Advanced Cyber Illness Treatmant

Davor Perat
Senior Technology Consultant

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

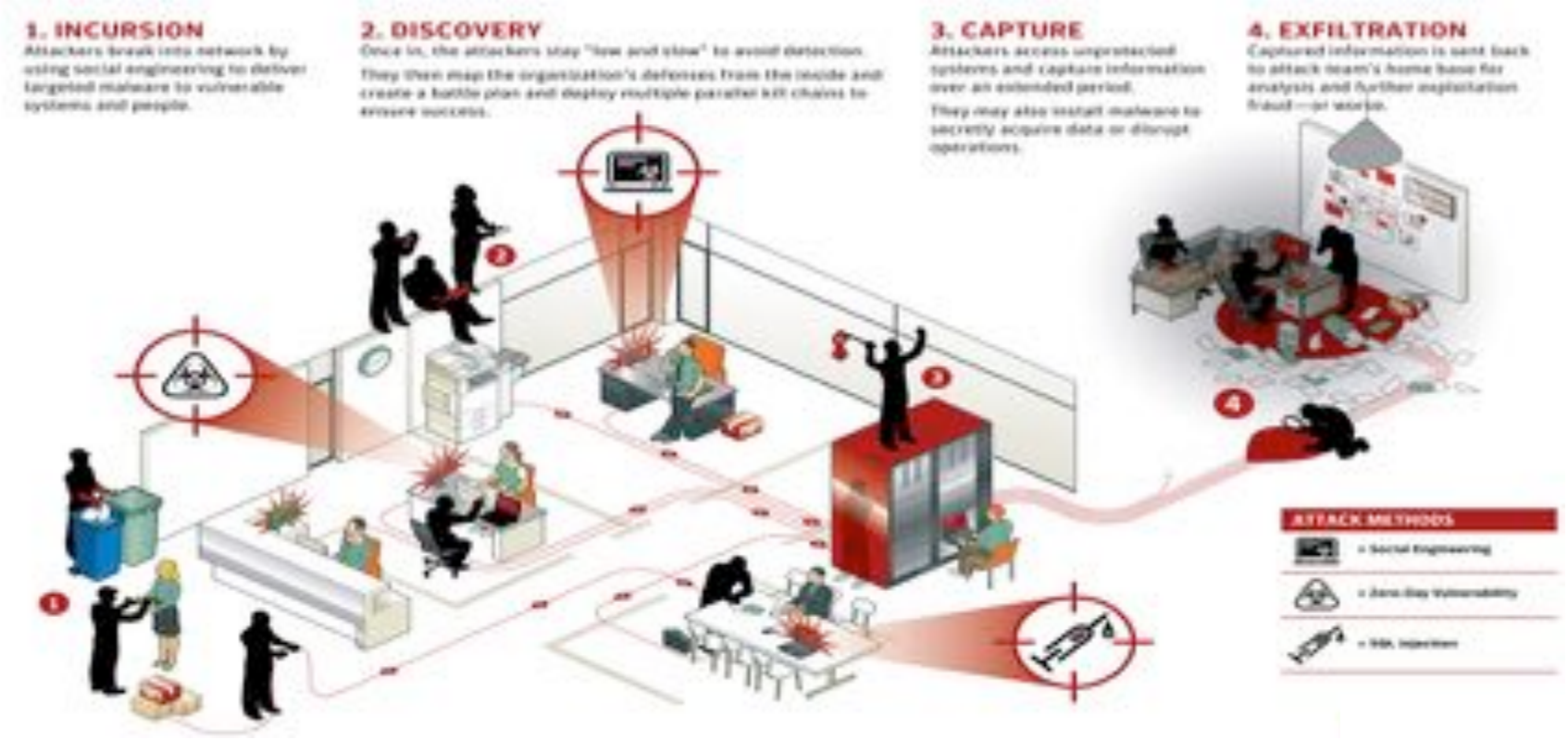
Uses previously unknown zero-day attacks, root kits, and evasive technologies

Persistent

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

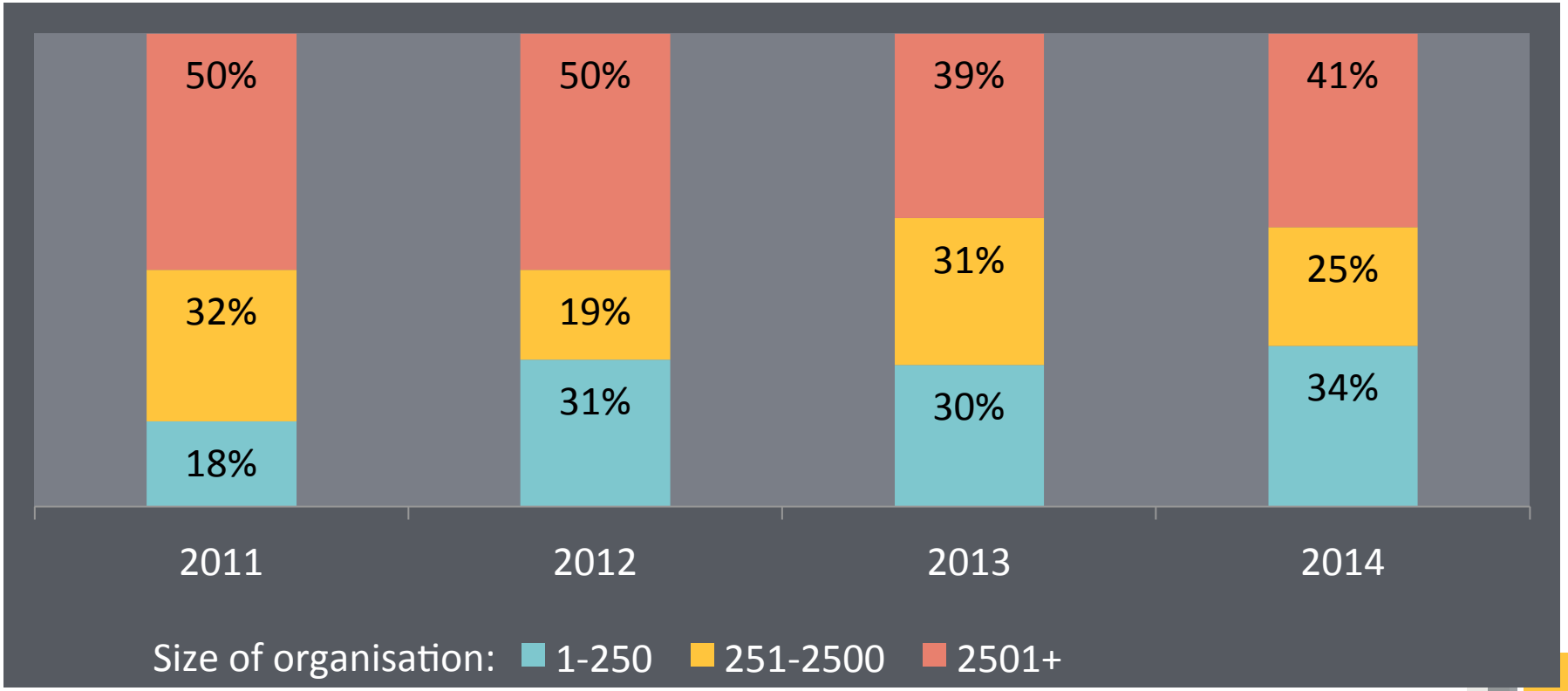
Copyright © 2014 Symantec Corporation

How They Work: Advanced Threats



Copyright © 2014 Symantec Corporation

What the likelihood is of being a target



Copyright © 2014 Symantec Corporation

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

Copyright © 2014 Symantec Corporation

What the results are of being a target (continued)

Commercially

Resource

Opex
Capex
Legal Fees
Time
Money

Theft

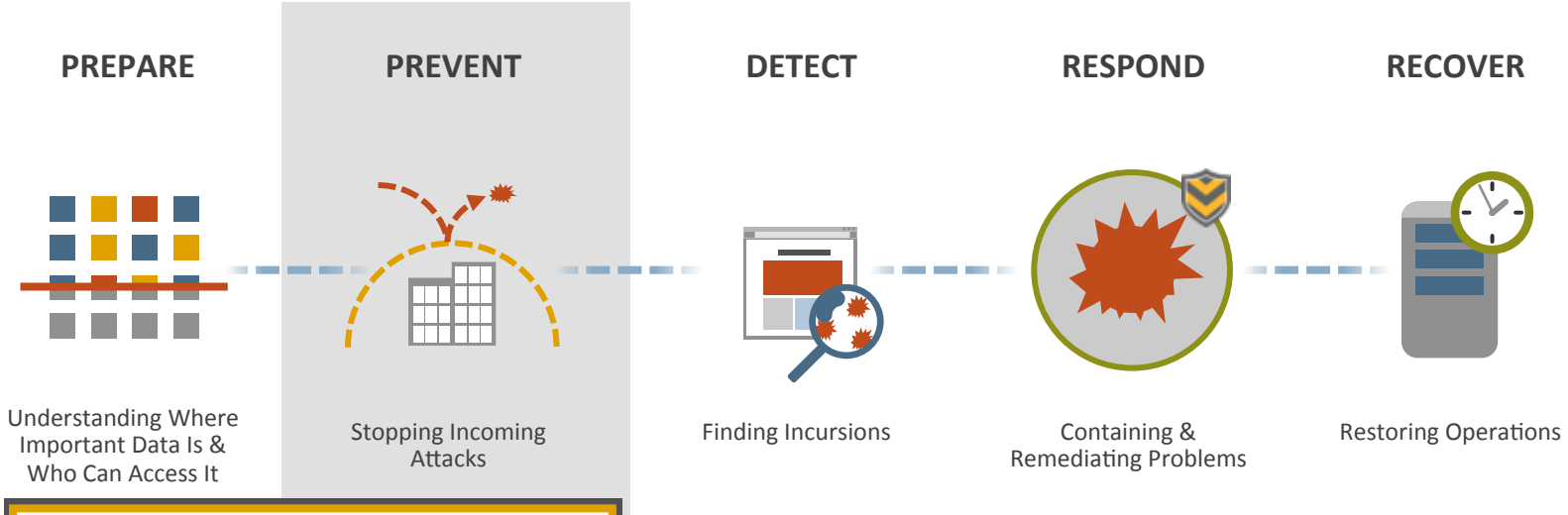
Intellectual Property
Money
Customer Data
Employee Data

Reputation

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

Copyright © 2014 Symantec Corporation

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

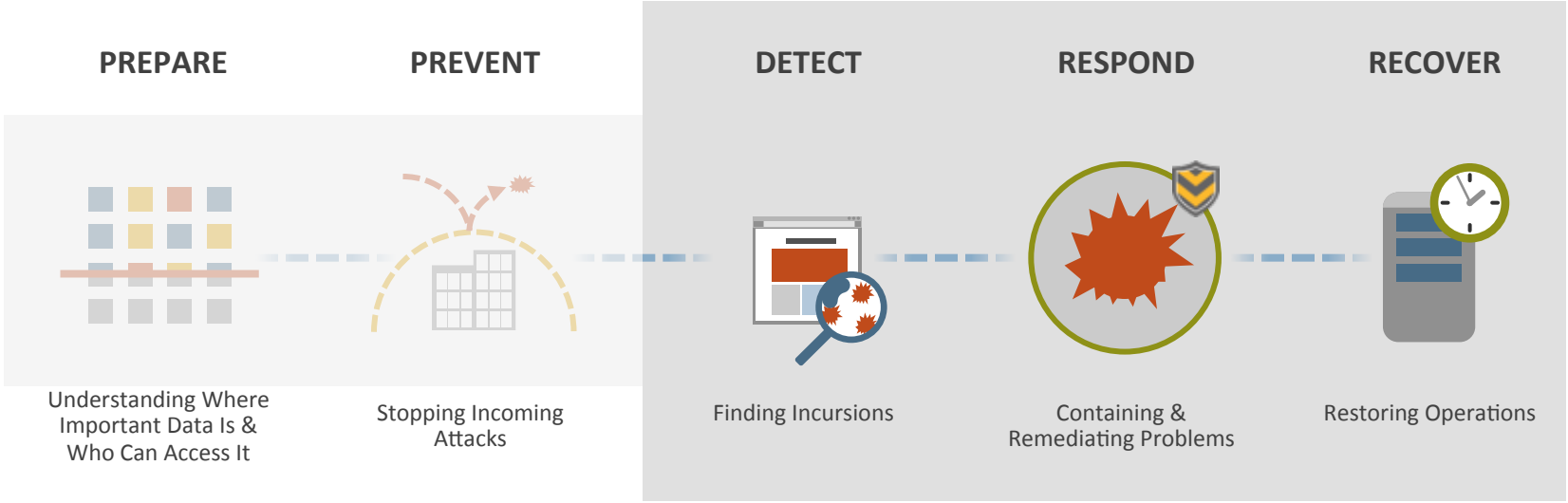


While prevention is still very important….

…you need to prepare to be breached.

Copyright © 2014 Symantec Corporation

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



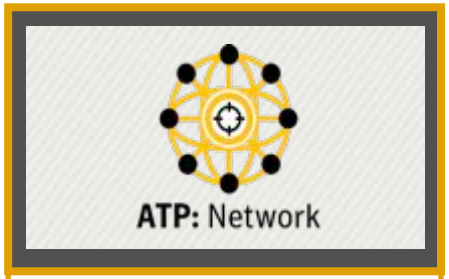
Copyright © 2014 Symantec Corporation

ATP Solution:

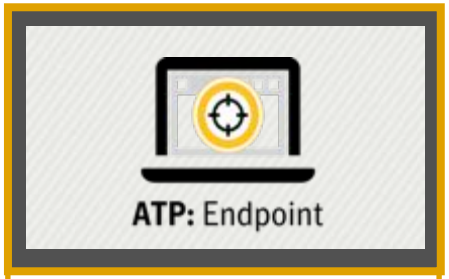
Identify suspicious files

Copyright © 2014 Symantec Corporation

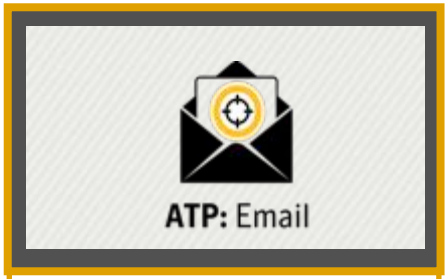
Symantec Advanced Threat Protection: Modules



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



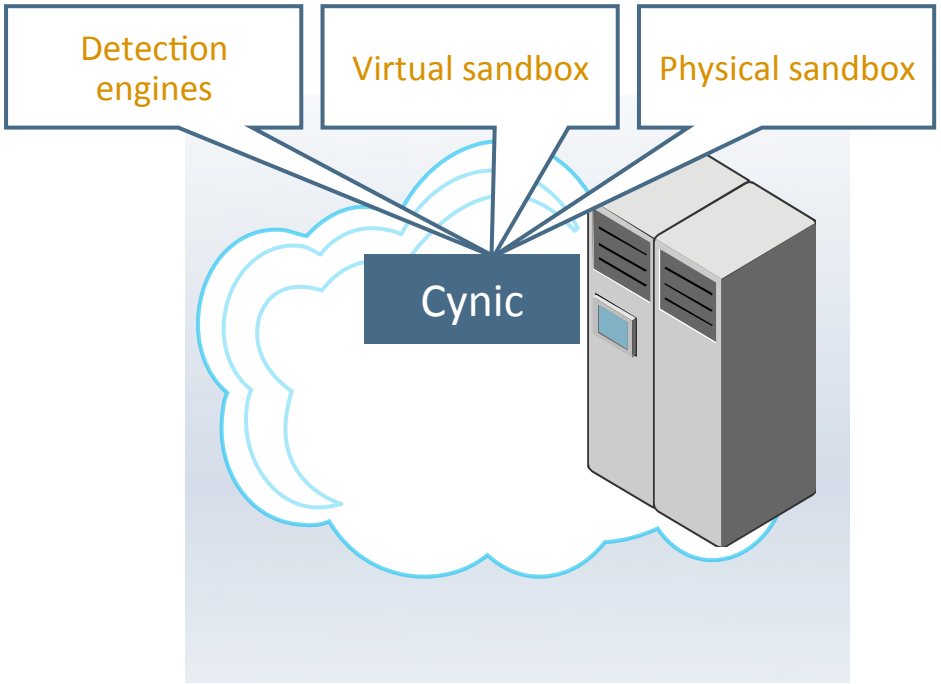
- Endpoint visibility (the foothold in most targeted attacks)
- Endpoint context, suspicious events, & remediation
- Requires SEP – no new agent – and deployed as a virtual or physical appliance



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

Copyright © 2014 Symantec Corporation

Symantec Advanced Threat Protection: Cynic



ATP: NETWORK

ATP: ENDPOINT

ATP: EMAIL

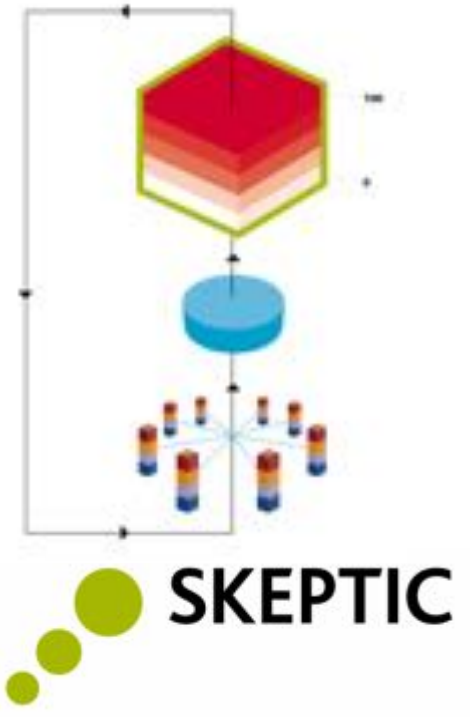
Copyright © 2014 Symantec Corporation

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



+ Questionable source

+ Suspect Attachment

+ Suspicious code in attachment

(+ Evidence of obfuscation)

(+ Unexpected encryption)

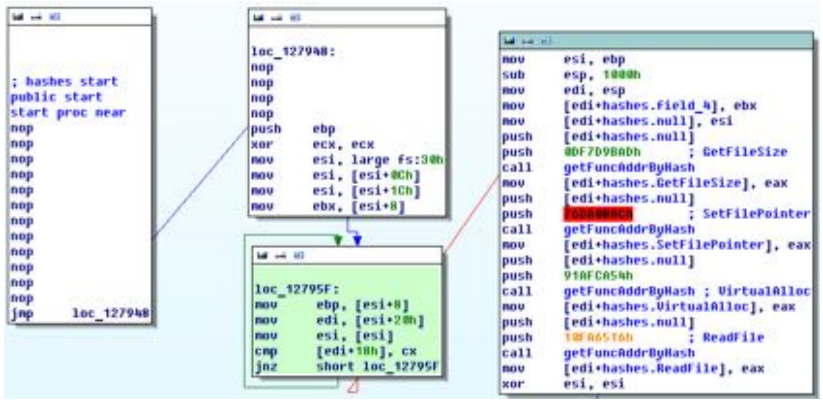
Heuristically detected malcode

Copyright © 2014 Symantec Corporation

* Not all suspicious elements required for conviction

SONAR

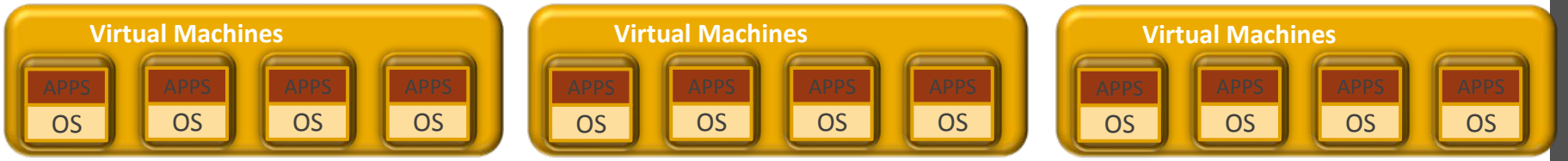
- Dynamic analysis
- Does not make detections on application type, but on how a process behaves.
- If it behaves maliciously, regardless of its type, it will trigger a detection



Copyright © 2014 Symantec Corporation

Virtual Execution

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



Copyright © 2014 Symantec Corporation

Physical Execution

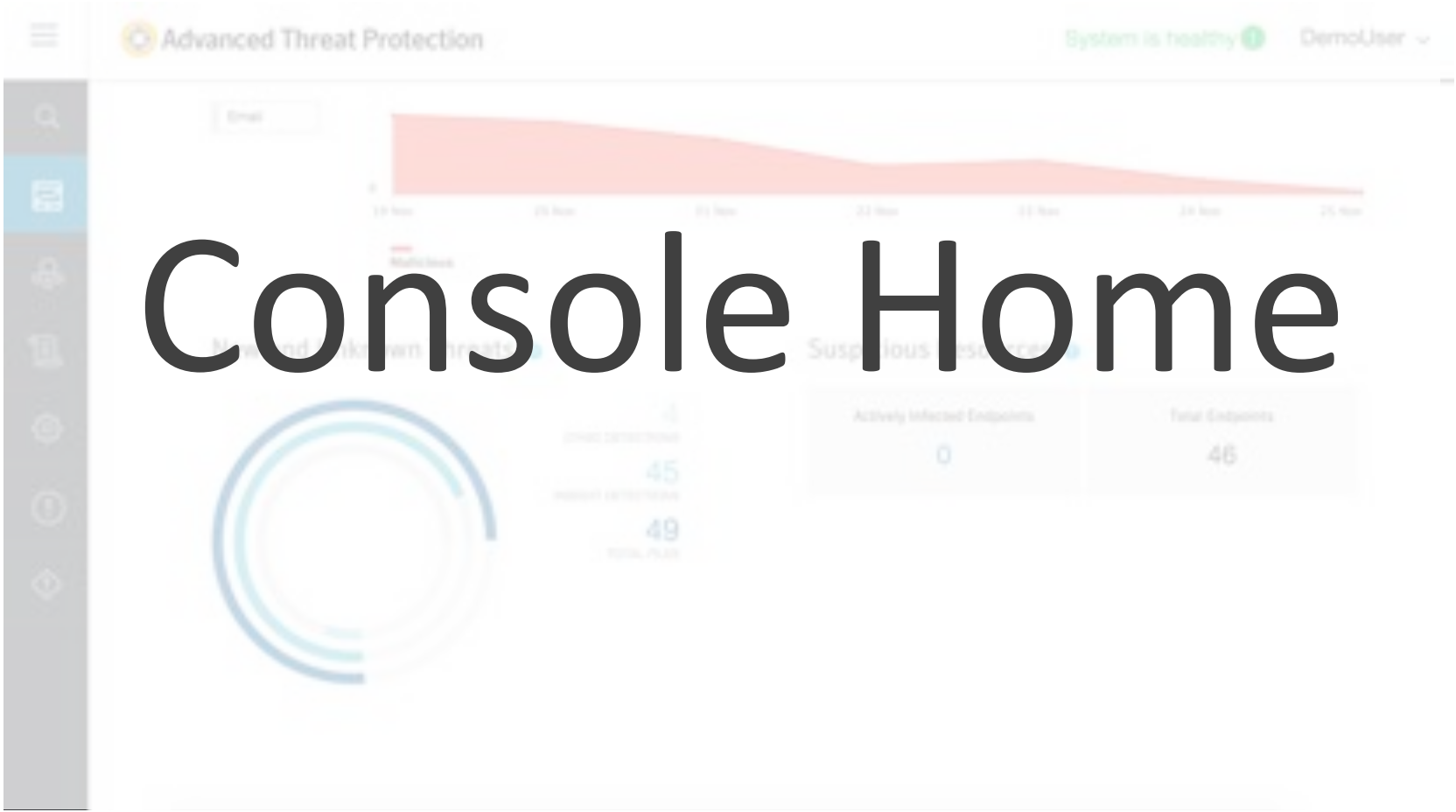
- Physical hardware
- Bare metal execution
  - No Virtualization

Copyright © 2014 Symantec Corporation

ATP Solution:

Search for Indicators of Compromise

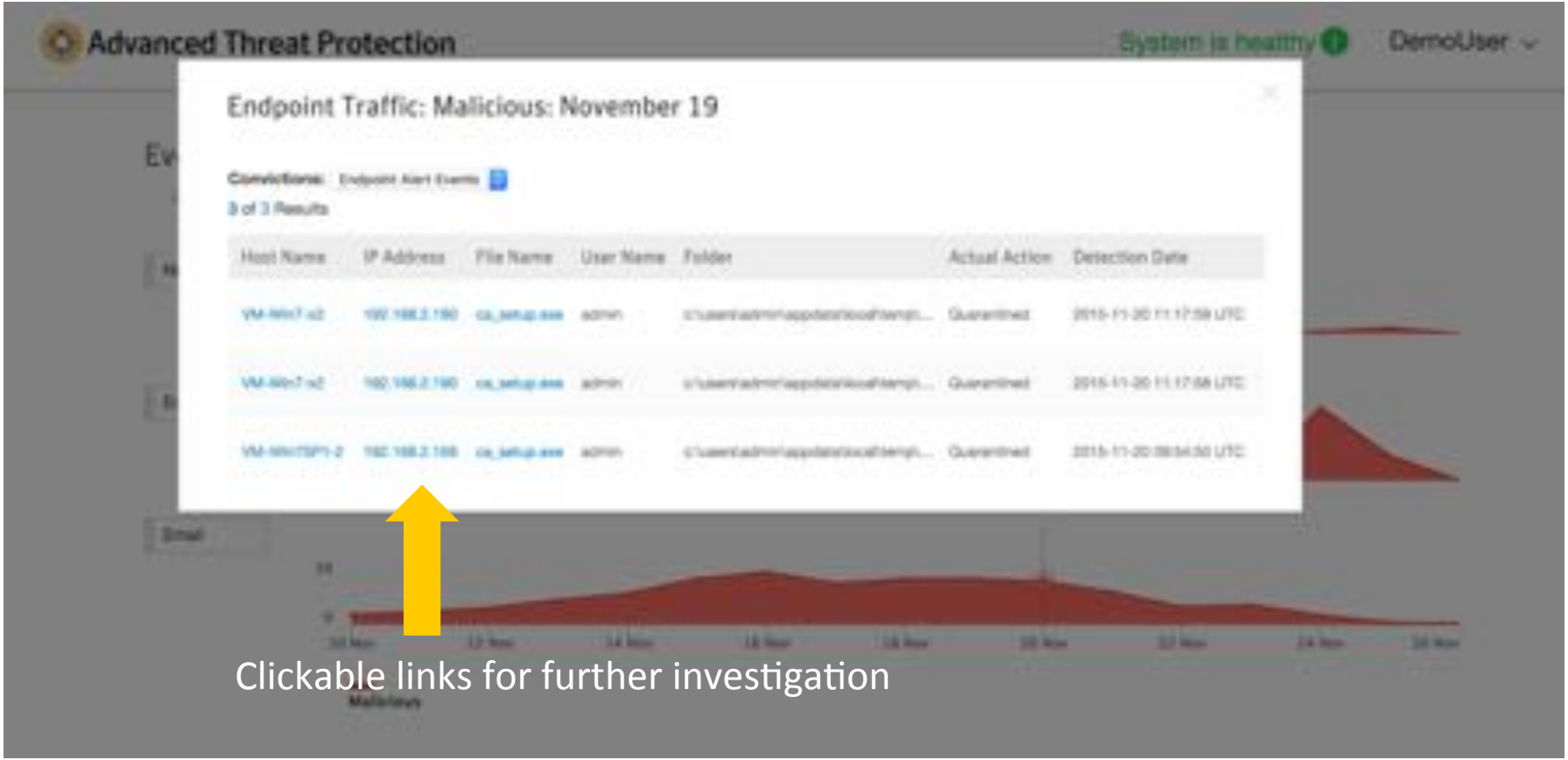
Copyright © 2014 Symantec Corporation



Console Home

Copyright © 2014 Symantec Corporation

Copyright © 2014 Symantec Corporation



Copyright © 2014 Symantec Corporation

ca_setup.exe

Bad

Not Available

No

SecurityRisk.BL

f98bc99cb8160d4e7f19fb76410ca4fab37c3d3dbfef6123b54c6c...

ea2ef30c99ececb1eda9aa128631ff31

Not Signed

Unknown

File Overview

6	0	0
0	1	

Global Reputation

Years ago

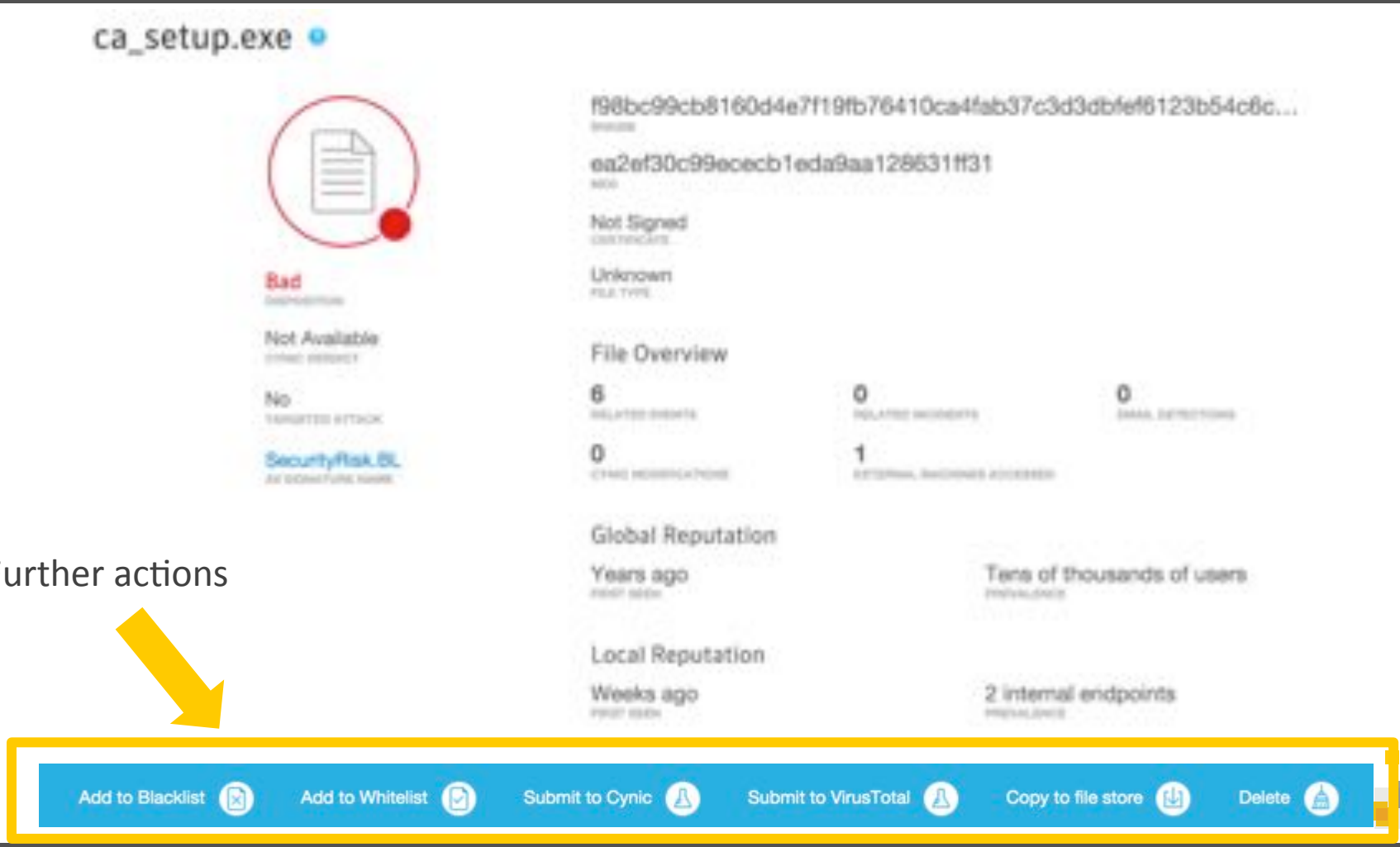
Tens of thousands of users

Local Reputation

Weeks ago

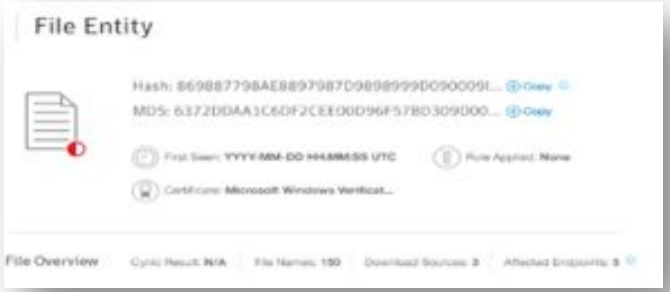
2 internal endpoints

Add to Blacklist | Add to Whitelist | Submit to Cynic | Submit to VirusTotal | Copy to file store | Delete



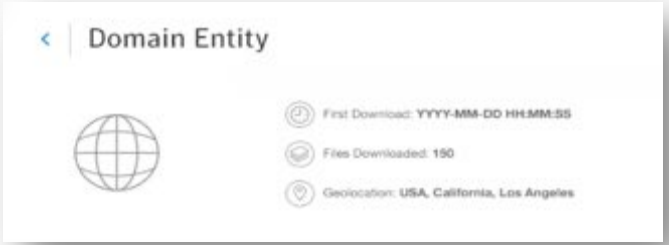
Further actions

Entity Point Pages

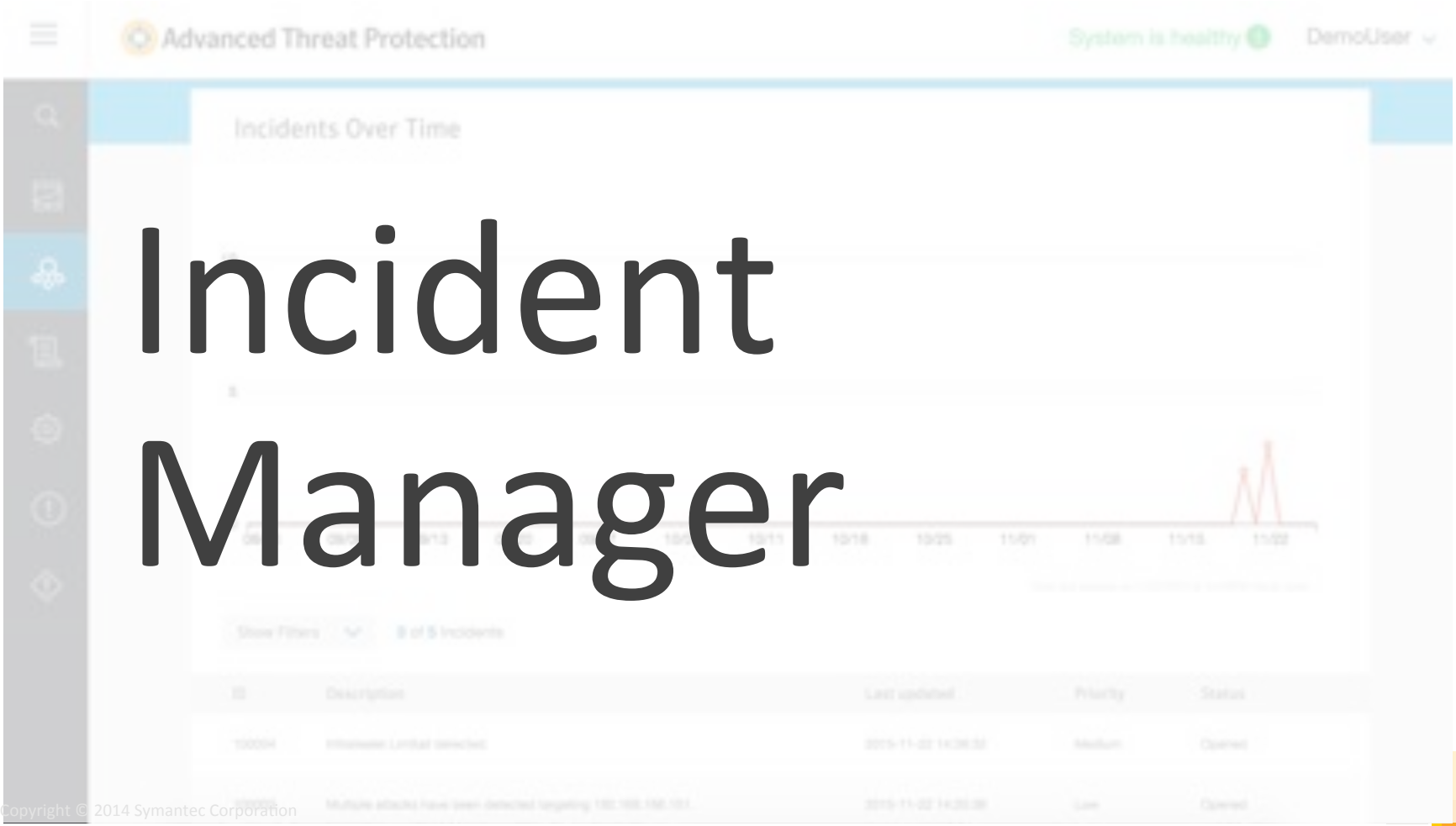


File Entity page
Related Incidents
Related Events
Seen on Endpoints
Files downloaded Origins
Files named associated with Hash
Cynic Results

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

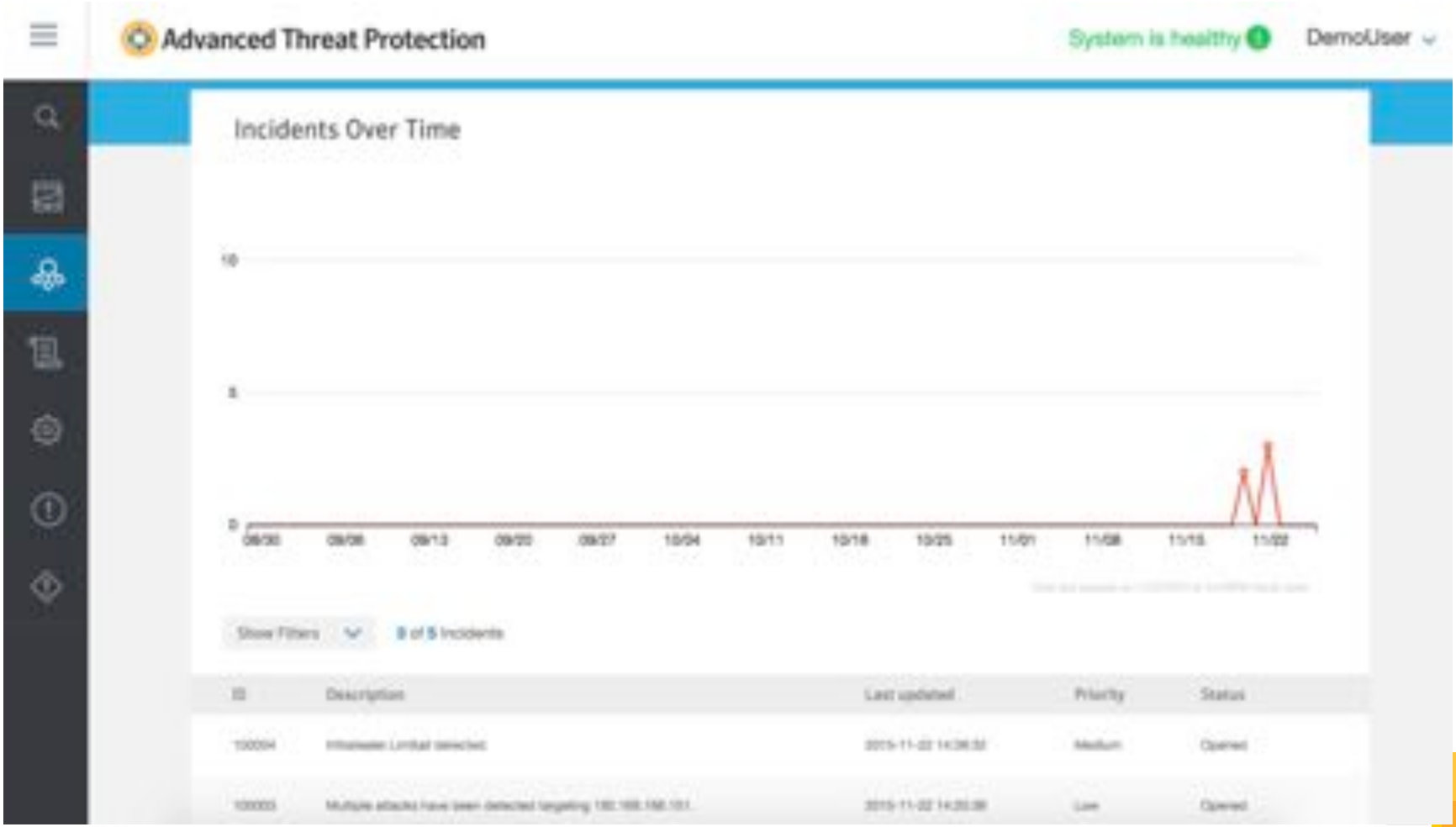


Endpoint Entity Page
Related Incidents
Related Events
Malicious Files
Malicious Connections



Incident Manager

Copyright © 2014 Symantec Corporation


Advanced Threat Protection
System is healthy
DemoUser
Incidents Over Time
10
5
0
08/30
09/06
09/13
09/20
09/27
10/04
10/11
10/18
10/25
11/01
11/08
11/15
11/22
Show Filters
0 of 5 Incidents
ID
Description
Last updated
Priority
Status

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 14:20:38	Low	Opened
100002	Multiple attacks have been detected from imbad.com.	2015-11-22 14:20:38	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

Copyright © 2014 Symantec Corporation

Searches

Copyright © 2014 Symantec Corporation

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)

Copyright © 2014 Symantec Corporation

Searches

Files using
- File name
- File Hash (SHA256, MD5)

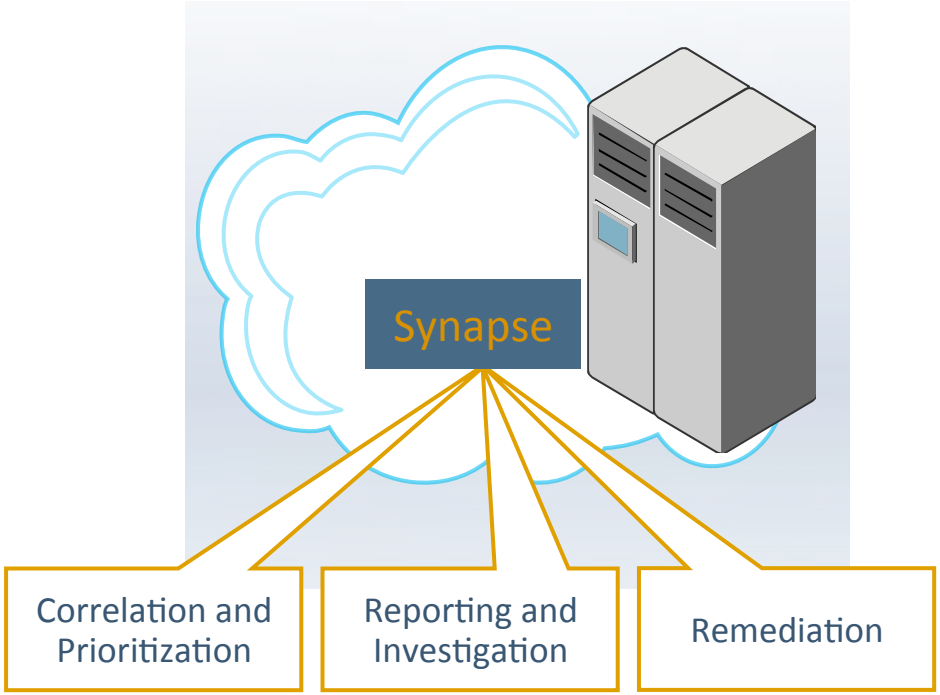
Endpoints using
- Host name
- IP Address (v4)
- Logon user

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.

Copyright © 2014 Symantec Corporation

Symantec Advanced Threat Protection: Synapse



ATP: EMAIL

ATP: NETWORK

ATP: ENDPOINT

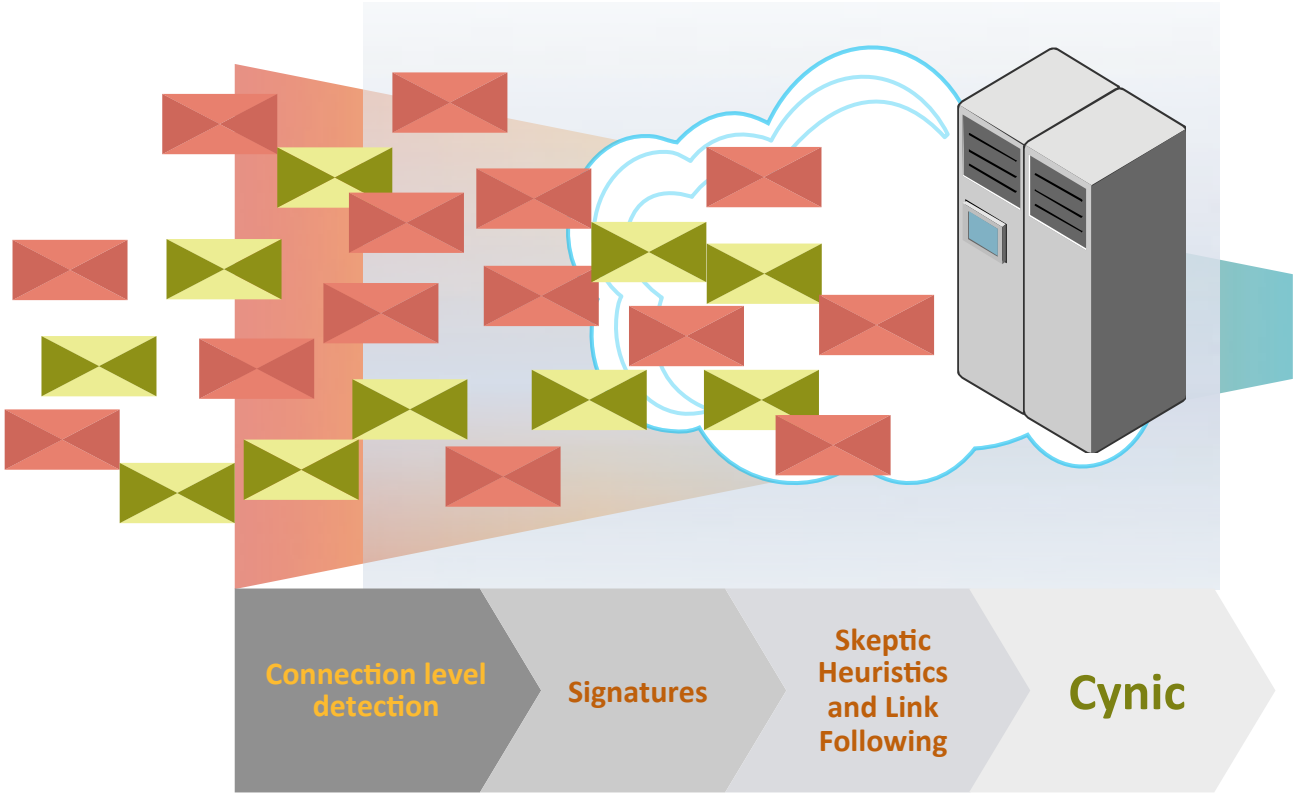
Copyright © 2014 Symantec Corporation

ATP Solution:

Block, isolate and remove the advanced persistent threats

Copyright © 2014 Symantec Corporation

First line of defense: ATP: Email

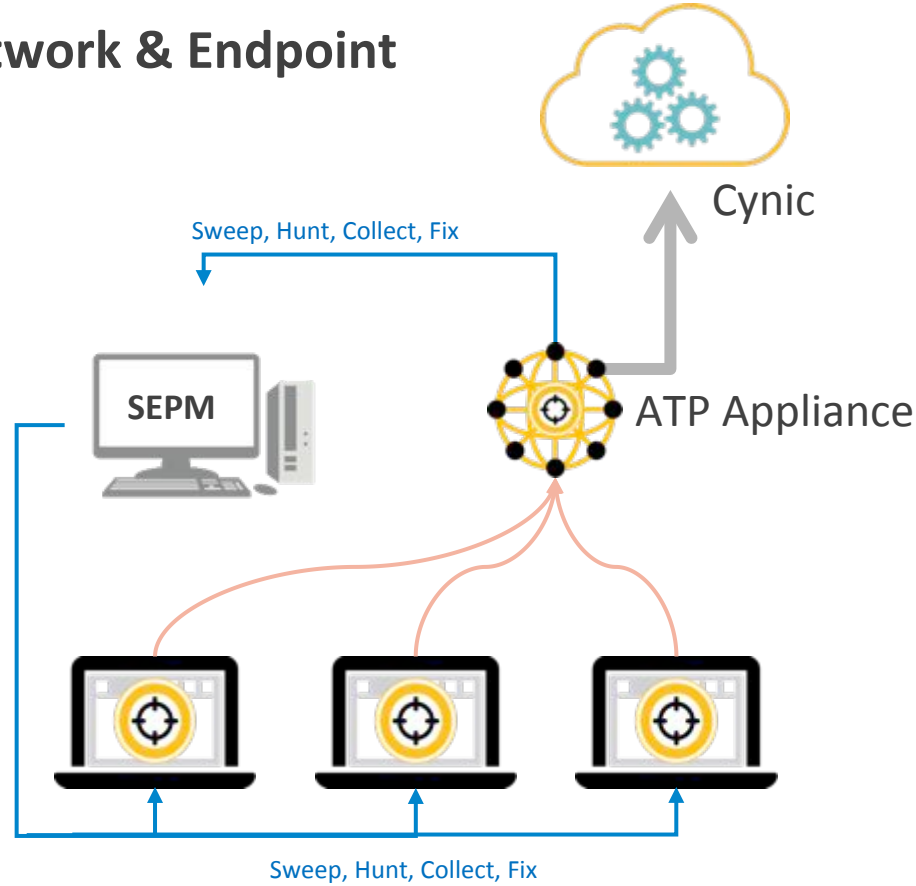


Anything without a verdict will be scanned by Cynic for a customer configured duration (≤ 20 mins)

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

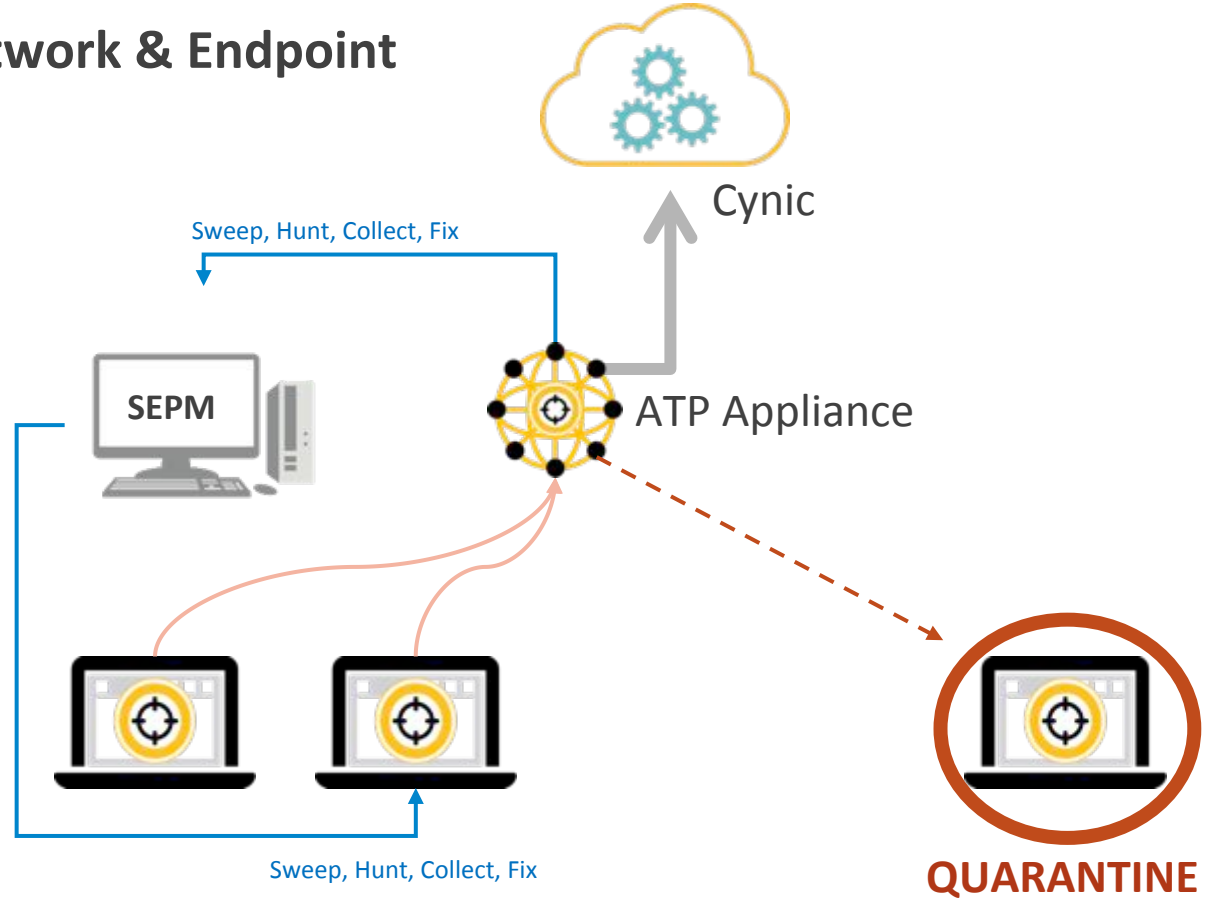
Copyright © 2014 Symantec Corporation

ATP: Network & Endpoint



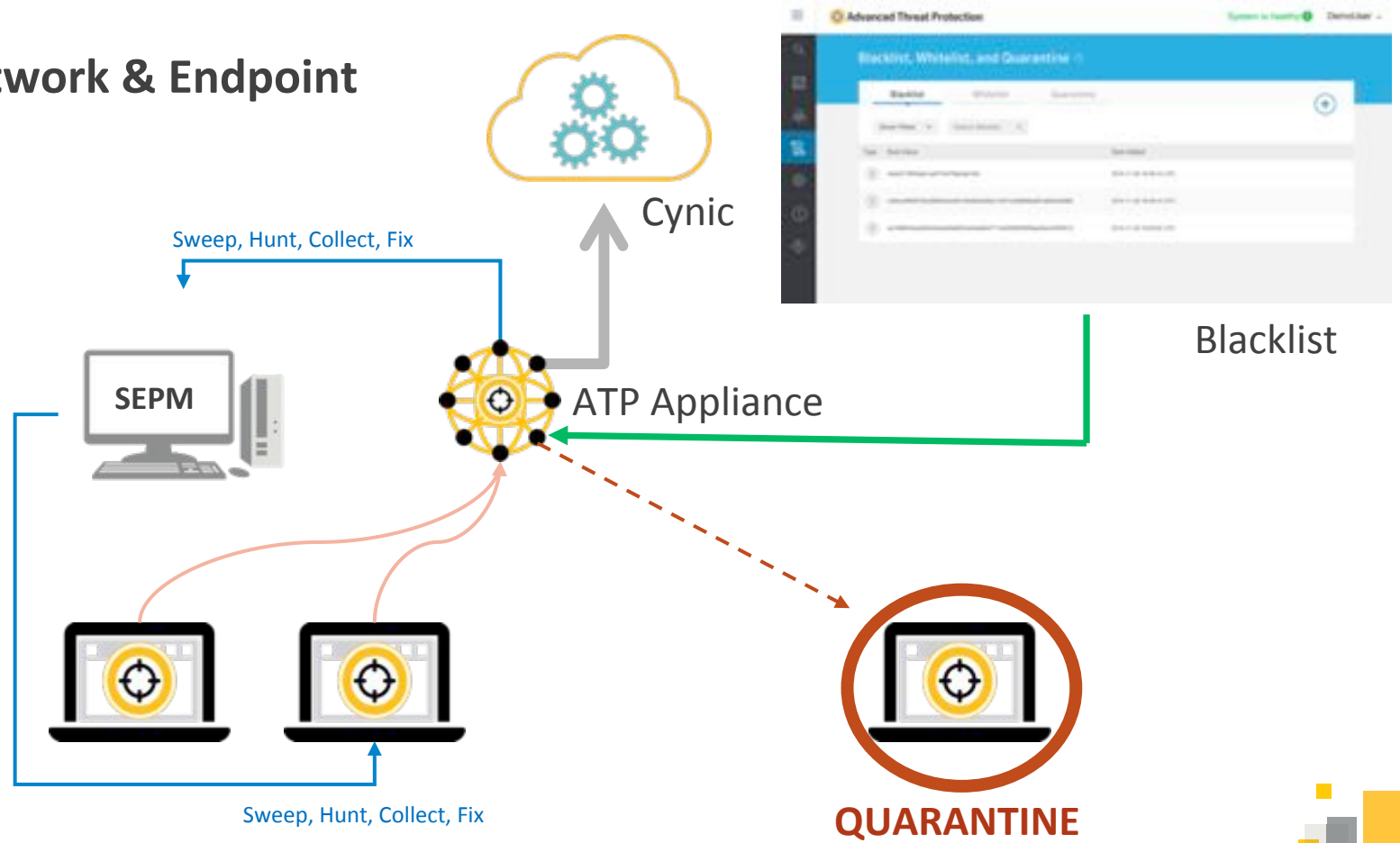
Copyright © 2014 Symantec Corporation

ATP: Network & Endpoint



Copyright © 2014 Symantec Corporation

ATP: Network & Endpoint



Copyright © 2014 Symantec Corporation

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

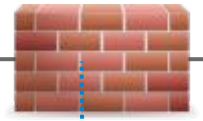
Copyright © 2014 Symantec Corporation

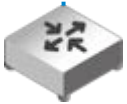
ATP Solution:

Minimize environmental changes

Copyright © 2014 Symantec Corporation

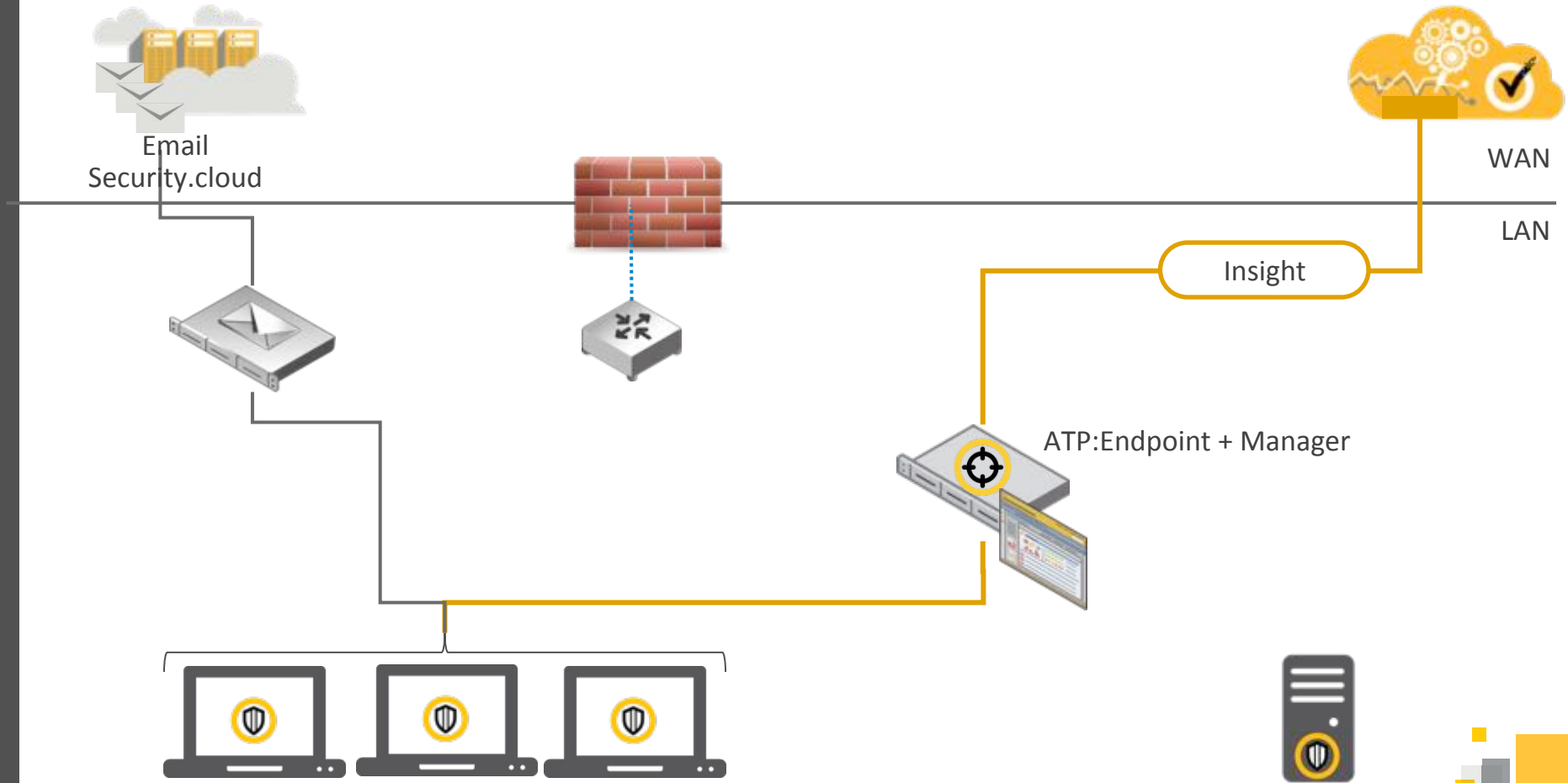
Email
Security.cloud

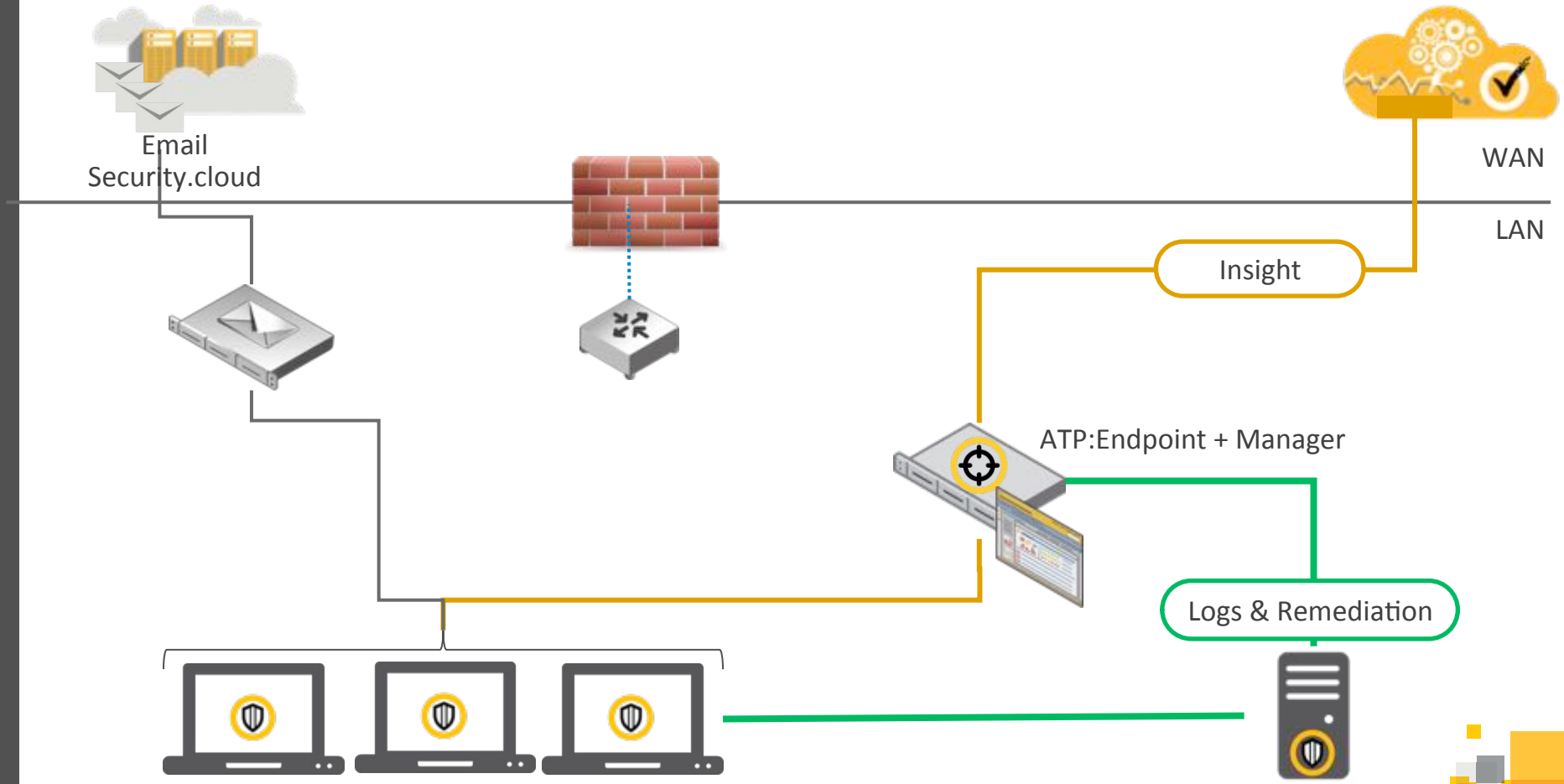


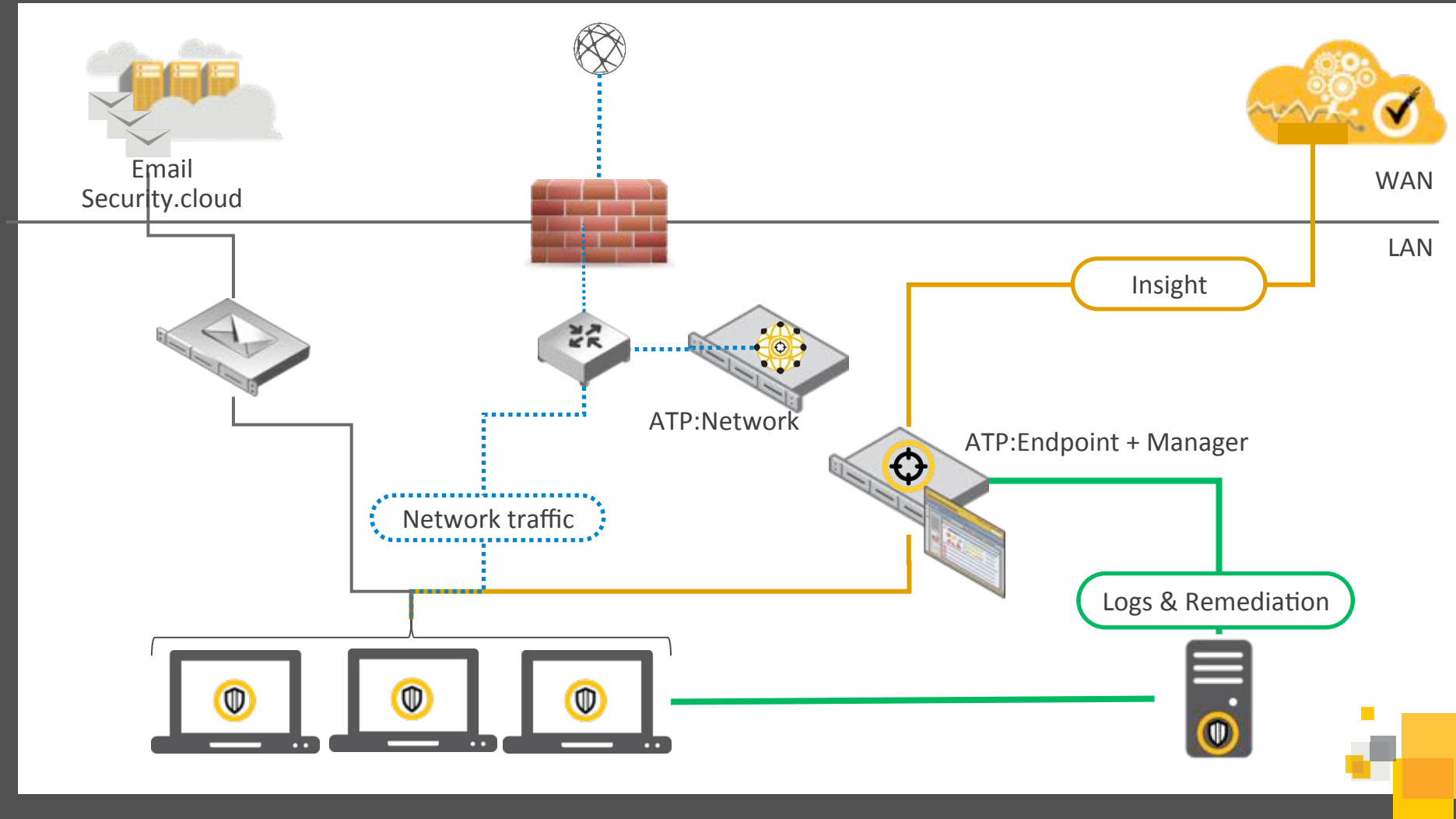


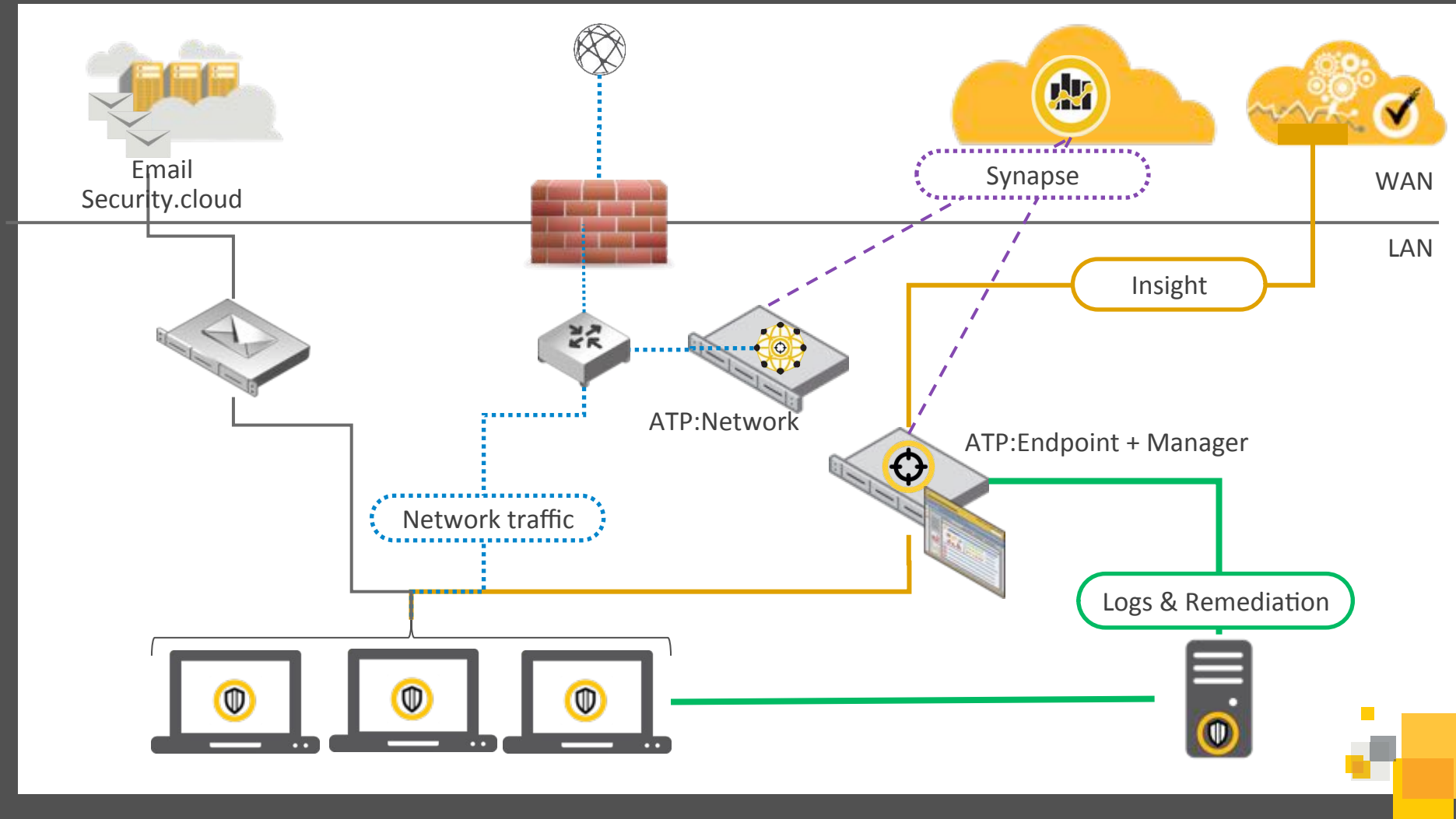
WAN

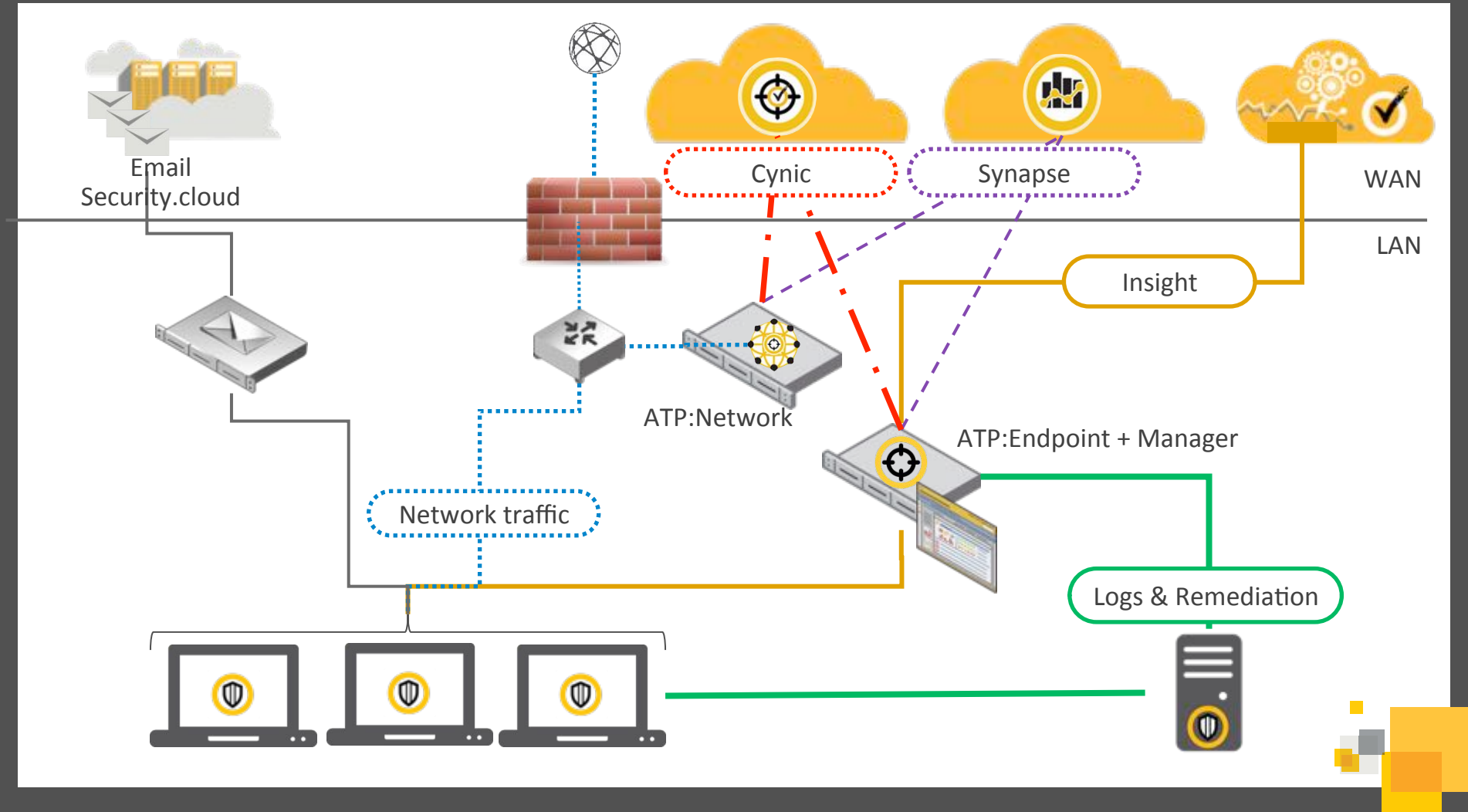
LAN

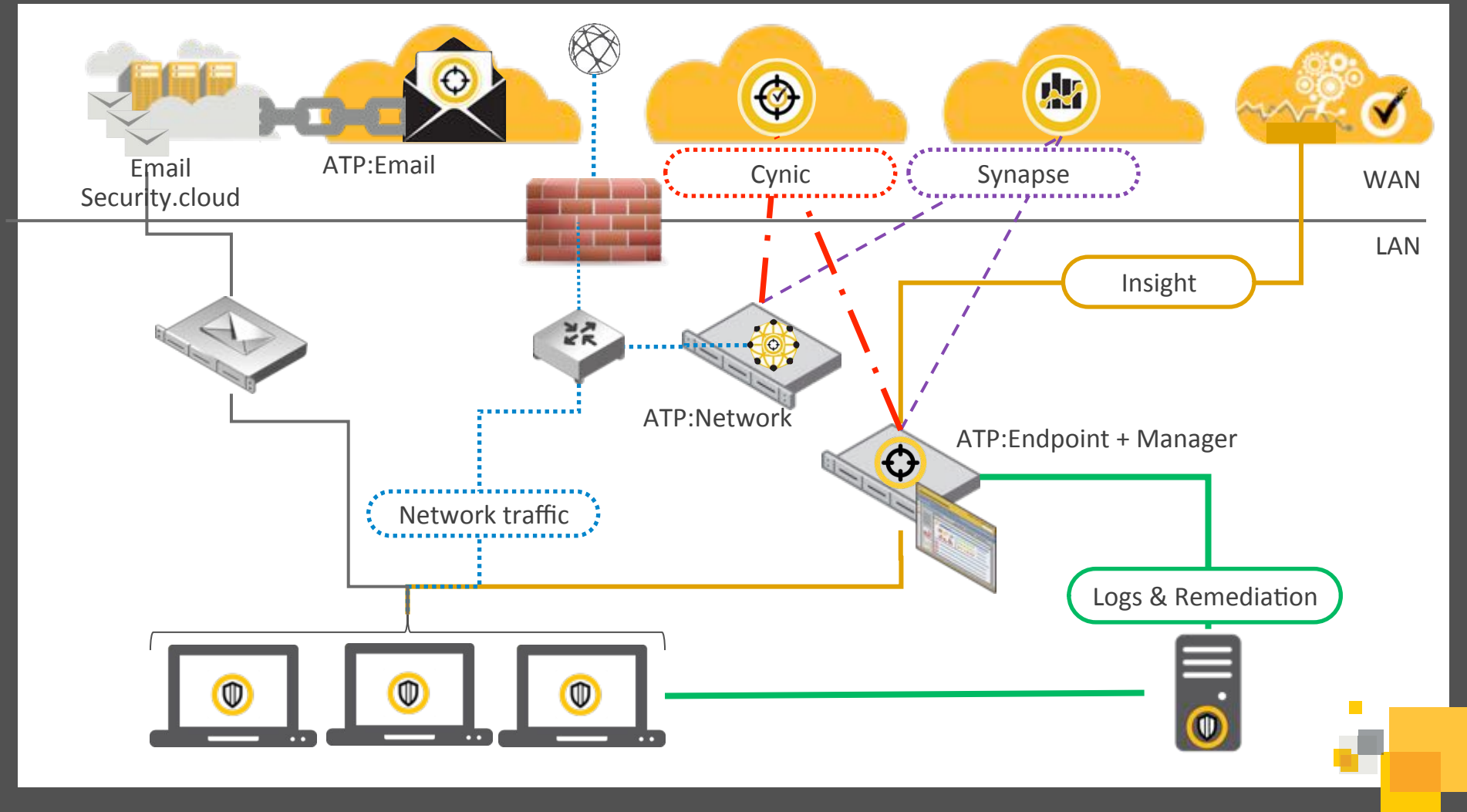

Email
Security.cloud
WAN
LAN
Insight
ATP:Endpoint + Manager

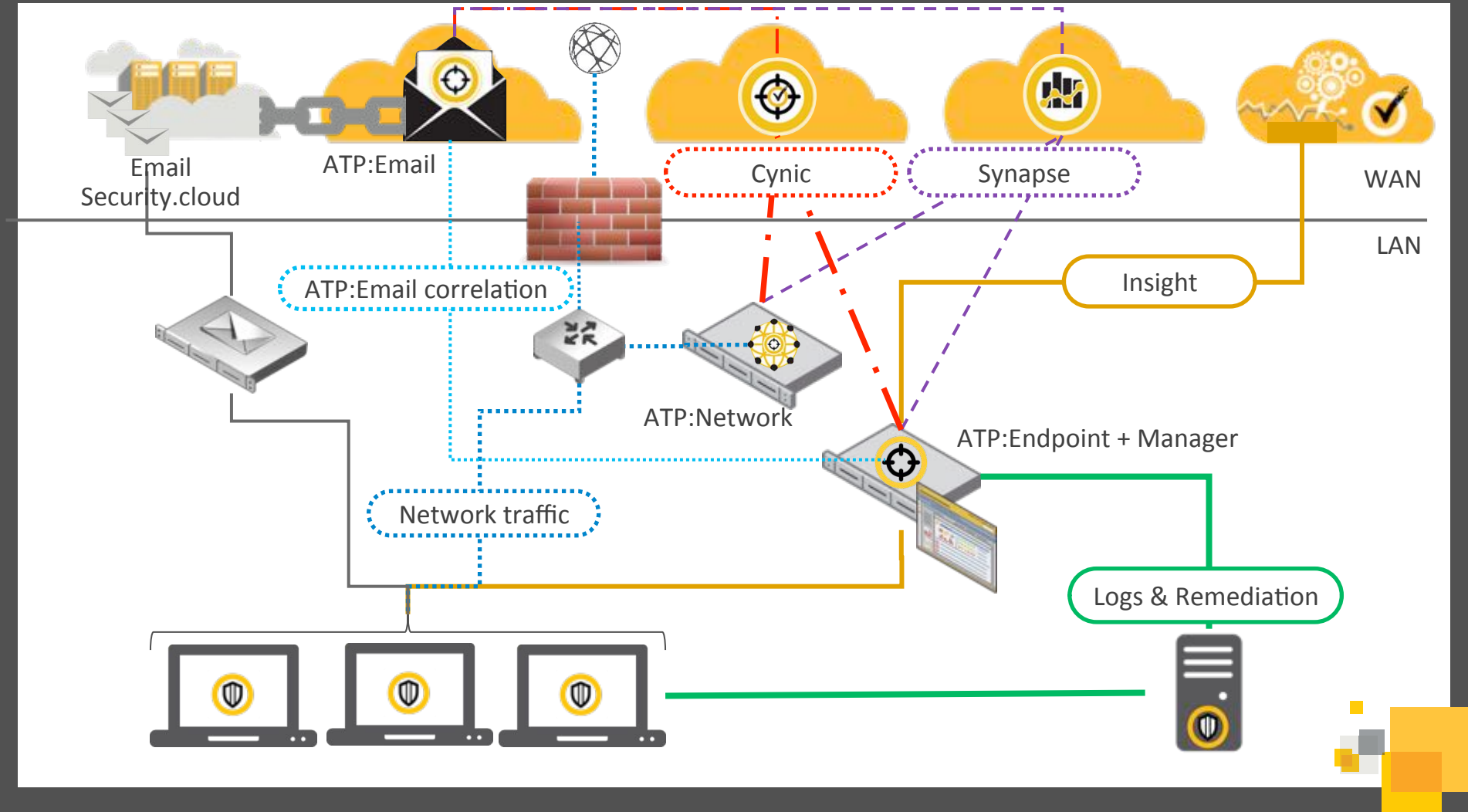

Email
Security.cloud
WAN
LAN
Insight
ATP:Endpoint + Manager
Logs & Remediation


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

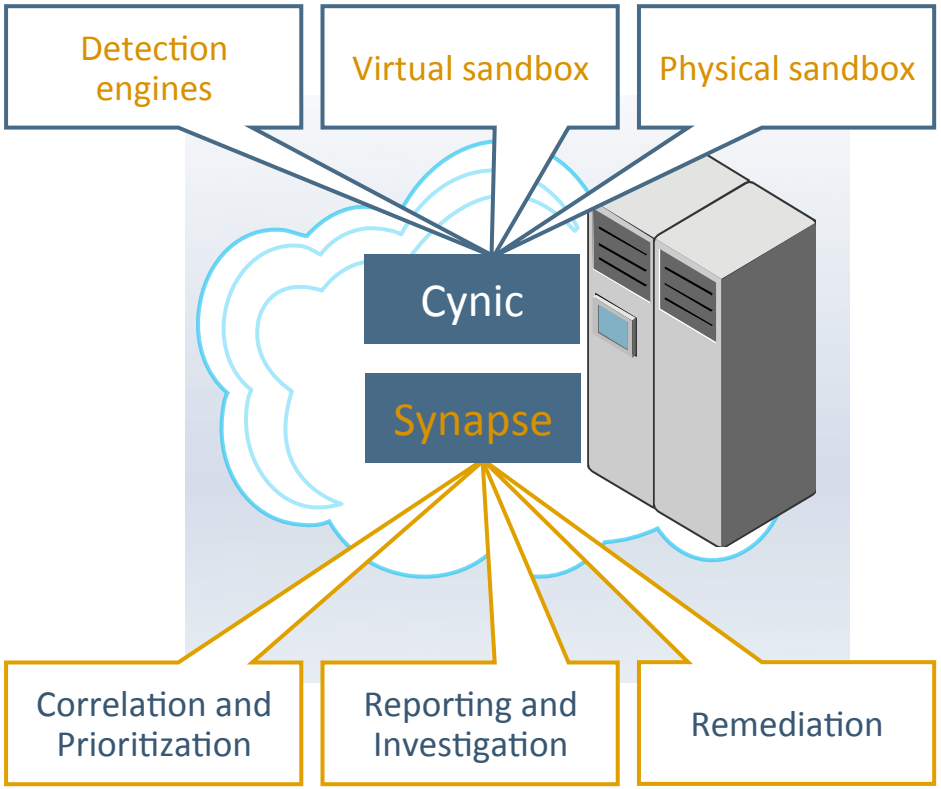

Email
Security.cloud
Synapse
WAN
LAN
Insight
ATP:Network
ATP:Endpoint + Manager
Network traffic
Logs & Remediation


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
ATP:Email correlation
Insight
ATP:Network
ATP:Endpoint + Manager
Network traffic
Logs & Remediation

Symantec Advanced Threat Protection



ATP: EMAIL

ATP: NETWORK

ATP: ENDPOINT

Copyright © 2014 Symantec Corporation

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

Premier (Value Based Services)

Remote Product Specialist (RPS)

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

Copyright © 2015 Symantec Corporation

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

Copyright © 2015 Symantec Corporation

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

Copyright © 2015 Symantec Corporation

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™