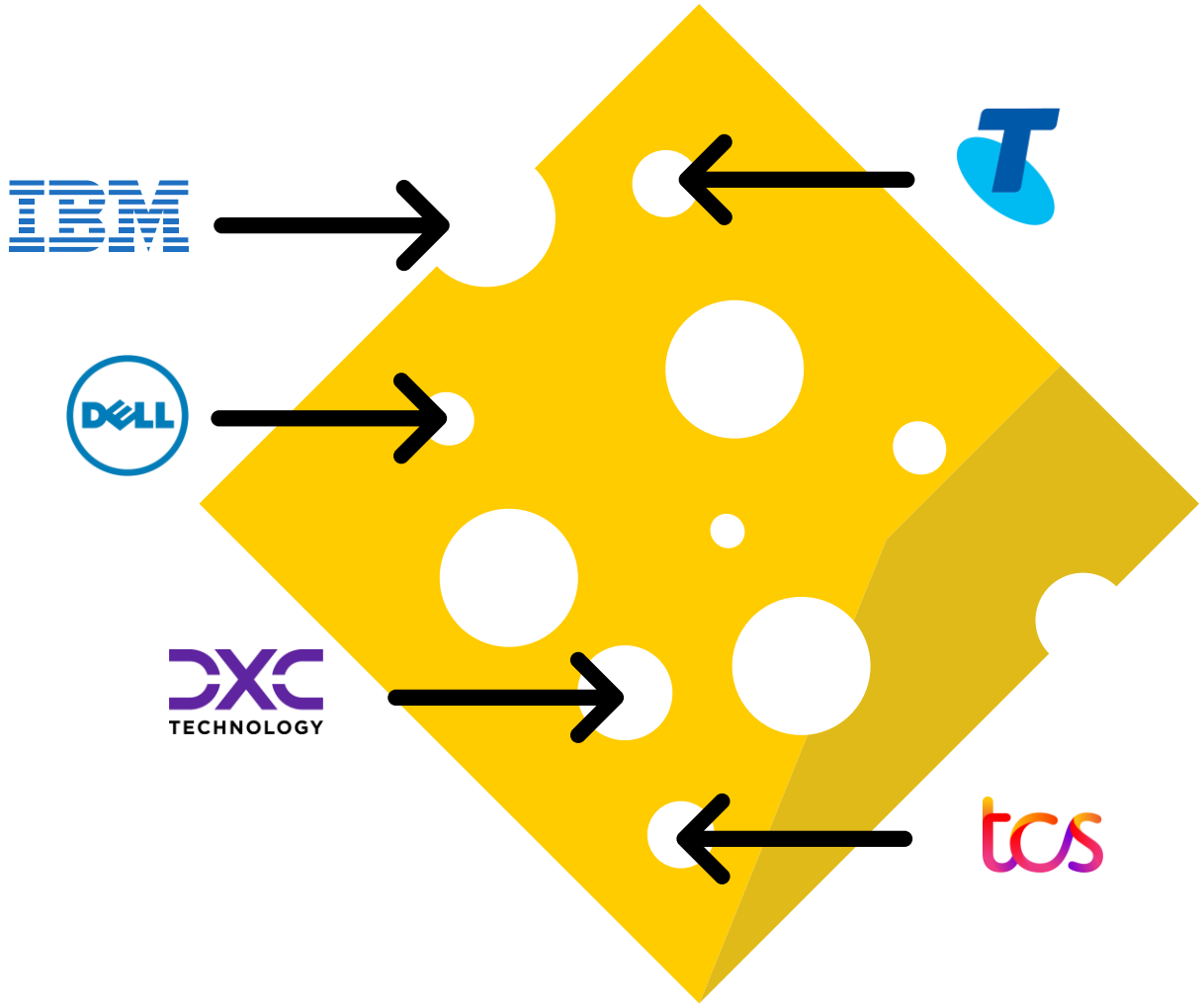
Identity is the new perimeter – Zero Trust



TRADITIONAL
Access enforced by firewalls and policy enforcement controls

MICRO SEGMENTATION
Access enforced by secure segmentation and individual control points around critical assets

Swiss cheese



One entry point

OUTCOMES

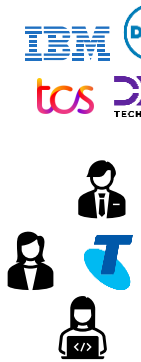
OBSERVABILITY

VERIFIABILITY

AUDITABILITY

3RD PARTY VENDORS

NEED ACCESS
TO WORK ON OUR SYSTEMS



STRUCTURED ENTRY

SINGLE
ENTRY POINT FOR **HIGH RISK**

ROBUST CYBER CONTROLS

PAM
PRIVILEDGED ACCESS MANAGEMENT

MFA
MULTI-FACTOR AUTHENTICATION

DLP
DATA LOSS PREVENTION

SECURE CONTROLLED ZONES

JUMPHOST
CONTROLLED

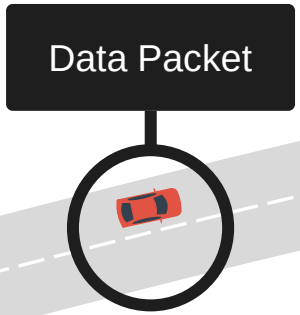
WE DO KNOW

WHO
has logged in

WHEN
they log in

WHAT
they are doing

How do we know what is going on now?



What we'd need to know

- How many and what type?
- Where are they coming from and going to?
- What road are they using?
- Do they hold a VIP? Is it bullet proof?
- Should the cars be going from here to there?
- Has a car suddenly started driving?
- Can we verify cars go to places they shouldn't?

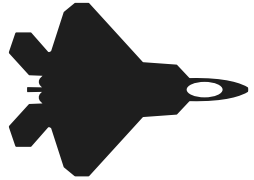
Creating a digital twin

Network Graph, compares the observed state with the declared state of the network, identifying anomalies

- Complete visibility of the network in near real-time
- Spotting of anomalies – Prod connected to Dev
- Identifying insecure protocols being used - ftp, telnet...
- Strengthen Cyber defence
- Grounding for Generative AI
- Know the impact of change – Risk - Blast zone
- Accelerated cloud migration & reduced outages
- Faster decommissioning of assets

70 Billion packets of data ingested every day and increasing

I feel the need, the need for speed



Manual is too slow and complex

Security must operate at machine speed

Firewall burns

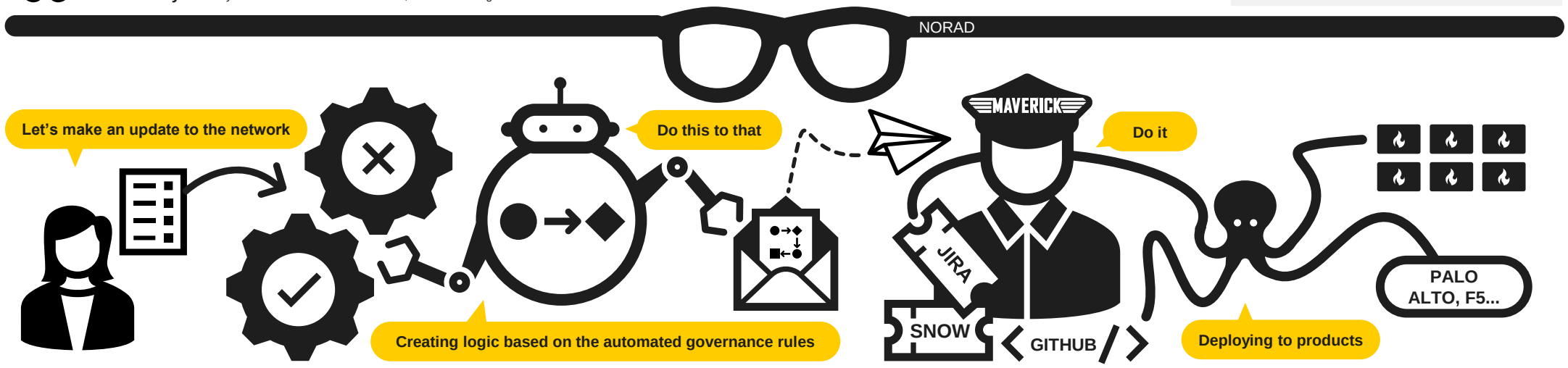
Patching

Detection

Automating our Network Services

Observability Visibility of the whole CBA network before, after and during

Observe network traffic, relationships, flows and protocols



Request
A request is made for a technology change

Make updates to network

Automated Governance
The request is checked against governance rules

Only an app can talk to a database

Governance Bot
The logic for the governance rules are applied

Connect application to the database

Payload
The directions of the logic are packaged together and sent

Logic for firewall changes packaged

Automation Framework
The directions are deployed and enforced

Create work tickets and get code

Deploy
The outputs are then deployed to the products

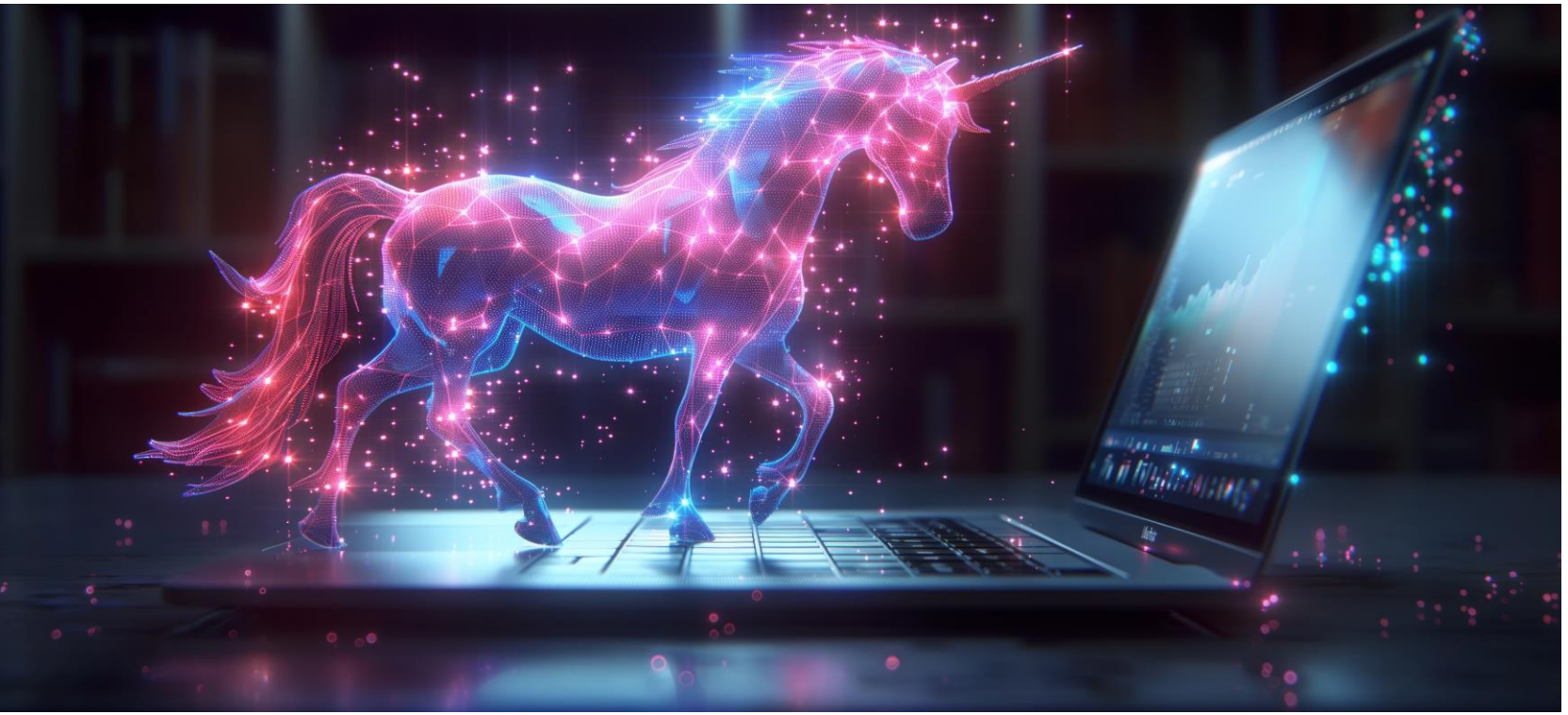
Deploy update to the firewalls

Product Endpoint/s
Changes to the products are made inline with the request

Firewalls updated

Talk to me Goose.

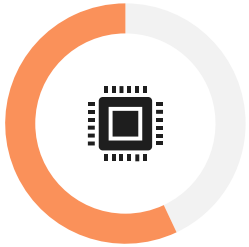
Can’t think about cyber in isolation



- Availability
- Customer experience
- Security
- Financial Management
- Risk & Impact

What worries me

The proliferation of digitisation of the world is the worry



57% of OT devices use firmware versions exposing them to more than 10 CVEs.
firmware reducing exploitable CVEs has been available for more than **10 years**
Imagine replacing the word OT with IT – what would you do?

1 in 3 IoT devices with known vulnerabilities on customer networks can't be patched

1 in 4 OT devices on customer networks use unsupported systems

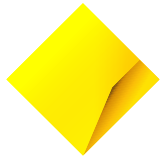
The number of DDoS-for-hire platforms continues to rise, with **20%** having emerged in the past year alone

Cyber has moved on from laptops and servers to **any entry point**

*Microsoft Digital Defence Report - October 2023

> This is a nice moment, let’s not ruin it

Thank you



Commonwealth Bank