Trend Micro Breach Assessment

Prepared for: Sample Report

Breach Assessment Summary

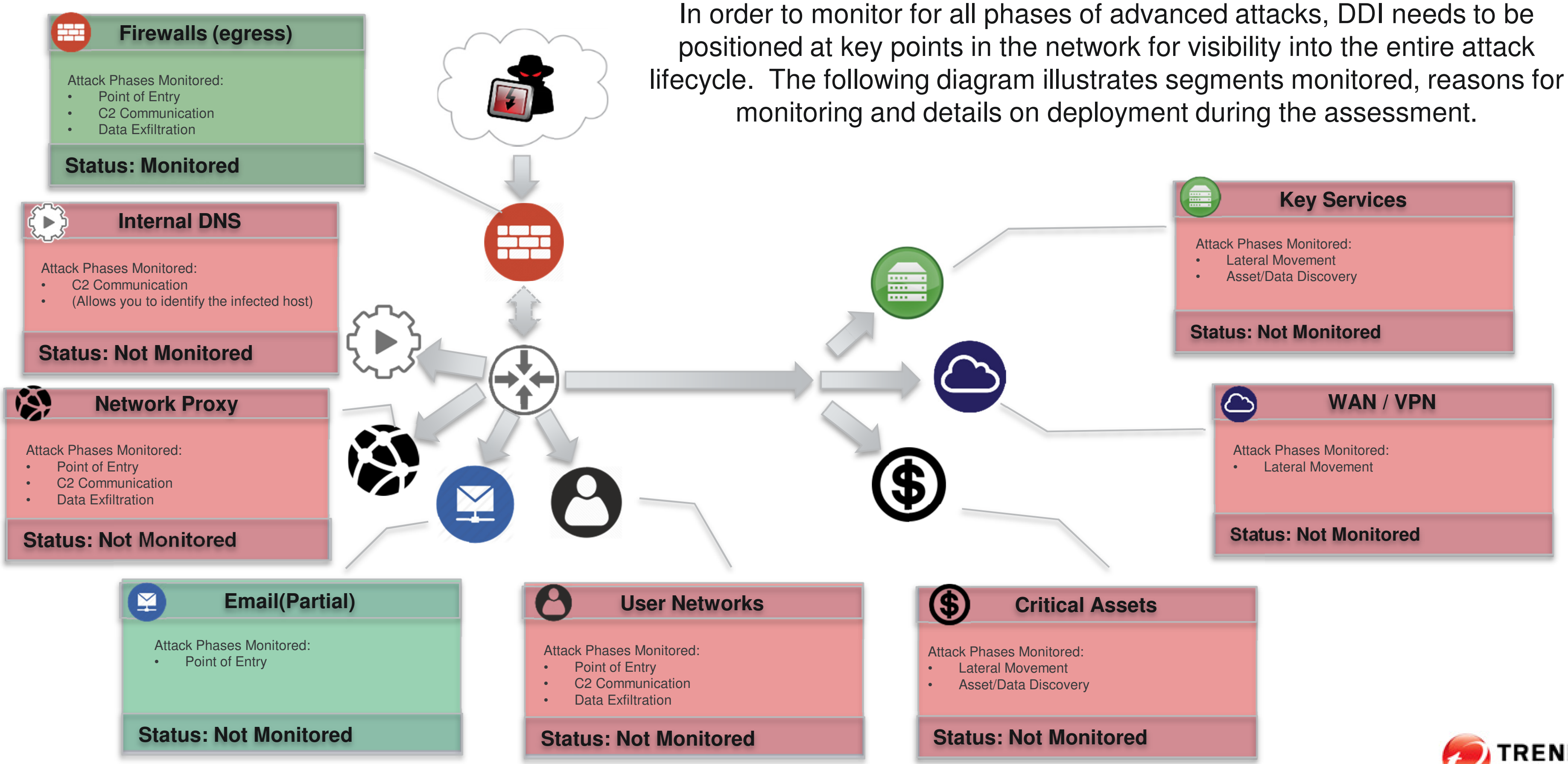
Trend Micro has completed a breach assessment on XXXX's internal networks and systems. The period of testing was from xx/19/2016 to xx/19/2016. The following document outlines findings, detail on infections, level of compromise and recommendations for improving security posture. Please review technical details on the following slides and recommendations slide for steps forward.

Host Alerts				Alert Totals		
Endpoint Infection	Lateral Movement	Ransomware		Weaponized Email	Command and Control	Zero Day Malware
20	0	5	ELEVATED	126	100	4

Results: Overall scoring on threat assessment is "ELEVATED". Elevated status indicates that "Point of Entry" infections were detected and internal hosts have active command and control channels...

DDI Placement / Monitored Segments

In order to monitor for all phases of advanced attacks, DDI needs to be positioned at key points in the network for visibility into the entire attack lifecycle. The following diagram illustrates segments monitored, reasons for monitoring and details on deployment during the assessment.



Firewalls (egress)

Attack Phases Monitored:
- Point of Entry
- C2 Communication
- Data Exfiltration

Status: Monitored

Internal DNS

Attack Phases Monitored:
- C2 Communication
- (Allows you to identify the infected host)

Status: Not Monitored

Network Proxy

Attack Phases Monitored:
- Point of Entry
- C2 Communication
- Data Exfiltration

Status: Not Monitored

Email(Partial)

Attack Phases Monitored:
- Point of Entry

Status: Not Monitored

User Networks

Attack Phases Monitored:
- Point of Entry
- C2 Communication
- Data Exfiltration

Status: Not Monitored

Critical Assets

Attack Phases Monitored:
- Lateral Movement
- Asset/Data Discovery

Status: Not Monitored

Key Services

Attack Phases Monitored:
- Lateral Movement
- Asset/Data Discovery

Status: Not Monitored

WAN / VPN

Attack Phases Monitored:
- Lateral Movement

Status: Not Monitored

TREND MICRO

Breached Hosts

There were a total of 20 Breached Hosts discovered during the Breach Assessment.

Host	Indicators
10.xx.xxx.x	Possible CRILOCK DNS Response: 3 WORM_SQLP1434.A – UDP: 80
10.xxx.xx.x (hostname)	Callback to domain in Suspicious Objects list: 3 Possible CONFICKER DNS Response: 21 Possible CRILOCK DNS Response: 9
10.xxx.xx.xx (xxxxxx)	Callback to domain in Suspicious Objects list: 3 Possible CONFICKER DNS Response: 23 Possible CRILOCK DNS Response: 7
10.xxx.xx.x (hostname)	Possible CRILOCK DNS Response: 2
xx.xx.xxx.x	Grayware-related User-Agent string in header - HTTP (Request): 2
xx.xxx.xx.x	DISCPY HTTP Request – Class 1: 1

And 14 others...

Ransomware – Hosts with Ransomware

There were a total of 5 Hosts with Ransomware alerts discovered during the Breach Assessment.

Host	Ransomware Alert Descriptions
xx.xxx.xxx.x	HEUR_JSRANSOM.O5 - SMTP (Email) JS_NEMUCOD.SMAA16 - SMTP (Email) JS_NEMUCOD.SMK13 - SMTP (Email) Ransomware URL in Web Reputation Services database - SMTP (Email)
xx.xxx.xx.x	Possible CRILOCK DNS Response HEUR_JSRANSOM.O5 - SMTP (Email) JS_NEMUCOD.SMAA16 - SMTP (Email) JS_NEMUCOD.SMK13 - SMTP (Email) Ransomware URL in Web Reputation Services database - SMTP (Email)
xx.xxx.xx.x	Possible CRILOCK DNS Response
10.xxx.xx.xx (hostname)	Possible CRILOCK DNS Response
10.xxx.xx.xx (hostname)	Possible CRILOCK DNS Response

Ransomware – Threats/Counts

There were 8 types of Ransomware threats discovered during the Breach Assessment.

Threat Description	Count
JS_NEMUCOD.SMK13 - SMTP (Email)	99
Ransomware URL in Web Reputation Services database - HTTP (Request)	55
Ransomware URL in Web Reputation Services database - SMTP (Email)	32
Possible CRILOCK DNS Response	25
HEUR_JSRANSOM.O5 - SMTP (Email)	1
JS_NEMUCOD.SMAA16 - SMTP (Email)	1
JS_NEMUCOD.SMK15 - POP3 (Email)	1
LOCKY - POP3 (Email)	1

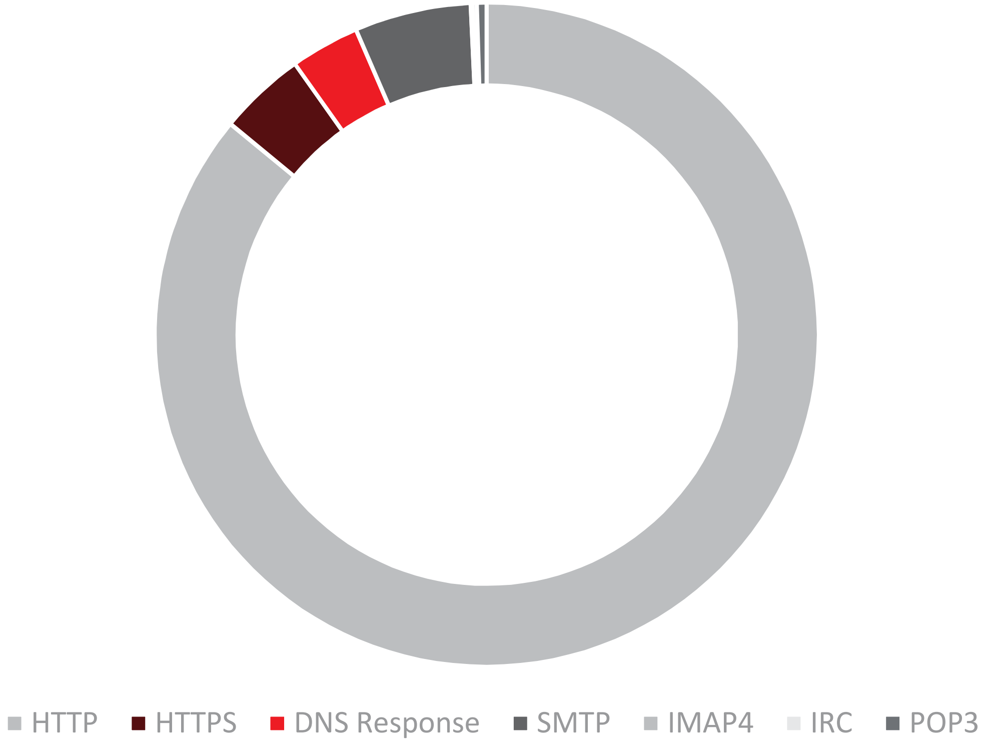
Zero-Day Malware Discovered

There was a total of 33 VA Discoveries made during the Breach Assessment. **4** of these 33 were not covered by the Anti-Virus solutions currently deployed at xxxxxxxxxxx.

File/Object	SHA1	Hosts Affected
C:\DOCUME~1\azaza\0016~1\out(1)\RI916C~1.EXE	982666E2BBF260DAEF175390B6F0220D113E625C	xx.xxx.xx.x (hostname)
C:\DOCUME~1\azaza\0016~1\out(1)\RICARD~1.EXE	FA626907AF1B803A2EF59F801C9C802093651B67	10.xxx.xx.x (hostname)
VB5U464R298X00C6Y.js	CE5ED7C7118114325E0E4EA5254834F1D4175FDA	10.xxx.xx.x
Resignation_exampley.xls	529A64DF87D66A1D7872893C6D07D70577249ABC	10.xxx.xx.x (hostname)

Protocol Distribution

A total of 2313 alerts were detected across 9 different protocols during the Breach Assessment.



Top Critical Malware Mapping

Malware Description	Total Alerts	Hosts Affected
Potential Threat (File was analyzed by Virtual Analyzer) - HTTP (Response)	2	2
JS_NEMUCOD.SMK13 - SMTP (Email)	99	1
VAWTRAK - HTTP (Request) - Variant 7	22	1
File was identified by Scan Engine and analyzed by Virtual Analyzer	11	1
Potential Threat (File was analyzed by Virtual Analyzer) - POP3 (Email)	9	1
File in Suspicious Objects list	8	1
Potential Threat (File was analyzed by Virtual Analyzer) - SMTP (Email)	5	1

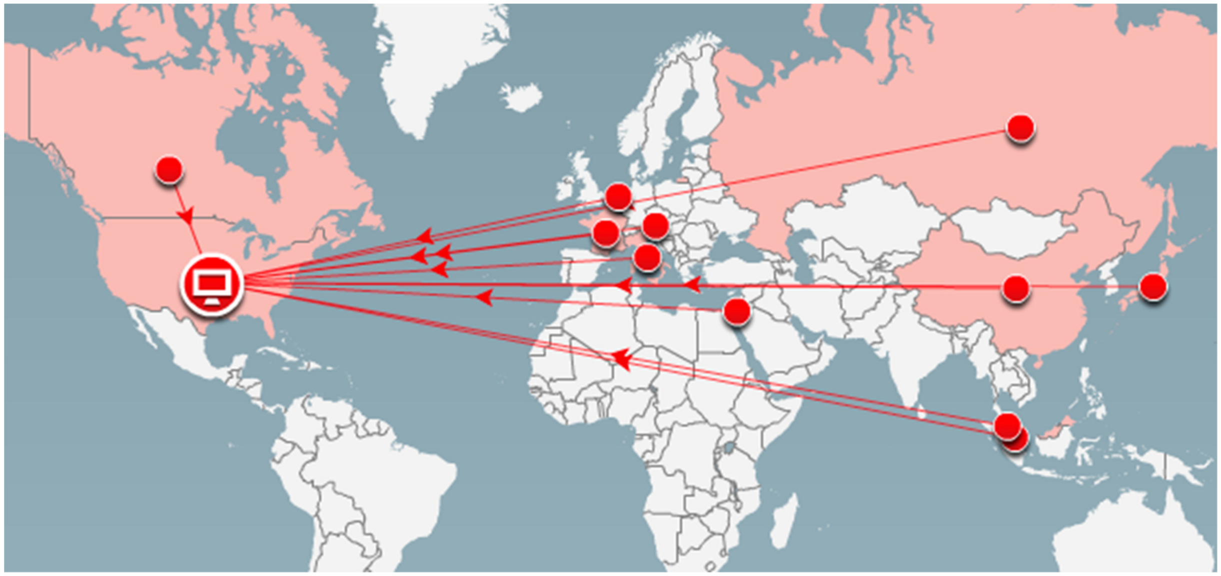
And 6 more...

C2 Detections

Hosts within XXXXXX's internal network were seen communicating with 23 distinct C2 Destinations

C2 Communications were observed from 20 individual hosts within XXXXXX's internal network

2 of the 23 distinct C2 destinations were discovered via Virtual Analysis/Sandboxing.



Hosts with Lateral Movement

Host	Descriptions	Destinations

Weaponized Emails

Recipient	Subject	Attachment/URL	Sender
johndoe@example.com	We're fighting back against OPEC	https://i.emlfiles.com/cmpimg/t/s.gif	bounce-mc.us13_60127241.464129-jon.vernon=ww.com@mail130.atl121.mcsv.net
Test.hidden@email.com	Votre sapin livré chez vous dès samedi matin !	http://newsletter.aunomdelarose.com/	aunomdelarose@newsletter.aunomdelarose.com
john2@example.com	Abax UK Invoice 4	Abax UK Invoice 4.zip	accounts@biomind.net
jane@example.com	ANTÓNIA, I feel very optimistic for you	http://news.welcome-order.com/	g-22264866782-22307-2200563870-1480392393120@bounce.news.welcome-order.com
jim@example.com	Cama de aviário melhora produtividade do pasto	http://www.anda.org.br/congresso/	bounce_55987959+a.11f17f45874256a4_11699e4bedad801_v53@zcsend.net
example@example.com	Resignation Letter	Resignation_xxxxxxxxx.xls	xxxxxx@outlook.com

And 120 more...

DDI – Sandboxing Evolved for Detecting Advanced Breaches

Network Traffic Analysis

* Advanced protocol analysis on 108+ protocols regardless of port.
* True Contextual Dynamic Analysis for multi-flow & multi-stage attacks.
* Reputation based detections on known bad IP's and domains.

Advanced Threat Security

* Detects unknown malware objects
* Advanced Heuristics engine detects hidden & obfuscated objects
* Detects malformed files embedded malicious content such as scripting

CENSUS File Prevalence

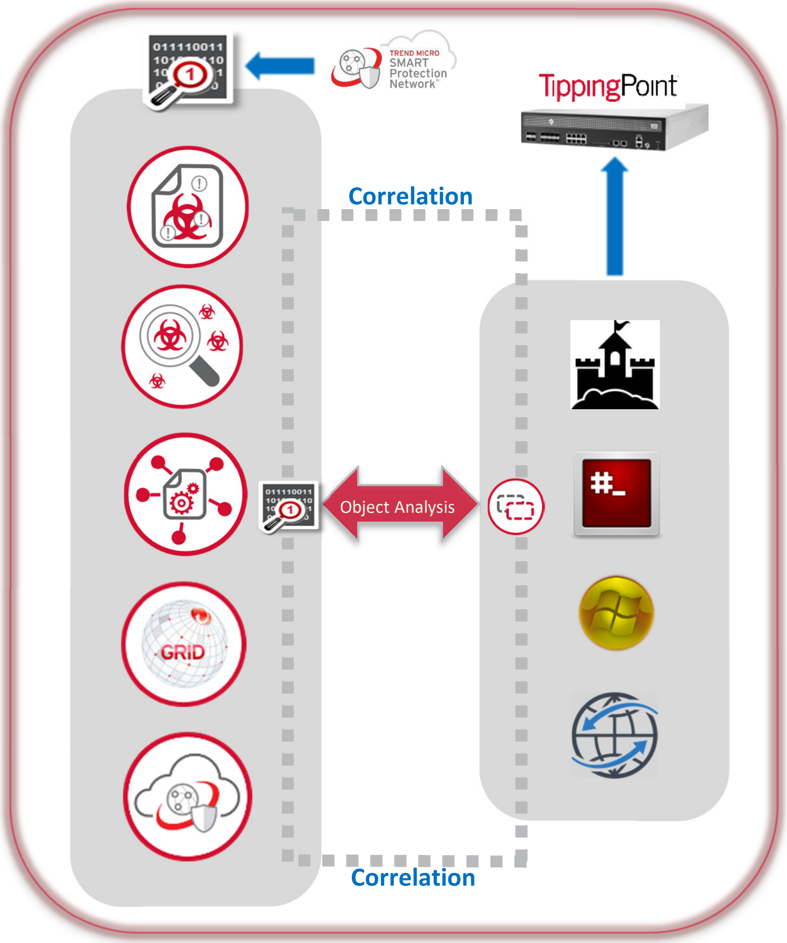
* Classification of file/hash prevalence
* Covers over 300+ million executables
* Flags & highlights unknown binaries

GRID Certified Software

* Catalogue of known "Goodware"
* Trend partners with 133 industries
* Substantially lowers false positives

RetroScan

* Retroscan analyzes logs collected and applies Trend Intelligence to uncover missed detections.



Advanced Sandboxing

* Full analysis for script, shell-code, payload detections
* Industry leading anti-evasion capacities continuously updated.
* Behavioral ransomware detection.
* Provides actionable intelligence on the attack, malicious object, detailed analysis, API system calls and C2 hits.

File and Script Emulation

* Proprietary emulators used for analysis on flash and scripted files.
* Ten+ 0-day (unknown) detections in customer environments during 2015

Gold/Custom Image Support

* Supports Importing custom sandbox images specific to your environment.
* Increases true-positive rate detections and allows for defining custom variables within the sandbox.

Live Mode

- After detonation, simulates users actual running environment.
- * Overall detection rate on C2/Dropper sites increased

* Multi-phase malware thwarted

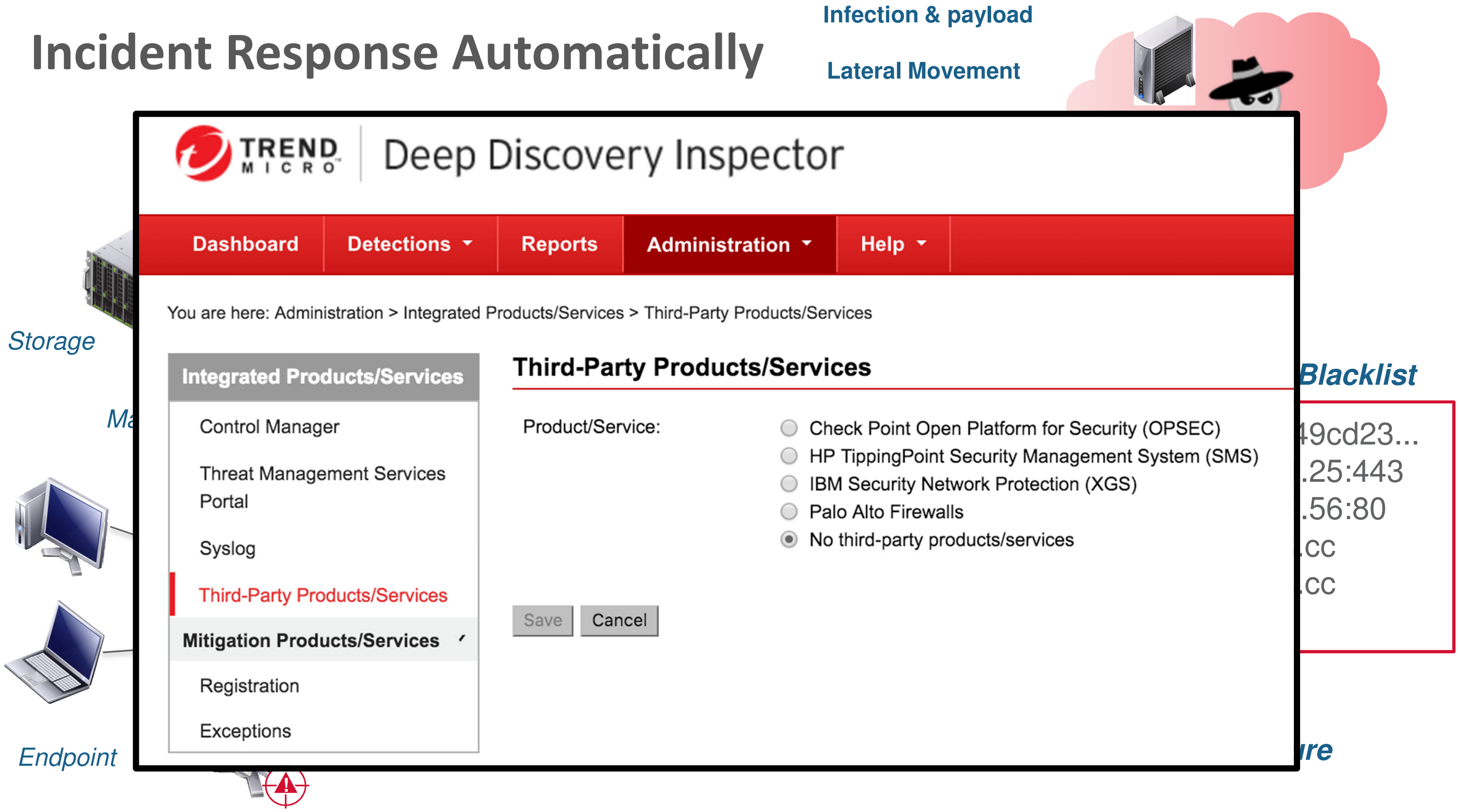
TREND MICRO

Recommendations

The following recommendations will help insure infected hosts are remediated, security posture is reviewed and steps taken to prevent future breaches and loss of company data. Recommendations will help Lower TCO, ROI & decrease Time to Remediation (TTR).

- Confirm reported infections on all endpoints and take necessary steps for remediation.
- Deploy DDI as a permanent solution on network segments monitored during the course of this assessment in addition to other critical segments of the network.
- Integrate detections and intelligence gathered from DDI into other Trend products: IMSVA, IWSVA and OSCE, TippingPoint, etc to provide automation of initial Incident Response Detection and Containment
- Continue to integrate Suspicious Objects (URLs, Domains, IPs, File Hashes) into Palo Alto Panorama for network enforcement.
- **Next Step: Architecture discussion to determine where to deploy DDI appliances**

Incident Response Automatically



TREND MICRO | Deep Discovery Inspector

Dashboard | Detections ▾ | Reports | Administration ▾ | Help ▾

You are here: Administration > Integrated Products/Services > Third-Party Products/Services

Integrated Products/Services

- Control Manager
- Threat Management Services Portal
- Syslog
- Third-Party Products/Services

Mitigation Products/Services

- Registration
- Exceptions

Third-Party Products/Services

Product/Service:

○ Check Point Open Platform for Security (OPSEC)
○ HP TippingPoint Security Management System (SMS)
○ IBM Security Network Protection (XGS)
○ Palo Alto Firewalls
● No third-party products/services

Save | Cancel

Resources