



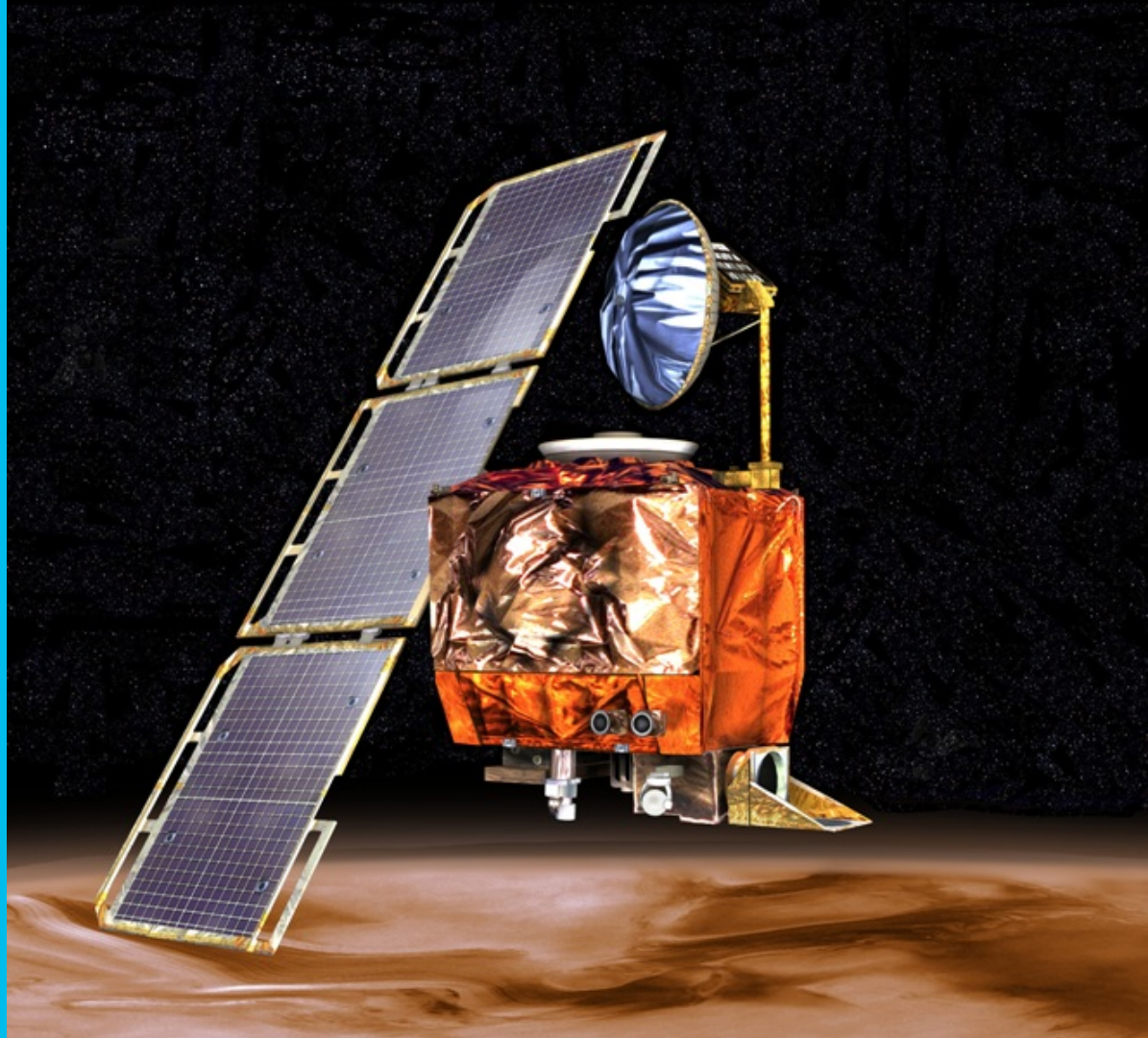
Is That Really You?

The Importance of Identity in BR&R

Richard Dean
CX Security Specialist
2nd June 2019



A (4.45x)
blast from
the past



EITHER
OR

“ There are two types of companies: those who **have been hacked**, and those who **don't yet know** they have been hacked^[1]

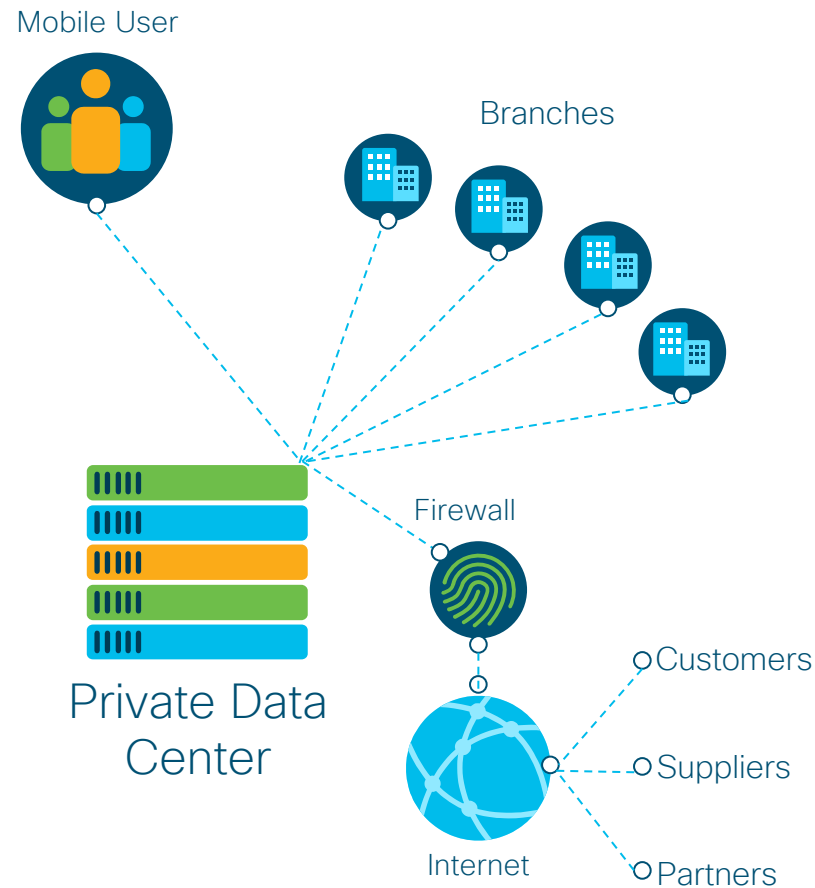
[1] John Chambers, "What does the Internet of Everything mean for security?" WEF, January 21, 2015.

CONTROL TO VISIBILITY

“ Enterprises are transforming their security spending strategy in 2017, moving **away from prevention-only** approaches to focus more on **detection and response** [2]

[2] Gartner: <http://www.gartner.com/newsroom/id/3638017>

THE GOOD OLD DAYS





TODAY'S SECURE, VIRTUAL ARCHITECTURE

Zero Trust | An Aside



A Zero Trust (ZT) architecture abolishes the idea of a trusted network inside a defined corporate perimeter. ZT mandates that enterprises create micro-perimeters of control around their sensitive data assets to gain visibility into how they use data across their ecosystem

1

Who | Securely identify the user

2

What | Securely identify the device

3

Where | Remove trust from the network



Who



Who

MFA



Who



Protect AD

et al.

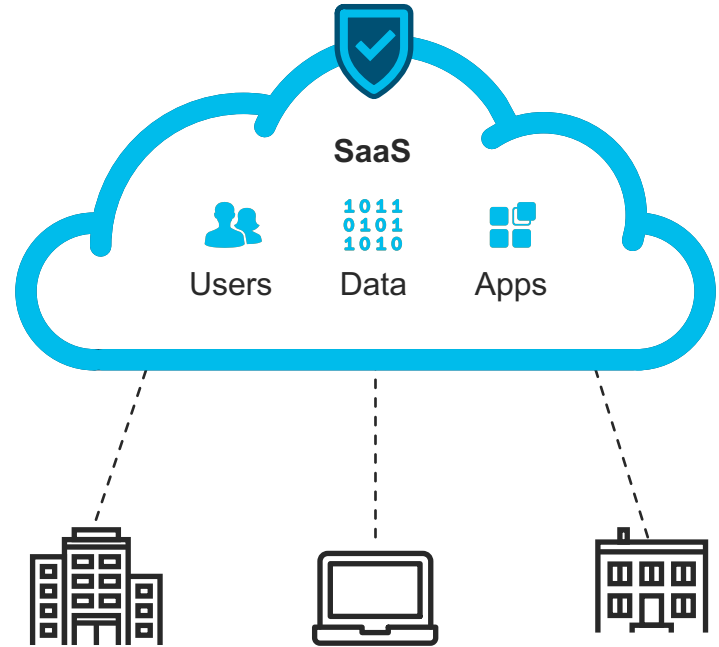
What



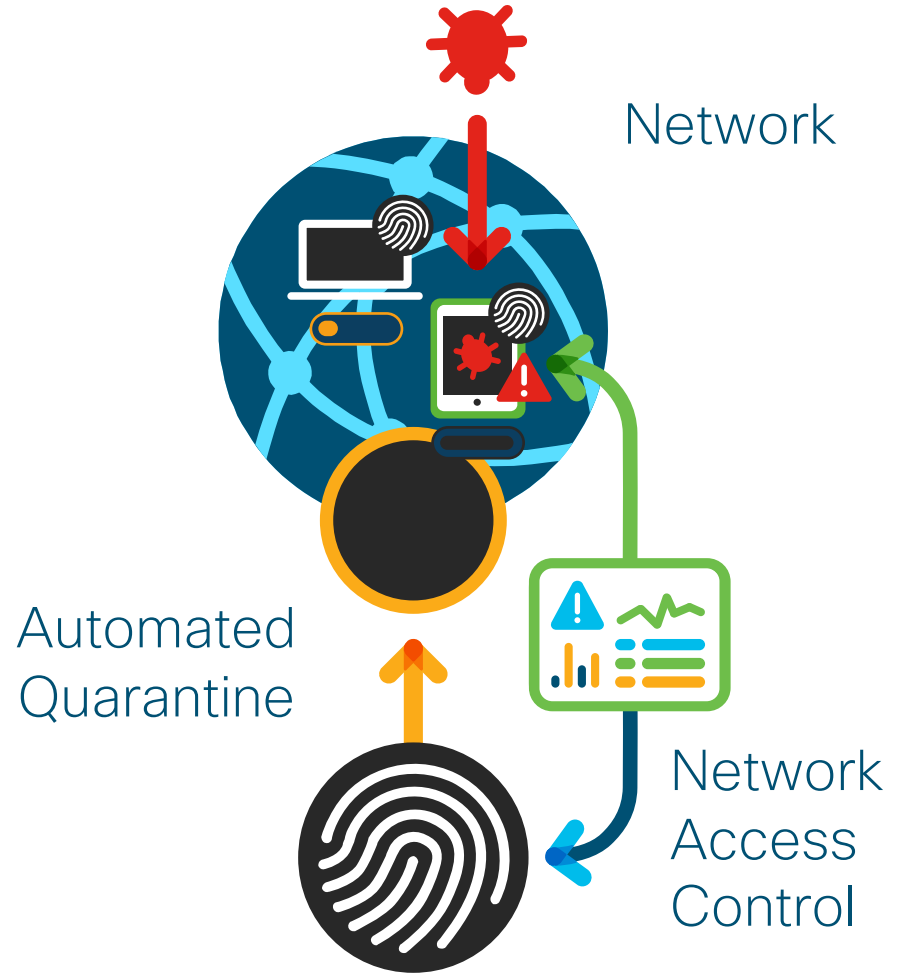
CATS : ALL YOUR BASE ARE BELONG
TO US.

Where

Cloud Access Security Broker (CASB)



Where



Breach Analysis

- 1 Who
- 2 What
- 3 Where

“ In over 50% of cases, logging will be insufficient to determine root cause, identify actions or attribute the actor

Cisco Incident Responder referring to initial state before pro-active work began

Key Points

- 1 MFA is Key – speak to DUO
- 2 Get a Zero Trust Strategy
- 3 Understand Your Data
- 4 Understand User Identity
- 5 Make sure you Log

Questions?



A (4.45x)
blast from
the past

