



# XGen: the secret ingredient of next-gen security

Karen Karagedyan  
Regional Account Manager





The world is changing very fast.  
Big will not beat small anymore.  
It will be the FAST beating the  
slow.”

~ *Murdoch*

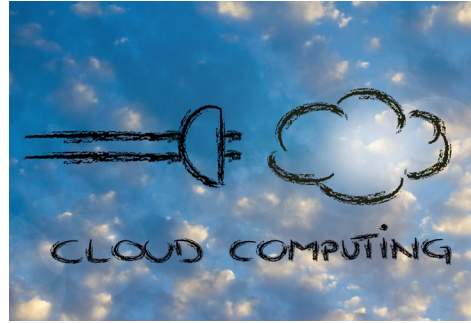
# CEO's Top Concerns

Operating in a Global Marketplace

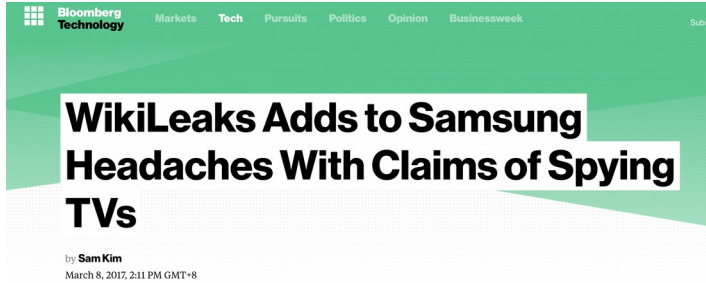
Keeping Costs Under Control

Regulation and Legislation

Talent Management





# Cyber Security Fear (March 2017)



**Change your passwords... again: Yet another Yahoo data breach affected 32 million accounts**

Data breaches becoming more complex, pervasive and damaging, finds Verizon's 2017 Data Breach Digest

## Verifone has been hit by a data breach at gas stations

BI Intelligence   
13h  925

## Arby's Data Breach Exposes 350,000 Records; 2017 Total Leaps Above 1 Million

HOME DEPOT

## Home Depot to Pay Banks \$25 Million in Data Breach Settlement

Jeff John Roberts  
6:44 AM SGT



## Uber, FitBit, OkCupid info exposed by massive data breach

The Verizon logo, consisting of the word "verizon" in a bold, lowercase sans-serif font, followed by a red checkmark symbol.

# Today's Business Reality

- Cyber attacks among **top 5 risks** says World Economic Forum
- **63%** of security professionals believe it is only a matter of time until their enterprise is targeted<sup>1</sup>
- **\$5.9M** is average cost of targeted attack<sup>3</sup>



1.Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security® Survey 2016

2.ISACA APT Awareness Study, 2013; 3. Verizon 2014 ; 4. Ponemon May 2014

# Cyberthreats (May 2017)

The image shows a ransomware window titled "Wana Decrypt0r 2.0" with a red background. The main heading reads "Ooops, your files have been encrypted!". Below this is a large padlock icon. A text box states: "Payment will be raised on 5/15/2017 23:37:34". The window contains several sections of text: "What Happened to My Computer?", "Can I Recover My Files?", and instructions on how to pay for decryption. At the bottom, there is a Bitcoin address: "13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94" and buttons for "Check Payment" and "Decrypt".

**Wana Decrypt0r 2.0**

Ooops, your files have been encrypted!

English

### What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

### Can I Recover My Files?

Yes. We guarantee that you can recover all your files safely and easily. But you have to pay for it. We will give you some of your files for free. Try now by clicking <Decrypt>. If you don't want to decrypt all your files, you need to pay. If you don't want to pay, you need to submit the payment. After that the price will be doubled. If you don't want to pay in 7 days, you won't be able to recover your files forever. If you don't want to pay in 6 months, you won't be able to recover your files forever.

Send \$300 worth of bitcoin to this address:

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Copy

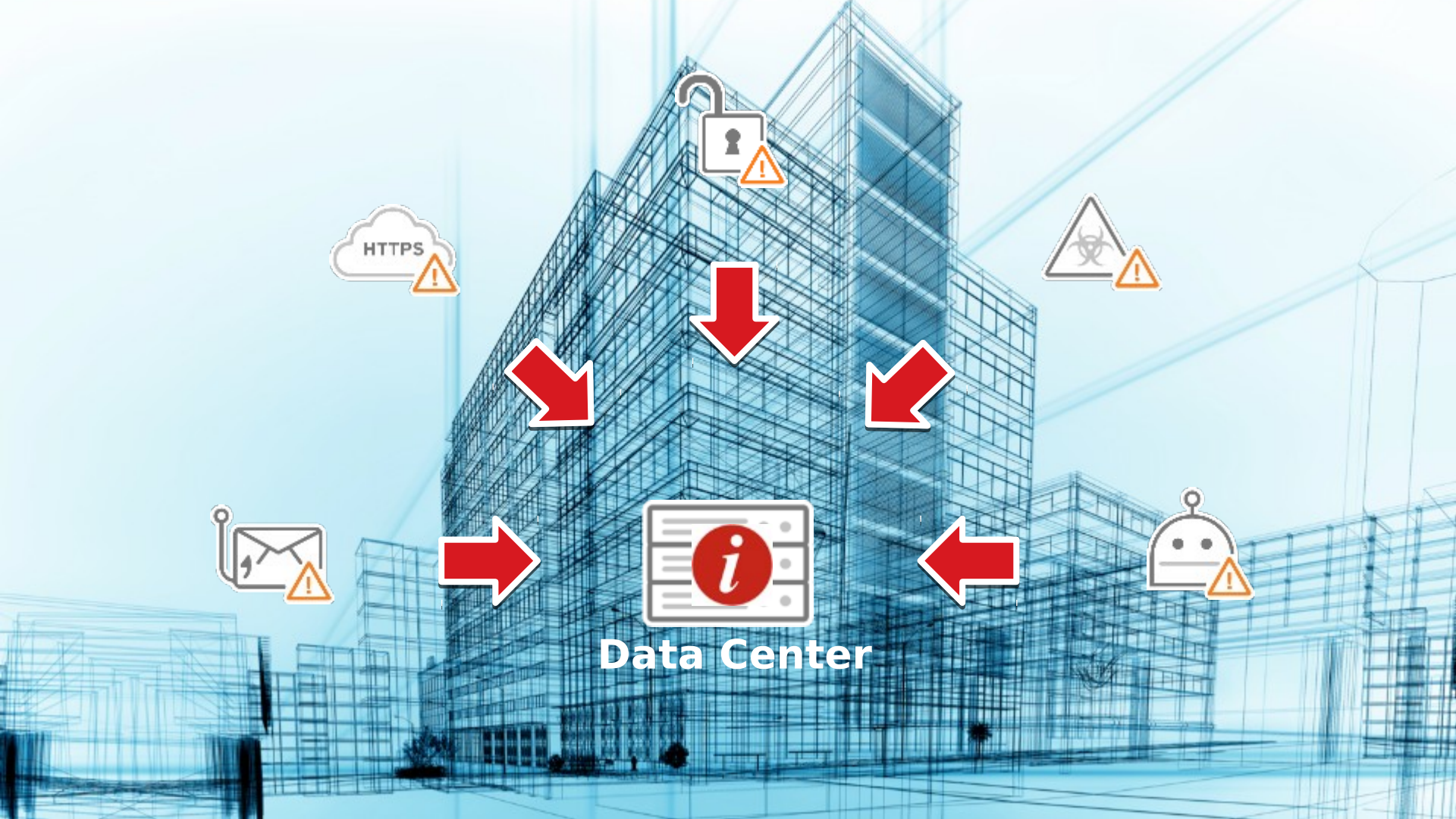
Check Payment Decrypt

The image shows a snippet of a news article from Kommersant.ru. The headline reads: "Кибератаки принесли вымогателям \$1 млрд". The website logo "Коммерсант.ru" is visible at the top left, and the URL "kommersant.ru" is at the bottom right.

**Коммерсант.ru**

## Кибератаки принесли вымогателям \$1 млрд

kommersant.ru



Data Center

 Complex Networks

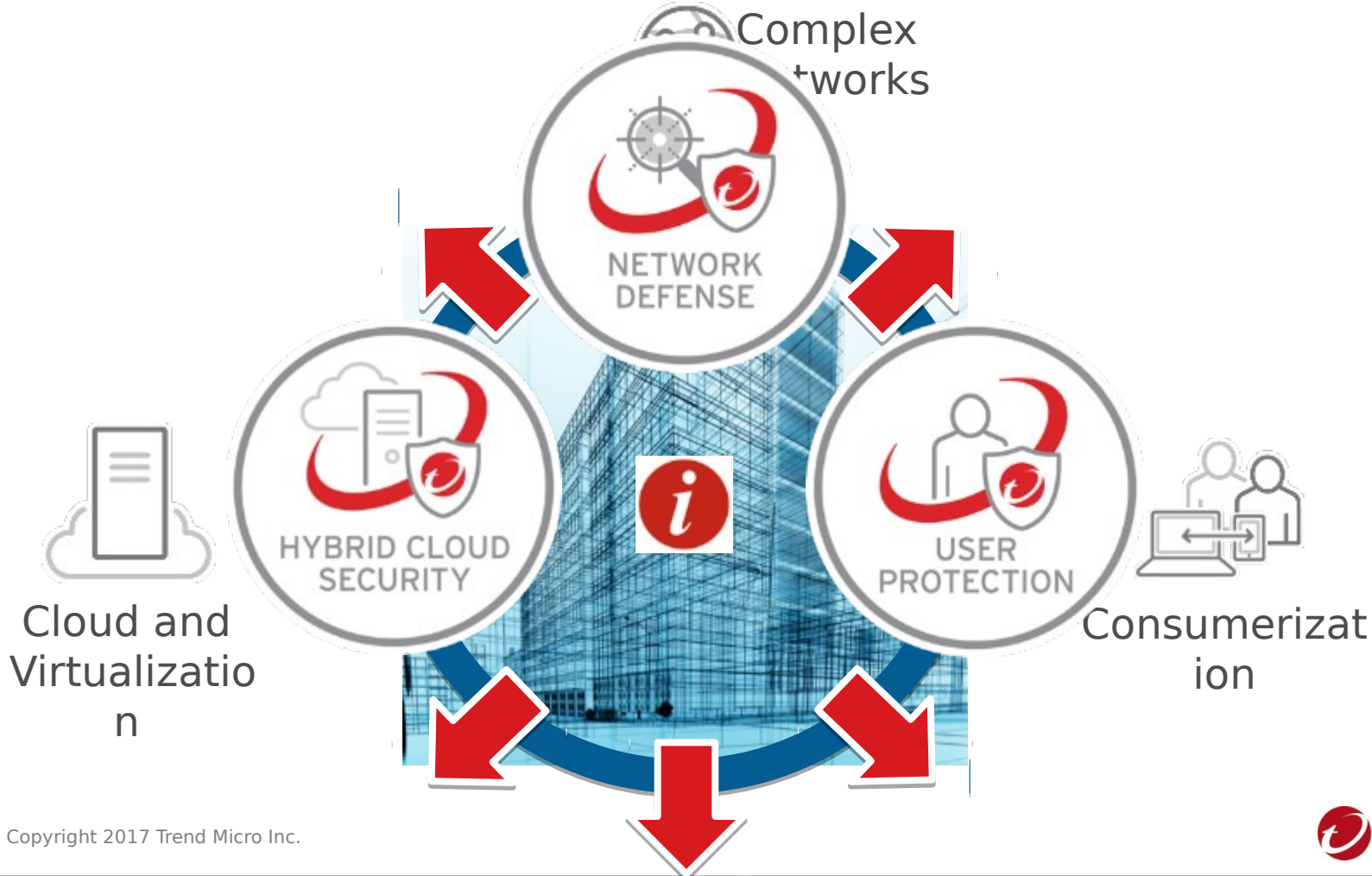


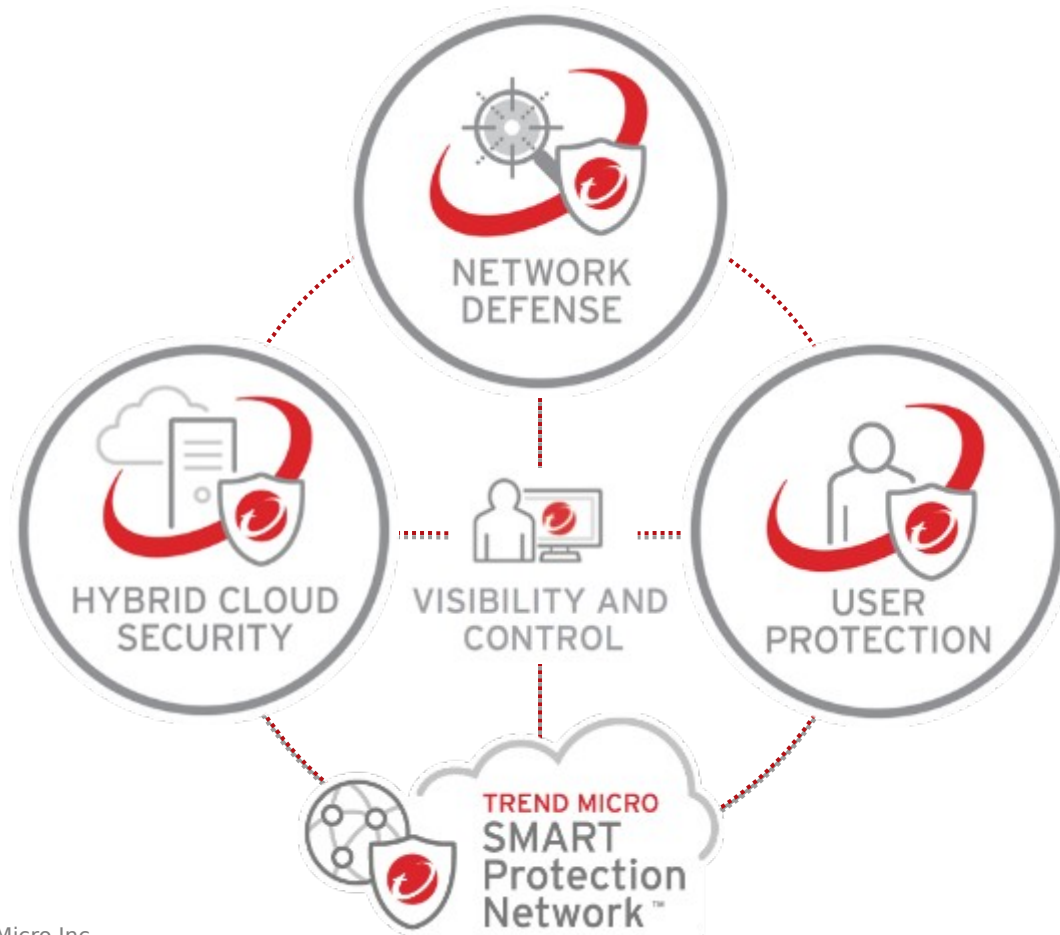
Cloud and  
Virtualization



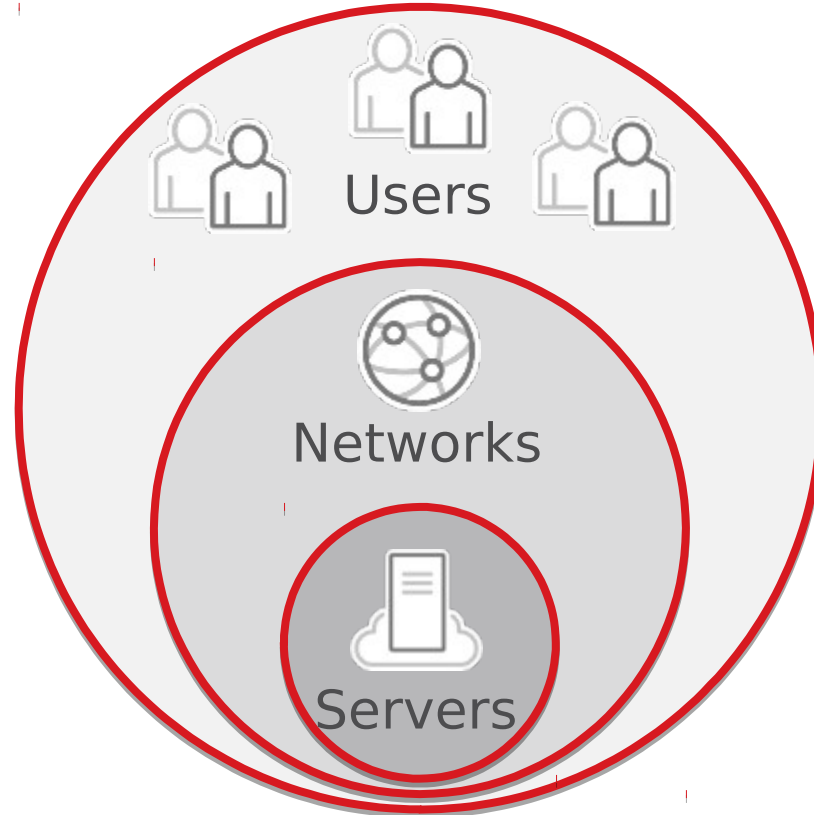
Consumerization







# Risk Management Requires Layered Protection



*Need for  
connected threat  
defense and  
centralized  
visibility  
increases*

# Connected Threat Defense: Better, Faster Protection

Enable rapid response through shared threat intelligence and delivery of real-time security updates

Gain centralized visibility across the system, and analyze and assess impact of threats

**RESPOND**

**PROTECT**

VISIBILITY AND CONTROL

**DETECT**

Assess potential vulnerabilities and proactively protect endpoints, servers and applications

Detect advanced malware, behavior and communications invisible to standard defenses

FSI

Mfg.

Public

Telco/IT Services

Util/Transport



# A Few Facts About Trend Micro

- 29 years focused on security software, now largest pure-play
- Headquartered in Japan, Tokyo Exchange Nikkei Index (4704)
- 8 consecutive years on Dow Jones Sustainability Indexes



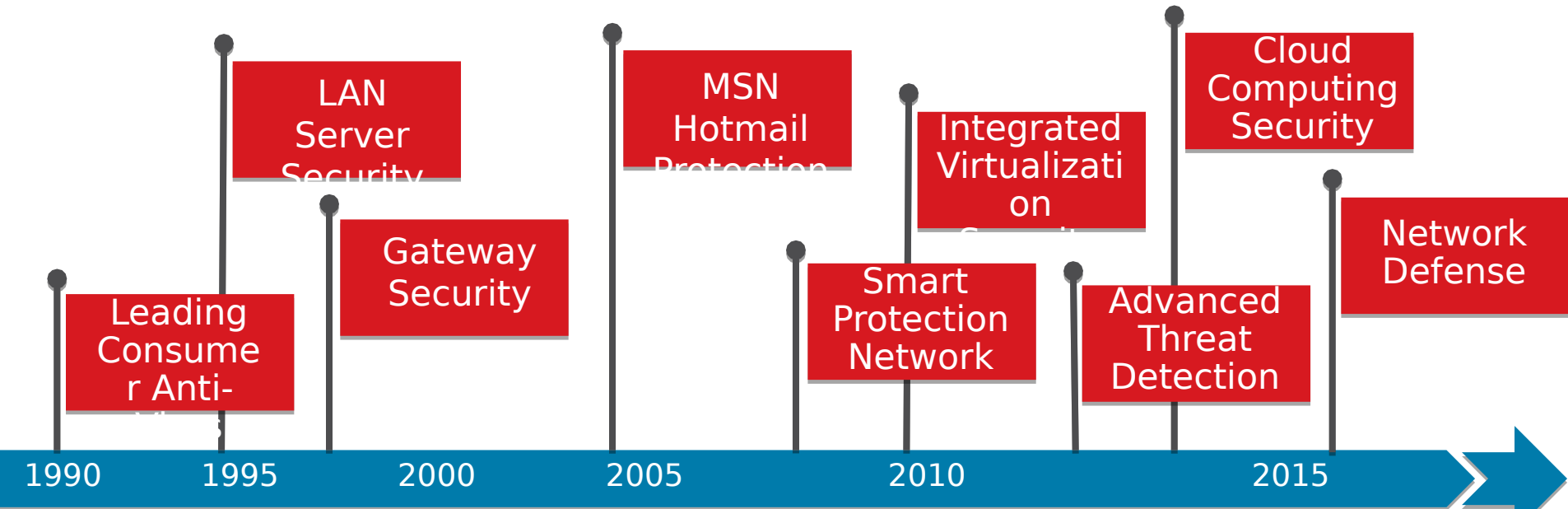
**500k commercial customers & 1.55M endpoints**

Businesses worldwide

# Why Trend Micro?

---

# Anticipated Key Shifts Well with Number of Firsts!

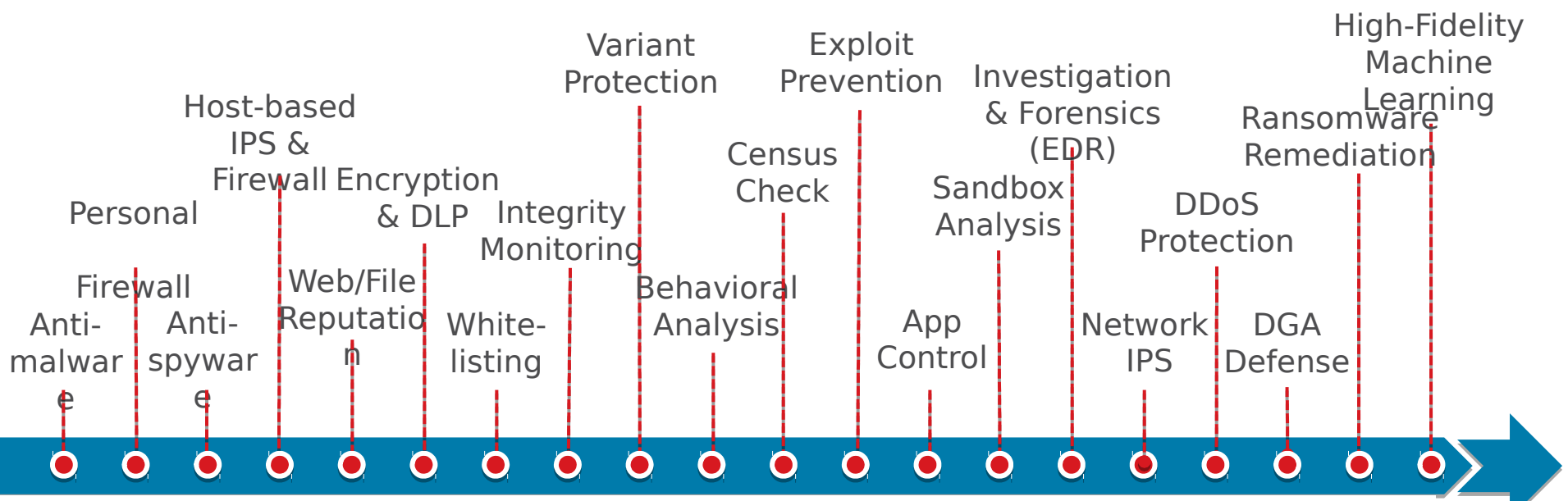




threats still out there. Must continually innovate to stay one step ahead.

# CONTINUOUS INNOVATION OF THREAT DEFENSE

## Techniques





**80%**

**Had network attacks or exploits their networks**

KNOWN BAD

KNOWN GOOD

Years ago, the threat landscape was black and white

## KNOWN BAD



Anti  
Malware



Blacklistin  
g



Whitelisti  
ng



Applicatio  
n Control

A number of classic threat defense techniques tackle these



Conte  
nt  
Filterin  
g



Encryption

# UNKNOWN



*Zero-day attacks*



*Ransomware*

Now, the “grey” is growing and is much harder to defend against



*Business  
Email  
Compromise*



*Lateral  
movement*



*Targeted  
attacks*

Only ~~60%~~ seconds

of information breaches  
are captured by  
transmission

# XGen<sup>TM</sup>

Delivering the best protection against the full  
range of  
KNOWN *and* UNKNOWN threats





# SMART. Unique Blend to Protect Endpoints

## Officescan XGEN Endpoint Protection

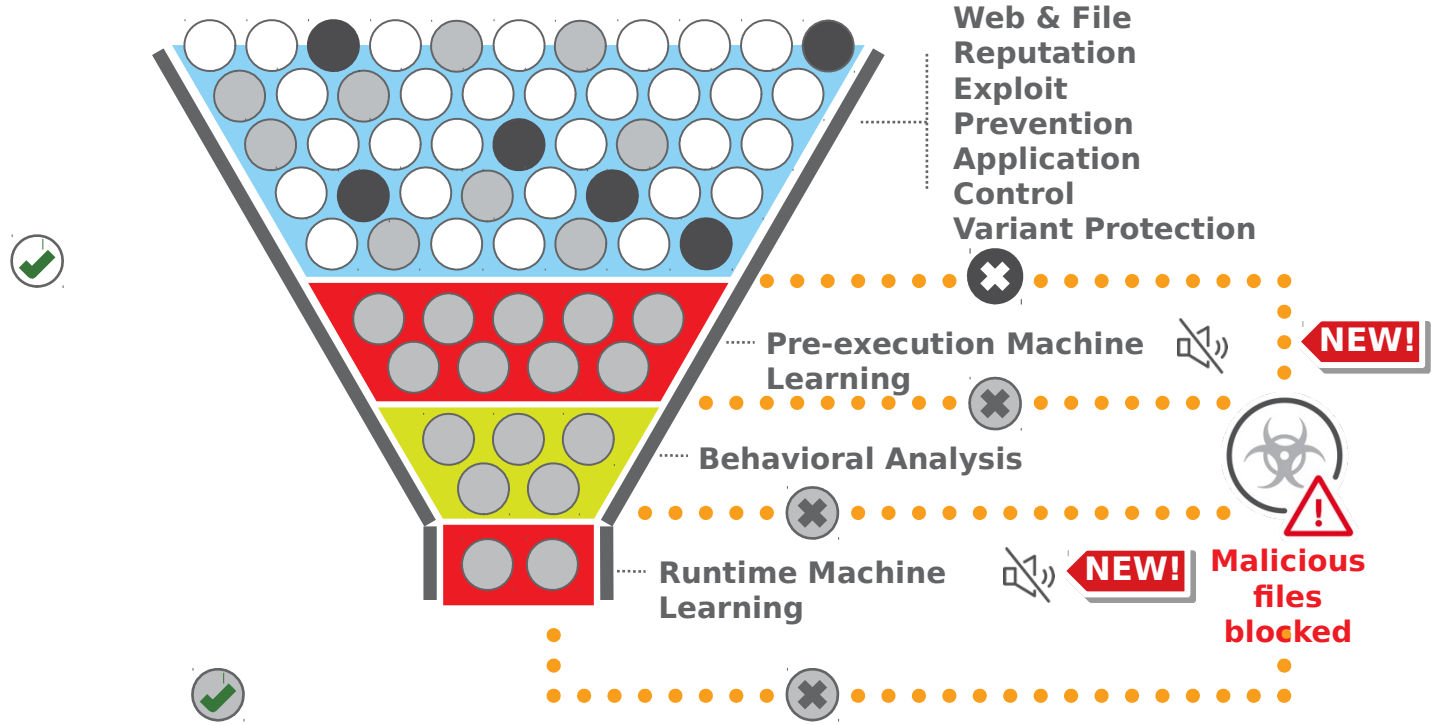
LEGEND

○ Known Good Data

● Known Bad Data

● Unknown Data

🔇 Noise Cancellation

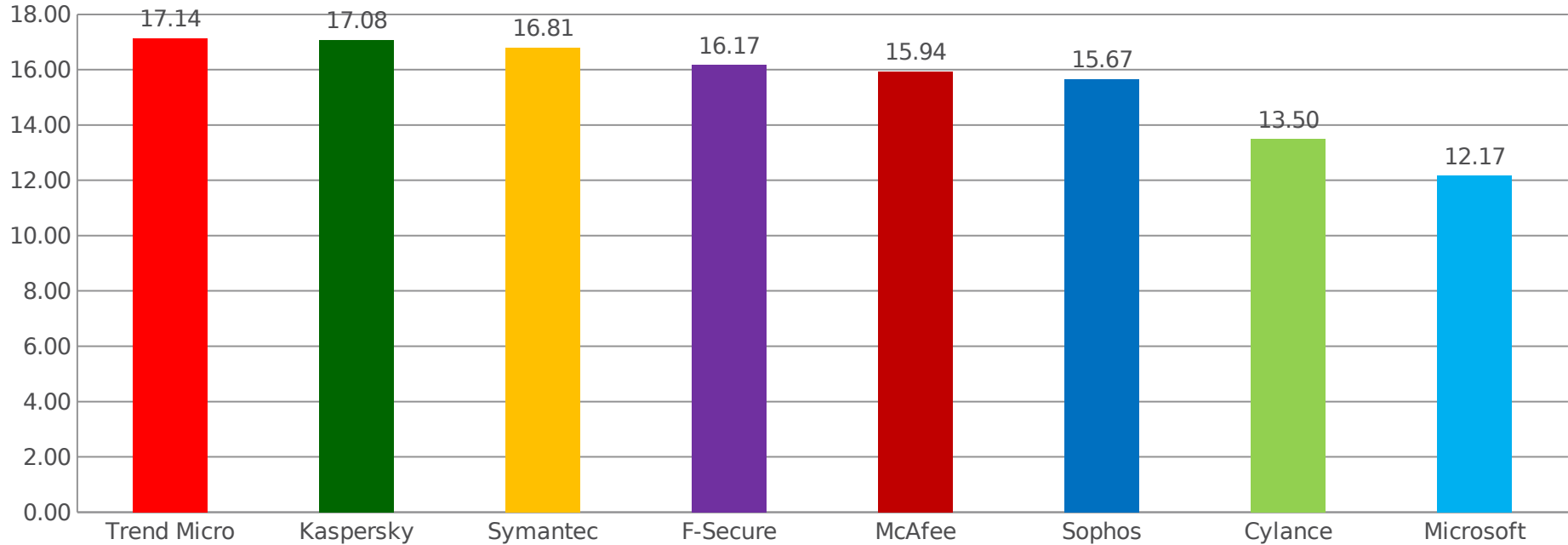


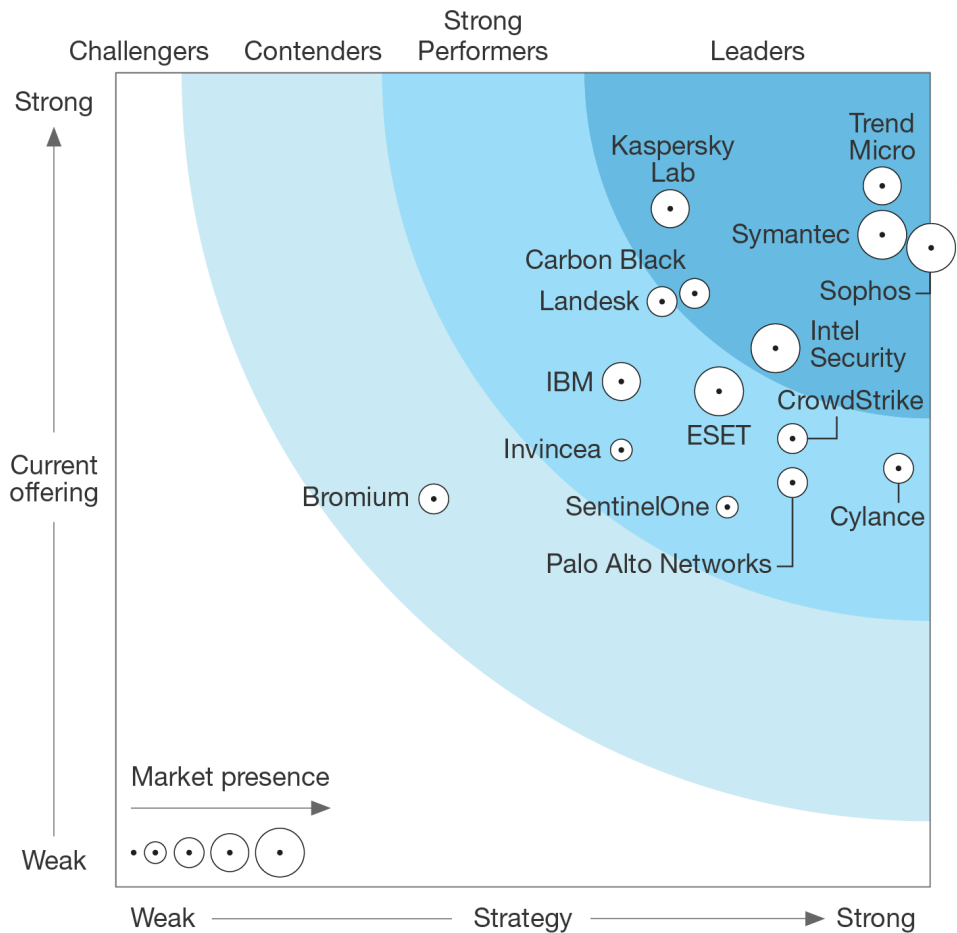
Safe files allowed



# Best Score for 3 Years

Includes performance, protection (prevalent & 0-day) & usability





# FORRESTER®

## Forrester Wave: Endpoint Security Suites, Q4 '16

# Gartner Magic Quadrant for Endpoint Protection Platforms

January 2017

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from

<https://resources.trendmicro.com/Gartner-Magic-Quadrant-Endpoints.html>

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.



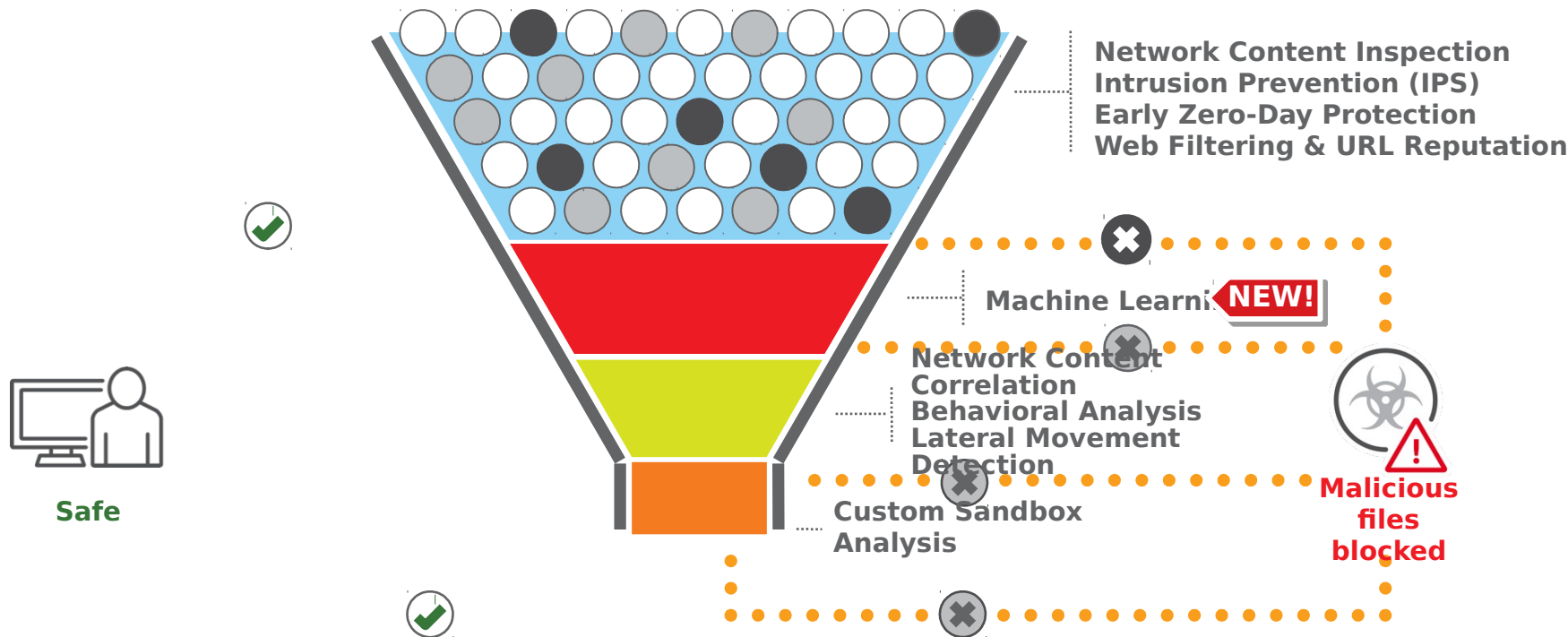


# Networks

## Deep Discovery/Tipping Point Network APT/IPS Protection

**LEGEND**

- Known Good (White circle)
- Known Bad (Black circle)
- Unknown (Grey circle)



Wire-speed

prevention

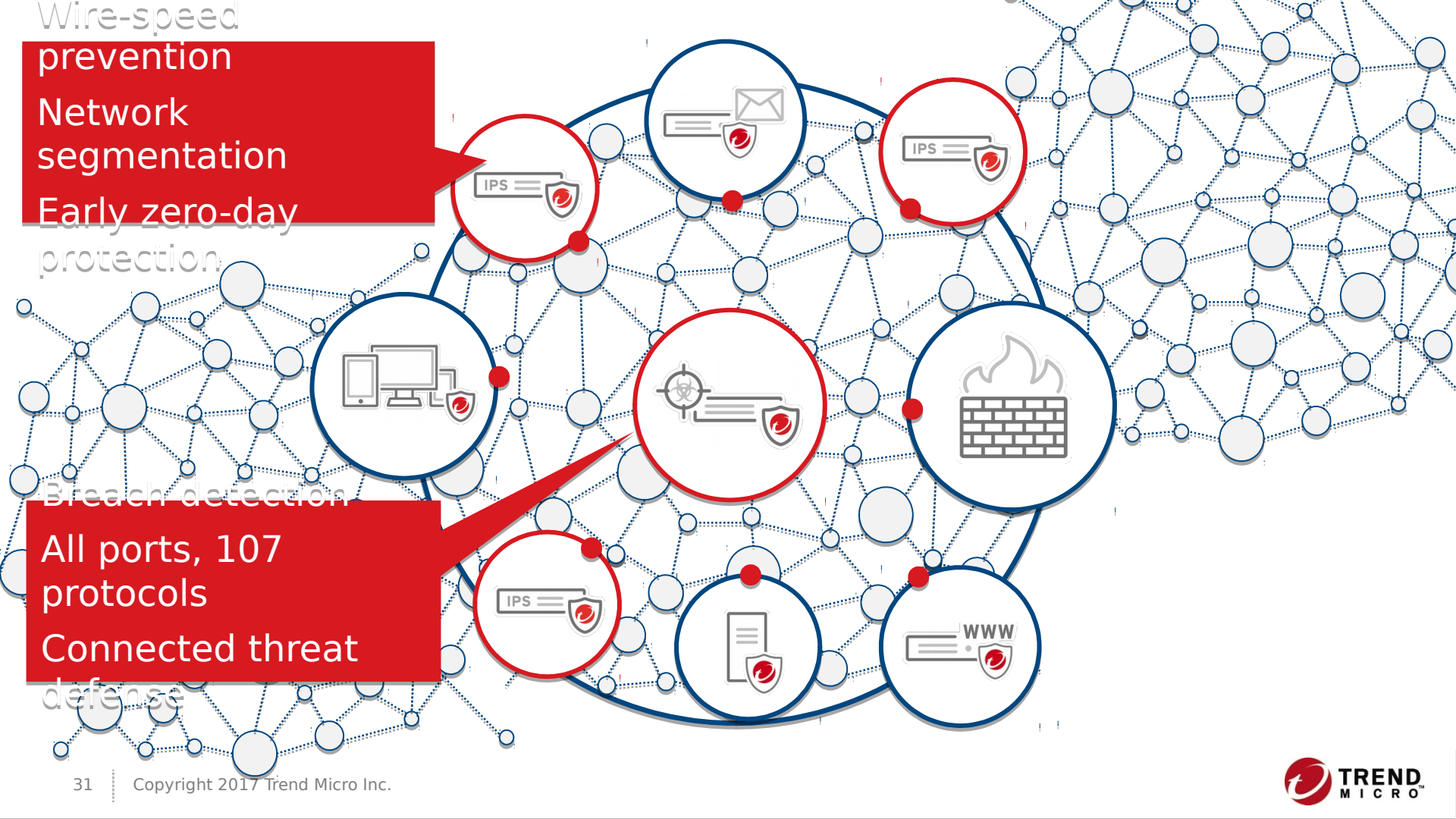
Network  
segmentation

Early zero-day  
protection

Breach detection

All ports, 107  
protocols

Connected threat  
defense





**RECOMMENDED**

Breach Detection System

**3 YEARS IN A ROW**

**99.8%** Detection Rate



TippingPoint

**RECOMMENDED**

Next-Generation IPS

**99.5%** Security Effectiveness



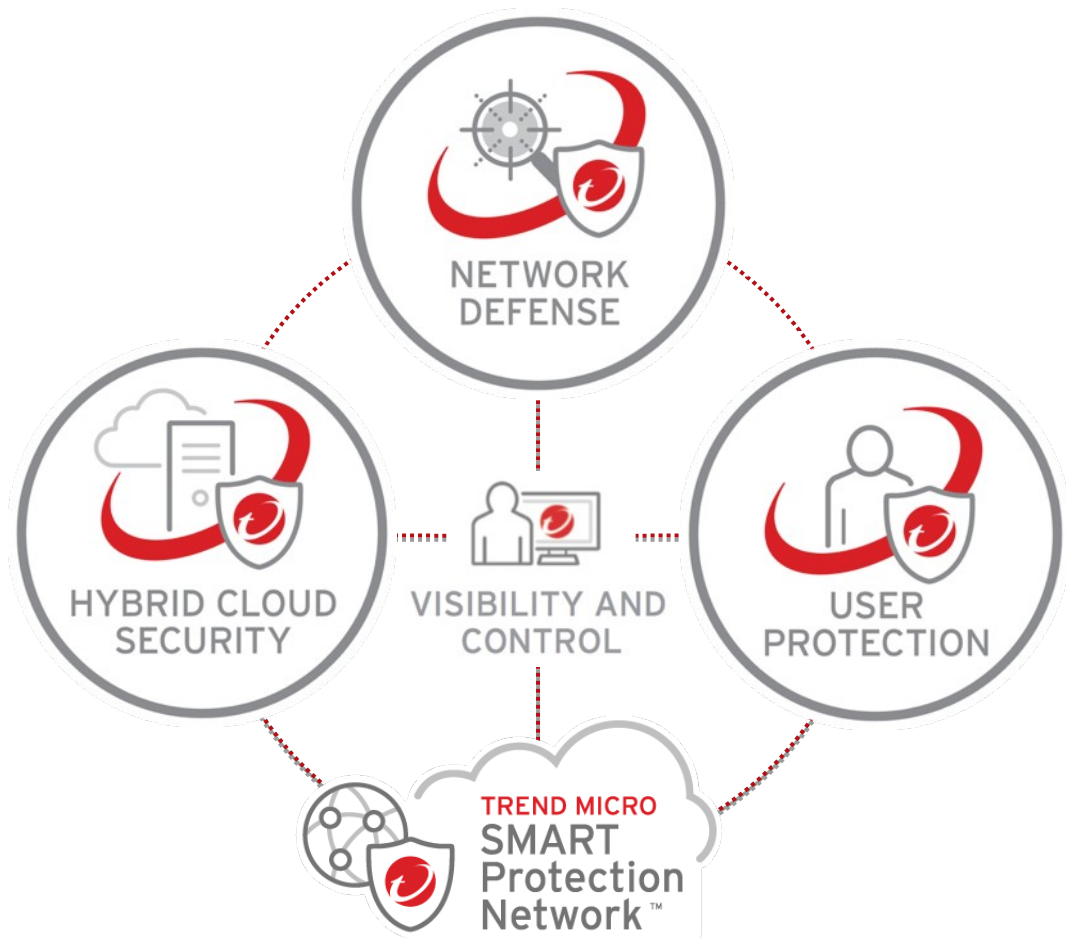
# Gartner Magic Quadrant for Intrusion Detection and Prevention Systems January, 2017

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from: <http://www.trendmicro.com/us/business/cyber-security/gartner-idps-report/>

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.



As of January 2017



# SMART: Unique Blend to Protect Workloads *Deep Security for Physical, VM and Cloud Instances*

LEGEND



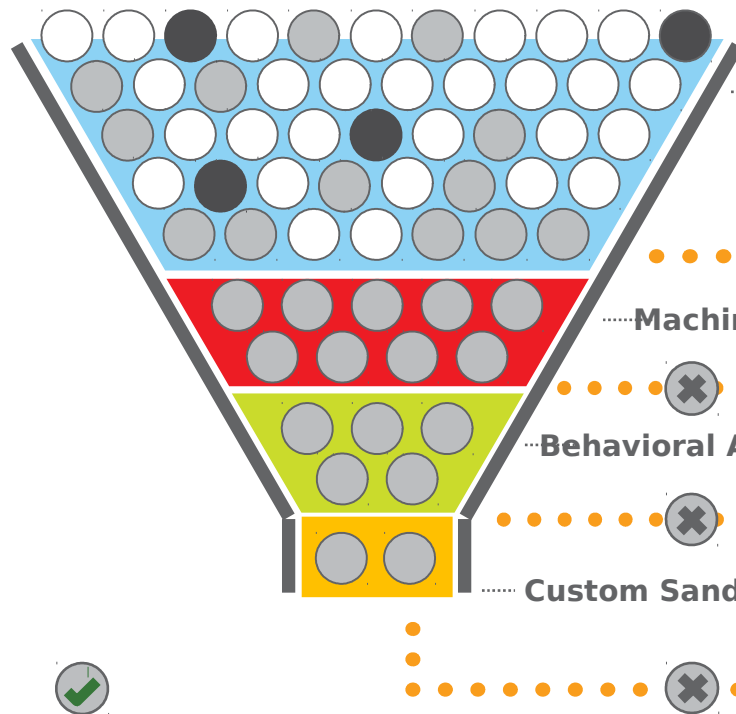
Known Good



Known Bad



Unknown



Anti-Malware & Web

Reputation

Intrusion Prevention (IPS) &  
Firewall

Integrity Monitoring & Log  
Inspection **NEW!**

Application Control

Machine Learning **SOON!**

Behavioral Analysis **NEW!**

Custom Sandbox Ar **NEW!**

Malicious  
files &  
actions  
blocked

Safe files &  
actions  
allowed

# Trend Micro DV Labs Advantage



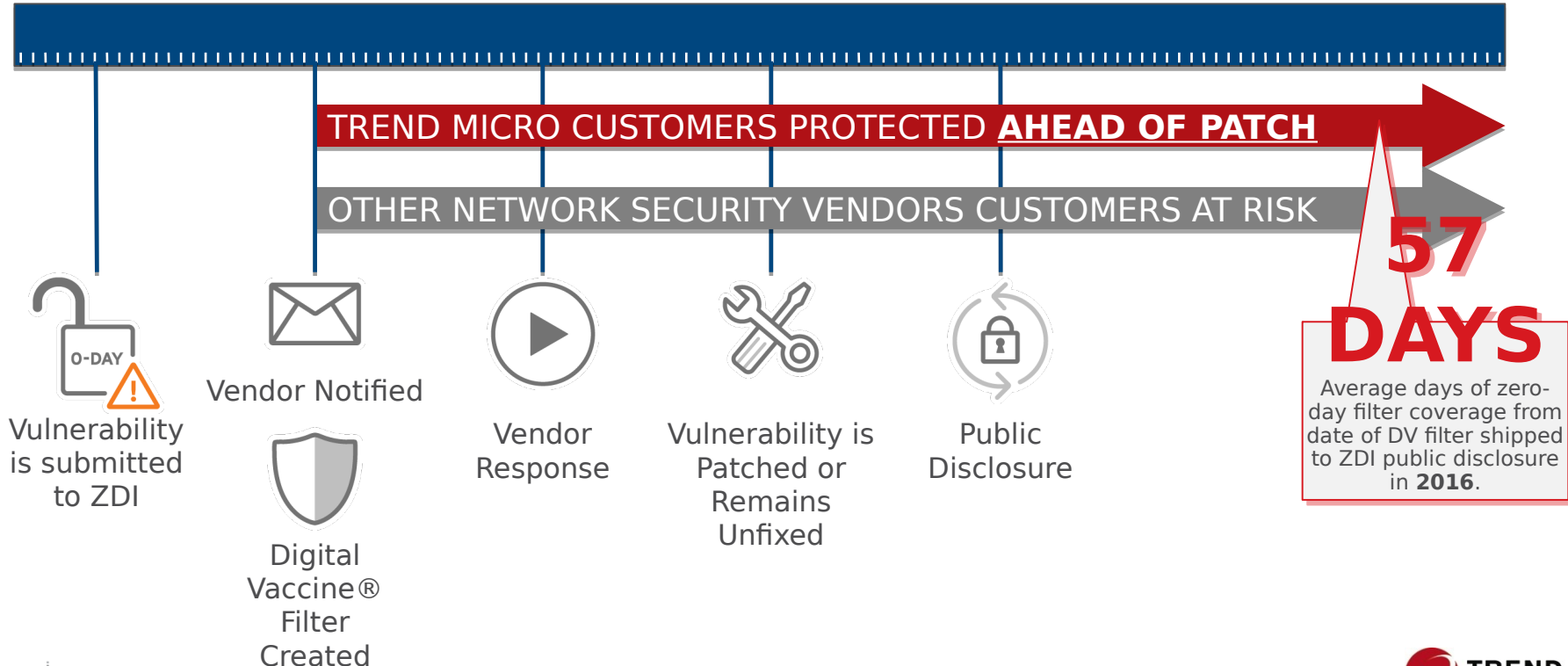
Over **650**  
vulnerabilities  
published in 2016

## DV Labs



Delivers **11** zero-  
day filters/week

# Zero Day Initiative: Preemptive Protection for “Undisclosed” Vulnerabilities



# Block early!



Microsoft

**#1** external supplier of bugs to MSFT

Average **181 days** of zero-day prediscovered filter coverage for 2015 bulletins



Adobe

**#1** external supplier of Adobe Reader vulnerabilities

Average **101 days** of zero-day prediscovered filter coverage for 2015 bulletins



OpenSSL vulnerability similar to Heartbleed

Digital Vaccine provided **43 days** of coverage before OpenSSL Group released a patch

Performance

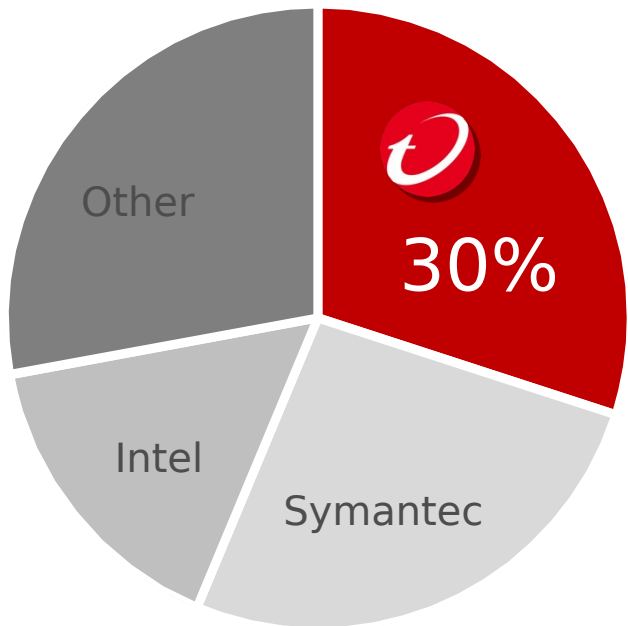
nce



**“Security  
can’t slow  
me down!”**



The **MARKET LEADER** in server security for the **7<sup>th</sup>** straight year!

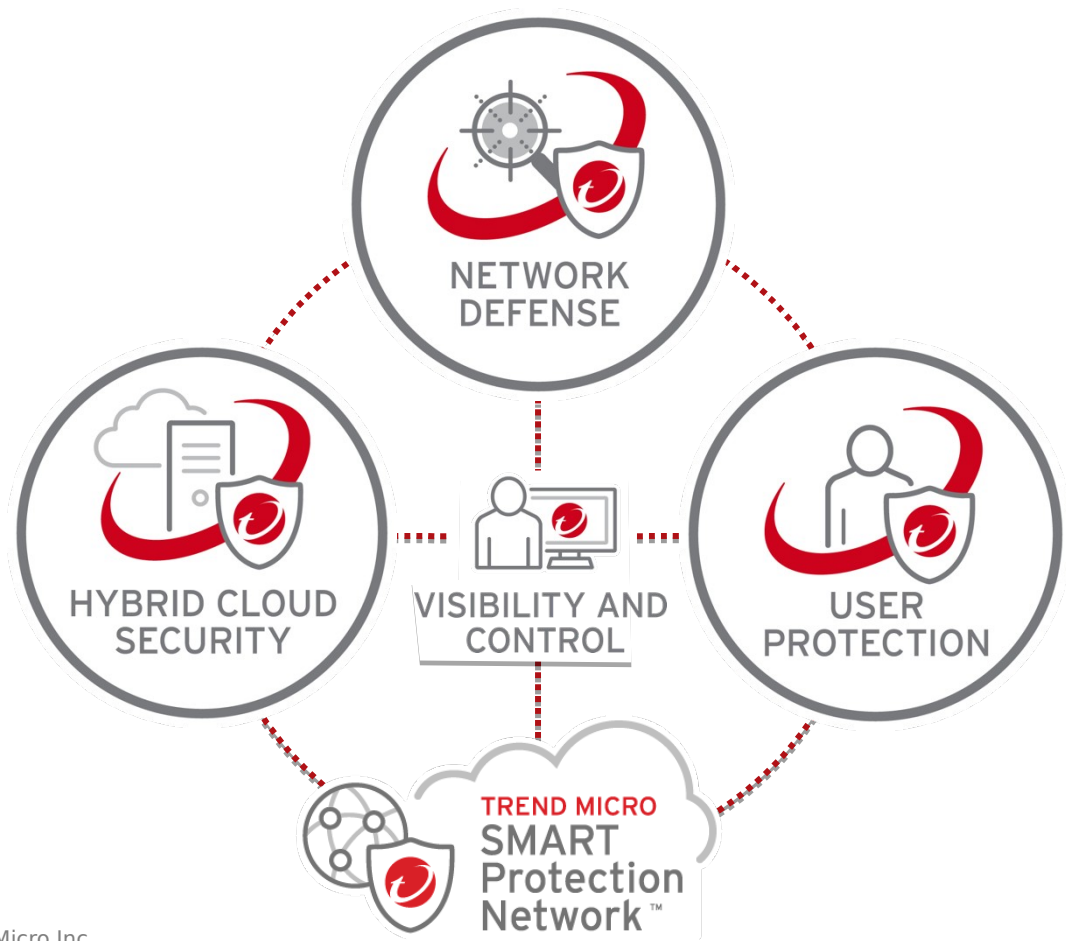


**CERTIFIED** for key environments AND for security



**EAL 2**

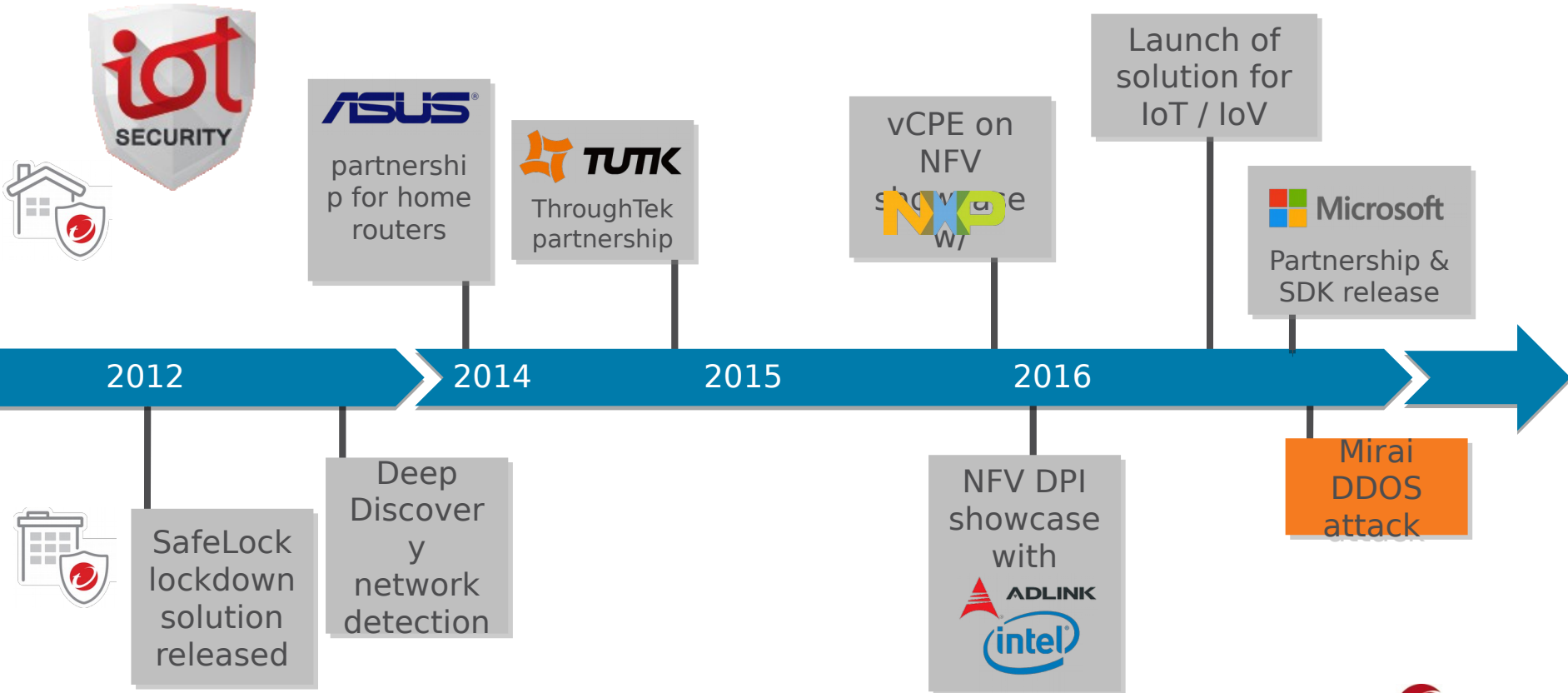




# Security Threats in the IoT Era



# Trend Micro IoT Initiatives Gaining Speed



# We Share Our Customers' Vision



A world **SAFE** for  
exchanging  
digital information

# Thank You

---