

RSAConference2016

Abu Dhabi | 15–16 November | Emirates Palace

SESSION ID: CEM-W06

Next Generation Endpoint Security – Confused?



#RSAC



Connect **to**
Protect

Greg Day

VP & Chief Security Officer, EMEA
Palo Alto Networks
@GreDaySecurity



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



symantec



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

CRN

NEWS, ANALYSIS AND
VARs AND TECHNOLOGY

HOME NEWS COMPANIES ▾ SLIDESHOWS VIDEO BLOGS

WOMEN OF THE CHANNEL JOBS TECHNOLOGIES ▾

Apps & OS ▾ Channel ▾ Cloud ▾ Components & Peripherals ▾ Data Center

* **CRN Exclusive: HP COO Flaxman Reaffirms Commitment**

[Like](#) [Share 2](#) [in Share](#) [Tweet](#) [G+](#)

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 2



Inside The Competitive Testing Battlefield of Endpoint Security

By Kevin Townsend on July 19, 2016

[in Share](#) [183](#) [G+](#) [7](#) [Tweet](#) [Recommend](#) [21](#) [RSS](#)



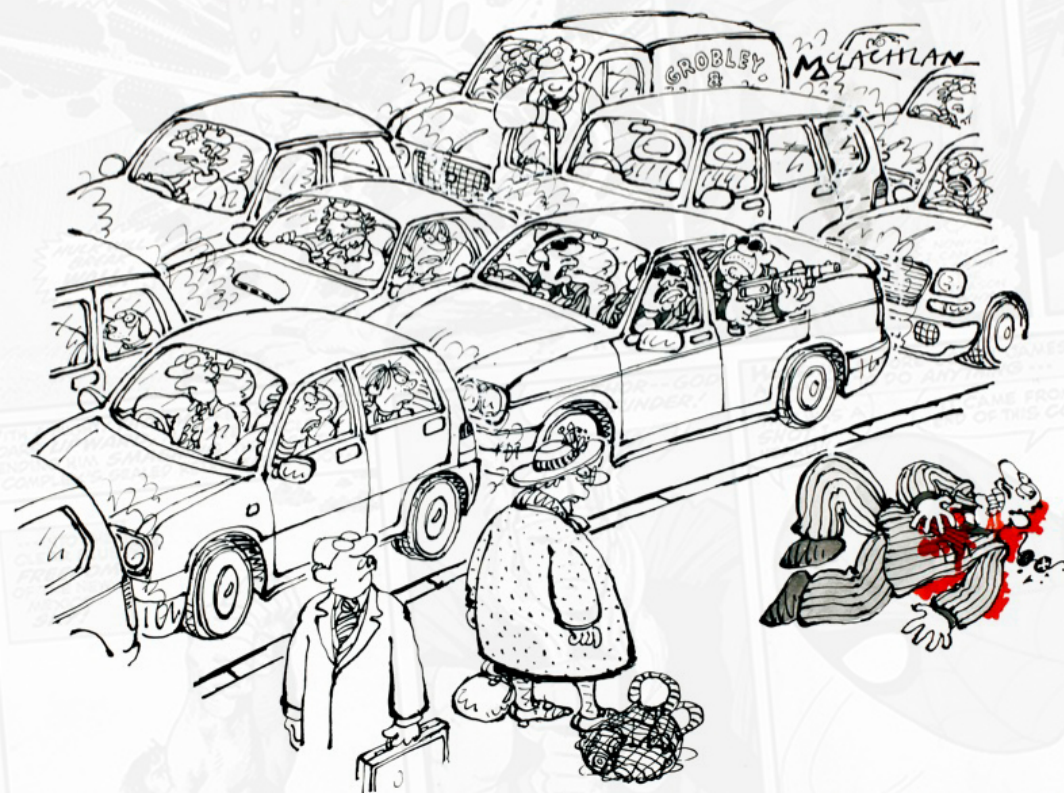
Traditional AV Firms Battle "Next-Gen" Endpoint Security Vendors for Share of Anti-malware Market

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.



RSA Conference 2016 Abu Dhabi

What simulated this debate: Evolution!



"A drive-by shooting in a traffic jam is not a good idea, O'Flanagan."



TeslaCrypt ransomware: splicing together new attacks

#RSAC



VT 54

Your private
data is
destroyed
10/11

Time left:

Show I

What happened?
All of your files were encrypted.
More information at: <http://alcor44.tk>

What does this mean?
This means that the files are encrypted.
With them, read the files.

How did this happen?
Especially for you,
All your files were encrypted.
Decrypting of YOUR files.

What do I do?
Alas, if you do not
If you really need your files,
For more specific information:
1. <http://alcor44.tk>
2. <http://alcor44.tk>
3. <http://alcor44.tk>

If for some reason:
1. Download and install the program.
2. After a successful installation.
3. Type in the address:
4. Follow the instructions.

IMPORTANT INFORMATION:
Your Personal PAGES:
<http://alcor44.tk>
<http://alcor44.tk>
<http://alcor44.tk>
Your Personal PAGES (using TOR):
Your personal code (if you open the site [or TOR] directly):

```
.text:00410000 1  PCHAF
.text:00410001 2  {
.text:00410002 3  PCHAF
.text:00410003 4  if
.text:00410004 5  PCHAF
.text:00410005 6  PCHAF
.text:00410006 7  PCHAF
.text:00410007 8  PCHAF
.text:00410008 9  STR
.text:00410009 10 PCHAF
.text:0041000A 11 PCHAF
.text:0041000B 12 PCHAF
.text:0041000C 13 PCHAF
.text:0041000D 14 PCHAF
.text:0041000E 15 STR
.text:0041000F 16 PCHAF
.text:00410010 17 PCHAF
.text:00410011 18 STR
.text:00410012 19 PCHAF
.text:00410013 20 PCHAF
.text:00410014 21 STR
.text:00410015 22 STR
.text:00410016 23 STR
.text:00410017 24 }
```

```
push edi
mov edi, [ebp+var_4]
push 0CEBF17E6h ; dwProcNameHash
push 2 ; dwModule
push 0 ; Dll
call GetProcAddressEx
add esp, 0Ch
push ebx
push esi
push 0
push 1
push 0
push edi
call eax
test eax, eax
jz short loc_412A37
mov ecx, [ebx]
mov byte ptr [esi+ecx], 0

; CODE XREF: sub_4129F0+3F'j
mov edi, [ebp+var_4]
push 0D4B3D42h ; dwProcNameHash
push 2 ; dwModule
push 0 ; Dll
call GetProcAddressEx
add esp, 0Ch
push edi
call eax
mov edi, [ebp+iv]
push 72760BB8h ; dwProcNameHash
push 2 ; dwModule
push 0 ; Dll
call GetProcAddressEx
add esp, 0Ch
push 0
push edi
call eax
```

2013

And mimics Cryptowall

Also leverages dynamic library & function loading

RSA Conference 2016 Abu Dhabi

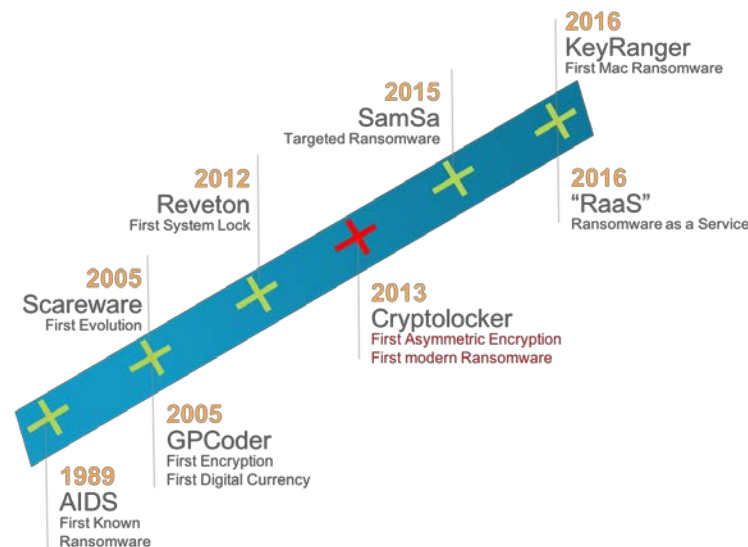


SAMSA (aka SAMAS, MOKOPONI)

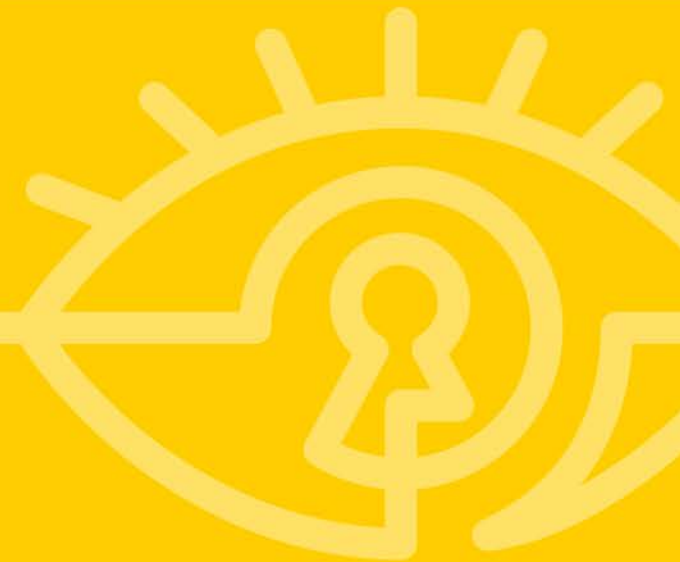
Ransomware & targeted (APT techniques)



- 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



```
C:\WINNT\System32\cmd.exe - toolkit
Checks Protections Disinfectants Misc. Tools Quit

Integrity checking FindVirus.Exe ... is ok.
Quick Find Virus version 1.9 - locates computer viruses
This program is more than 140 months old. New viruses come out all the
time - we would suggest that you upgrade your copy.

296 + 61 viruses, trojans and variants.
Copyright S & S International, phone +44 442 877877.
To keep this software up-to-date, phone us to register it.
Checking memory for viruses ...

That disk could not be read. Perhaps it is unformatted?
The partition sector cannot be read.
This disk has not got a partition virus.
C:\DOCUME~1\GDAY\APPLIC~1\MACROM~1\FLASHP~1\MACROM~1.COM\SUPPORT

F I N D V I R U || CTRL-BREAK - Abort || F1 - Help || 18:16:35
```

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)

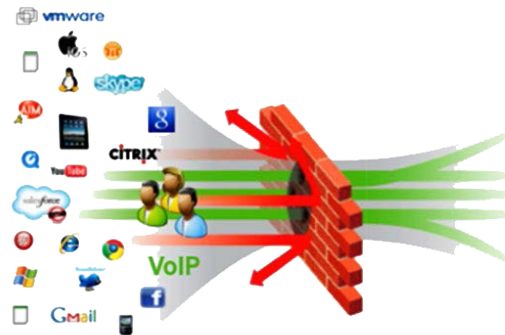


Other traditional approaches: Application control/System lockdown/HIDS/FW



- **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



Symantec Critical System Protection: Hack-Proof at Black Hat

Created: 13 Aug 2012 | 8 comments



Another year, another exciting Black Hat Conference. For the second consecutive year, Symantec challenged conference attendees to "Capture the Flag." While Symantec ran several smaller contests, the main event was run by placing a flag on an unpatched Windows 2003 server running several vulnerable applications, protected by Symantec solutions. After two days of attempts by more than 50 skilled hackers, the Symantec protected systems remained hack-proof.

So what prevented some of the best in the world from prevailing? Symantec Critical System Protection and Symantec Endpoint Protection.

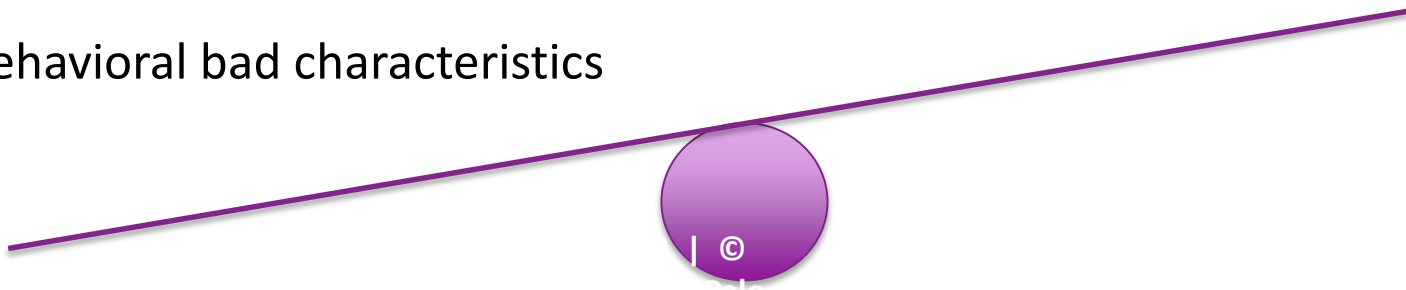
- Symantec Critical System Protection secured the system by sandboxing the OS and applications. The attacks known or unknown that were thrown at the box were contained and jailed from accessing resources on the system. The flags were locked down to only allow authorized access to the data.
- Symantec Endpoint Protection was leveraged to thwart network based attacks and black-list hackers IP addresses that were attempting to enumerate or exploit the system.

Symantec Critical System Protection is policy-based protection that offers comprehensive protection for vSphere, stops zero-day attacks, targeted attacks and provides real-time visibility and control of an organization's compliance posture.

If you missed out on the fun at the Symantec booth we hope to see you at Black Hat next year.

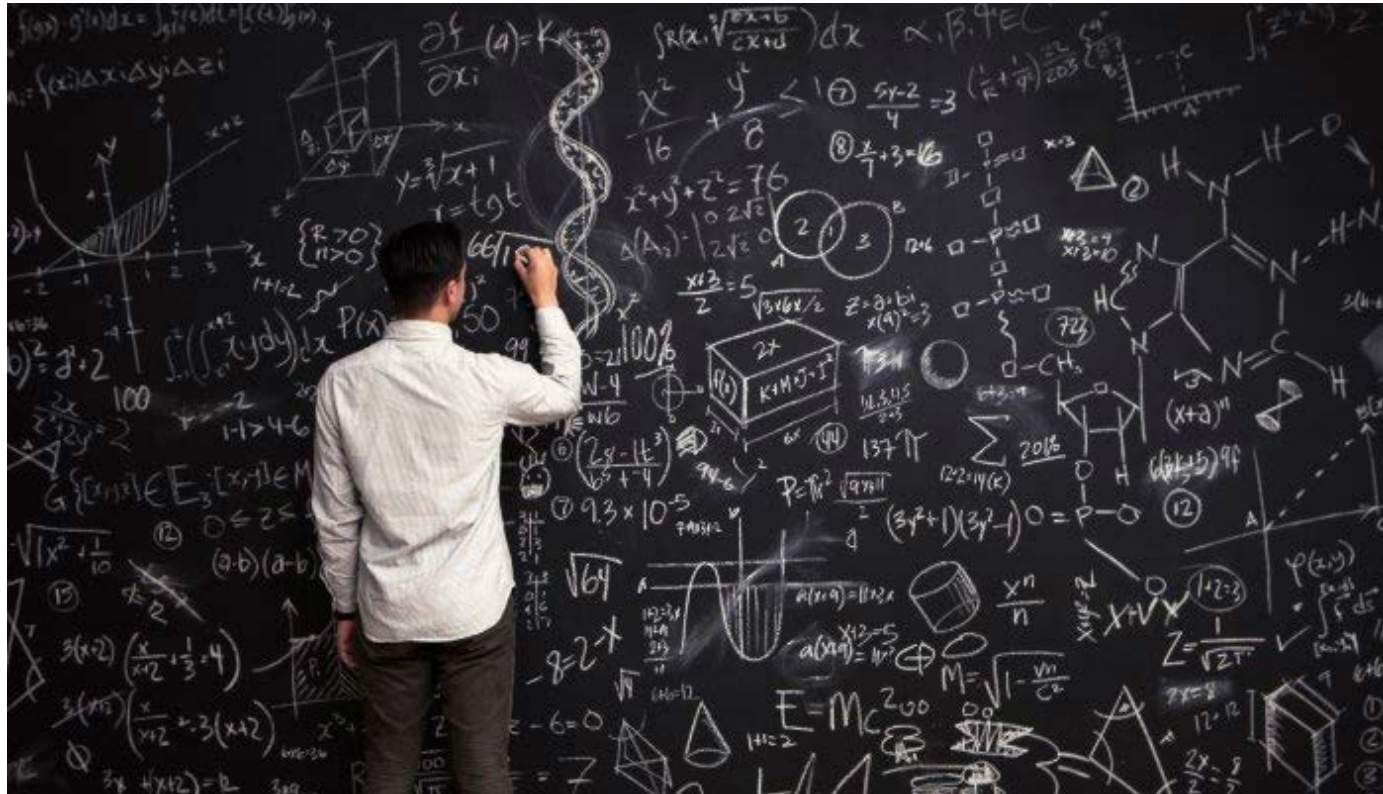
Traditional techniques

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



NG endpoint techniques

#RSAC



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

Static Analysis

File Anomaly Detection

Static Signatures

String & Code Block Detection

Machine Learning &
Static Analysis

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

1,000,000s

Malware

Millions of new malware variations



Core Techniques
2-4

Exploitation Techniques

Only two to four new exploit techniques

~10s

Malware Techniques

Tens of new malware sub-techniques

RSAConference2016 Abu Dhabi

- 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)

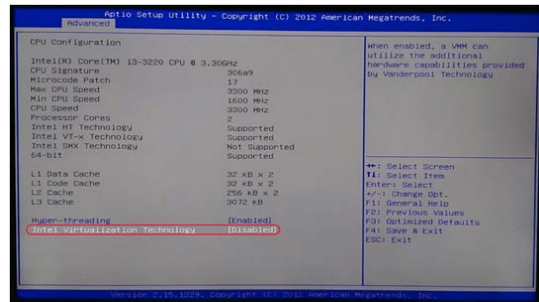
- The scale and scope of data it can analysis
 - Real time, historic (how far: back 24-48hrs, longer?)
 - Time taken to gather the results (computing power to process data volumes)

NG: Self discovery - Sandboxing

#RSAC



- 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



VirusTotal Policy Change Rocks Anti-Malware Industry

By Kevin Townsend on May 12, 2016



A VirusTotal Policy Change Has Exacerbated the Bad ¹⁹ood Between Traditional and Next-gen Anti-malware Companies



RSA[®]Conference2016 Abu Dhabi

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)

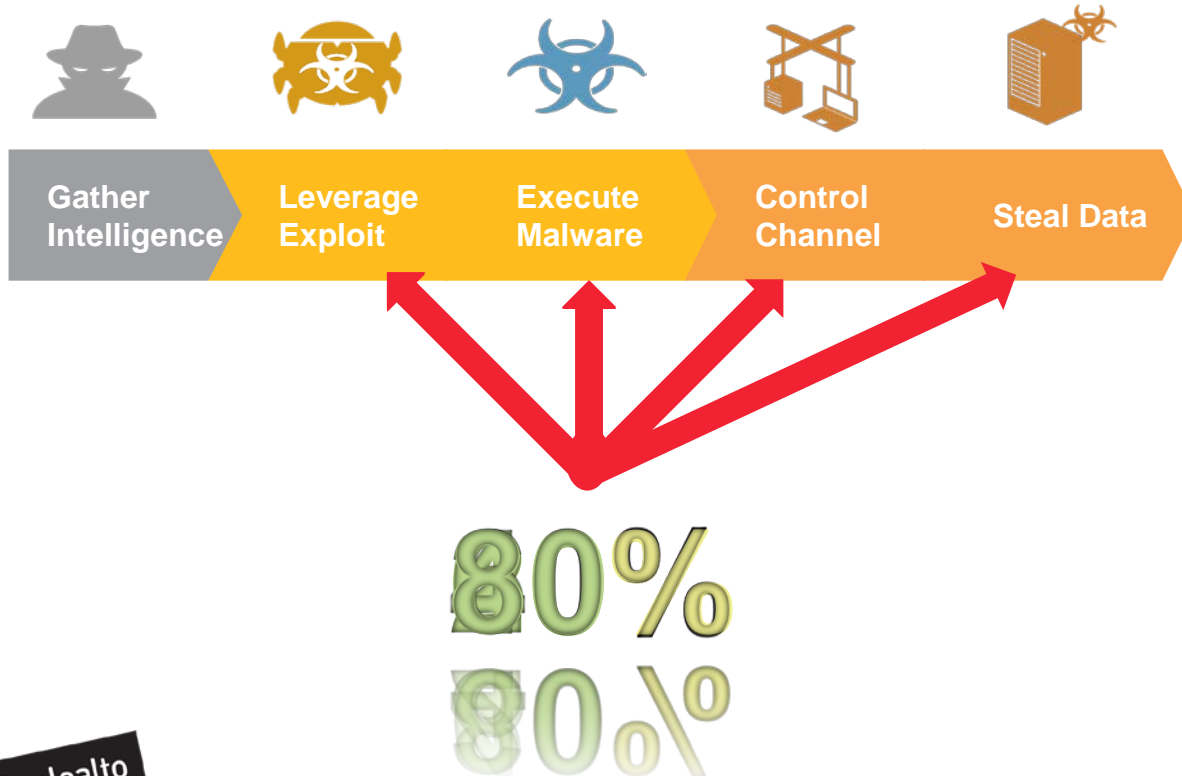
■ Sandboxing

■ Machine learning

■ Big data (statistical/mathematical 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

#RSAC

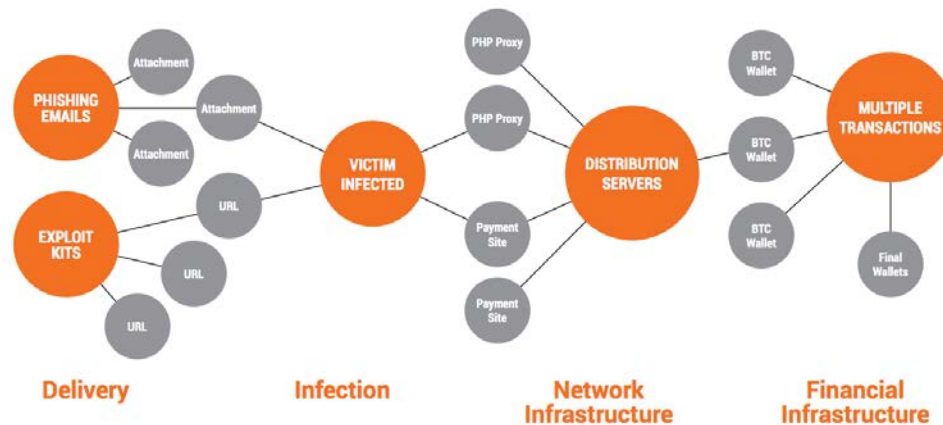
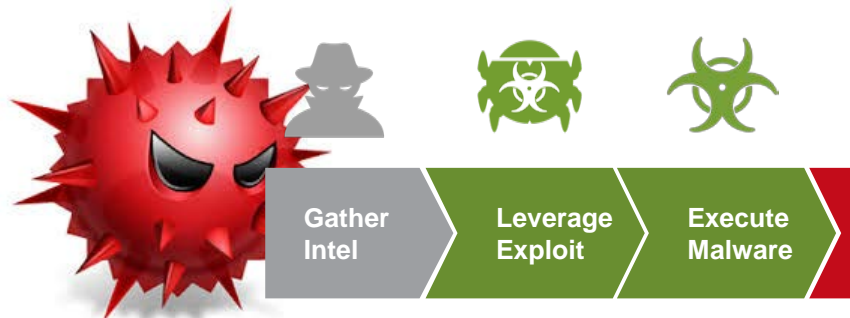
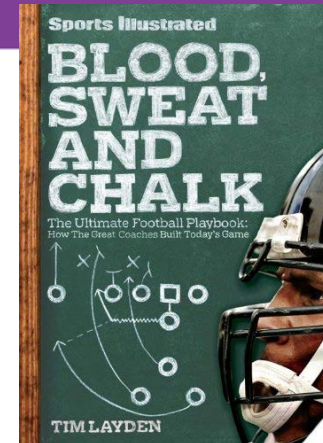
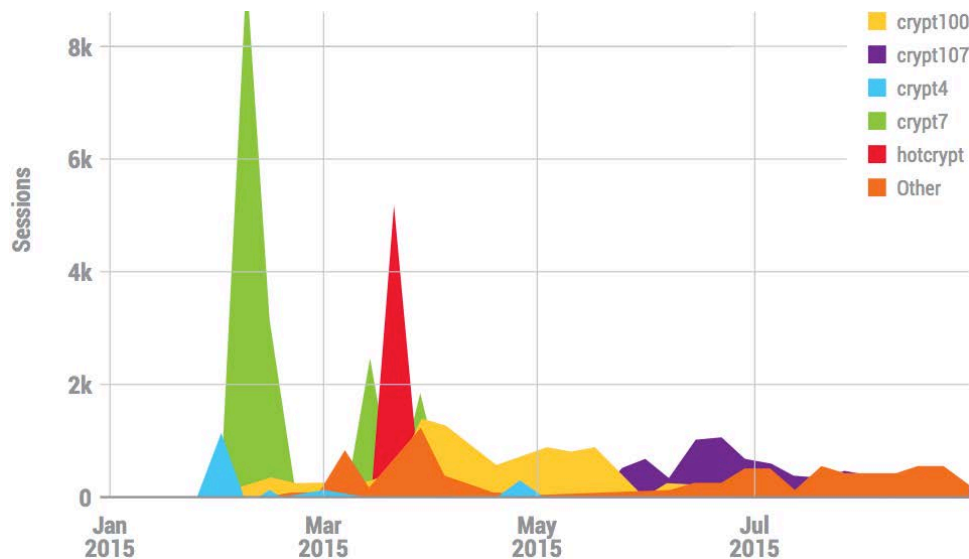


FIGURE 1 Anatomy of a CW3 attack. Source: Cyber Threat Alliance

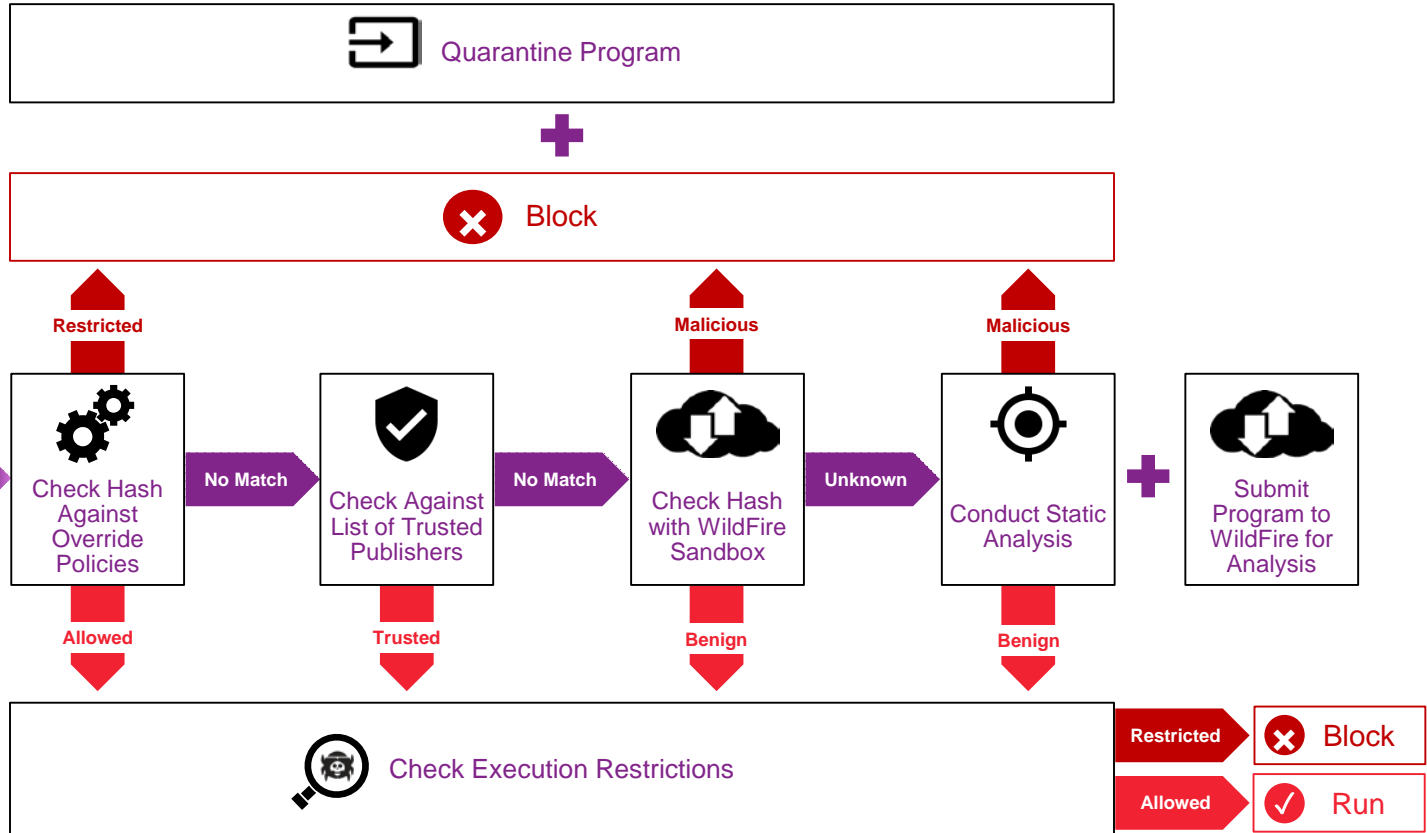
Campaigns



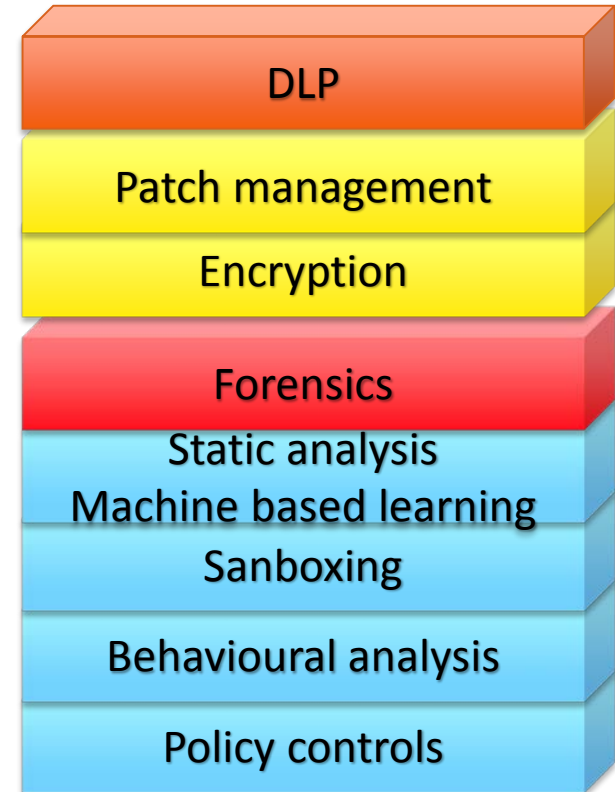
Protection in depth = NG techniques together



User Attempts
to Execute a
Program



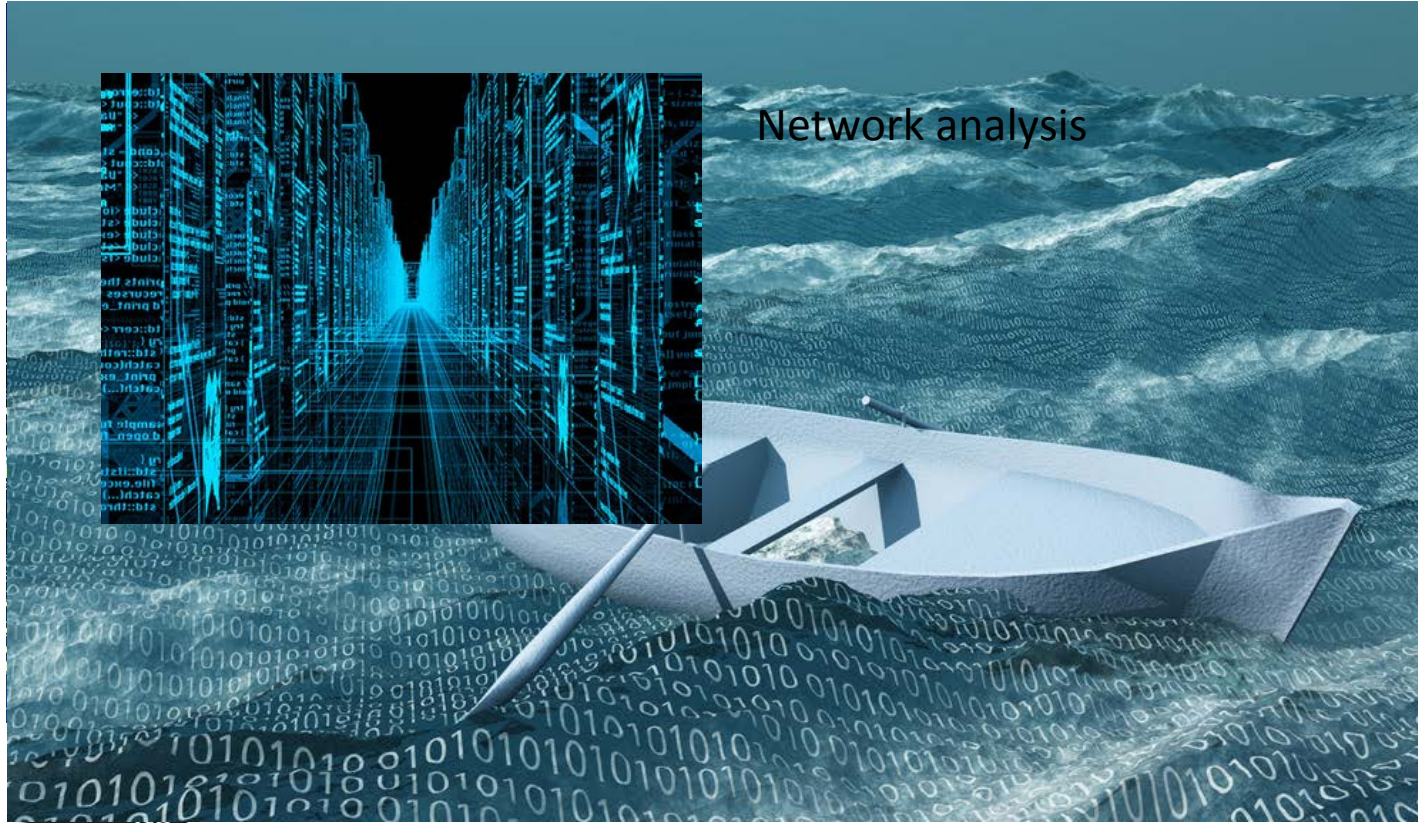
Building the endpoint stack for the future..



So does all this this work?



#RSAC



Network analysis



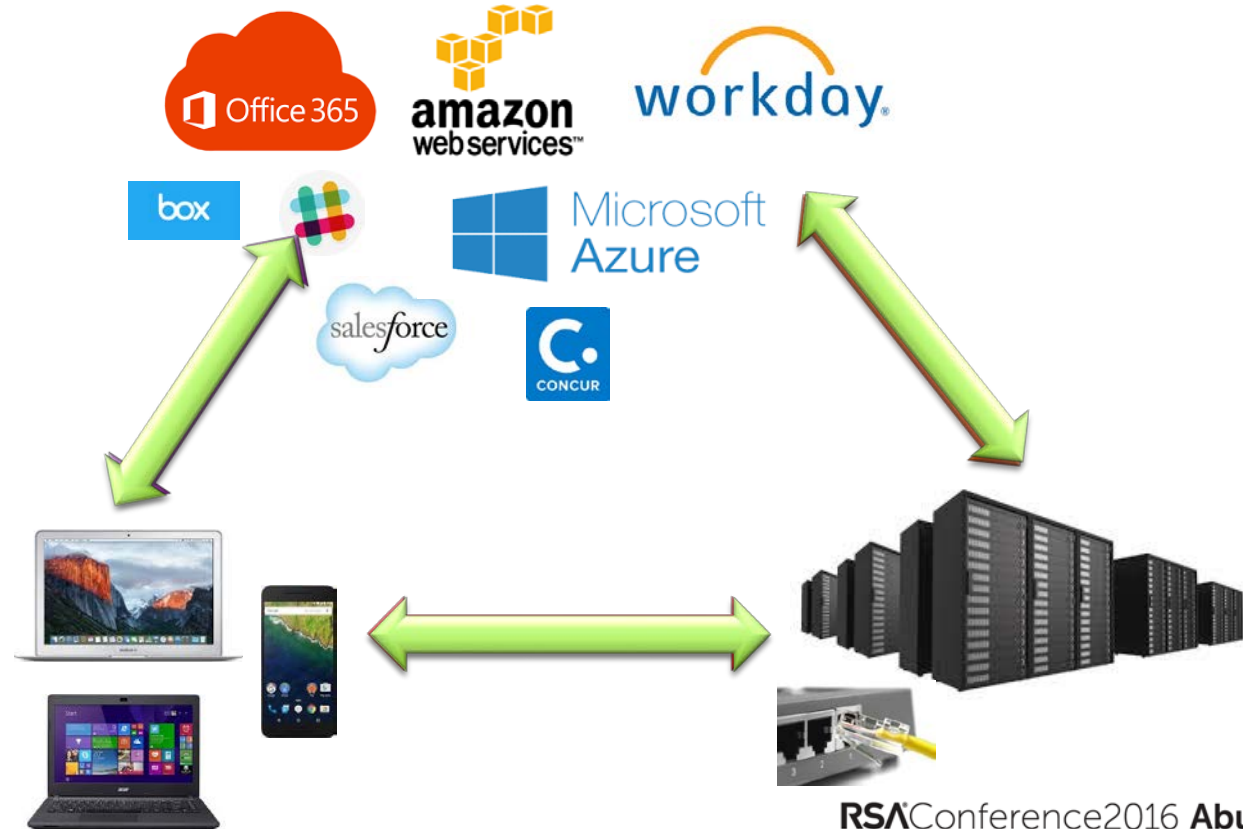
Endpoint analysis



RSA Conference 2016 Abu Dhabi

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...

- 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?

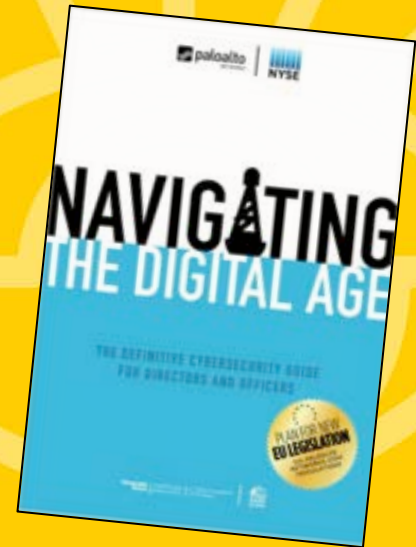


GDay@PaloAltoNetworks.com

GregDaySecurity

uk.linkedin.com/in/gregday

+44 (0) 7799 661164



<https://www.securityroundtable.org/>