guardtime

IoT and M2M Opportunity

Matthew Johnson

CTO Guardtime

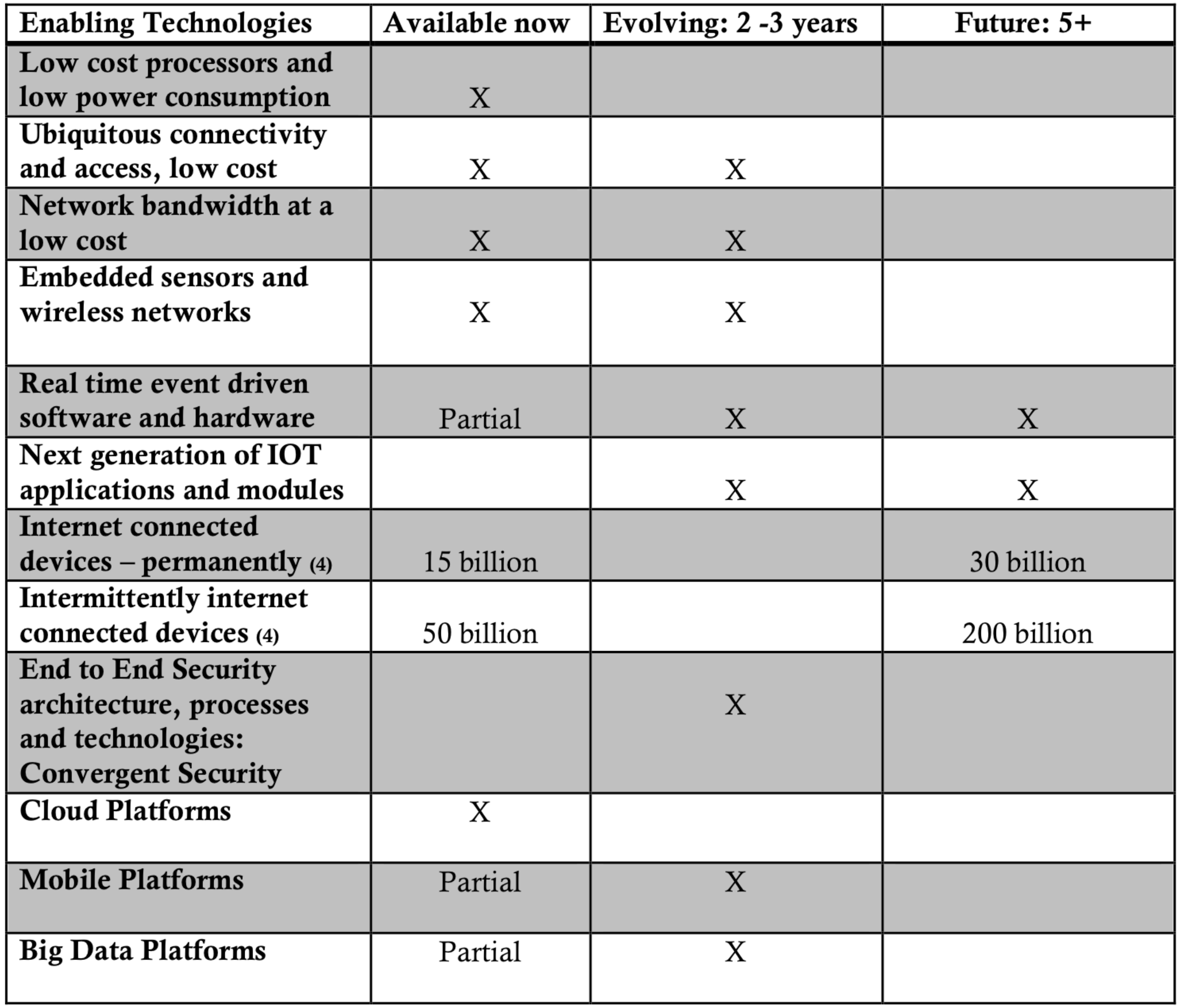
Gartner definition:

“The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal state or the external environment.”

IoT value proposition:

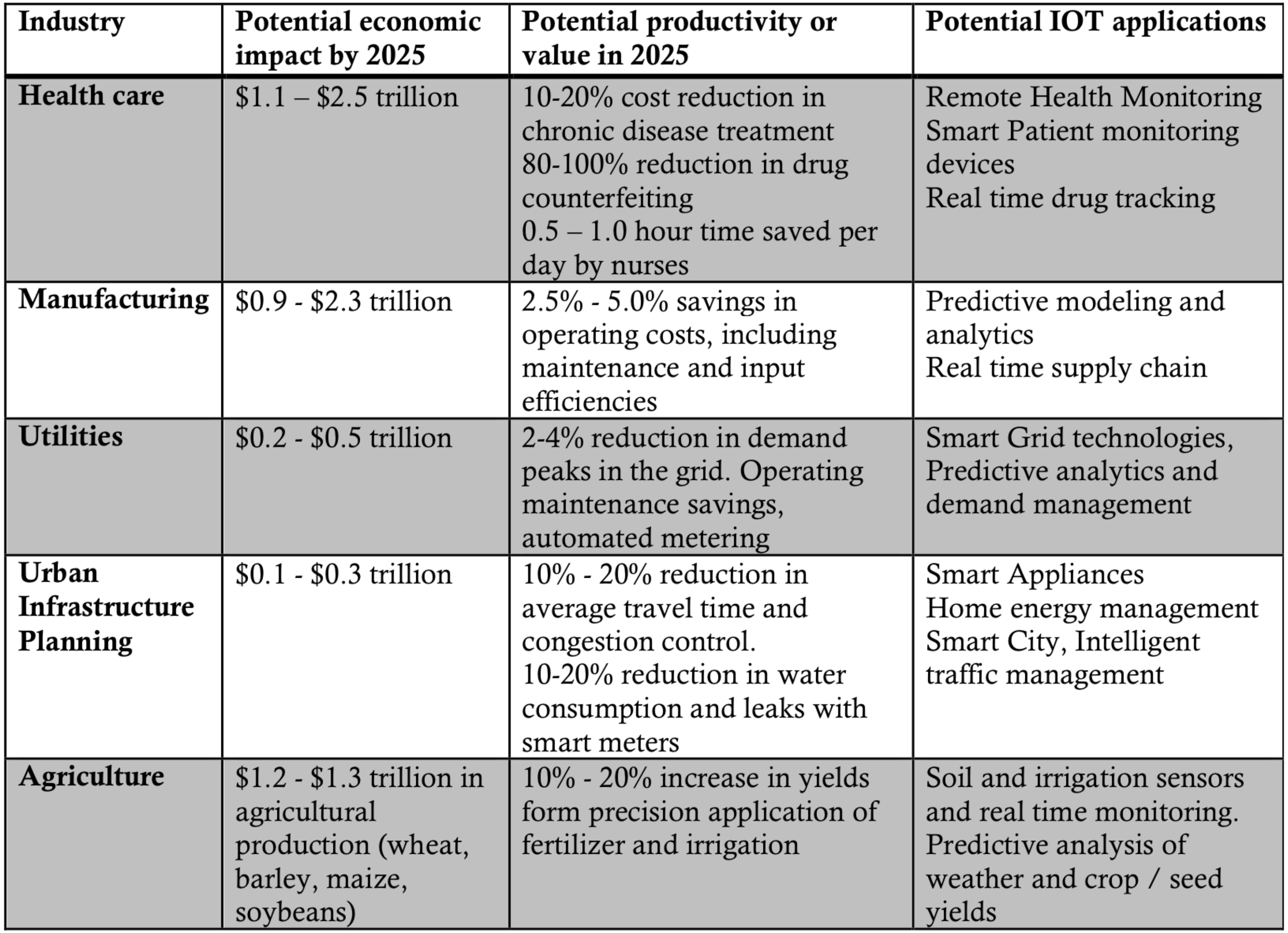
Internet of Things enables an entity to adapt, pivot and predict in real time to social, political, economic, and environmental events, allowing the entity to simultaneously manage risk, optimize revenue and manage waste.

- Changes quality of life, health and environment
- Changes patterns of consumption
- Creates opportunities for entrepreneurs
- Creates new products and services
- Shifts surplus between producers or industries
- Drive economic growth or productivity
- Posses new regulatory and legal challenges



Enabling Technologies	Available now	Evolving: 2 -3 years	Future: 5+
Low cost processors and low power consumption	X		
Ubiquitous connectivity and access, low cost	X	X	
Network bandwidth at a low cost	X	X	
Embedded sensors and wireless networks	X	X	
Real time event driven software and hardware	Partial	X	X
Next generation of IOT applications and modules		X	X
Internet connected devices – permanently (4)	15 billion		30 billion
Intermittently internet connected devices (4)	50 billion		200 billion
End to End Security architecture, processes and technologies: Convergent Security		X	
Cloud Platforms	X		
Mobile Platforms	Partial	X	
Big Data Platforms	Partial	X	

Source: GE



Industry	Potential economic impact by 2025	Potential productivity or value in 2025	Potential IOT applications
Health care	$1.1 – $2.5 trillion	10-20% cost reduction in chronic disease treatment 80-100% reduction in drug counterfeiting 0.5 – 1.0 hour time saved per day by nurses	Remote Health Monitoring Smart Patient monitoring devices Real time drug tracking
Manufacturing	$0.9 - $2.3 trillion	2.5% - 5.0% savings in operating costs, including maintenance and input efficiencies	Predictive modeling and analytics Real time supply chain
Utilities	$0.2 - $0.5 trillion	2-4% reduction in demand peaks in the grid. Operating maintenance savings, automated metering	Smart Grid technologies, Predictive analytics and demand management
Urban Infrastructure Planning	$0.1 - $0.3 trillion	10% - 20% reduction in average travel time and congestion control. 10-20% reduction in water consumption and leaks with smart meters	Smart Appliances Home energy management Smart City, Intelligent traffic management
Agriculture	$1.2 - $1.3 trillion in agricultural production (wheat, barley, maize, soybeans)	10% - 20% increase in yields form precision application of fertilizer and irrigation	Soil and irrigation sensors and real time monitoring. Predictive analysis of weather and crop / seed yields

Source: GE

A GE and Siemens Perspective on IoT/M2M Security

- **Information Technology (IT):** systems, applications, networks, servers, storage and clients to enable the automation of business processes. Hosted in Data Centers, with varying degrees of availability metrics and security clearance. Infrastructure to support and protect the Consumer Internet (B2C) and Value Chains (B2B). IT security is mature.
- **Operational Technology (OT):** is hardware and software operating in real time environments that senses, detects and responds to changes in monitoring and/or control of physical devices. Located in plants or buildings, close to physical assets being monitored and controlled. Infrastructure to support and protect oil & gas plants, utilities, manufacturing and transportation. OT security is still evolving.
- **Telecommunications Network (TN):** A cellular network is a wireless network distributed over land areas called Cells, served by a transceiver (cell site or base station). Cellular networks generally consist of the following components: Switching Systems responsible for performing call processing and subscriber related functions. Base station system. Operation and support systems, that connects switching and base station infrastructure, monitor and control the cellular network.

But… As Gartner states:

"Attacks are relentless, hackers' ability to penetrate systems and information is never fully blocked, and systems must be assumed to be continuously compromised."

*Annualized cost to Fortune 500 Community per year is USD ~10M. There's only 15% ROI for current security technologies**

*Ponemon Institute

2,437,287,926

The Billions of Known Records Compromised Since 2013

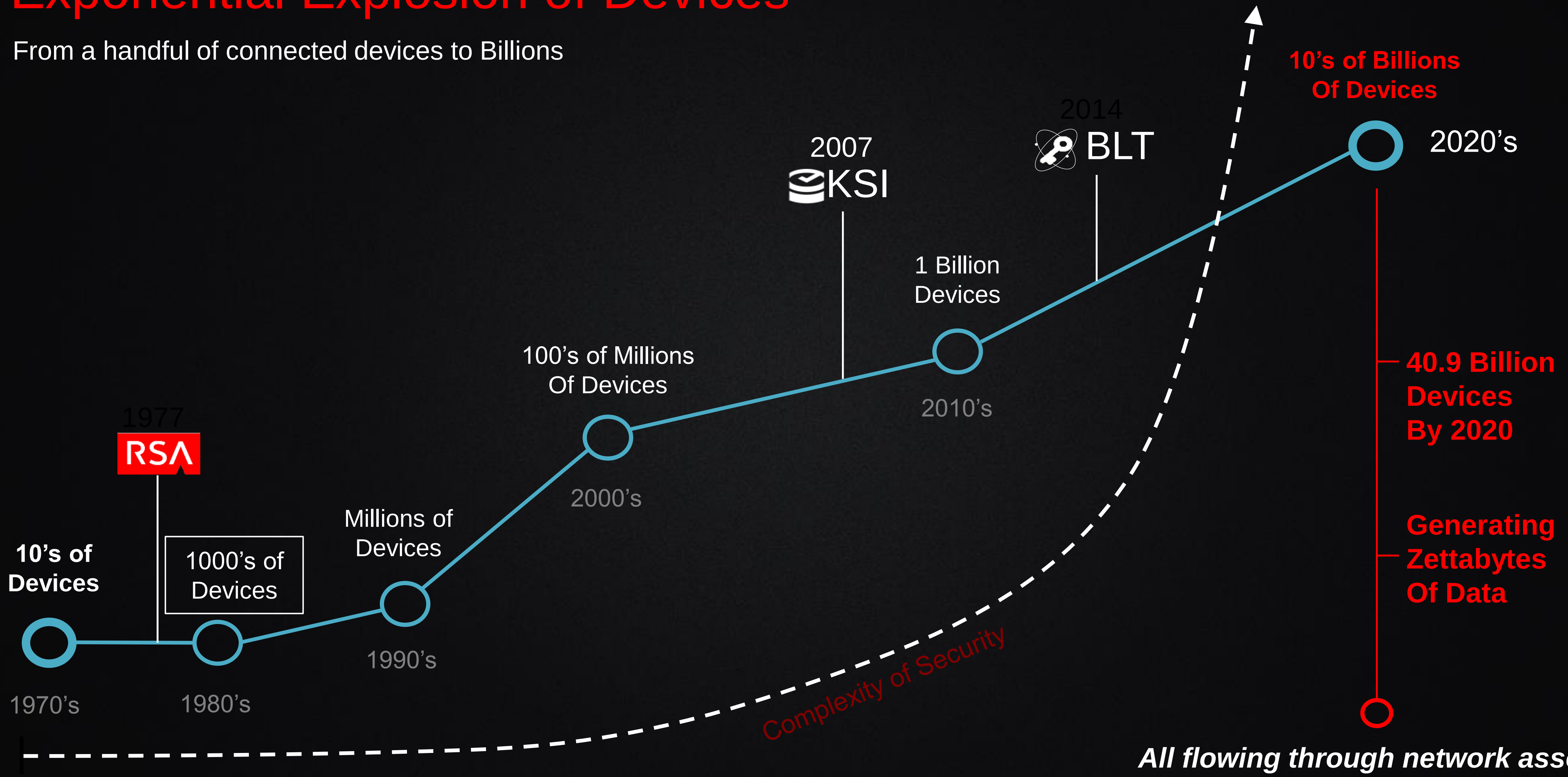
(Approximately 33% of human population)

*Source: BreachLevelIndex.com

guardtime

Exponential Explosion of Devices

From a handful of connected devices to Billions



10's of Devices

1970's

1977

RSA

1000's of Devices

1980's

Millions of Devices

1990's

100's of Millions Of Devices

2000's

2007

KSI

1 Billion Devices

2010's

2014

BLT

10's of Billions Of Devices

2020's

40.9 Billion Devices By 2020

Generating Zettabytes Of Data

Complexity of Security

All flowing through network assets.

guardtime

There's Always Vulnerabilities

New Protocol Attacks

The Heartbleed Bug

Anatomy of a "goto fail" - Apple's SSL bug

US-CERT

Alert (TA14-290A)

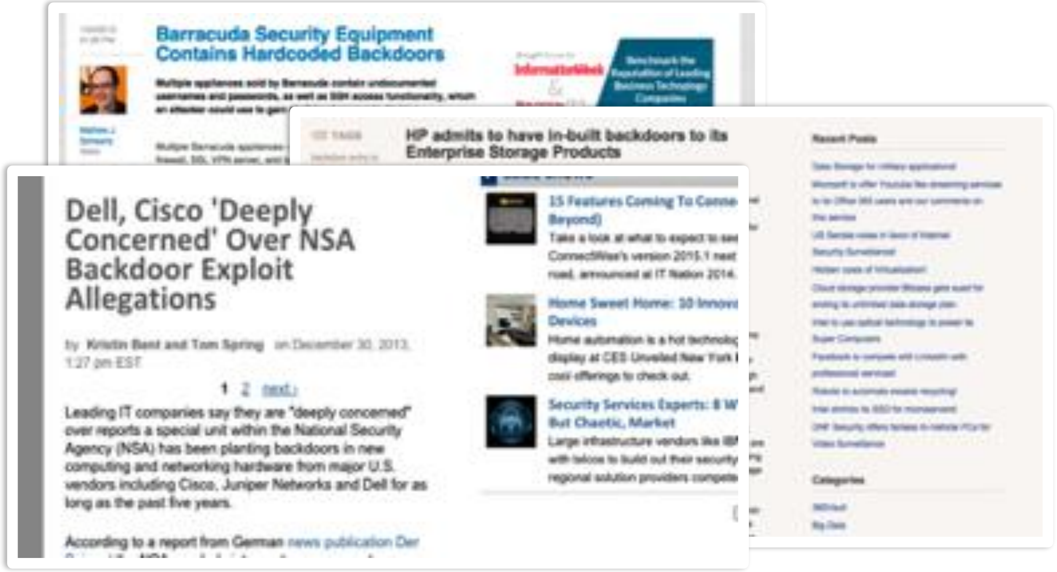
SSL 3.0 Protocol Vulnerability and POODLE Attack

Systems Affected

Overview

- 'Zero Day Problem'
- Implementation Specific Vulnerabilities
- Practice and Policy Vulnerabilities
- Trust Anchor Vulnerabilities

New Hardware Backdoors



Barracuda Security Equipment Contains Hardcoded Backdoors

HP admits to have in-built backdoors to its Enterprise Storage Products

Dell, Cisco 'Deeply Concerned' Over NSA Backdoor Exploit Allegations

by Kristin Bent and Tom Spring on December 30, 2013, 1:27 pm EST

1 2 next ›

Leading IT companies say they are "deeply concerned" over reports a special unit within the National Security Agency (NSA) has been planting backdoors in new computing and networking hardware from major U.S. vendors including Cisco, Juniper Networks and Dell for as long as the past five years.

According to a report from German news publication Der

15 Features Coming To Conne Beyond)

Take a look at what to expect to see ConnectWise's version 2015.1 next road, announced at IT Nation 2014.

Home Sweet Home: 10 Innova Devices

Home automation is a hot technolog display at CES Unveiled New York I cool offerings to check out.

Security Services Experts: 8 W But Chaotic, Market

Large infrastructure vendors like IBM with telcos to build out their security regional solution providers compete

- Malicious Insiders
- Exposure of Secrets (Key Compromise)
- Misconfiguration Issues
- Increased abstraction via SDN and NFV

All paving the way for **Persistent Cyber Attacks**

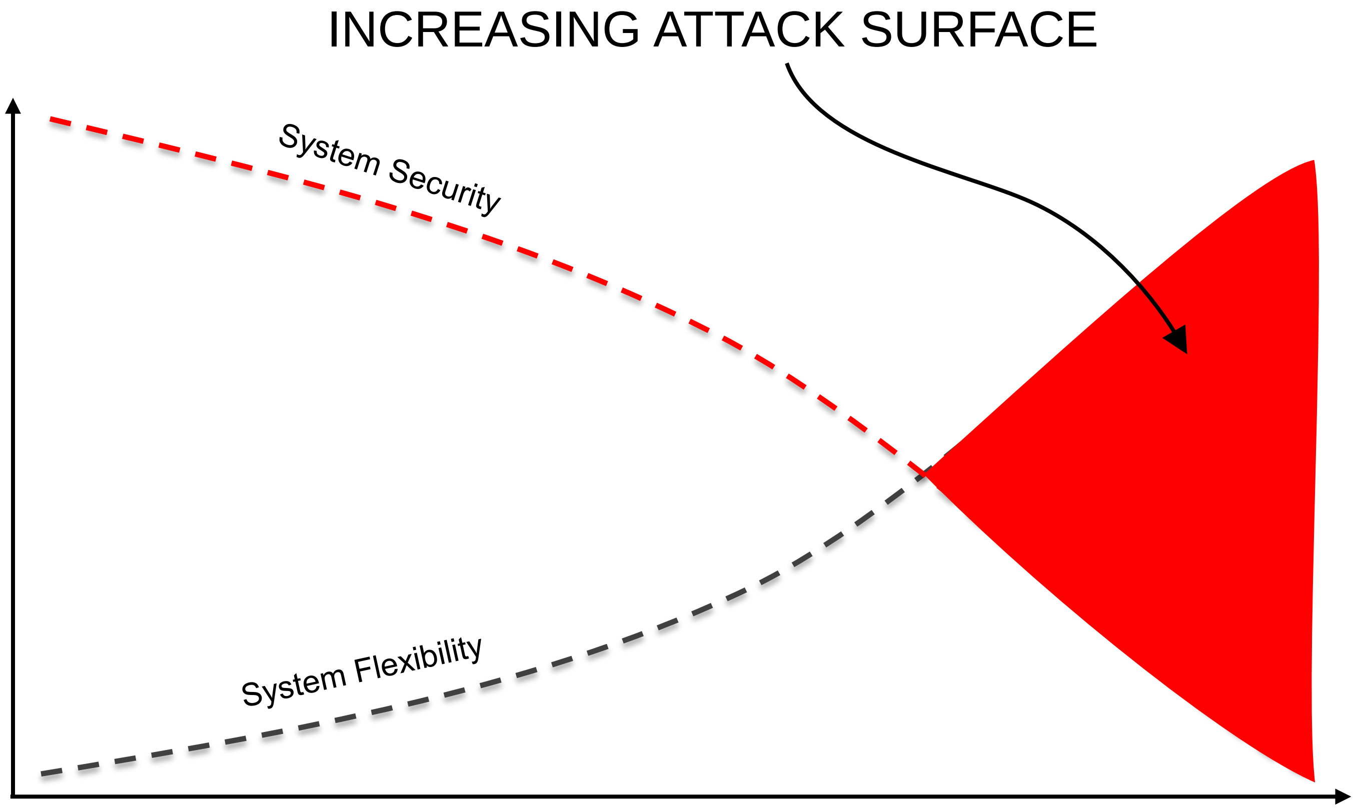
guardtime

You are ALWAYS under attack.

Welcome to the new world.

guardtime

Increasing Attack Surface



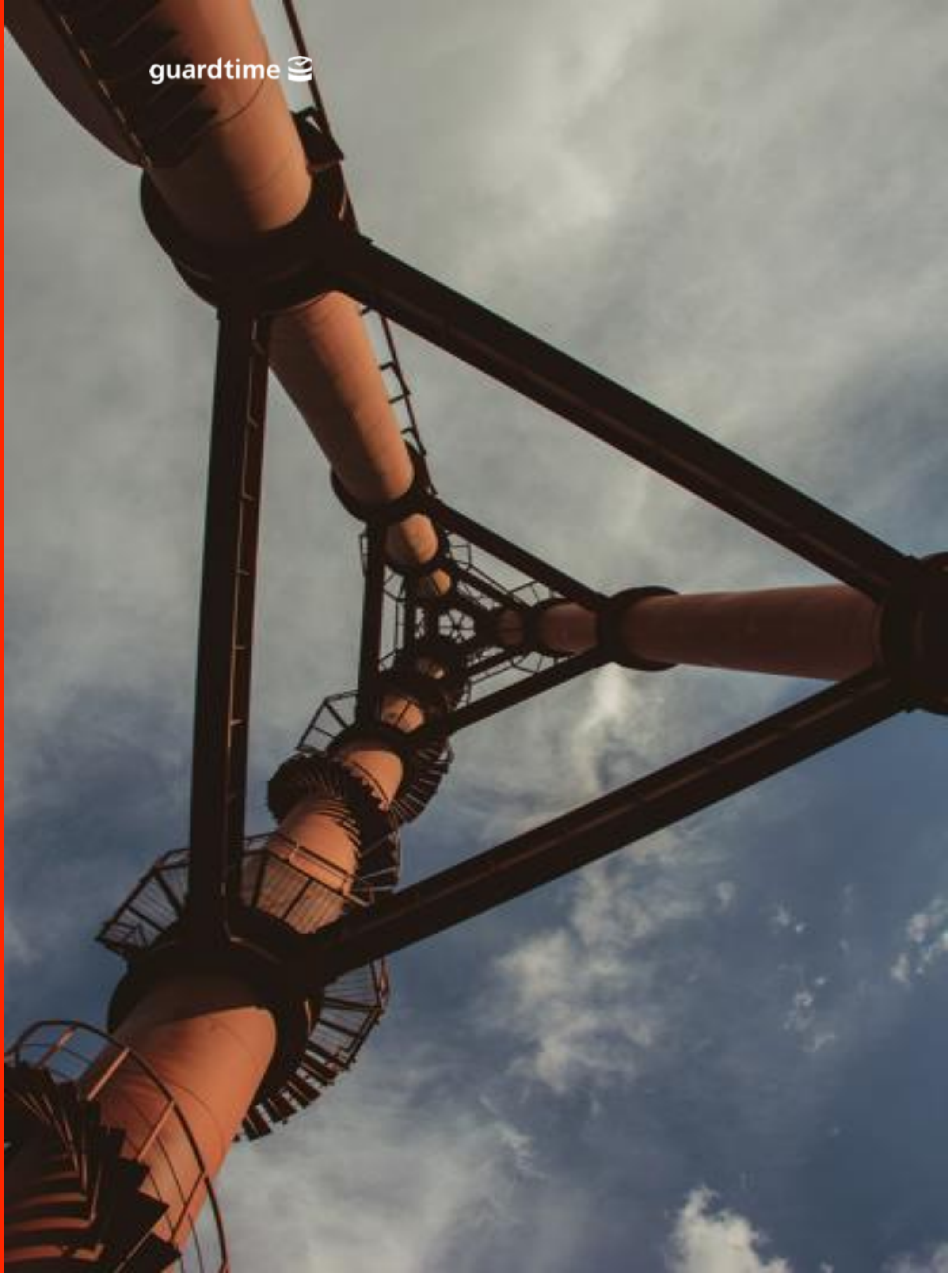
Expanding Flexibility & Capability = Increasing Attack Surface

Technology is experiencing a breakdown of trust

As the world becomes more digitally dependent on a fundamentally insecure and poorly instrumented foundation.

The old guard of perimeter-based defense is ineffective and we need to compliment these ‘solutions’…

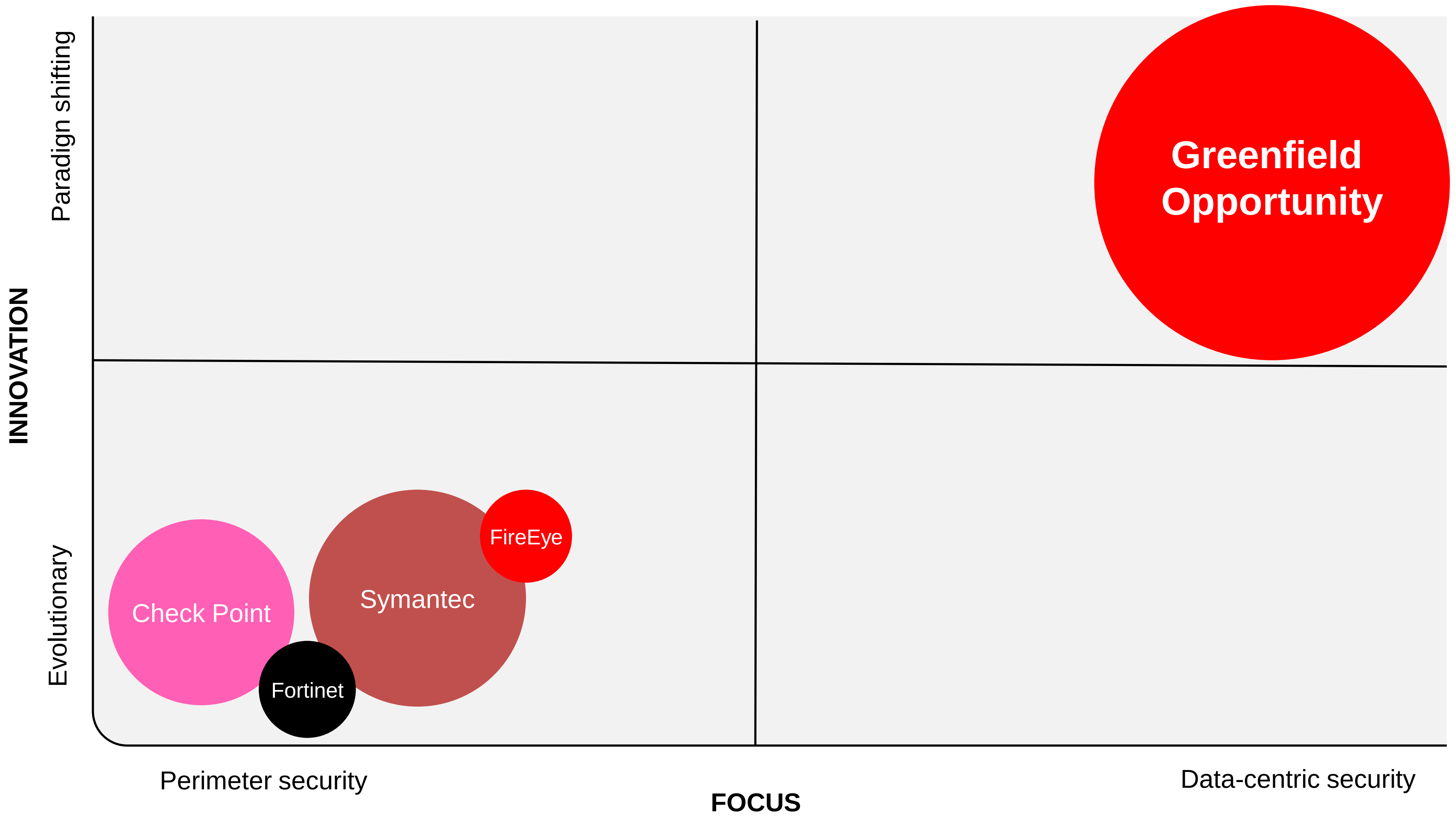
It’s time to defend the DATA.



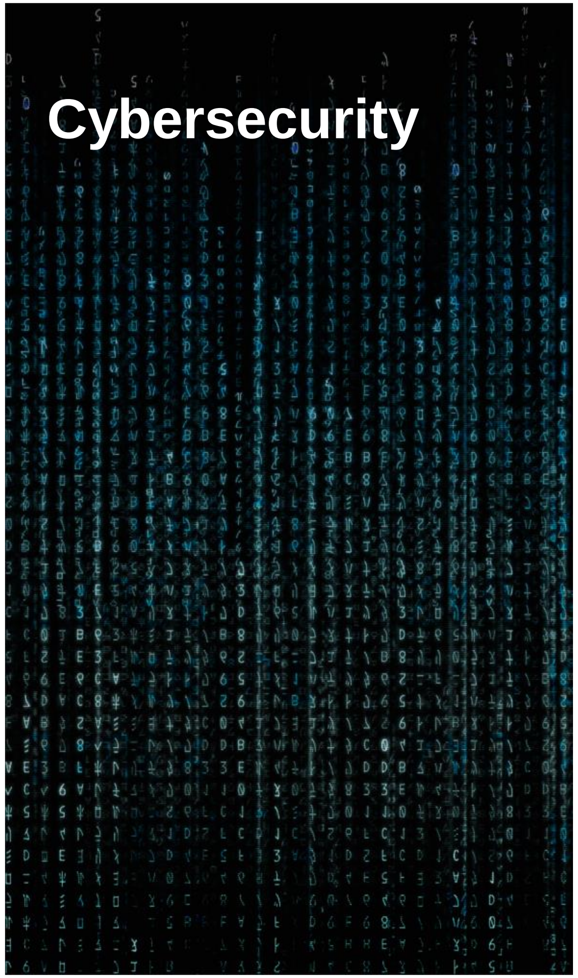
The IoT and M2M network infrastructure of the future must be built on a base of independently verifiable truth and integrity to support safety and mission critical functions.

guardtime

Cybersecurity Industry: Positioning



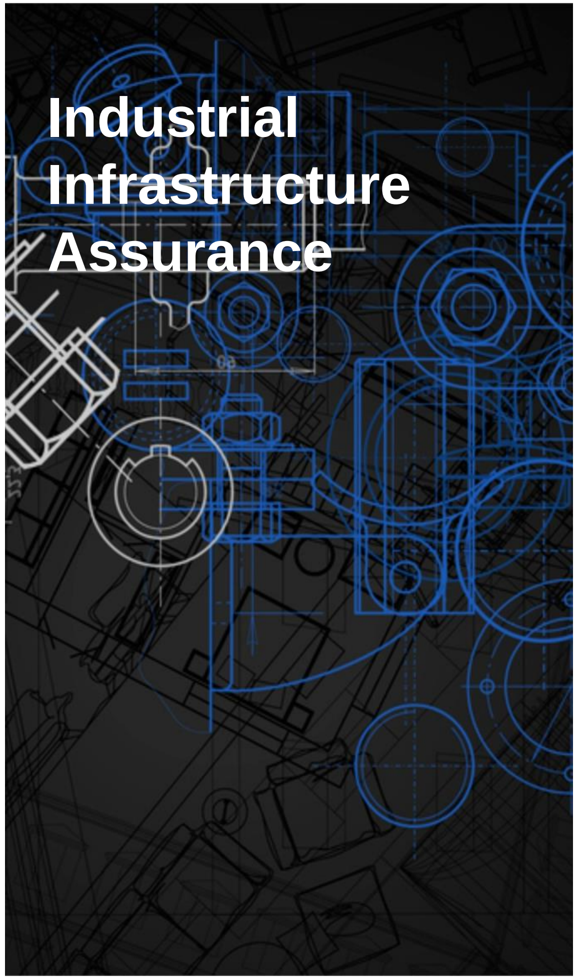
Data Centric Security Solutions



Cybersecurity

Internet-of-things Security

Big data Regulatory Compliance



Industrial Infrastructure Assurance

The Breach is Inevitable

and

100% Protection is Impossible

but for the first time in history,

100% Detection is Possible

Trust vs. Truth

Microsoft former chief privacy adviser Caspar Bowden has said for years that he does not trust Microsoft as a company, nor does he trust its software.

During an internal strategy conference in 2011, with Microsoft deputy general counsel, cloud management personnel and the NTOs in attendance, Bowden warned: *"If you sell Microsoft cloud computing to your own governments then this [FISA] law means that the NSA can conduct unlimited mass surveillance on that data."*

http://www.theguardian.com/world/2013/sep/30/microsoft-privacy-chief-nsa

It’s All About the Data