RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

CHANGE

Challenge today's security thinking

SESSION ID: SPO-R05A

IoT, the Next BYOD—Will We Make the Same Mistakes?

Greg Day

VP & Chief Security Officer, EMEA
Palo Alto Networks

Twitter: @GregDaySecurity

Linkedin: https://uk.linkedin.com/in/gregday

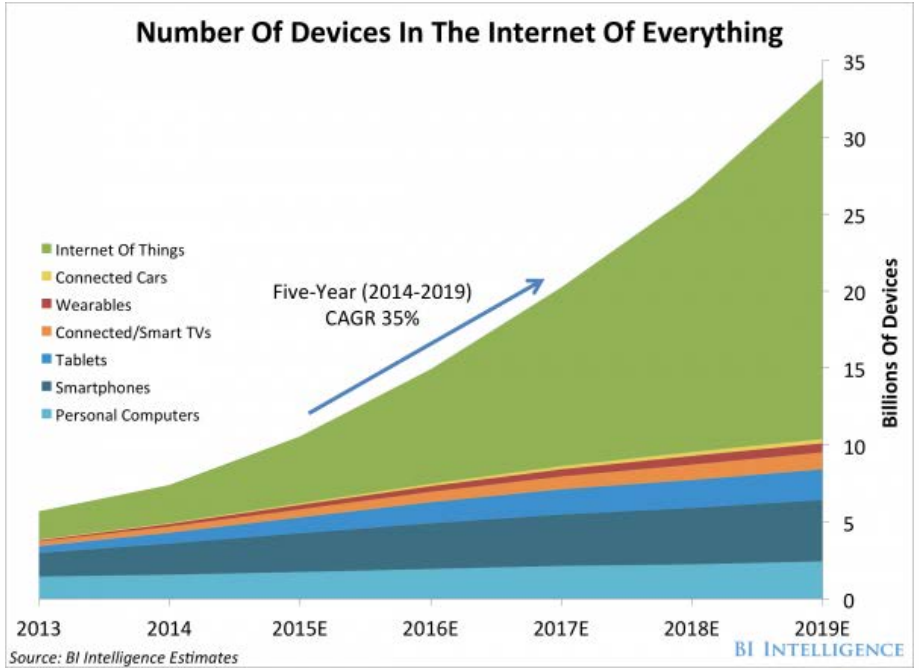
CxO business concerns for 2016

1. Internet of Everything – creeping into the business without right strategy & policies.
   - Top threat discussed were DDoS ransoming & loss of control and associated impact.
2. Security has already failed - RSA conference took this as the key takeaway.
3. Operating in restricted markets – China and Russia, etc - concerns of IP control.
4. Threat Intel – useless or valuable?
5. Insider Threat - how to detect this before it has impact?
6. Cyberwarfare techniques – getting caught in the crossfire and should they be developing their own offensive capabilities (e.g. disrupting the attacker).
7. Skills shortages - need to be as smart as the adversary and as dynamic.

Why? - 2015-2025

- 50% Enterprises adopt M2M tech (2015)
- 171mn wearable's will sold in 2016 (28% adoption)
  - Top being fitness & smart watches
- 1.9Bn home devices (2019)
- 50bn IP enabled things (2020)
- 90% of cars connected (2020)
  - 95mil telematics enabled cars (2025)
- Approx. 73% of revenue

  healthcare &manufacturing (2025)



http://www.ironpaper.com/webintel/articles/internet-things-market-statistics-2015/#.VieqzdZjp94

http://www.cmo.com/articles/2015/4/13/mind-blowing-stats-internet-of-things-iot.html

http://info.csgi.com/m2m-internet-of-things

Societal impact - Telematics

- 54.5 million units in 2020*
- Convergence - Connecting systems
  - iOS9 Apple CarPlay
  - Lollipop (5.0) Andriod Auto

Hacking cars

- 2013 - Toyota Prius & Ford Escape
- 2015 - Jeep

- http://www.telecomstechnews.com/news/2014/sep/19/car-telematics-subscribers-to-reach-1589m-by-2020/

Enabling IoT in business

We've been conditioned to think in terms of opposites

Sunrise

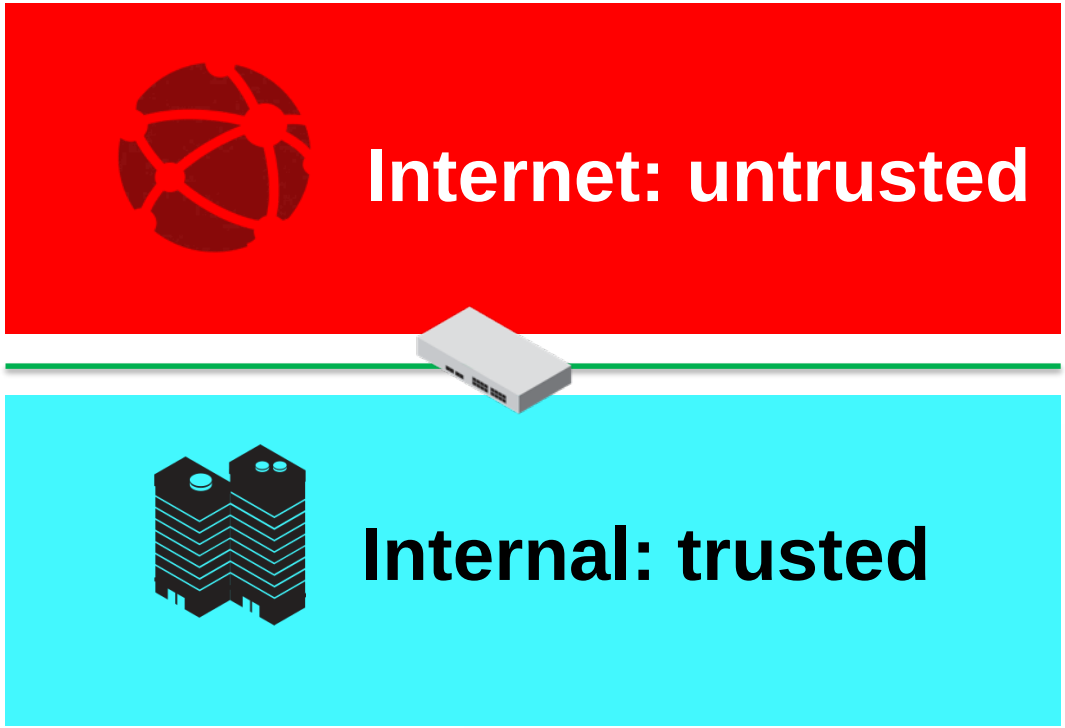
Moonrise

Do opposites create balance?

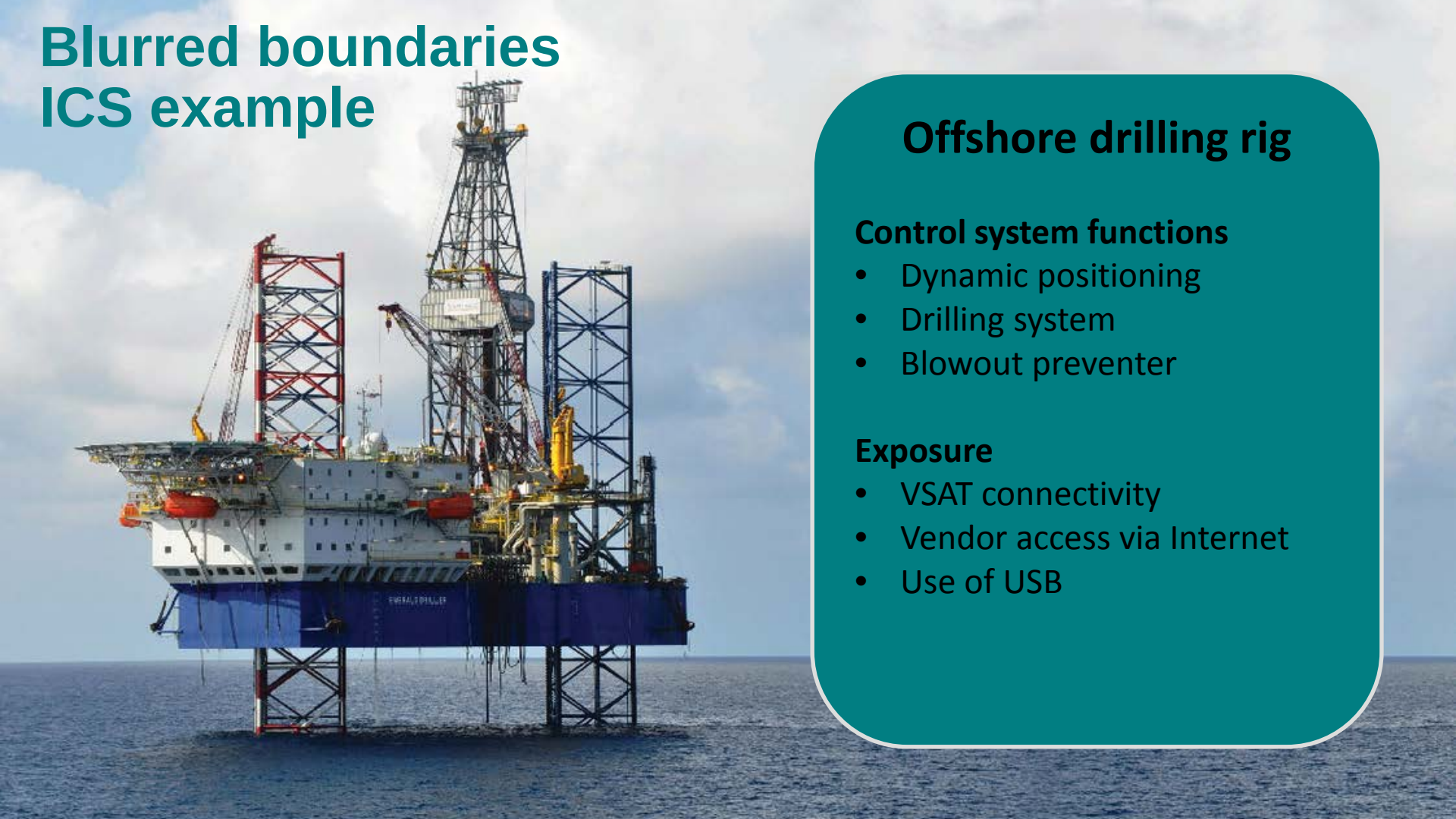
Sith

Jedi

The same goes for the way we design networks



Blurred boundaries
ICS example



Offshore drilling rig

Control system functions

- Dynamic positioning
- Drilling system
- Blowout preventer

Exposure

- VSAT connectivity
- Vendor access via Internet
- Use of USB

IoT drives a playground of bad behavior on trusted networks

Malicious / vulnerable devices

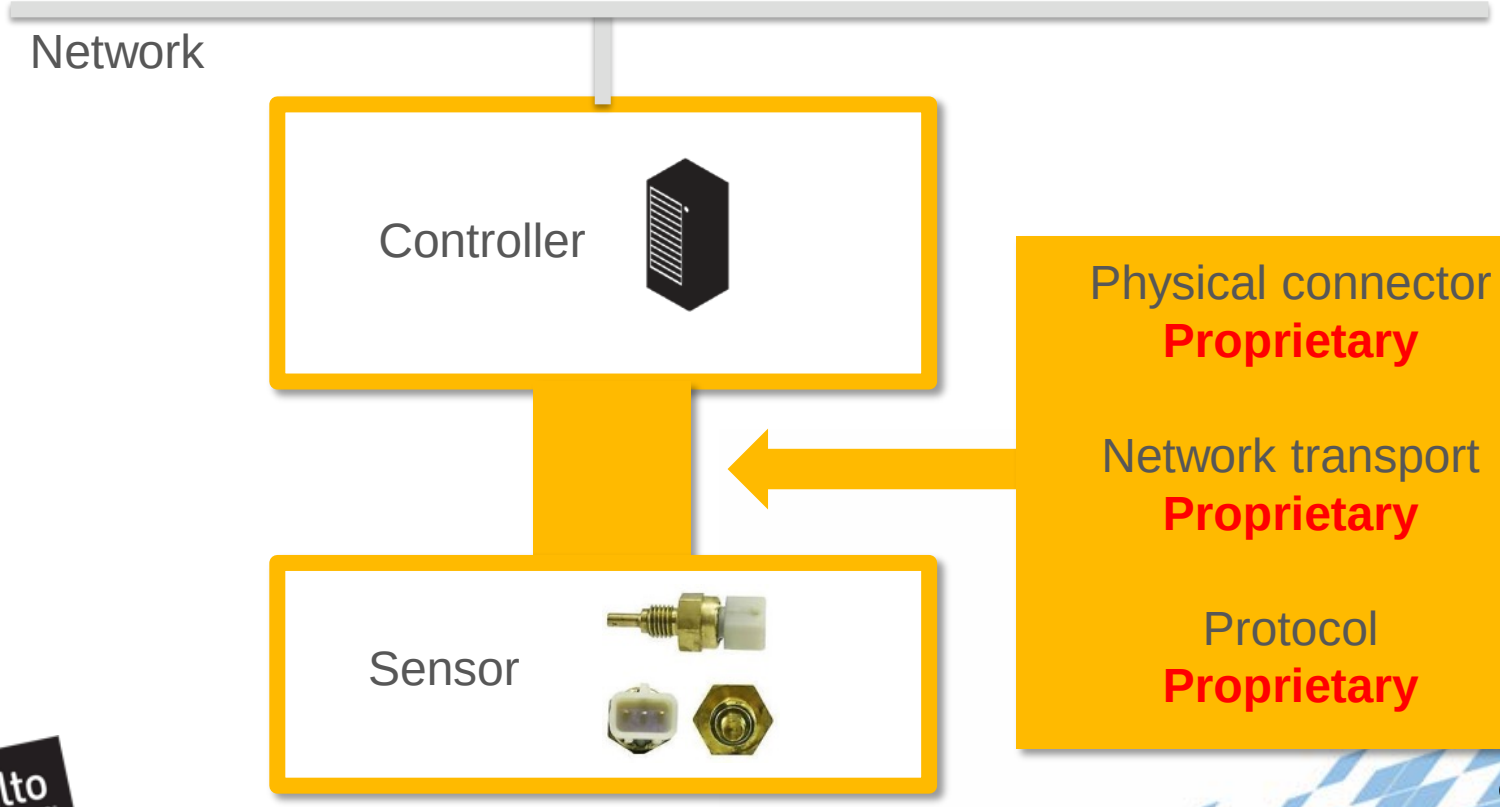
Unauthorized use

Volume

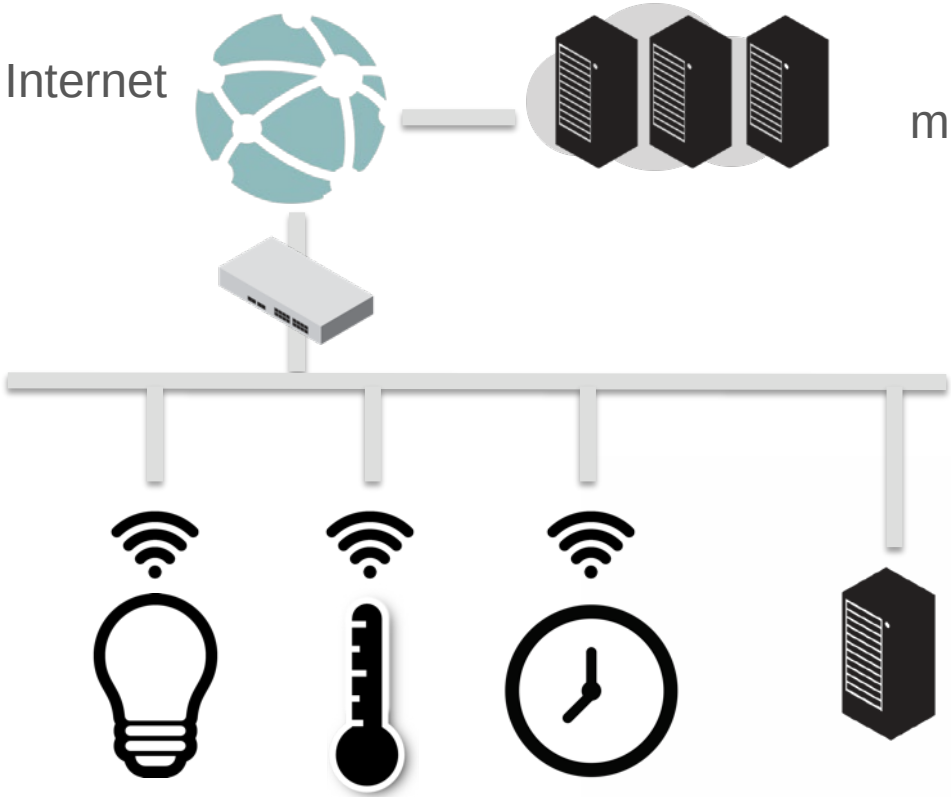
Inappropriate use

Command & control

The foundations for IoT are not new

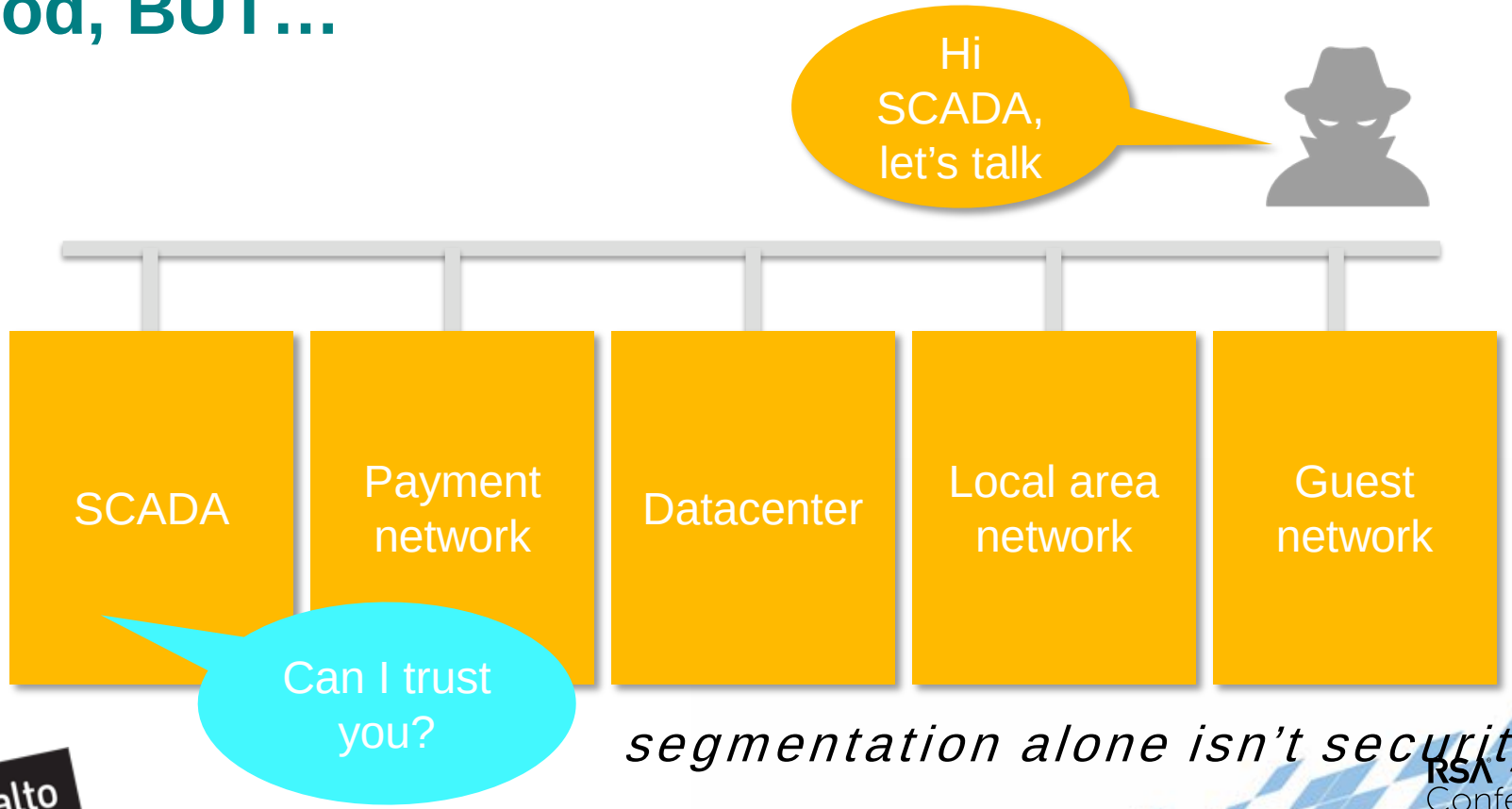


IoT changed standard interfaces & architecture



- Architectural shifts make control difficult
- Scale
- Accessibility makes everything a target

Lessons from SCADA / PCI – segmentation is good, BUT…

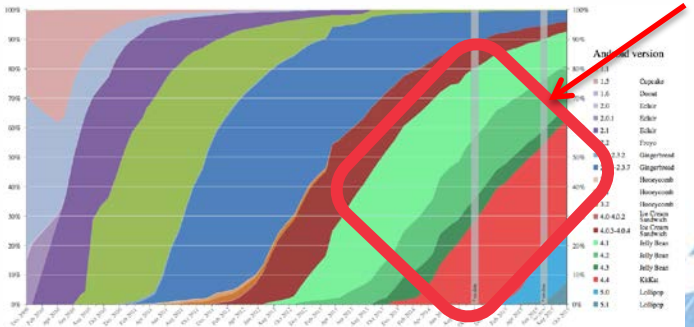


segmentation alone isn't security.

Security Best Practices for IoT

8 core considerations to enabling IoT

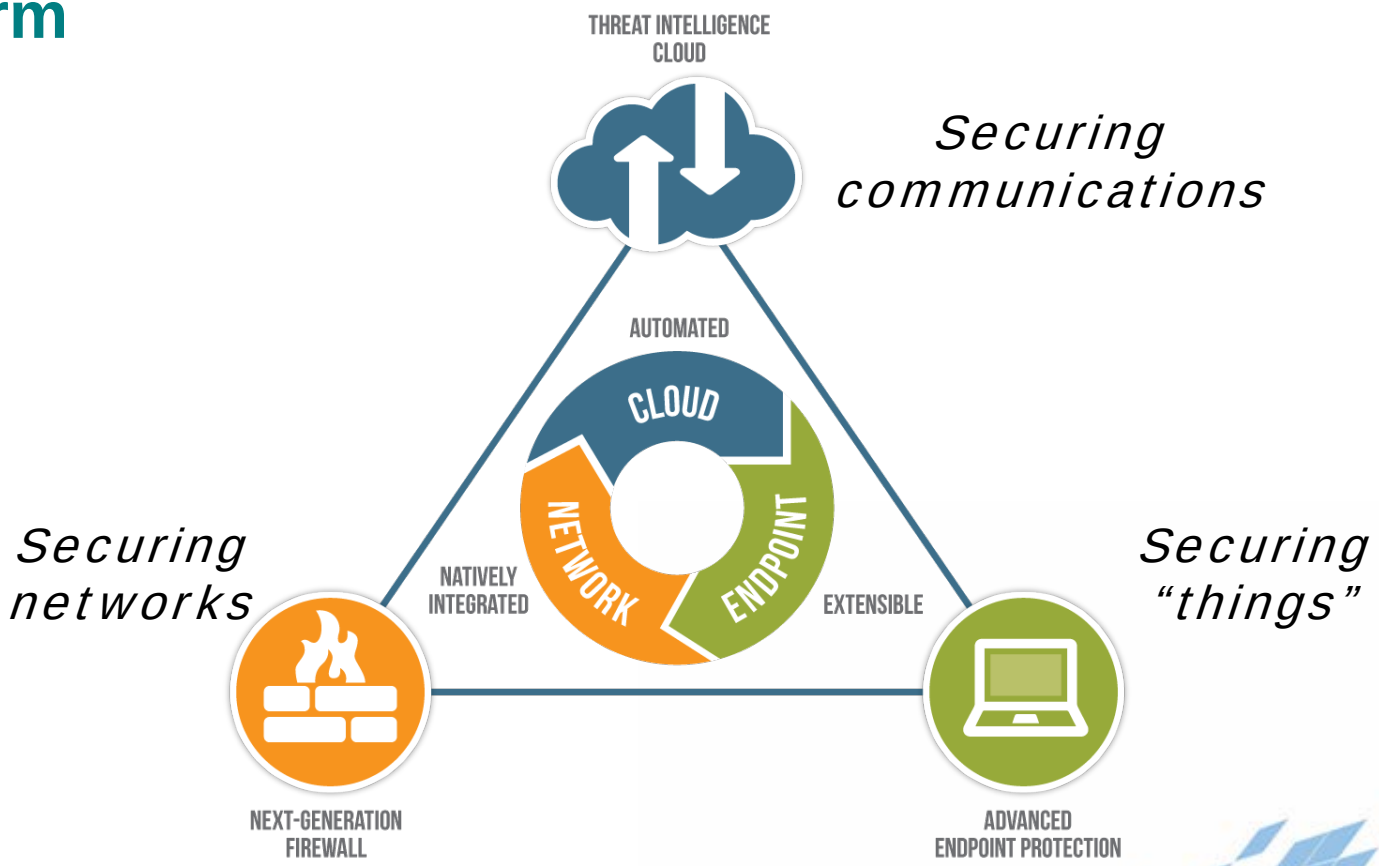
1. What is the business/personal use case?
2. What is the acceptable usage policy
3. Visibility & control (how do you identify, segment)
4. Trusted / Untrusted – Zero trust
5. Enforcement (risks awareness, education, policy)
   - What is the security base line?
6. IoT security platform (don't isolate)
7. Ongoing visibility of the cyber risk
8. Supporting users



Jelly bean & Kitkat (69%)

https://en.wikipedia.org/wiki/Android_version_history#/media/File:Android_historical_version_distribution_-

Architecture: an integrated & automated security platform



Philosophy

Zero trust

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Thank you

Greg Day

VP & Chief Security Officer, EMEA

Palo Alto Networks

GDAY@PaloAltoNetworks.com

GregDaySecurity

https://uk.linkedin.com/in/gregday