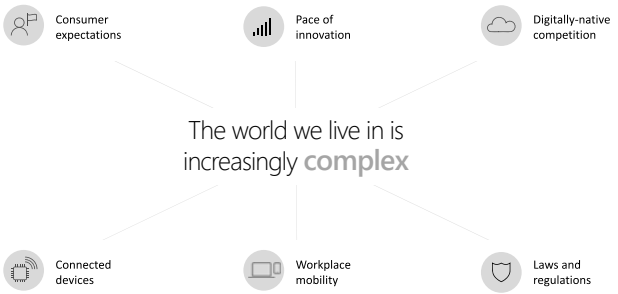
Shaping tomorrow's cybersecurity landscape

Cyberwater, October 2018, Oslo

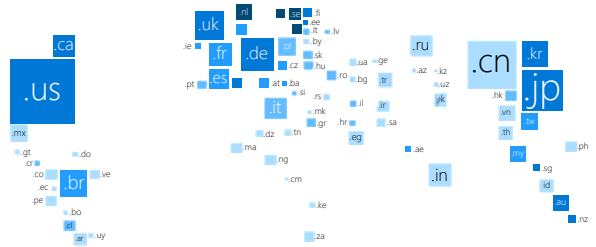
Mark Smitham
Senior Manager of Cybersecurity Policy

Microsoft



2005 Internet user map

Microsoft



Sizing Legend	Percent Penetration of Internet Users	Number of Internet Users							
☐ = 5M Internet Users	0 20 40 60 80 100	China	USA	India	Brasil	Japan	Germany	UK	S. Korea
☐ = 10M Internet Users		111M	201M	26M	38M	86M	57M	42M	35M

2015 Internet user map

Microsoft

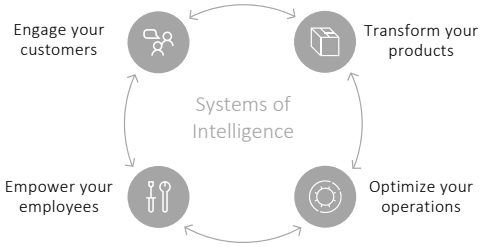
Sizing Legend	Percent Penetration of Internet Users	Number of Internet Users							
☐ = 5M Internet Users	0 20 40 60 80 100	China	USA	India	Brasil	Russia	Germany	Mexico	Nigeria
☐ = 10M Internet Users		751M	287M	283M	127M	90M	72M	68M	66M

2025 Internet user map

Microsoft

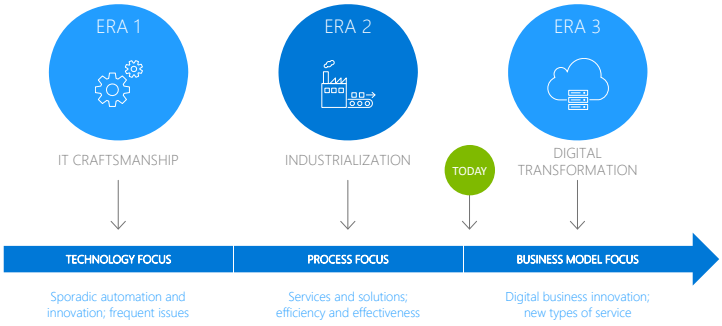
Sizing Legend	Percent Penetration of Internet Users	Number of Internet Users							
☐ = 5M Internet Users	0 20 40 60 80 100	China	USA	India	Brasil	Russia	Germany	Mexico	Nigeria
☐ = 10M Internet Users		1.1B	317M	708M	173M	124M	74M	106M	126M

DIGITAL TRANSFORMATION



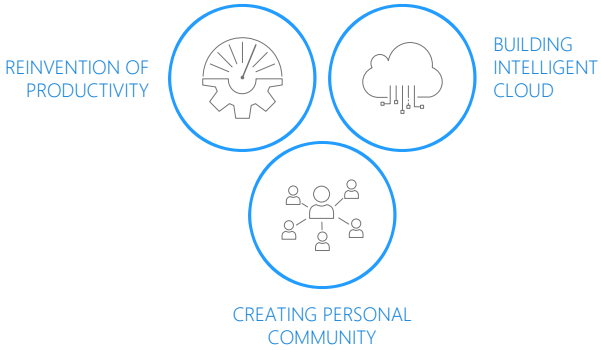
IT's role increases dramatically

Microsoft



The three pillars of cloud

Microsoft



CLOUD MOMENTUM CONTINUES TO **ACCELERATE**

"By 2020, a corporate 'no-cloud' policy will be as **rare** as a 'no-internet' policy is today."[1]

"The question is no longer: 'How do I move to the cloud?' Instead, it's 'Now that I'm in the cloud, how do I make sure I've **optimized my investment** and risk exposure?"[2]

"By 2020 clouds will stop being referred to as 'public' and 'private'. It will simply be **the way business is done** and IT is provisioned."[3]

[1]Gartner: Smarter with Gartner, Why a No-Cloud Policy Will Become Extinct, February 2, 2016
[2]KPMG: 2014 Cloud Survey Report, Elevating business in the cloud, December 10, 2014
[3]IDC: IDC Market Spotlight, Cloud Definitions and Opportunity, April 2015

"Businesses and users are going to embrace technology only if they can trust it."

Satya Nadella
Chief Executive Officer
Microsoft Corporation

OUR COMMITMENT TO **YOU**

- SECURITY
- PRIVACY & CONTROL
- COMPLIANCE
- TRANSPARENCY
- RELIABILITY

OUR COMMITMENT TO **YOU**

- We'll help you keep your data secure
- Your data is private and under your control
- We manage your data in accordance with the law
- You know what we are doing with your data
- We provide enterprise grade uptime for cloud services

MICROSOFT IS **DOING MORE** TO EARN YOUR TRUST

HOLISTIC APPROACH TO **SECURITY**

LEADERSHIP IN **COMPLIANCE**

COMMITMENT TO **TRANSPARENCY & PRIVACY**

HOLISTIC APPROACH TO **SECURITY**

Platform

Intelligence

Partners

Microcontrollers (MCUs)
low-cost, single chip computers

9 BILLION new MCU devices built and deployed every year

Fewer than 1% of MCUs are connected today.

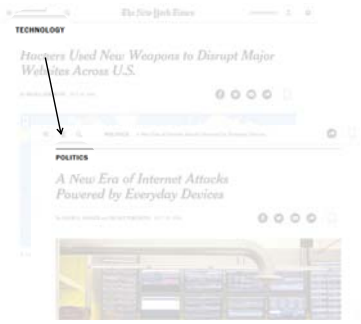
Connected devices create profoundly better customer experiences.

How does a consumer know the compressor in their fridge needs to be replaced?

Option 1
Melted ice cream

Option 2
Predictive maintenance

And, expose your business to unequalled risks…



Observations on October 21,2016 Botnet Attack

Device Security is a socioeconomic concern
DAY 1 the attack is **Technology** headline in NY Times
DAY 2 the attack is **Politics** headline

The attack exploited well-understood weaknesses
Weak common passwords, no early detection, no remote update, etc.

Future attacks could be much larger
This attack was small; just 100K devices
Imagine a 100M-device attack

Future attacks could create huge liability exposure
Hackers could "brick" an entire product line in a day
Actuating devices could cause property damage or loss of life

The internet security battle.
We've been fighting it for ***decades.***
We have experience to share.

The 7 properties of highly secured devices

- Hardware Root of Trust
- Defense in Depth
- Small Trusted Computing Base
- Dynamic Compartments
- Certificate-Based Authentication
- Failure Reporting
- Renewable Security

Some properties depend only on hardware support

Hardware Root of Trust

Hardware Root of Trust

Unforgeable cryptographic keys generated and protected by hardware

- Hardware to protect **Device Identity**
- Hardware to **Secure Boot**
- Hardware to attest **System Integrity**

Some properties depend on hardware and

Defense in Depth | Dynamic Compartments | Small Trusted Computing Base

Dynamic Compartments

Internal barriers limit the reach of any single failure

- Hardware to **Create Barriers**
- Software to **Create Compartments**

Some properties depend on hardware, software and cloud

Certificate-Based Authentication | Failure Reporting | Renewable Security

Renewable Security

Device security renewed to overcome evolving threats

- Cloud to **Provide Updates**
- Software to **Apply Updates**
- Hardware to **Prevent Rollbacks**

Azure Sphere empowers manufacturers to create highly-secured, connected MCU devices

SECURITY

Peace of mind

Every device built with Azure Sphere is secured by Microsoft. For its 10 year lifetime.

PRODUCTIVITY

Faster time to market

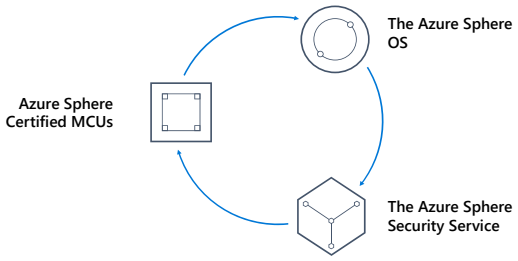
The Azure Sphere developer experience shortens OEM time to market.

OPPORTUNITY

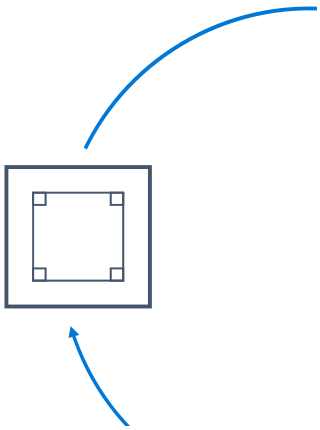
The future is now

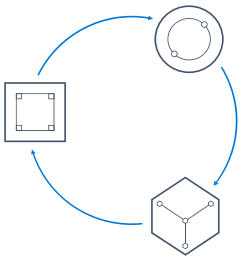
Azure Sphere empowers OEMs to create new customer experiences and business models.

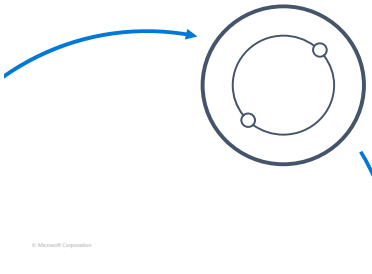
Azure Sphere is an end-to-end solution for securing MCU powered devices



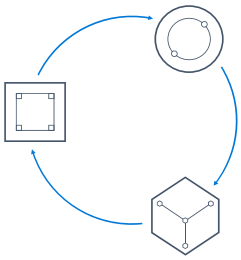
Azure Sphere Certified MCUs
from silicon partners, with built-in Microsoft security technology provide connectivity and a dependable **hardware root of trust.**

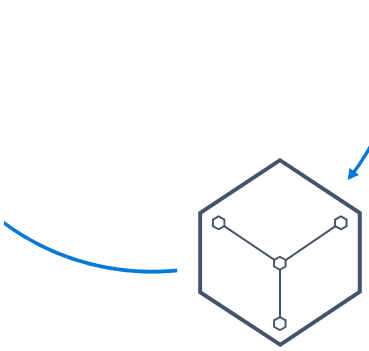






The Azure Sphere OS
secured by Microsoft for the devices 10-year lifetime to create **a trustworthy platform** for new IoT experiences





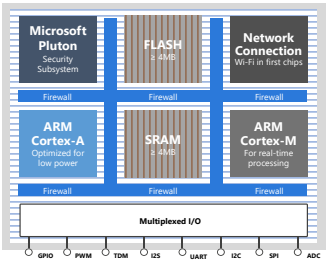
The Azure Sphere Security Service
guards every Azure Sphere device; it **brokers trust** for device-to-device and device-to-cloud communication, **detects emerging threats**, and **renews device security.**

Azure Sphere certified MCUs create a secured root of trust for connected, intelligent edge devices

Connected with built-in networking

Secured with built-in Microsoft silicon security technology including the Pluton Security Subsystem

Crossover real-time and application processing power brought to MCUs for the first time



Our Silicon Partners

MediaTek

ARM

STMicroelectronics

NXP

Silicon Labs

Nordic

Nuvoton

Hilscher

Toshiba

VeriSilicon

Qualcomm

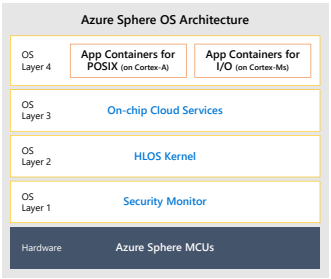
The Azure Sphere OS is optimized for IoT, security, and agility

Secure Application Containers
Compartmentalize code for agility, robustness & security

On-chip Cloud Services
Provide update, authentication, and connectivity

Custom Linux kernel
Empowers agile silicon evolution and reuse of code

Security Monitor
Guards integrity and access to critical resources



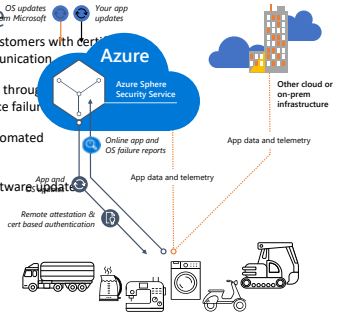
The Azure Sphere Security Service connects and protects every Azure Sphere device

Protects your devices and your customers with de… based authentication of all communication

Detects emerging security threats throu… automated processing of on-device failu…

Responds to threats with fully automated on-device updates of OS

Allows for easy deployment of software updates to Azure Sphere powered devices



Azure Sphere is Open.

Azure Sphere empowers manufacturers to create highly-secured, connected MCU devices

SECURITY

Peace of mind

Every device built with Azure Sphere is secured by Microsoft. For its 10 year lifetime.

PRODUCTIVITY

Faster time to market

The Azure Sphere developer experience shortens OEM time to market.

OPPORTUNITY

The future is now

Azure Sphere empowers OEMs to create new customer experiences and business models.

What's Next

SECURED FROM THE SILICON UP

Order Azure Sphere dev kits:

1. Pre-order available through end of August
2. Direct order begins in September

Place your dev kit order and request a call with one of our dedicated agents.

Attend an Azure Sphere event in your market:

1. Azure Sphere at Ignite in Orlando, FL
2. IoT in Action event series in: DE, JP, AU, CN, ES, TW, US

Find an IoT in Action event near you. Check out Azure Sphere articles on Forbes, the Wall Street Journal, and PC Magazine.

Stay up to date on Azure Sphere:

1. Learn how the seven properties can secure your products
2. Discover videos and helpful materials

Visit the Azure Sphere website to learn more about the IoT revolution.

Cyber risk landscape

Microsoft

Actors	Objectives	Actions	Impacts

Many methods of attack

Permissive environment

Escalating conflicts

Geopolitics and technical evolution drive government response

Microsoft

Systems

Societies

Sovereignty

Cyberattacks cause immense costs

Microsoft

- 71% of companies admit they fell victim to a successful cyberattack the prior year
- $400bn cost of cyberattacks to companies each year
- $3tr estimated economic cost of cyberattacks by 2020
- 140+ Median # of days between infiltration and detection
- 160m Data records compromised from top 8 breaches in 2015
- 556m victims of cybercrime per year

Cyberattacks also create wider problems

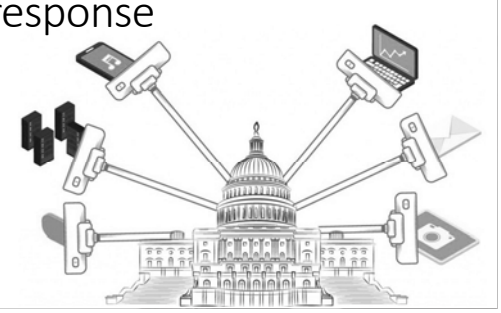
Microsoft

IMPACT GOES BEYOND FINANCES

- SIGNIFICANT ORGANIZED CRIME ELEMENT
- DISRUPTION AND DANGERS TO CRITICAL INFRASTRUCTURE AND SYSTEMS
- INVASIONS OF PRIVACY
- REDUCED INNOVATION
- CONTENT RELATED CRIME, AND EXTREMIST RECRUITING
- DECREASED TRUST

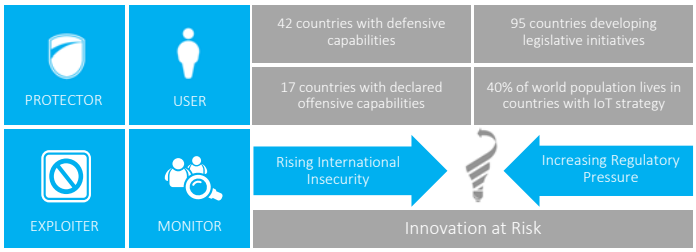
Microsoft

Government response



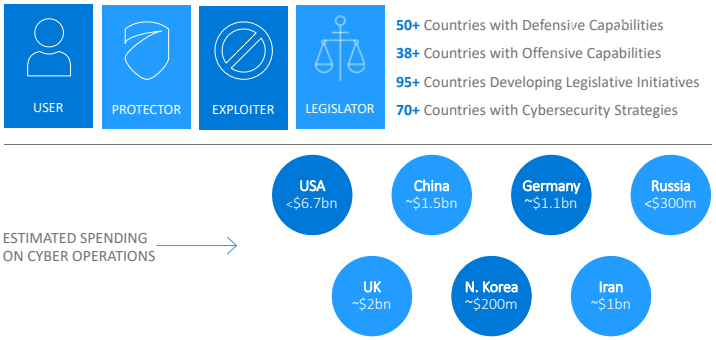
Security response

Microsoft



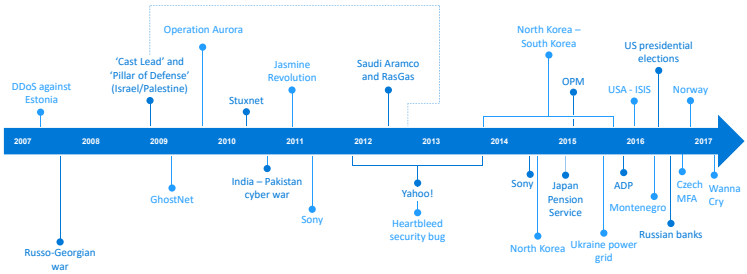
Governments heavily involved in cyberspace

Microsoft



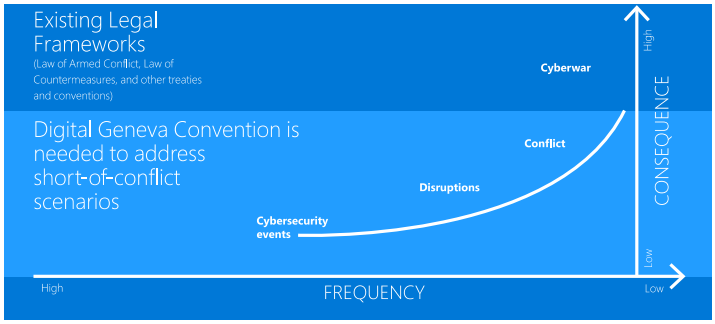
Government sponsored cyberattacks are increasing

Microsoft



Risk to civilians from cyber-conflict needs a response

Microsoft



Our call to action

Microsoft

- Undertake to create politically binding then legally binding agreements committing governments to certain, acceptable behaviors in cyberspace.
- Drive forward a tech sector accord that commits the ICT industry to objectives and actions that will protect users and the wider internet, and will ensure the sector's neutral status in any cyber-conflict.
- Support the establishment and operation of politically-neutral, independent, transparent and peer-reviewed accountability organization.
- Identify and provide avenues for multi-stakeholder input and involvement in the development of cyberspace policies and agreements.

Microsoft

Digital transformation for future water utilities and services can unlock the potential of the cloud.

We firmly believe that every customer deserves a trustworthy cloud experience and we are committed to delivering that experience in the cloud.

Microsoft