


# Next line of defense: Internet of Things

Kent Stuart, Product Marketing Manager

Dell, Inc.



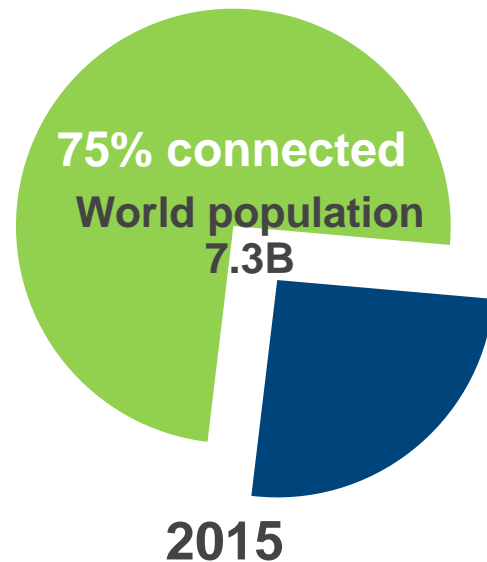
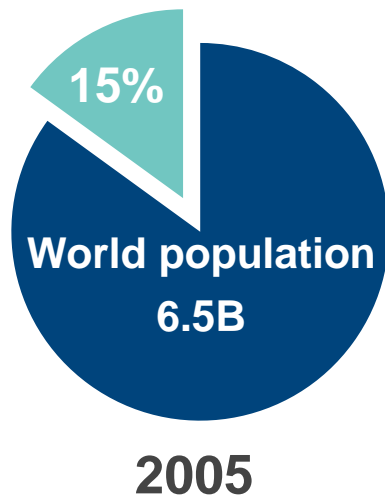
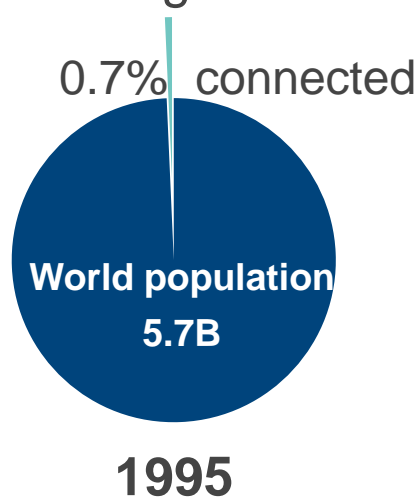
# Agenda

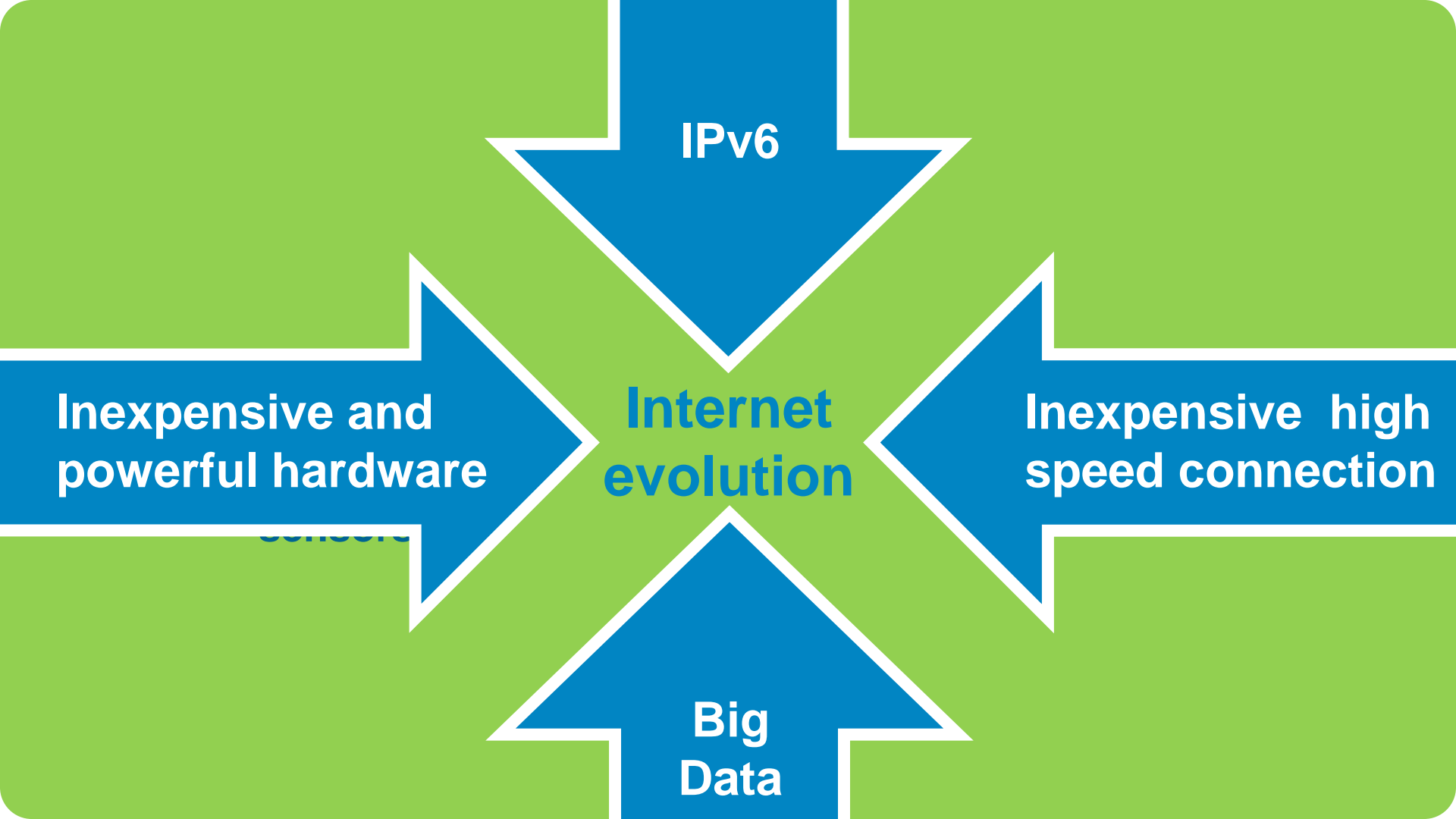
- How we got here
    - Is IoT the next trend for cyber criminals?
  - How it is going to roll out
    - Who will build
  - Downside scenarios
  - Mitigation
- 



# Evolution or revolution

- People interacting with their computer
- People interacting with computers – rise of the internet
- Connecting machines to the internet





**IPv6**

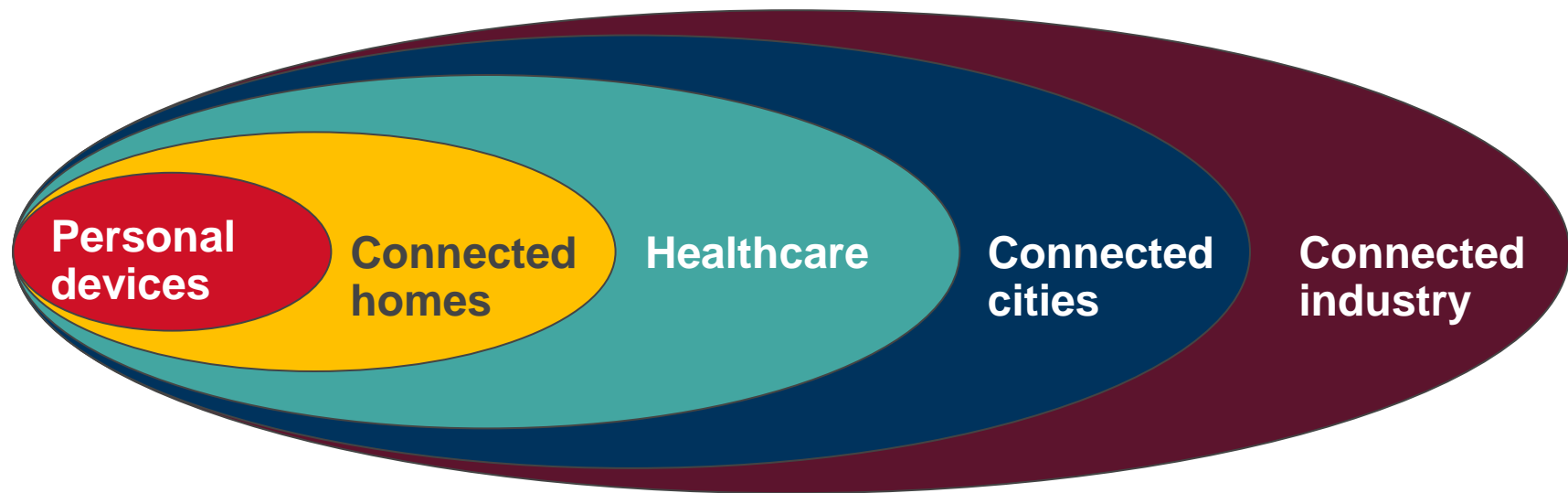
**Inexpensive and  
powerful hardware**

**Internet  
evolution**

**Inexpensive high  
speed connection**

**Big  
Data**

# Where you will see it



# Where does it take us?

- Make life easier –
  - RFIDs in retail to handle walk through checkout
  - Cars recognize people –my name is my password (entry, customer settings),
  - Improve life of the elderly, and hospital quality of care
  - Helping rehabilitation and augmenting human systems
  - drones for delivery of packages
  - Imagine printing replacement parts for your car or broken appliance
- Improve efficiencies -
  - Locating stolen items
  - Military may be leading the way here
  - Imagine custom manufacturing, shorter time to market
  - Tighter linkages between supply and demand
- Link diagnostics to actions – your car can schedule a repair – fleet management
- Your phone becomes even more important and central to your life



# Looking at vulnerabilities – for consumers



Kashmir Hill, Forbes Staff

Welcome to The Not-So Private Parts where technology & privacy collide

+ Follow (1,810)

TECH | 8/27/2013 @ 3:47 PM | 23,539 views

## 'Baby Monitor Hack' Could Happen To 40,000 Other Foscam Users

### Forbes

htt



Adrian  
Kingsley-  
Hughes  
Contributor

TECH | 7/09/2012 @ 6:24AM | 15,404 views

I write  
about  
hardware

## How Hackers Can Steal A BMW In Under 3 Minutes

### CONTROL AND WATCH YOUR HOME FROM ANYWHERE

Introducing the New NetCam HD+ with  
Premium Glass Lens & Night Vision

SHOP NOW

## Your TV might be watching you

CNNMoney

By Erica Fink and Laurie Segall @CNNTech August 1, 2013: 11:32 AM ET



# Looking at vulnerabilities –for business

- Smart manufacturing
  - You are told that you have adequate inventory when you do not
- Energy management
  - Gas stations run out of gas when their controls say they have plenty
  - Building HVAC shuts down
- Fleet management
  - Makes your car think it has been serviced
  - Does not provide proper location information
- Smart buildings
  - Compromise entry
- Smart cities
  - What if the power went off on your block, in the subway?





# What would IoT exploits look like?

## Using existing threats

- DDoS attacks –
  - larger networks, lower cost to initiate
- The rise of false positives/false negatives
- Man in the Middle attack

## Emerging new threats

- Firmware attack
  - USB attack
  - Printer and Phone attack
- Compromise your wearable - break into your home, break into bank



# Security concerns have common threads

1

The network as we know it is exploding and becoming more complex. The complexity of giving cyber criminals more and new avenues of attack.

2

Existing sensor technology looks to be easily penetrated – embedded software may have upgrade challenges

3

Appears that security is not a key design or feature concern on early devices  
Lots of new features may obscure missing security

4

How does a device know the person issuing directions or viewing data is authorized to do so?

5

Nodes are susceptible to breach and can become sources of disruption

6

Communication needs to restrict on who can see it (encryption and authorization)



# The simple protections – use what you have

- Secure your passwords
  - Change default passwords
  - Maintain a password policy
- Know what you have.
  - Maintain current updates on your devices and applications
- Scope for the future
- Enable all your security features – do not compromise
- Change the way you communicate
  - VPN
  - Encryption
- Build a higher level of security consciousness



# Guidance for creators

- Make security a part of the design process
  - Balance security with features and performance
    - › This includes the User Experience as well as the hardware
  - How are you ensuring the integrity of the data
  - Ensure information is going to the right place
  - What are the privacy features?
- What happens when you have been compromised?
  - Have an independent mode of operation
  - How can you reset/update the system?
  - Independent/autopilot/safe mode?



# Considerations for users/consumers

- Ask questions
  - What information is being sent?
  - How is it being sent?
  - What happens when there is a breach?
  - How to I turn it off, stop sending data?
  - How is the firmware updated?
- Insist on security features
  - New devices need firewalls
- Businesses – ongoing penetration testing
  - What is your OEM doing for the products you purchase



# What can you do to protect yourself and your organization?

Network

Hardware

Anti malware  
Intrusion protection

Communications

VPN  
Encryption



# How to avoid the storm

With each new connection cyber risks expand, and an available threat surface grows to affect not just the device, but the system to which it connects.

- **Update software /firmware**
- **Protect the network**
- **Harden your storage capabilities**
- **Make communications secure**
- **Control Access and privacy**
- **Certify the legitimacy of connections**
- **Build security awareness with your staff**



# Thank you

