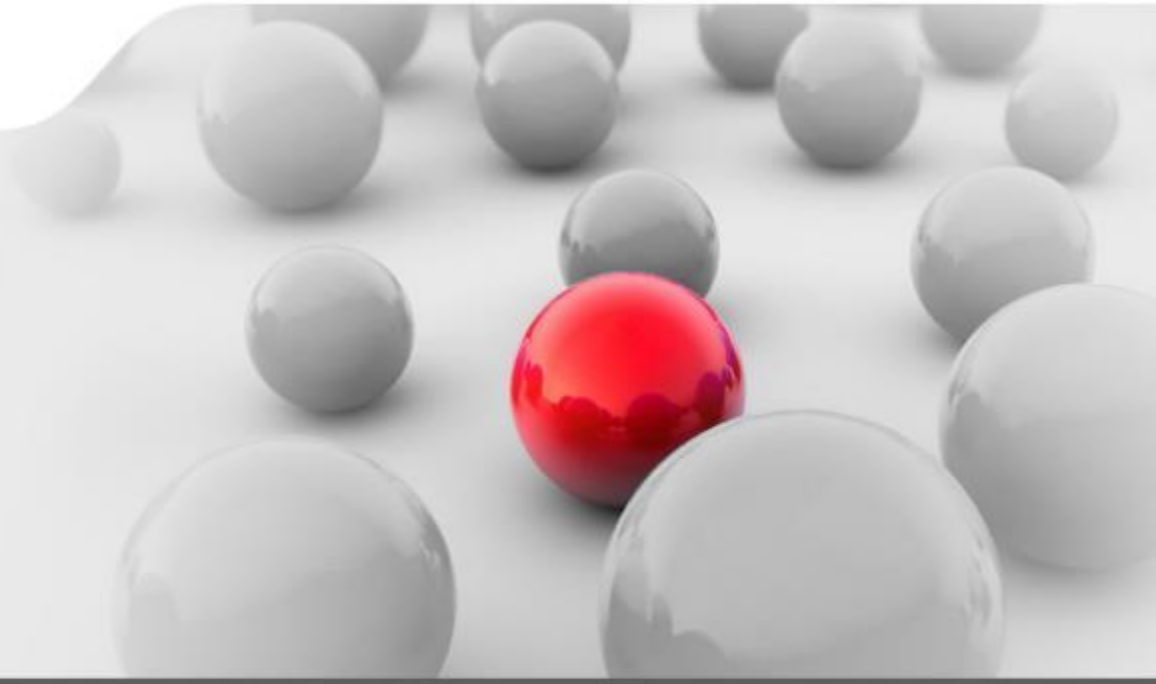
Counterpoint
Technology Market Research



The Anatomy of IoT Security

Satyajit Sinha
Research Analyst
IoT and Mobility

March 2018

Counterpoint
Technology Market Research

Mission

- We help our partners make decisions with accurate data, delivered in timely manner.

Research Activities

- Connected devices, digital consumer goods, software & applications
- Emerging and disruptive technologies
- Internet of Things (IoT)
- Tailored research as well as syndicated reports
- Seminars and workshops
- Consulting and customized projects

Key IoT Denominators

1

- One billion cellular-IoT connections by 2020

2

- Four Pillars of security: Hardware, Software, Network and Cloud

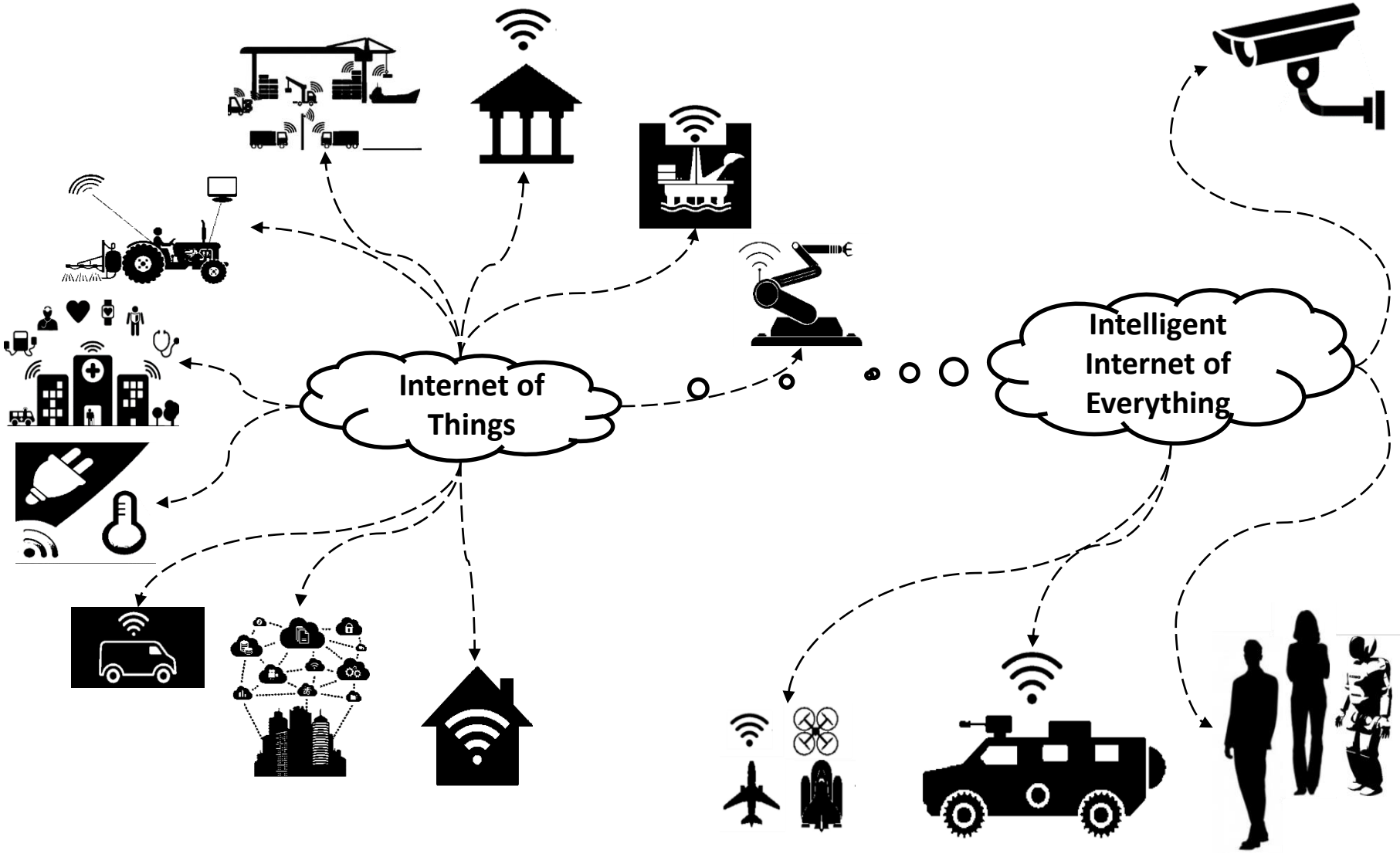
3

- Three major verticals under threat - Connected **Car**, **Healthcare** and Smart **Cities**

4

- **Understand**: Cybercrime is a '**Business**', not just a '**System Glitch**'

IoT Ecosystem and Evolution

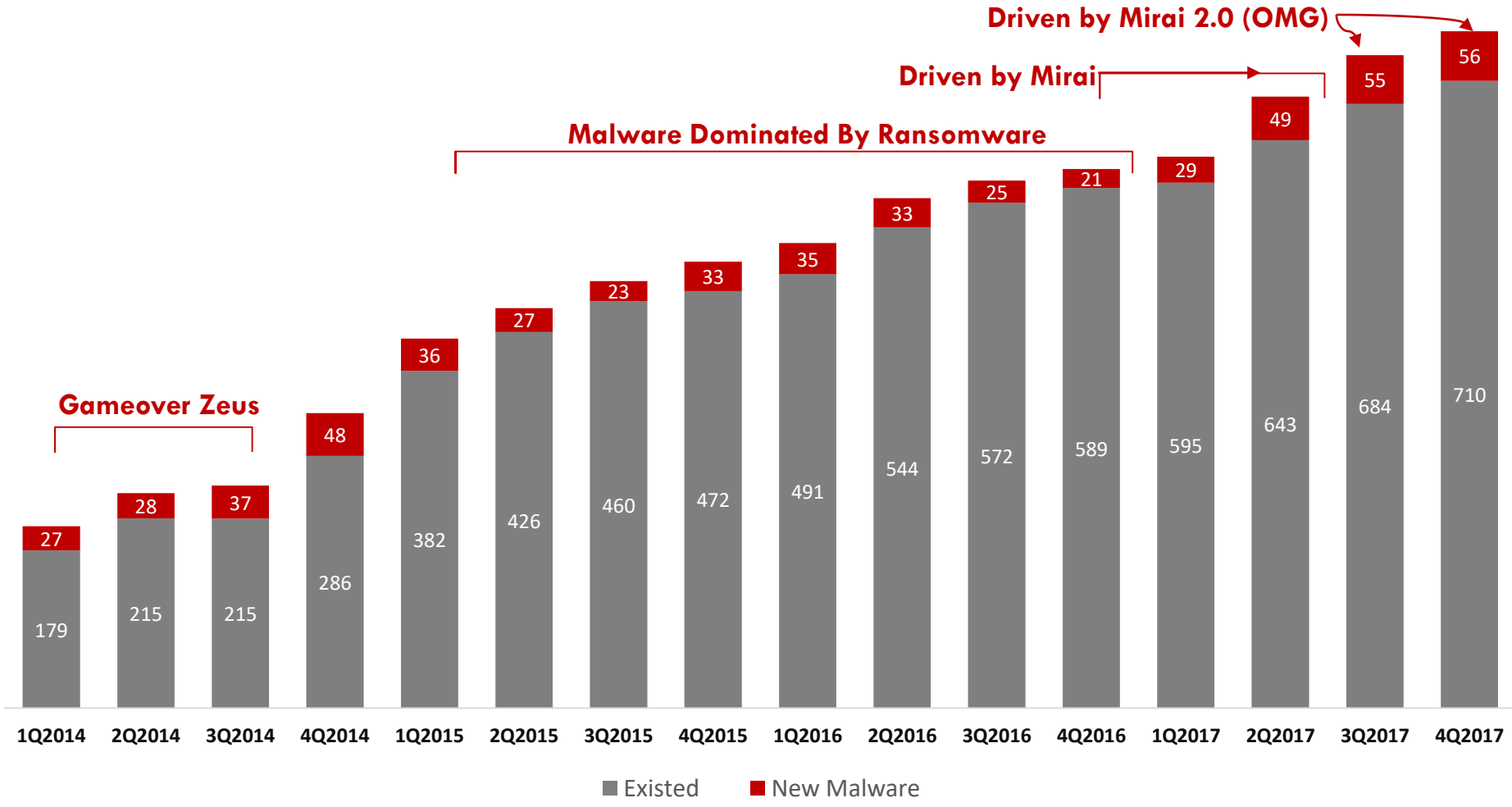


Malware is Eating IoT World

Mirai : Turning point of IoT Security

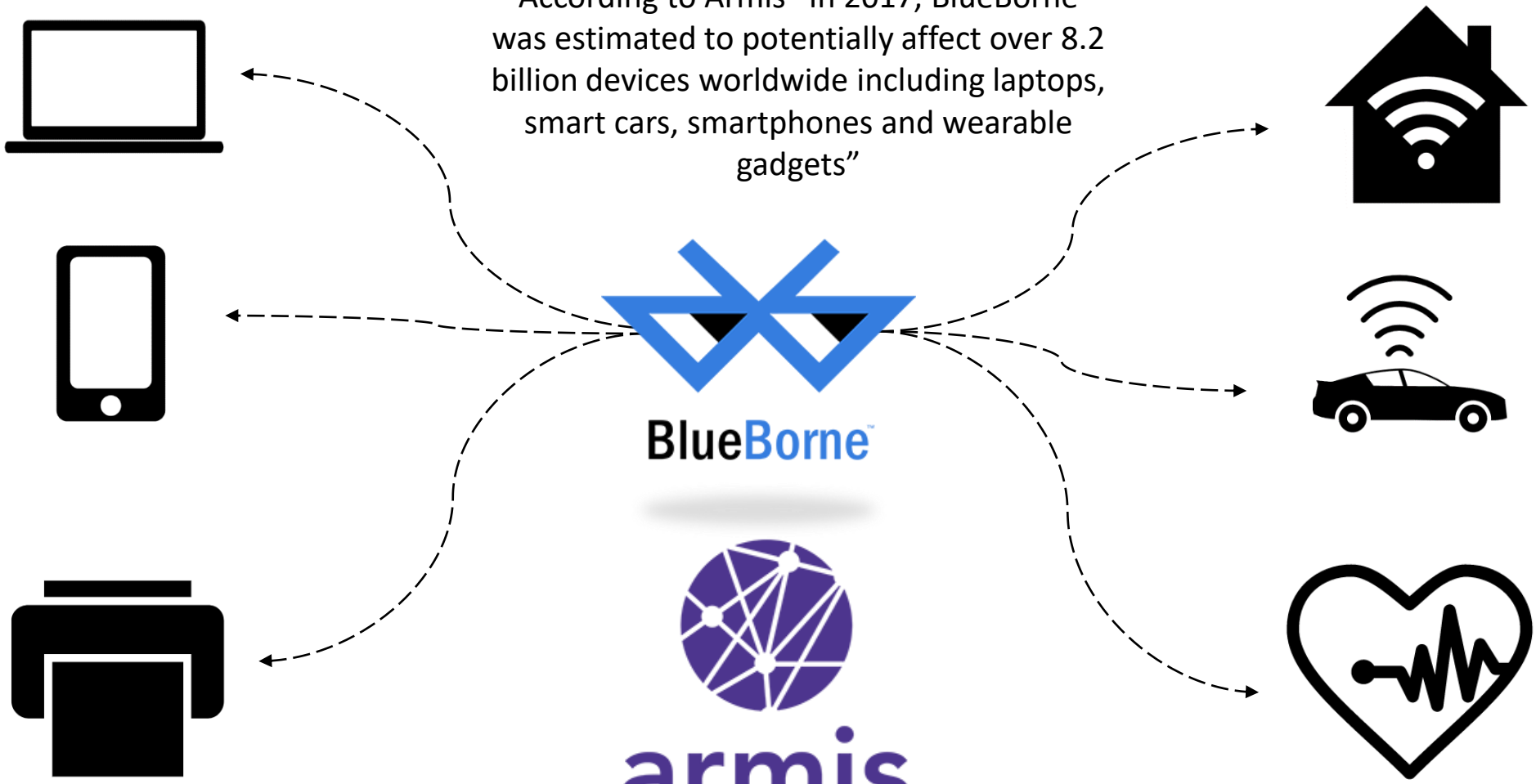
Rise of Malware in M2M/IoT Devices

(number of Malware, in million)



Malware attack not limited to online: BlueBorne Attacks via Bluetooth

According to Armis "In 2017, BlueBorne was estimated to potentially affect over 8.2 billion devices worldwide including laptops, smart cars, smartphones and wearable gadgets"

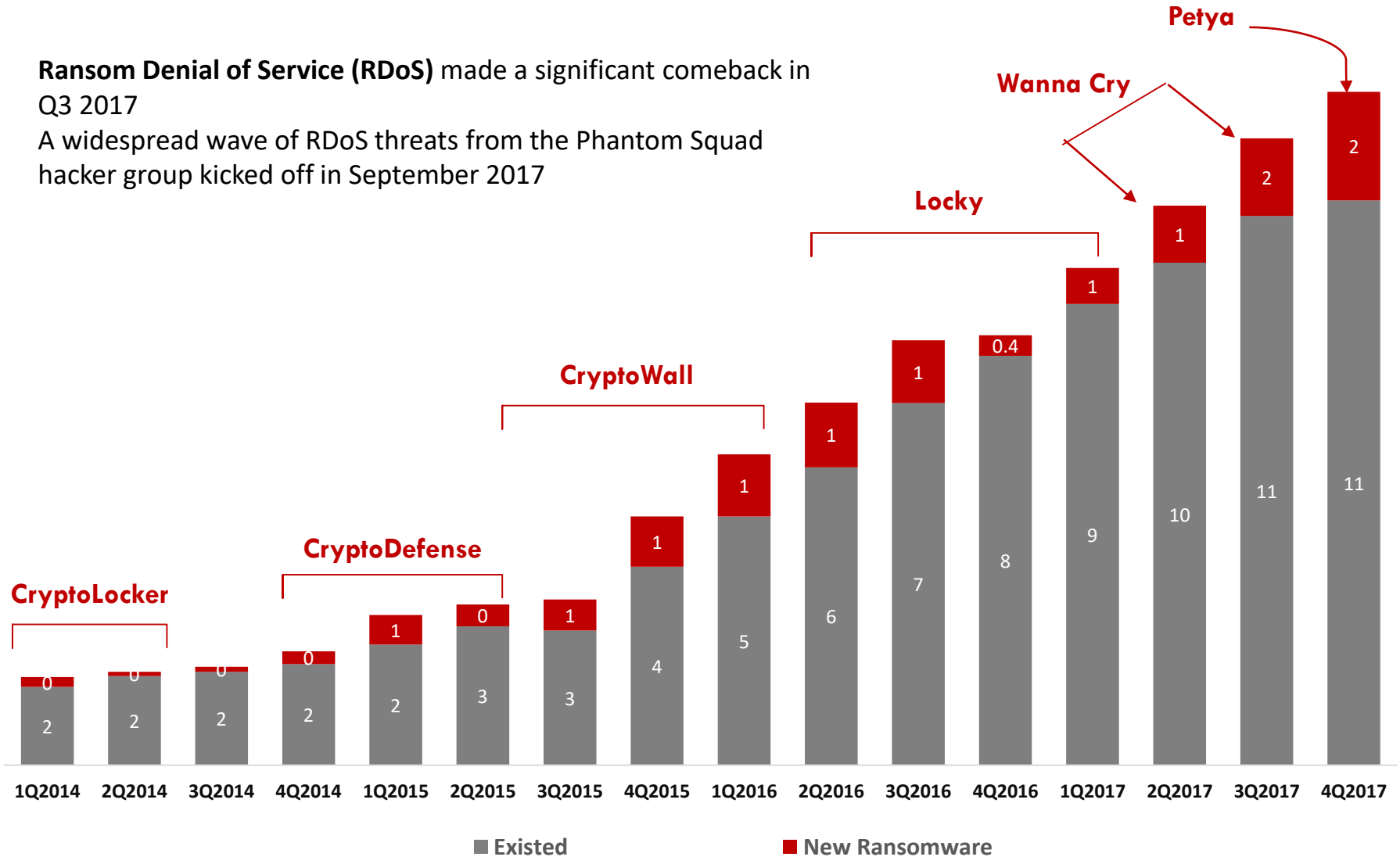


Ransomware : The latest Threat

Rise of Ransomware

(number of Malware, in million)

- **Ransom Denial of Service (RDoS)** made a significant comeback in Q3 2017
- A widespread wave of RDoS threats from the Phantom Squad hacker group kicked off in September 2017



End to End Security : Key to Secure IoT Data

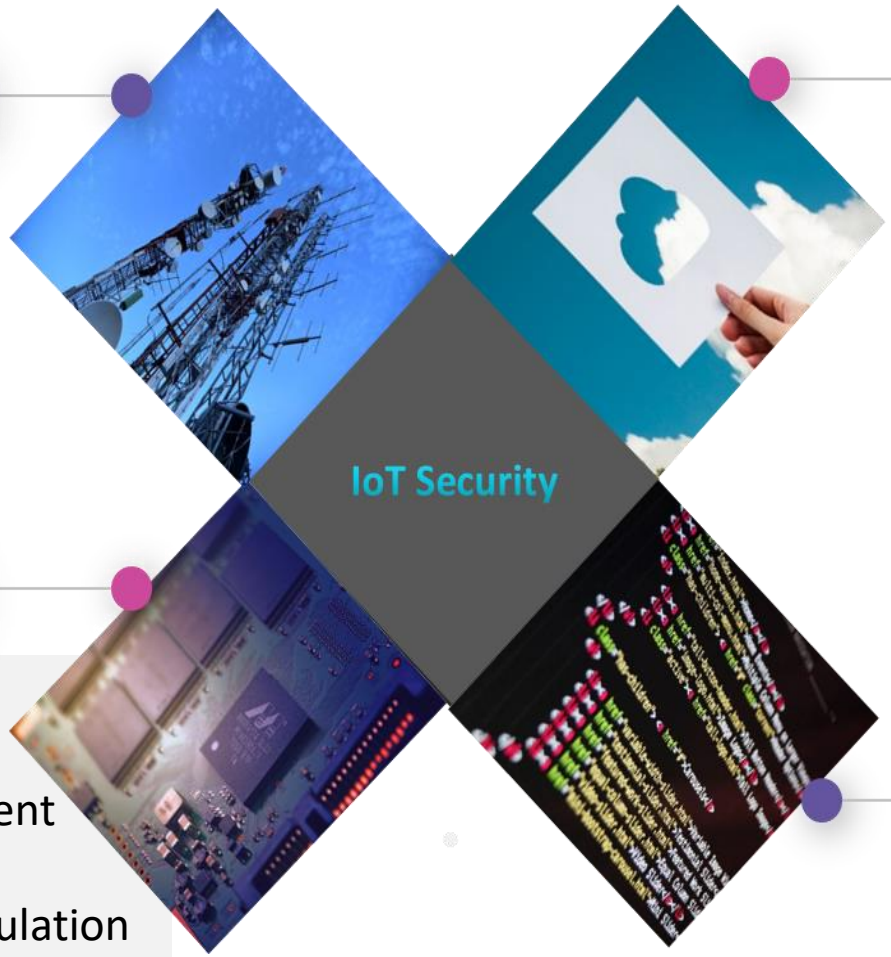
End to End IoT Security and Threats

IoT Network Security

- Man in the Middle
- DDoS/RDoS
- Virus (Trojans)

IoT Cloud Security

- Insecure APIs
- Service Traffic Hijacking
- Data Breach /Data Loss



IoT Hardware Security

- Low Cost Hardware Tampering
- Fake ADAS message sent V2V or V2X.
- Malicious data manipulation cause traffic outages

IoT Software Security

- Buffer overflows
- Malware

Major Vendors and their Specialisation - I

IoT Hardware Security

Embedded
SECURE RF
Securing the Internet of Things
SEQUITUR LABS
Rambus
NXP
Atmel
MICROCHIP
arm

Mobile
avast
baimos technologies
Lookout
Skycure
KASPERSKY
ZIMPERIUM
TRUSTONIC

Vehicles
Trillium
CUJO AI
MOCANA
ARGUS CYBER SECURITY
BAYSHORE
IoTium
sentryo
mPrest SYSTEMS LTD.

IoT Software Security

Database
QADIUM
1010DATA
Cockroach LABS
accelerite

Cloud
RedLock
skyhigh
afero
evident.io

Application
Twistlock
aqua
Qttify
appthority
Aporeto
TRUSTONIC

IoT Network Security

Gateway/Router
CLOUDFLARE
keezel
FILAMENT

End Point
CYLANCE
DUO SECURITY
MORPHISEC Moving Target Defense
CROWDSTRIKE
WEBROOT Smarter Cybersecurity
arm

Network Visibility
NOZOMI NETWORKS
SCADAfence
Karamba Security
PFP CYBERSECURITY
Bastille
SECURITY FOR THE INTERNET OF RADIOS
MOBILEUM

IoT Cloud Security

Perimeter and Network

Firewall	NGFW	IDS	IPS	VAS	Antivirus	Malware
BROCADE	Check Point SOFTWARE TECHNOLOGIES LTD.	KISMET + SOLUTIONS	WIRESHARK	Qualys.	McAfee	Check Point SOFTWARE TECHNOLOGIES LTD.
Barracuda	JUNIPER NETWORKS	ALERT LOGIC Security. Compliance. Cloud.	SURICATA	ALERT LOGIC Security. Compliance. Cloud.	Symantec.	OPSWAT
Cyberoam		SNORT	IBM	tenable		McAfee
		OSSEC	radware	OpenVAS		Symantec.
		SURICATA	SNORT			VMRAY

Application and Endpoint

EDR	Certificate Manager	WAF	PT	Web Gateway
McAfee	zscaler	BROCADE	RAPID7	Hewlett Packard Enterprise
Symantec.	OUTLIER	Barracuda		netsparker
		Trustwave		AppScan
		IMPERVA		IBM Security
				zscaler

Data Security

iDaas	FIM	DB VAS
Centrify	tripwire	Trustwave
onelogin	OSSEC	IMPERVA
okta		greensql Database Security & Compliance
		IBM

GRC and Audit

GRC	Audit
ThreadFix Powered by Denim Group	OPTIV
RSA	Open-AudIT
MetricStream	
TRIPLEHELIX	

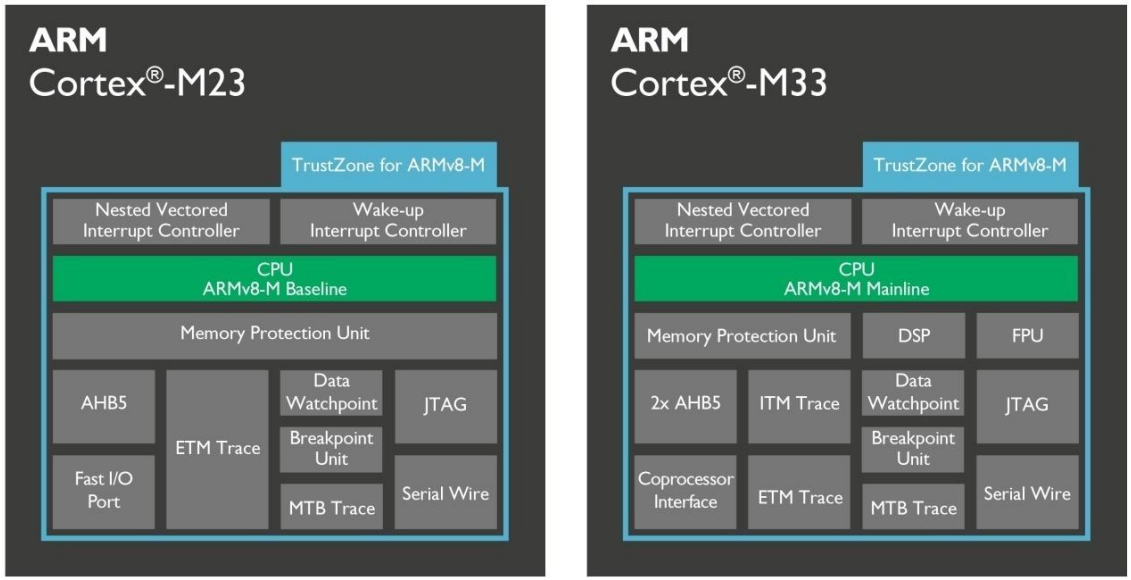
Security Orchestration

Malware	
netflexity	algosec
CloudPassage	tufin
AVANAN THE CLOUD SECURITY PLATFORM	Intellitactics
McAfee	CloudLock

Key Solution Against Threats

Is Trust Platform Module Good Enough ?

For: Ultra Low Power Processor →



← **For: High Performance**

ARM Trust Zone + Platform Security Architecture

arm

Analyse

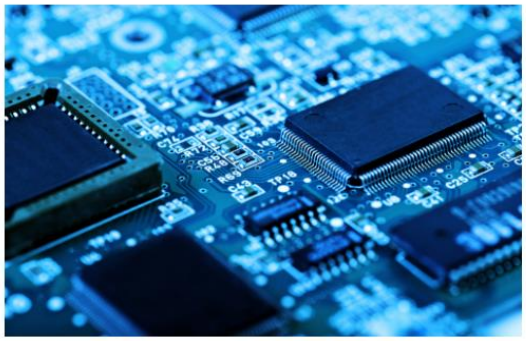
Threat Models and Security Analysis.

Architect

Architecture specifications.

Implement

Source code (OSS) and Hardware IP.



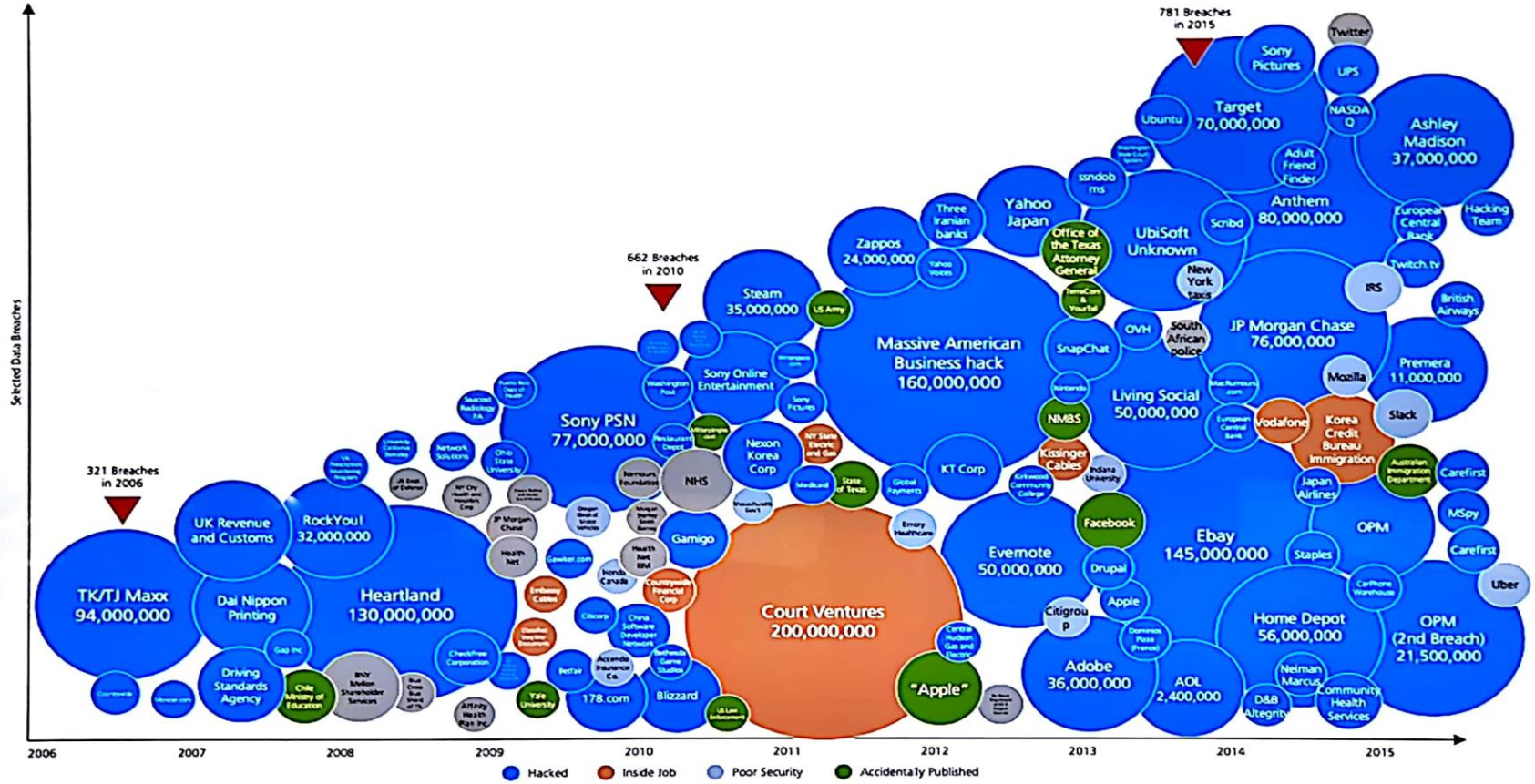
Major Solutions: Impacting the Industry

TRUSTONIC

DARKMATTER
GUARDED BY GENIUS

gemalto
security to be free

Data Breaches Continue to Escalate

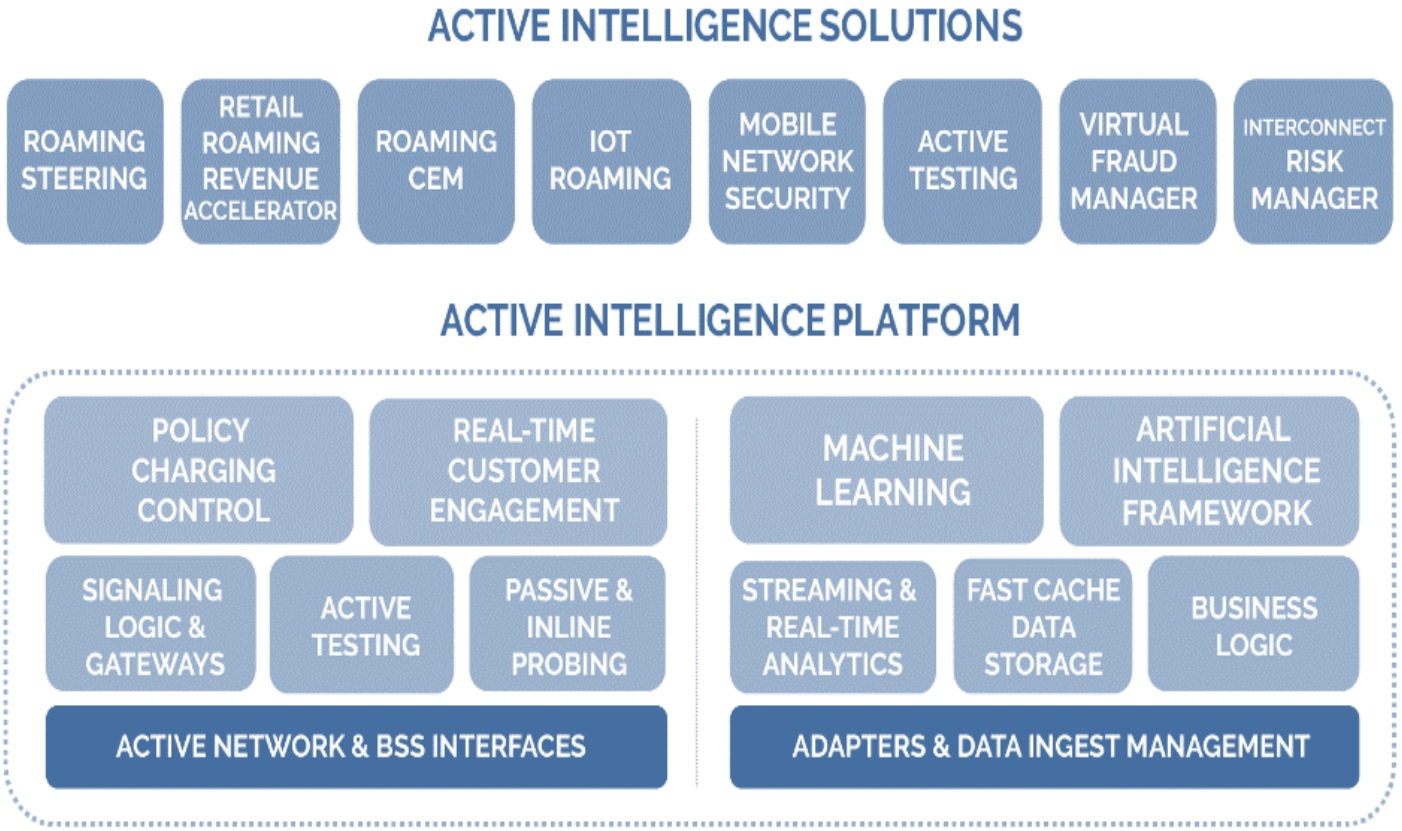


Source: Identity Theft Resource Cente, DataBreaches net, IdTheftCentre, informationisbeautiful net, press news reports and Risk Based Security (Data Breach Report, December 2015)

Major Solutions: Impacting the Industry

MOBILEUM

- The solution detects threats using analytics on a Hadoop based platform and correlates messages from multiprotocol signalling data. Real-time threat protection is available using firewalling at the interconnecting points.
- The one of the few vendors that initiated the adoption of artificial Intelligence and machine learning in network security .



Future of IoT Security

AI and Machine learning in Security: Plays important role on both sides

AI could go beyond monitoring and will provide a competitive edge to defenders that have primarily been absent from most cybersecurity technologies to date.

Threats by AI

VS

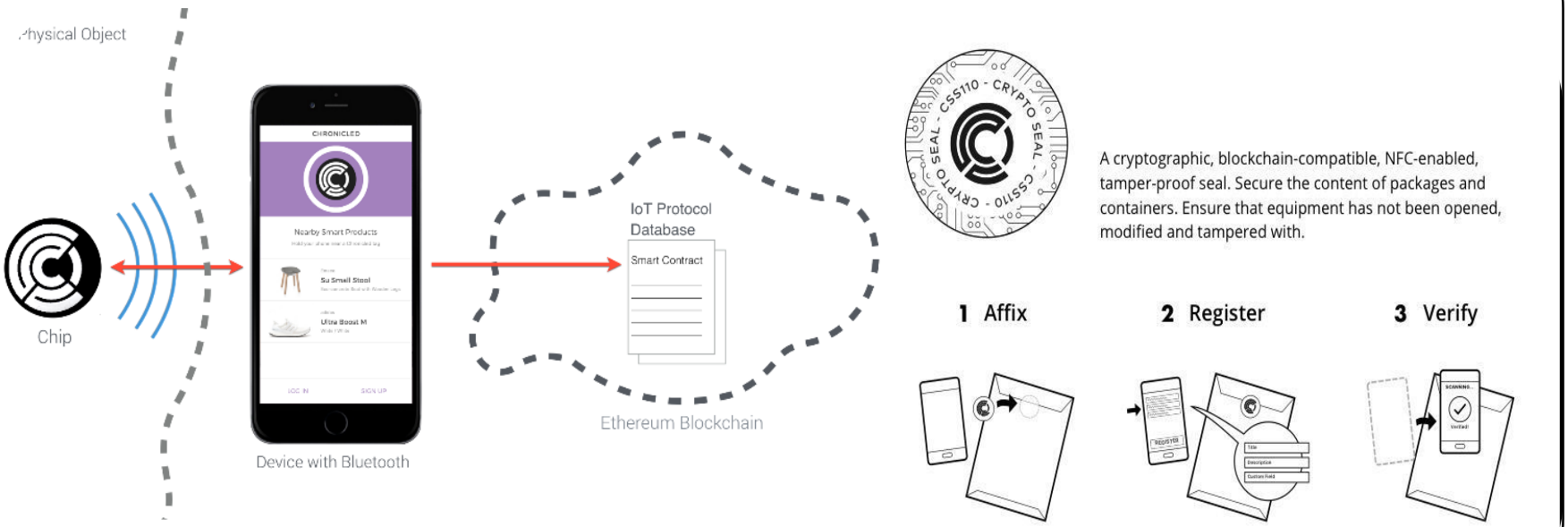
Safe Guarding IoT

On the flip side, attackers may deploy AI that will initiate automated hacks that are able to study and learn about the systems they target, and identify vulnerabilities, on the fly

Future of IoT Security : Blockchain

- In case of IoT, the blockchain will require infrastructure to manage device authentication, security and control layers, which is considerably more complex.
- **Asset tracking** – Chronicled A new pharmaceutical seal from Chronicled combines NFC chips with blockchain to track and secure prescription drugs.

Chronicled asset tracking blockchain concept showing single application Crypto Seal



The Upcoming Epidemic

Connected Car In-security:

- In **1Q2010,** more than 100 drivers in Austin, Texas found their cars disabled or the horns honking out of control.
- On **20th Feb 2018**, Tesla Cloud Servers Hacked By Cryptojackers. The hackers weren't content just to steal the sensitive data they found, so they also installed some cryptocurrency mining clients.

Fast and Furious car hack stunt, may turn real

Security in IoT Healthcare : Major Breach

- **On 29th august 2017,** The Food and Drug Administration issued an alert about the first recall of a network-connected implantable device due to cybersecurity vulnerabilities. .
- The recall of the Abbot cardiac devices was the key moment in the evolution of connected medical devices.
- Although there have been no reports of actual harm to patients due to hackers exploiting the vulnerabilities in the devices, that number can go from zero to a lot of patients quickly if hackers decide to launch attacks.

FDA recalls network-connected implantable devices

Abbott

FDA

Key Takeaways and Future Outlook

1

- Hacks to continue
- Default credentials (the easiest path) used frequently
- Evolution: Hackers will find other entry points
- Malware is currently basic – But more professional and well-funded attackers in future

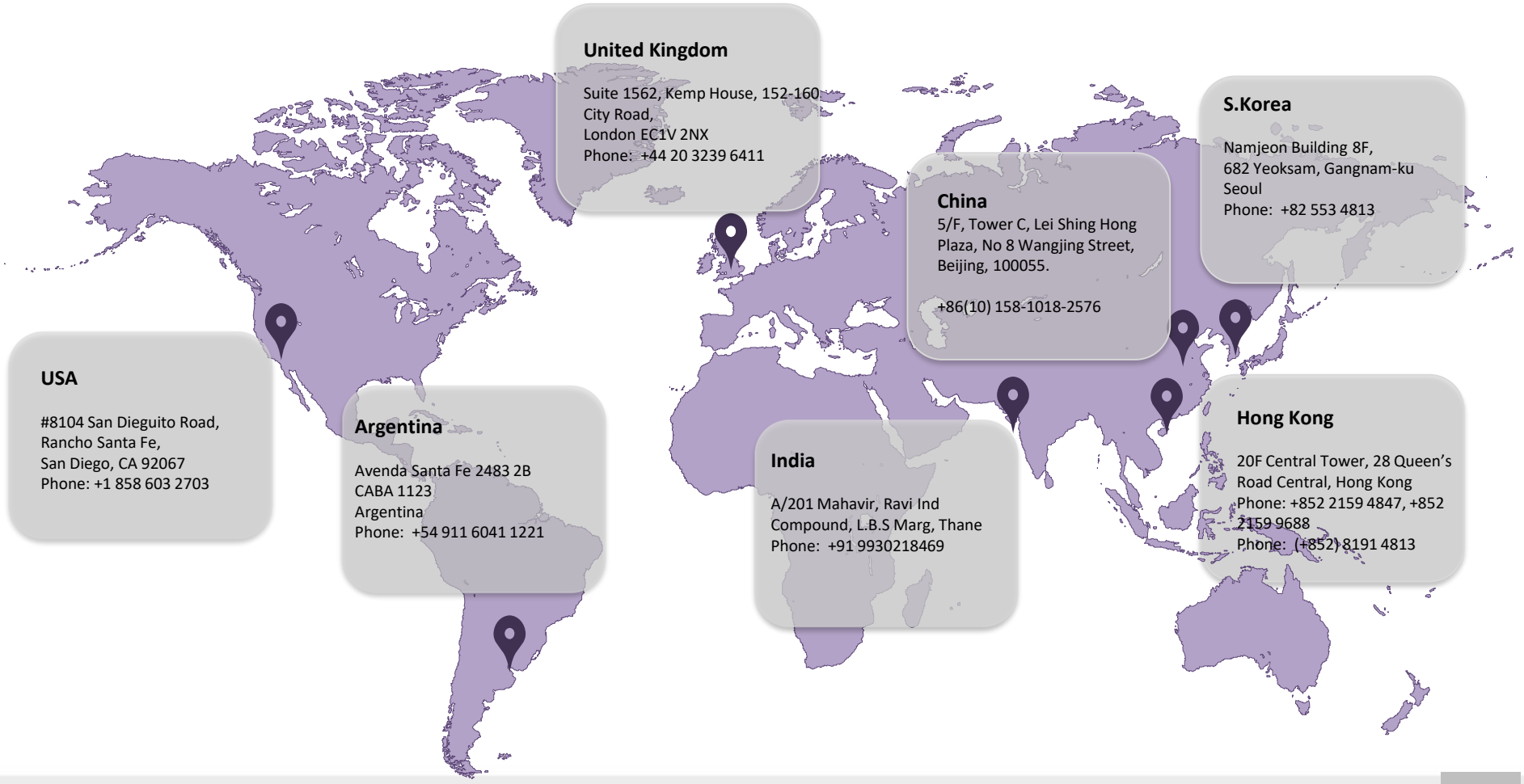
2

- More collaborations like “Cyber Threat Alliance” with concerted offerings
- Next gen offerings will fight malwares and botnets and learn/evolve on their own

3

- AI, ML and Blockchain will open doors for Intelligent Internet of Everything (IIoE)
- AI rewriting its own code to self-evolve and defend against ‘advance intelligent attacks’ in future

Contact Information



United Kingdom

Suite 1562, Kemp House, 152-160
City Road,
London EC1V 2NX
Phone: +44 20 3239 6411

China

5/F, Tower C, Lei Shing Hong Plaza, No 8 Wangjing Street, Beijing, 100055.

+86(10) 158-1018-2576

S.Korea

Namjeon Building 8F,
682 Yeoksam, Gangnam-ku
Seoul
Phone: +82 553 4813

USA

#8104 San Dieguito Road,
Rancho Santa Fe,
San Diego, CA 92067
Phone: +1 858 603 2703

Argentina

Avenda Santa Fe 2483 2B
CABA 1123
Argentina
Phone: +54 911 6041 1221

India

A/201 Mahavir, Ravi Ind Compound, L.B.S Marg, Thane
Phone: +91 9930218469

Hong Kong

20F Central Tower, 28 Queen's Road Central, Hong Kong
Phone: +852 2159 4847, +852 2159 9688
Phone: (+852) 8191 4813