The Power of Dynamic Threat Intelligence to Stop APT's

CYSOFT

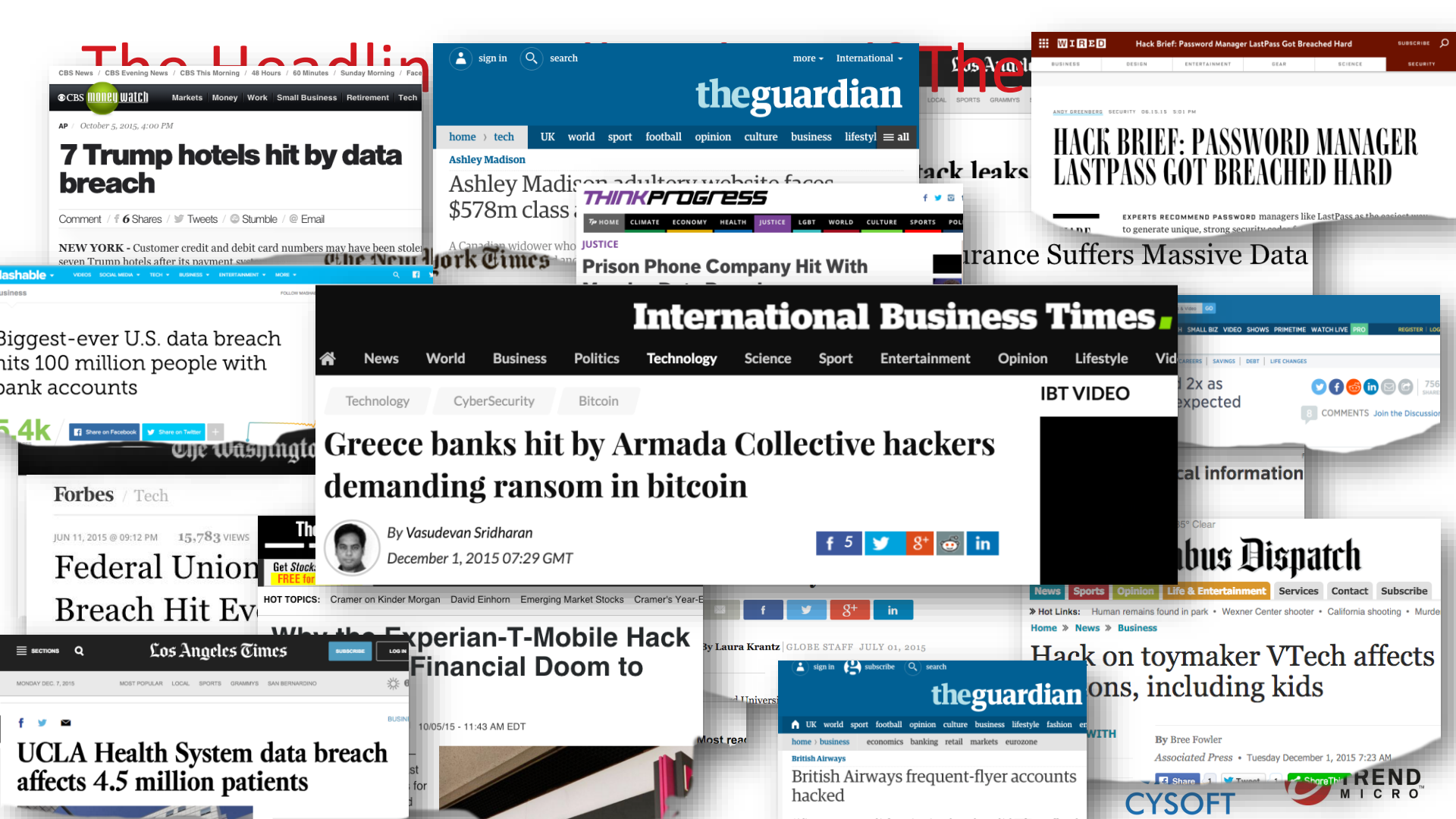
Securing Systems Effectively

TREND MICRO™

Evren BILGIC

Senior Sales Engineer, Mediterranean Region

evren_bilgic@trendmicro.com


CBS News
CBS Money Watch
Markets Money Work Small Business Retirement Tech
AP October 5, 2015, 4:00 PM
7 Trump hotels hit by data breach
Comment 6 Shares Tweets Stumble Email
NEW YORK - Customer credit and debit card numbers may have been stole
seven Trump hotels after its payment
sign in search more International
theguardian
home tech UK world sport football opinion culture business lifestyl all
Ashley Madison
Ashley Madi
$578m class
THINKPROGRESS
HOME CLIMATE ECONOMY HEALTH JUSTICE LGBT WORLD CULTURE SPORTS
JUSTICE
Prison Phone Company Hit With
WIRED
Hack Brief: Password Manager LastPass Got Breached Hard
SUBSCRIBE
BUSINESS DESIGN ENTERTAINMENT GEAR SCIENCE SECURITY
ANDY GREENBERG SECURITY 06.15.15 5:01 PM
HACK BRIEF: PASSWORD MANAGER LASTPASS GOT BREACHED HARD
EXPERTS RECOMMEND PASSWORD managers like LastPass as the easiest
to generate unique, strong security
The New York Times
rance Suffers Massive Data
Biggest-ever U.S. data breach
hits 100 million people with
bank accounts
5.4k
Share on Facebook
Share on Twitter
International Business Times
News World Business Politics Technology Science Sport Entertainment Opinion Lifestyle
Technology CyberSecurity Bitcoin
Greece banks hit by Armada Collective hackers demanding ransom in bitcoin
By Vasudevan Sridharan
December 1, 2015 07:29 GMT
IBT VIDEO
2x as
expected
COMMENTS Join the Discussion
cal information
Forbes / Tech
JUN 11, 2015 @ 09:12 PM 15,783 VIEWS
Federal Union
Breach Hit Ev
HOT TOPICS: Cramer on Kinder Morgan David Einhorn Emerging Market Stocks Cramer's Year-E
Why the Experian-T-Mobile Hack
Financial Doom to
By Laura Krantz | GLOBE STAFF JULY 01, 2015
10/05/15 - 11:43 AM EDT
Most rea
Los Angeles Times
SECTIONS
SUBSCRIBE
MONDAY DEC. 7, 2015
MOST POPULAR LOCAL SPORTS GRAMMYS SAN BERNARDINO
UCLA Health System data breach affects 4.5 million patients
sign in subscribe search
theguardian
UK world sport football opinion culture business lifestyle fashion
home business economics banking retail markets eurozone
British Airways
British Airways frequent-flyer accounts hacked
Dispatch
News Sports Opinion Life & Entertainment Services Contact Subscribe
Hot Links: Human remains found in park • Wexner Center shooter • California shooting • Murde
Home » News » Business
Hack on toymaker VTech affects
ons, including kids
By Bree Fowler
Associated Press • Tuesday December 1, 2015 7:23 AM
Share
CYSOFT
TREND MICRO

The Other Half of the Story

79%

Have network attacks or exploits

Source: Live proof of concepts – 101 customers, 2015

Today's business reality

- **75%** of attacks require little skill to execute[1]…

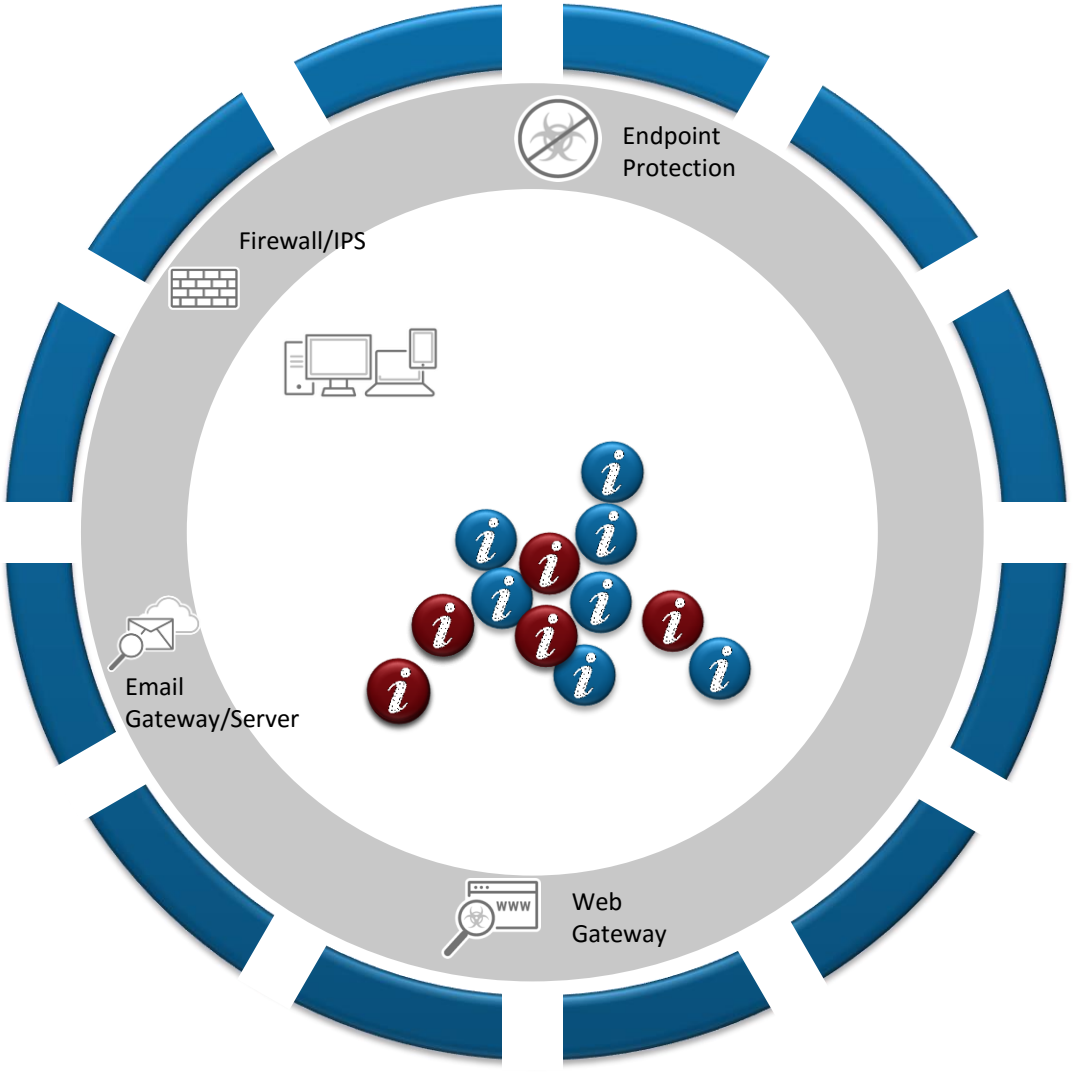
…yet require advanced skills to detect and remediate

- **63%** of security professionals believe it is only a matter of time until their enterprise is targeted[2]
- **$5.9M** is average cost of targeted attack[3]

1. Verizon
2: Source: ISACA APT Awareness Study, 2013
3. Ponemon May 2014

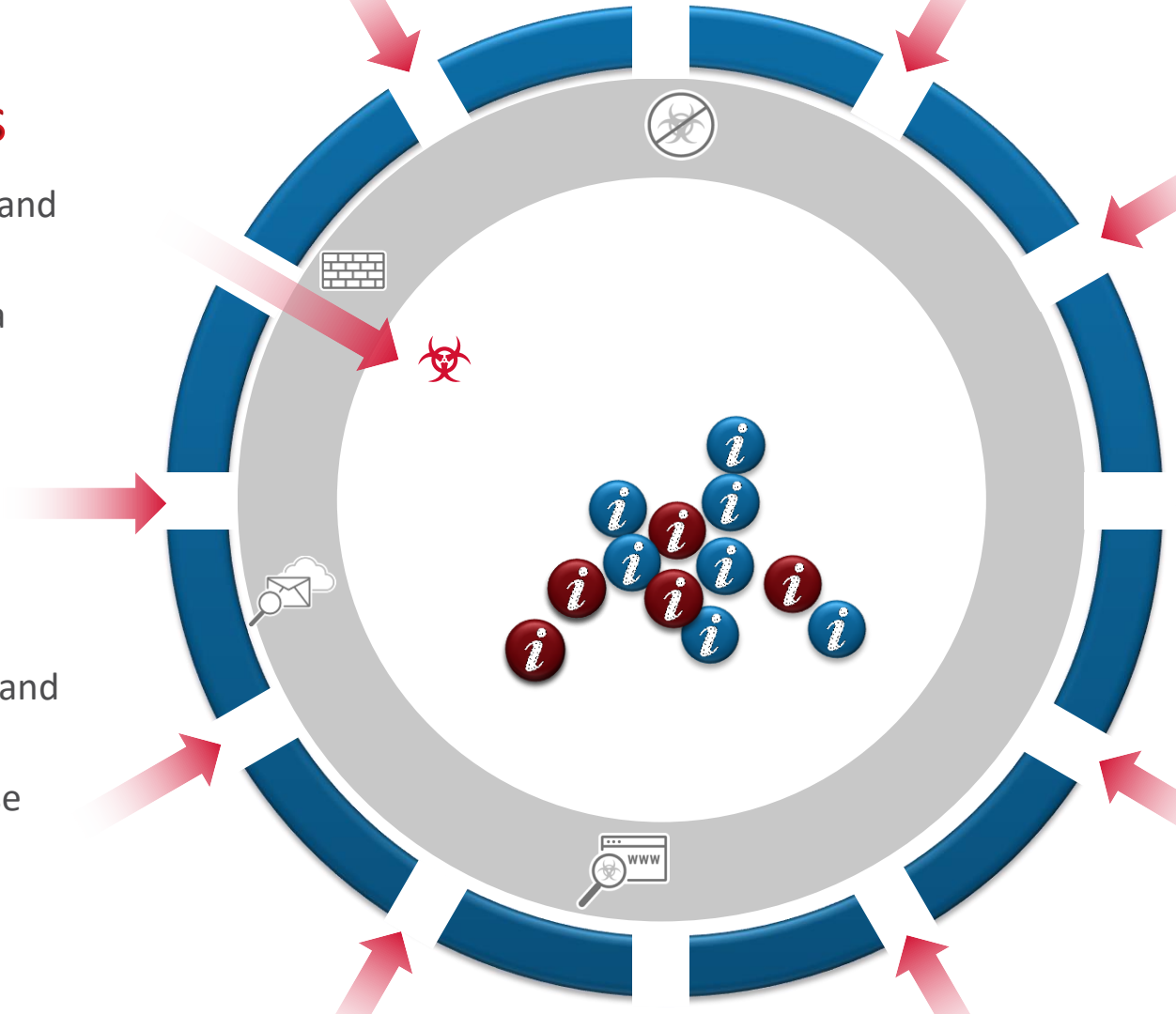
Advanced Attacks

- Problem: Data has to be moved and shared in and out.
- Traditional approaches provide a baseline



Advanced Attacks

- Problem: Data has to be moved and shared
- Traditional approaches provide a baseline
- New attacks use sophisticated methods to gain access
  - All ports, all protocols
  - Spear phishing
  - Island hopping
- Once inside, attacks can change and start stealing data.
- Tracking back and analyzing these attacks are complex and require specialized knowledge.

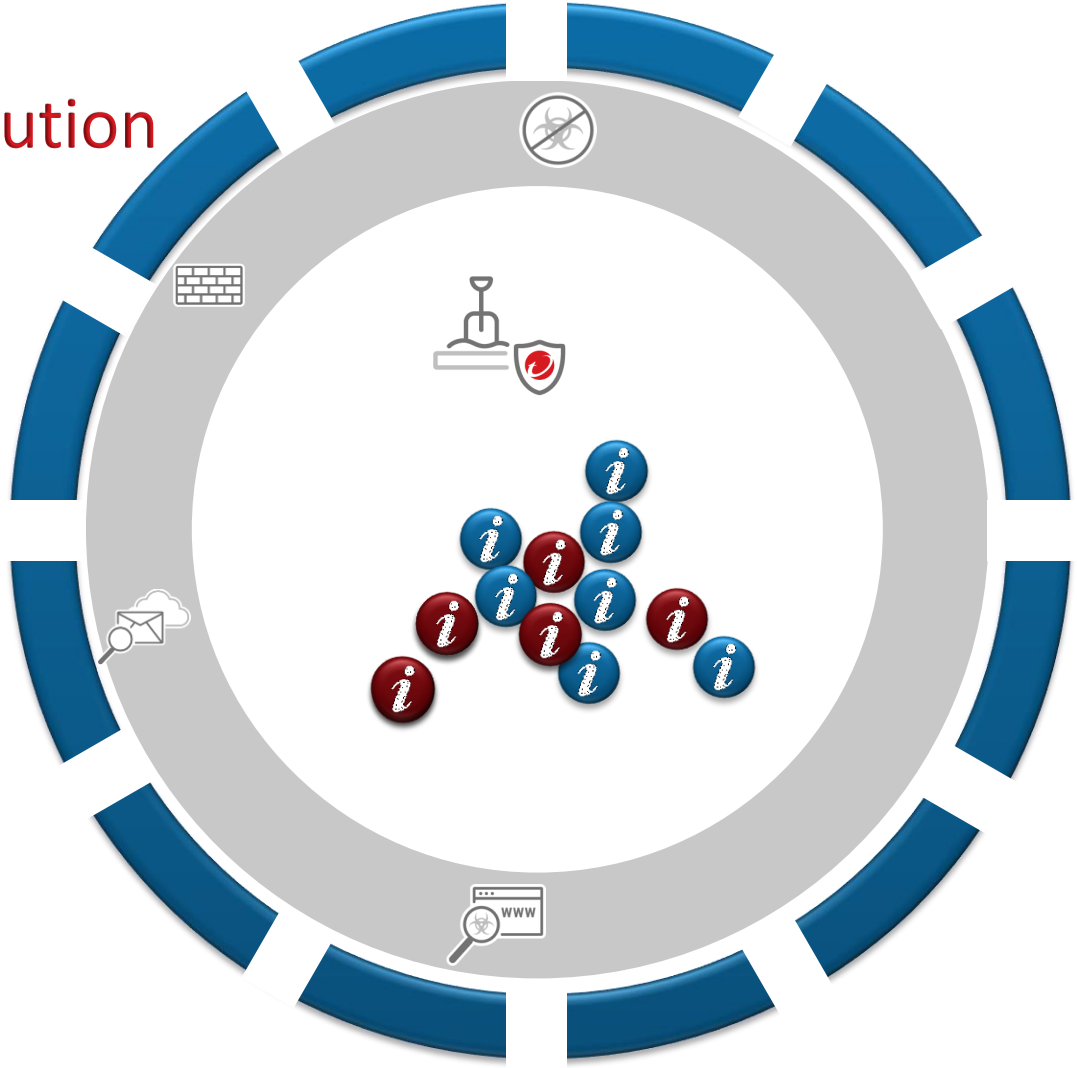


Dealing with Targeted Attacks:

- Traditional defences still work. Who can afford to replace them?
- Network sizing means organizations just need more sandboxes
- Specialized labour to analyze advanced malware is hard to find
- Time and expense reacting to advanced threats is growing

A Network Defense Solution

- Organizations need to protect and leverage existing investments in security infrastructure
- A centralized Deep Discovery solution to integrate with those existing investments extends their reach.



Deep Discovery Products

NETWORK DEFENSE

Deep Discovery Email

Deep Discovery Analyzer

Analysis of suspicious payloads and URLs with custom sandbox. Ability to share insight with both Trend Micro and third party solutions

Deep Discovery Inspector

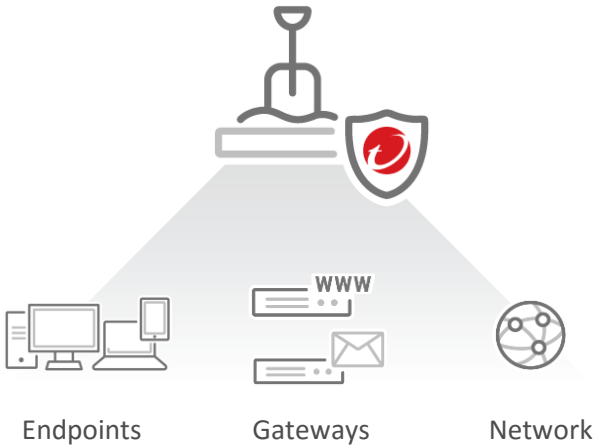
Detect targeted attacks by monitoring *all* network traffic, plus analysis of network payloads with custom sandbox

CYSOFT

TREND MICRO

Deep Discovery Analyzer

– Integrated Sandboxing Analysis



An open sandboxing analysis server to enhance the targeted attack protection of Trend Micro and 3rd party security products

- Detection of advanced malware
- Detailed analysis & reporting
- Open Web Services API
- Custom Defense IOC intelligence sharing

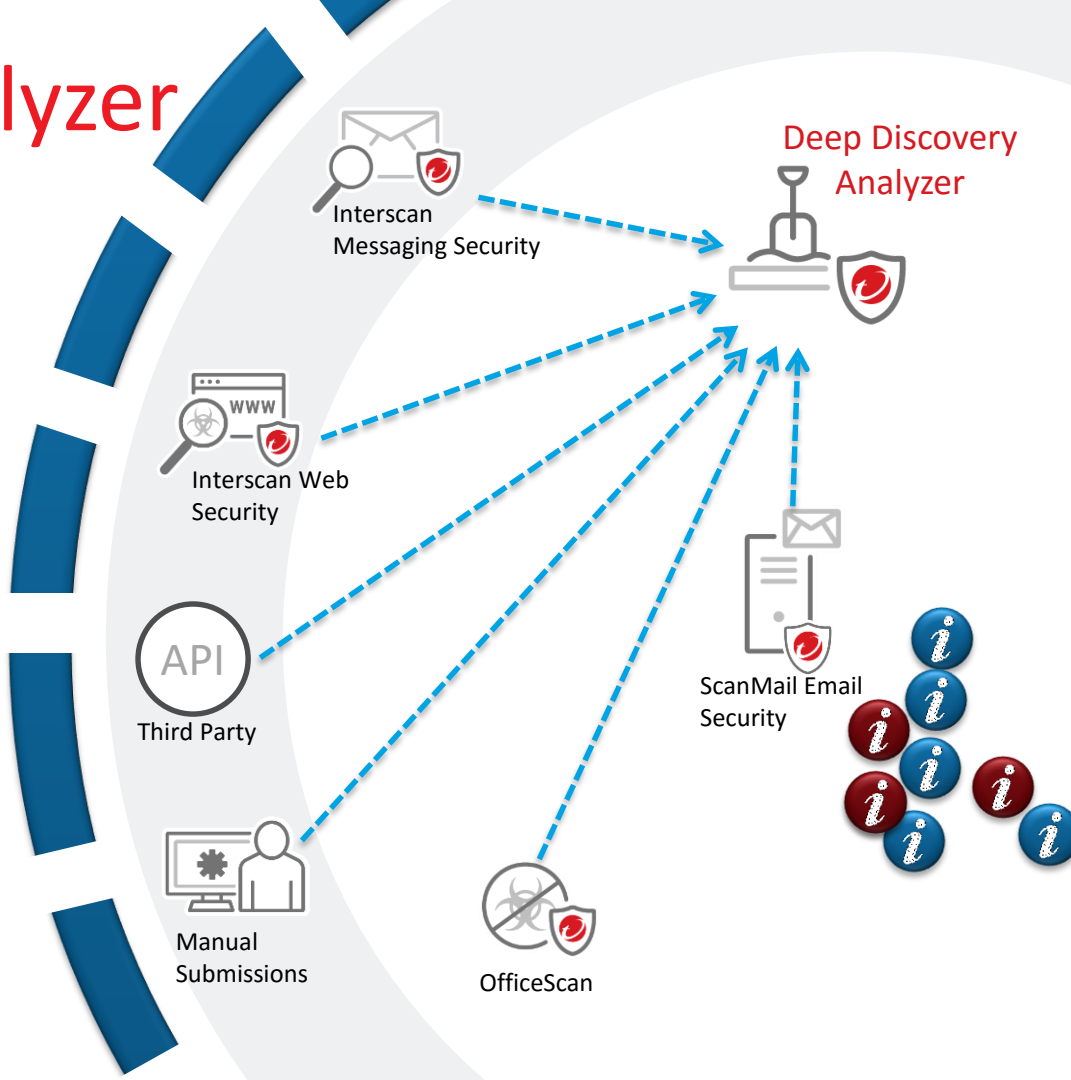
➢ ***Enhance the threat protection of your existing security investments***

Key Features

Custom Sandboxes		Custom sandbox images precisely match your desktop and server environments (language, OS, configuration) to accurately detect the threats targeting your organization vs. a standard sandbox that can be evaded.
Broad Analysis Engines		Multiple detection engines and correlation rules analyze a wide range of file types and URLs to detect all attack aspects – not just malware
Global Threat Intelligence		Real-time cloud intelligence & research powers detection accuracy and continuously updates engines and rule sets
URL and File Analysis		Integrated solution can analyze all document types, URLs and exe files.
Seamless Integration		Shared IOC data from new sandbox detections updates Trend Micro and 3rd party products to create a real-time custom defense

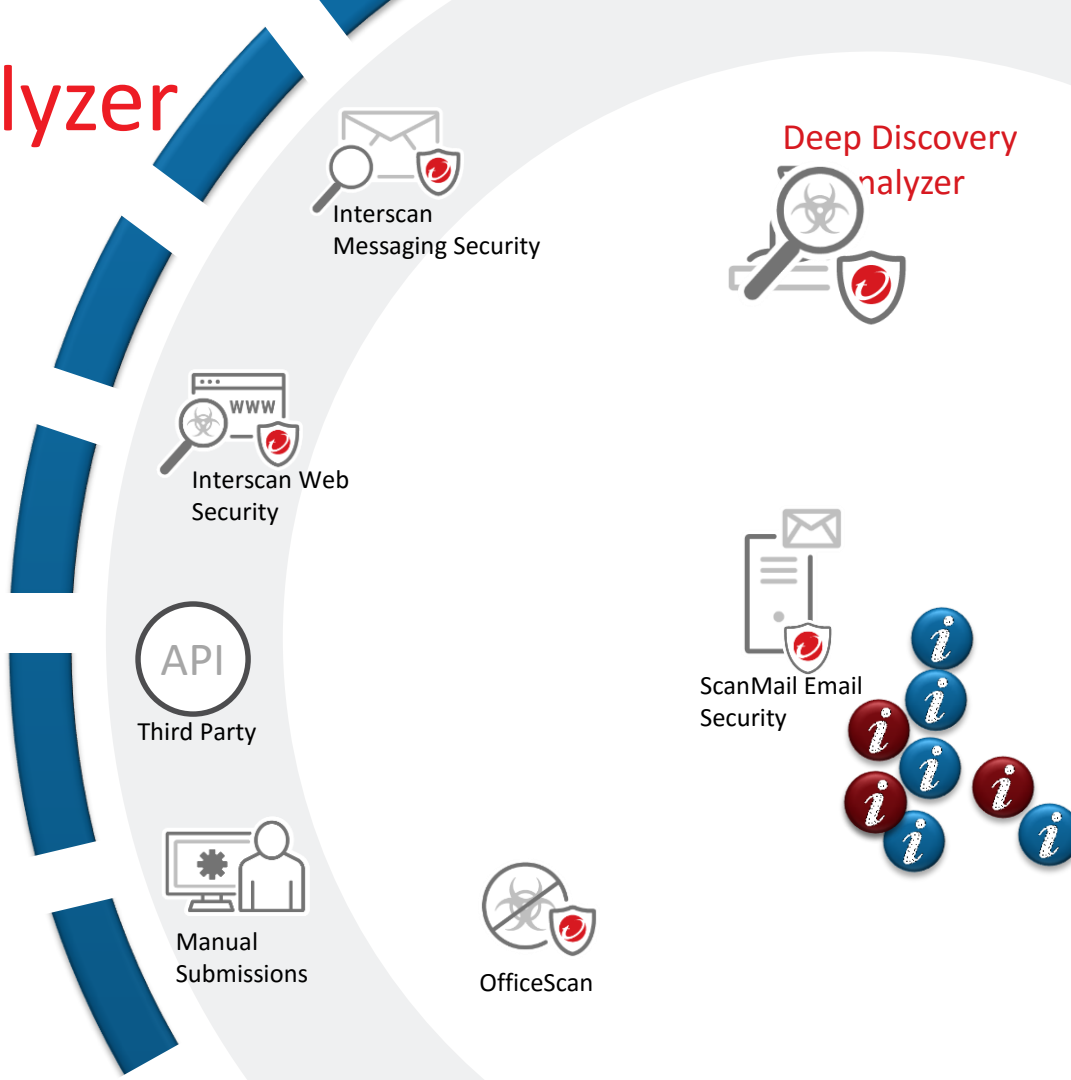
Deep Discovery Analyzer

- Suspicious objects that are discovered by InterScan and Scanmail Security products are sent to Analyzer sandbox
- OfficeScan will also be able to send suspicious objects
- Analyzer offers a Web API that allows third party products to submit to Analyzer
- System administrators also have the ability to manually submit samples



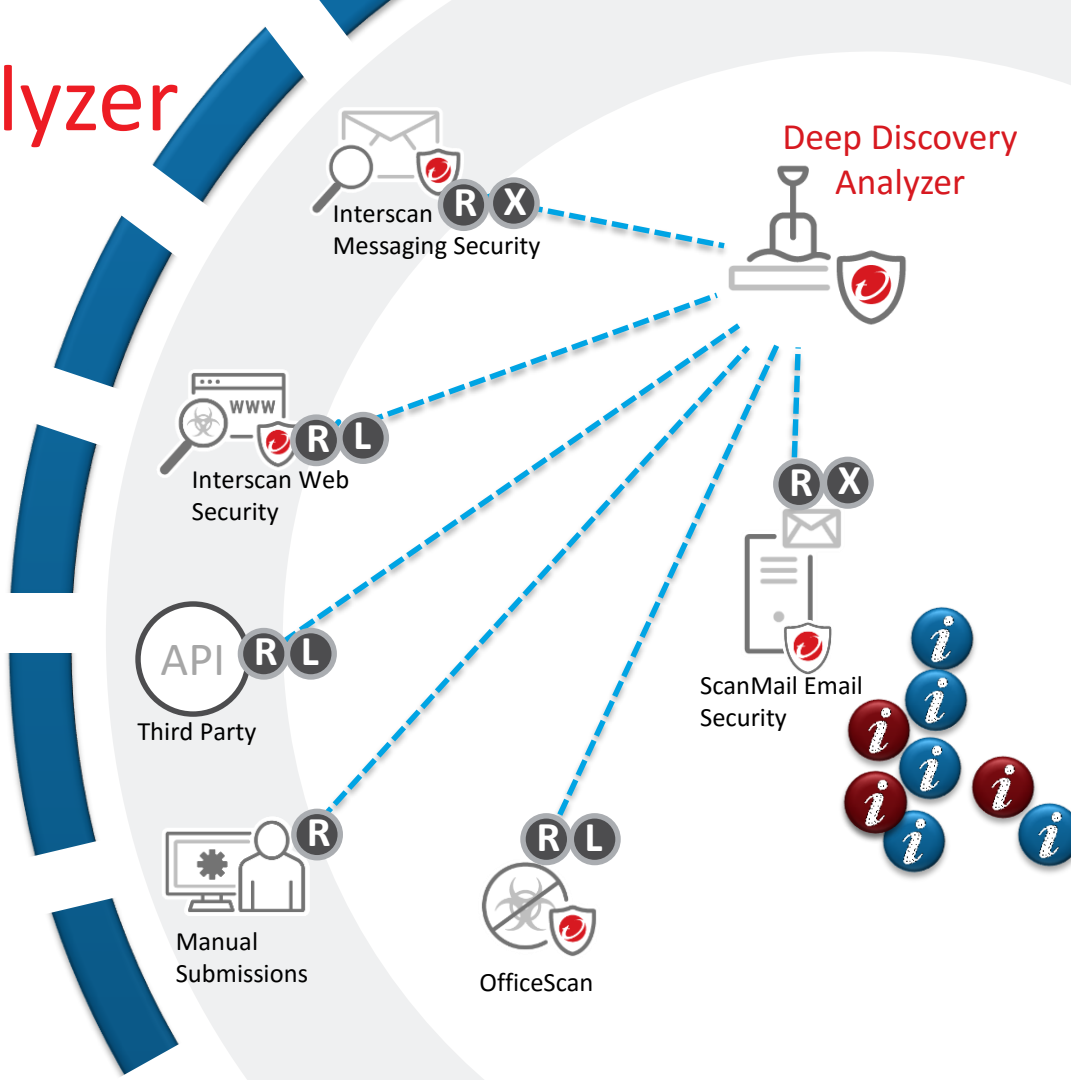
Deep Discovery Analyzer

- Suspicious URLs, Files, and exe files are executed in the Deep Discovery Analyzer and analyzed for:
  - Advanced malware
  - Command and Control (C&C)
  - Anti-security, self-preservation
  - Autostart or other system configuration
  - Deception, social engineering
  - File drop, download, sharing or replication
  - Hijack, redirection, or data theft
  - Malformed, defective or with known malware traits
  - Process, service or memory object change
  - Rootkit, cloaking
  - Suspicious network or messaging activity
  - Other threat characteristics



Deep Discovery Analyzer

- Results/Reports are sent back to requesting system.
  - Based on risk score
  - Highly configurable
- In some cases black lists are automatically updated such that similar attacks in future are thwarted.
- Emails can be blocked in real time



R Reporting

L Black List / Patterns / IOCs

X Email Blocking

Top 3 Solution Differentiators

Smart
Better detection

Simple
Low cost to deploy & manage

Security that fits
Fits evolving ecosystem & enables sharing of intelligence across solution areas

Smart

Proven detection of targeted attacks

TREND MICRO™ DEEP DISCOVERY

MOST EFFECTIVE

recommended breach detection system

2 YEARS RUNNING

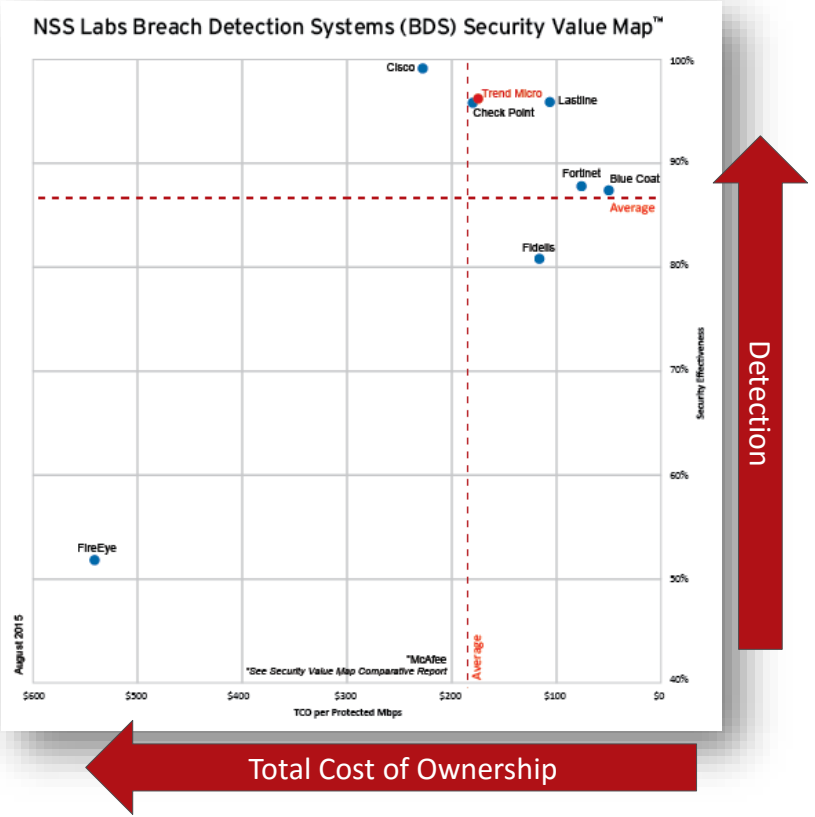
NSS LABS RECOMMENDED

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

ICSA Labs
Advanced Threat Defense

Certified

Test Period:	Q4 2015
Certified Since:	12 / 2015



Simple

Low cost to deploy & manage

- Single centralized appliance that seamlessly integrates into existing infrastructure with a common management console
- Highly visual, interactive web interface offers the most relevant threat intelligence at your fingertips
- Zero-cost access to the Trend Micro Smart Protection Network (global threat intelligence)

Security That Fits

Fits evolving ecosystem & enables sharing of threat intelligence across solution areas

- Integration with existing security investments
- Automatic threat intelligence sharing with Trend Micro products
- Sharing of threat intelligence with other security products

Targeted Attack Simulation Game

http://targetedattacks.trendmicro.com

CYSOFT

TREND MICRO

Securing Systems Effectively

TREND MICRO™

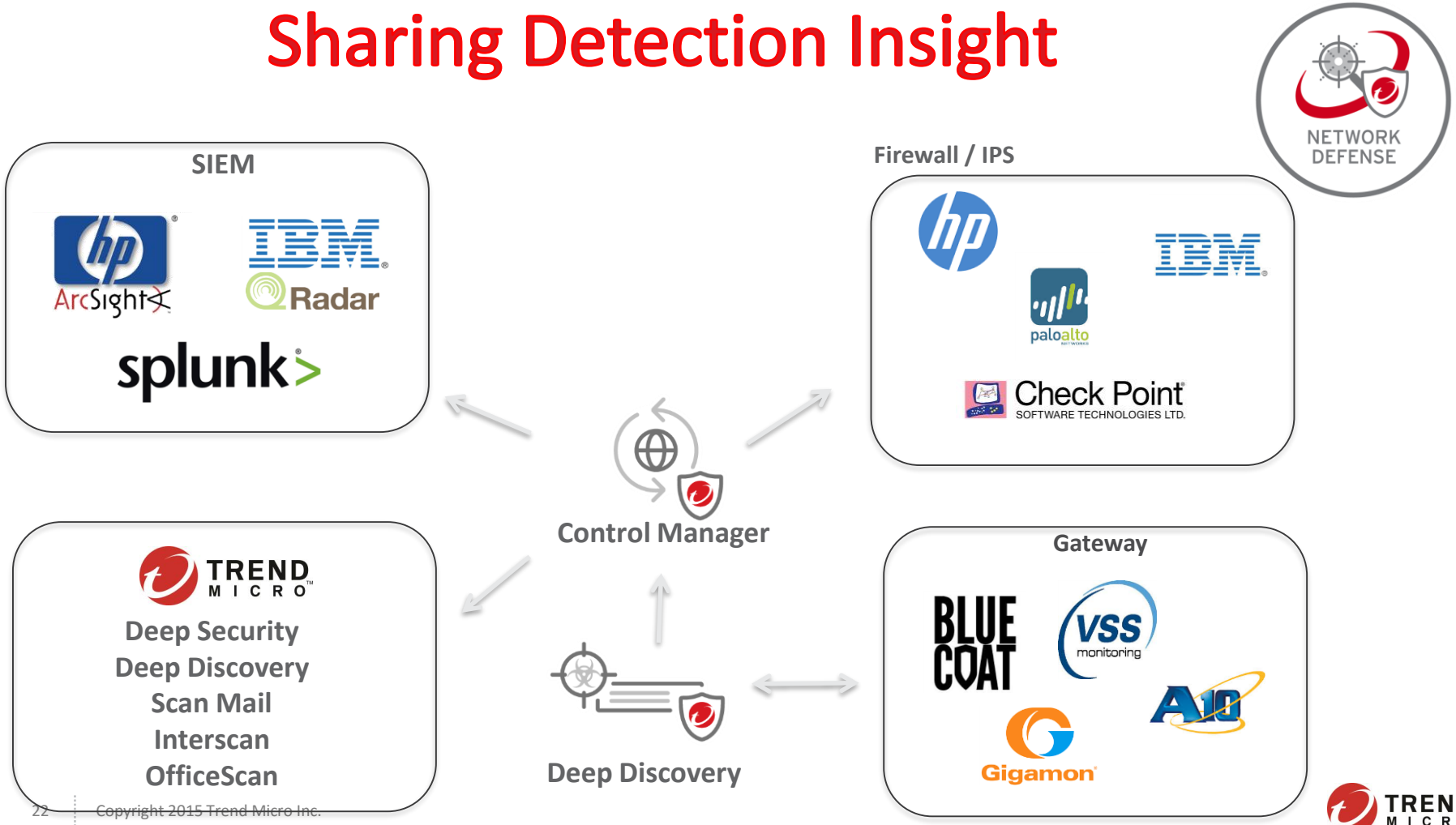
Thanks..

We are at Olympia Hall, Booth O17

Ευχαριστώ..

Back-up Slides

Sharing Detection Insight



Trend Micro: Connected Threat Defense

Enable rapid response through delivery of real-time signatures and security updates

Assess potential vulnerabilities and proactively protect endpoints, servers and applications

Analyze risk and nature of attack and attacker, and assess impact of threats retrospectively

Detect advanced malware, behavior and communications invisible to standard defenses