Combating APTs with the Custom Defense Solution

Hans Liljedahl

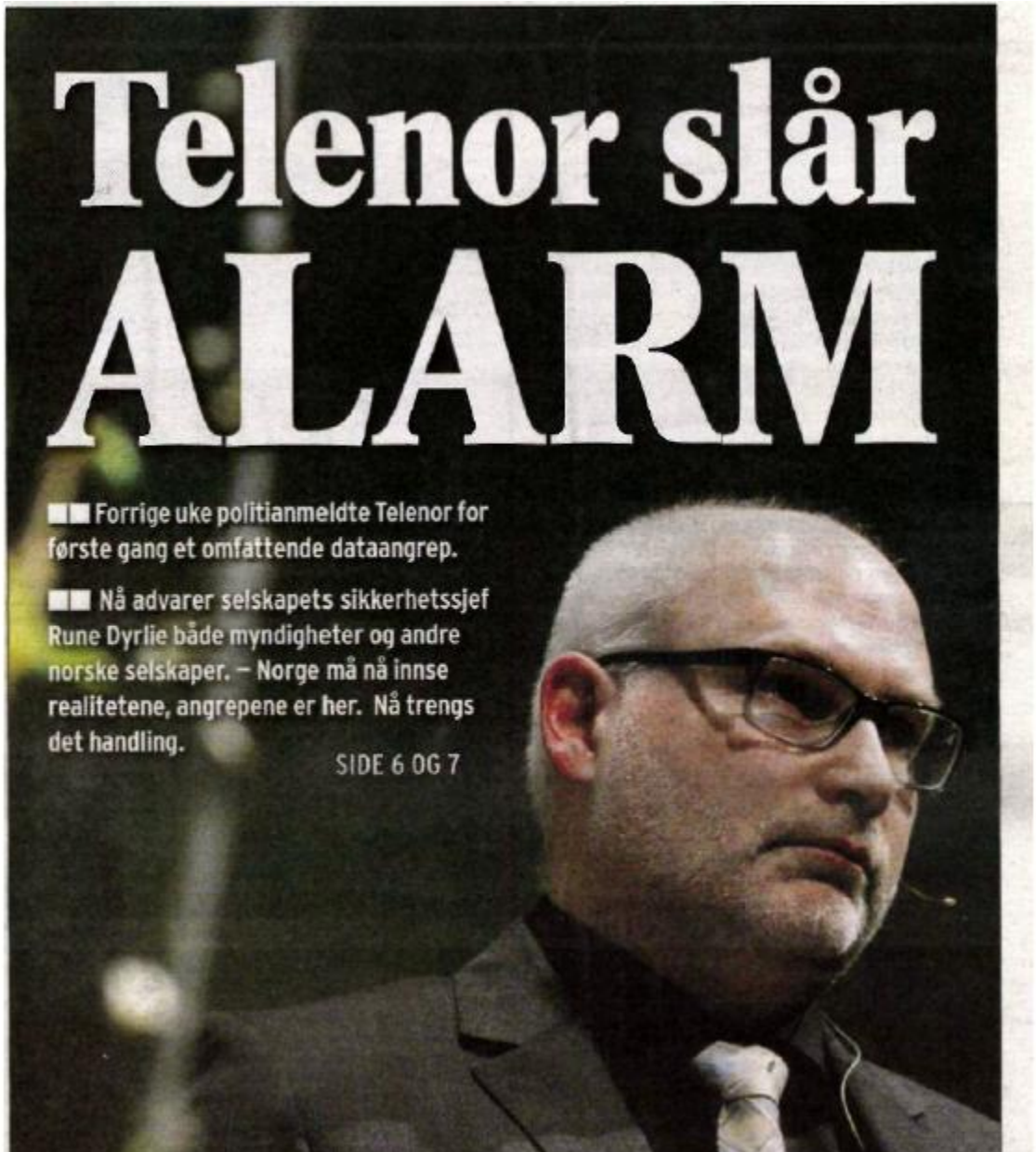
Peter Szendröi

RSA

Attack Overview :

1. Two spear phishing emails were sent over a two-day period targeted at low to mid-level employees with subject "2011 Recruitment Plan" and .xls attachment with the same title.
2. xls file contained an exploit through an Adobe Flash zero-day vulnerability that installed a backdoor using a Poison Ivy RAT variant set in a reverse-connect mode
3. Attackers moved laterally to identify users with more access and admin rights to relevant services and servers of interest.
4. Access was then established to staging servers at key aggregation points.
5. Data of interest was moved to the internal staging servers, aggregated, compressed, and encrypted for extraction.
6. FTP was then used to transfer password protected RAR files to a compromised machine at a hosting provider.
7. Files were subsequently removed from the host to cover up traces of the attack.

Telenor- Norway



TREND MICRO

DigiNotar

Attack Overv

1. Attacker locat
Web servers in e
2. Diginotar usec
defense method
and attackers. m
time to gain acc
3. With access to the CA servers, more than 531 (identified) rogue certificates were issued.
4. Rogue certificates were transmitted to attacker's external IP server, using a proxy tunneling tool.
5. 300.000 Iranian Gmail accounts spyed on.
6. DigiNotar filed for bankruptcy in a Netherland court.

Analysts and Influencers Urge Action

— Adoption of Advanced Threat Detection

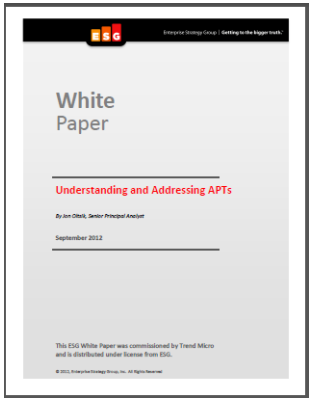
"You need to know what's accessing the data, how the data's being used, and what's happening on your network."

John Kindervag
Principal Analyst Serving Security & Risk Professionals
Forrester Research, Inc.

Gartner®

*"We must **assume** we will be compromised and must have better detection capabilities in place that provide visibility as to when this type of breach occurs."*

Neil MacDonald
VP and Gartner Fellow
Gartner, Inc.



"Hardening existing security defenses... won't be enough to deal with the sophistication and perseverance of APTs."

Jon Oltsik
Senior Principal Analyst,
Enterprise Strategy Group

TREND MICRO™

Trend Micro

What We Do

Recognized global **leader** in server, virtualization and cloud security

Innovative security solutions

Protecting the exchange of digital information for businesses and consumers

How We Do It

1,200 threats experts in 12 TrendLabs locations around the globe; **1492** R&D engineers

$400M USD and 500 engineers invested over last 4 years to develop cloud-related solutions

Global Threat Intelligence

Who We Are

Eva Chen: CEO and Founder	
Co-founded:	1988
Offices:	36
Global Employees:	4942
Revenue:	$1.2B USD
Cash Assets:	$900M USD
Operating Income:	$330M USD
Headquarters:	Tokyo

Trend Micro is the largest independent security provider

Protecting 48 of 50 top global corporations

TREND MICRO

Trend Micro

Our Personal Journey to the Cloud

Smart Protection Network

Mobility

Virtualization

Cloud Computing

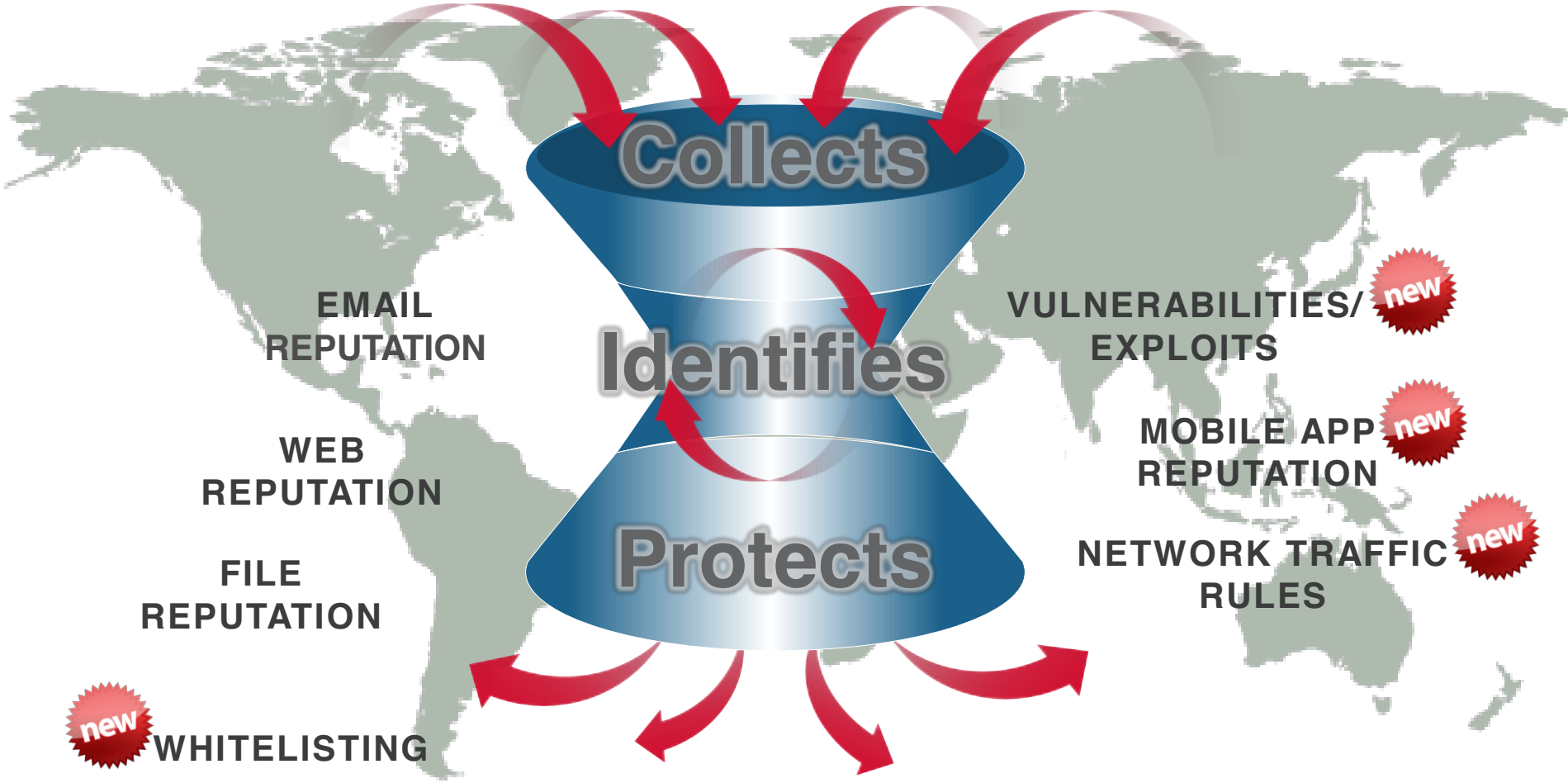
Industry Leading Solutions Build on **25 Year History of Innovation**

Dedicated Focus on **Security**

TREND MICRO™

TREND MICRO SMART PROTECTION NETWORK™

GLOBAL SENSORNET

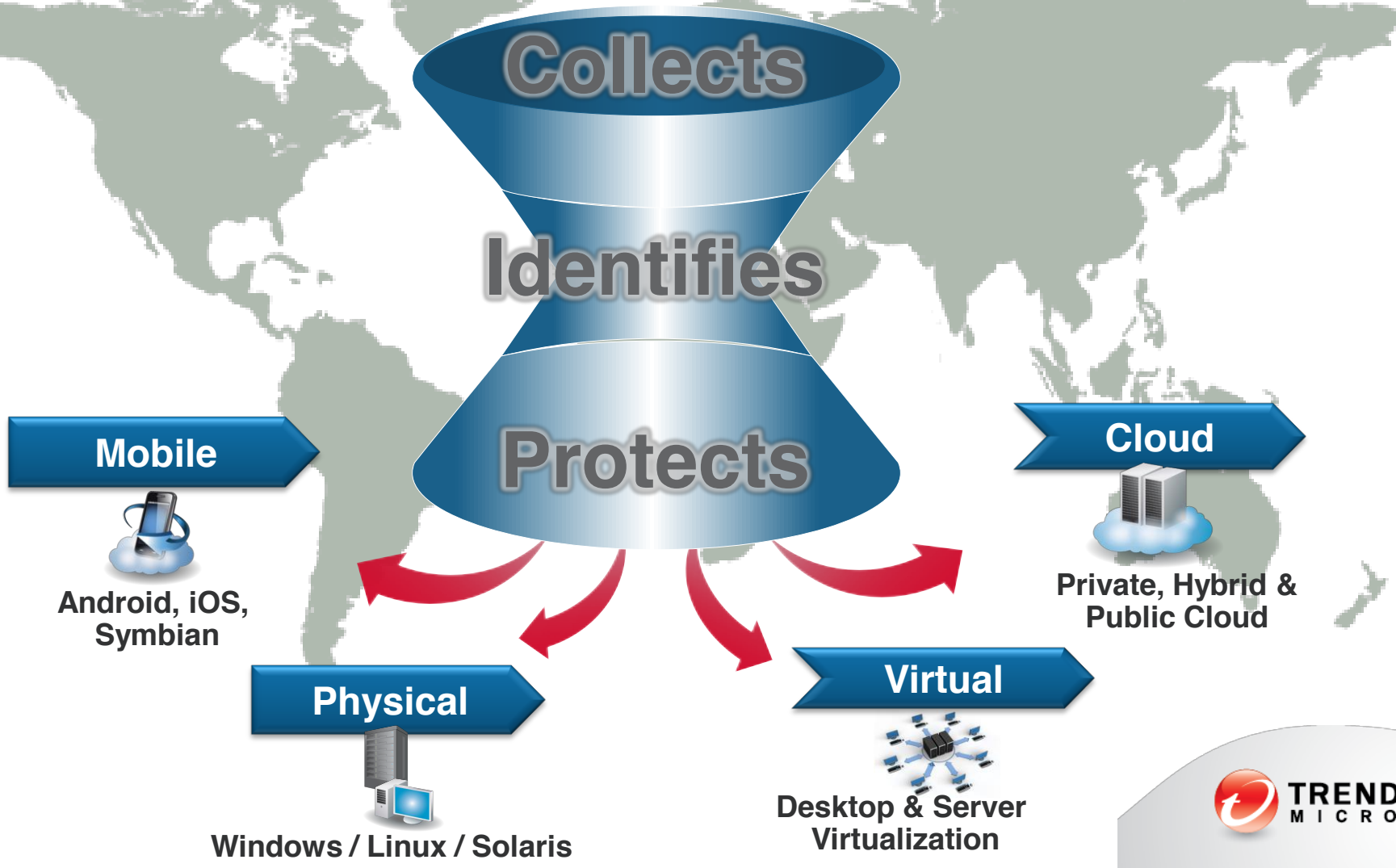


TREND MICRO™

TREND MICRO SMART

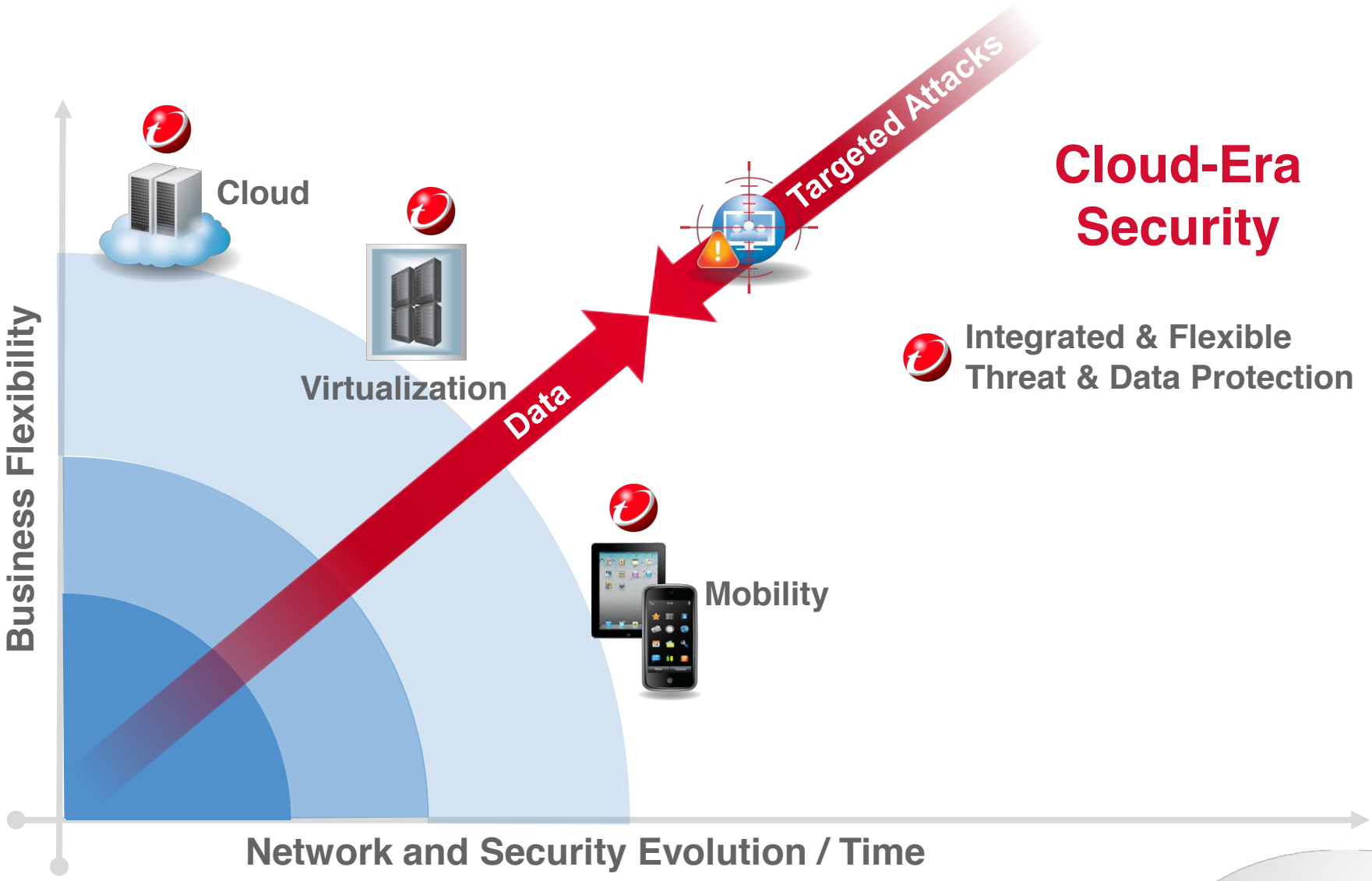
Daily Statistics:

1.15B threat samples...6TB threat feeds…10B URL queries…7M new files...



TREND MICRO

Evolution of Security



Cloud-Era Security

Integrated & Flexible
Threat & Data Protection

TREND MICRO

"On one hand, I'm grateful that we've never been targeted for a cyber-attack. On the other hand, I'm insulted that nobody thinks we're worth the effort!"

We see the TIP of the APT ICEBERG

RSA The Security Division of EMC
Google
SONY make.believe
LOCKHEED MARTIN
HONDA The Power of Dreams
citi
Adobe
ADP
epsilon Marketing As Usual. Not A Chance.™

99 % Unreported*

APTs
Cyber Espionage
Targeted Attacks
Cyber Threats

*** Former CIO of US Dept of Justice**

The Reality

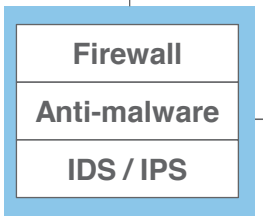
- **One new threat** created every second [1]
- A **cyber intrusion** happens every 5 minutes [2]
- Over **90%** of enterprises have malware [1]
- Almost **75%** have one or more bots [1]

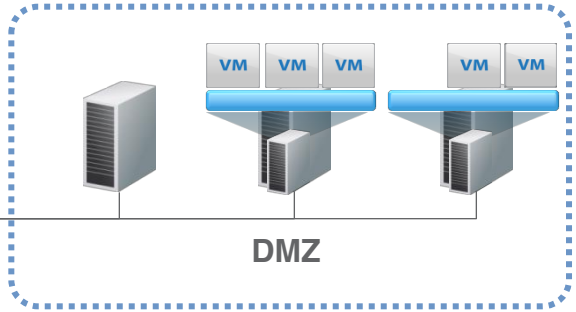
Sources: 1: Trend Micro, 2012, 2: US-Cert 2012

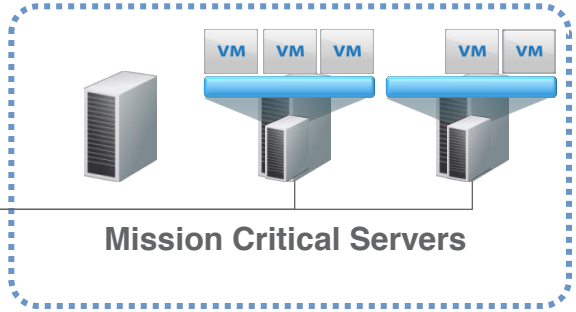
TREND MICRO

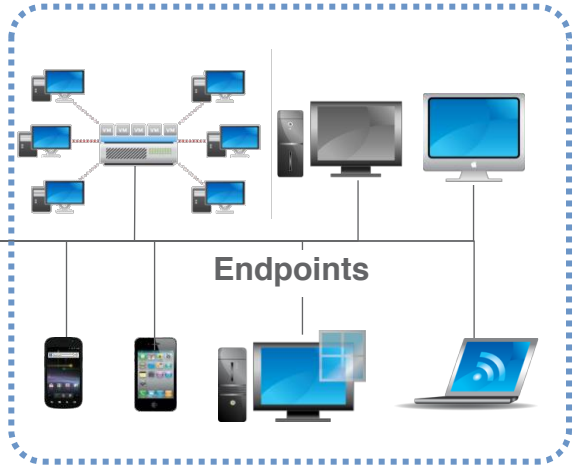
Today's Enterprise Challenges

IaaS









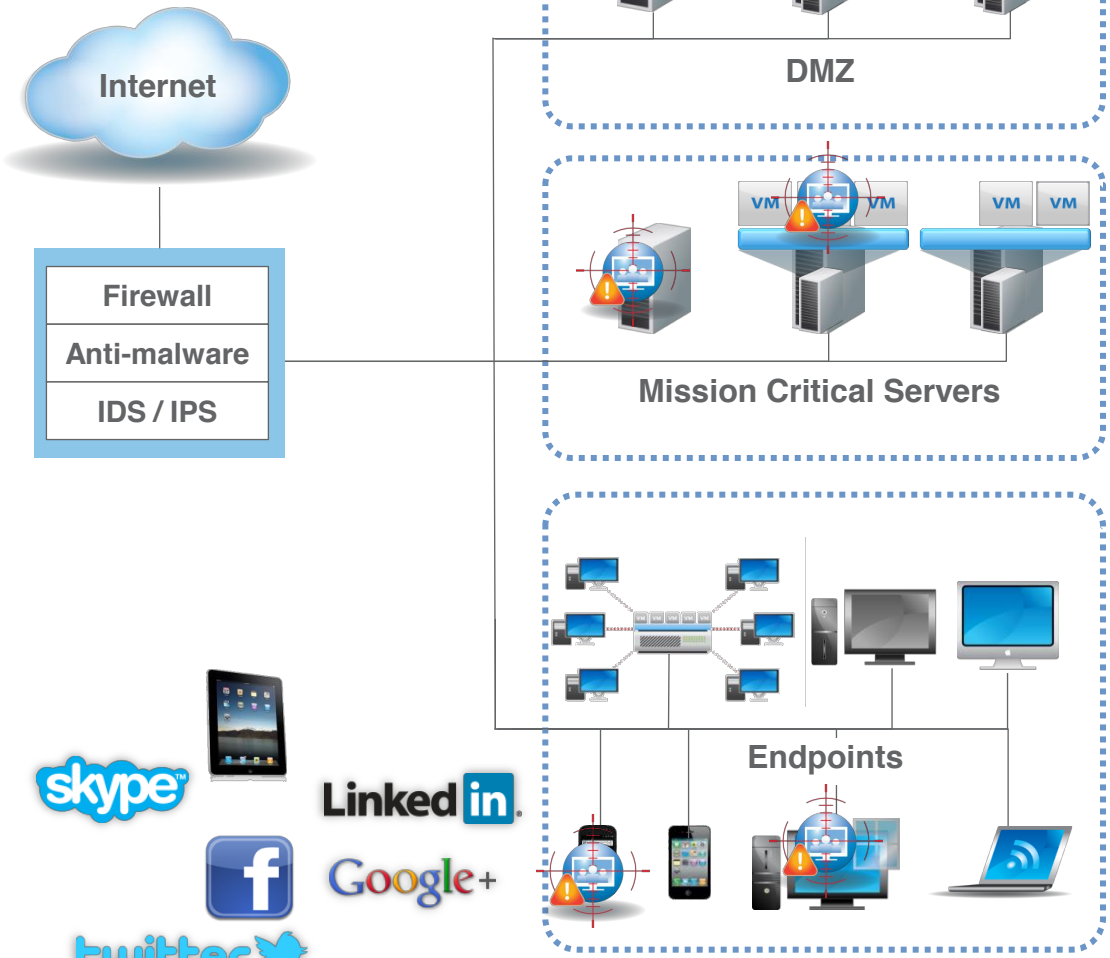
- Data in motion
- Social Media
- Virtualization and Cloud
- Traditional defenses bypassed by low and slow attacks

SaaS

TREND MICRO

Today's Enterprise Challenges

IaaS

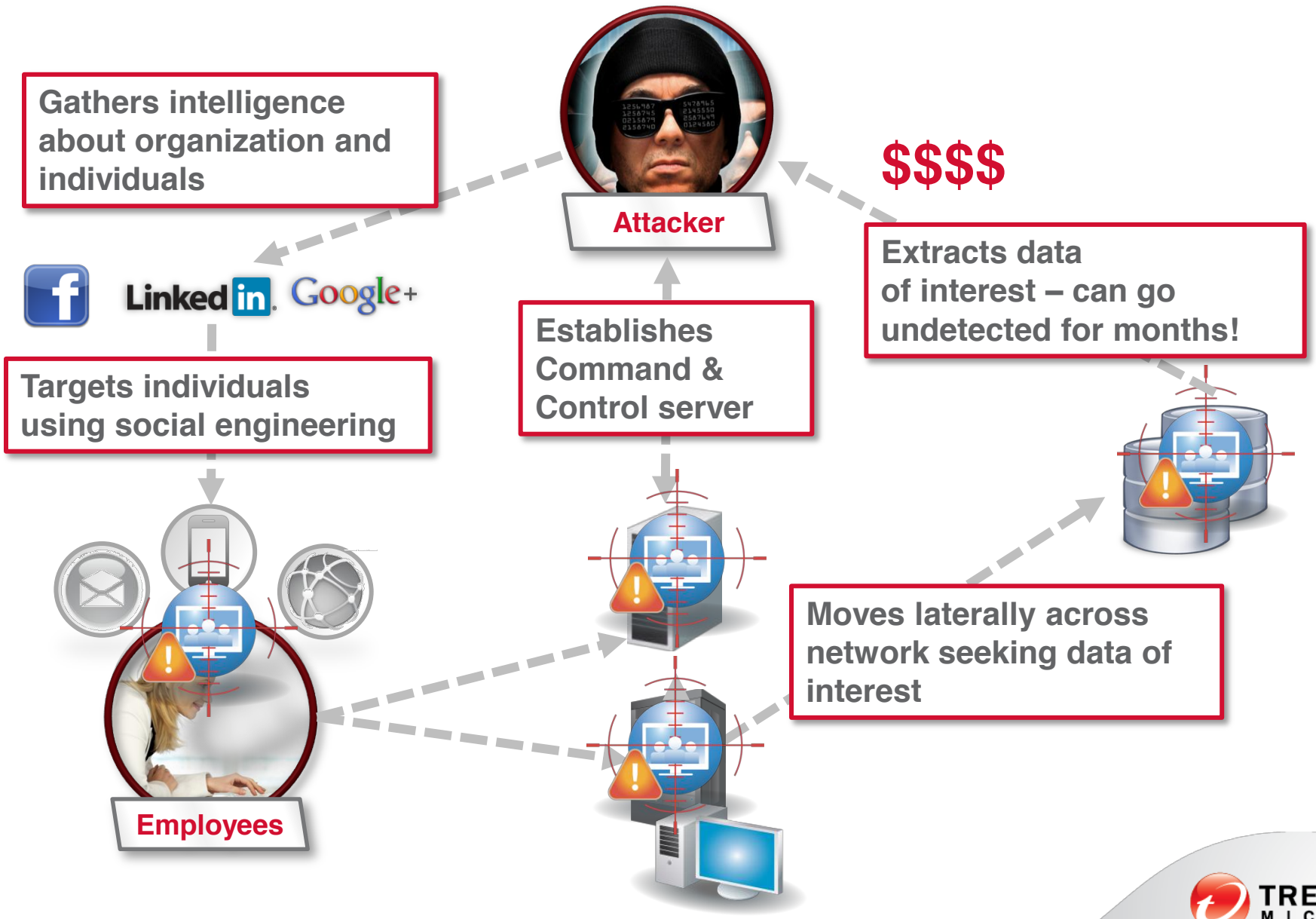


…are ***Customized*** to Attack ***Your*** Defenses

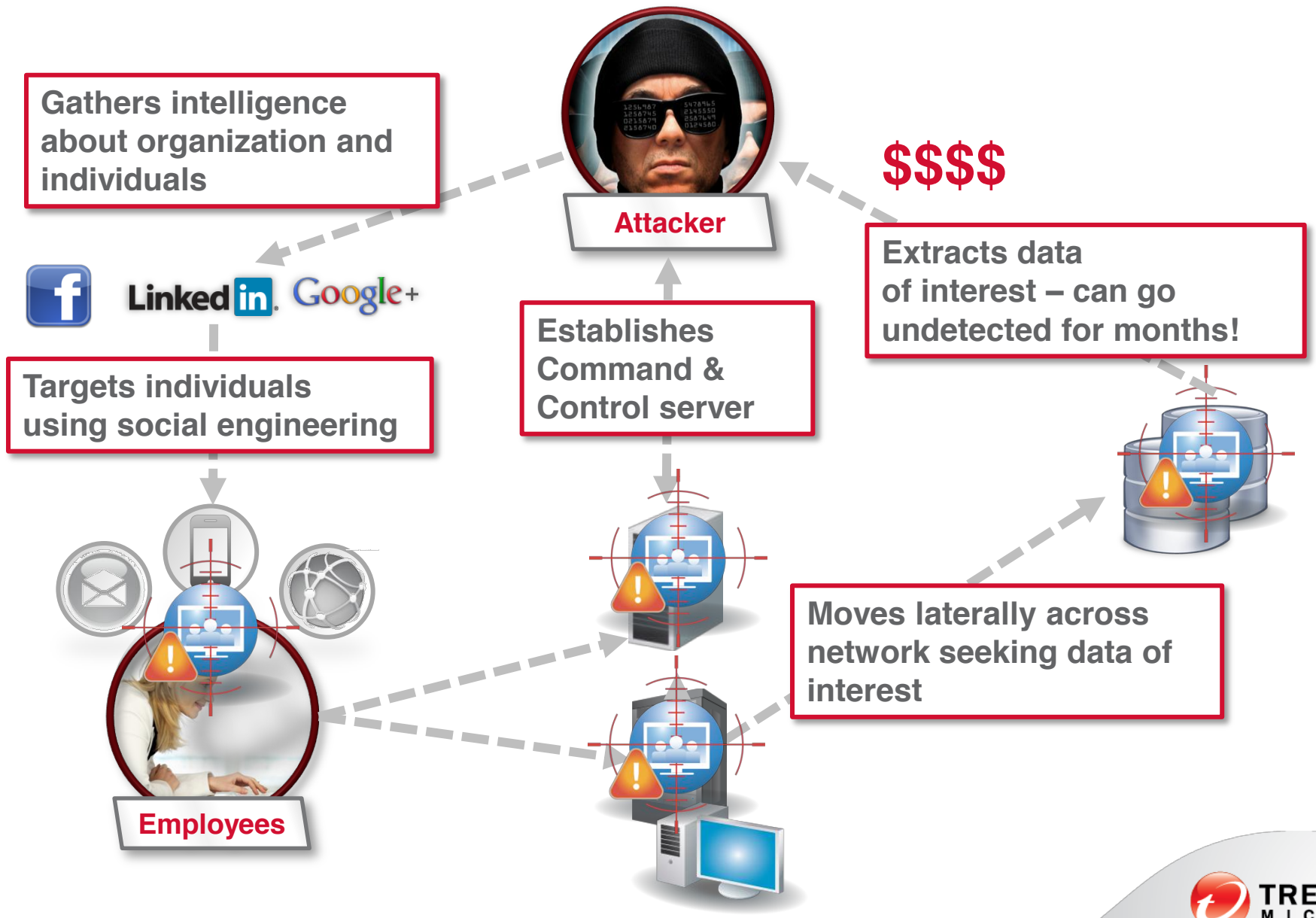
SaaS

TREND MICRO

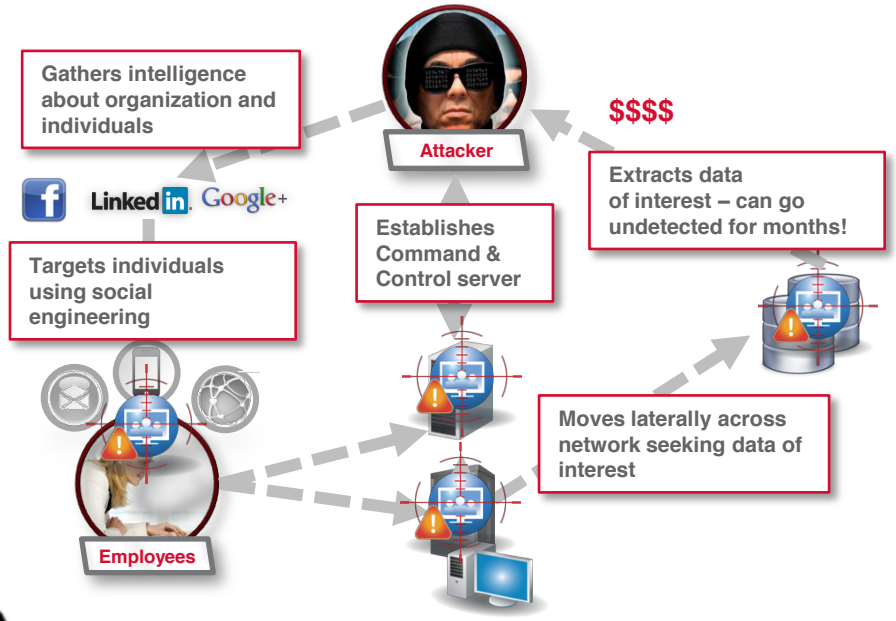
Today's Attacks: Social, Sophisticated, Stealthy!



TREND MICRO


Gathers intelligence about organization and individuals
Attacker
$$$$
Extracts data of interest – can go undetected for months!
LinkedIn
Google+
Targets individuals using social engineering
Establishes Command & Control server
Moves laterally across network seeking data of interest
Employees

TREND MICRO



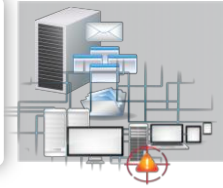
A Custom Attack NEEDS a Custom Defense!

TREND MICRO

The Custom Defense

A complete lifecycle to combat the attacks that matter to you

Detect



Specialized threat detection capability on the network and protection points

Analyze

Deep local analysis with custom sandboxing and custom global intel to fully assess threats

Adapt

Custom security blacklists & signatures block further attack at network, gateway, endpoints

Respond

Attack profiles and network-wide event intelligence guide rapid containment & remediation

TREND MICRO

The Custom Defense In Action

Adaptive Protection for All Trend Products

Network

Deep Discovery Inspector

Endpoint Security

OfficeScan

Server Security

Deep Security

Messaging Security

SMEX / SMLD
IMSVA
(Mail Server, Gateway)

Web Security (Gateway)

IWSVA

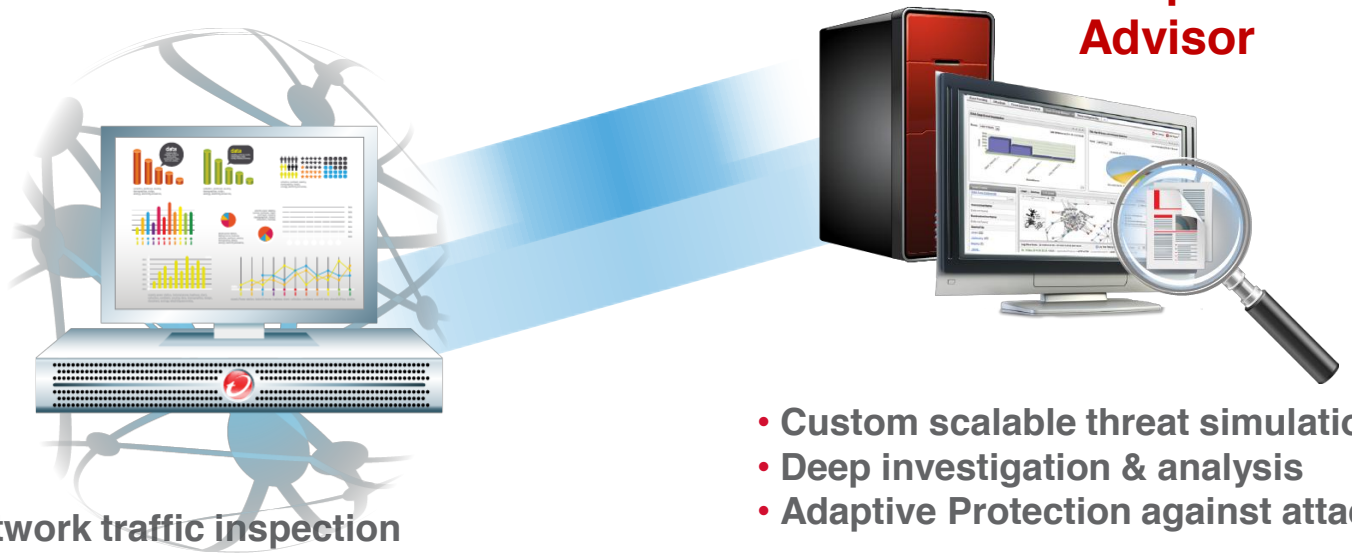
- IP/Domain blacklist updates
- AV signature updates
- SIEM Integration

TREND MICRO

Deep Discovery

The custom detection, intelligence and response capabilities you need to deploy a *Custom Defense* against the APTs & targeted attacks that matter to you

Deep Discovery Inspector



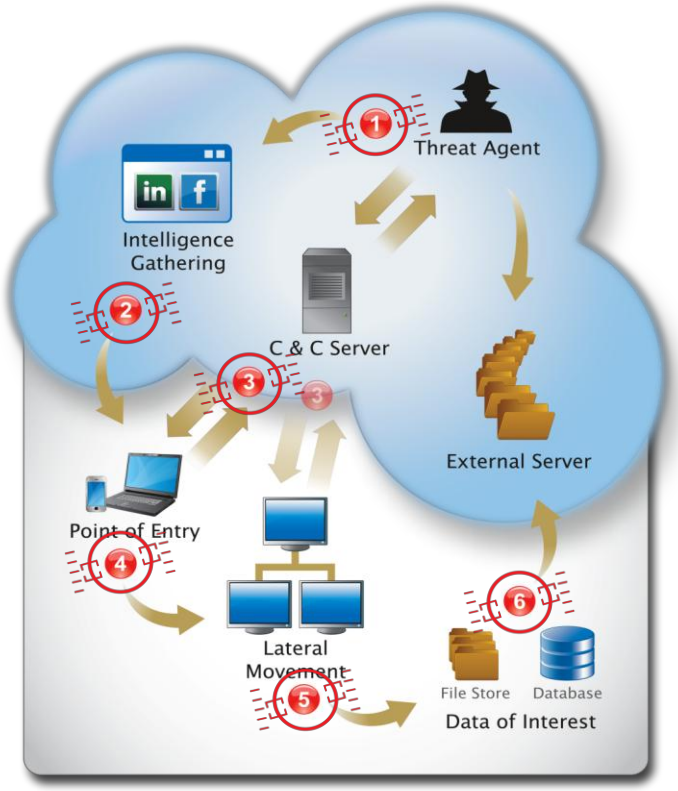
- Network traffic inspection
- Custom threat detection
- Real-time analysis & reporting

Deep Discovery Advisor

- Custom scalable threat simulation
- Deep investigation & analysis
- Adaptive Protection against attack

Visibility – Insight – Control

Deep Discovery Inspector



Advanced Threat Protection Across the Attack Sequence

- Malicious Content
- Suspect Communication
- Attacker Behavior

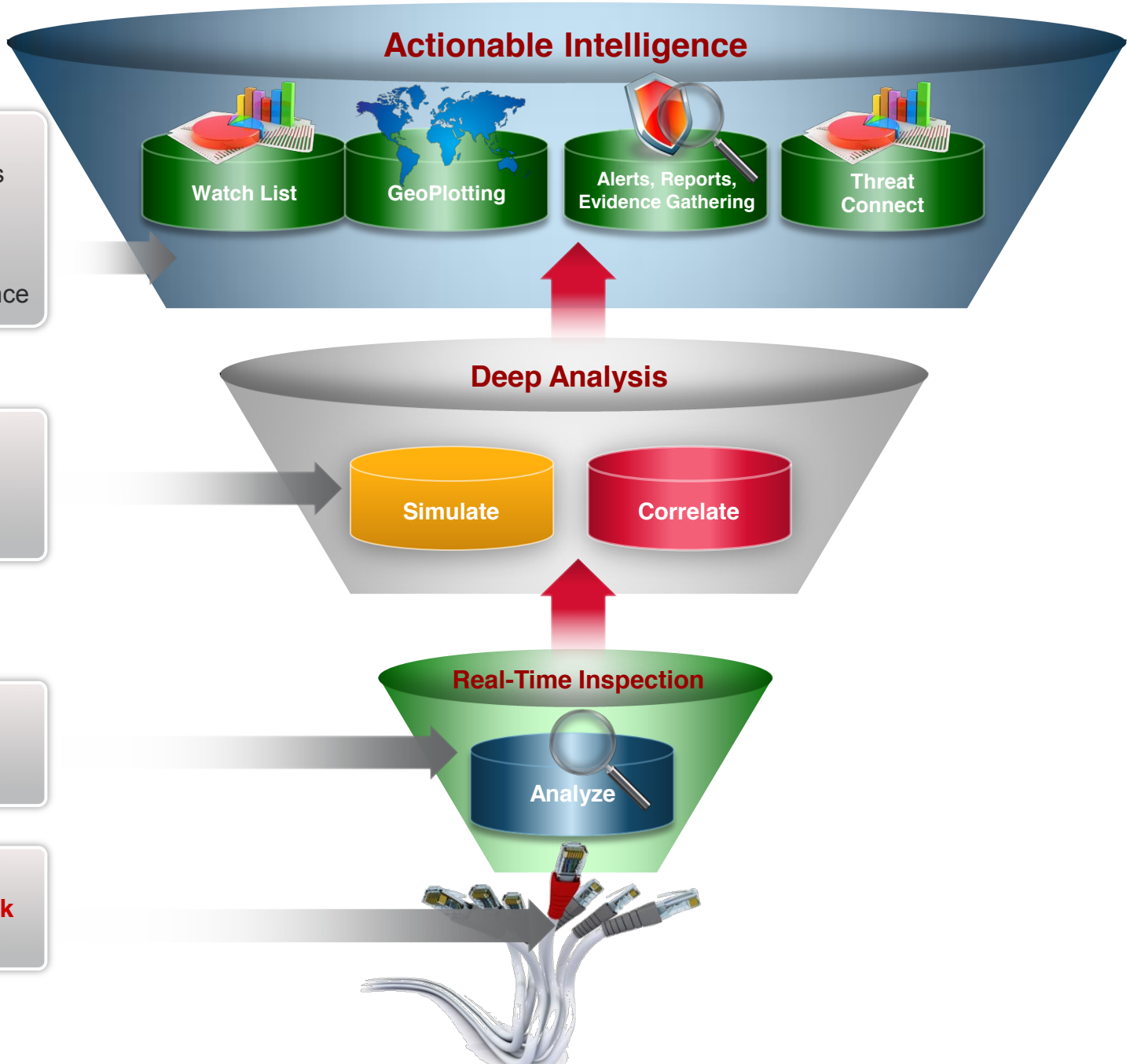
TREND MICRO

Visibility
– Real-time Dashboards
Insight
– Risk-based Analysis
Action
– Remediation Intelligence

Identify Attack Behavior & Reduce False Positives

Detect Malicious Content and Communication

Out of band network data feed of all network traffic



Deep Discovery Advisor

Threat Analyzer

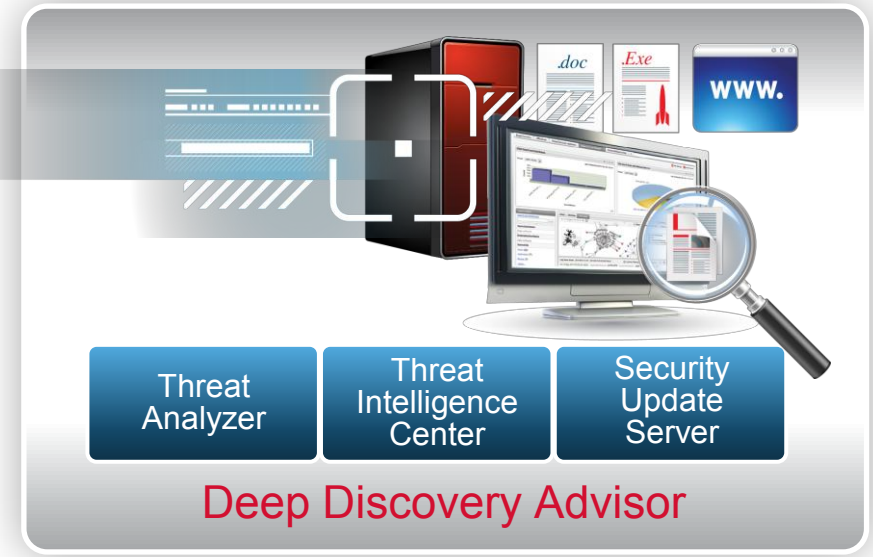
- In-depth threat simulation & analysis
- Custom sandbox execution environments
  - 24 Sandboxes per unit
- Scalable to 50,000 samples/day
- Integration with Deep Discovery Inspector
- Open, automated and manual submission

Threat Intelligence Center

- In-depth analysis of incidents & events
- Risk-focused monitoring & investigation
- Trend Micro & open security event collection
- Context-relevant actionable intelligence
- **Deep Discovery Inspector centralised reporting**

Security Update Server

- IP/URL blacklist export
- Custom security signature updates (future)



- **Custom scalable threat simulation**
- **Deep investigation & analysis**
- **Actionable intelligence & results**

Supports clustering of up to 5 units for analysing up to 50,000 samples/day

TREND MICRO

Deep Discovery Functionality Summary

Functionality	Deep Discovery Inspector	Deep Discovery Advisor
Network Traffic Analysis	Yes	No
File Sandboxing + Number	Yes (1)	Yes (24)
Hardware Appliance Option	Yes (500Mbps / 1Gbps)	Yes
Virtual Appliance Option	Yes (100,250, 500Mbps, 1Gbps)	No
Management / Analysis interface	Yes	Yes
Threat Connect	Yes	Yes
Threat Investigation Centre	No	Yes
Reporting / Analysis Consolidation	No	Yes
Integration with other Trend Solutions	No	Yes
Clustering	No	Yes

Your Custom Defense Starts With…

- Single Appliance
- Monitors 80+ different protocols across multiple ports
- Tailors sandboxes to your environment
- Analyzes with Global Threat Intelligence
- Handles BYOD, complex environments
  - Beyond Microsoft, mobile devices, laptops, Mac, and virtualization

TREND MICRO

Recognize & Respond to APTs

Deep Discovery Inspector

IaaS

- **Single** Appliance
- **Detects** attacks using 80+ Protocols
- **Detonates** in Sandbox tailored to your environment
- **Analyzes** based on Global Threat Intelligence
- **Adapts** security and **Responds** to threats to your unique environment including BYOD

Improves *Your* Defenses with **Custom Defense**

TREND MICRO

Over 600 Enterprise & Government Customers

Medical Center of Central Georgia

▶ *Protecting medical devices and the hospital operations*

The Medical Center of Central Georgia

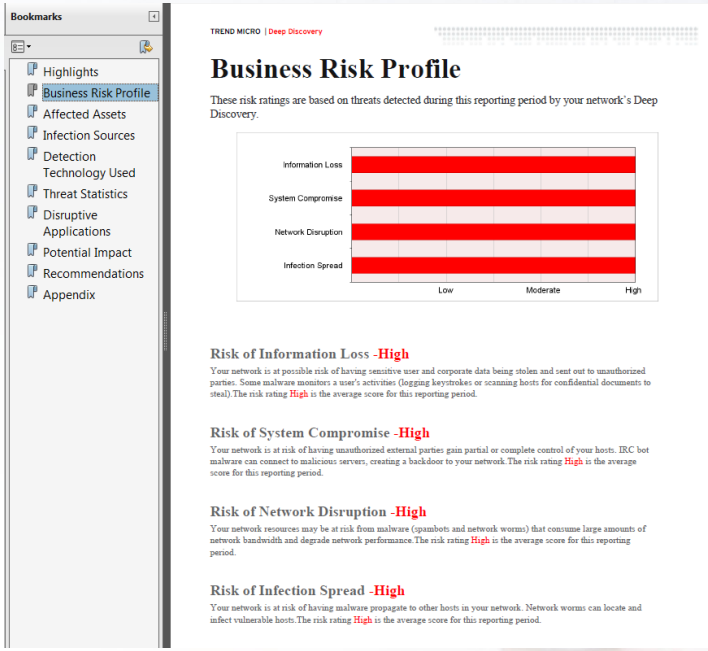
2nd largest hospital in Georgia

Network-wide visibility, control and confidence

"Trend Micro Threat Management System has already paid for itself. In the first 48 hours, this tool detected viruses on biomedical devices from several manufacturers."

Next Steps

- 2 Week Risk Assessment
- Where You Have Been Targeted?
  - Monitor Your Network
  - Review Results
  - Produce Report
- What We Have Seen?
  - 90% have active malicious malware
  - Malware on Hospital CFO Admin's PC identified in 30 minutes
  - Brazil Gov't Agency detected 11K security issues in 2 week POC
  - Major television station discovered cross-site scripting (XSS) and malware in 10 minutes!



TREND MICRO

TREND MICRO™

Thank You