Symantec™

Advanced Threat Protection

Technical Overview

Agenda

1 Advanced Threat Protection Prevent advanced persistent threats

2 Advanced Threat Protection Identify suspicious files

3 Advanced Threat Protection Search for Indicators of Compromise

4 Advanced Threat Protection Block, isolate and remove the advanced persistent threats

5 Advanced Threat Protection Minimize environmental changes

6 Symantec Product Integration and Support

7 Additional Resources and Summary

Let’s get started!

What are Advanced Threats ?

Targeted

Targets specific organizations and/or nations for business or political motives

Stealthy

Uses previously unknown zero-day attacks, root kits, and evasive technologies

Persistent

Sophisticated command and control systems that continuously monitor and extract data from the specific target

How They Work: Advanced Threats

1. INCURSION

Attackers break into network by using social engineering to deliver targeted malware to vulnerable systems and people.

2. DISCOVERY

Once in, the attackers stay "low and slow" to avoid detection.

They then map the organization's defenses from the inside and create a battle plan and deploy multiple parallel kill chains to ensure success.

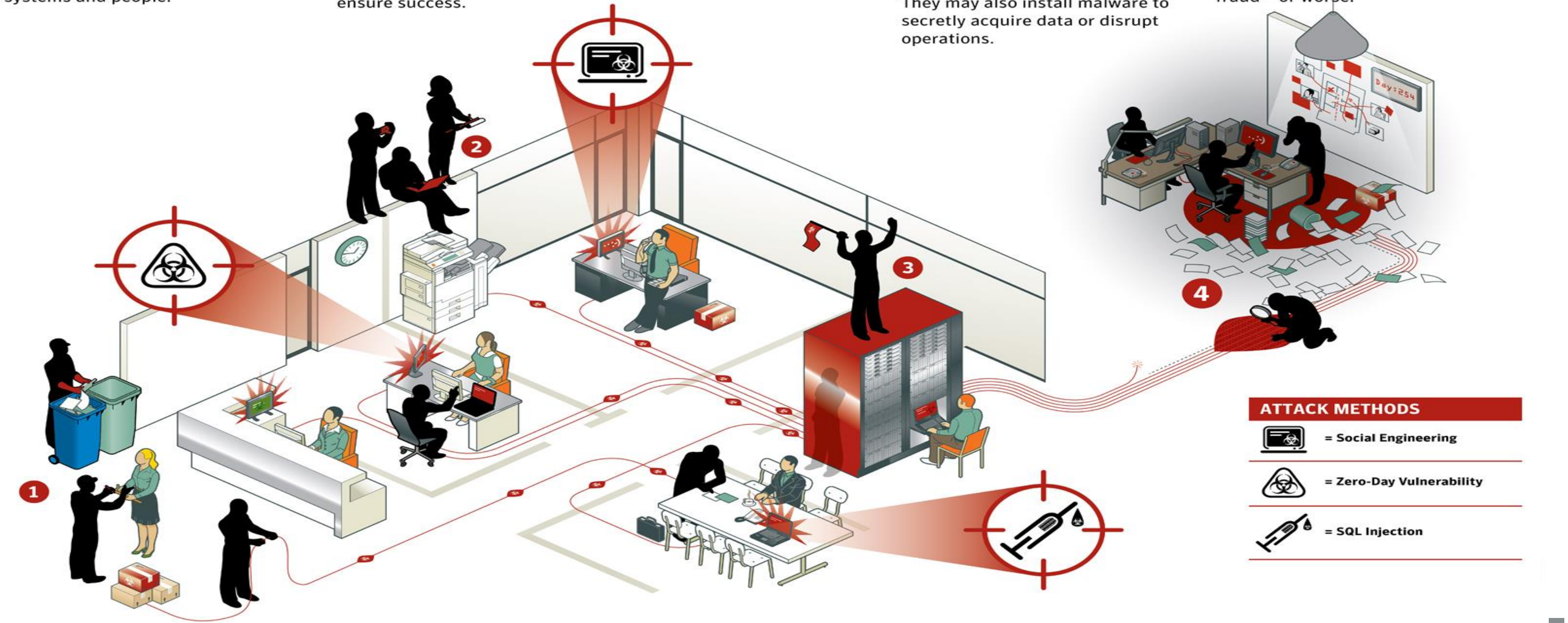
3. CAPTURE

Attackers access unprotected systems and capture information over an extended period.

They may also install malware to secretly acquire data or disrupt operations.

4. EXFILTRATION

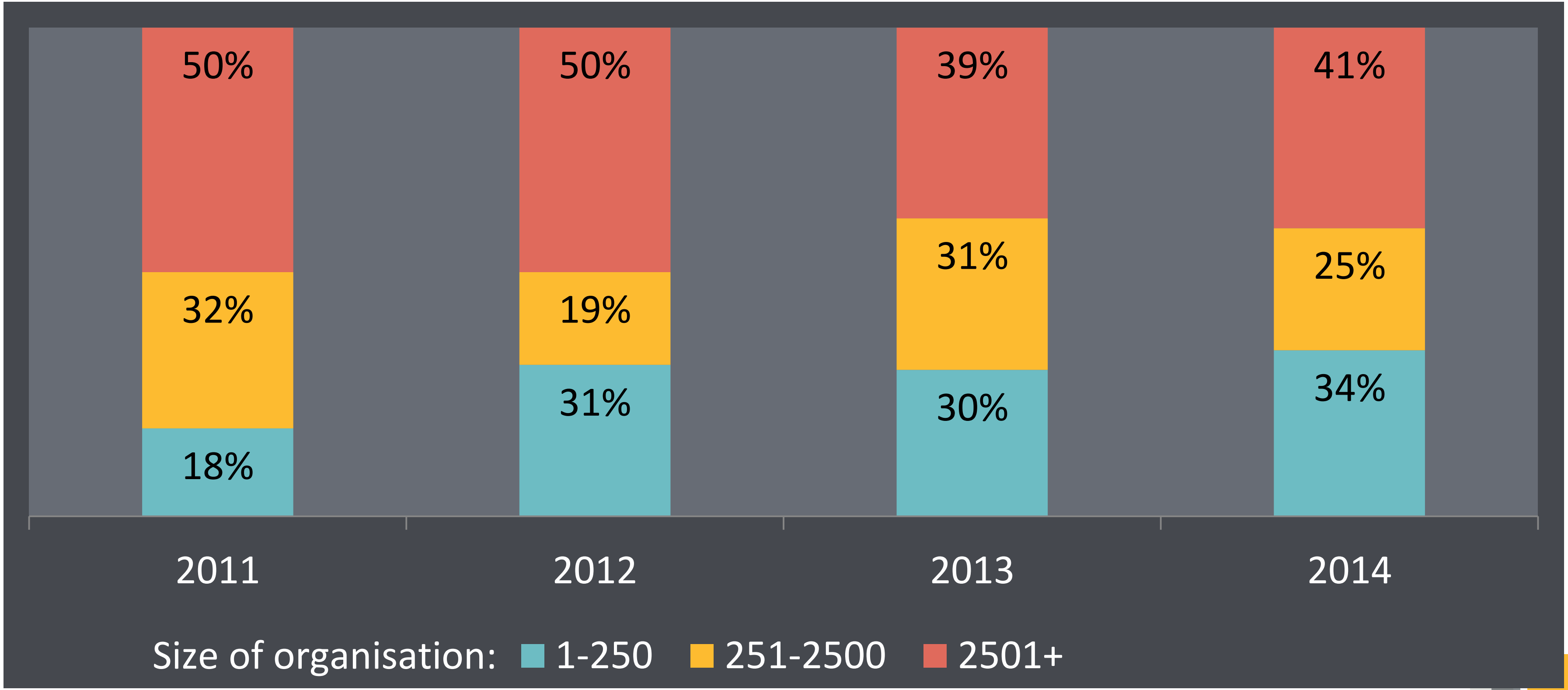
Captured information is sent back to attack team's home base for analysis and further exploitation fraud—or worse.



ATTACK METHODS

- = Social Engineering
- = Zero-Day Vulnerability
- = SQL Injection

What the likelihood is of being a target



What the results are of being a target

Technically

66%

Breaches undetected for 30 days
or more

243

Is the average number of days before detection

4

Months is the average time to remedy once detection has occurred

What the results are of being a target (continued)

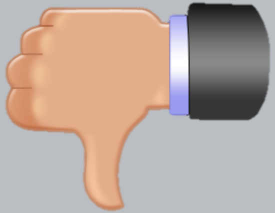
Commercially

Resource

Opex
Capex
Legal Fees
Time
Money

Theft

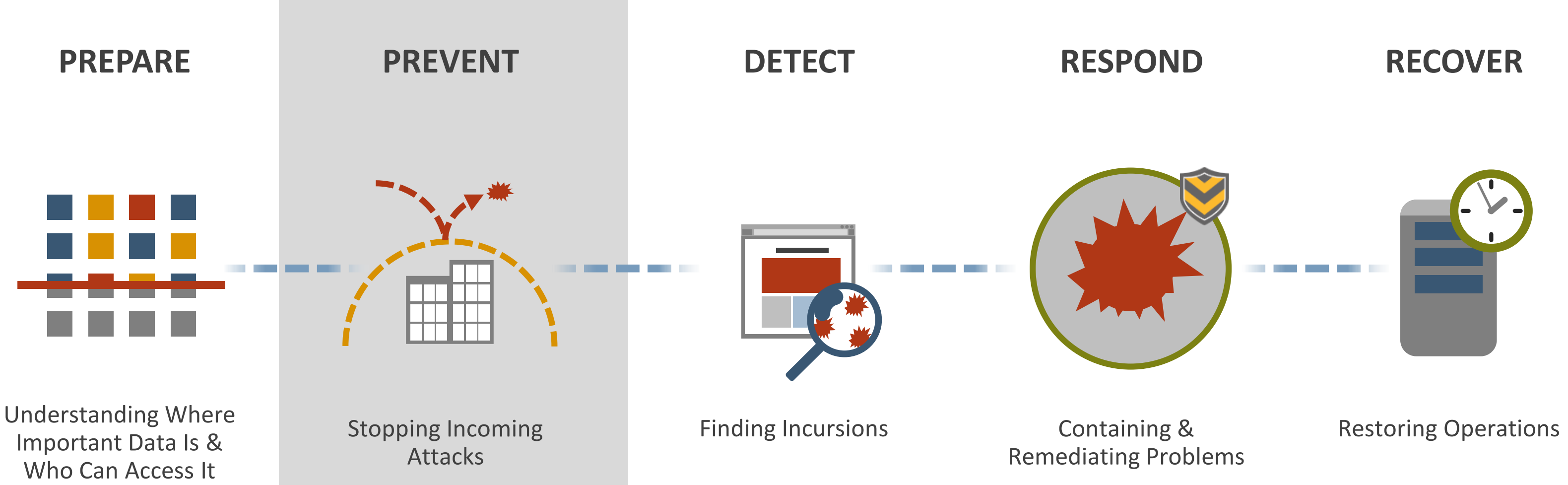
Intellectual Property
Money
Customer Data
Employee Data



Reputation

Brand Reputation can be affected if a breach is reported in the press

Even with the best prevention technologies, can you stop advanced persistent threats?



PREPARE

Understanding Where Important Data Is & Who Can Access It

PREVENT

Stopping Incoming Attacks

DETECT

Finding Incursions

RESPOND

Containing & Remediating Problems

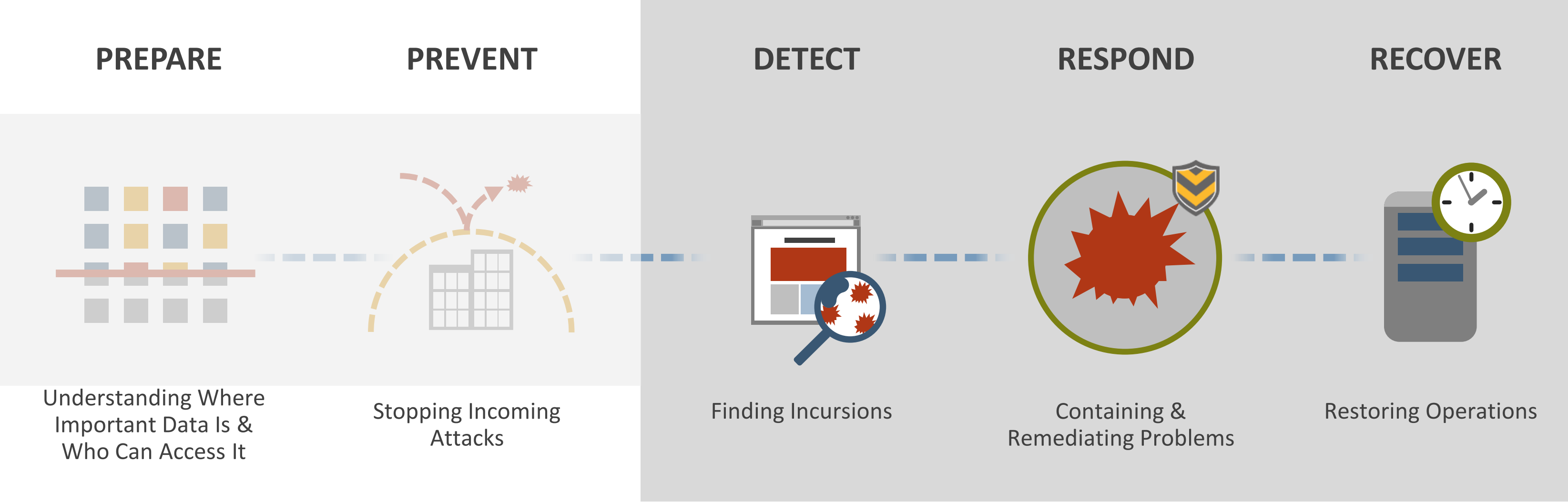
RECOVER

Restoring Operations

While prevention is still very important….

…you need to prepare to be breached.

If you are breached, how fast can you detect, respond and recover?



PREPARE

Understanding Where Important Data Is & Who Can Access It

PREVENT

Stopping Incoming Attacks

DETECT

Finding Incursions

RESPOND

Containing & Remediating Problems

RECOVER

Restoring Operations

ATP Solution:

Identify suspicious files

Symantec Advanced Threat Protection: Modules

ATP: Network

- Network visibility into all devices & all protocols
- Automated sandboxing, web exploits, command & control
- Deployed off a TAP as virtual or physical appliance

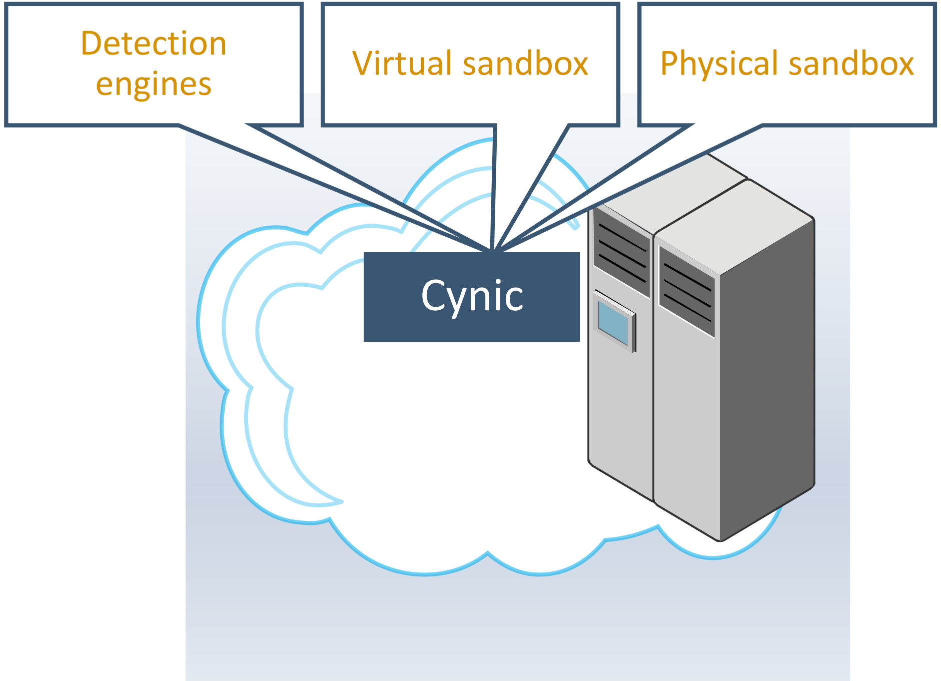
ATP: Endpoint

- Endpoint visibility (the foothold in most targeted attacks)
- Endpoint context, suspicious events, & remediation
- Requires SEP – no new agent – and deployed as a virtual or physical appliance

ATP: Email

- Email visibility (still the number one incursion vector)
- Email trends, targeted attack identification, sandboxing
- Cloud-based easy add on to Email Security.cloud

Symantec Advanced Threat Protection: Cynic



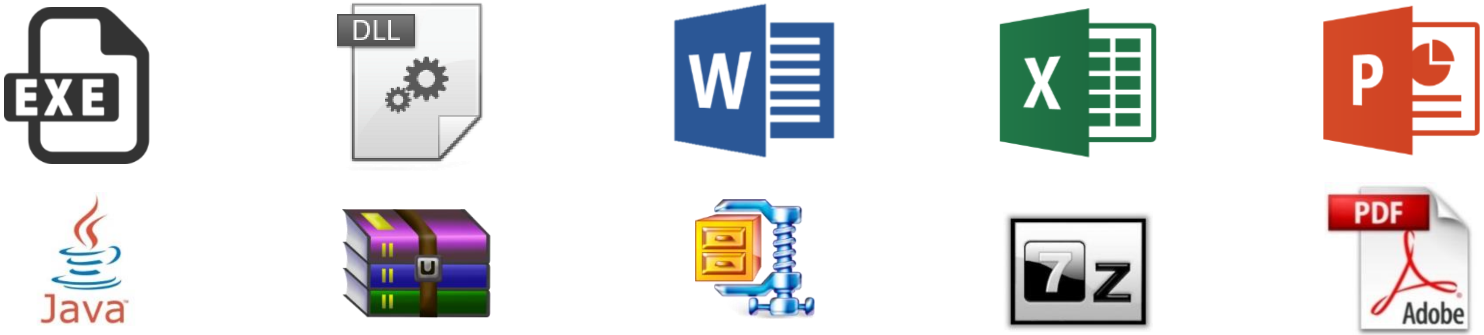
ATP: NETWORK

ATP: ENDPOINT

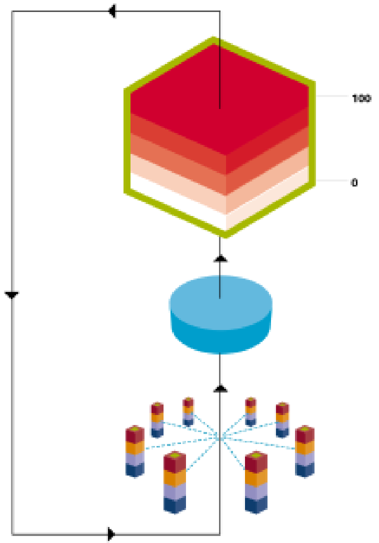
ATP: EMAIL

Cynic - File Types

- Windows binaries: EXE, DLL, SYS (drivers), OCX (ActiveX controls), SCR (Screen Savers)
- Office docs: Word, Excel, PowerPoint
- Java applets
- Compressed files (rar, zip, 7z)
- Adobe Acrobat



Skeptic:
pseudo equation for heuristic analysis



SKEPTIC

\+ Questionable source

\+ Suspect Attachment

\+ Suspicious code in attachment

(+ Evidence of obfuscation)

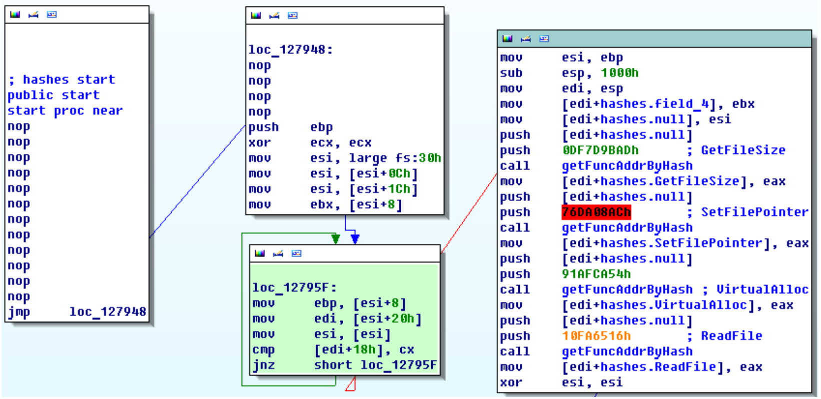
(+ Unexpected encryption) ______

Heuristically detected malcode

* Not all suspicious elements required for conviction

SONAR

- Dynamic analysis
- Does not make detections on application type, but on how a process behaves.
- If it behaves maliciously, regardless of its type, it will trigger a detection



```
; hashes start
public start
start proc near
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
jmp     loc_127948
```

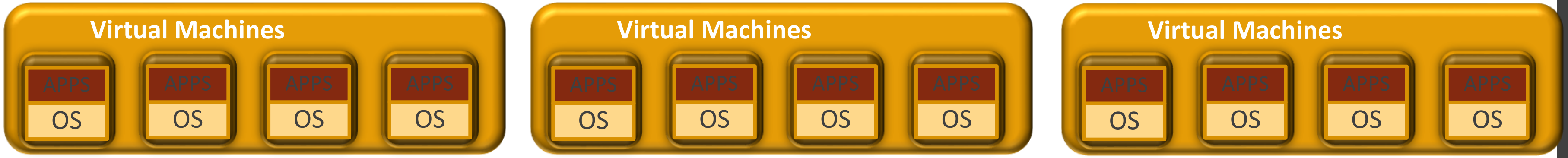
```
loc_127948:
nop
nop
nop
nop
push    ebp
xor     ecx, ecx
mov     esi, large fs:30h
mov     esi, [esi+0Ch]
mov     esi, [esi+1Ch]
mov     ebx, [esi+8]
```

```
loc_12795F:
mov     ebp, [esi+8]
mov     edi, [esi+20h]
mov     esi, [esi]
cmp     [edi+18h], cx
jnz     short loc_12795F
```

```
mov     esi, ebp
sub     esp, 1000h
mov     edi, esp
mov     [edi+hashes.field_4], ebx
mov     [edi+hashes.null], esi
push    [edi+hashes.null]
push    0DF7D9BADh      ; GetFileSize
call    getFuncAddrByHash
mov     [edi+hashes.GetFileSize], eax
push    [edi+hashes.null]
push    76DA08ACh       ; SetFilePointer
call    getFuncAddrByHash
mov     [edi+hashes.SetFilePointer], eax
push    [edi+hashes.null]
push    91AFCA54h
call    getFuncAddrByHash ; VirtualAlloc
mov     [edi+hashes.VirtualAlloc], eax
push    [edi+hashes.null]
push    10FA6516h       ; ReadFile
call    getFuncAddrByHash
mov     [edi+hashes.ReadFile], eax
xor     esi, esi
```

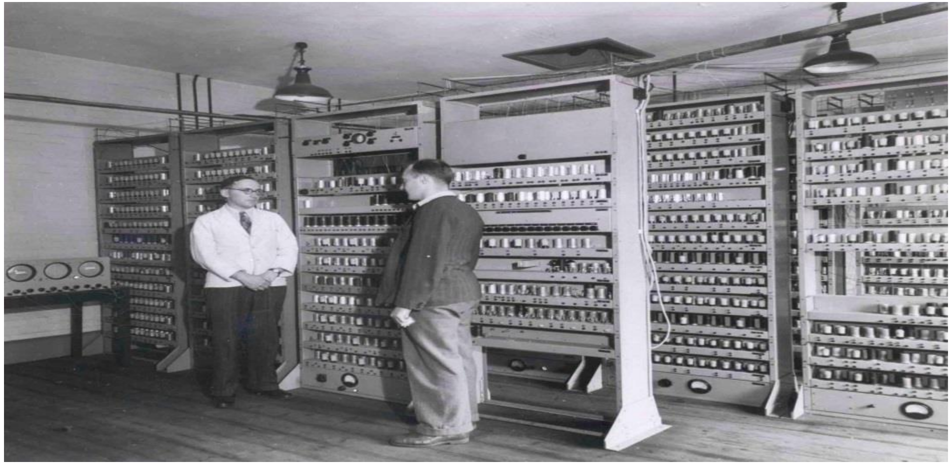
Virtual Execution

- VM execution with mimicked end user behavior
- Range of OS and apps
- VM execution range of OS and applications
- VM communication analysis



Physical Execution

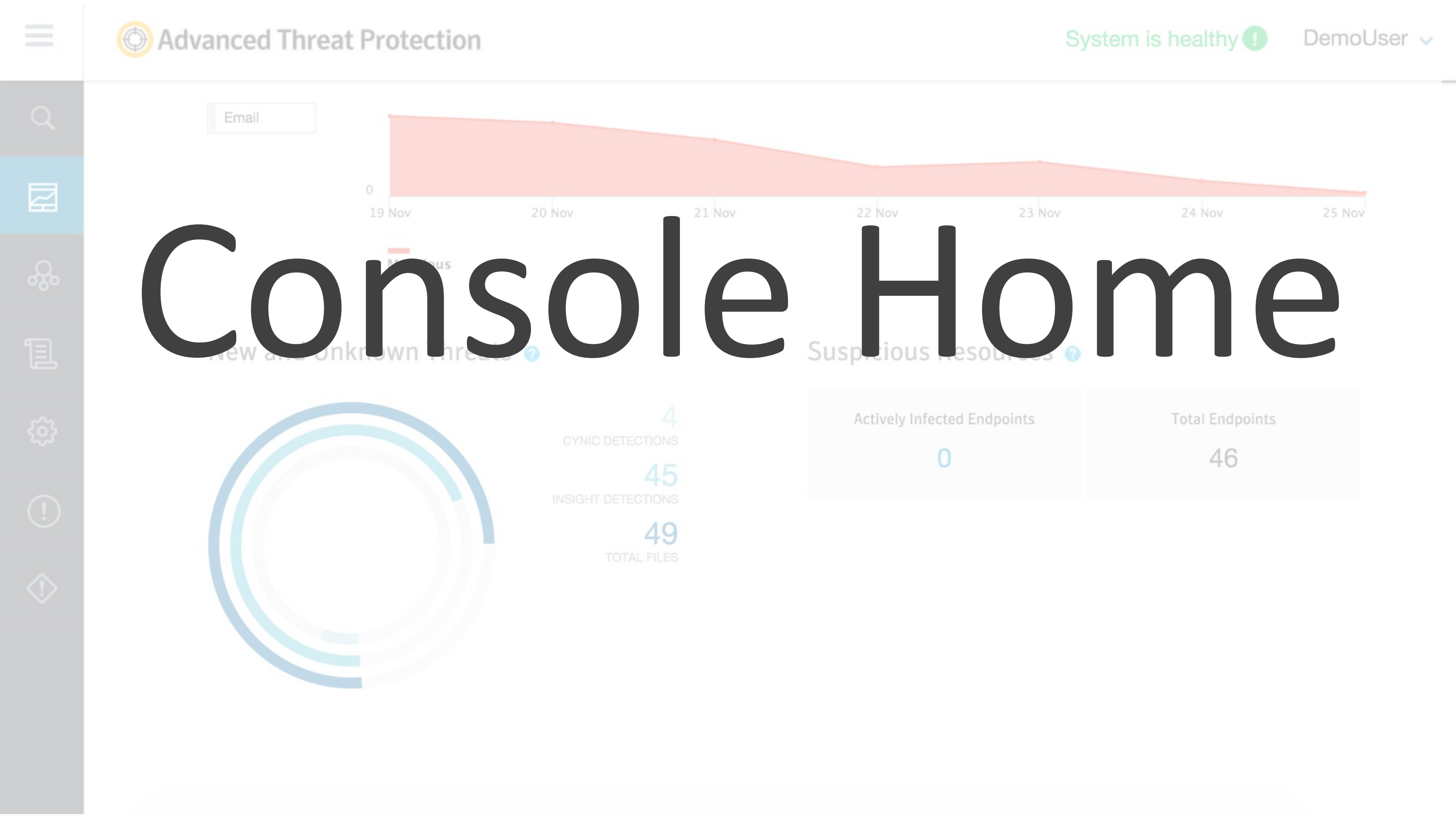
- Physical hardware
- Bare metal execution
  - No Virtualization

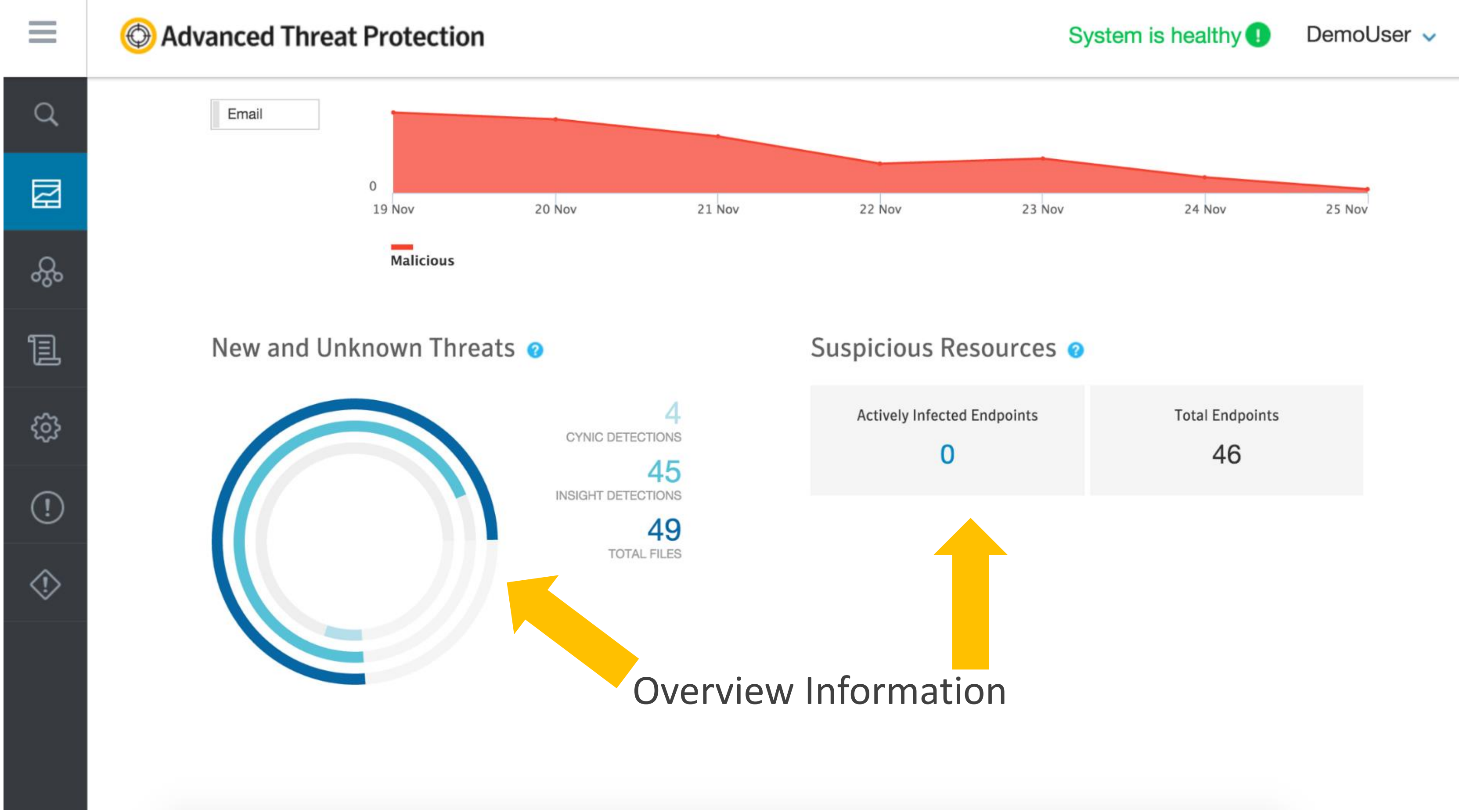


ATP Solution:

Search for Indicators of Compromise

Console Home





New and Unknown Threats

4 CYNIC DETECTIONS

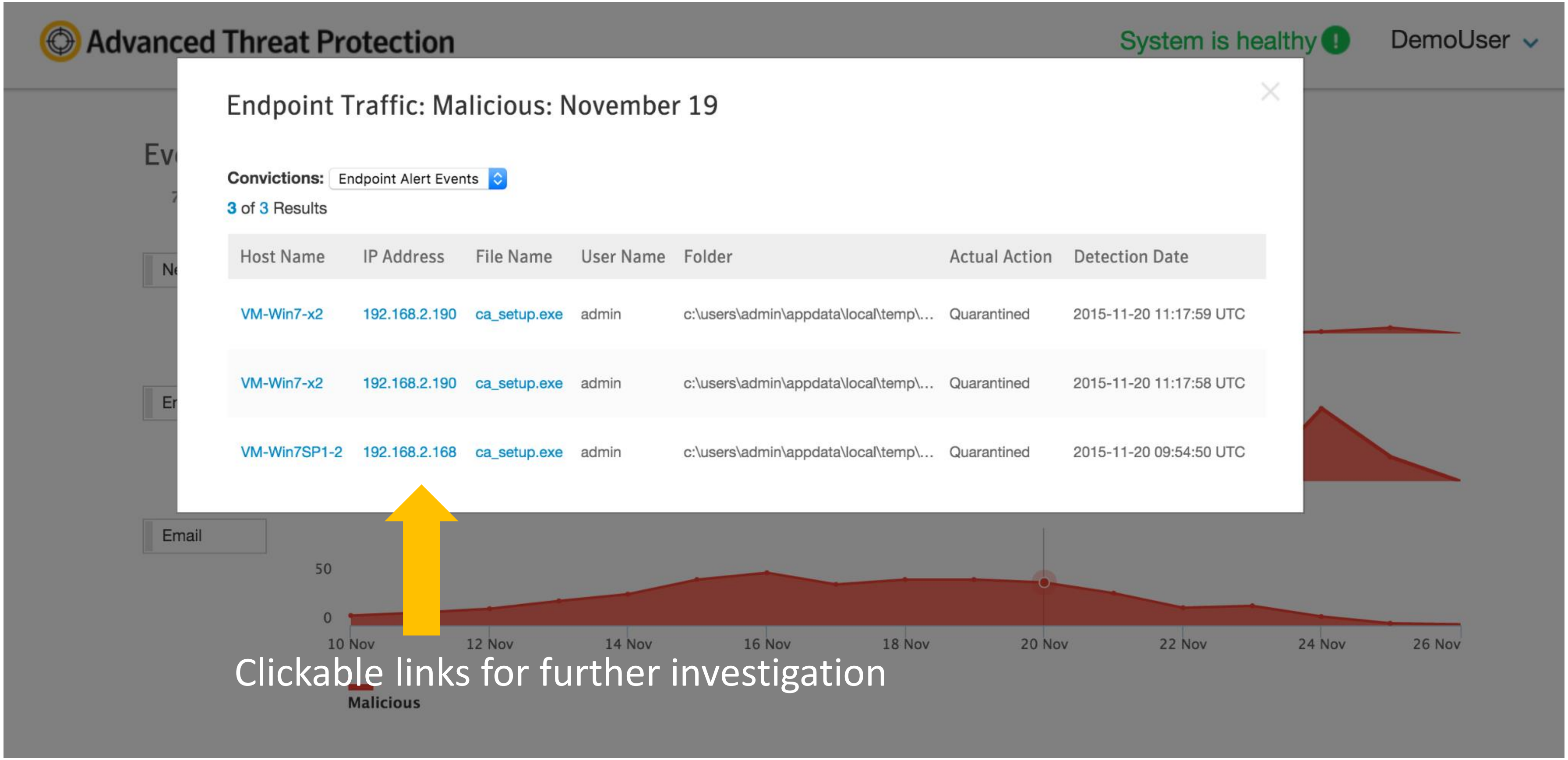
45 INSIGHT DETECTIONS

49 TOTAL FILES

Suspicious Resources

Actively Infected Endpoints	Total Endpoints
0	46

Overview Information



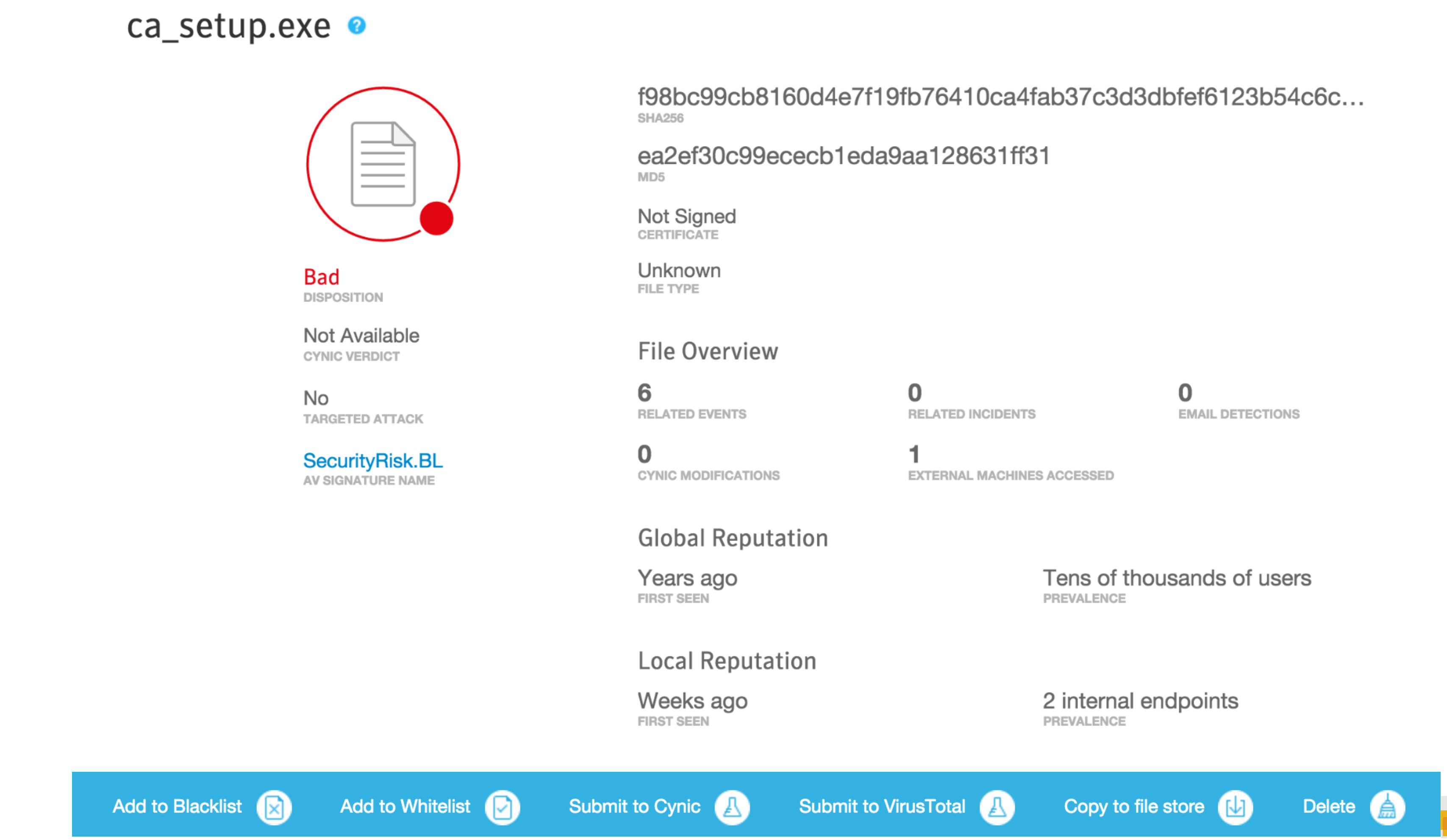
Endpoint Traffic: Malicious: November 19

Convictions: Endpoint Alert Events

3 of 3 Results

Host Name	IP Address	File Name	User Name	Folder	Actual Action	Detection Date
VM-Win7-x2	192.168.2.190	ca_setup.exe	admin	c:\users\admin\appdata\local\temp\...	Quarantined	2015-11-20 11:17:59 UTC
VM-Win7-x2	192.168.2.190	ca_setup.exe	admin	c:\users\admin\appdata\local\temp\...	Quarantined	2015-11-20 11:17:58 UTC
VM-Win7SP1-2	192.168.2.168	ca_setup.exe	admin	c:\users\admin\appdata\local\temp\...	Quarantined	2015-11-20 09:54:50 UTC

Clickable links for further investigation



ca_setup.exe

Bad
DISPOSITION

Not Available
CYNIC VERDICT

No
TARGETED ATTACK

SecurityRisk.BL
AV SIGNATURE NAME

f98bc99cb8160d4e7f19fb76410ca4fab37c3d3dbfef6123b54c6c...
SHA256

ea2ef30c99ececb1eda9aa128631ff31
MD5

Not Signed
CERTIFICATE

Unknown
FILE TYPE

File Overview

6
RELATED EVENTS

0
RELATED INCIDENTS

0
EMAIL DETECTIONS

0
CYNIC MODIFICATIONS

1
EXTERNAL MACHINES ACCESSED

Global Reputation

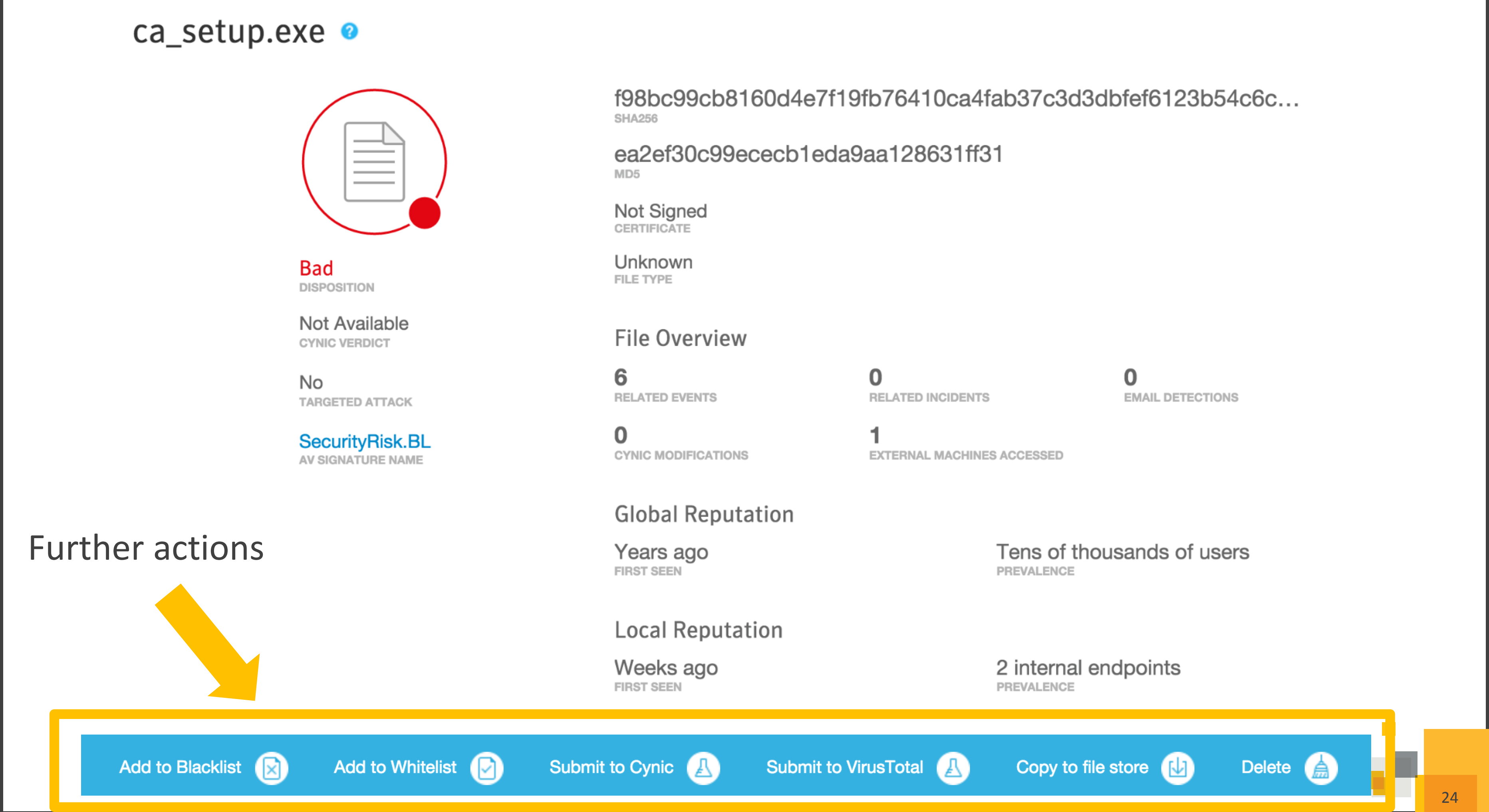
Years ago
FIRST SEEN

Tens of thousands of users
PREVALENCE

Local Reputation

Weeks ago
FIRST SEEN

2 internal endpoints
PREVALENCE



ca_setup.exe

Bad
DISPOSITION

Not Available
CYNIC VERDICT

No
TARGETED ATTACK

SecurityRisk.BL
AV SIGNATURE NAME

f98bc99cb8160d4e7f19fb76410ca4fab37c3d3dbfef6123b54c6c...
SHA256

ea2ef30c99ececb1eda9aa128631ff31
MD5

Not Signed
CERTIFICATE

Unknown
FILE TYPE

File Overview

6 RELATED EVENTS	0 RELATED INCIDENTS	0 EMAIL DETECTIONS
0 CYNIC MODIFICATIONS	1 EXTERNAL MACHINES ACCESSED	

Global Reputation

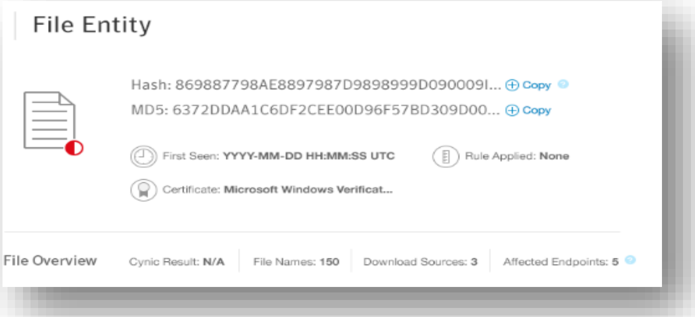
Years ago FIRST SEEN	Tens of thousands of users PREVALENCE

Local Reputation

Weeks ago FIRST SEEN	2 internal endpoints PREVALENCE

Further actions

Entity Point Pages



File Entity

Hash: 869887798AE8897987D9898999D090009I... ⊕ Copy

MD5: 6372DDAA1C6DF2CEE00D96F57BD309D00... ⊕ Copy

First Seen: **YYYY-MM-DD HH:MM:SS UTC**

Rule Applied: **None**

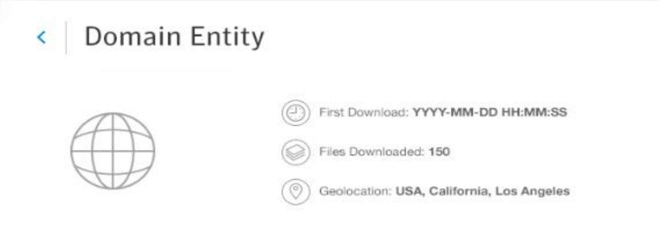
Certificate: **Microsoft Windows Verificat...**

File Overview

Cynic Result: **N/A** | File Names: **150** | Download Sources: **3** | Affected Endpoints: **5**

File Entity page
Related Incidents
Related Events
Seen on Endpoints
Files downloaded Origins
Files named associated with Hash
Cynic Results

Domain Entity Page
Related Incidents
Files downloaded
Endpoints that communicated
IP’s Associated with Domain

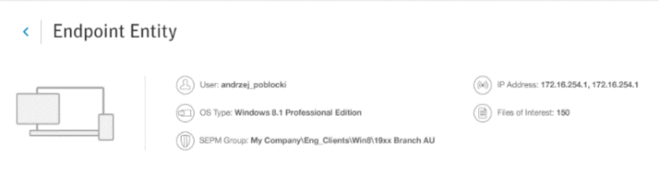


Domain Entity

First Download: **YYYY-MM-DD HH:MM:SS**

Files Downloaded: **150**

Geolocation: **USA, California, Los Angeles**



Endpoint Entity

User: **andrzej_poblocki**

OS Type: **Windows 8.1 Professional Edition**

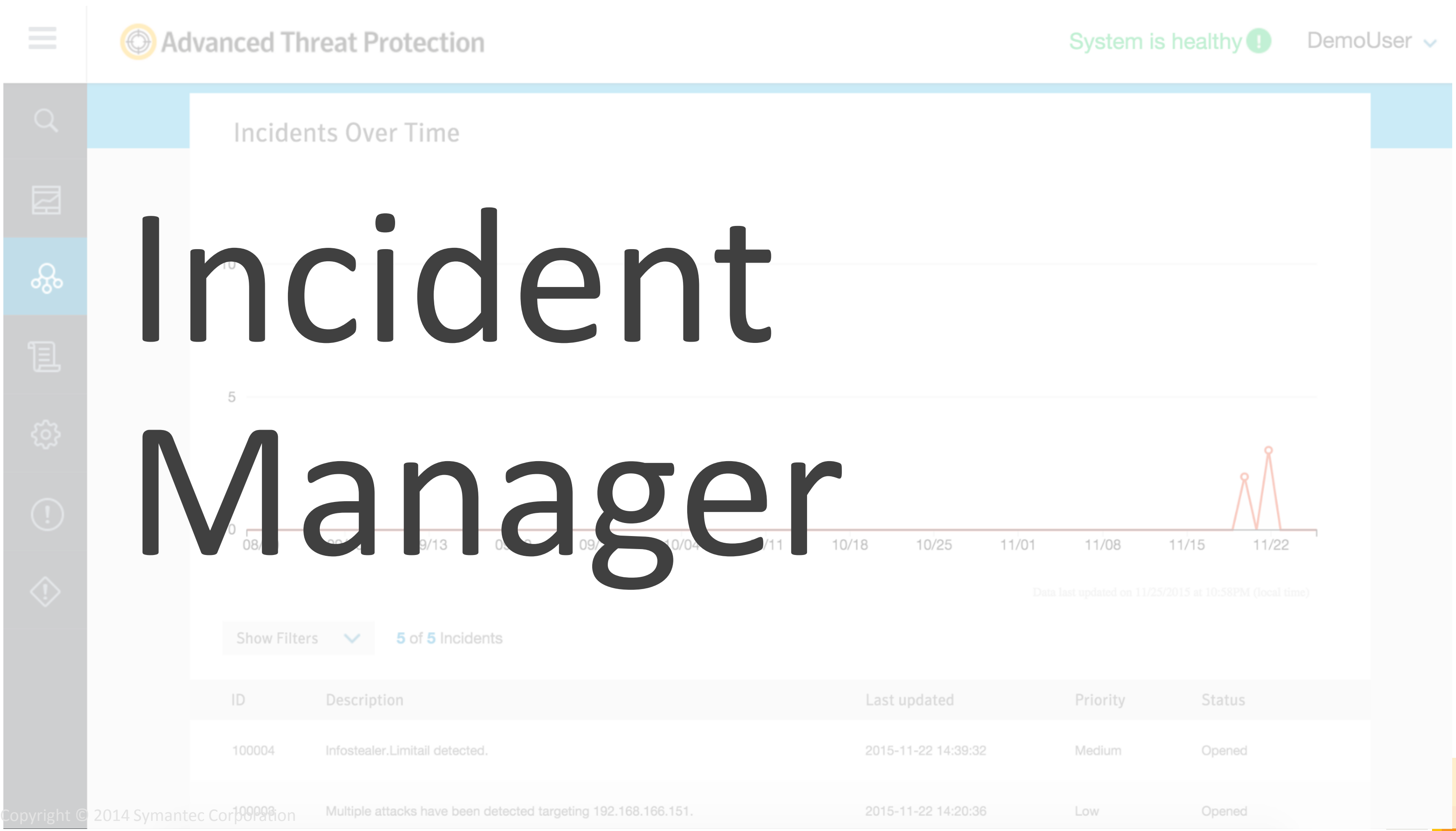
SEPM Group: **My Company\Eng_Clients\Win8\19xx Branch AU**

IP Address: **172.16.254.1, 172.16.254.1**

Files of Interest: **150**

Endpoint Entity Page
Related Incidents
Related Events
Malicious Files
Malicious Connections

Incident Manager



Advanced Threat Protection

System is healthy

DemoUser

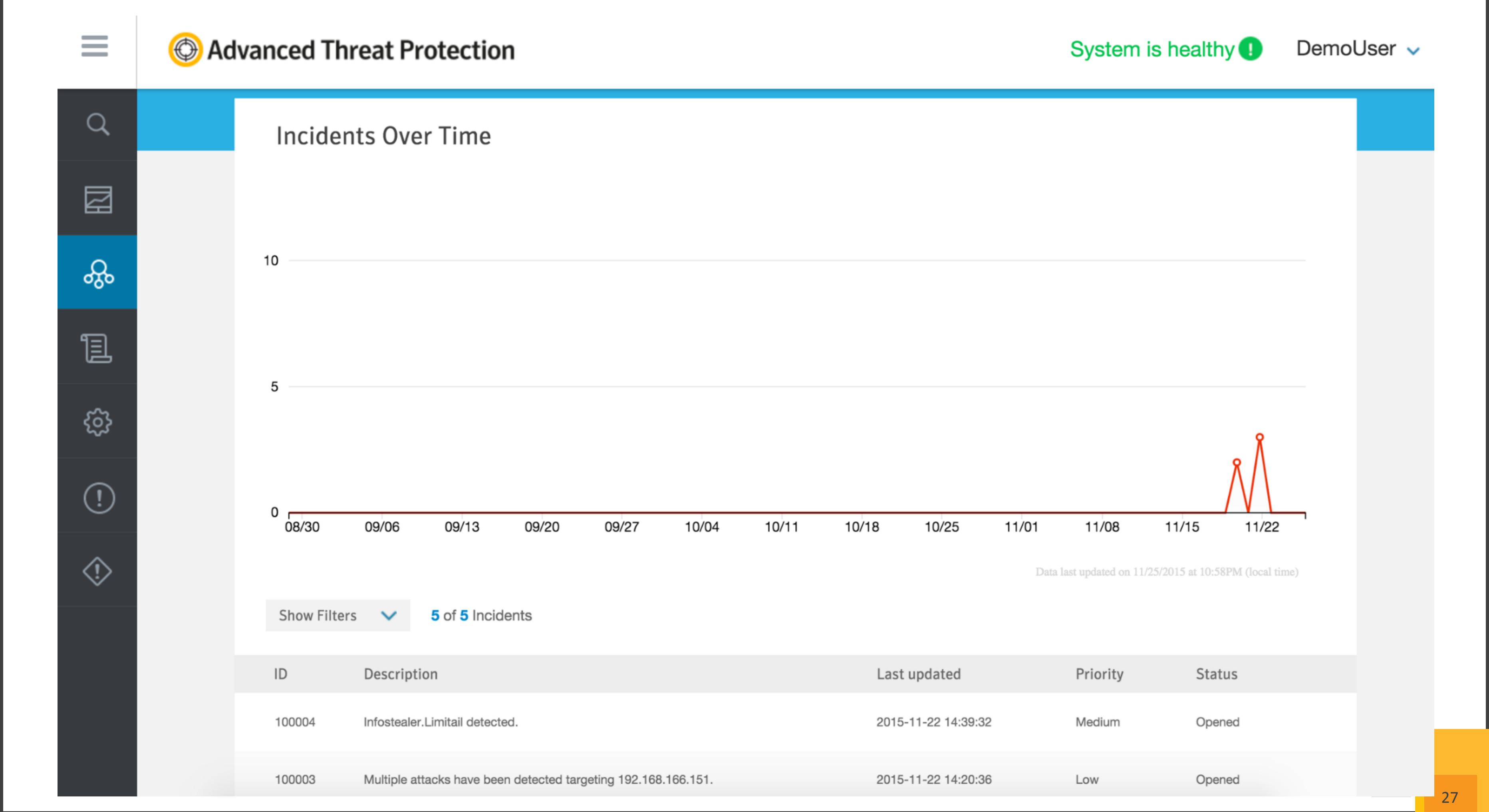
Incidents Over Time

Data last updated on 11/25/2015 at 10:58PM (local time)

Show Filters

5 of 5 Incidents

ID	Description	Last updated	Priority	Status
100004	Infostealer.Limitail detected.	2015-11-22 14:39:32	Medium	Opened
100003	Multiple attacks have been detected targeting 192.168.166.151.	2015-11-22 14:20:36	Low	Opened



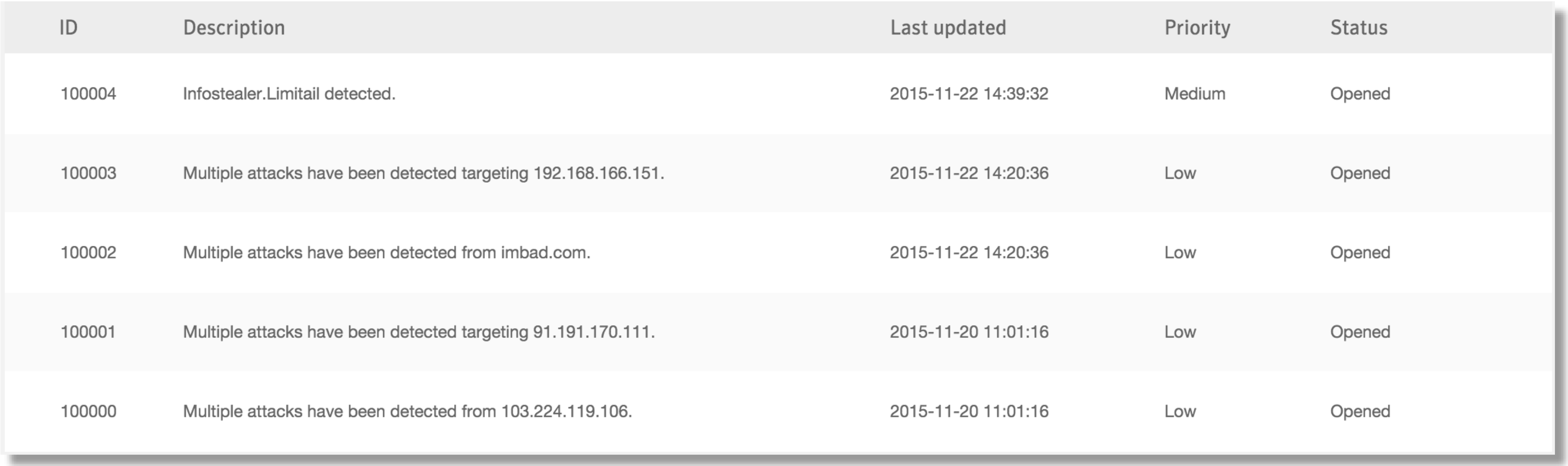
Incidents Over Time

Data last updated on 11/25/2015 at 10:58PM (local time)

5 of 5 Incidents

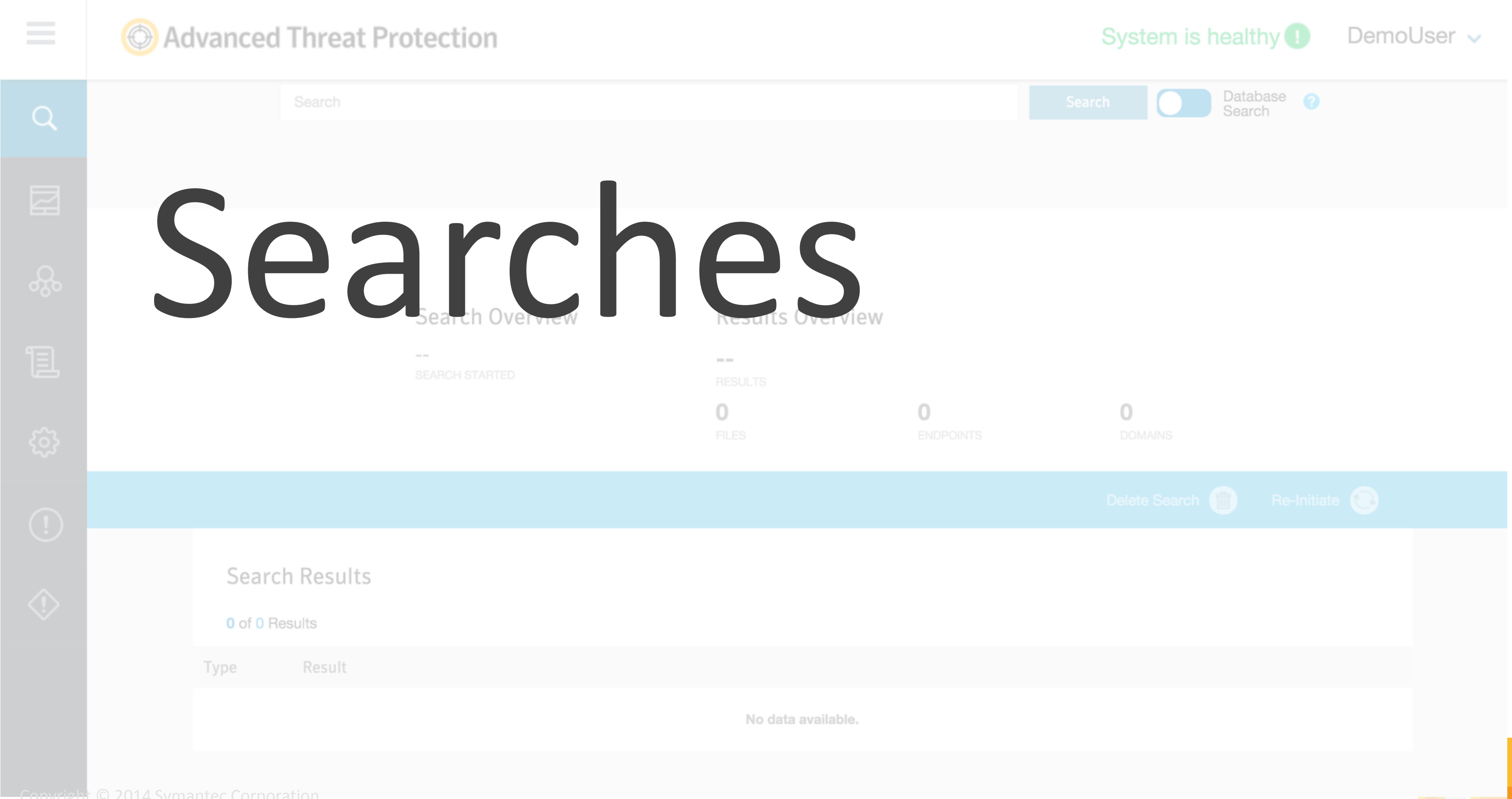
ID	Description	Last updated	Priority	Status
100004	Infostealer.Limitail detected.	2015-11-22 14:39:32	Medium	Opened
100003	Multiple attacks have been detected targeting 192.168.166.151.	2015-11-22 14:20:36	Low	Opened

Incident Tracking



ID	Description	Last updated	Priority	Status
100004	Infostealer.Limitail detected.	2015-11-22 14:39:32	Medium	Opened
100003	Multiple attacks have been detected targeting 192.168.166.151.	2015-11-22 14:20:36	Low	Opened
100002	Multiple attacks have been detected from imbad.com.	2015-11-22 14:20:36	Low	Opened
100001	Multiple attacks have been detected targeting 91.191.170.111.	2015-11-20 11:01:16	Low	Opened
100000	Multiple attacks have been detected from 103.224.119.106.	2015-11-20 11:01:16	Low	Opened

Searches



0 of 0 Results

No data available.

Types of Searches

- Inline (Datastore)
  - Searches local data store for artifacts
  - Seconds to return results
  - Artifacts are generated from endpoint and network sensor events
  - Examples (file, hash, domain name, hostname, username, IP)
  - PE File types (exe,dll,com,scr,msi,drv,sys,ocx,cpl)

- Endpoint Interrogation
  - Searches endpoint for artifacts
  - Results can be delayed based on factors
  - Examples (file, hash, registry)
  - All file types (PE, Non PE)

Searches

Files using

- File name
- File Hash (SHA256, MD5)

Endpoints using

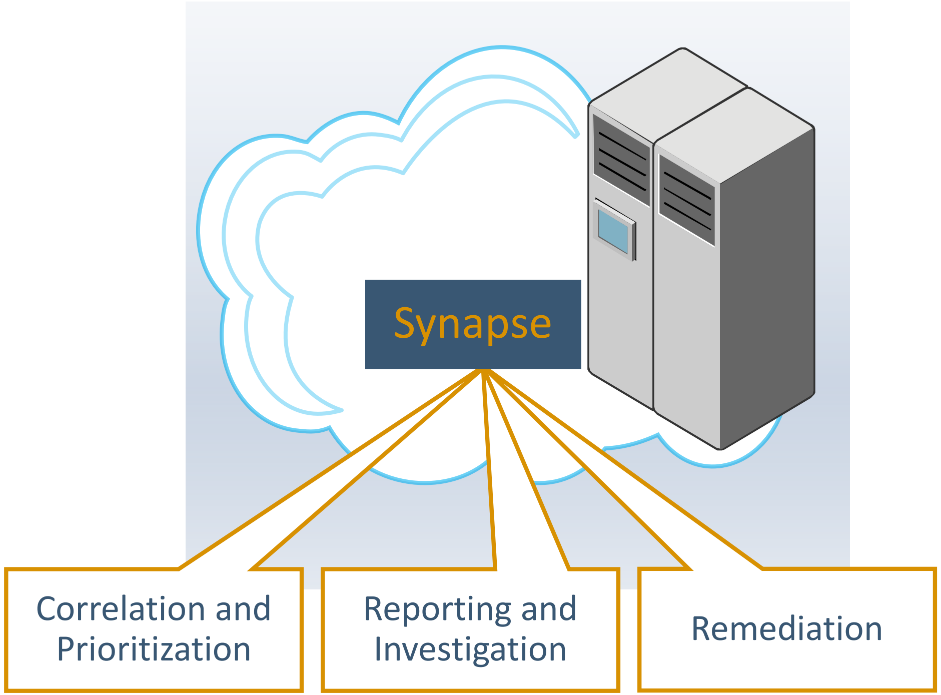
- Host name
- IP Address (v4)
- Logon user

External domains using

- Domain name
- Domain URL
- Domain IP address

- We check if the provided value is present anywhere in the above fields i.e. file name, MD5, sha2, hostname etc. i.e. contains match.

Symantec Advanced Threat Protection: Synapse



Synapse

Correlation and Prioritization

Reporting and Investigation

Remediation

ATP: EMAIL

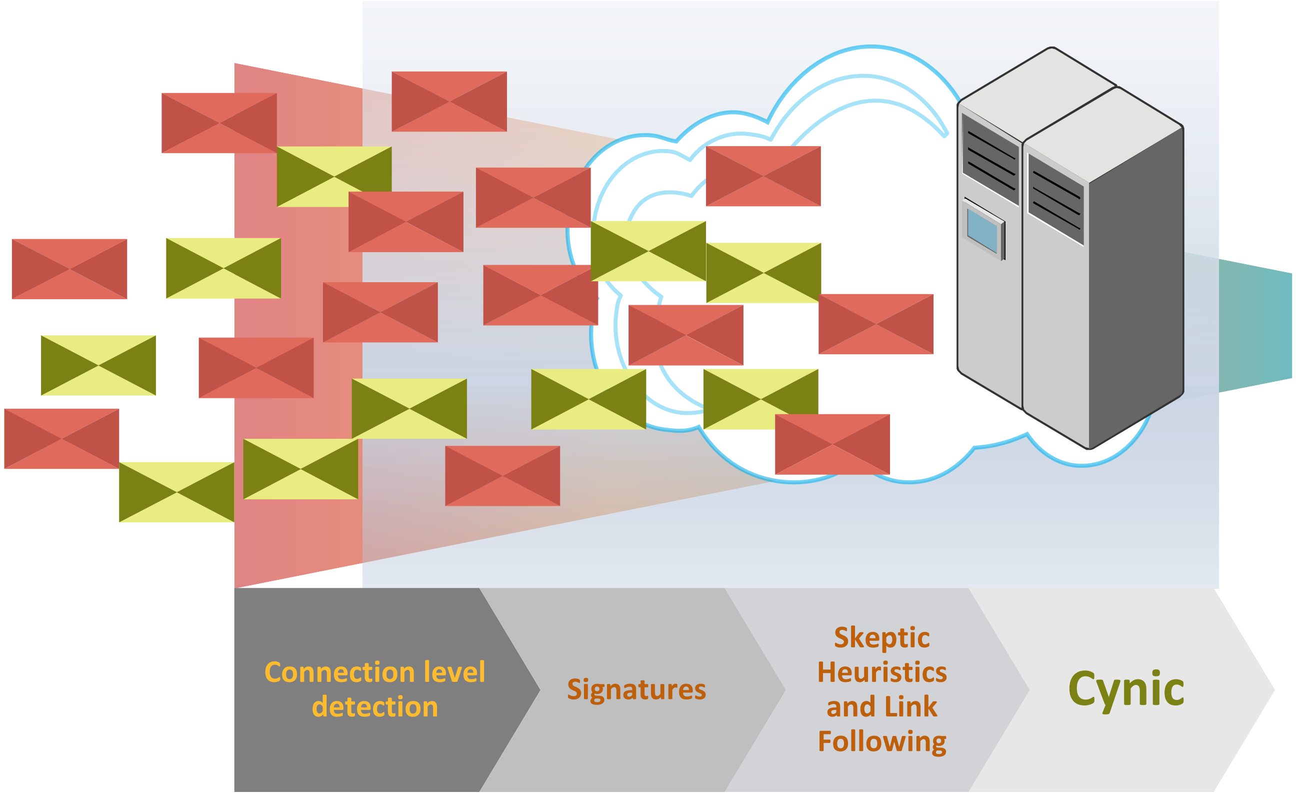
ATP: NETWORK

ATP: ENDPOINT

ATP Solution:

Block, isolate and remove the advanced persistent threats

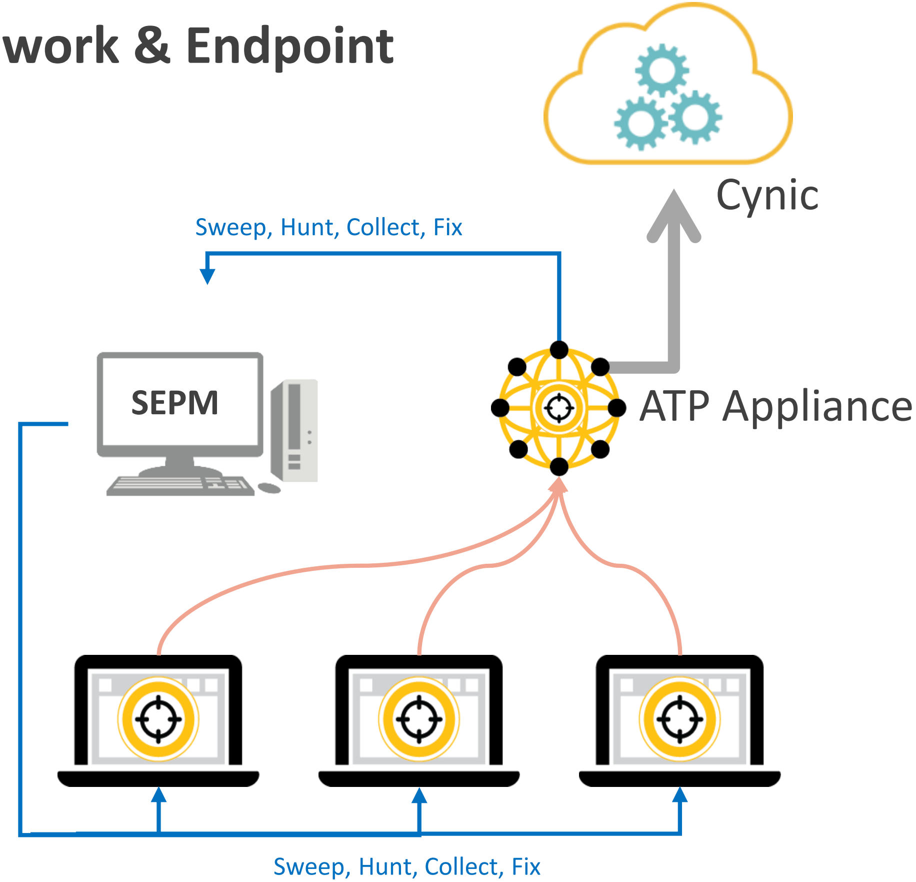
First line of defense: ATP: Email


Connection level detection
Signatures
Skeptic Heuristics and Link Following
Cynic

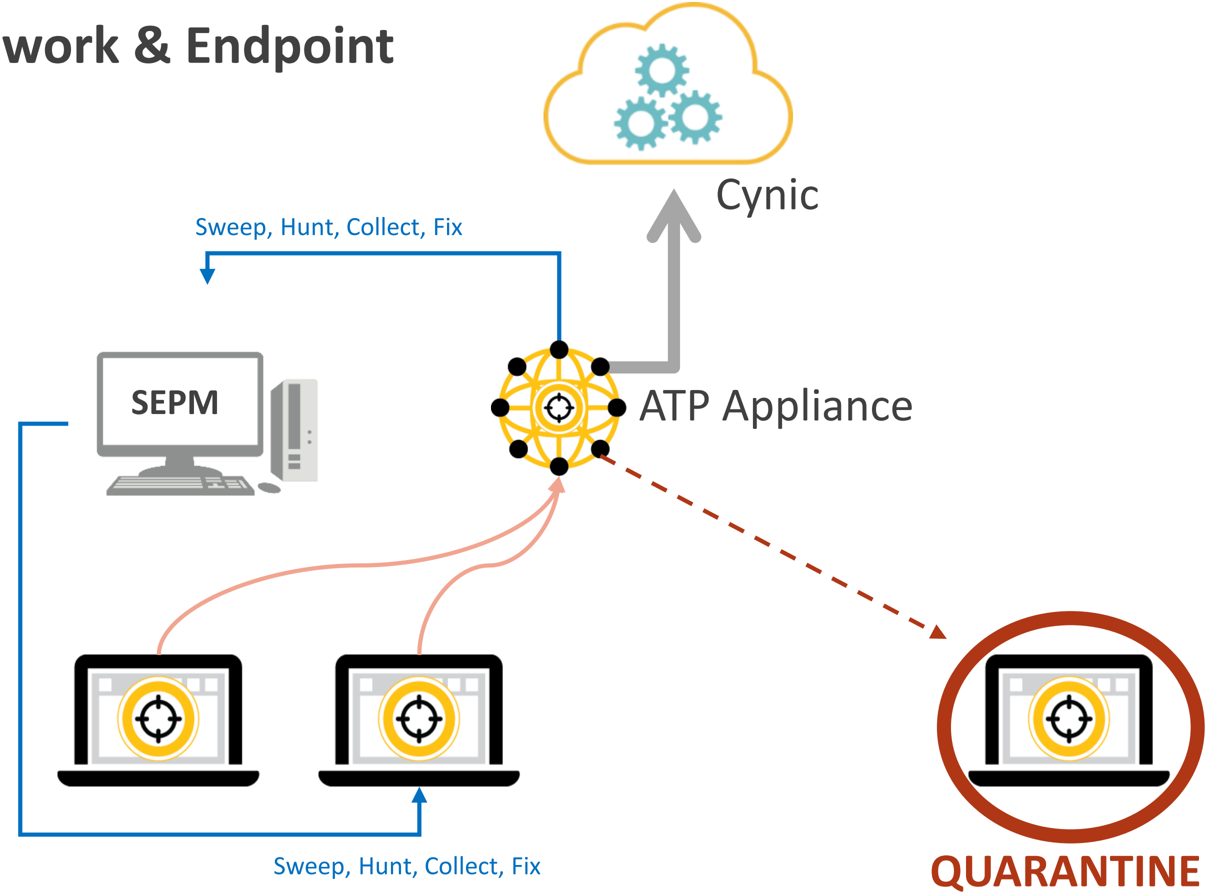
Anything without a verdict will be scanned by Cynic for a customer configured duration (≤ 20 mins)

Malicious mail is quarantined and logged as soon as a detection method flags it

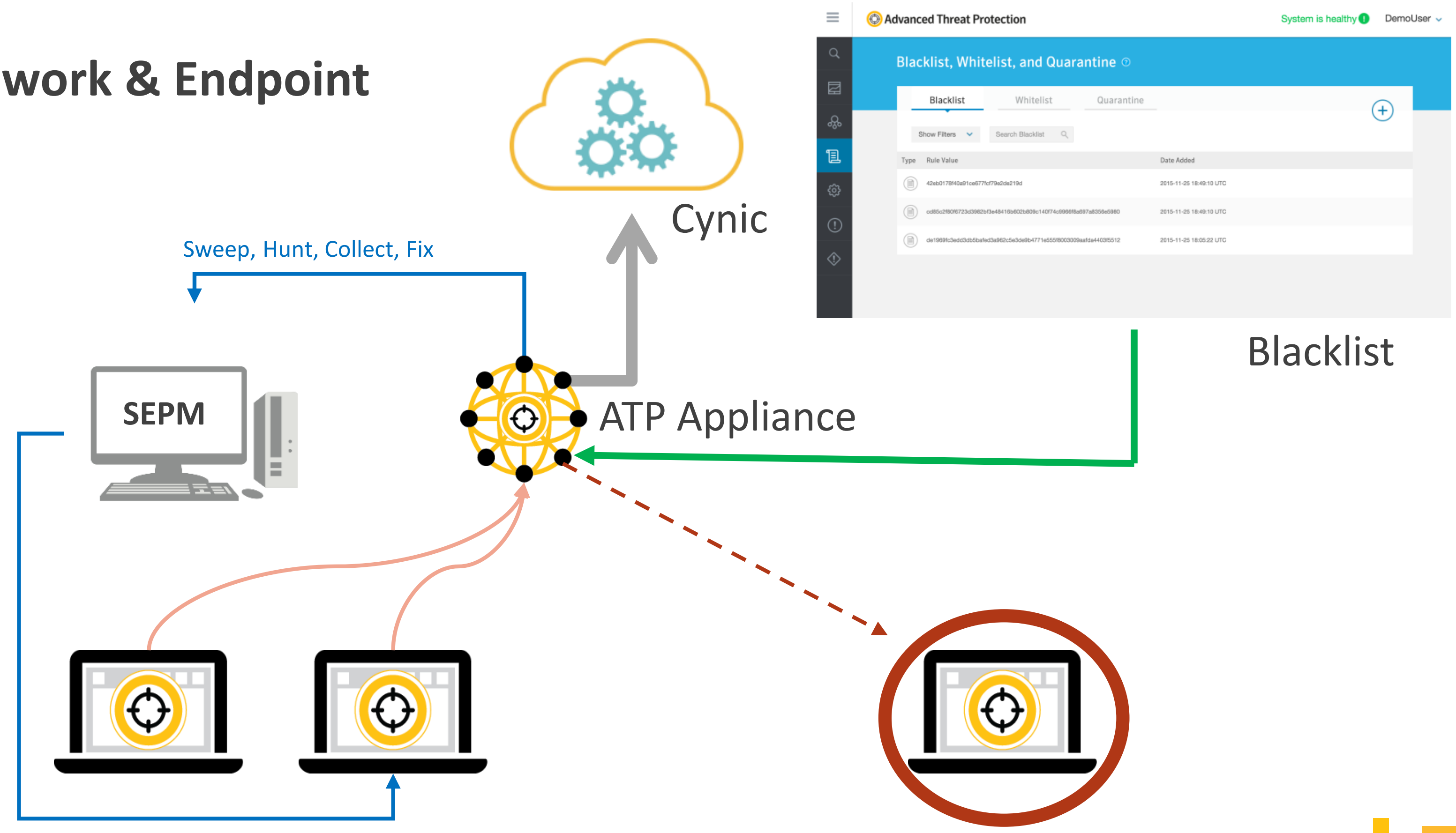
ATP: Network & Endpoint



ATP: Network & Endpoint



ATP: Network & Endpoint



Advanced Threat Protection   System is healthy   DemoUser

Blacklist, Whitelist, and Quarantine

Blacklist | Whitelist | Quarantine

Show Filters   Search Blacklist

Type	Rule Value	Date Added
	42eb0178f40a91ce677fcf79e2de219d	2015-11-25 18:49:10 UTC
	cd85c2f80f6723d3982bf3e48416b602b809c140f74c9966f8a697a8356e5980	2015-11-25 18:49:10 UTC
	de1969fc3edd3db5bafed3a962c5e3de9b4771e5551800309aafda4403f5512	2015-11-25 18:05:22 UTC

Blacklist / Whitelist Valid Entries

Domain

www.google.com
.gov.ca

URL

gov.ca/dmv
http://stanford.edu/news
http://gość.pl/a

IP/ IP Subnet

fe80::250:56ff:fe99:3903
10.10.10.10/24
10.10.10.10/255.255.255.0

SHA256 Hash

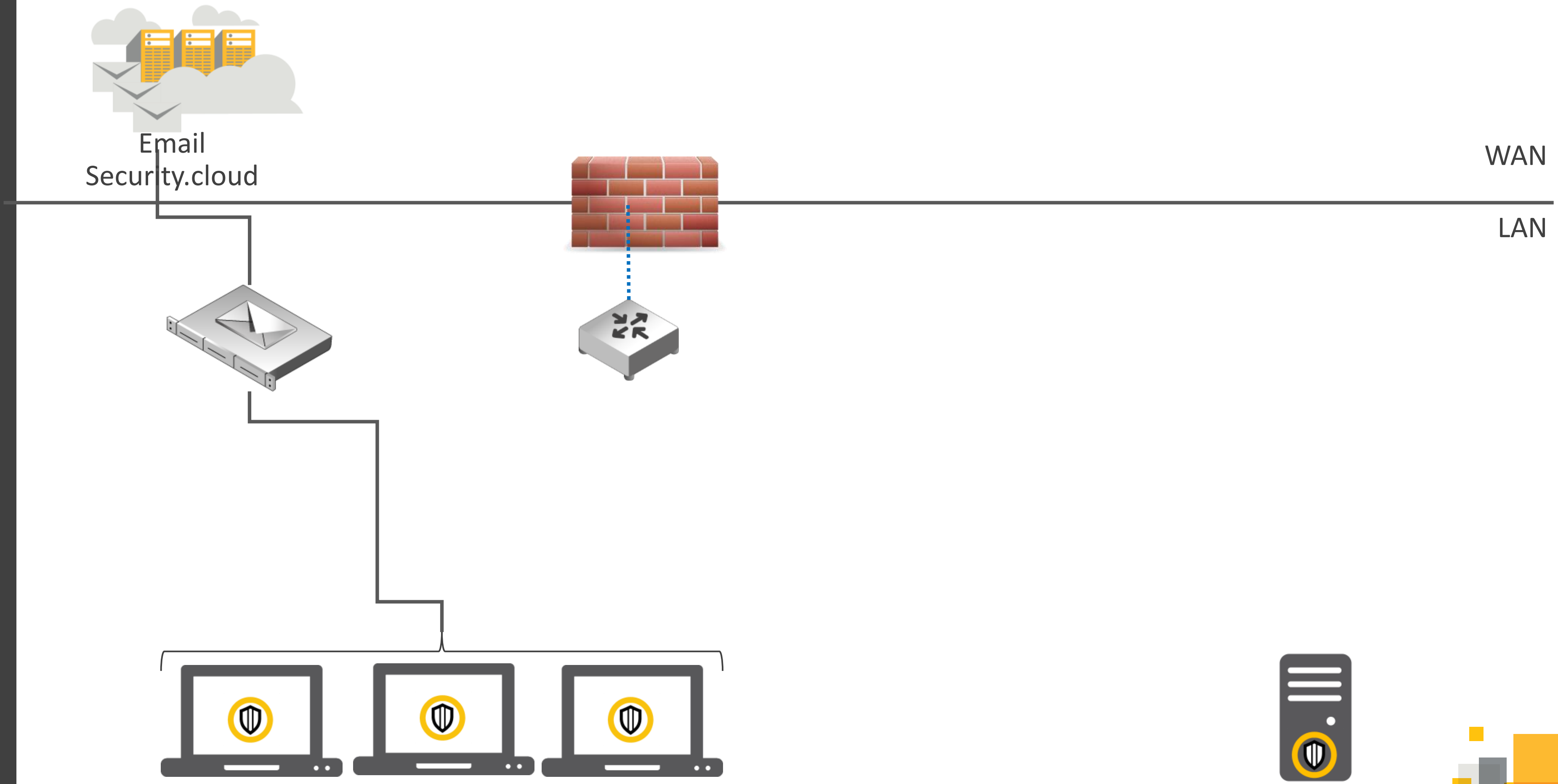
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b854

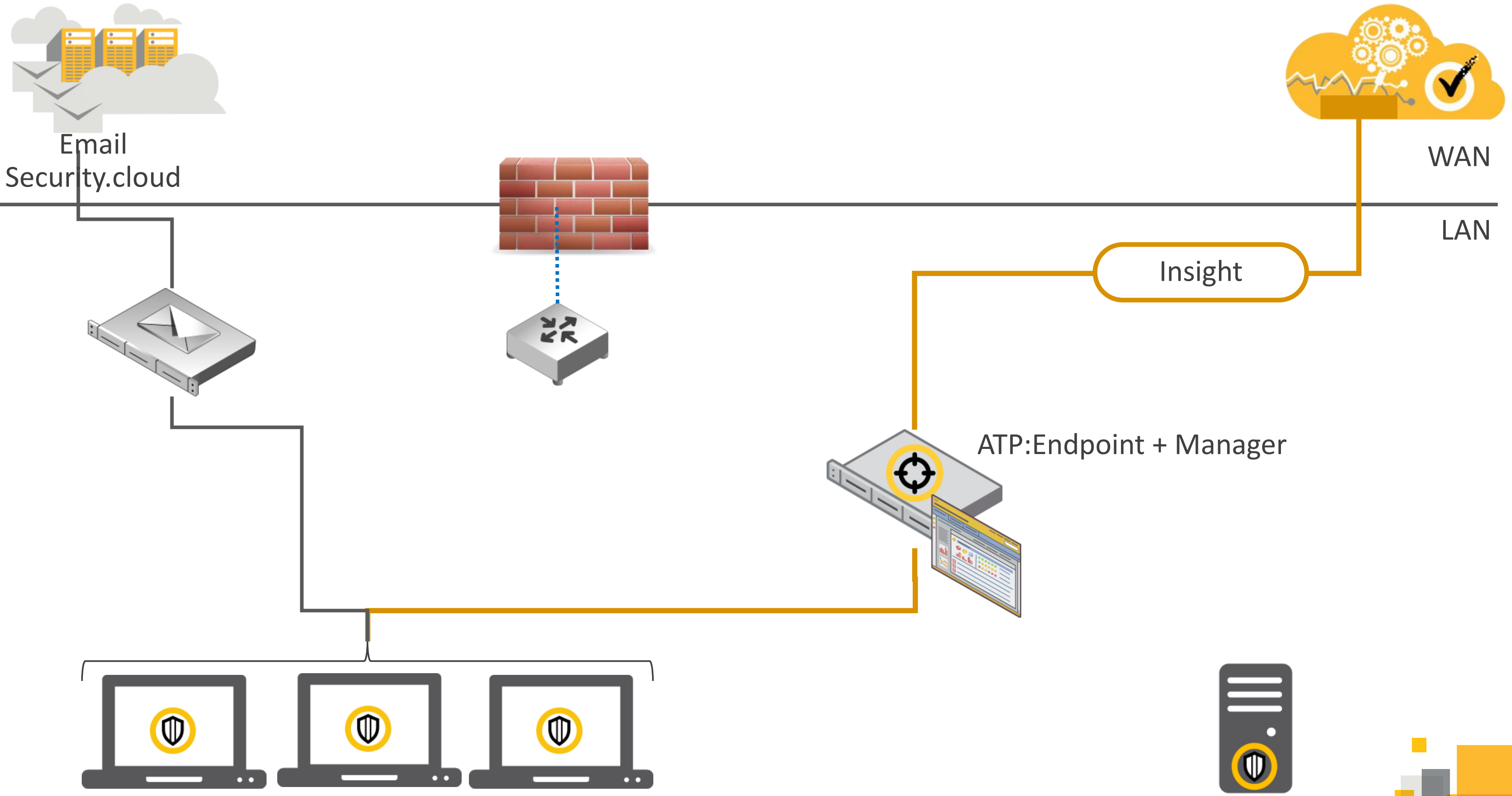
MD5 hash

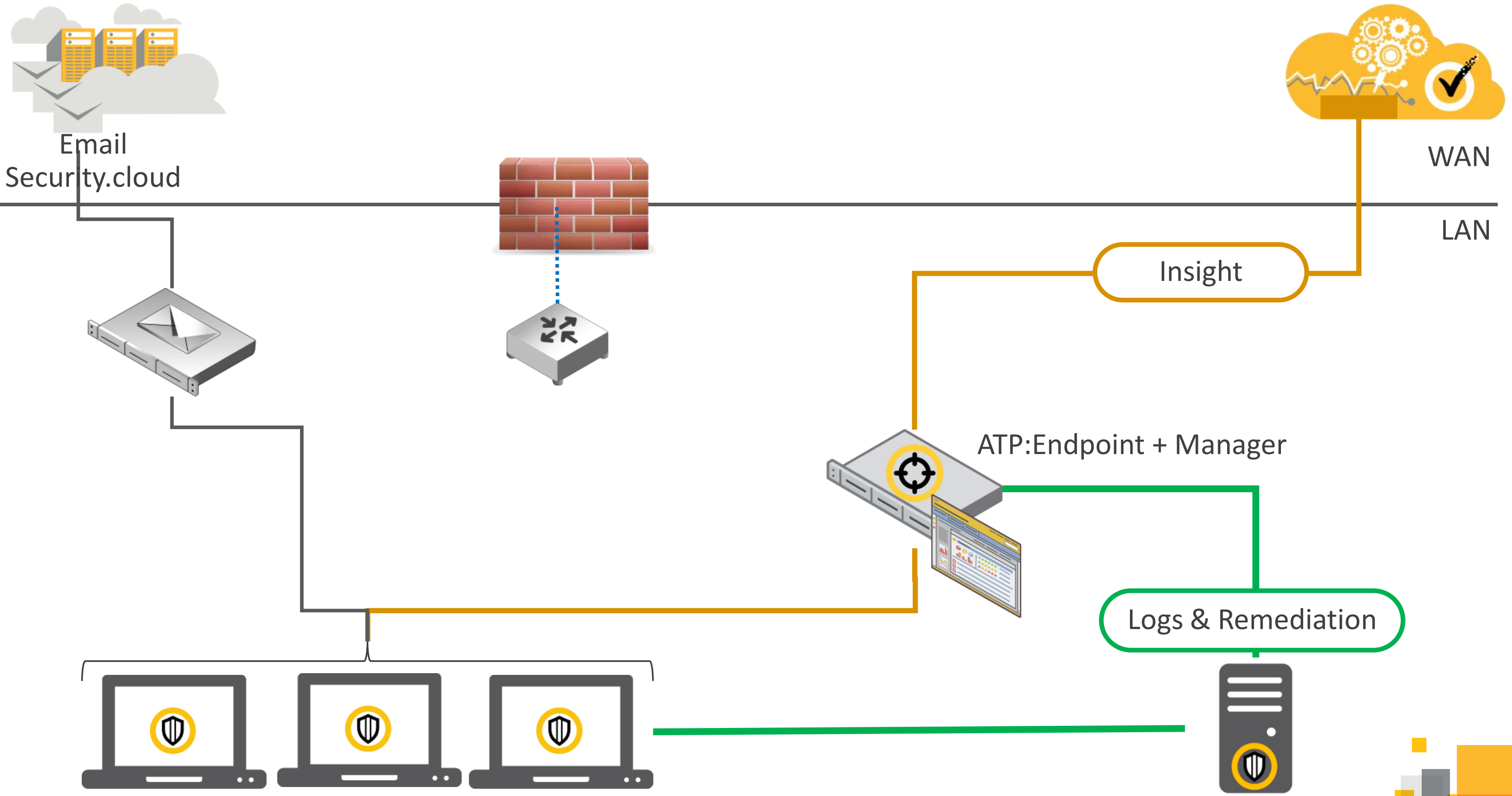
fe58cec593d7cdf2e0e9d13dfe1020b8

ATP Solution:

Minimize environmental changes


Email
Security.cloud
WAN
LAN


Email
Security.cloud
WAN
LAN
Insight
ATP:Endpoint + Manager



Email Security.cloud

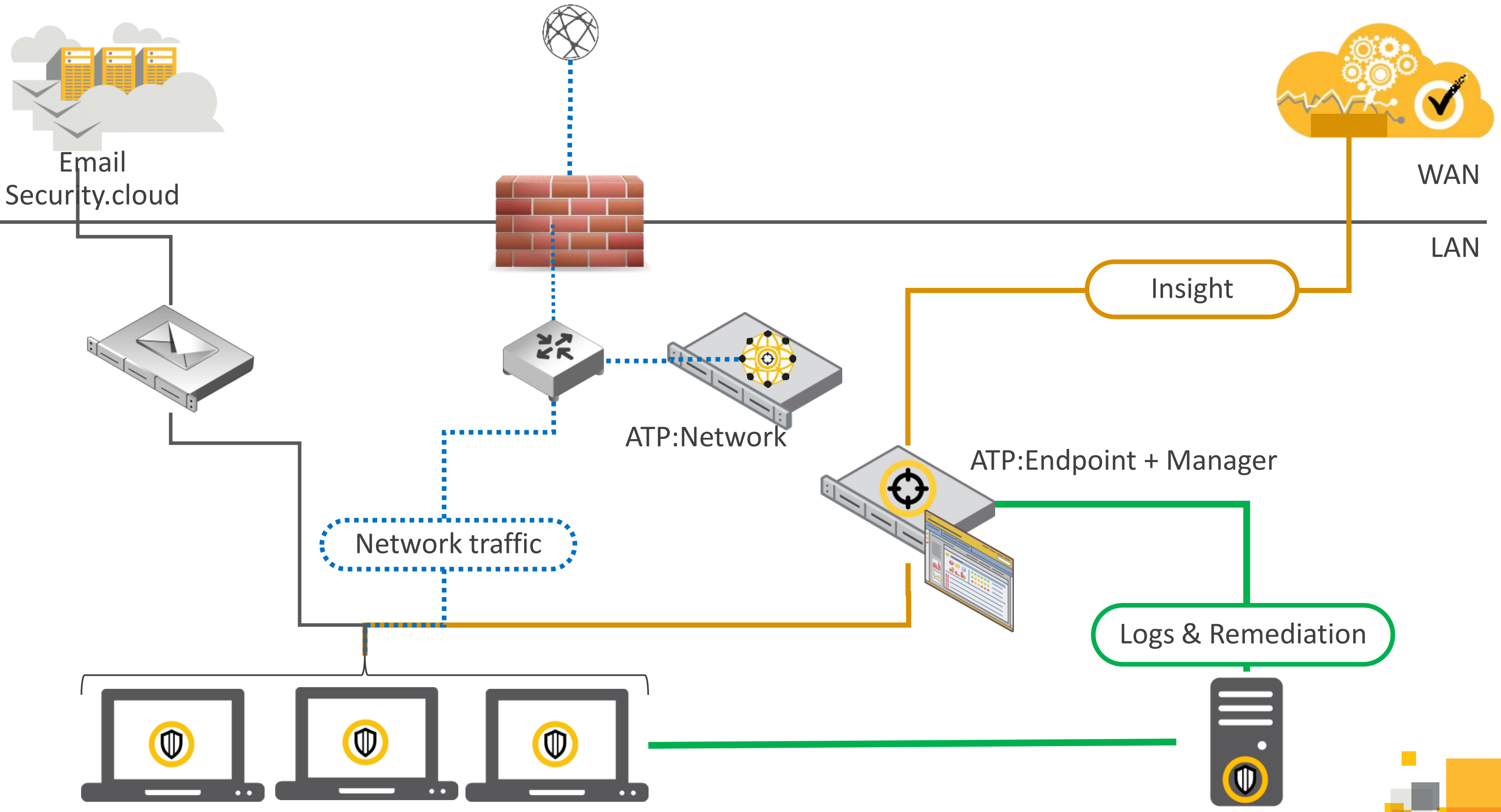
WAN

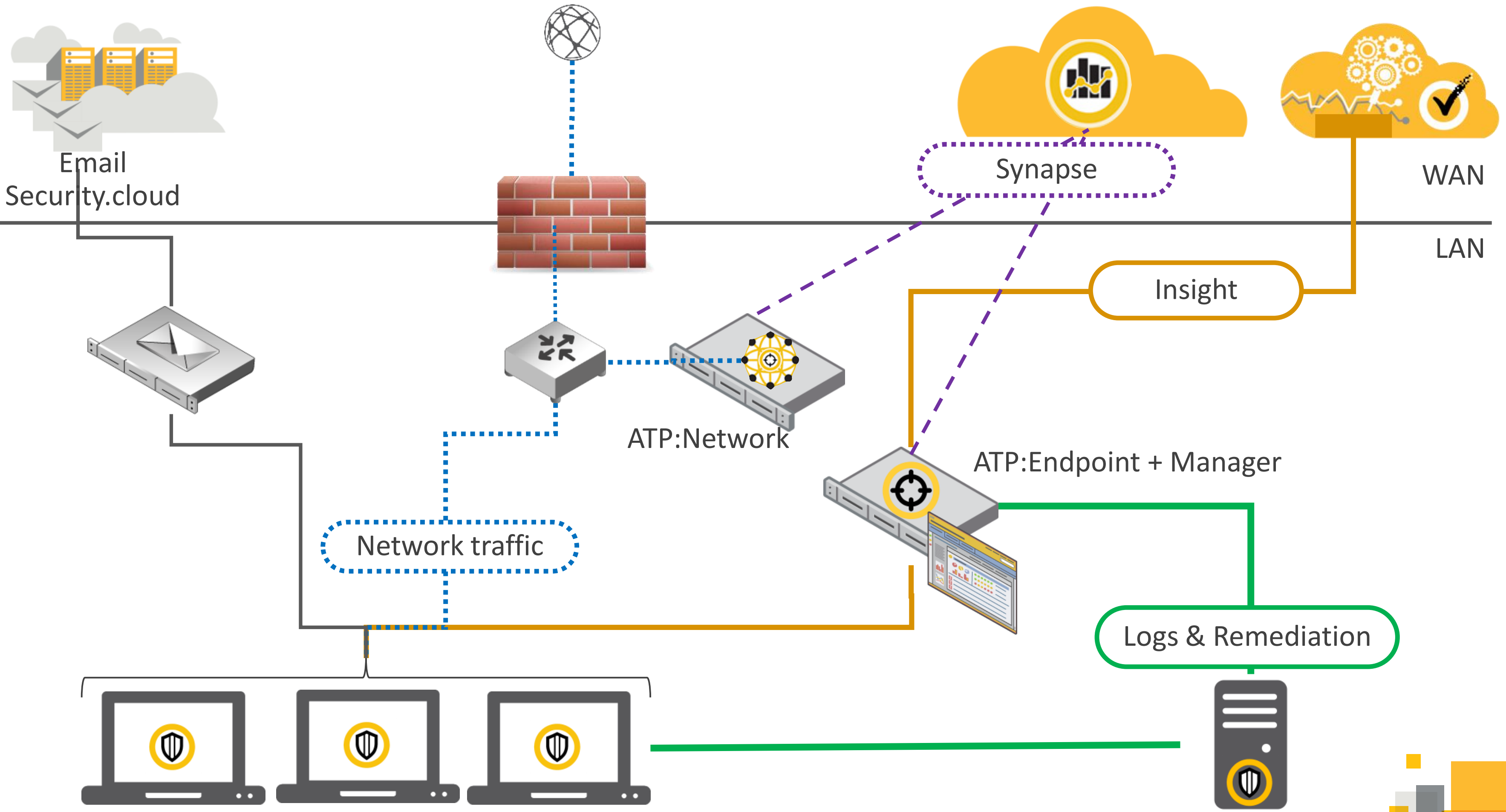
LAN

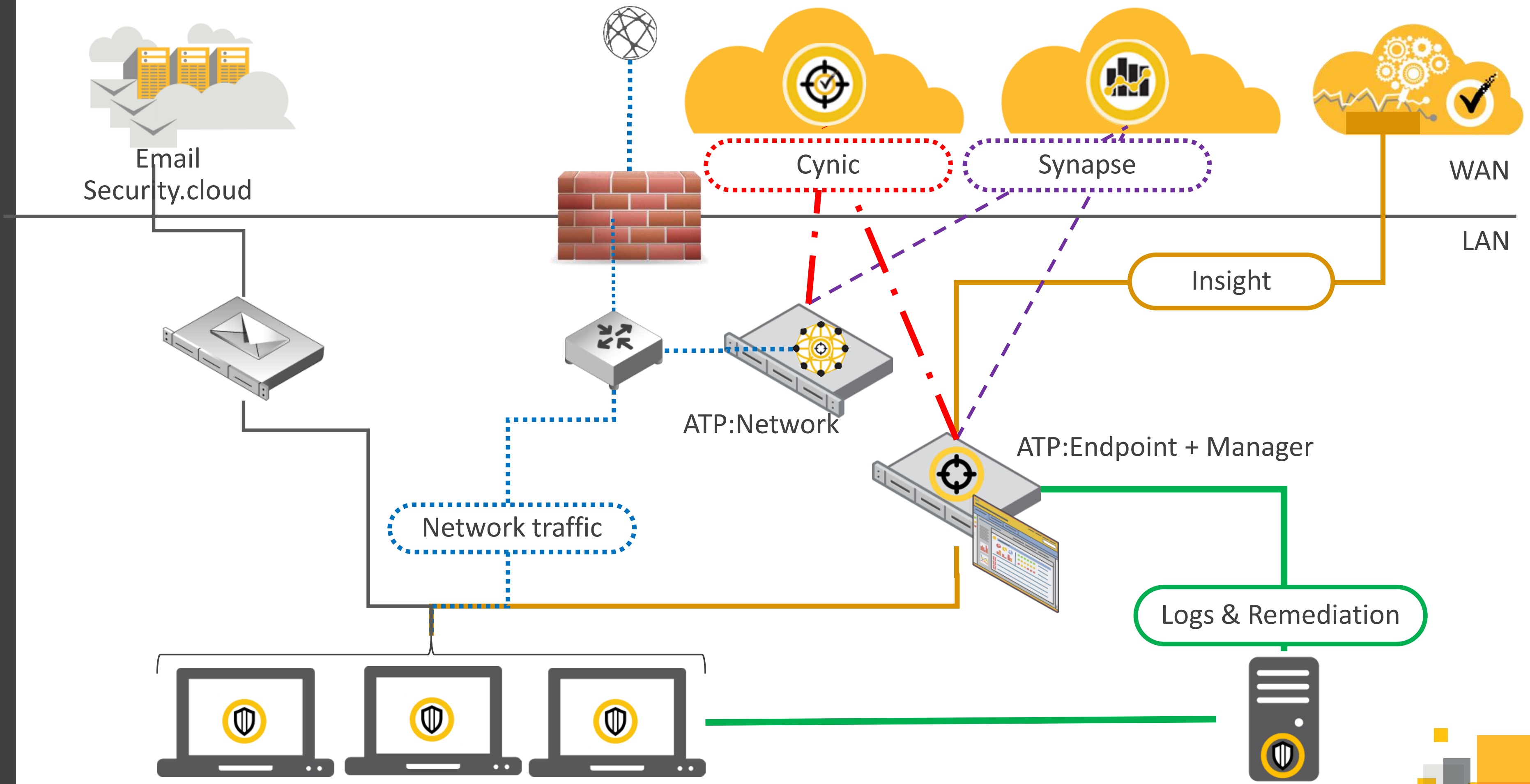
Insight

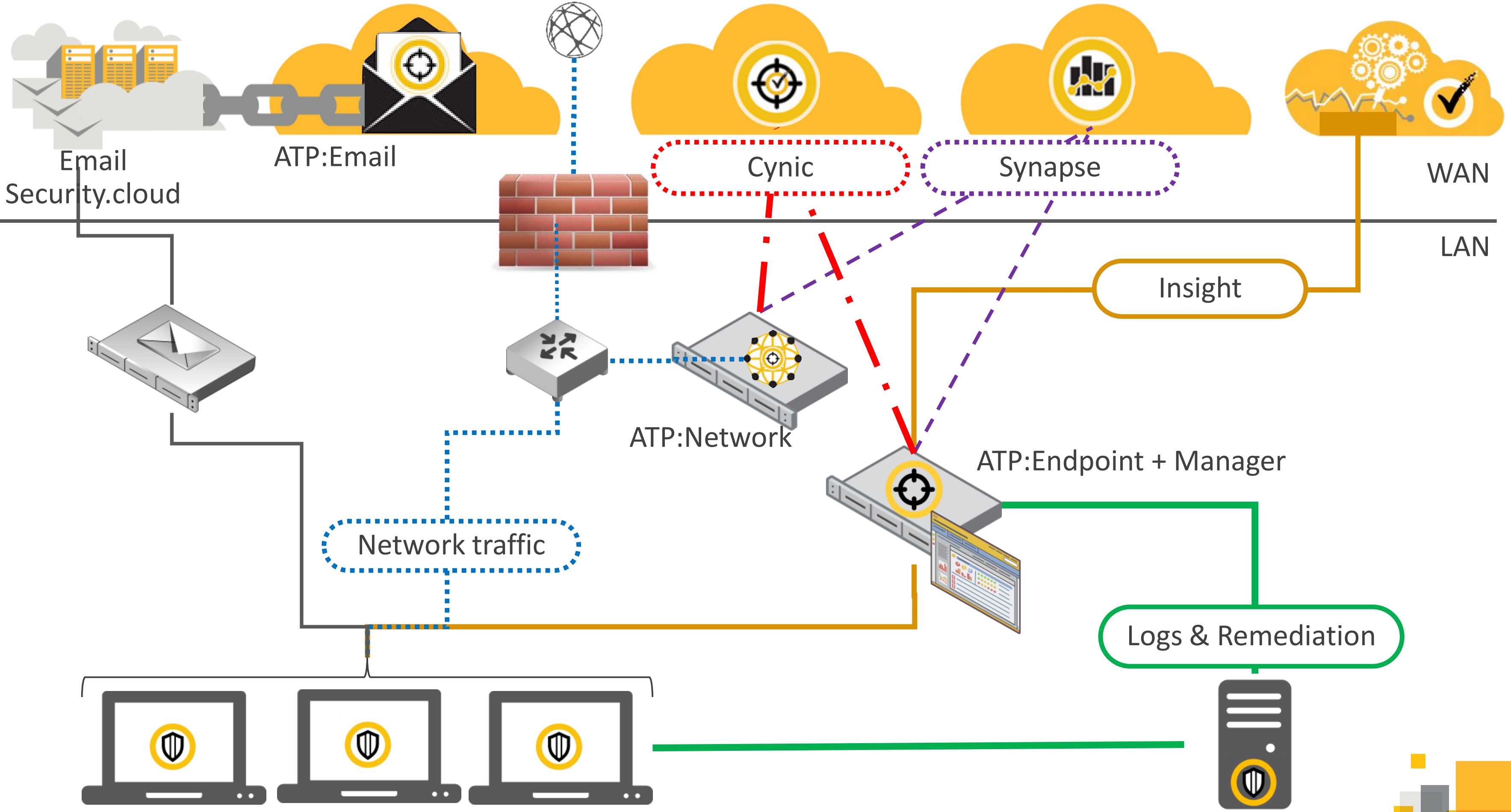
ATP:Endpoint + Manager

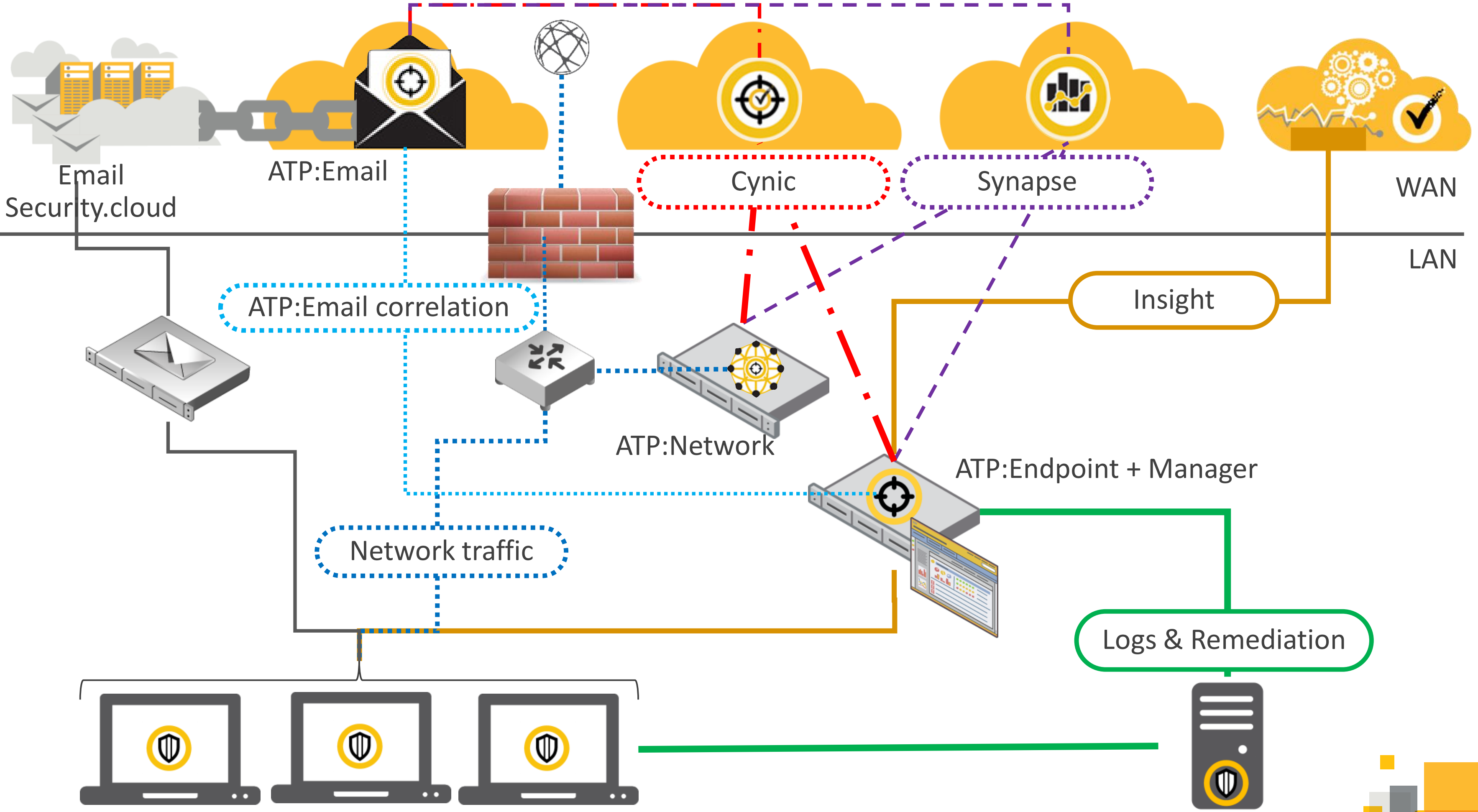
Logs & Remediation


Email
Security.cloud
WAN
LAN
Insight
ATP:Network
ATP:Endpoint + Manager
Network traffic
Logs & Remediation

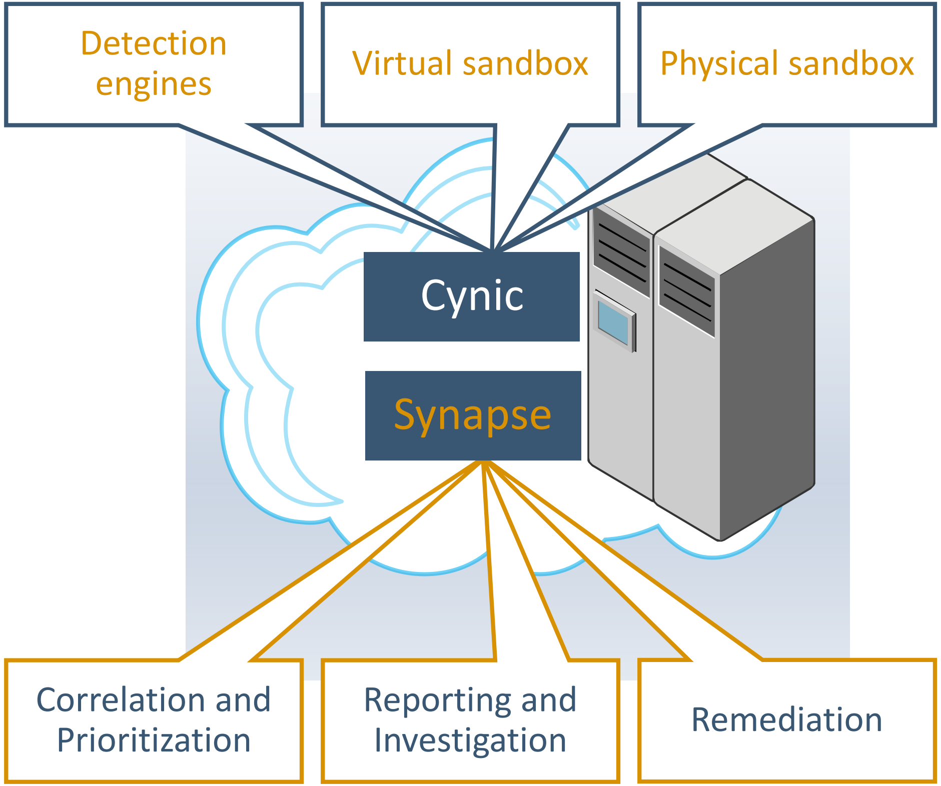

Email
Security.cloud
Synapse
WAN
LAN
Insight
ATP:Network
ATP:Endpoint + Manager
Network traffic
Logs & Remediation


Email
Security.cloud
Cynic
Synapse
WAN
LAN
Insight
ATP:Network
ATP:Endpoint + Manager
Network traffic
Logs & Remediation


Email
Security.cloud
ATP:Email
Cynic
Synapse
WAN
LAN
Insight
ATP:Network
ATP:Endpoint + Manager
Network traffic
Logs & Remediation


Email Security.cloud
ATP:Email
Cynic
Synapse
WAN
LAN
Insight
ATP:Email correlation
ATP:Network
ATP:Endpoint + Manager
Network traffic
Logs & Remediation

Symantec Advanced Threat Protection



ATP: EMAIL

ATP: NETWORK

ATP: ENDPOINT

Symantec Services

Helping you with all of your product needs

Symantec Technical Services Supports You

Consulting Services

Help me **DESIGN** it, **INSTALL** it, **ENHANCE** it

Education Services

Help me **LEARN** about it & **USE** it

Support Services

Help me **FIX** it

Business Critical Services

Remote Product Specialist (RPS)

Premier (Value Based Services)

Help me **UNLOCK VALUE** & **OPTIMIZE** it

Symantec Education Services Offers Effective Product Training

Education Services

A broad range of training solutions to help you get the most out of Symantec products.

- Achieve expected value for your products.
- Learn how Symantec products can solve your business problems today and tomorrow.
- Gain best practice insight to keep your investments running smoothly long-term.
- For more information visit training.symantec.com

Services for ATP – more help, more success!
What to sell and who to contact

Service	What it is	Available when?	Global Contacts	Website

Education Course Offering	ATP Incident Response Course available as Instructor Led Training or via Virtual Academy	Mid-2016	americas_education@symantec.com;
			emea_education@symantec.com;
			apj_education@symantec.com
				Education Services website

BCS Premier for ATP	Symantec's premium Support Services offering, designed to simplify support, maximize return and protect IT infrastructure.	At Product GA	Contact BCS team members from the internal SAVO page or PartnerNet	BCS Contact Page
BCS Proactive Services for ATP	Review of customer's ATP configuration and initial reporting from ATP console	At Product GA	Contact BCS team members from the internal SAVO page or PartnerNet	BCS Contact Page
Consulting Services for ATP	On-site Implementation Services, Solution Assessment & Optimization & Residency Services	At Product GA	ask_consulting_americas@symantec.com ask_consulting_asiapacificjapan@symantec.com ask_consulting_emea@symantec.com	Consulting website

Additional Resources and Summary

RESOURCES

If you would like to know more about Advanced Threat Protection please visit: https://www.symantec.com/advanced-threat-protection/

SUMMARY

During this presentation we have discussed how Advanced Threat Protection enables a customer to prevent advanced persistent threats, identify suspicious files and search for Indicators of Compromise. We also learned how ATP can block, isolate and remove the advanced persistent threats while minimizing environmental changes by leveraging a company’s existing Symantec security investment.

Symantec™