RSAConference2016

Abu Dhabi | 15–16 November | Emirates Palace

Connect to Protect

SESSION ID: CEM-W06

Next Generation Endpoint Security – Confused?

Greg Day

VP & Chief Security Officer, EMEA

Palo Alto Networks

@GreDaySecurity

#RSAC

Brief Intro

20+ yrs Dr Solomon's AV & McAfee/Intel:

- Wrote anti-malware behavioral solution, several patents
- Lead consultancy practice (CLAS)
- Ran Malware Forensics training/EMEA Cybercrime program

3yrs EMEA CTO at Symantec:

- Lead EMEA security strategy
- Vice Chair Tech UK Cyber Security working group, Council of Europe Cybercrime committee

2 yrs EMEA CTO FireEye:

- Strategic Oversight Board for the UK GOV CISP, NCA Industry Steering group

1+ yrs EMEA VP & CISO Palo Alto Networks

Greg Day

McAfee An Intel Company symantec. FireEye

paloalto NETWORKS

paloalto NETWORKS

Questions we will answer

- Do I need a new (NG) endpoint security capability?
- What are the different between traditional and NG?
  - What are the techniques available?
- How do I evaluate which is best for me?
- What does the the future endpoint security stack look like?
  - What factors should I consider?

Is the endpoint

sport football opinion culture business lifestyle fashion envi

Antivirus software is dead, says sec expert at Symantec

Information chief at Norton developer says software in general misse attacks and its future lies in responding to hacks

Hackers are said increasingly to use novel methods and bugs in the software of computers to Photograph: Dale O'Dell/Alamy

Antivirus software only catches 45% of malware attacks and is "dead" to a senior manager at Symantec.

Remarks by Brian Dye, senior vice-president for information security company, which invented commercial antivirus software in the 1980s develops and sells Norton Antivirus, suggest that such software leave vulnerable.

CRN

NEWS, ANALYSIS AND P
VARs AND TECHNOLOGY

HOME | NEWS | COMPANIES ▾ | SLIDESHOWS | VIDEO | BLOGS
WOMEN OF THE CHANNEL | JOBS | TECHNOLOGIES ▾

Apps & OS ▾ | Channel ▾ | Cloud ▾ | Components & Peripherals ▾ | Data Ce

* CRN Exclusive: HP COO Flaxman Reaffirms Commitment

Like 2 | Share 2 | Share | Tweet | G+1

Cylance, Sophos Trade Heated Words, With A Reseller Partner Caught In The Middle

by Sarah Kuranda on June 28, 2016, 11:31 am EDT

Printer-friendly version
Email this CRN article

A war of words between Cylance and Sophos that began last week continues to escalate, with both sides now accusing the other of throwing their mutual reseller partner under the bus.

SECURITY WEEK

INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe (Free) | CISO Forum

Home › Endpoint Security

Inside The Competitive Testing Battlefield of Endpoint Security

By Kevin Townsend on July 19, 2016

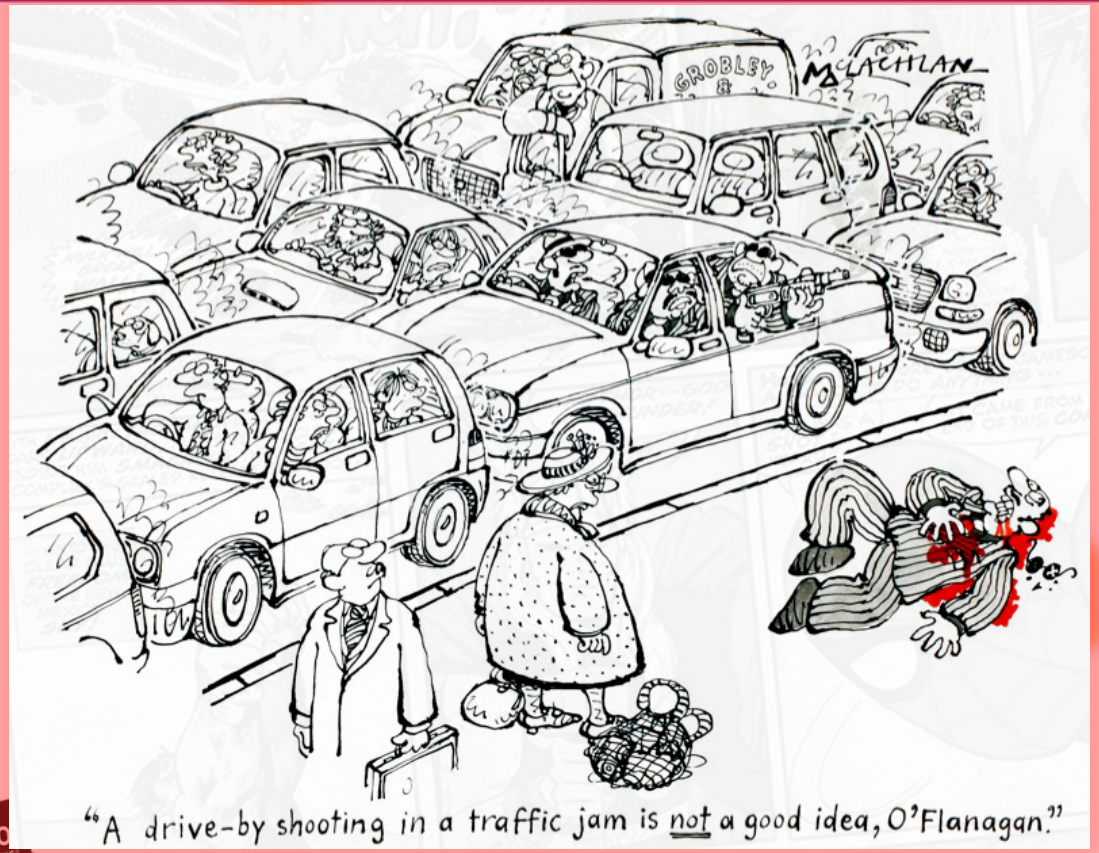
Share 183 | G+1 7 | Tweet | Recommend 23 | RSS

Traditional AV Firms Battle "Next-Gen" Endpoint Security Vendors for Share of Anti-malware Market

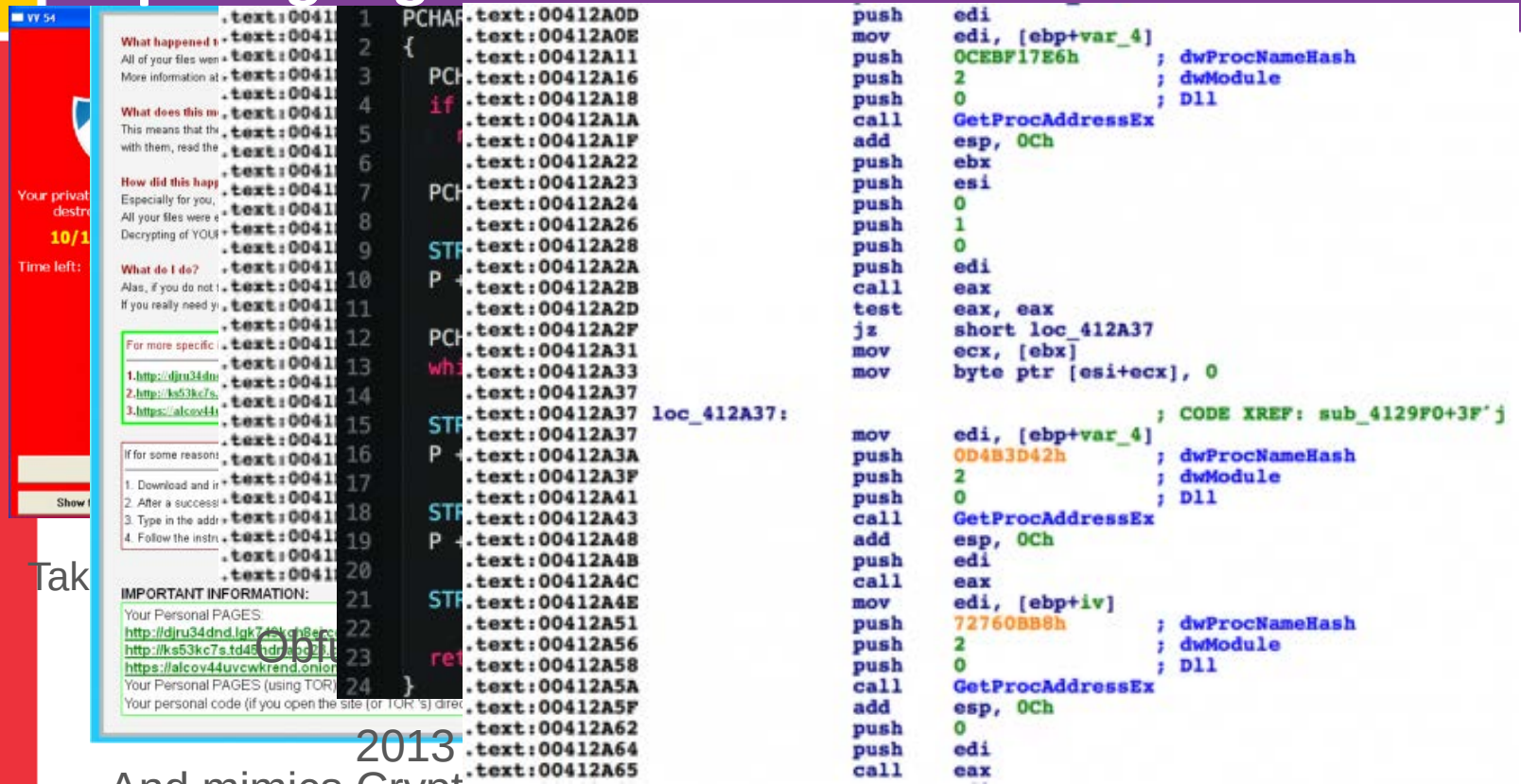
There is bad feeling between what can be described as traditional antivirus (Trad AV) and next generation antivirus (Next-Gen Endpoint Security, or ES). It's not universal, but it does exist.

paloalto NETWORKS

What simulated this debate: Evolution!



TeslaCrypt ransomware: splicing together new attacks



Tak

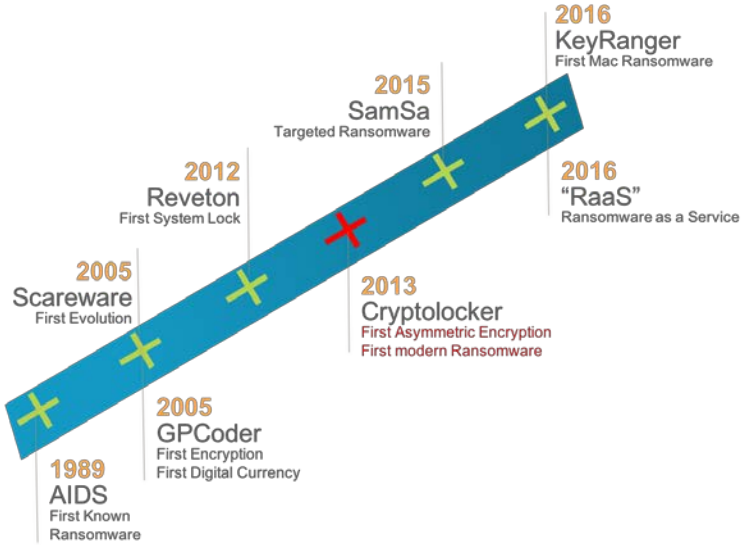
Oct 2013

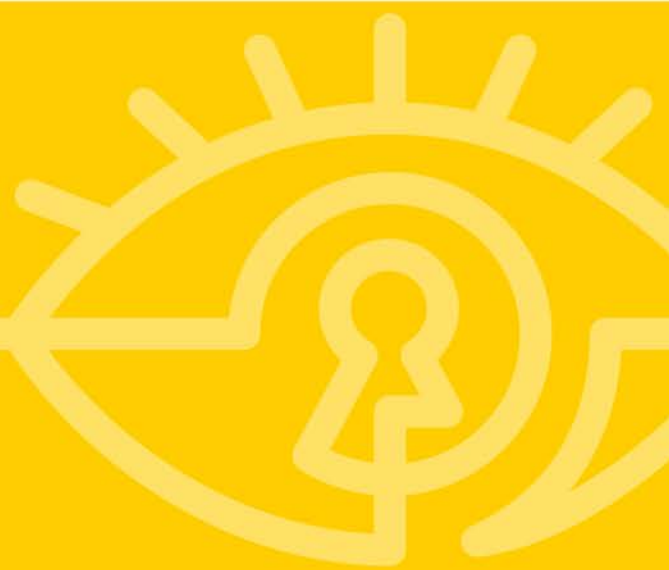
And mimics Cryptowall

Also leverages dynamic library & function loading

SAMSA (aka SAMAS, MOKOPONI)
Ransomware & targeted (APT techniques)

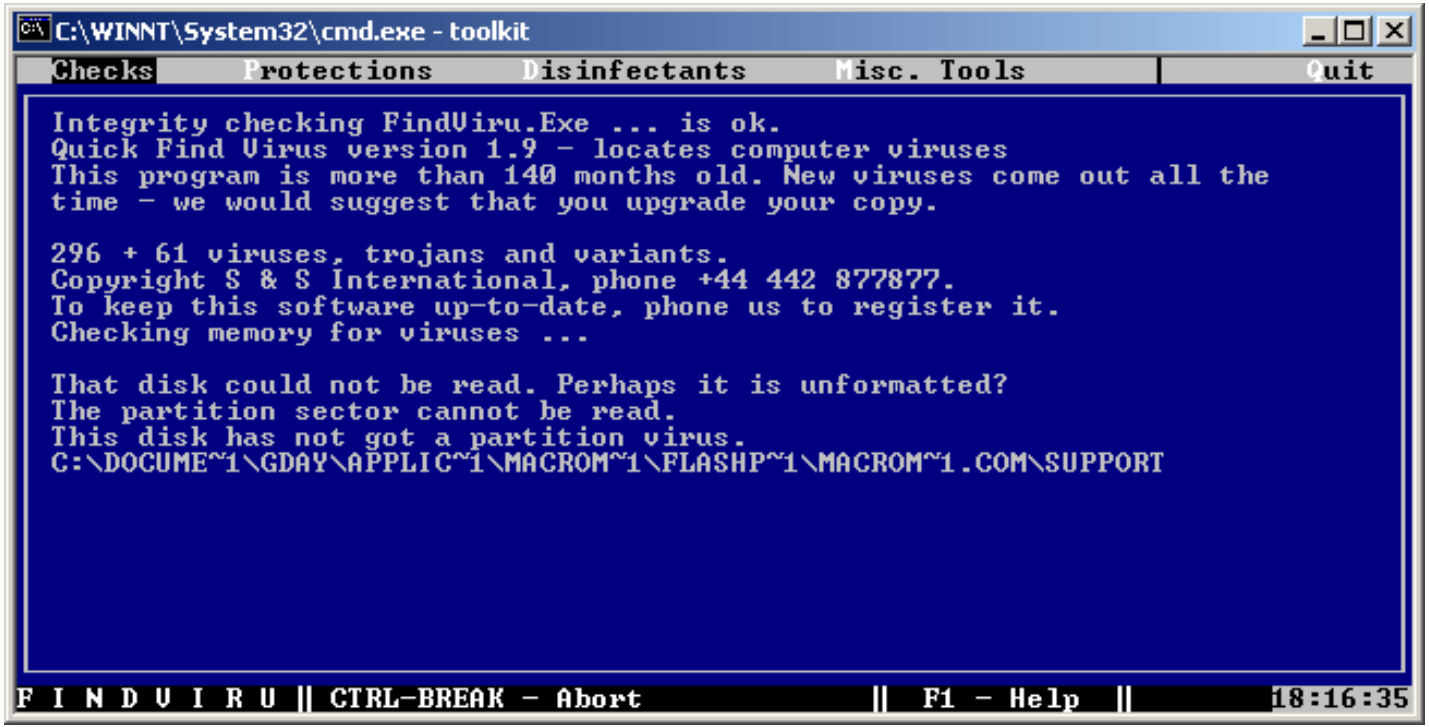
- Targeted attack + ransomware
- Over $70k in BTC payments to attackers
- Entry point to network (targeted)
  - network mapped for victims
  - SamSa deployed
- Smaller demands per-PC infection, larger per-company
- 2 interesting payments of 40 BTC, Feb 3rd and 5th





Traditional endpoint security

Traditional Endpoint



Anti-Virus – Not just signatures

- Leveraging the Cloud
  - McAfee Artemis (faster patterns) GTI
  - Symantec Insight (file reputation) GIN
- Heuristics/Generic Detection
  - Generic detection – malware family based pattern
    - Pattern match for threat attribute
  - Symantec Sonar – updated and customizable heuristics
- In memory process scanning (Where no files written to disk)

Other traditional approaches: Application control/System lockdown/HIDS/FW

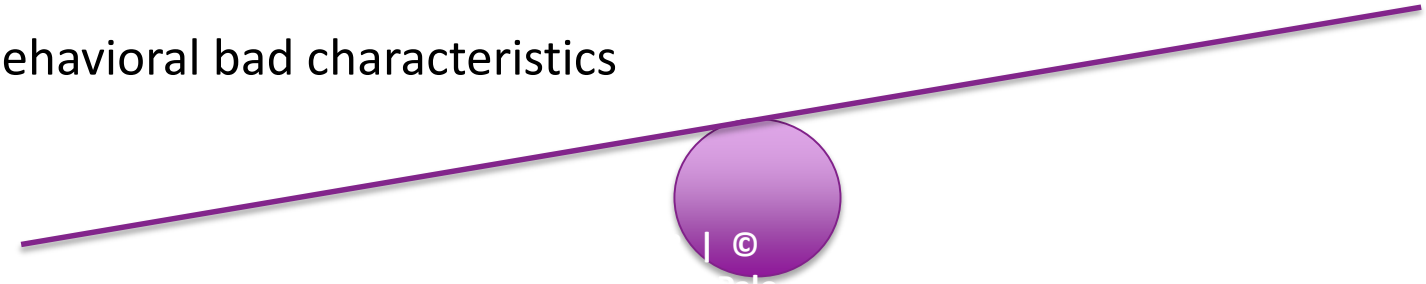
- **Common techniques based around**
  - Pattern match for known exploits (IDS/IPS)
    - McAfee Buffer Overflow protection
  - System lockdown (whitelist/backlisting)
    - Communications, Applications, File integrity
    - Account based & IR response policies
    - Microsoft Application protection

- **The Good, Bad and Ugly**
  - Tuning, tuning, tuning…
    - Manual or snapshot
    - Only as strong as the levels of lockdown
  - Lightweight, No Updates, just versions updates

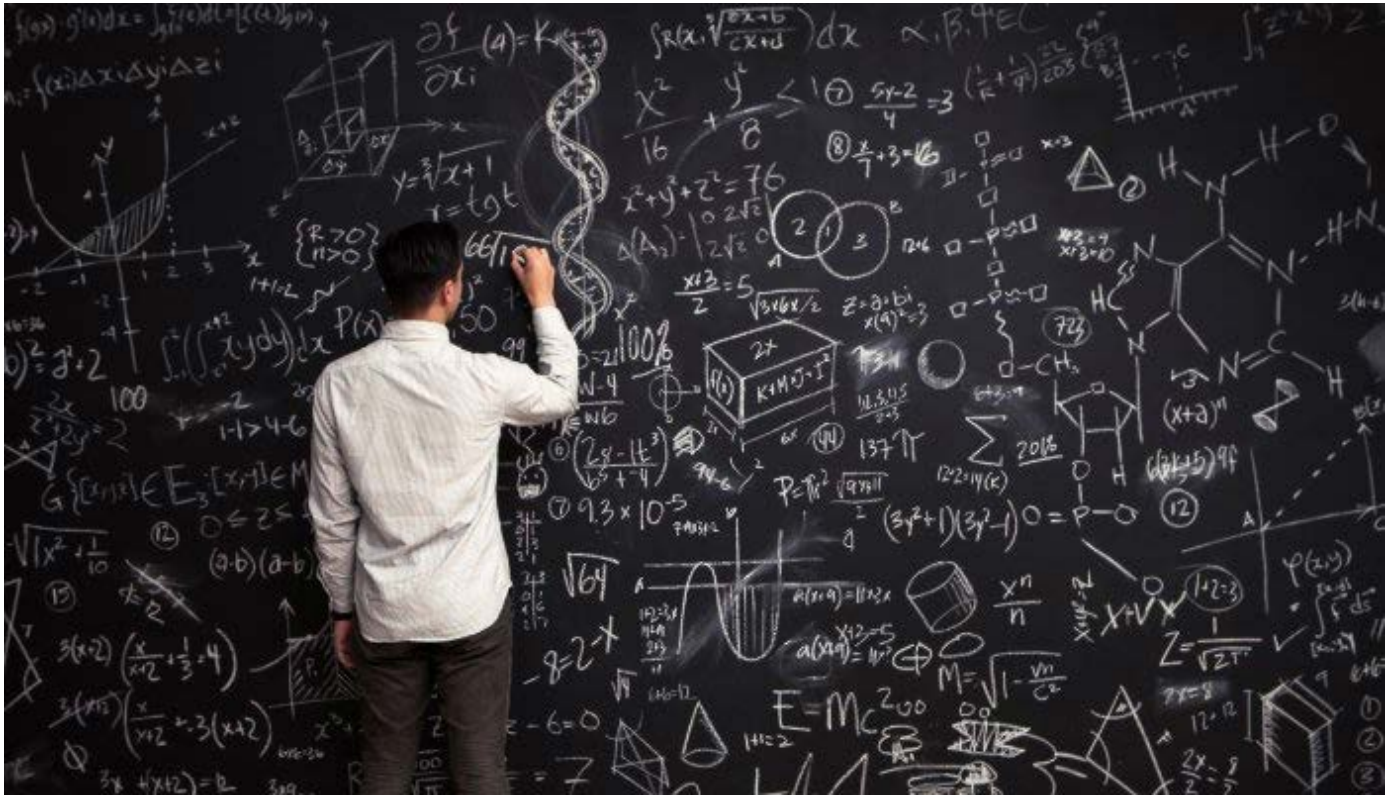
Summary

Traditional techniques

- Block known bads (sigs)
- Exploit detection (IDS/IPS)
- Black & White listing
- Behavioral bad characteristics

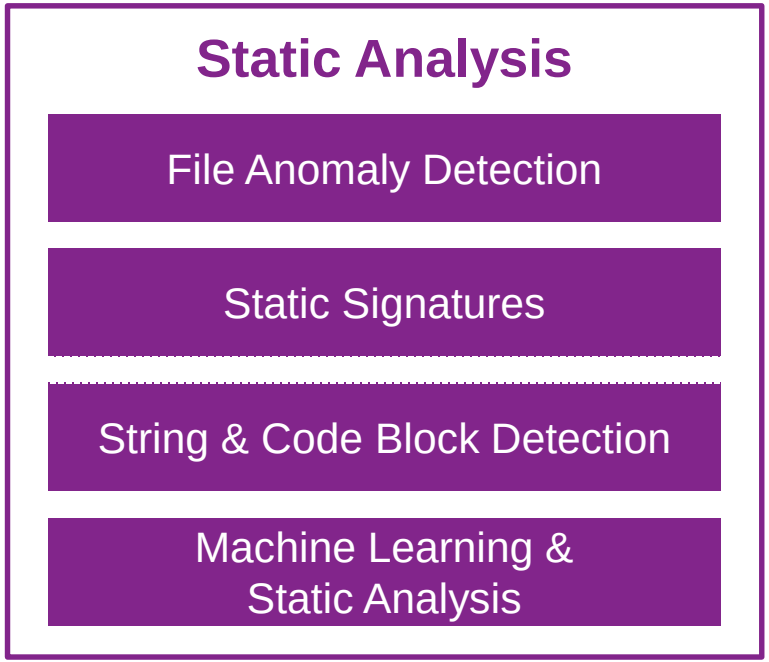


NG endpoint techniques



Static analysis

- Can be more than just MD5 signatures
- Balancing signatures against performance?
  - Everything versus what in the wild
    - Need to link to unknown detection capabilities…



NG: Machine Learning

- Looking at the building blocks of an attack
- Typically done on machine
- Requires current knowledge of how attacks are functioning
- Typically deterministic scoring
  - Been used in SPAM engines for years

NG: behavioral analysis techniques

- Replacement for heuristics/anomaly detection tools
  - Buffer Overflow = Buffer Overflow x1000 variations
  - Exploit techniques, rather than anomaly detection
  - Compromise techniques, rather than blocking registry & file

Individual Attacks

1,000s

Software Vulnerability Exploits

Thousands of new vulnerabilities and exploits

Core Techniques

2-4

Exploitation Techniques

Only two to four new exploit techniques

1,000,000s

Malware

Millions of new malware variations

~10s

Malware Techniques

Tens of new malware sub-techniques

NG: Statistical/mathmatical analysis

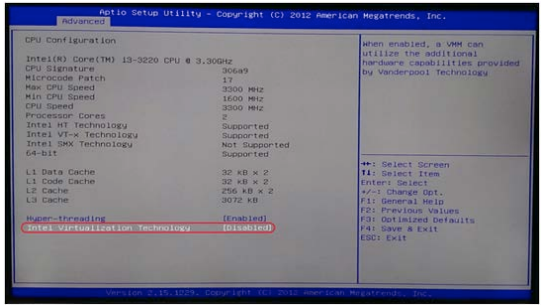
- Commonly used for Detection & Forensic analysis
  - Often used in conjunction with behavioral detection techniques
  - Anomaly detection (scope will influence accuracy)
- Accuracy often leverages additional techniques, to prevent
  - Big data lookups (DNS, File – VirusTotal, etc..)
    - Reverse heuristics (can be looking to validate known good)

Forensics (value depends on what data you pass to it)

- The scale and scope of data it can analysis
  - Real time, historic (how far: back 24-48hrs, longer?)
    - Time taken to gather the results (computing power to process data volumes)

NG: Self discovery - Sandboxing

- Provides
  - Emulation to see the real behavior
    - Validation of what happens, see's whole attack
  - Allows broad gathering of IOC data
    - Requires CPU power to deal with volume
- Where to put the Sandbox (Speed vs CPU power)
  - On Device or network
    - Browser, APPs or OS
  - In the Cloud
  - Hybrid
- Anti-sandbox evasion techniques detection



Confidence in the process…. supporting the greater good

SECURITY WEEK

INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

VirusTotal Policy Change Rocks Anti-Malware Industry

By Kevin Townsend on May 12, 2016

A VirusTotal Policy Change Has Exacerbated the Bad Blood Between Traditional and Next-gen Anti-malware Companies

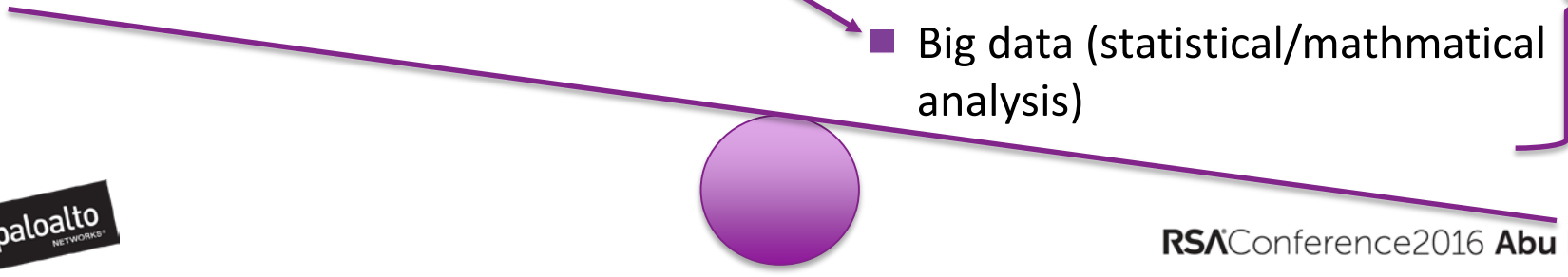
Summary – Evolution of techniques

Traditional techniques

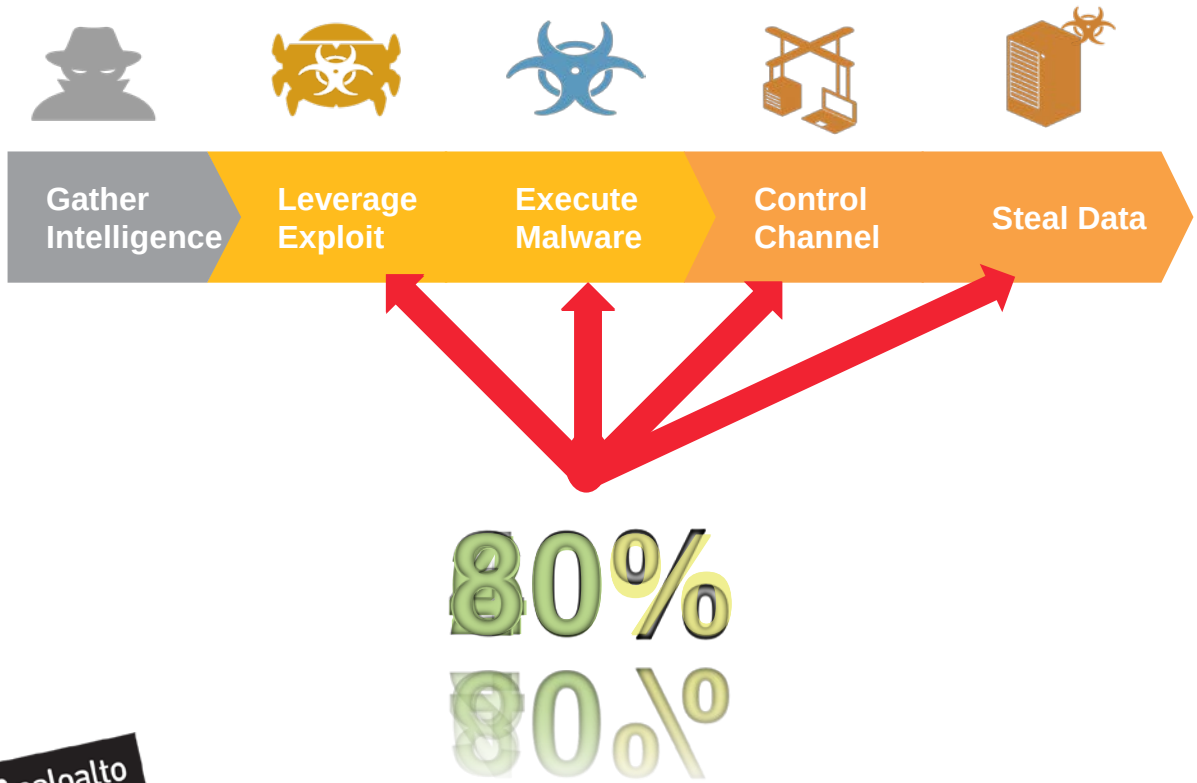
- Block known bads (sigs)
- Exploit detection
- White & black listing
- Behavioral bad characteristics

NG techniques

- Static analysis
- Behavioral techniques & threat specific whitelisting (playbooks)
- Sandboxing
- Machine learning
- Big data (statistical/mathmatical analysis)



How much confidence to block/act?



How do I measure effectiveness?

What are you looking to test?

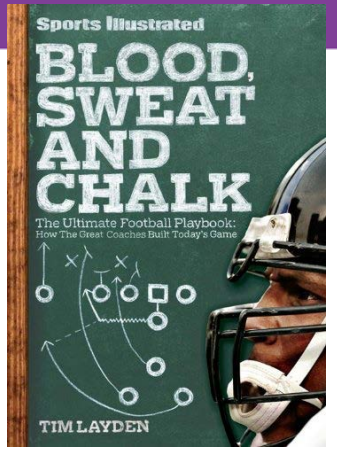
- Ability to detect zero day threats
  - What level of breach is acceptable to you? – Ransomware
- Ability to detect traditional threats

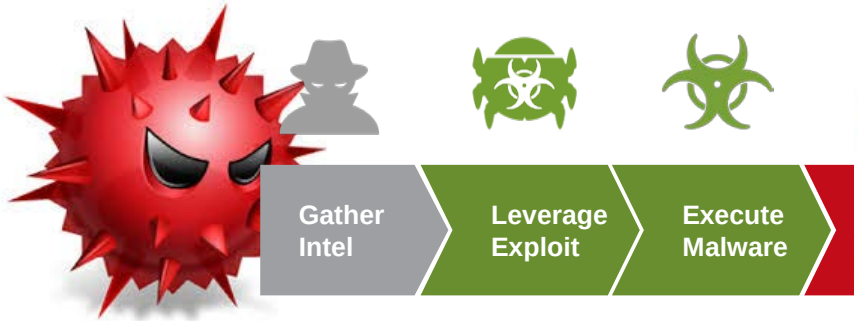
What testing?

- Independent tests
  - AV-comparitives, SELabs, NSS labs, AV-Test, etc…
- In- house testing
  - Detection
  - Manageability
  - How does endpoint security fit into your broader ecosystem?

Endpoint security is more than detection/prevention

Player, play, playbook





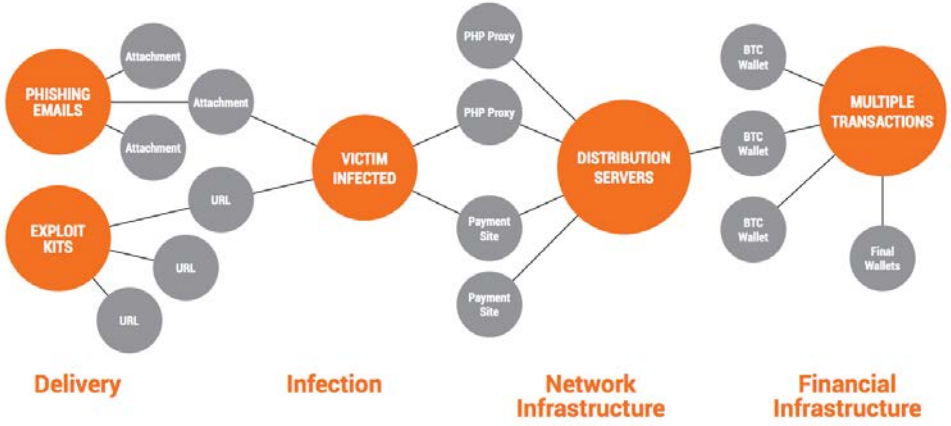
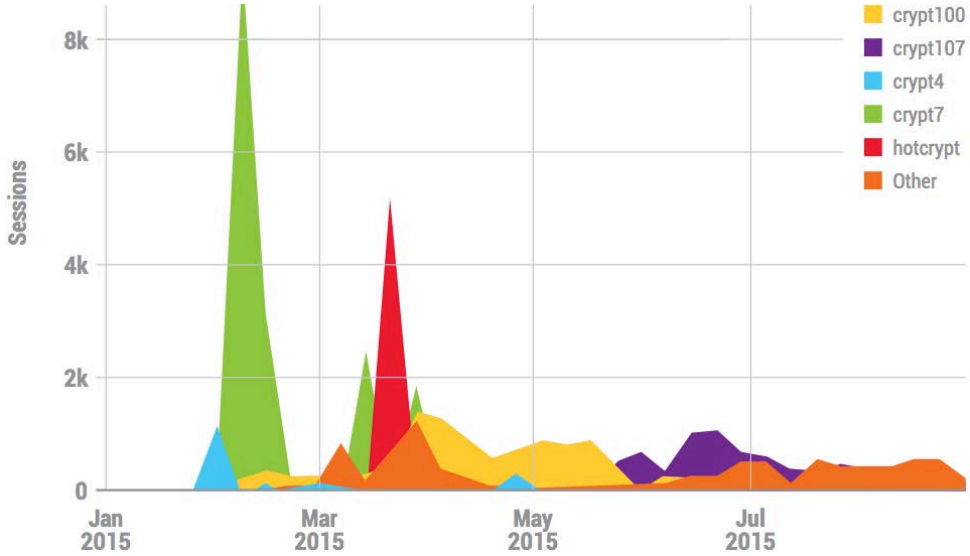
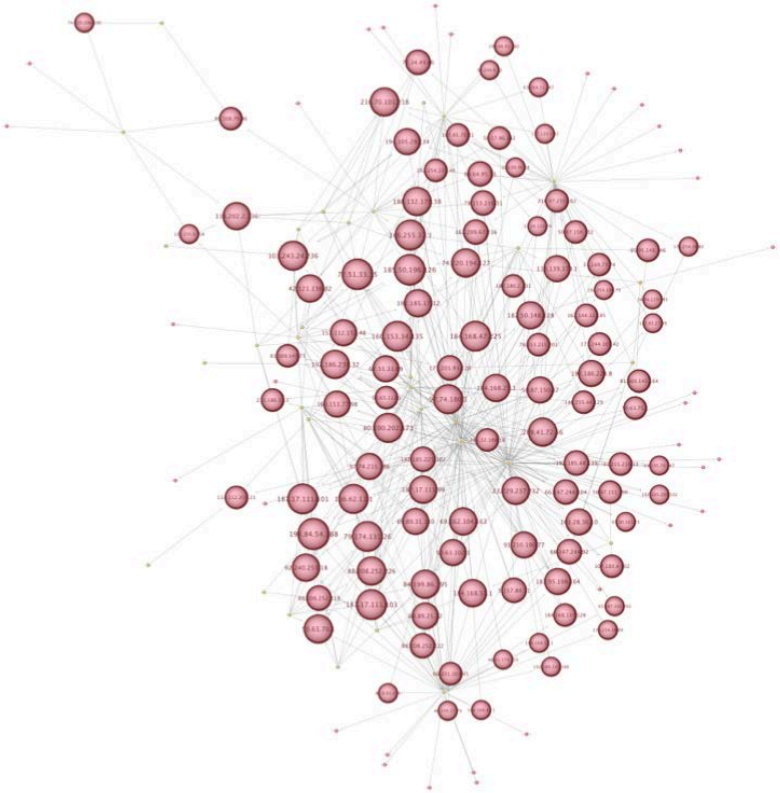


FIGURE 1 Anatomy of a CW3 attack. *Source: Cyber Threat Alliance*

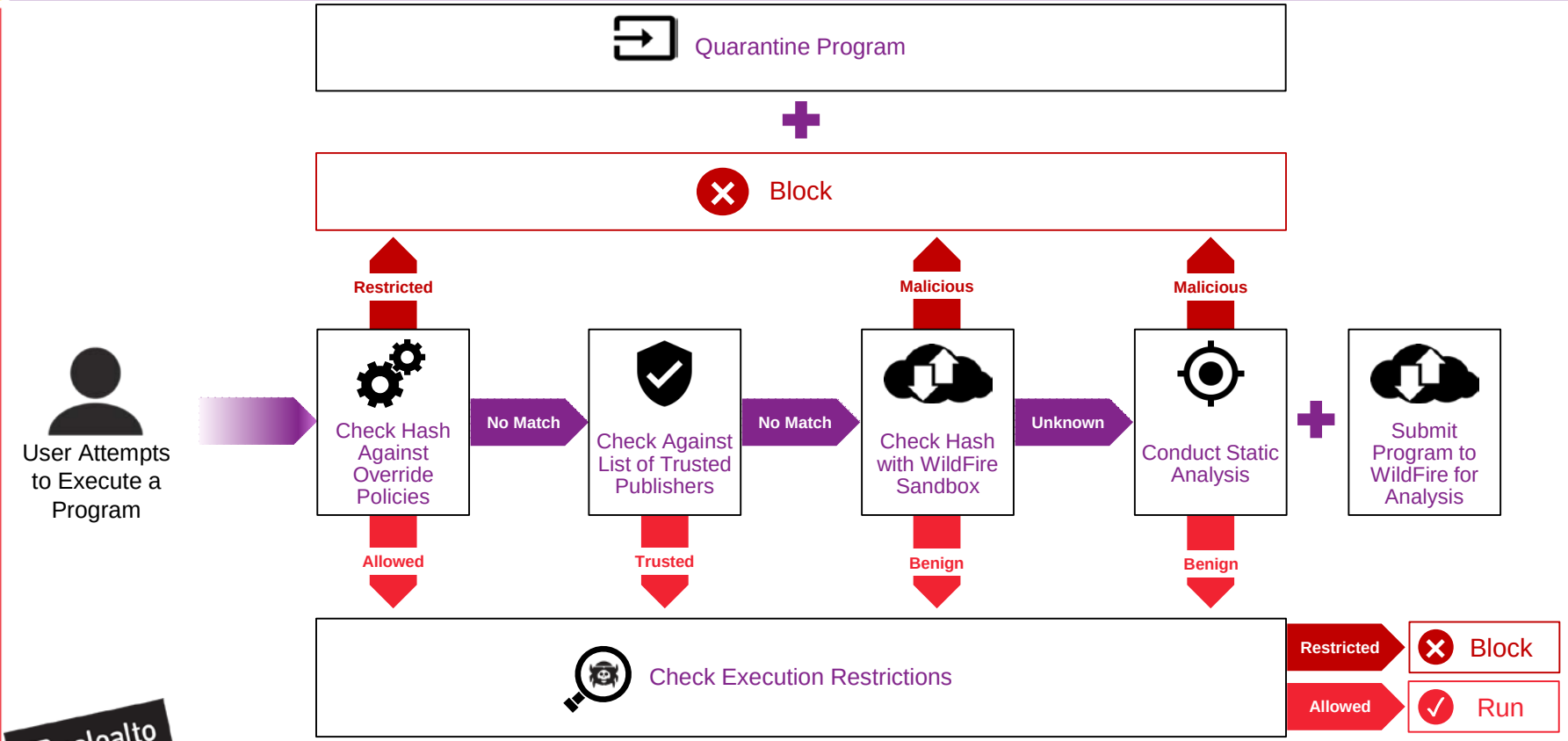
paloalto NETWORKS

Campaigns

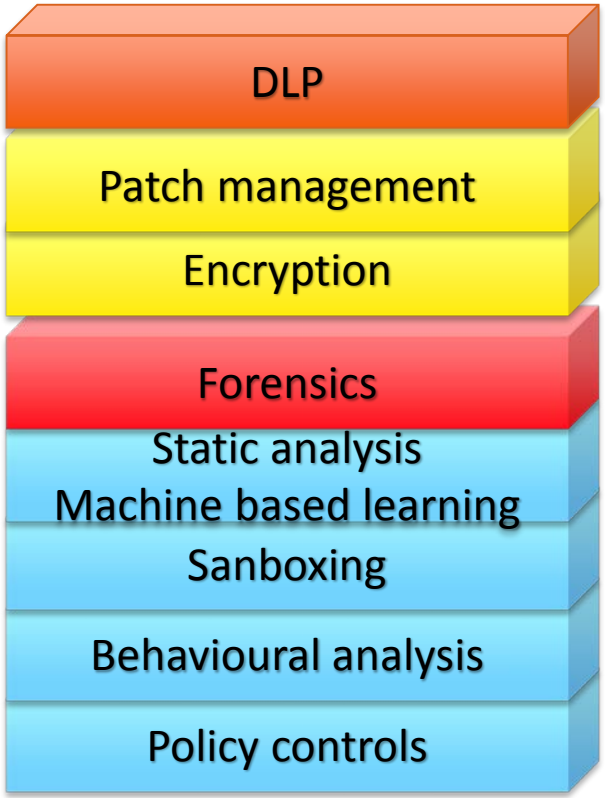

crypt100
crypt107
crypt4
crypt7
hotcrypt
Other
Sessions
8k
6k
4k
2k
0
Jan 2015
Mar 2015
May 2015
Jul 2015



Protection in depth = NG techniques together

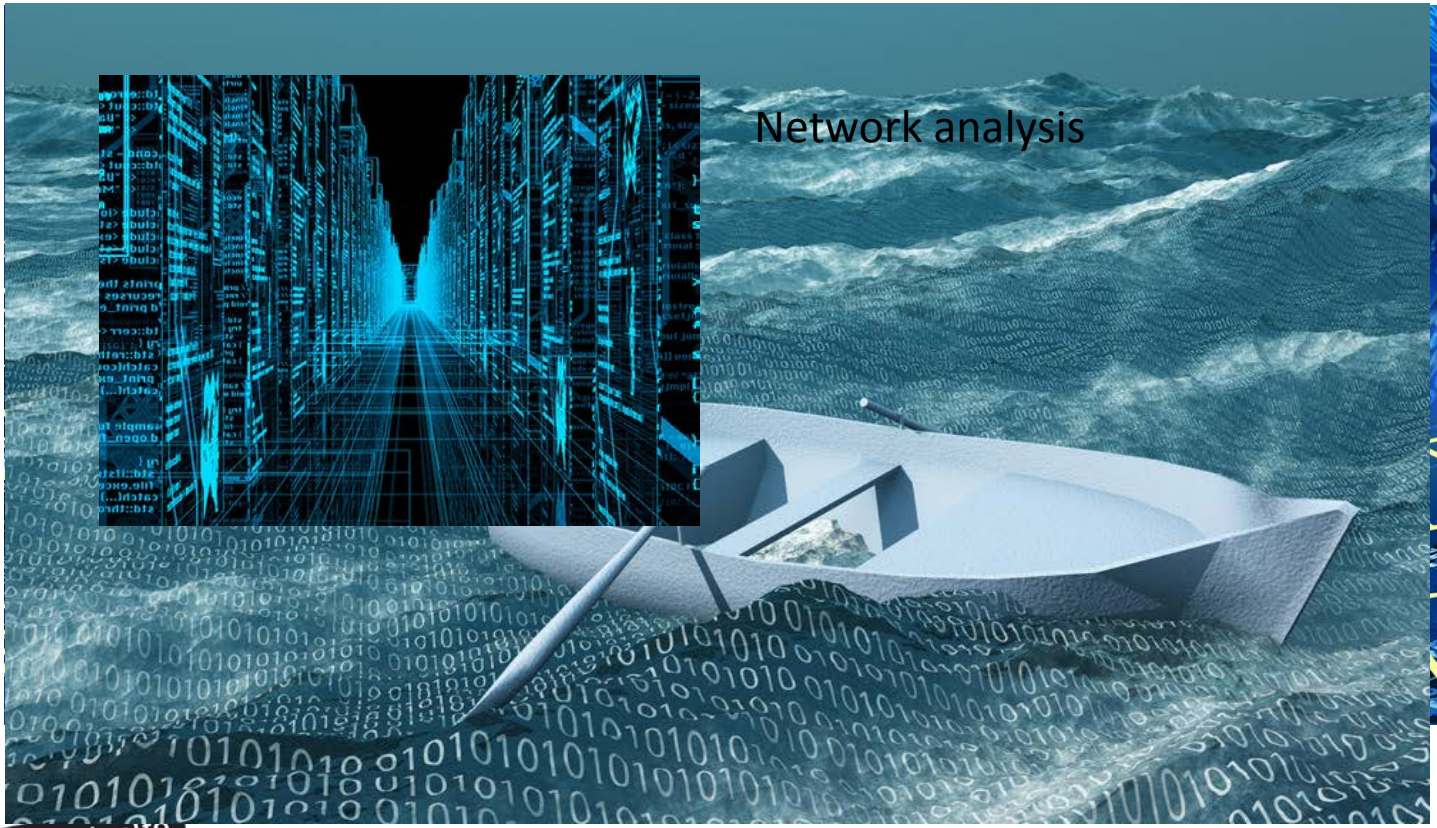


Building the endpoint stack for the future..



paloalto NETWORKS

So does all this this work?



Building out the security platform
Defragmenting the broader capabilities

Other things to consider?

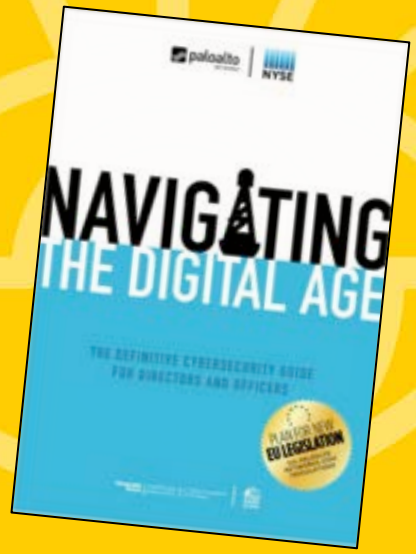
- Think big picture and long term
  - Connected or silo'ed analysis?
  - Integration with broader security platforms (learn & share)
- Compliance
  - Microsoft Security Centre approved (user pop-ups)
  - Regulation compliant – PCI-DSS, etc…

Takeaways

- What are you looking to achieve?
- Define what your endpoint stack requires for your business!
- Look at industry tests, but also DO YOUR OWN testing
  - Criteria should include
    - Prevention/Detection of what is most impactful to your business
    - Manageability/Usability
    - Integration between capabilities
    - Integration into your broader security platform

Thank you….

QUESTIONS?



GDay@PaloAltoNetworks.com
GregDaySecurity
uk.linkedin.com/in/gregday
+44 (0) 7799 661164

https://www.securityroundtable.org/