Advanced Threat Protection

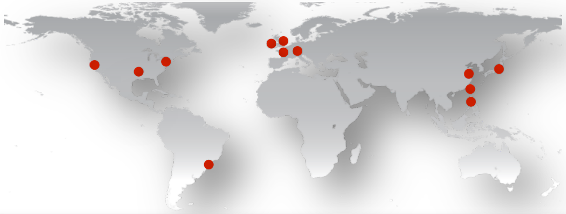
Veli-Pekka Kusmin
Senior Sales Engineer
6.11.2014

A world **safe** for exchanging digital information

CEO	Eva Chen
Founded	1988, United States
Headquarters	Tokyo, Japan
Employees	5,217
Offices	36
2013 Sales	$1.1B USD

New malware every ½ second

Global Threat Intelligence
- 1,200+ experts worldwide



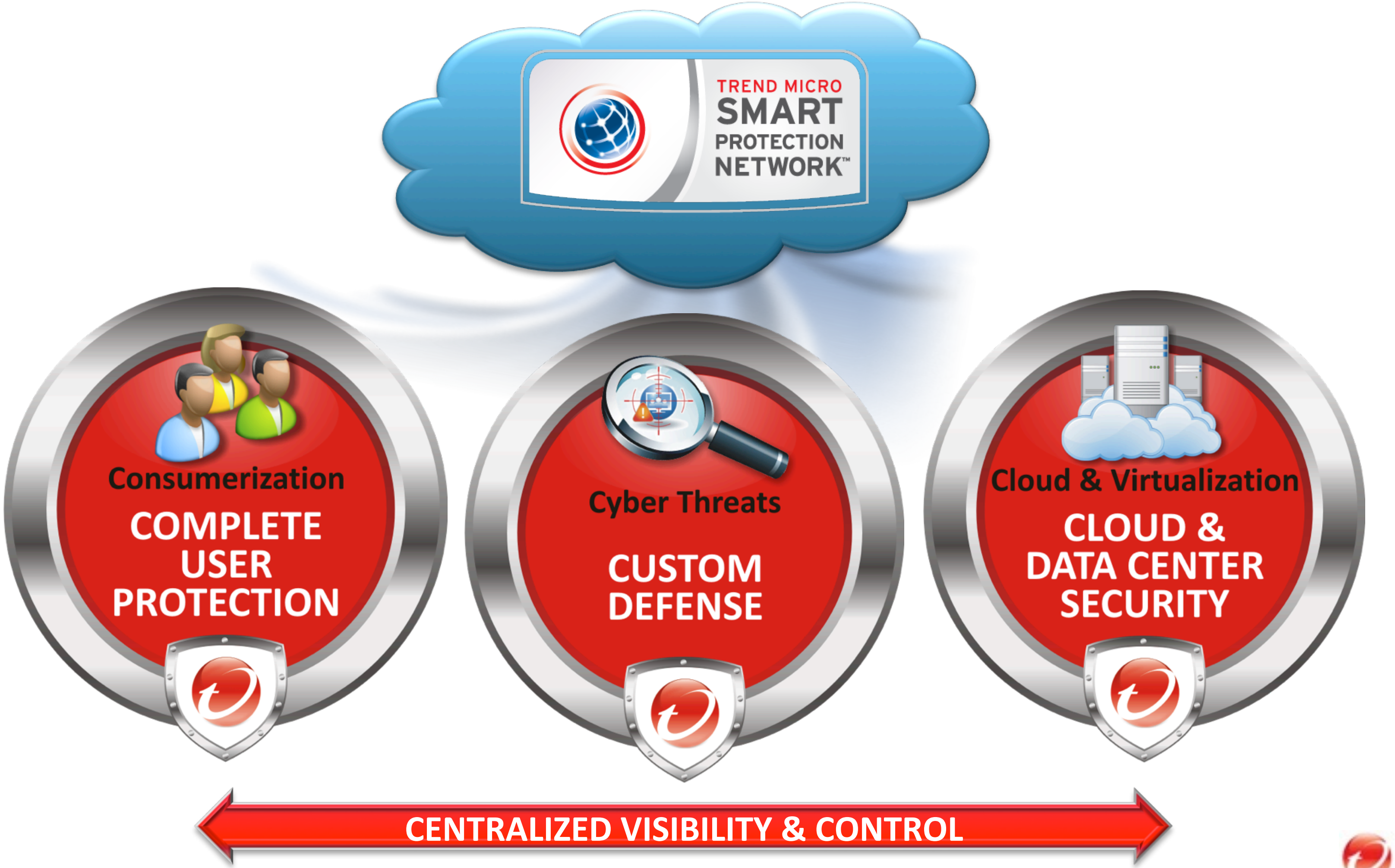
96% of the top 50 global corporations.

100% of the top 10 automotive companies.

100% of the top 10 telecom companies.

80% of the top 10 banks.

90% of the top 10 oil companies.



TREND MICRO SMART PROTECTION NETWORK™

Consumerization

COMPLETE USER PROTECTION

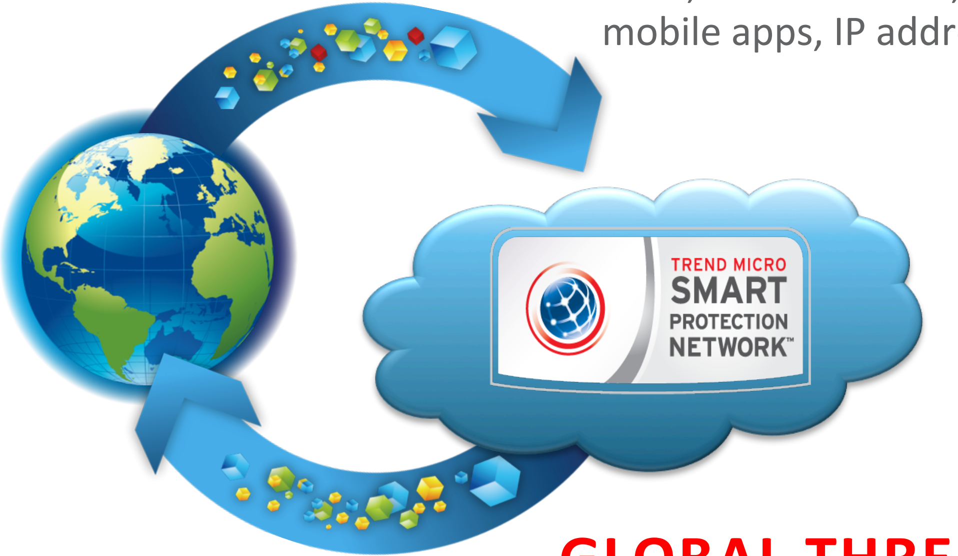
Cyber Threats

CUSTOM DEFENSE

Cloud & Virtualization

CLOUD & DATA CENTER SECURITY

CENTRALIZED VISIBILITY & CONTROL



COLLECTS VIA GLOBAL SENSORNET

- Honeypots, customers, threat researchers, community…
- Over 300M nodes; 8.6B threat events daily
- URLs, vulnerabilities, files, domains, network traffic, threat actors, mobile apps, IP addresses, exploit kits

BIG DATA ANALYTICS

- Identifies using data mining, machine learning, modeling and correlation
- 100 TB data; 500K unique threats identified daily

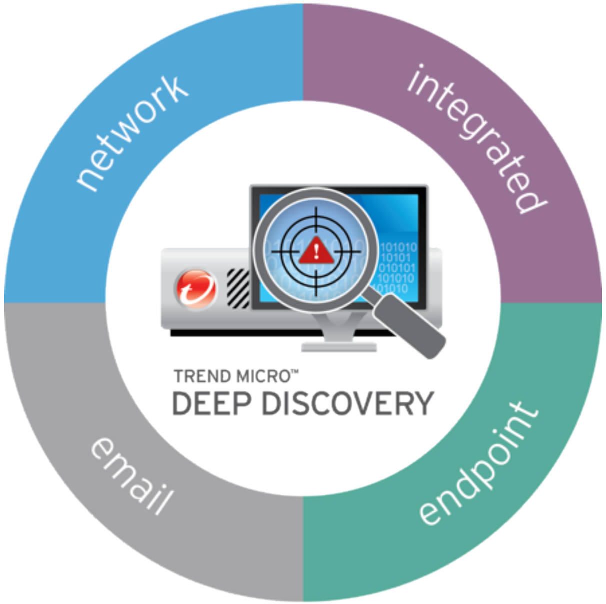
GLOBAL THREAT INTELLIGENCE

- 250M threats blocked daily
- Email reputation, file reputation, web reputation, network traffic rules, mobile app reputation, known vulnerabilities/exploits, threat actor research, C&C…

Deep Discovery

Advanced Threat Protection Platform

NSS LABS RECOMMENDED
Trend Micro™ Deep Discovery
TOP SCORE
in breach detection
NSS Labs 2014 Breach Detection Tests



Deploy protection where it matters most to your organization

Defends against targeted attacks invisible to standard security products

- Advanced malware
- Command & Control communication
- Attacker activity and lateral movement

Detect, Analyze & Respond To Targeted Attacks

Deep Discovery Products

Network-wide attack detection

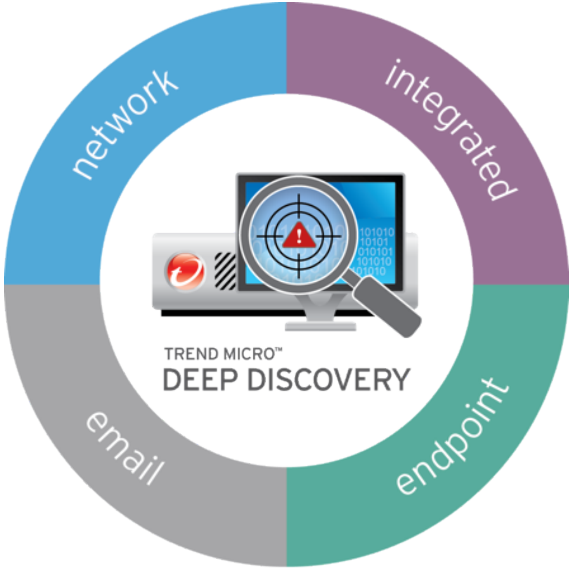
Inspector

Detect and analyze targeted attacks anywhere on your network

Analyzer

Integrated sandboxing

Improve the threat protection of your existing security investments



Email attack protection

Email Inspector

Stop the targeted attacks that can lead to a data breach

Endpoint Sensor

Endpoint Investigation

Investigate & respond to attacks with network detection + endpoint intelligence

Deploy protection where it matters most to your organization

Key Technologies

Specialized Detection Engines

Multiple detection engines and correlation rules analyze a wide range of traffic to detect all attack aspects – not just malware

Virtual Analyzer

Custom sandbox images precisely match your system configurations to accurately detect the threats targeting your organization

Global Threat Intelligence

Real-time cloud intelligence & research powers detection accuracy and continuously updates engines and rule sets (SPN)

Threat Connect Portal

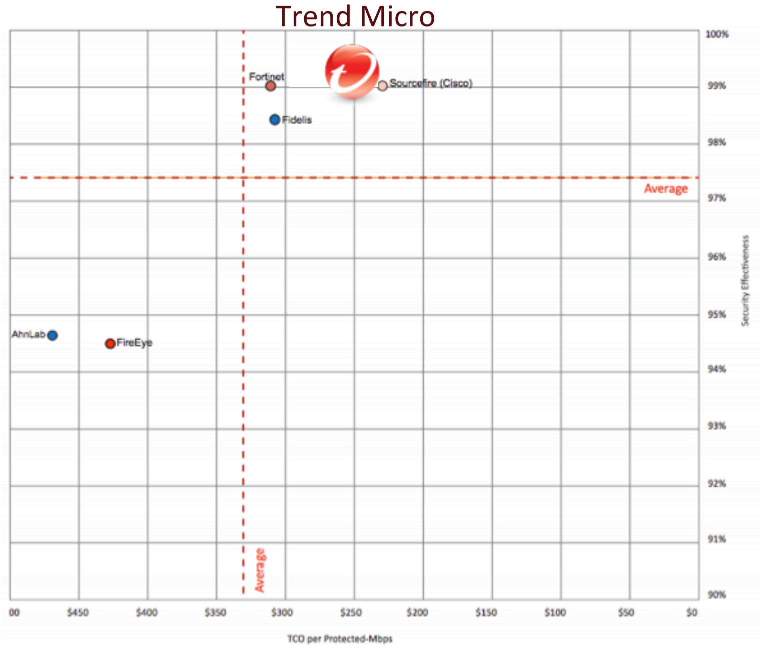
Integrated portal delivers Smart Protection Network & research intel relevant to your attack – malware profiles, C&C networks, and more

Custom Defense Integration

Shared IOC data from new sandbox detections updates Trend Micro and 3rd party products to create a real-time custom defense

NSS LABS
RECOMMENDED

Top Score in Breach Detection
2014 NSS Labs Breach Detection Tests



NSS LABS RECOMMENDED

Trend Micro™ Deep Discovery
TOP SCORE
in breach detection

NSS Labs 2014 Breach Detection Tests

NSS LABS RECOMMENDED

Trend Micro™ Deep Discovery
25% LOWER TCO
vs vendor average

NSS Labs 2014 Breach Detection Tests

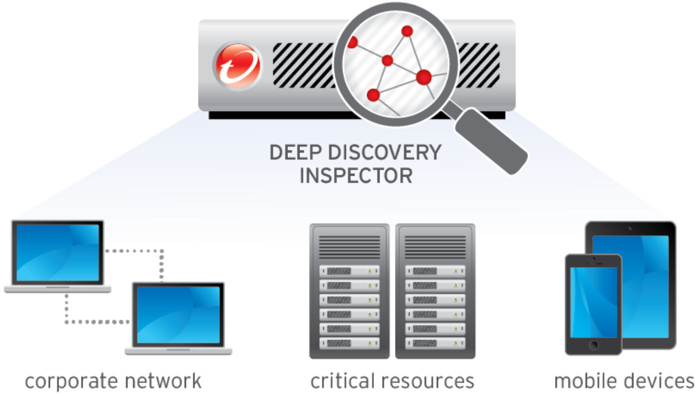
Product				Breach Detection	NSS Tested Throughput
Trend Micro Deep Discovery Inspector Model 1000 v3.5				99.1%	1,000 Mbps
HTTP Malware	Email Malware	Exploits	Stability and Reliability	Evasions	False Positive Rate
97%	100%	100%	PASS	94%	0%

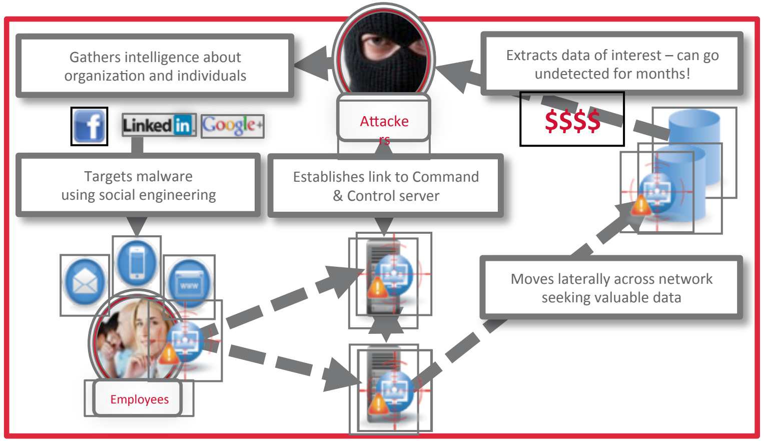
TREND MICRO

Deep Discovery Inspector

Deep Discovery Inspector

– Network-Wide Attack Detection




Gathers intelligence about organization and individuals
Linkedin
Google+
Attacke rs
Extracts data of interest – can go undetected for months!
$$$$
Targets malware using social engineering
Establishes link to Command & Control server
Moves laterally across network seeking valuable data
Employees

- *Web, Email, 80+ Protocols & Apps*
- *Inbound – Outbound – Internal Traffic*
- *Integrated Custom Defense solution*

⊖ Advanced Malware

⊖ C&C Communication

⊖ Attacker Activity

Deep Discovery Inspector

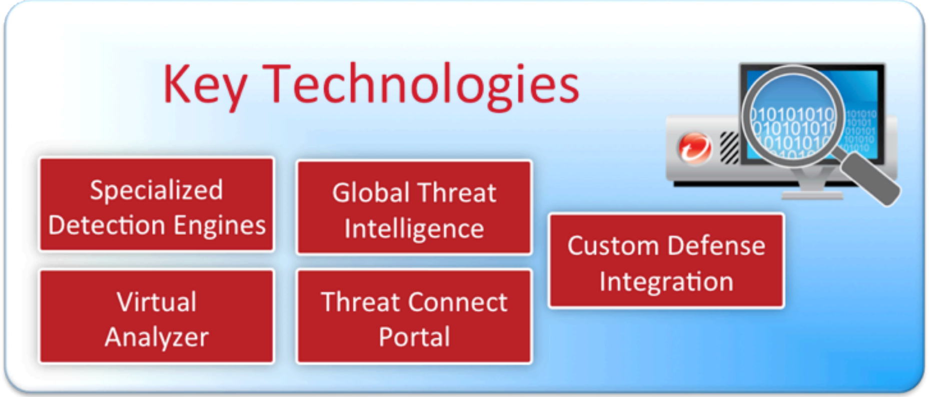
Network-Wide Attack Detection

NSS LABS RECOMMENDED

Trend Micro™ Deep Discovery
TOP SCORE
in breach detection

NSS Labs 2014 Breach Detection Tests

- Single appliance
- Detection across all network traffic
  - Malware, C&C, attacker activity across 80+ protocols and all ports
- Custom sandboxing analysis provides more accurate detection


Key Technologies
Specialized Detection Engines
Global Threat Intelligence
Custom Defense Integration
Virtual Analyzer
Threat Connect Portal

- Global threat intelligence drives rapid assessment and response
- Handles BYOD and other complex environments
  - Detection beyond Windows: mobile, Mac, Android, legacy systems and specialty devices…

Deep Discovery Technologies

Entry point

Lateral Movement

Exfiltration

360°Approach

- Content Inspection
- Document Emulation
- Payload Download
- Behavior Tracing
- Exploit Detection
- Network Monitoring

Network Content Inspection Engine

Advanced Threat Security Engine

IP & URL reputation

Virtual Analyzer

Network Content Correlation Engine

More than
80 protocols analyzed

HTTP SMTP DNS FTP

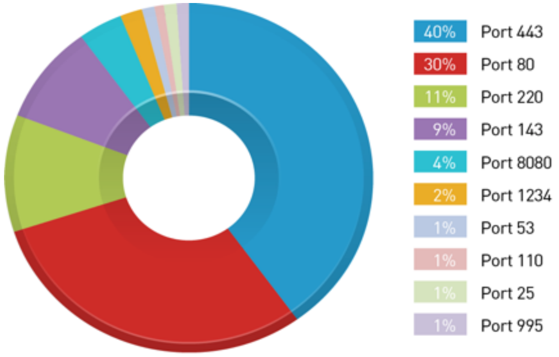
CIFS SQL P2P -----

Embedded doc exploits
Drive-by downloads
Dropper
Unknown Malware
C&C access
Data stealing
Worms/Propagation
Backdoor activities
Data exfiltration…

The Need for 360 Degree Detection

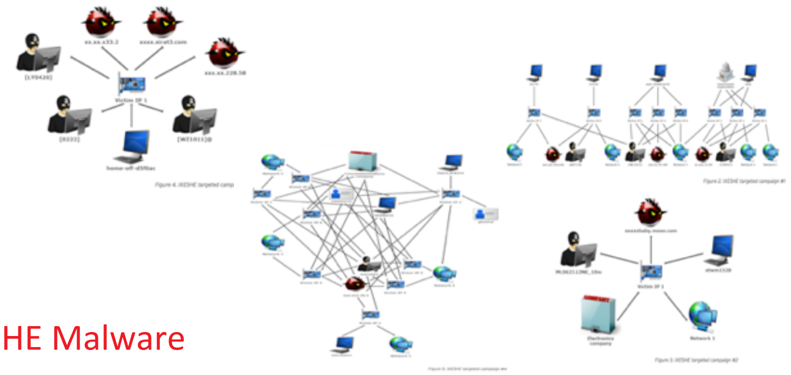
Attackers use a changing variety of protocols, applications, ports, C&C addresses to evade detection

Poison Ivy



www
POP3
SMTP
IMAP
msn

EvilGrab Malware



IXESHE Malware

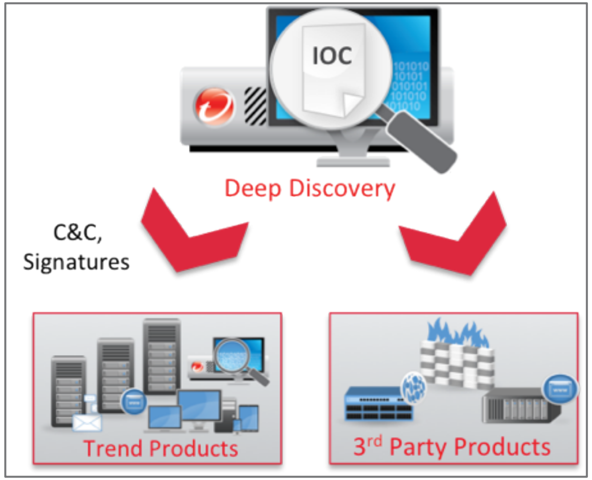
How Deep Discovery Detection Works

	Attack Detection	Detection Methods
Advanced Malware	• Zero-day & known malware • Emails containing embedded document exploits • Drive-by downloads	• Decode & decompress embedded files • Custom sandbox simulation • Browser exploit kit detection • Malware scan *(Signature & Heuristic)*
C&C Communication	• C&C communication for all malware: bots, downloaders, data stealing, worms, blended… • Backdoor activity by attacker	• Destination analysis (URL, IP, domain, email, IRC channel, …) via dynamic blacklisting, white listing • Smart Protection Network reputation of all requested and embedded URLs • Communication fingerprinting rules
Attacker Activity	• Attacker activity: scan, brute force, tool download , … • Data exfiltration • Malware activity: propagation, downloading, spamming, …	• Rule-based heuristic analysis • Extended event correlation and anomaly detection techniques • Behavior fingerprinting rules

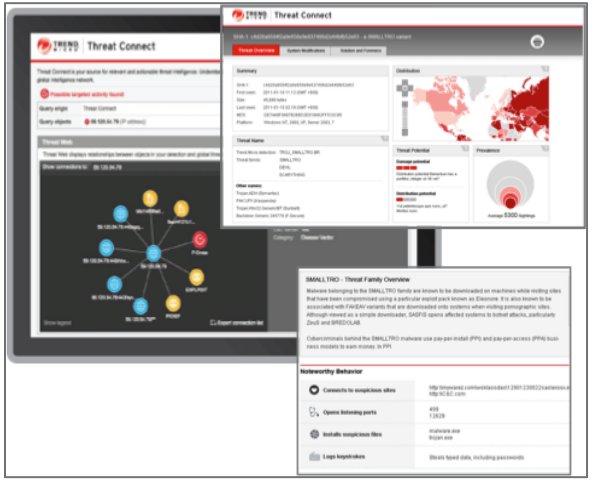
Monitoring 80+ protocols and applications across all network ports

Responding to an Attack

Adapt Security, Analyze Threat, Fully Assess & Remediate



Custom Defense
IOC Sharing



Threat Name: Trend Micro detection: TROJ_SMALLTRO.BR; Threat family: SMALLTRO, DEVIL, SCARYTHING

Other names: Trojan.ADH (Symantec); Trojan-PWS.Win32 Generic!BT (Sunbelt); Backdoor.Generic.345776 (F-Secure)

SMALLTRO - Threat Family Overview

Malware belonging to the SMALLTRO family are known to be downloaded on machines while visiting sites that have been compromised using a particular exploit pack known as Eleonore. It is also known to be associated with FAKEAV variants that are downloaded onto systems when visiting pornographic sites. Although viewed as a simple downloader, SASFIS opens affected systems to botnet attacks, particularly ZeuS and BREDOLAB.

Cybercriminals behind the SMALLTRO malware use pay-per-install (PPI) and pay-per-access (PPA) business models to earn money. In PPI

Noteworthy Behavior

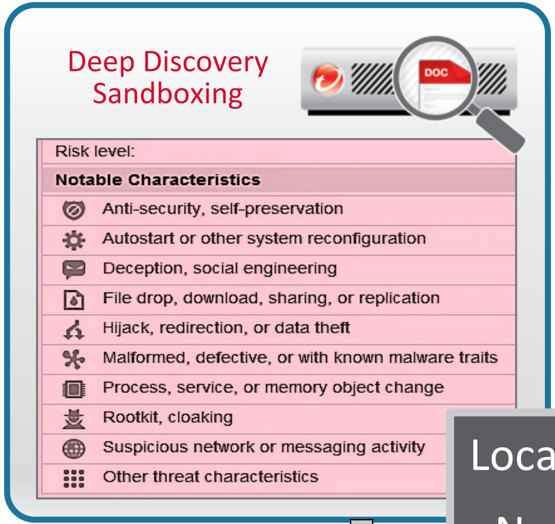
Connects to suspicious sites	http://mywarez.com/wsklaosdasl12901230022sasleroso.e http://lC6C.com
Opens listening ports	499 12629
Installs suspicious files	malware.exe trojan.exe
Logs keystrokes	Steals typed data, including passwords

Threat Connect
Portal

Deep Discovery
Endpoint Sensor

Custom Defense IOC Sharing

Updates Trend Micro and 3rd party security products to prevent further attack.



Deep Discovery Sandboxing

Risk level:

Notable Characteristics

- Anti-security, self-preservation
- Autostart or other system reconfiguration
- 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

New IOC intelligence from analysis

Local Blacklist:

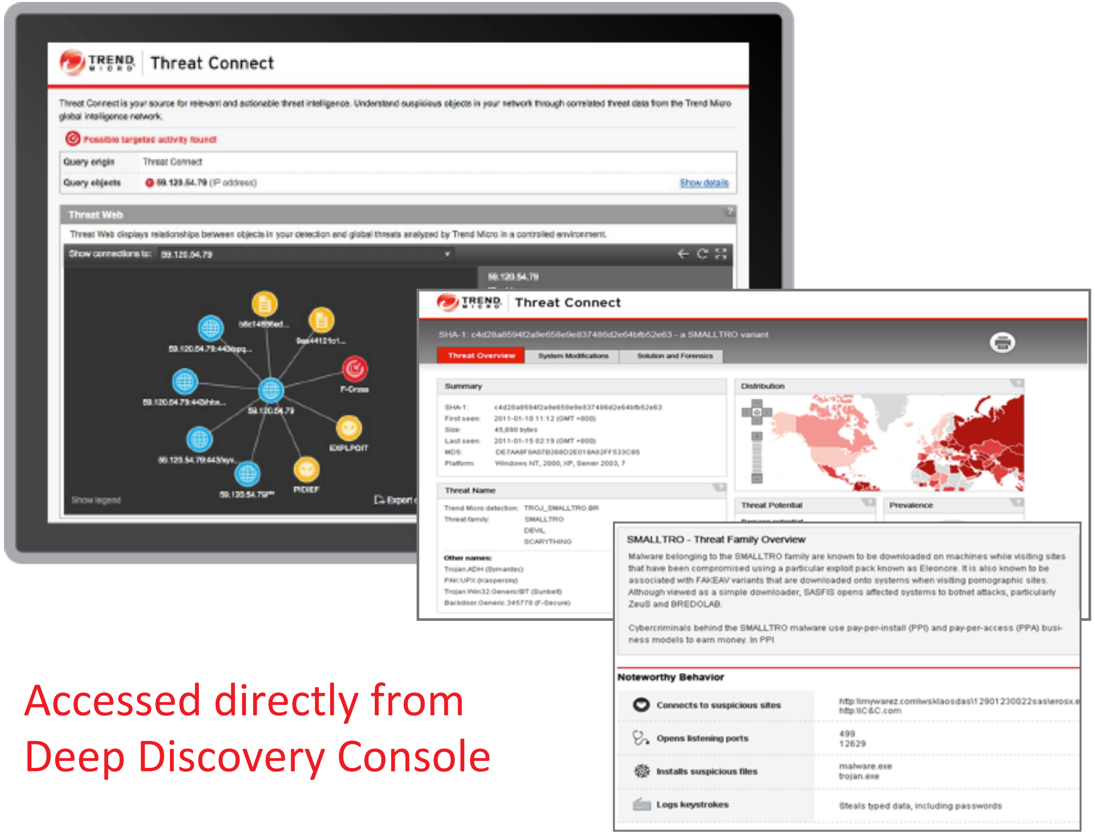
- New C&C addresses
- Malware hash id
- Additional (planned)

Control Manager

Trend Products

3rd Party Products

Threat Connect Portal



TREND MICRO | Threat Connect

Threat Connect is your source for relevant and actionable threat intelligence. Understand suspicious objects in your network through correlated threat data from the Trend Micro global intelligence network.

Possible targeted activity found

Query origin	Threat Connect	
Query objects	59.120.54.79 (IP address)	Show details

Threat Web

Threat Web displays relationships between objects in your detection and global threats analyzed by Trend Micro in a controlled environment.

Show connections to: 59.120.54.79

TREND MICRO | Threat Connect

SHA-1: c4d28a8594f2a9e658e9e837486d2e64bfb52e63 - a SMALLTRO variant

Summary

SHA-1:	c4d28a8594f2a9e658e9e837486d2e64bfb52e63
First seen:	2011-01-10 11:12 (GMT +800)
Size:	45,690 bytes
Last seen:	2011-01-15 02:19 (GMT +800)
MD5:	DE7AA9F8A07B268D2E018A82FF533C85
Platform:	Windows NT, 2000, XP, Server 2003, 7

Distribution

Threat Name

Trend Micro detection:	TROJ_SMALLTRO.BR
Threat family:	SMALLTRO DEVIL SCARYTHING

Other names:

Trojan.ADH (Symantec)
PAK:UPX (Kaspersky)
Trojan.Win32.Generic!BT (Sunbelt)
Backdoor.Generic.345778 (F-Secure)

Threat Potential

Prevalence

SMALLTRO - Threat Family Overview

Malware belonging to the SMALLTRO family are known to be downloaded on machines while visiting sites that have been compromised using a particular exploit pack known as Eleonore. It is also known to be associated with FAKEAV variants that are downloaded onto systems when visiting pornographic sites. Although viewed as a simple downloader, SASFIS opens affected systems to botnet attacks, particularly ZeuS and BREDOLAB.

Cybercriminals behind the SMALLTRO malware use pay-per-install (PPI) and pay-per-access (PPA) business models to earn money. In PPI

Noteworthy Behavior

Connects to suspicious sites	http://mywarez.com/wsklaosdas/12901230022saslerosx.e http://C&C.com
Opens listening ports	499 12629
Installs suspicious files	malware.exe trojan.exe
Logs keystrokes	Steals typed data, including passwords

Accessed directly from Deep Discovery Console

Threat profile: What are the characteristics, origins and variants of this malware.

Related IPs/Domains: What are the known C&C comms for this attack.

Attack Group/Campaign: Who and what is behind this threat.

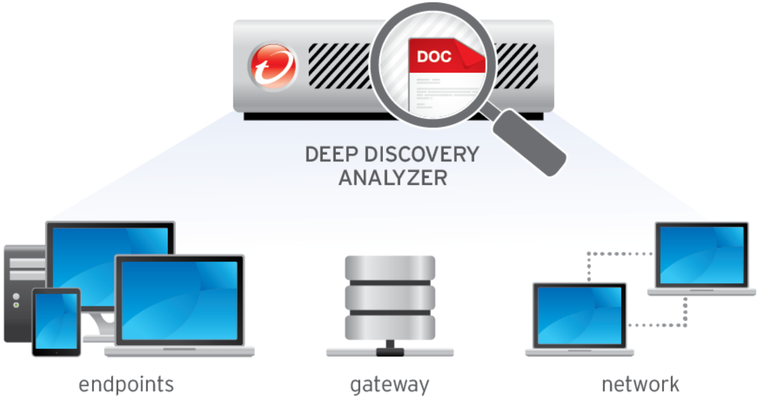
Containment and remediation: What to look for, how to eradicate.

TREND MICRO SMART PROTECTION NETWORK™

Deep Discovery Analyzer

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

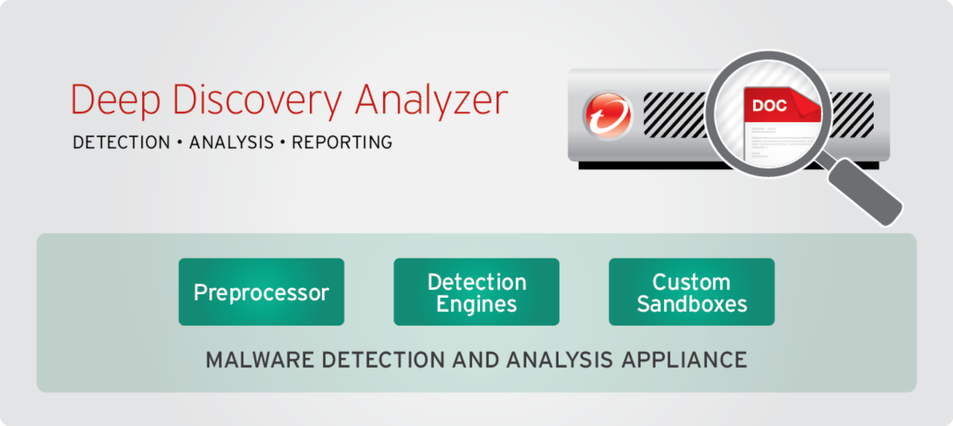
➢ ***Enhance the threat protection of your existing security investments***

Deep Discovery Analyzer

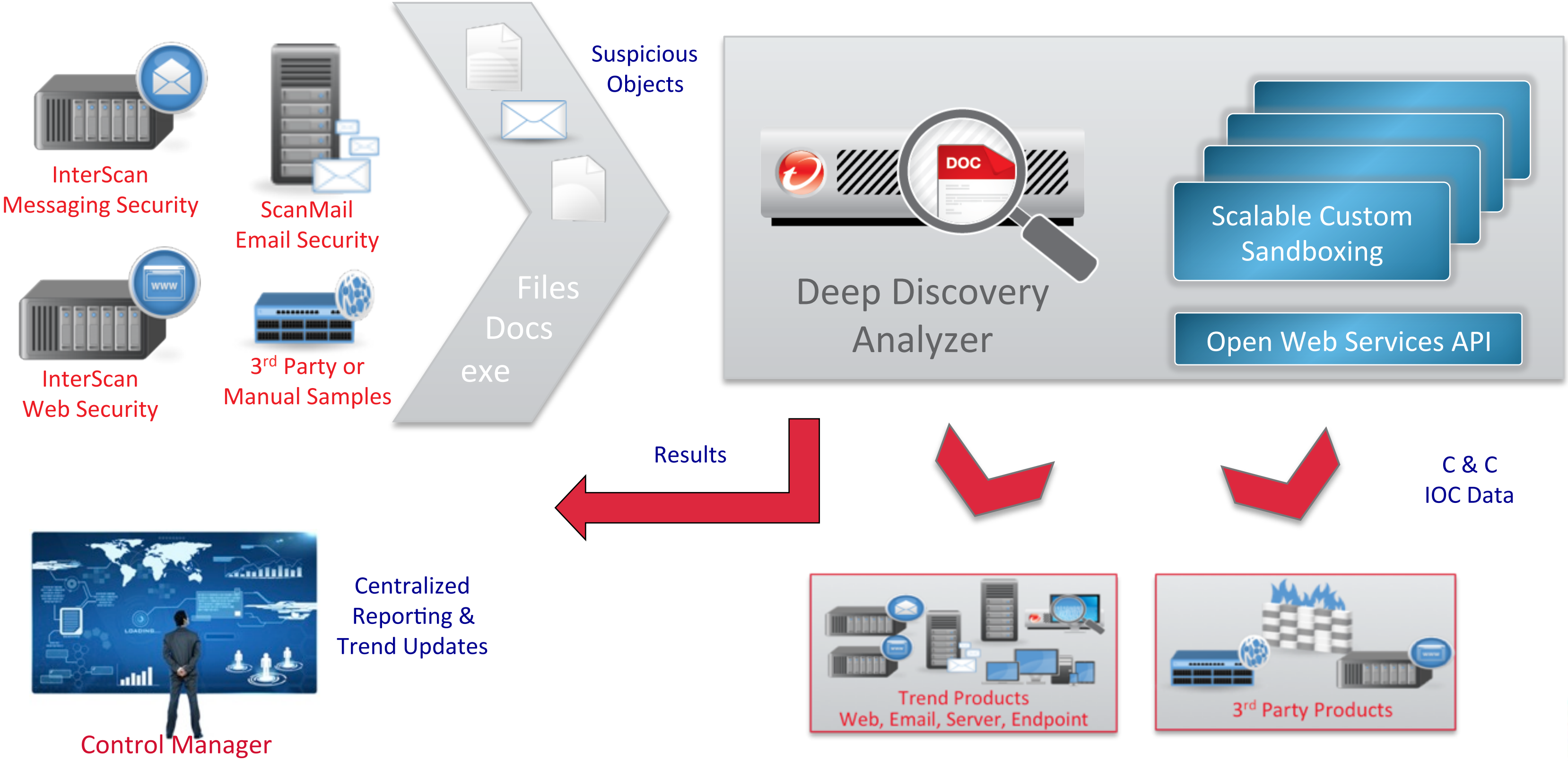
Scalable sandboxing server

Key Features

- Custom sandbox images
- Multiple detection engines
- Broad file analysis range
- Document exploit detection
- URL analysis
- Trend Micro product integration, open API, manual submission
- Detailed Reporting and Custom Defense IOC sharing


Deep Discovery Analyzer
DETECTION • ANALYSIS • REPORTING
DOC
Preprocessor
Detection Engines
Custom Sandboxes
MALWARE DETECTION AND ANALYSIS APPLIANCE

Analyzer: Sandboxing & Intelligence Sharing



InterScan Messaging Security

ScanMail Email Security

InterScan Web Security

3rd Party or Manual Samples

Files

Docs

exe

Suspicious Objects

Deep Discovery Analyzer

Scalable Custom Sandboxing

Open Web Services API

Results

C & C IOC Data

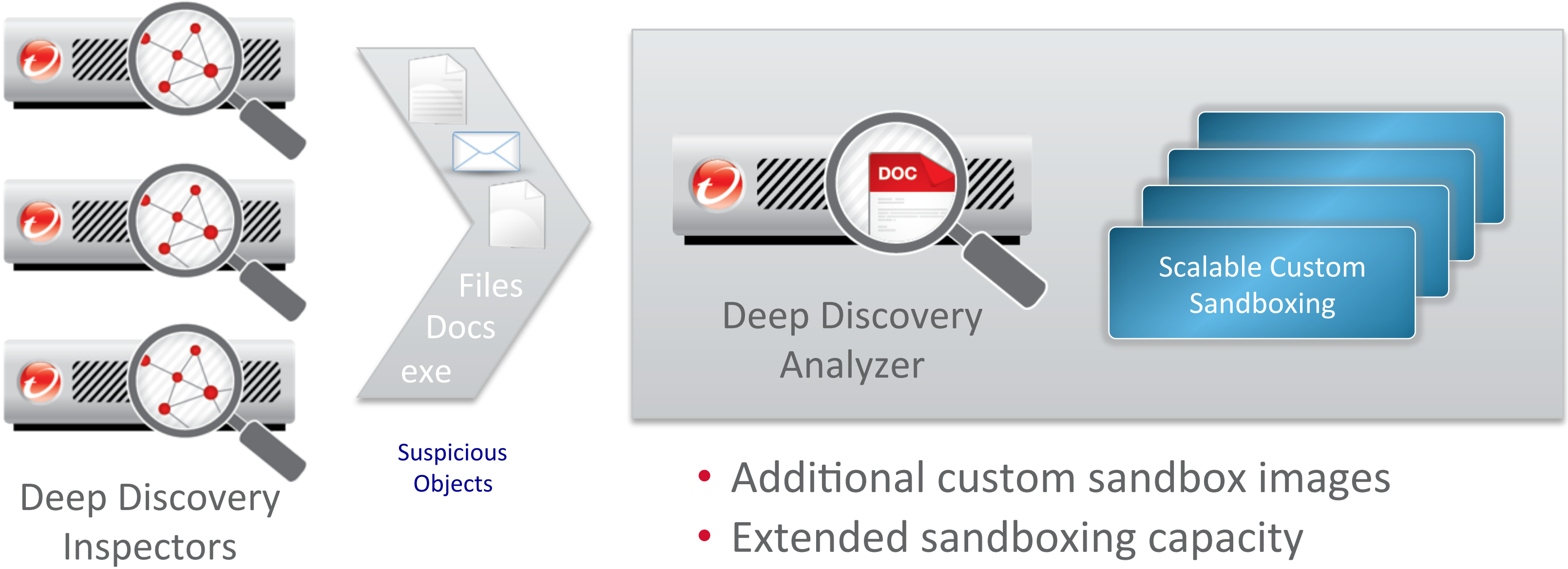
Centralized Reporting & Trend Updates

Control Manager

Trend Products Web, Email, Server, Endpoint

3rd Party Products

Deep Discovery: Inspector + Analyzer

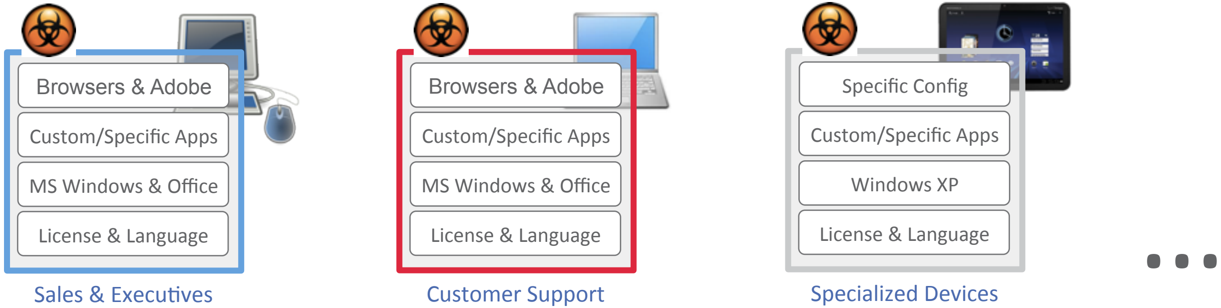


- Additional custom sandbox images
- Extended sandboxing capacity
- Sandboxing for Inspector virtual appliances
- Central reporting & analysis of malware
- Sharable resource with Trend/other products

Why Custom Sandboxing Is Essential

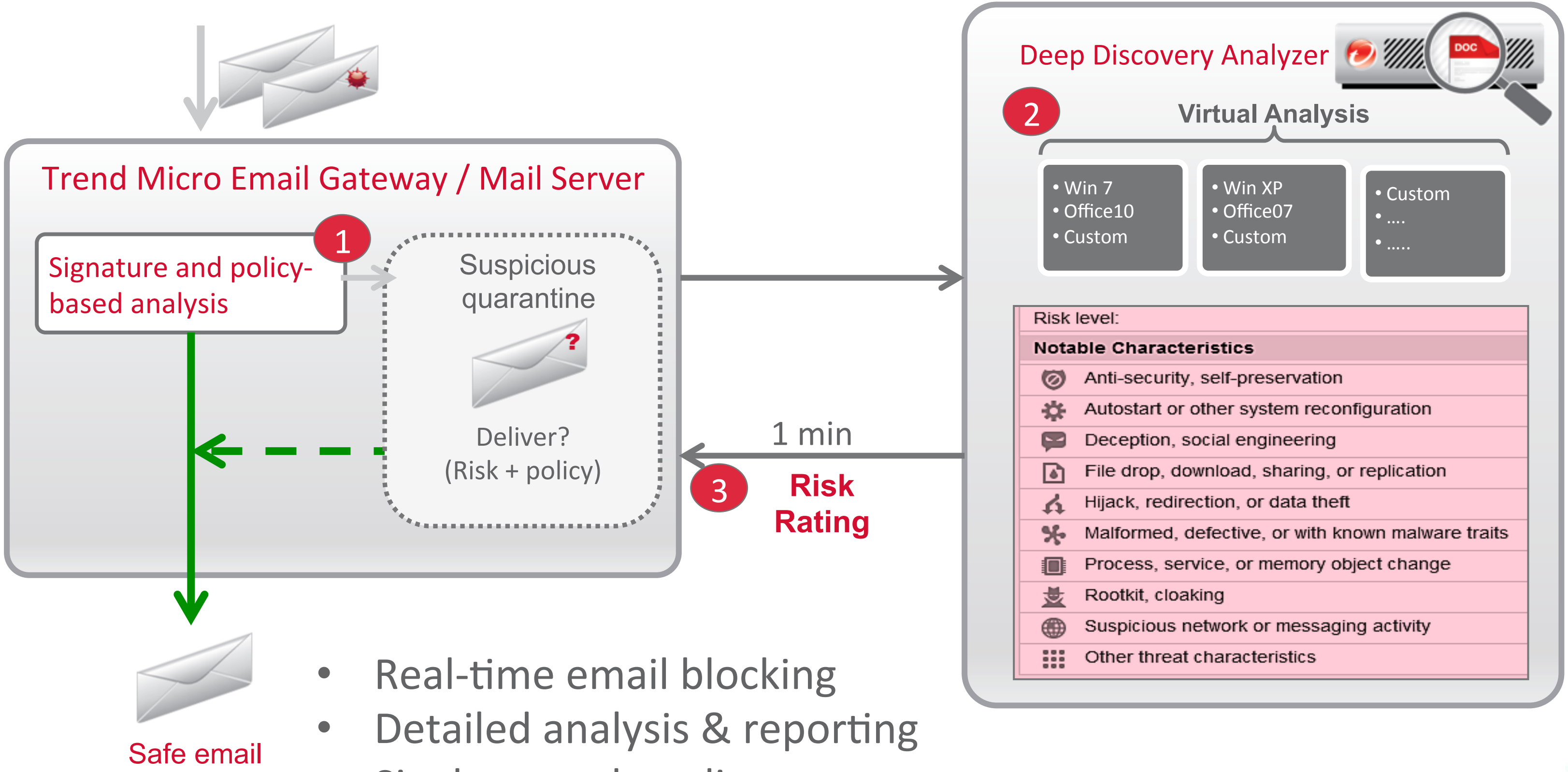
Accurate detection of *your* attackers

- Identify custom malware targeting your organization
  - E.g., Your Windows license, language, applications
  - Handle differing desktop environments across departments
- Triage malware that does not affect your organization
  - E.g., older/other versions & patches of Windows or key applications
- Thwart evasion techniques based on configuration checks
  - E.g., Generic Windows license, English language, limited/standard apps



Sales & Executives	Customer Support	Specialized Devices
Browsers & Adobe	Browsers & Adobe	Specific Config
Custom/Specific Apps	Custom/Specific Apps	Custom/Specific Apps
MS Windows & Office	MS Windows & Office	Windows XP
License & Language	License & Language	License & Language

Targeted Email Attack Protection



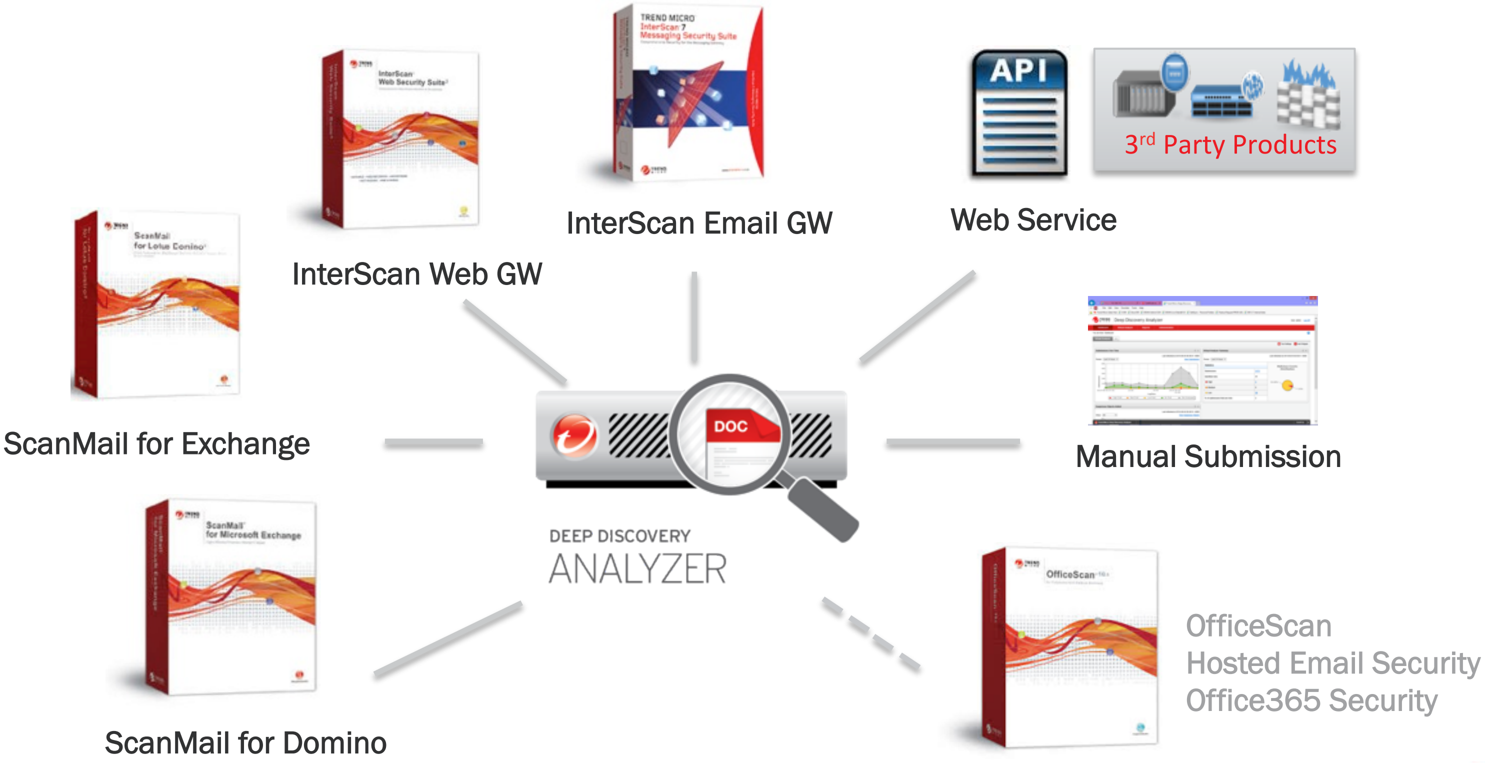
Risk level:

Notable Characteristics

- Anti-security, self-preservation
- Autostart or other system reconfiguration
- 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

- Real-time email blocking
- Detailed analysis & reporting
- Single-console policy management

Trend Micro - Analyzer Integration



TREND MICRO InterScan 7 Messaging Security Suite
InterScan Web Security Suite
ScanMail for Lotus Domino
ScanMail for Microsoft Exchange
OfficeScan
API
3rd Party Products
DOC

InterScan Web GW

InterScan Email GW

Web Service

ScanMail for Exchange

Manual Submission

DEEP DISCOVERY ANALYZER

ScanMail for Domino

OfficeScan
Hosted Email Security
Office365 Security

Deep Discovery Email Inspector

Deep Discovery Email Inspector

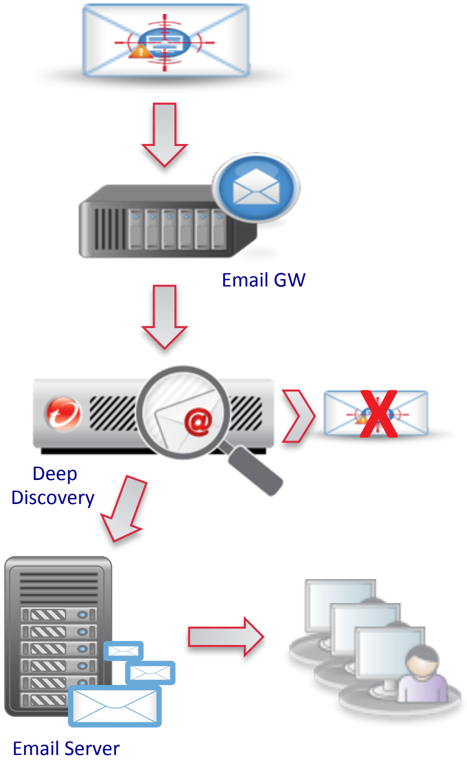
Targeted Email Attack Protection

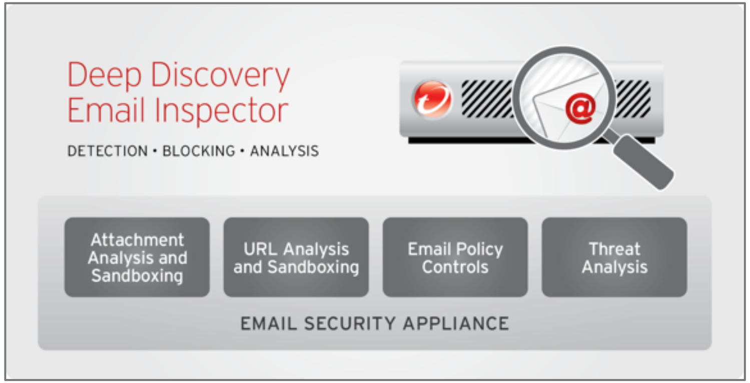
A dedicated email appliance that detects and blocks emails containing malicious content or URL references

- Custom sandboxing and detection engines analyze email attachments
- Full analyzes embedded URL destinations
- Derives passwords for protected files
- Co-exists with other email security products

➢ ***Stop targeted emails that lead to data breach***

Email Inspector – At a Glance





Deep Discovery Email Inspector

DETECTION • BLOCKING • ANALYSIS

Attachment Analysis and Sandboxing

URL Analysis and Sandboxing

Email Policy Controls

Threat Analysis

EMAIL SECURITY APPLIANCE

- Attachments: Analyzed with detection engines & sandboxing
- Passwords: Intelligently derived using heuristics & lists
- URLs: Reputation, scanning & sandboxing for malware & exploits
- Custom Sandboxing: Configured to precisely match your systems
- Policy Controls: Make it simple to customize security policies
- Threat Analysis: Tools & intelligence to assess the nature of the attack

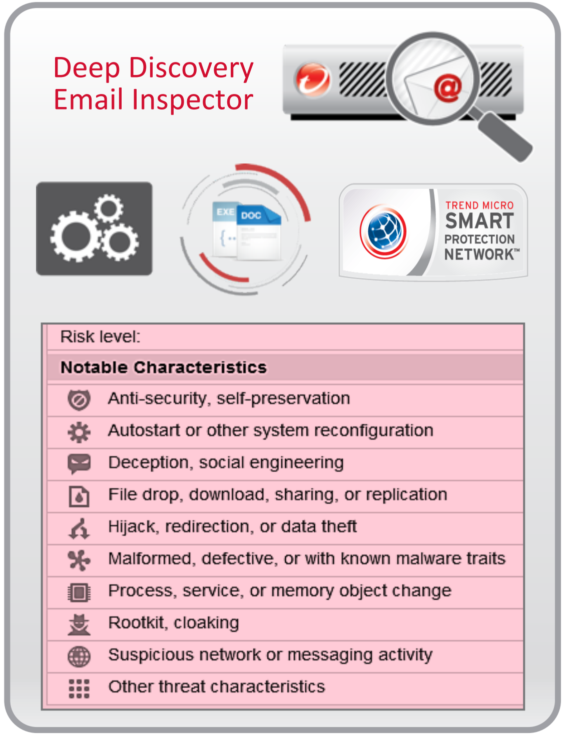
Advanced Threat Protection blocks targeted email attacks

Email Inspector – Better Detection

Trend Micro™ Deep Discovery TOP SCORE in breach detection

NSS Labs 2014 Breach Detection Tests

Same technology!!



Risk level:
Notable Characteristics
Anti-security, self-preservation
Autostart or other system reconfiguration
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

Detection Engines, Custom Sandboxing, Global Intelligence

Attachment Analysis

- Attachments are unpacked, decompressed, and unlocked using heuristic rules and customer-supplied keywords
- Detection engines and custom sandboxing analysis identify advanced malware and document exploits
- Analyzes a wide range of file types and content including: Windows executables, Microsoft Office, PDF, Zip, Java

URL Analysis

- URLs are reputation-checked via Smart Protection Network
- Page content is scanned and sandboxed to discover redirects, advanced malware, and exploits used in drive-by downloads

Email Inspector – How It Works

Beyond Detection

DEEP DISCOVERY
EMAIL INSPECTOR

Password-protected Attachments

Content examination, heuristics, and customer-defined keywords aid the analysis of password-protected files and Zip files

Policy Management

Quarantine, deletion, forward-with-tag are configurable by detection severity. Sandbox analysis can be controlled by attachment type

Threat Connect Portal

Integrated portal delivers global intelligence relevant to your attack – malware profiles, C&C networks, attack group, and more

Deep Discovery Endpoint Sensor

Deep Discovery Endpoint Sensor

Endpoint & Server Attack Detection

Endpoint & Servers
On-premise, Remote, Cloud-based

A context-aware endpoint security monitor designed to speed the discovery, investigation and response to security incidents:

- Records detailed system activities
- Performs multi-level search across endpoints
- Uses rich search criteria including:
  - OpenIOC, Yara, Deep Discovery results
- Compatible with any AV security solution

➢ ***Detect and assess the nature and extent of targeted attacks***

General Search Capabilities

Multi-level search based on:

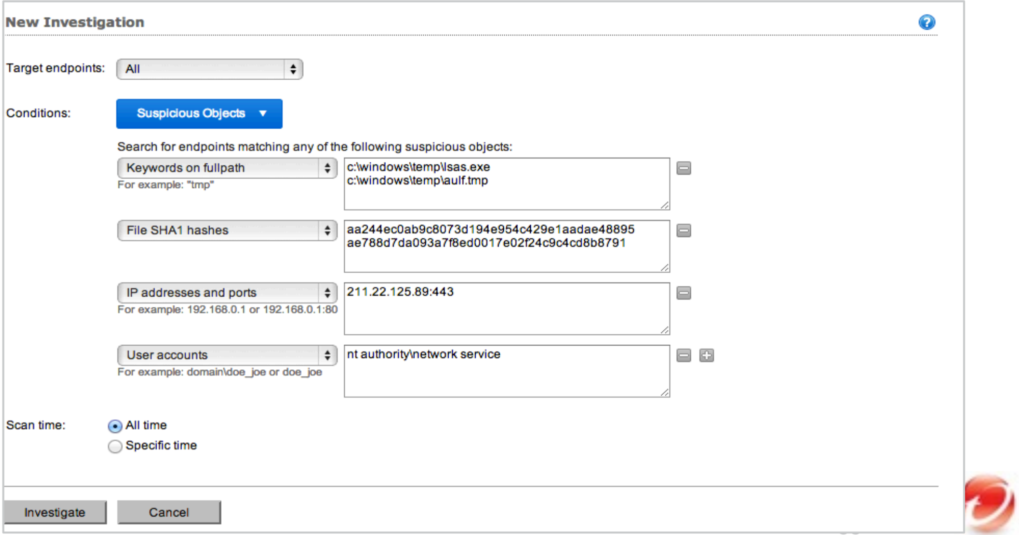
- Communications
  - IP, Port, URL, Domain, DNS
- Malware or any file
  - Sha1 hash
- Registry activity
- Running processes
- User account activity

Input: Individual parameters, YARA and OpenIOC files

Available standalone & in Control Manager console

How can I…?

- Confirm an alert indicating an endpoint may have been infiltrated?
- Analyze actual malware behavior & result?
- See which endpoints have active C&C communications ?
- Discovery which endpoints are infected by specific malware?
- Understand the extent to which an attack has spread across my network?



New Investigation

Target endpoints: All

Conditions: Suspicious Objects ▼

Search for endpoints matching any of the following suspicious objects:

Keywords on fullpath
For example: "tmp"
c:\windows\temp\lsas.exe
c:\windows\temp\aulf.tmp

File SHA1 hashes
aa244ec0ab9c8073d194e954c429e1aadae48895
ae788d7da093a7f8ed0017e02f24c9c4cd8b8791

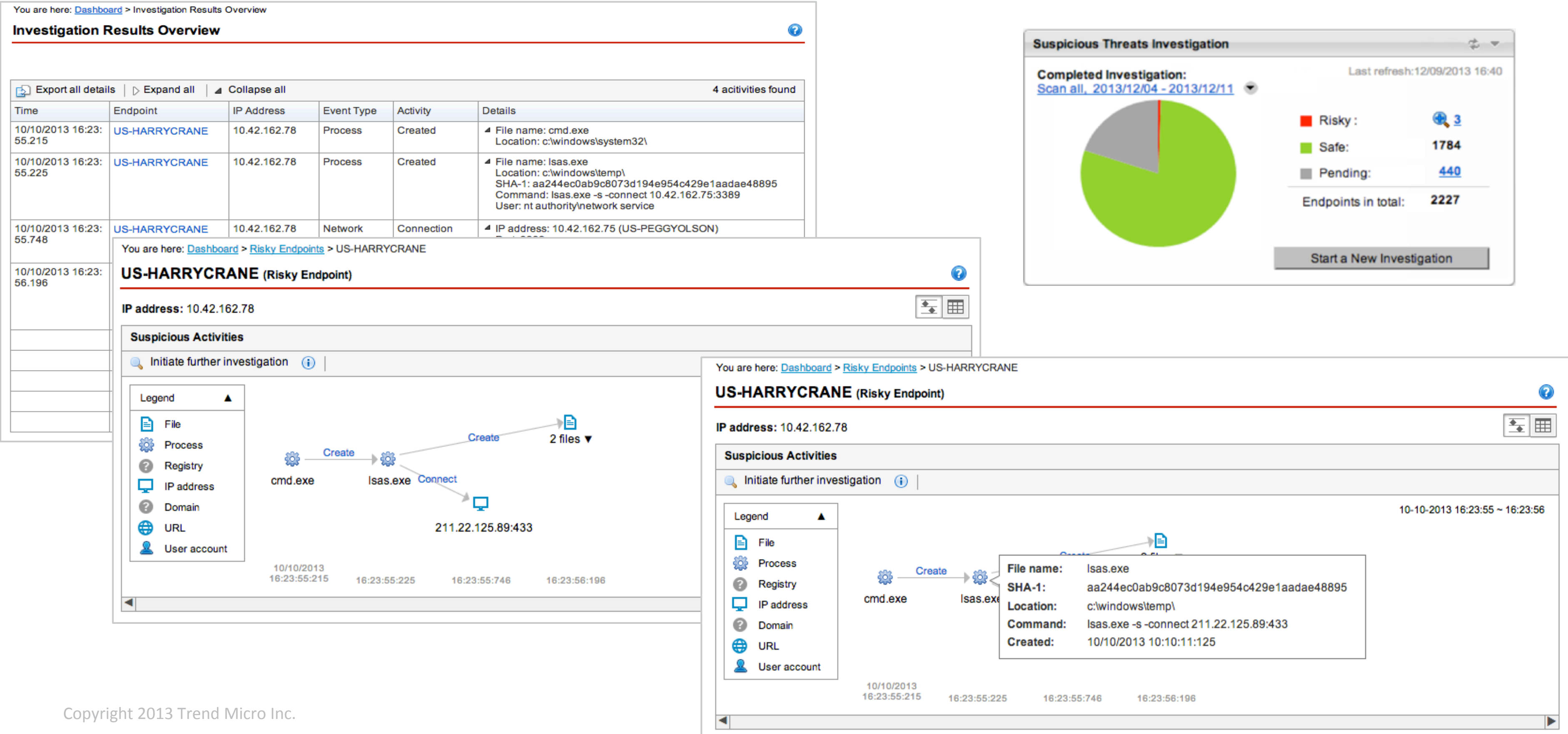
IP addresses and ports
For example: 192.168.0.1 or 192.168.0.1:80
211.22.125.89:443

User accounts
For example: domain\doe_joe or doe_joe
nt authority\network service

Scan time:
● All time
○ Specific time

Search Results

- Search summary
- Individual endpoint flow & drilldown
- Context and network aware



You are here: Dashboard > Investigation Results Overview

Investigation Results Overview

Export all details | ▷ Expand all | ◢ Collapse all — 4 acitivities found

Time	Endpoint	IP Address	Event Type	Activity	Details
10/10/2013 16:23:55.215	US-HARRYCRANE	10.42.162.78	Process	Created	◢ File name: cmd.exe Location: c:\windows\system32\
10/10/2013 16:23:55.225	US-HARRYCRANE	10.42.162.78	Process	Created	◢ File name: lsas.exe Location: c:\windows\temp\ SHA-1: aa244ec0ab9c8073d194e954c429e1aadae48895 Command: lsas.exe -s -connect 10.42.162.75:3389 User: nt authority\network service
10/10/2013 16:23:55.748	US-HARRYCRANE	10.42.162.78	Network	Connection	◢ IP address: 10.42.162.75 (US-PEGGYOLSON)
10/10/2013 16:23:56.196					

Suspicious Threats Investigation

Completed Investigation:
Scan all, 2013/12/04 - 2013/12/11

Last refresh:12/09/2013 16:40

🟥 Risky :	3
🟩 Safe:	1784
▨ Pending:	440
Endpoints in total:	2227

Start a New Investigation

You are here: Dashboard > Risky Endpoints > US-HARRYCRANE

US-HARRYCRANE (Risky Endpoint)

IP address: 10.42.162.78

Suspicious Activities

Initiate further investigation

You are here: Dashboard > Risky Endpoints > US-HARRYCRANE

US-HARRYCRANE (Risky Endpoint)

IP address: 10.42.162.78

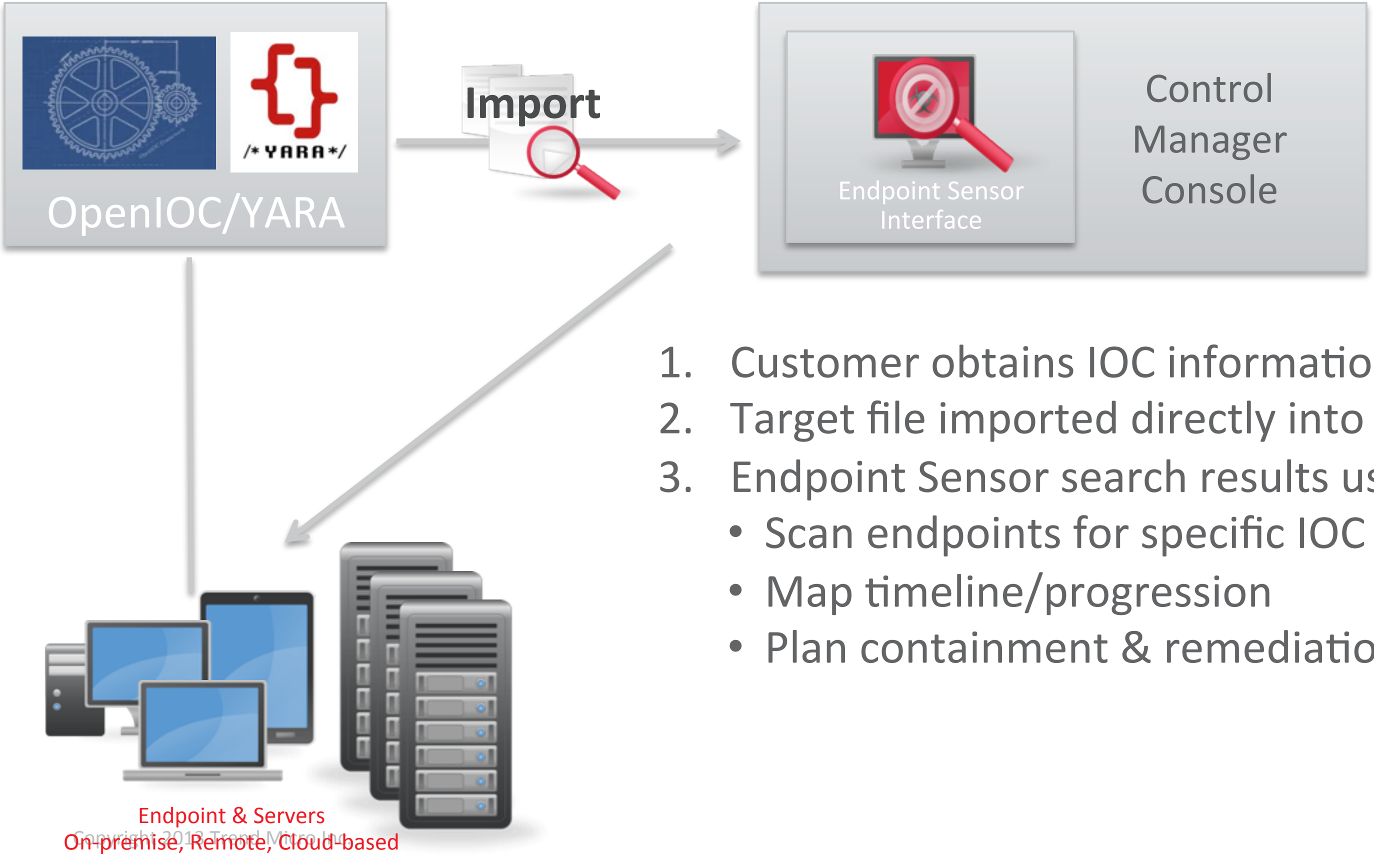
Suspicious Activities

Initiate further investigation

10-10-2013 16:23:55 ~ 16:23:56

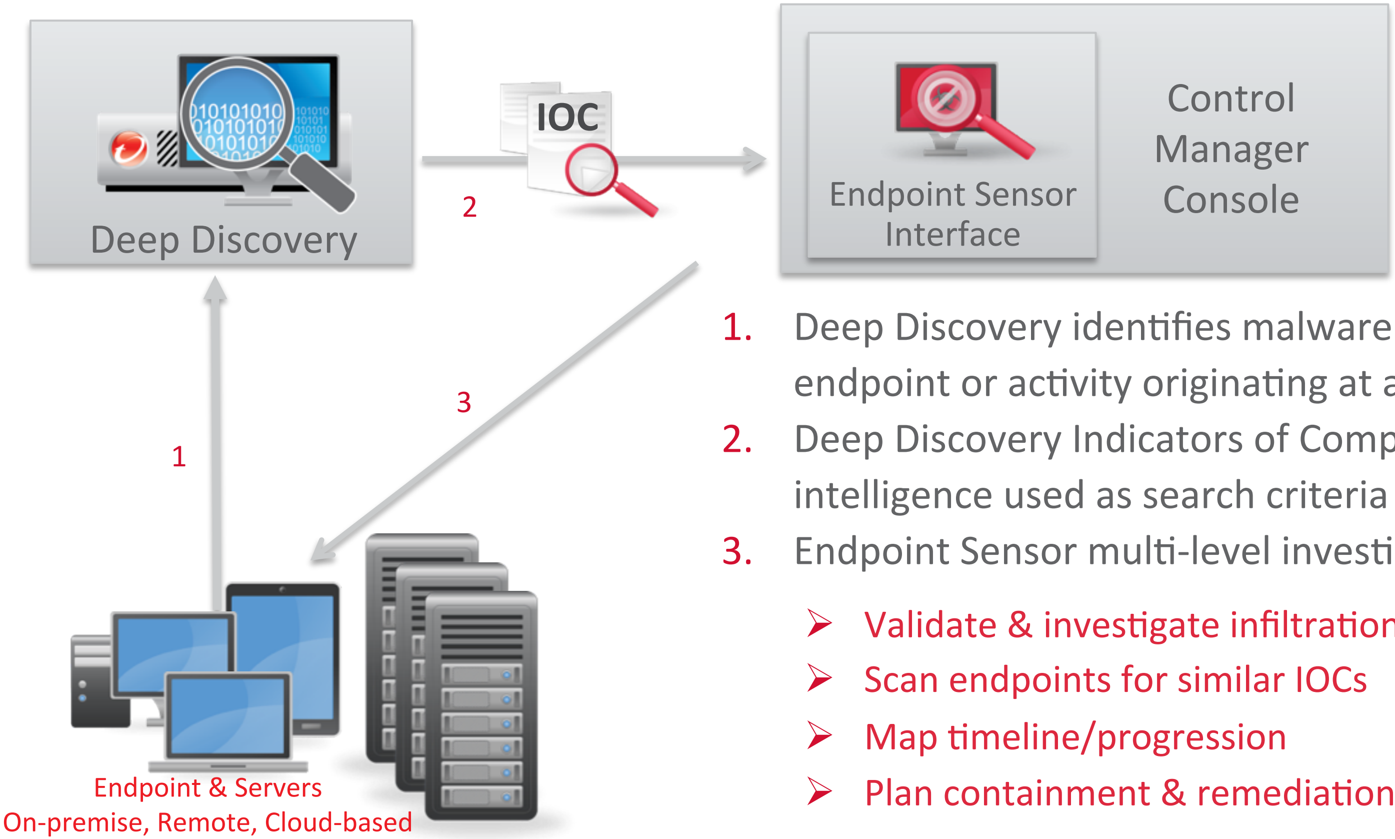
File name:	lsas.exe
SHA-1:	aa244ec0ab9c8073d194e954c429e1aadae48895
Location:	c:\windows\temp\
Command:	lsas.exe -s -connect 211.22.125.89:433
Created:	10/10/2013 10:10:11:125

Use Case: Public/Custom OpenIOC or YARA files



1. Customer obtains IOC information or YARA signature
2. Target file imported directly into Endpoint Sensor search
3. Endpoint Sensor search results used to:
    - Scan endpoints for specific IOC profile
    - Map timeline/progression
    - Plan containment & remediation

Deep Discovery: Investigation & Response



1. Deep Discovery identifies malware sent to an endpoint or activity originating at an endpoint
2. Deep Discovery Indicators of Compromise (IOC) intelligence used as search criteria
3. Endpoint Sensor multi-level investigations:
   - Validate & investigate infiltrations
   - Scan endpoints for similar IOCs
   - Map timeline/progression
   - Plan containment & remediation

Deep Discovery Summary

Deep Discovery Products

Network-wide attack detection

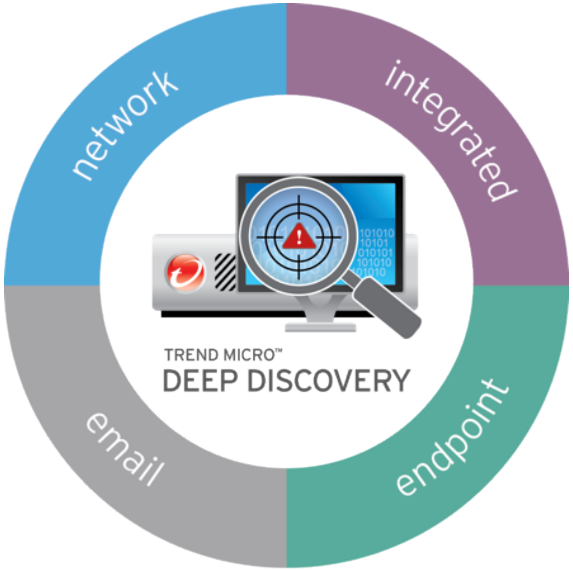
Inspector

Detect and analyze targeted attacks anywhere on your network

Integrated sandboxing

Analyzer

Improve the threat protection of your existing security investments



Email attack protection

Email Inspector

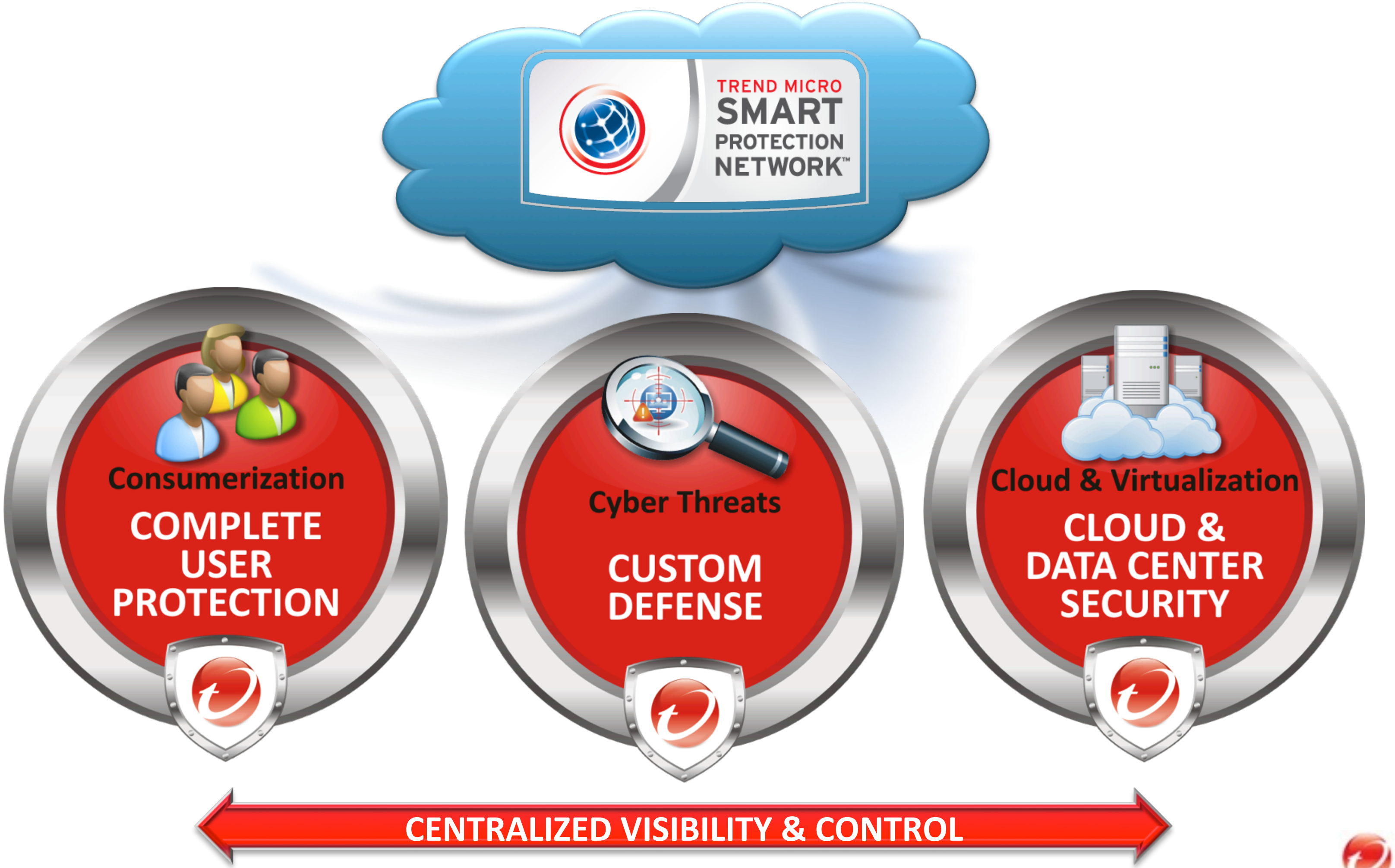
Stop the targeted attacks that can lead to a data breach

Endpoint Investigation

Endpoint Sensor

Investigate & respond to attacks with network detection + endpoint intelligence

Deploy protection where it matters most to your organization



TREND MICRO SMART PROTECTION NETWORK™

Consumerization

COMPLETE USER PROTECTION

Cyber Threats

CUSTOM DEFENSE

Cloud & Virtualization

CLOUD & DATA CENTER SECURITY

CENTRALIZED VISIBILITY & CONTROL

Thank you!

Veli-Pekka Kusmin
veli-pekka_kusmin@trendmicro.com
☎ +358 50 67181