RSA®Conference2016

Abu Dhabi | 15–16 November | Emirates Palace

Connect to Protect

SESSION ID: SPO1-W06B

Moving Beyond Legacy Endpoint Security Technology

Richard Melick

Technology and Product Evangelist
Cylance
@RCMelick

#RSAC

RSA®Conference2016 **Abu Dhabi**

"If you need a machine and don't buy it, then you will ultimately find that you have paid for it and don't have it." *- Henry Ford*
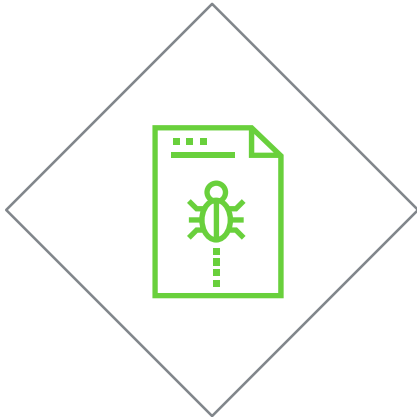
The Current Endpoint Cannot Keep Up

- Legacy technology is reactive

- Reactive cannot scale with the amount and speed of today's malware

  - 99% of malware hashes are seen for only 58 seconds or less

  - In 93% of data breaches, compromise occurred in minutes or less

  - 362,000 new crypto-ransomware variants were spotted in 2015 (source: Symantec)

RSAConference2016 **Abu Dhabi**

- Data breach news has become a part of daily life

- Yahoo, Cisco, FourSquare, Home Depot, United Airlines, OPM, Anthem Blue Shield, JPMorgan Chase

- 5,195 known data breaches since 2005
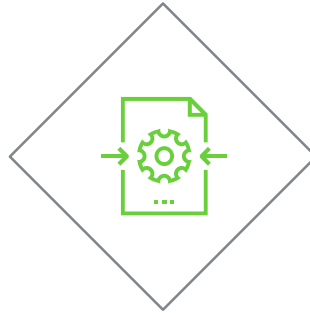 - That's only counting US based data breaches

CYLANCE

RSA Conference2016 Abu Dhabi

900,875,242
Breached Records

CYLANCE

The Layered Approach

AV

HIPS/
Anti-Exploitation

Sandboxing

Behavioral

EDR

RSA Conference2016 Abu Dhabi

The Reactive Solution

ALL KNOWN
MALWARE

+

NEW MALWARE
(LAST 24 HOURS)

COLLECT

TRIAGE AND
CLASSIFY

HUMAN MALWARE
RESEARCHERS
AND AUTOMATION

CLOUD
THREAT DB

SIGNATURE
FILE

SECURITY ADMIN
UPDATES

TEST
SIGNATURE FILE

DEPLOY
SIGNATURE

ZERO-DAY
MALWARE

RSAConference2016 Abu Dhabi
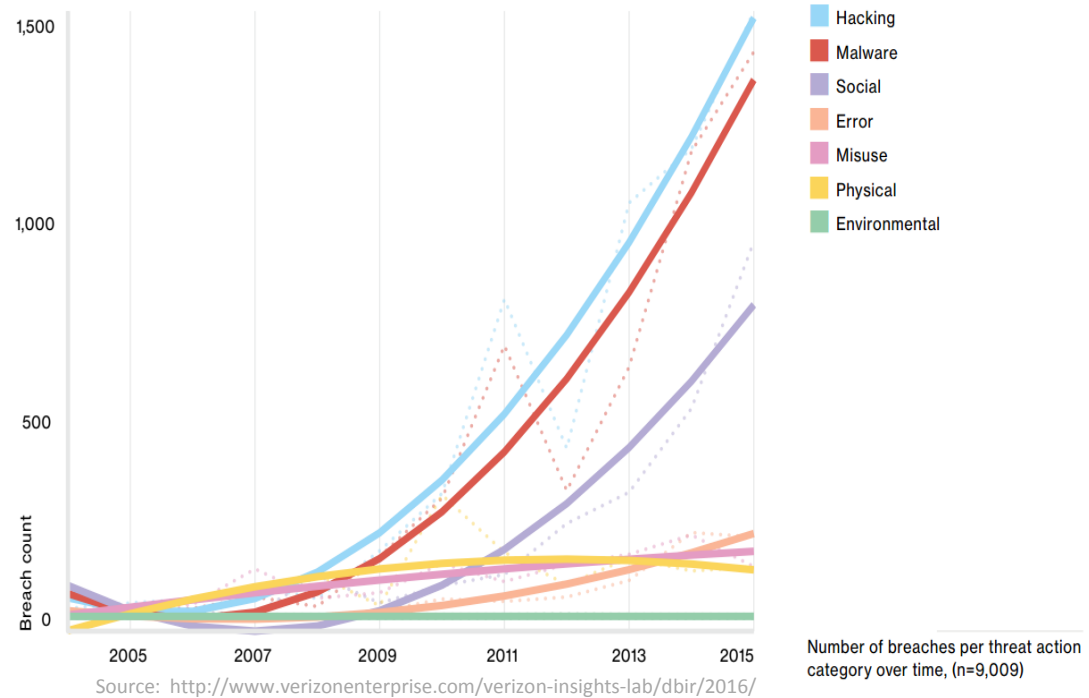
CYLANCE

RSA®Conference2016 **Abu Dhabi**
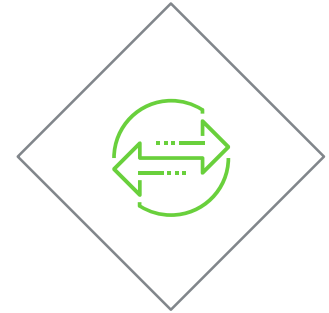
"Today's AV model makes everyone a sacrificial lamb." *- Zheng Bu and Rob Rachwald, FireEye*
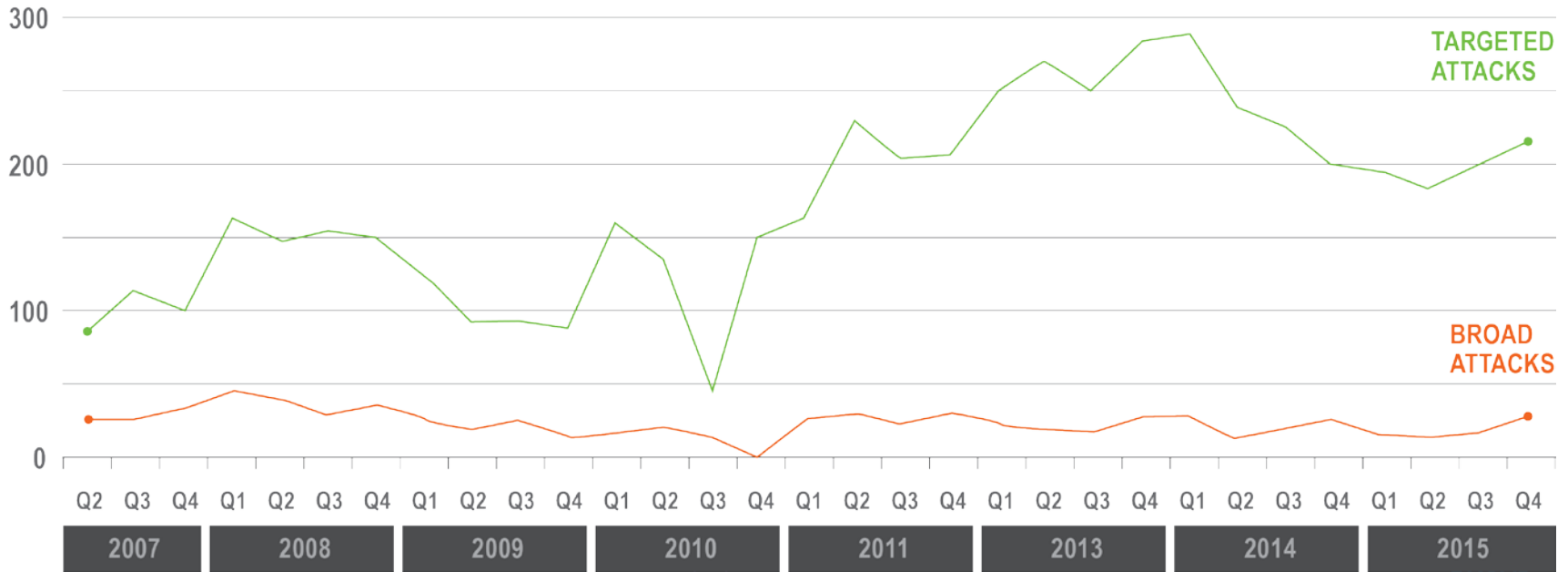
2016 Verizon DBIR

- Malware is used in 90% of cyber incidents

- Adversaries create huge numbers of malware variants to avoid detection... or they design one just for you

- Unique malware is the norm rendering traditional AV totally useless.

Number of breaches per threat action category over time, (n=9,009)

Source: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

CYLANCE

RSAConference2016 Abu Dhabi

Source: CyberFactors, a subsidiary of CyberRisk Partners and CloudInsure.com
http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014

RSAConference2016 Abu Dhabi

The Standard Security Philosophy

- Customers expected to invest more time, money, and energy

- The security results are staying the same
  - 370,000 pieces of malware recorded daily (AV-Test)
  - 5,195 known data breaches since 2005
    - 1.7 data breaches PER day
  - These are all the known and reported attacks

- Customers deserve a different approach to security

CYLANCE

RSAConference2016 **Abu Dhabi**

The Cost of a Breach

- Cyber Crime costs jump 19% in 2016

- Unmitigated attack is $40,000 per hour for businesses

- Average annual losses to companies worldwide now exceed $7.7 million

- Some companies studied lost up to $65 million

Source: Ponemon Institute - http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/

CYLANCE

RSAConference2016 Abu Dhabi

"The traditional signature-based approaches to endpoint security are dead…" *– David Duncan, Webroot*
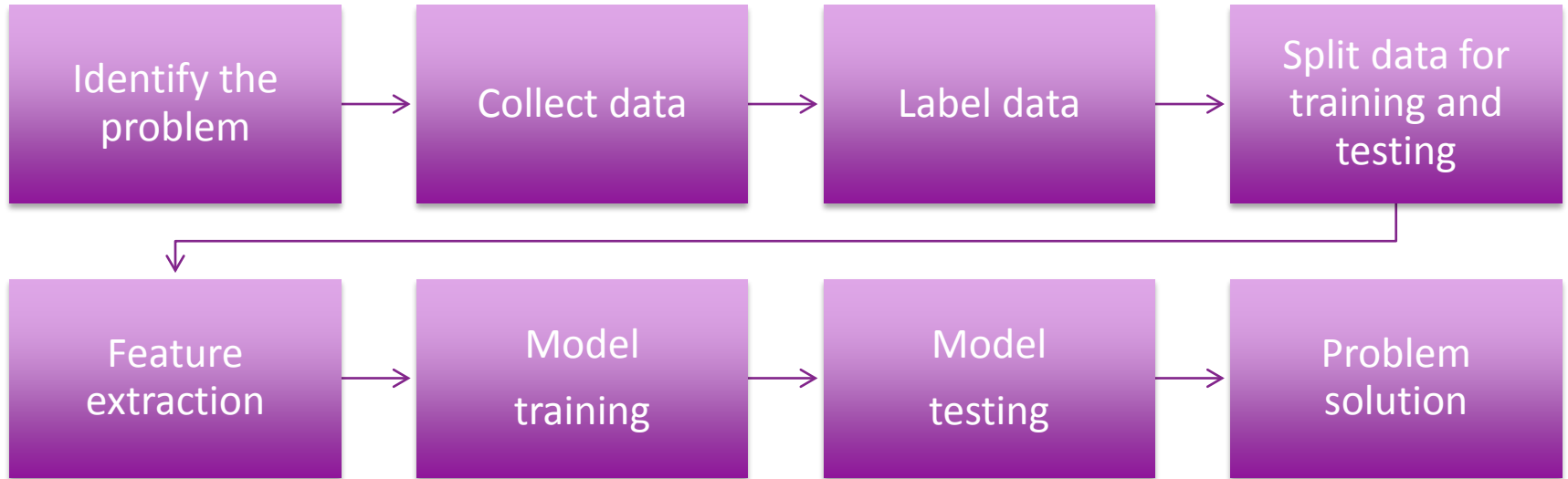
AI & Machine Learning Goes Mainstream

Prediction Using Past Data

- Self-driving cars

- Personalized recommendations for customers

- Improving medical diagnostics

- Predicting insurance premiums

- It is in our hands

CYLANCE

RSAConference2016 **Abu Dhabi**

Building a Machine Learning Model

```
Identify the problem  →  Collect data  →  Label data  →  Split data for training and testing
                                                                    ↓
Feature extraction  →  Model training  →  Model testing  →  Problem solution
```

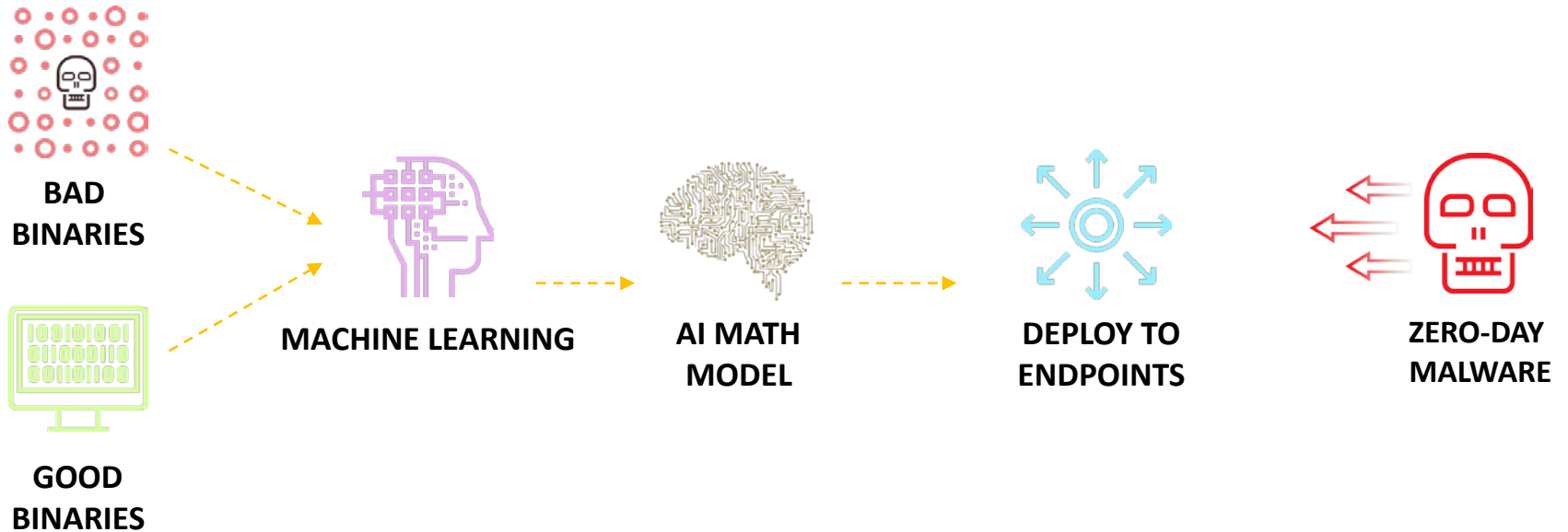CYLANCE

RSAConference2016 **Abu Dhabi**

Building a Machine Learning Model

- Progress your endpoint prevention capabilities

    - Leverage machine learning

    - Learn from the past attacks

    - Predict future attacks

    - Prevent execution

    - Automated security

CYLANCE

RSA Conference2016 **Abu Dhabi**

The AI Approach to Security

BAD BINARIES

GOOD BINARIES

MACHINE LEARNING

AI MATH MODEL

DEPLOY TO ENDPOINTS

ZERO-DAY MALWARE

CYLANCE

RSAConference2016 **Abu Dhabi**

Tackling Security Challenges with AI

- Volume of malware not slowing
- Progress your endpoint prevention capabilities
  - Leverage machine learning
    - Automate
    - Learn from the past
    - Predict future attacks
    - Prevent execution
  - Test and compare legacy vs NG

CYLANCE

RSAConference2016 **Abu Dhabi**

"If you can't get to some level of AI or machine learning with the volume of activity that you're trying to understand when you're [defending] networks from activity of concern, if you can't get to scale, you are always behind the power curve" *- Adm. Michael Rogers, NSA*

Can You Afford To Just Be Reactive?

RSAConference2016 **Abu Dhabi**

So What's Next

- Next Week
  - Asses your current security infrastructure
  - Identify the security needs of your environment
  - Define your 2017 security standards

- Next Month
  - Identify the areas your security needs improvement to meet your 2017 security standards
  - Research products for review that obtain that standard with efficiency, speed, and high-scalability in mind

- Within 3 Months
  - Select and deploy a security system that meets your 2017 goals

CYLANCE

RSAConference2016 **Abu Dhabi**