The beginning of the end(point): where we are now and where we'll be in five years

Adrian Sanabria, Senior Security Analyst, 451 Research

Adrian Sanabria (@sawaba)

Industry Analyst: 3 years

Red Team: 4 years

Blue Team: 5 years

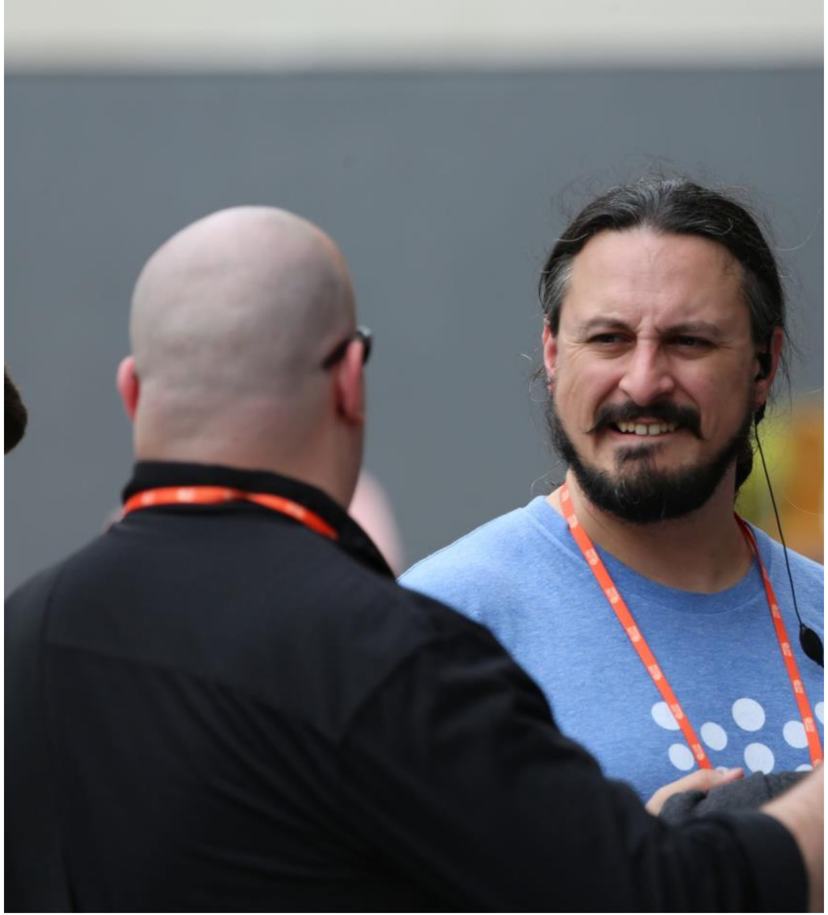
IT: 4 years

Opinionated

Goofball

Compulsive researcher

Embraces awkwardness →



TL;DL

The Big Picture

Industry

The Market View

Industry

The Buyer's View

Analysis

Trends and the Future

451 Research

Why are we here?

- Disruption in the endpoint security market
- Confused buyers
- Confused sellers
- Current and future opportunities

I WONDER WHY MAN WAS PUT ON EARTH. WHAT'S OUR PURPOSE? WHY ARE WE HERE?
TIGER FOOD.
11-14
WATTERSON
© 1994 Watterson/Distributed by Universal Uclick

TL;DL, or *before I lose you in my rant…*

IT and consumer technology has changed

Attacker TTPs have changed

Defenses stayed the same…

Sorry, no, they got *worse*

Industry missteps

Products that only work at corporate HQ

Products that break the user

Assuming any one layer must achieve 100% efficacy

Products that bury the customer in data

Making consumers a secondary priority

TL;DL

The Big Picture

Industry

The Market View

Industry

The Buyer’s View

Analysis

Trends and the Future

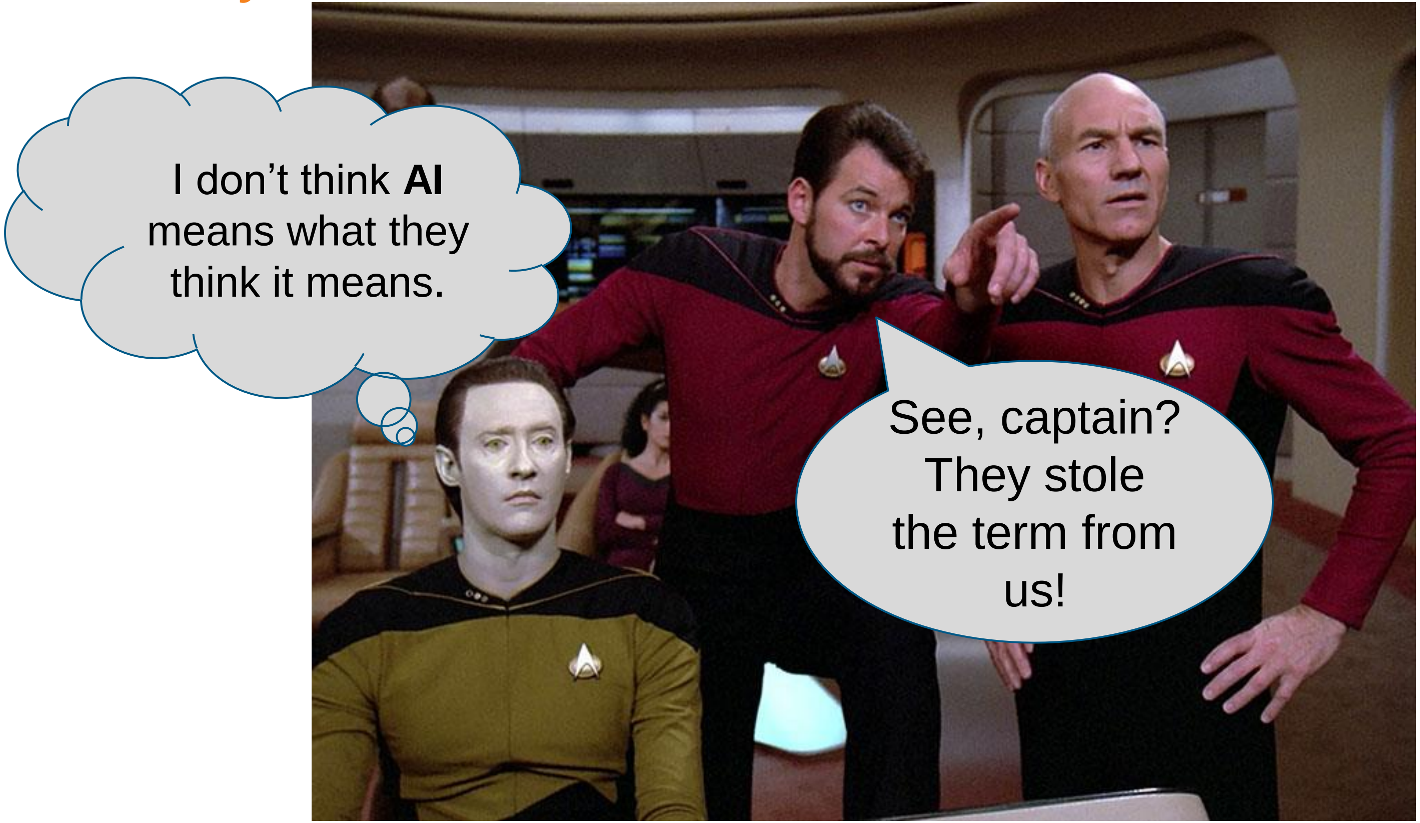
The evolution of endpoint security

2002	**Endpoint Security =** AV
2005	**Endpoint Security =** AV, VPN client, NAC client, host-based FW, HIPS, FDE, patching, device/port control, FIMaaaaaaa, this is so confusing!
2006	Heavy consolidation
2008	**Endpoint Security =** EPP (AV ‘suites’)

The evolution of endpoint security

2010	Rise of the ~~advanced, sophisticated~~ moderately well-read adversary
2015	**Endpoint Security =** AV, NGAV, EDR, Threat Hunting, Isolation, Exploit Prevaaaaaaaaaaaaa, this is so confusing!
2016+	Heavy consolidation
2018	Endpoint Security = NGEPP? (please, no)

The only time I want to hear "Next Generation"


I don't think **AI** means what they think it means.
See, captain? They stole the term from us!

The Attacker Landscape has changed, permanently

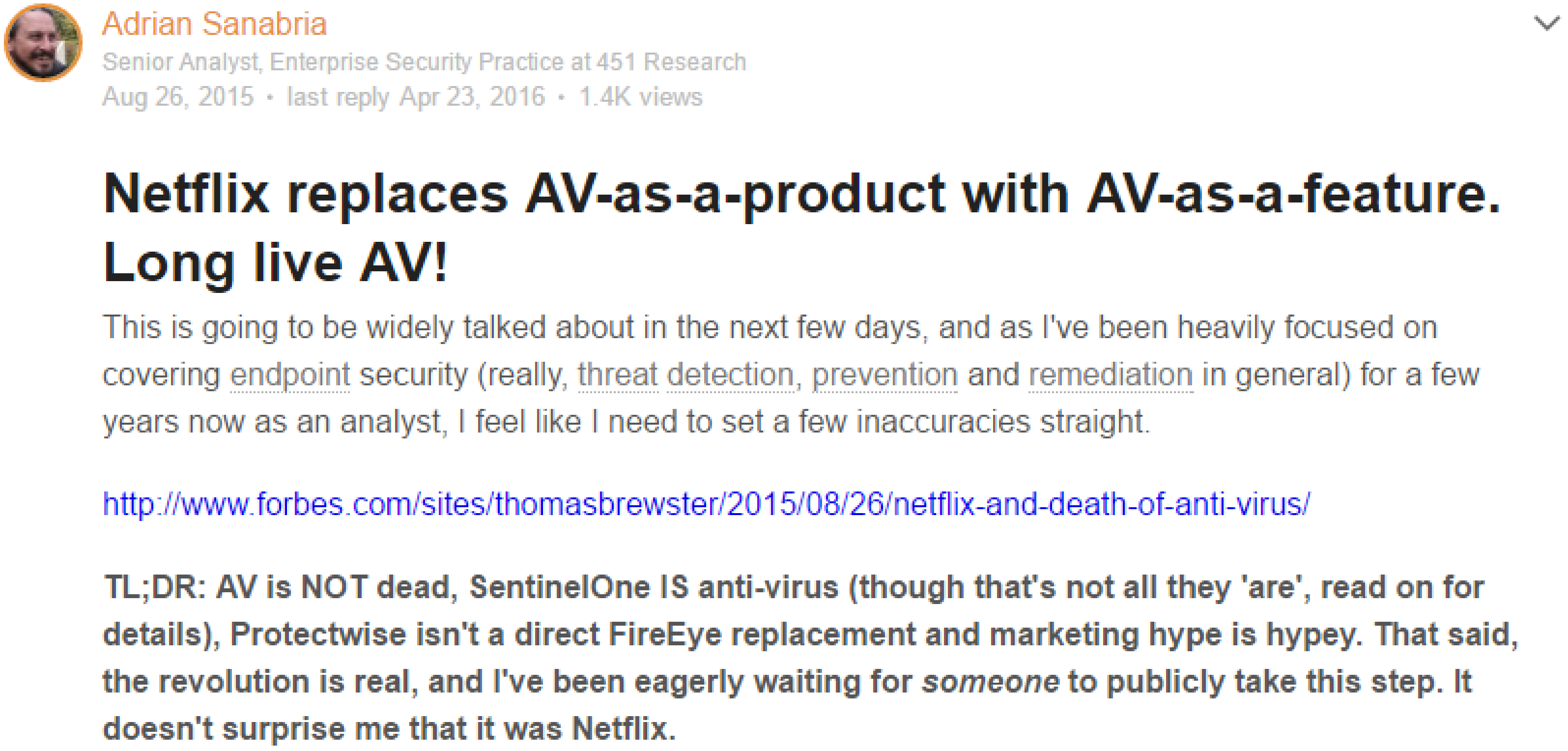
Is antivirus dead?

“Nobody wants to say antivirus is dead, but let’s just say they’re planning ahead for the wake and eyeing the stereo.”

Wendy Nather, 451 Research (2013)

451 Research

Is antivirus dead?



Adrian Sanabria

Senior Analyst, Enterprise Security Practice at 451 Research

Aug 26, 2015 • last reply Apr 23, 2016 • 1.4K views

Netflix replaces AV-as-a-product with AV-as-a-feature. Long live AV!

This is going to be widely talked about in the next few days, and as I've been heavily focused on covering endpoint security (really, threat detection, prevention and remediation in general) for a few years now as an analyst, I feel like I need to set a few inaccuracies straight.

http://www.forbes.com/sites/thomasbrewster/2015/08/26/netflix-and-death-of-anti-virus/

TL;DR: AV is NOT dead, SentinelOne IS anti-virus (though that's not all they 'are', read on for details), Protectwise isn't a direct FireEye replacement and marketing hype is hypey. That said, the revolution is real, and I've been eagerly waiting for *someone* to publicly take this step. It doesn't surprise me that it was Netflix.

451 Research

Is antivirus dead?

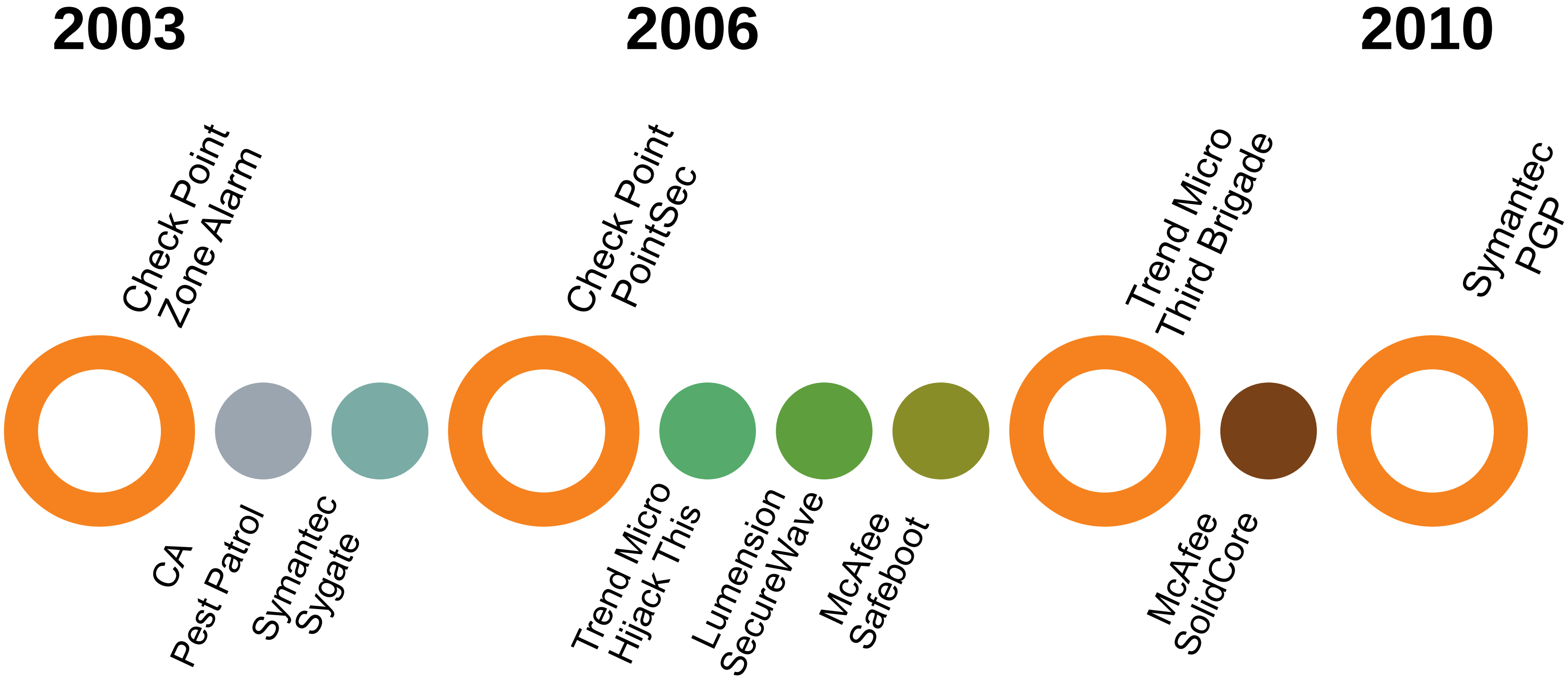
What’s dead, if anything, then?

The traditional *process* of addressing endpoint threats is fundamentally **broken**, and is in the process of being replaced

There’s no Advanced, just the new Normal.

sometimes we just have to
let things go

The First Great Endpoint Security Consolidation



~30 acquisitions

Events that helped kickstart the Second Great Endpoint Security Consolidation

Before 2010

2003-2009

- Mostly adjacent endpoint security/management technologies
- Took our eyes ‘off the ball’
- Got waaaay too excited about whitelisting
- Laptops instead of Desktops

After 2010

2010: Stuxnet (whaaat?!)

- State-sponsored malware

2013: APT1 (uh-oh)

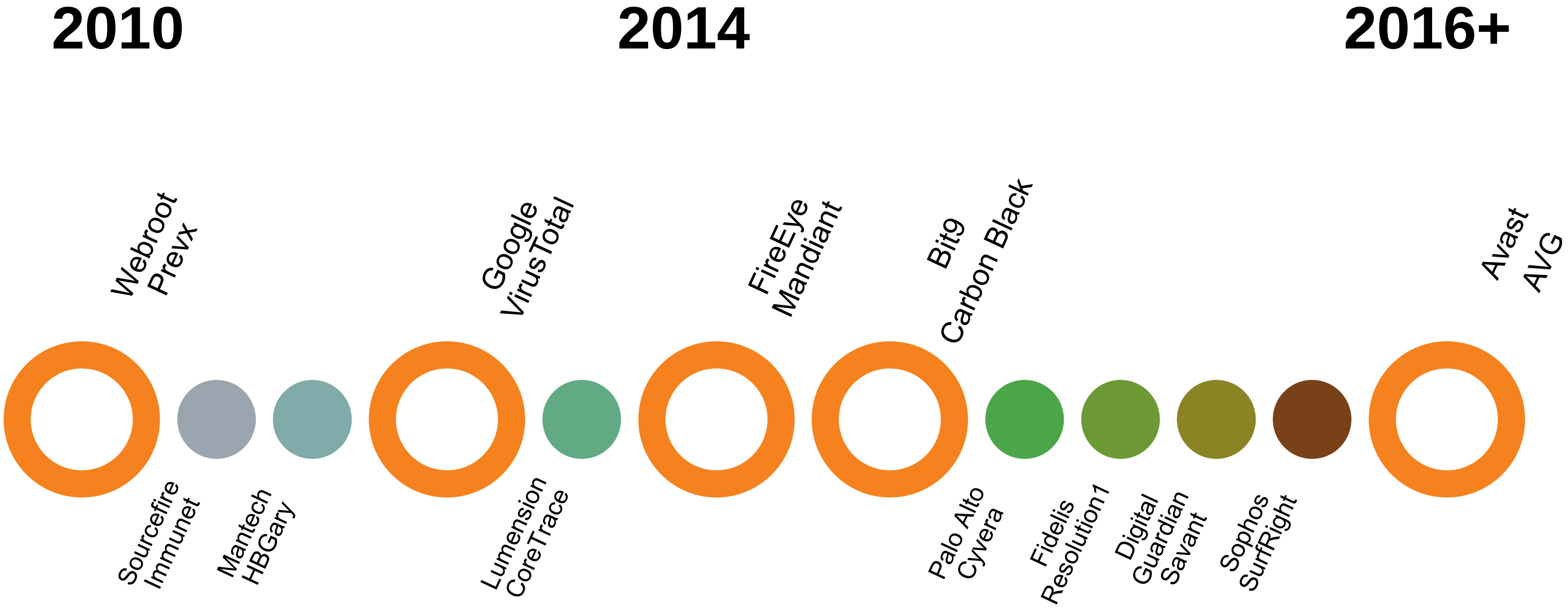
- More state-sponsored malware

2013: Snowden (oh crap)

- Domestic malware, threats and attack tools

2014: Ransomware (HALP!)

The Second Great Endpoint Security Consolidation



26 acquisitions (so far)

Stats and Facts!

13% run one endpoint security product

26.9% run two

59% run three or more concurrently

Why?

Stats and Facts!

67% using endpoint config mgmt

65% using HIDS/HIPS

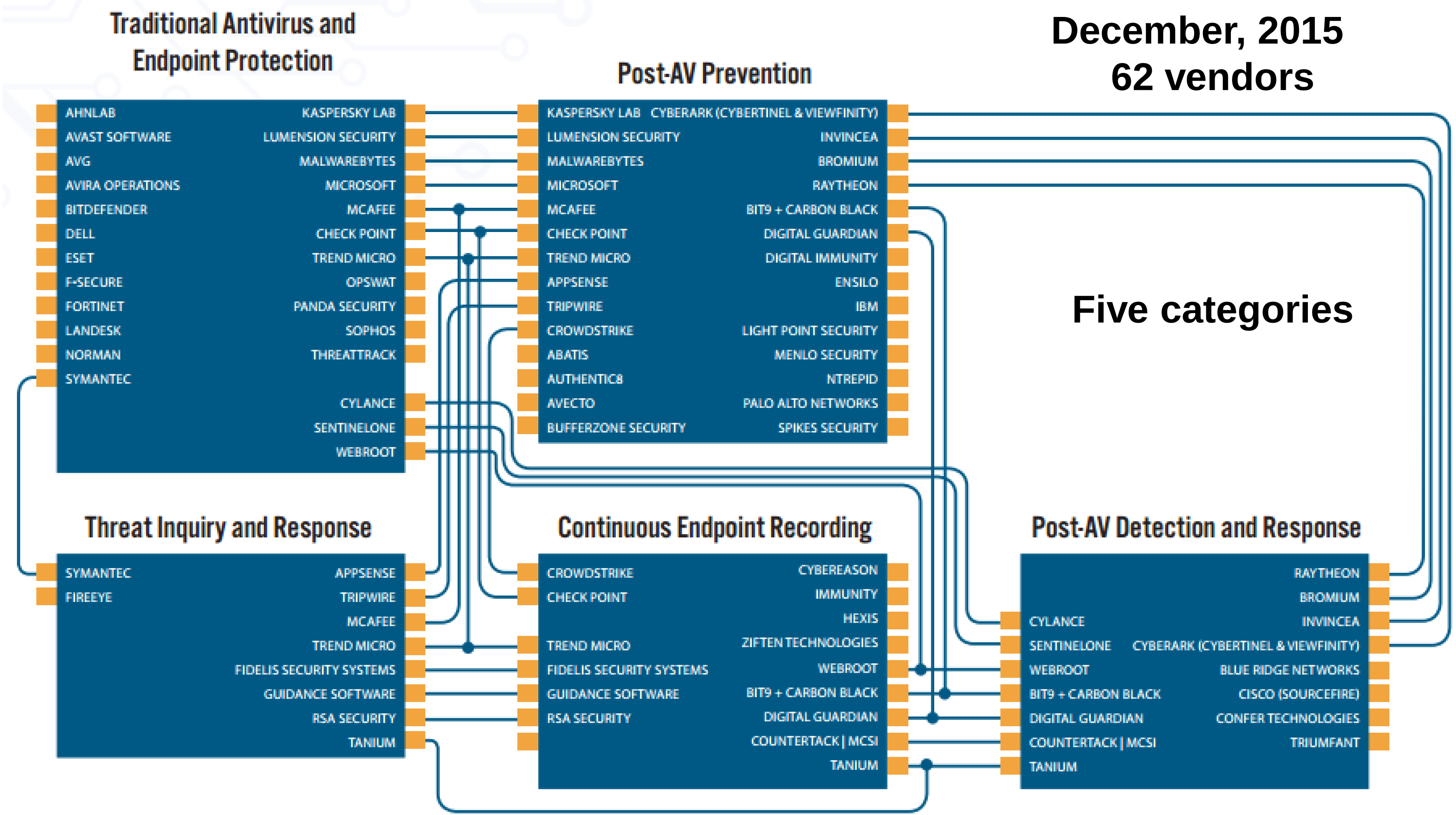
59% using FDE

56% using NAC

49% using FIM

47% using Whitelisting

December, 2015
62 vendors



Traditional Antivirus and Endpoint Protection

- AHNLAB
- AVAST SOFTWARE
- AVG
- AVIRA OPERATIONS
- BITDEFENDER
- DELL
- ESET
- F-SECURE
- FORTINET
- LANDESK
- NORMAN
- SYMANTEC

- KASPERSKY LAB
- LUMENSION SECURITY
- MALWAREBYTES
- MICROSOFT
- MCAFEE
- CHECK POINT
- TREND MICRO
- OPSWAT
- PANDA SECURITY
- SOPHOS
- THREATTRACK
- CYLANCE
- SENTINELONE
- WEBROOT

Post-AV Prevention

- KASPERSKY LAB
- LUMENSION SECURITY
- MALWAREBYTES
- MICROSOFT
- MCAFEE
- CHECK POINT
- TREND MICRO
- APPSENSE
- TRIPWIRE
- CROWDSTRIKE
- ABATIS
- AUTHENTIC8
- AVECTO
- BUFFERZONE SECURITY

- CYBERARK (CYBERTINEL & VIEWFINITY)
- INVINCEA
- BROMIUM
- RAYTHEON
- BIT9 + CARBON BLACK
- DIGITAL GUARDIAN
- DIGITAL IMMUNITY
- ENSILO
- IBM
- LIGHT POINT SECURITY
- MENLO SECURITY
- NTREPID
- PALO ALTO NETWORKS
- SPIKES SECURITY

Threat Inquiry and Response

- SYMANTEC
- FIREEYE

- APPSENSE
- TRIPWIRE
- MCAFEE
- TREND MICRO
- FIDELIS SECURITY SYSTEMS
- GUIDANCE SOFTWARE
- RSA SECURITY
- TANIUM

Continuous Endpoint Recording

- CROWDSTRIKE
- CHECK POINT
- TREND MICRO
- FIDELIS SECURITY SYSTEMS
- GUIDANCE SOFTWARE
- RSA SECURITY

- CYBEREASON
- IMMUNITY
- HEXIS
- ZIFTEN TECHNOLOGIES
- WEBROOT
- BIT9 + CARBON BLACK
- DIGITAL GUARDIAN
- COUNTERTACK | MCSI
- TANIUM

Post-AV Detection and Response

- CYLANCE
- SENTINELONE
- WEBROOT
- BIT9 + CARBON BLACK
- DIGITAL GUARDIAN
- COUNTERTACK | MCSI
- TANIUM

- RAYTHEON
- BROMIUM
- INVINCEA
- CYBERARK (CYBERTINEL & VIEWFINITY)
- BLUE RIDGE NETWORKS
- CISCO (SOURCEFIRE)
- CONFER TECHNOLOGIES
- TRIUMFANT

Five categories

The market now, 10 months later

Prevention
(pre-execution)

Detection
(post-execution)

77
Vendors

Data collection

50/50 split complementary/ primary

Prevention: Primary

Subcategory	Examples
AV Suites, aka ‘EPP’	Symantec, McAfee, Trend, Malwarebytes, BitDefender, Kaspersky, Sophos, etc
Newcomers, aka **“Next-Gen” AV**	Cylance, Invincea, Sentinel One, CrowdStrike

NGAV? *MY* definition (not Gartner's)

The ability to stop threats without prior knowledge of them

What is prior knowledge?

- Signatures
- IoCs
- Malware analysis sandbox
- Blacklisting

Prevention: Detection

- Behavioral analysis: Software
- Behavioral analysis: Users
- Kernel shims
- Deception
- In-memory scanning

Prevention vs Detection: a question of cost

Endpoint Data Collection

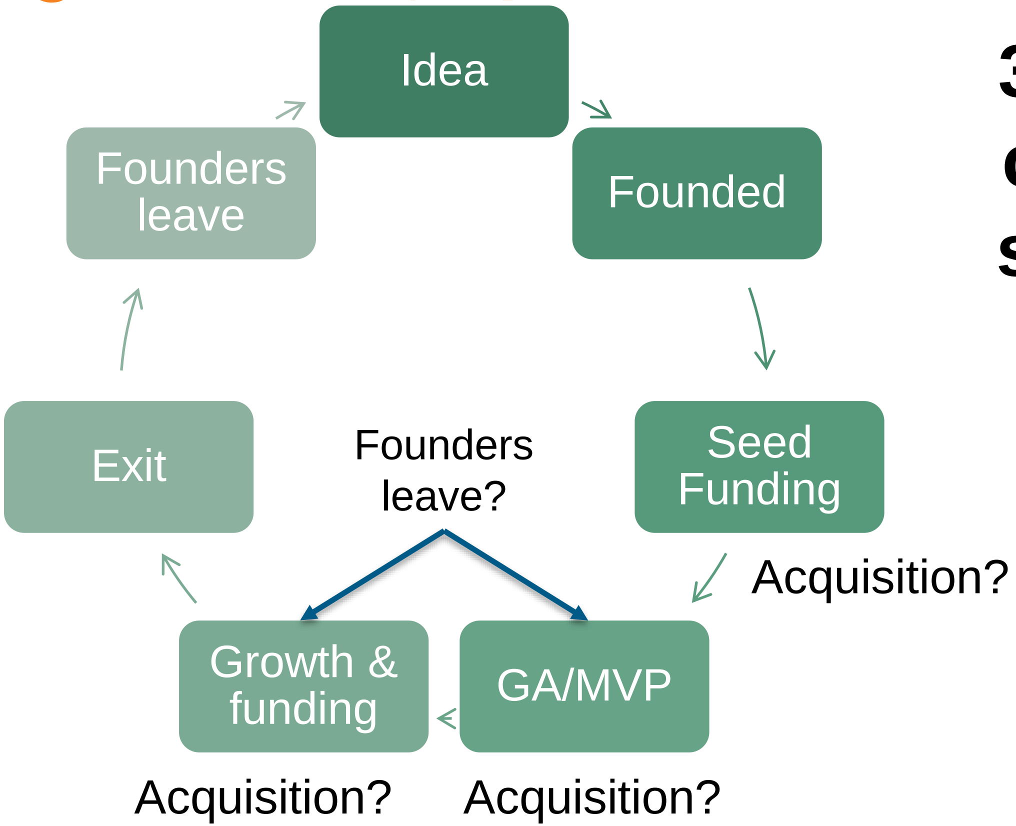
- Many use cases:
  - detection
  - forensics
  - incident response
- No more blind spot

What about remediation and response?

Who is gonna clean this up?

- Remediation vs Containment
  - Remediation is actually cleaning up the malware, artifacts with intent of returning a system to a production-ready state
  - Containment is limiting the damage of an attack, e.g. network isolation/quarantine, killing processes, blocking C2…)
- Automated Endpoint Remediation
  - Usually part of a solution that records all endpoint events/activities, allowing it to "undo" what an attacker or malware has done.

Understanding the startup cycle



Idea

Founded

Seed Funding

Acquisition?

GA/MVP

Acquisition?

Growth & funding

Acquisition?

Founders leave?

Exit

Founders leave

3-5 year cycle in security

Adrian’s Endpoint Security Roadmap

1. Better malware mousetrap
2. AV Certification (newer vendors)
3. Non-malware attacks
4. EPP features (newer vendors)
5. Data visibility
6. More robust and resilient platforms

Do enterprises even *need* better AV?

Hardening Windows

- CIS benchmarks (hardening)
- Ad-blocking
- Remove unnecessary software/features
- Least privilege:
  - flash click-to-run,
  - disable/restrict java plugin
  - selective whitelisting

Free/OSS Tools

- Microsoft EMET
- Microsoft AppLocker
- Artillery (Binary Defense)
- OSSEC (Trend Micro)
- El Jefe (Immunity)
- ~~Cylance Detect~~
- Sandboxie (Invincea)
- AIDE (FIM)
- ROMAD
- 0Patch

TL;DL The Big Picture

Industry The Market View

Industry The Buyer's View

Analysis Trends and the Future

451 Research

I have data: Voice of the Enterprise

451 Research has a panel of highly accredited senior IT executives who participate in surveys focused on enterprise IT trends. This proprietary panel consists of 30,000+ IT decision-makers in North America and Europe. Respondents of this Information Security survey are members of the panel who were qualified based on their expertise in their organization's IT deployment.

The Voice of the Enterprise: Information Security survey wave was completed during the month of June & July 2016. The survey represents more than 930 completes from pre-qualified IT decision-makers primarily based in North America and Europe. In addition to regular quarterly topics, this survey focuses on organizational dynamics around the information security function within enterprises.

What’s happening in the enterprise?

Endpoint sec is **ubiquitous**

Endpoint sec is **mature**

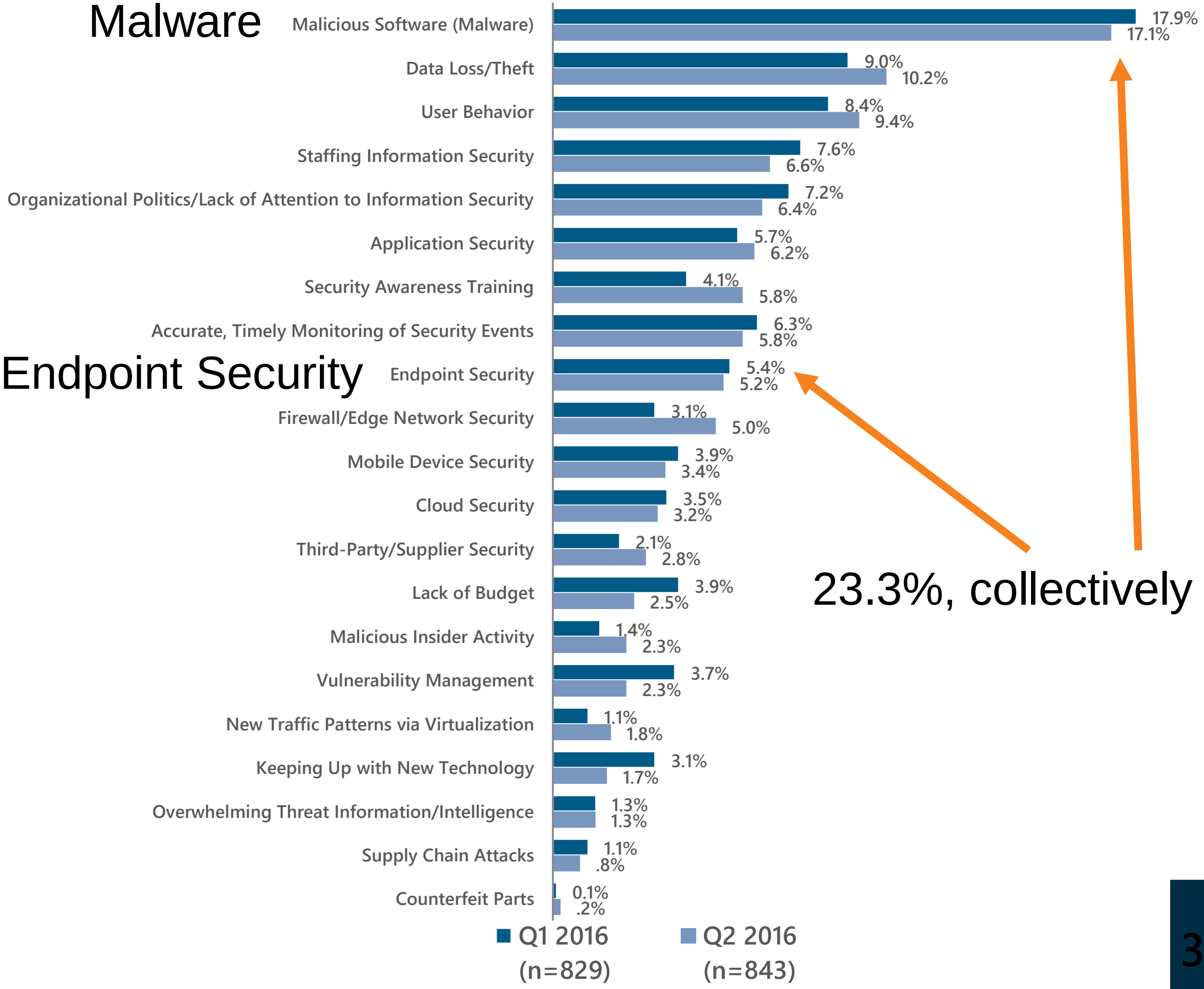
It is the #1 change Enterprises are planning to make in 2016

Why?

Top Security Pain Point

Q4. What do you consider your top internal information security pain point within your organization for the previous 90 days?

Source: 451 Research, Voice of the Enterprise: Information Security, Organizational Dynamics 2016



Malware

Endpoint Security

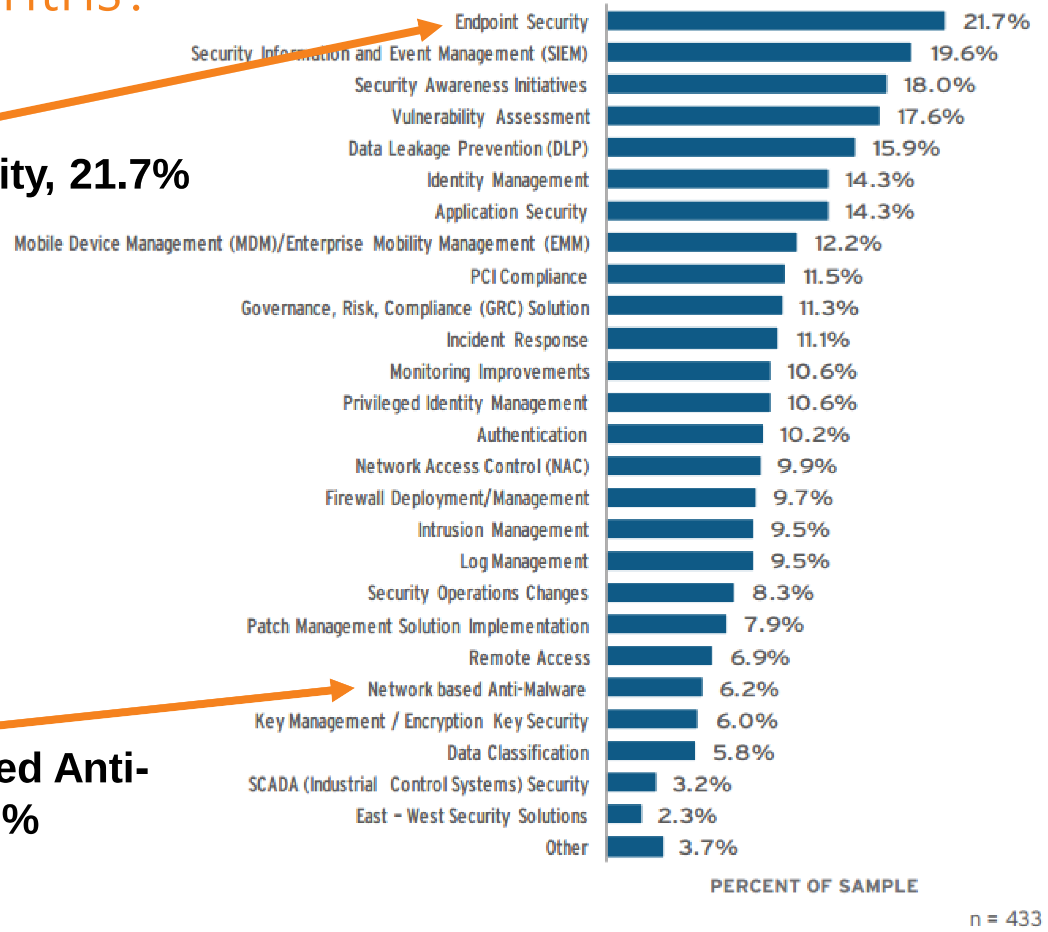
23.3%, collectively

451 Research | Voice of the Enterprise

“How would you rate your current suite of Endpoint Security tools against…

Use Case	% effective or very effective
Detecting Known Malware	**75%**
Preventing Known Malware	**68%**
Detecting Unknown Malware	**29%**
Preventing Unknown Malware	**25%**
Detecting and/or preventing non-malware attacks	**40%**

What are your organization's top three Infosec projects over the next 12 months?



#1: Endpoint Security, 21.7%

#22: Network-based Anti-Malware, 6.2%

451 Research

TL;DL

The Big Picture

Industry

The Market View

Industry

The Buyer’s View

Analysis

Trends and the Future

What are the big problems?

- We no longer have one perimeter: we have **many**
- Sloppy defense in depth
- Information asymmetry
- Market currently unstable (still consolidating)
- Blind Spots
- Blaming the user (aka “stop clicking links”)
- Discarding useful tech because it wasn’t a silver bullet
- Ending the leapfrogging and so much more!

From one perimeter to many

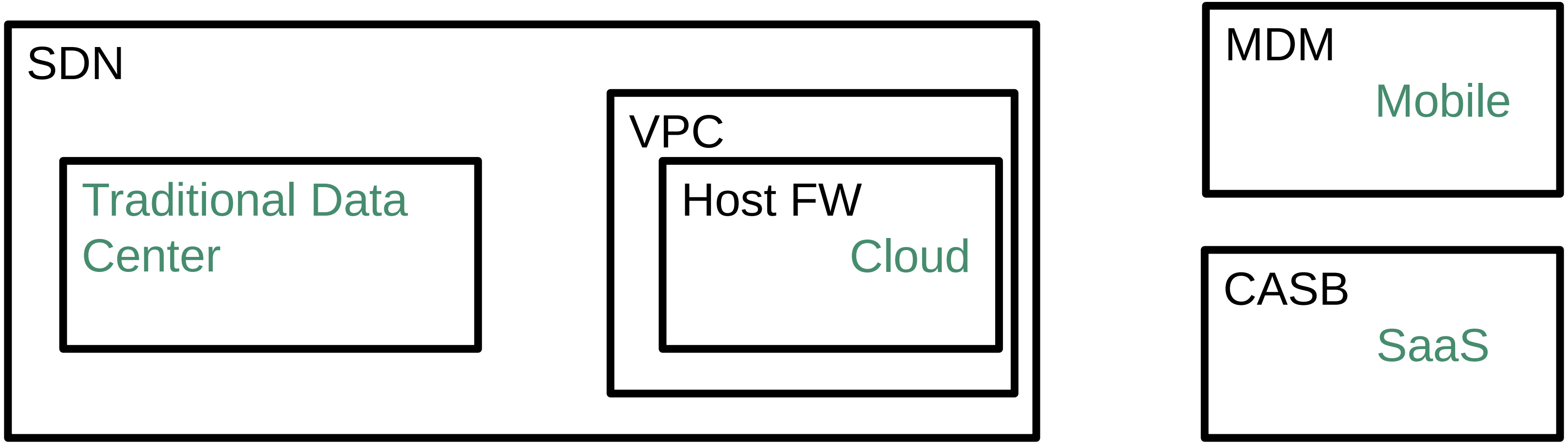
Mobile

Traditional Data Center

Cloud

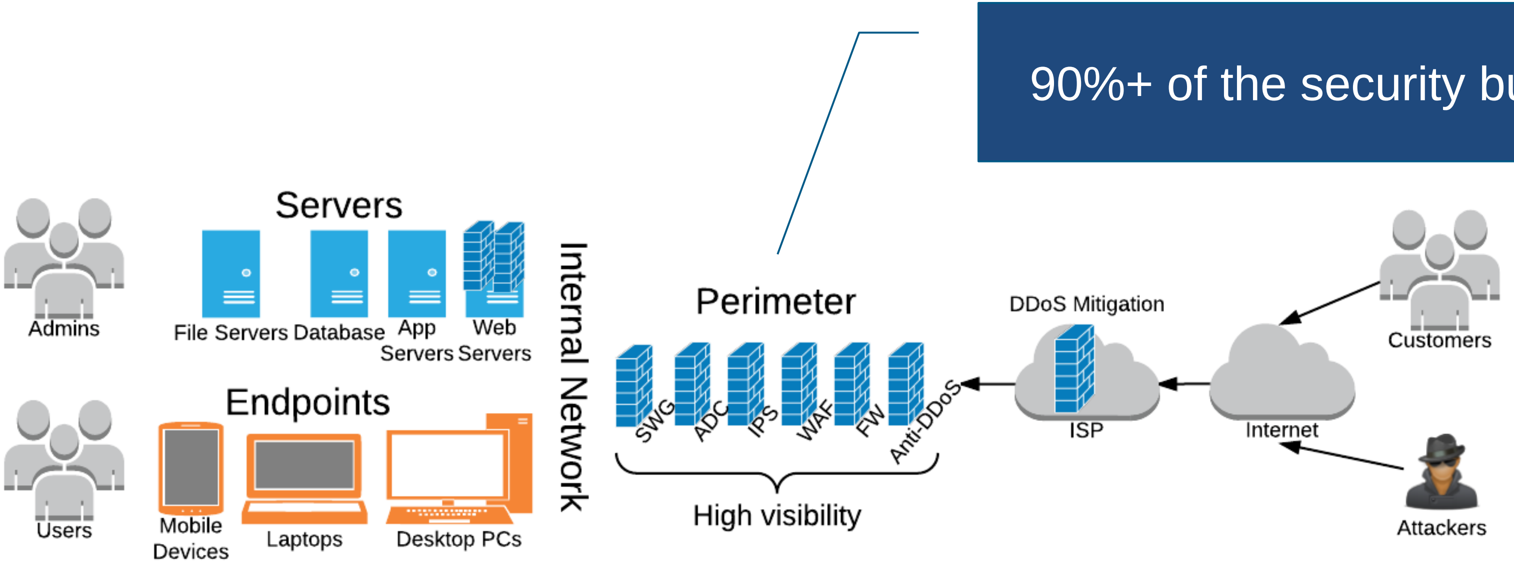
SaaS

From one perimeter to many



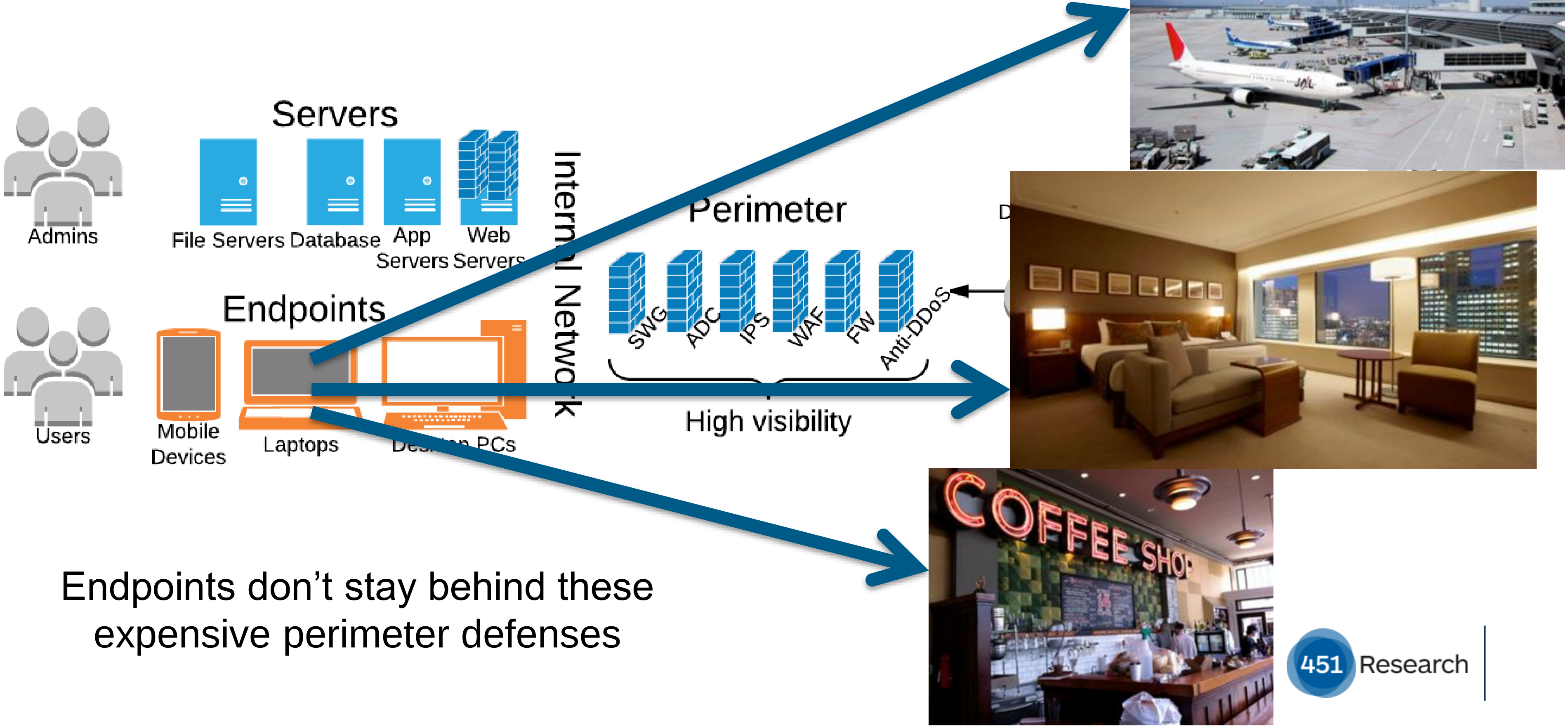
Why are we still investing so heavily in the perimeter?

90%+ of the security budget*



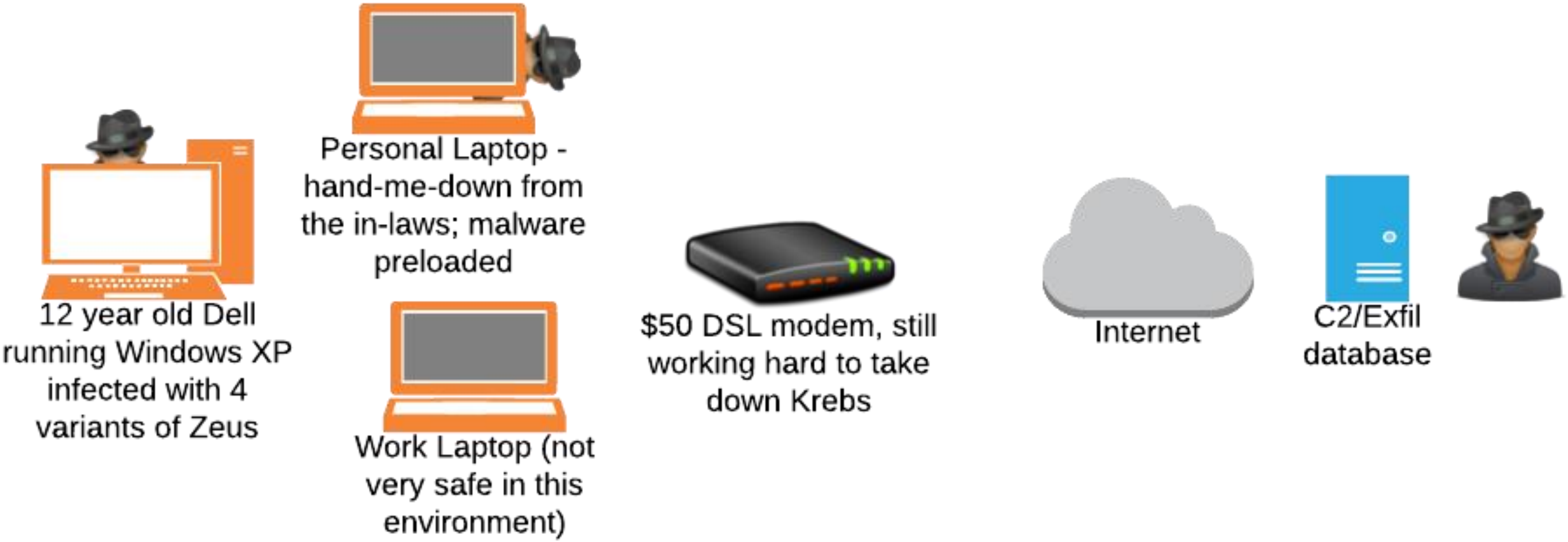
* - I made this number up. We have the number, I just didn't look it up.

Why are we still investing so heavily in th



Endpoints don’t stay behind these expensive perimeter defenses

This is where many of your employees *actually* work



12 year old Dell running Windows XP infected with 4 variants of Zeus

Personal Laptop - hand-me-down from the in-laws; malware preloaded

Work Laptop (not very safe in this environment)

$50 DSL modem, still working hard to take down Krebs

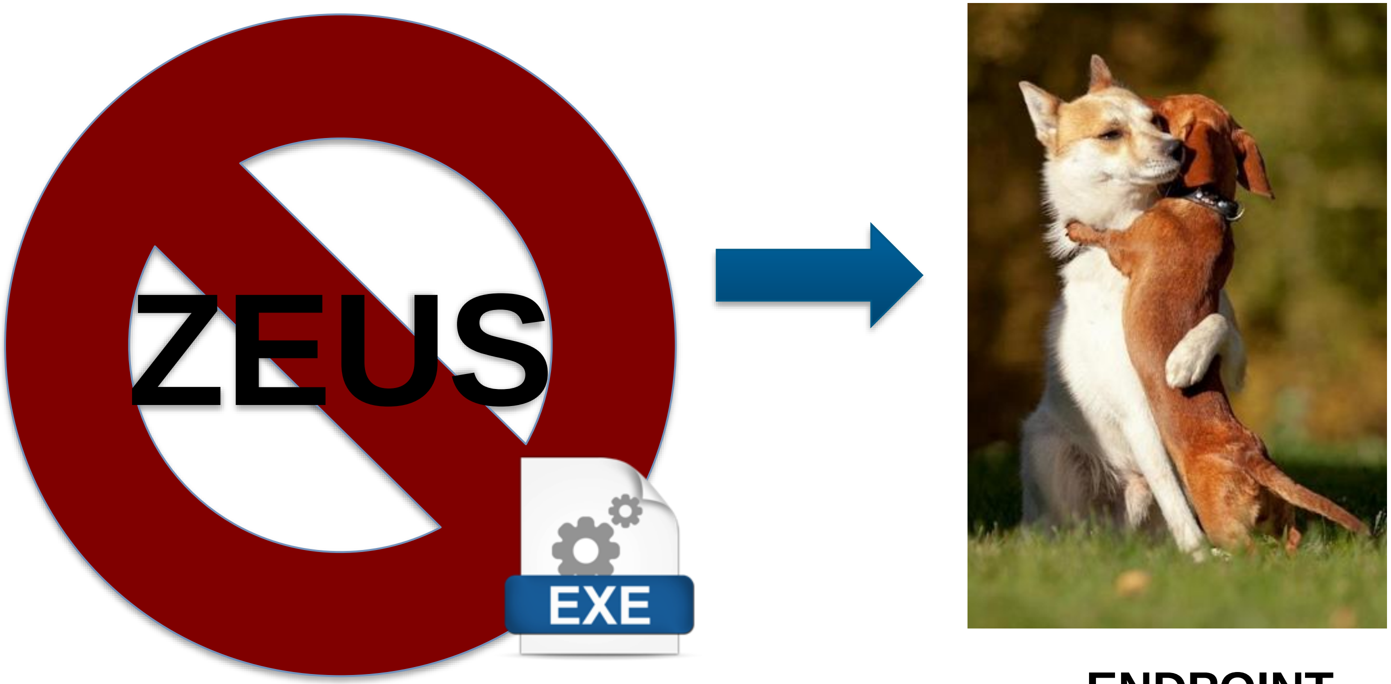
Internet

C2/Exfil database

Conclusion? Security controls MUST travel with the asset.

Story time!

Advanced Malware Detection, Day 1:



NETWORK

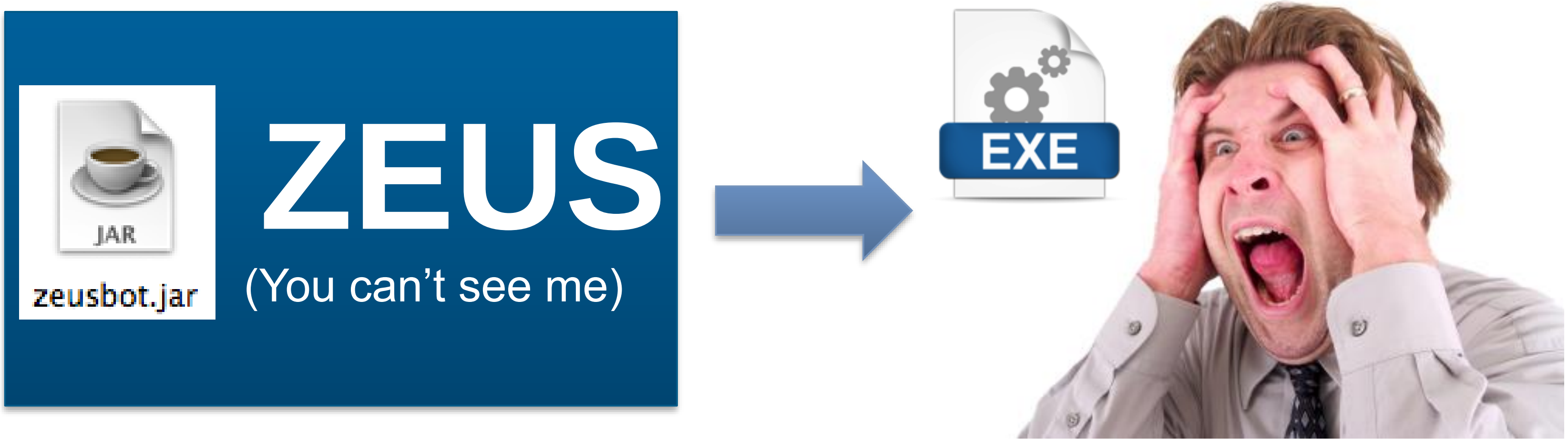
ENDPOINT

Advanced malware protection story, part 1

Once upon a time, the company I worked for acquired a malware analysis sandbox product. Life was good; malicious Win32 binaries were detected and blocked. They did not reach the endpoint.

Story time!

Advanced Malware Detection, Day 2:



JAR

zeusbot.jar

ZEUS

(You can’t see me)

EXE

NETWORK

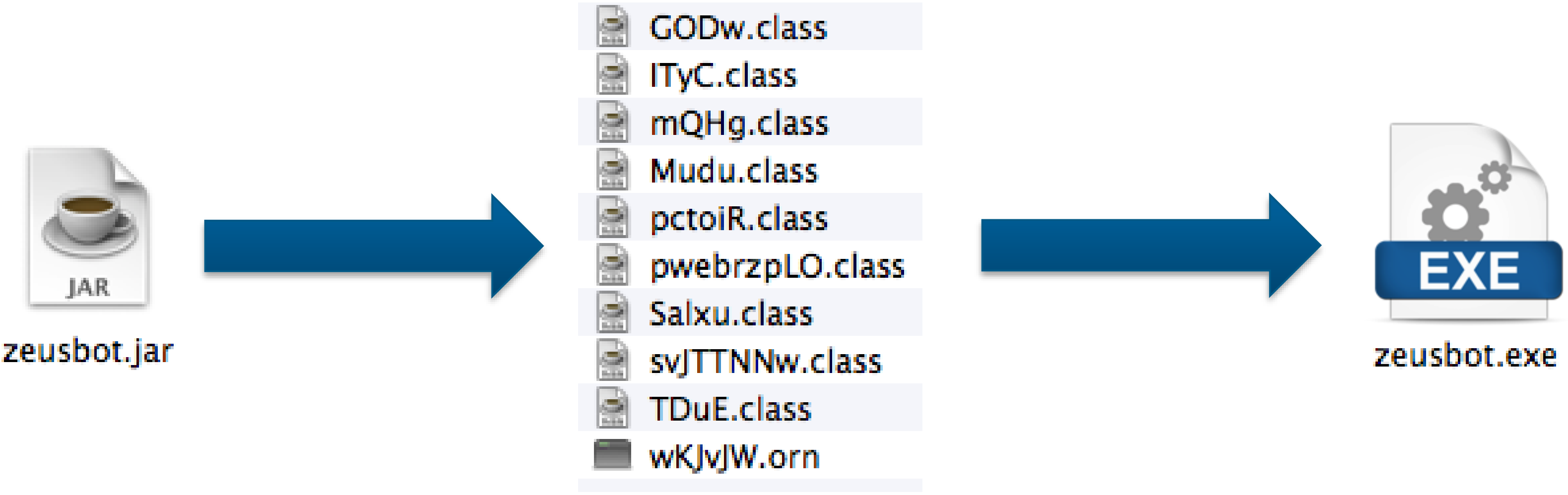
ENDPOINT

Advanced malware protection story, part 2

The attackers realized Win32 binaries were easily detectable in a network stream, and decided they'd create a Java JAR 'wrapper' to evade detection. It worked! The bad guys were back in business, and it didn't take long for them to figure out how to evade these defenses, that were years in the making.

Story time!

The bad guys *will* find a way to evade preventative controls.



GODw.class
ITyC.class
mQHg.class
Mudu.class
pctoiR.class
pwebrzpLO.class
Salxu.class
svJTTNNw.class
TDuE.class
wKJvJW.orn

Advanced malware protection story, part 3

They didn’t even write any new malware – really all the JAR file did, once it got onto the endpoint, was reassemble the same malware used previously, which was broken into pieces across a handful of .class files and obfuscated to evade detection.

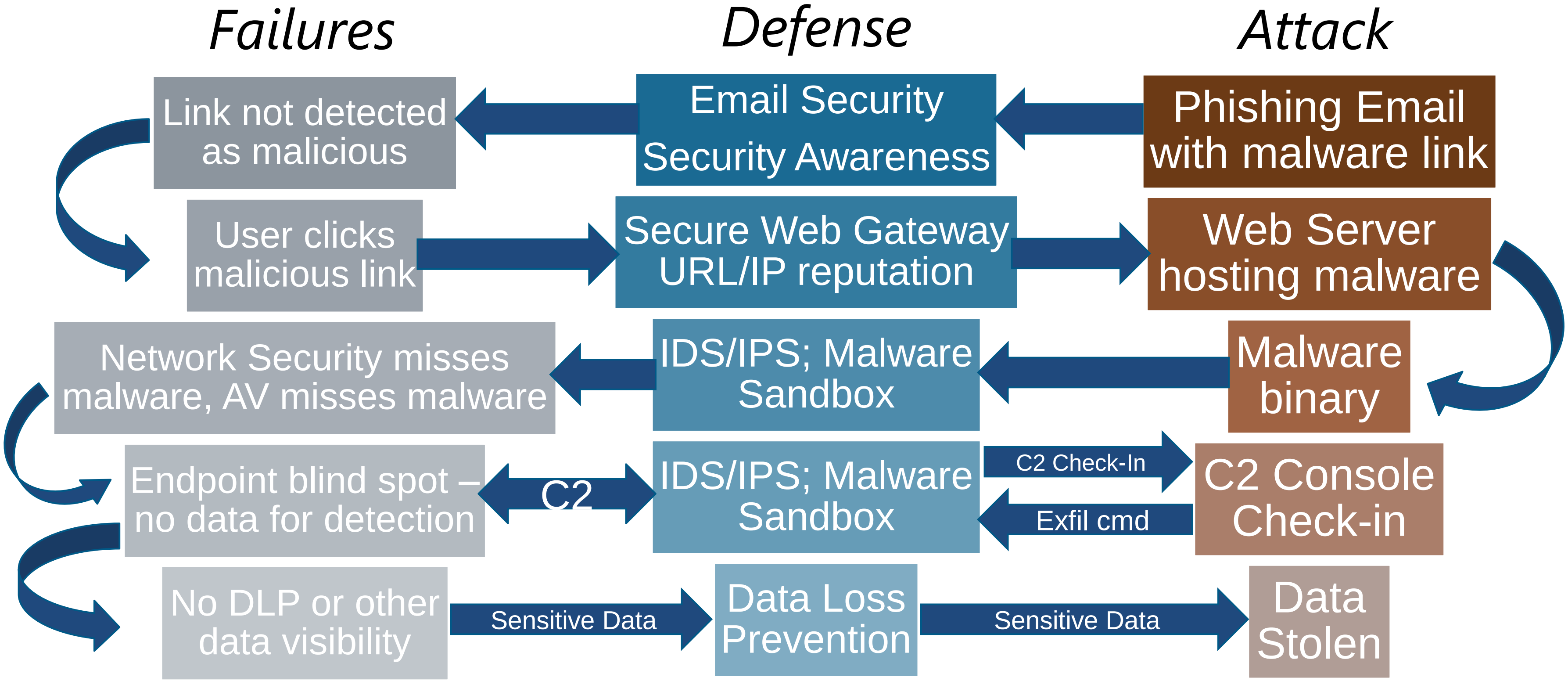
Advanced malware protection story, part 4

Finally, we realized that the majority of our issues with malware were not at the headquarters location anyway, but at our smaller branch offices. Since this malware sandbox product was very expensive, we could only afford to buy one, and the corporate headquarters seemed the most rational place to put it.

Advanced malware protection story - conclusions

- The product was easily evadable, and required months address attacker evasions, whereas attackers needed only days or hours to update evasion tactics.
- The product architecture (expensive, monolithic hardware appliance) made it impossible to place the product where it would maximize value.

How ~~Defense~~Expense in depth fails: an example



Failures

Defense

Attack

Phishing Email with malware link

Email Security

Security Awareness

Link not detected as malicious

User clicks malicious link

Secure Web Gateway URL/IP reputation

Web Server hosting malware

Malware binary

IDS/IPS; Malware Sandbox

Network Security misses malware, AV misses malware

Endpoint blind spot – no data for detection

C2

IDS/IPS; Malware Sandbox

C2 Check-In

Exfil cmd

C2 Console Check-in

No DLP or other data visibility

Sensitive Data

Data Loss Prevention

Sensitive Data

Data Stolen

Conclusion? Find fewer, but more effective solutions and put the time into configuring/tuning them.

Design for the real world

"Customers never enable the more effective functionality in our product!"

--Engineer, at a large incumbent AV vendor

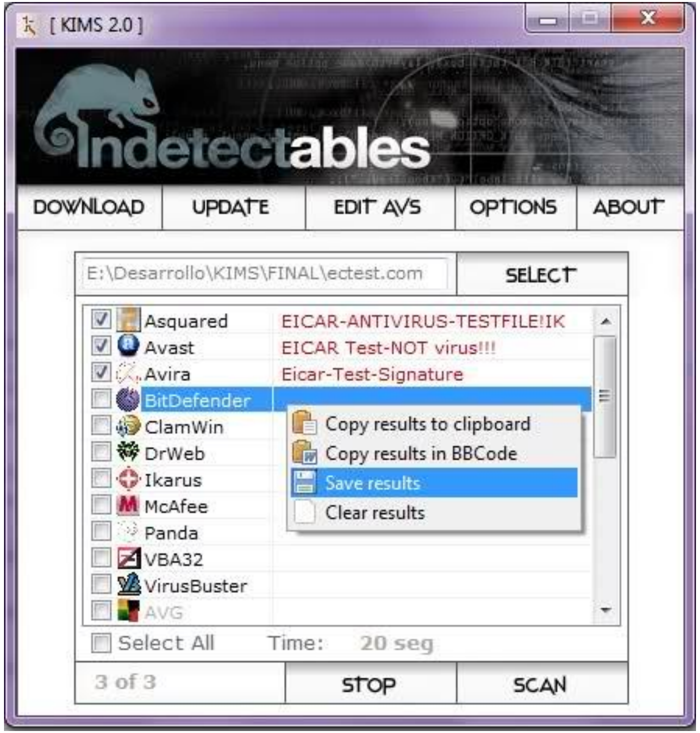
Conclusion? Products should adapt to users based on user type, user behavior – not the other way around. Also enable technologies critical to efficacy by default – don't hide them in a sea of configuration options!

Information Asymmetry

AV isn't just protecting against 'known threats'

It *is* a known threat.

To the bad guys!



E:\Desarrollo\KIMS\FINAL\ectest.com

☑ Asquared	EICAR-ANTIVIRUS-TESTFILE!IK
☑ Avast	EICAR Test-NOT virus!!!
☑ Avira	Eicar-Test-Signature
☐ BitDefender	
☐ ClamWin	
☐ DrWeb	
☐ Ikarus	
☐ McAfee	
☐ Panda	
☐ VBA32	
☐ VirusBuster	
☐ AVG	

☐ Select All Time: 20 seg

3 of 3

Conclusion? A detection engine alone will never stop determined adversaries – it must be part of a coordinated, layered defense

Blind spots: the traditional enterprise has **four**

Endpoint

East-West Traffic

Cloud/SaaS

Data

PEBKAC

PWNED

Proactive Solutions for Stupidity
Includes club with nail in it
Distributing
CLUE to
USERS
O'REALLY®
Leonidas

O'Really - Distributing Clue to Users *by BOFHcam*

NOT
PWNED

iOS

If you already know what can and will go wrong...

DESIGN FOR IT!

Don't punish the user

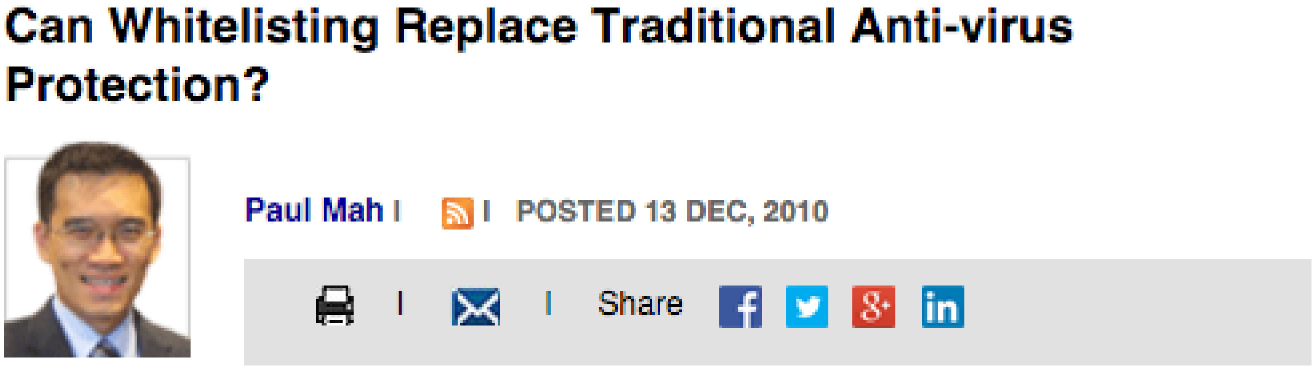
Explanation for previous three slides

The jist of this slide is that blaming the user for getting infected with malware is akin to blaming the cow you crashed your car into for you not wearing your seatbelt.

The threat is known, so there’s no excuse for not preparing appropriately for it. iOS is used here as an example of a platform that’s user friendly (i.e. proving that effective security doesn’t have to ‘get in the way’), but doesn’t commonly have issues with malware.

Furthermore, iOS protects users without need for any special training. Conclusion? Windows (or 3rd party Windows security) needs to be able to adapt to users’ needs.

Discarding useful tech because it wasn't a silver bullet



Can Whitelisting Replace Traditional Anti-virus Protection?

Paul Mah | | POSTED 13 DEC, 2010

2011: "By 2015, more than 50% of enterprises will have instituted 'default deny' policies that restrict the applications users can install."

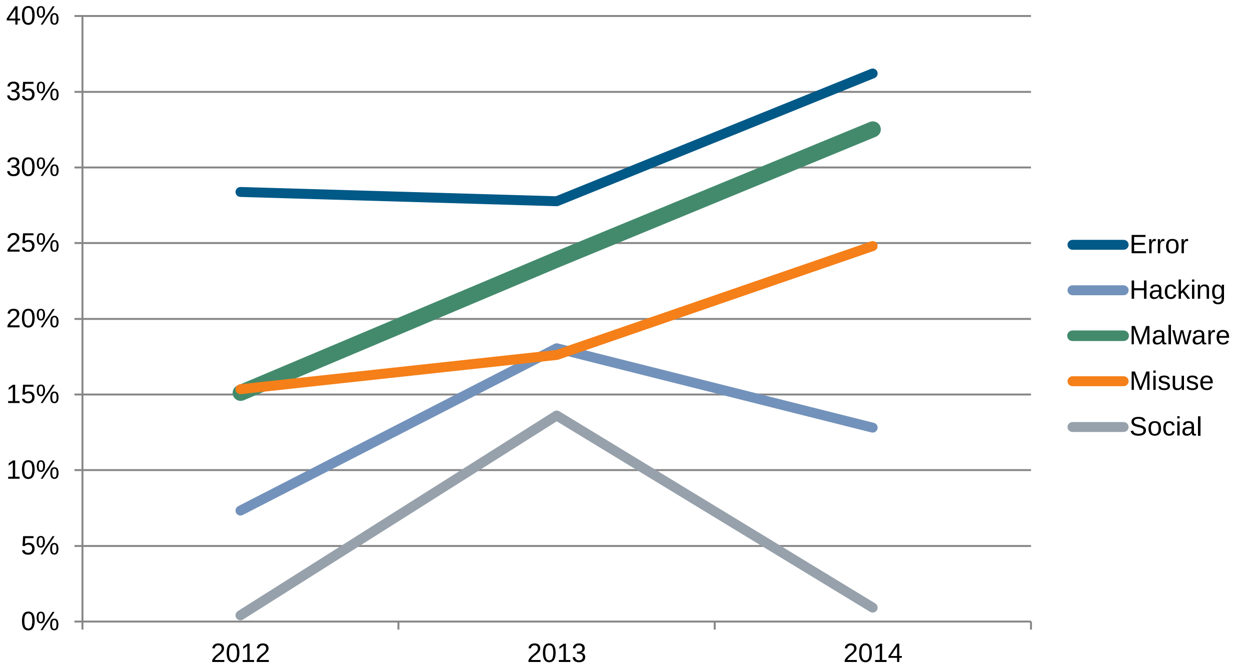
Technologies like Whitelisting and NAC failed commercially because the use cases were overbearing and too much work to manage. More recent attempts show that a more selective application of these technologies can be successful and effective.

Myth: Solving the malware problem changes everything!

How big a part of the breach problem is malware?

15% in 2012
24% in 2013
33% in 2014

Solving malware still doesn't solve 2/3rds of the problem.



Source: Verizon Enterprise Solutions

Stop playing leapfrog and start playing chess

“Stop playing leapfrog” explanation

Too often, we come up with solutions that only think one step ahead. Take, for example, that many ransomware solutions are encryption-specific. It is a poor assumption that all ransomware will use encrypted data as the leverage to force victims into paying. The reality is that we’re already seeing ransomware using other approaches:

- locking people out of systems by setting/changing passwords
- taking data and threatening to expose it

Instead, we need to start thinking many ‘moves’ ahead, like in chess. When we make this change, how will attackers react? We’ll find that we’re actually pretty good at predicting attacker behavior, we just need to make a better habit of thinking about solutions capable of lasting for five years instead of six-months.

The solution isn’t simple.

We can’t get rid of AV

1. R&D work done by AV firms is irreplaceable
2. Signatures still necessary to track and communicate existing threats
3. Compliance
4. AV Certification

New entrants can’t yet replace AV

1. Remediation isn’t there yet
2. Prevention isn’t complete without detection
3. Malware isn’t the only issue
4. Curse of complementing

Conclusion? Customers will continue using multiple products until consolidation completes.

The answer? Layers.

Prevention

Known Threats
Blacklists, reputation filtering, threat intel, signature-based network and endpoint tech

Unknown Threats
Exploit prevention, malware sandboxes, isolation security, app whitelisting

Detection

Known Threats
Anti-Virus, IDS/IPS, WAF, threat intel

Unknown Threats
Behavioral analytics, anomaly detection, red flags, binary analysis

Response/Remediation

Anti-virus, automated incident response/remediation tools, automated endpoint remediation, reimaging PCs

Thanks!

Adrian Sanabria - @sawaba

451 Research®

NEW YORK
LONDON
BOSTON
WASHINGTON, D.C.
SAN FRANCISCO