Hybrid Cloud Security

How to protect your physical, virtual or cloud servers

Webinar - March 2017-03-10 - 11h00-12h00

Presentators / Moderators

Stefaan Van Hoornick

Senior Sales Engineer – HCS Belux
Stefaan_vanhoornick@trendmicro.be
https://www.linkedin.com/in/stefaanvanhoornick/

Jerry Zwanenburg

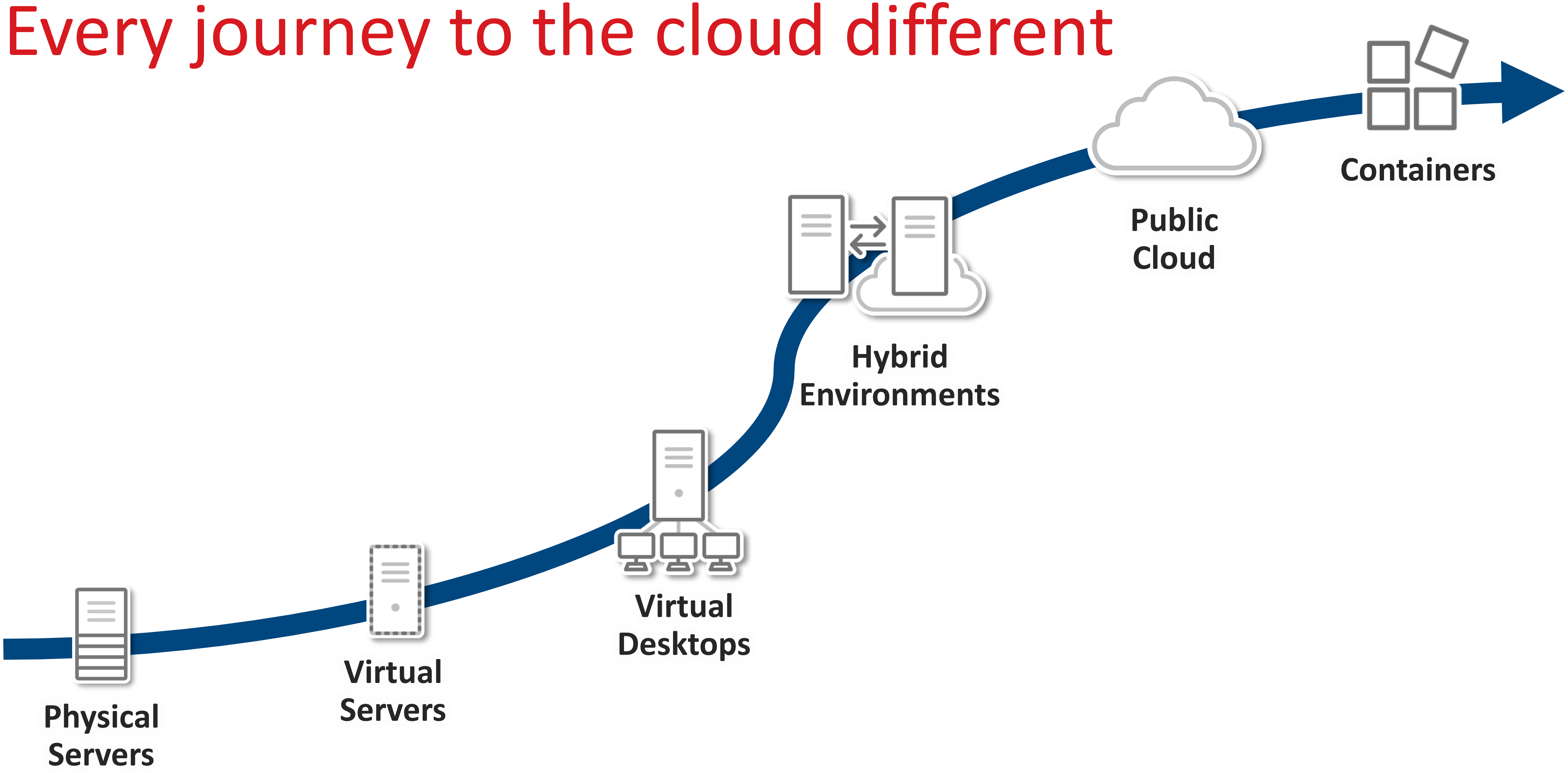
Technical Sales Manager – HCS NL
Jerry_Zwanenburg@trendmicro.com
https://www.linkedin.com/in/jerry-zwanenburg-980245/

Agenda

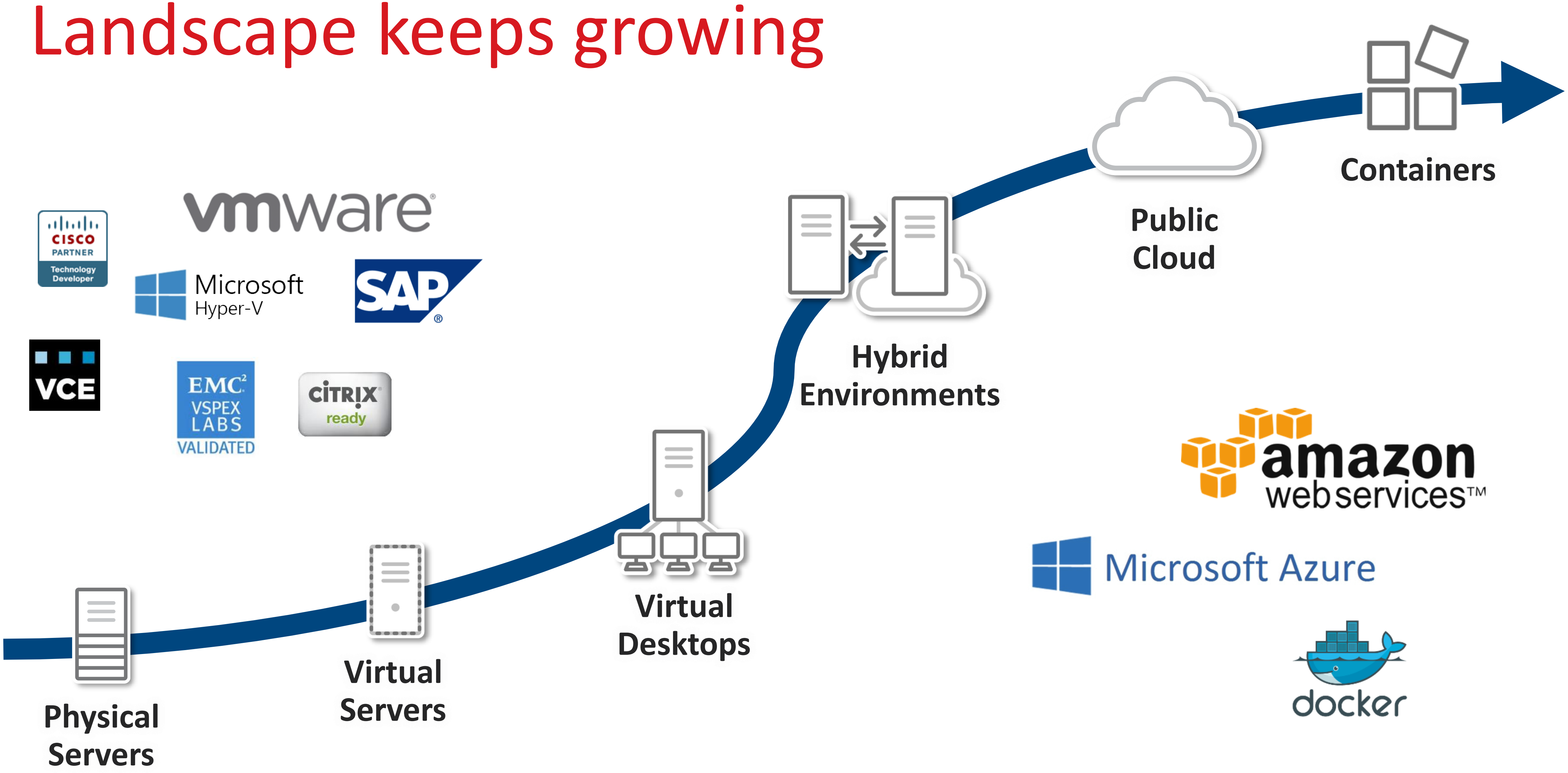
- Evolution and Strategy
- What's New in Deep Security
- Solving Server Zero-Day Threats
- Wrap-up

Evolution and Strategy

Every journey to the cloud different



Landscape keeps growing



Physical Servers

Virtual Servers

Virtual Desktops

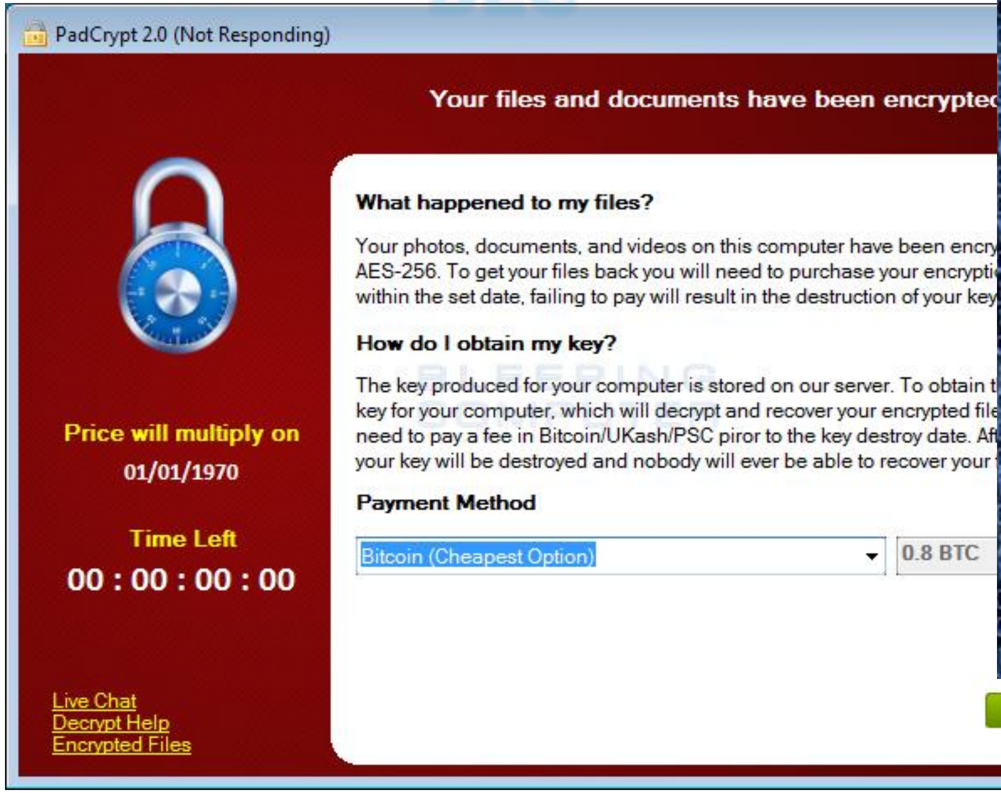
Hybrid Environments

Public Cloud

Containers

Changing Threat Landscape

BEC



PadCrypt 2.0 (Not Responding)

Your files and documents have been encrypted

What happened to my files?

Your photos, documents, and videos on this computer have been encry
AES-256. To get your files back you will need to purchase your encrypti
within the set date, failing to pay will result in the destruction of your key

How do I obtain my key?

The key produced for your computer is stored on our server. To obtain t
key for your computer, which will decrypt and recover your encrypted file
need to pay a fee in Bitcoin/UKash/PSC piror to the key destroy date. Af
your key will be destroyed and nobody will ever be able to recover your

Payment Method

Bitcoin (Cheapest Option) 0.8 BTC

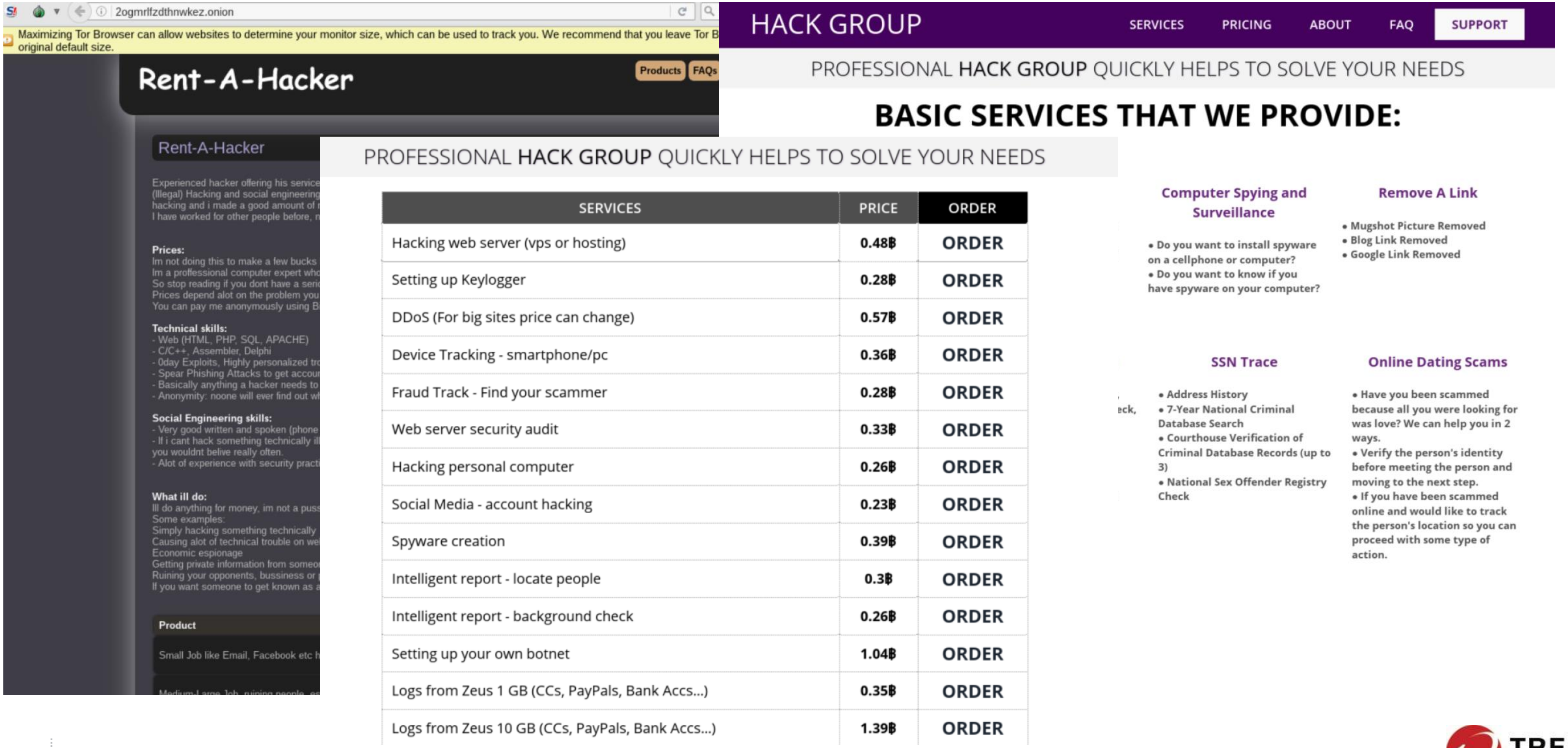
Price will multiply on
01/01/1970

Time Left
00 : 00 : 00 : 00

Ransomware

0-Day Malware

How easy is to get access to attack resources:



2ogmrlfzdthnwkez.onion

Maximizing Tor Browser can allow websites to determine your monitor size, which can be used to track you. We recommend that you leave Tor B
original default size.

Rent-A-Hacker

Rent-A-Hacker

Experienced hacker offering his service
(Illegal) Hacking and social engineering
hacking and i made a good amount of
I have worked for other people before, n

Prices:
Im not doing this to make a few bucks
Im a proffessional computer expert who
So stop reading if you dont have a seri
Prices depend alot on the problem you
You can pay me anonymously using B

Technical skills:
- Web (HTML, PHP, SQL, APACHE)
- C/C++, Assembler, Delphi
- 0day Exploits, Highly personalized tro
- Spear Phishing Attacks to get accoun
- Basically anything a hacker needs to
- Anonymity: noone will ever find out wh

Social Engineering skills:
- Very good written and spoken (phone
- If i cant hack something technically ill
you wouldnt belive really often.
- Alot of experience with security practi

What ill do:
Ill do anything for money, im not a puss
Some examples:
Simply hacking something technically
Causing alot of technical trouble on we
Economic espionage
Getting private information from someo
Ruining your opponents, bussiness or
If you want someone to get known as a

Product

Small Job like Email, Facebook etc h

Medium-Large Job, ruining people, es

PROFESSIONAL **HACK GROUP** QUICKLY HELPS TO SOLVE YOUR NEEDS

SERVICES	PRICE	ORDER
Hacking web server (vps or hosting)	0.48฿	ORDER
Setting up Keylogger	0.28฿	ORDER
DDoS (For big sites price can change)	0.57฿	ORDER
Device Tracking - smartphone/pc	0.36฿	ORDER
Fraud Track - Find your scammer	0.28฿	ORDER
Web server security audit	0.33฿	ORDER
Hacking personal computer	0.26฿	ORDER
Social Media - account hacking	0.23฿	ORDER
Spyware creation	0.39฿	ORDER
Intelligent report - locate people	0.3฿	ORDER
Intelligent report - background check	0.26฿	ORDER
Setting up your own botnet	1.04฿	ORDER
Logs from Zeus 1 GB (CCs, PayPals, Bank Accs...)	0.35฿	ORDER
Logs from Zeus 10 GB (CCs, PayPals, Bank Accs...)	1.39฿	ORDER

HACK GROUP

PROFESSIONAL **HACK GROUP** QUICKLY HELPS TO SOLVE YOUR NEEDS

BASIC SERVICES THAT WE PROVIDE:

Computer Spying and Surveillance

- Do you want to install spyware on a cellphone or computer?
- Do you want to know if you have spyware on your computer?

Remove A Link

- Mugshot Picture Removed
- Blog Link Removed
- Google Link Removed

eck,

SSN Trace

- Address History
- 7-Year National Criminal Database Search
- Courthouse Verification of Criminal Database Records (up to 3)
- National Sex Offender Registry Check

Online Dating Scams

- Have you been scammed because all you were looking for was love? We can help you in 2 ways.
- Verify the person's identity before meeting the person and moving to the next step.
- If you have been scammed online and would like to track the person's location so you can proceed with some type of action.

Malware

New 'nasty' ransomware encourages victims to attack other computers

Popcorn Time malware offers users free removal if they get two other people to install link and pay

Alex Hern

@alexhern

Monday 12 December 2016 11.55 GMT

1751

If the software gets a full release, its innovative
the more widespread variants of this type of malwa

A new ransomware variant has been

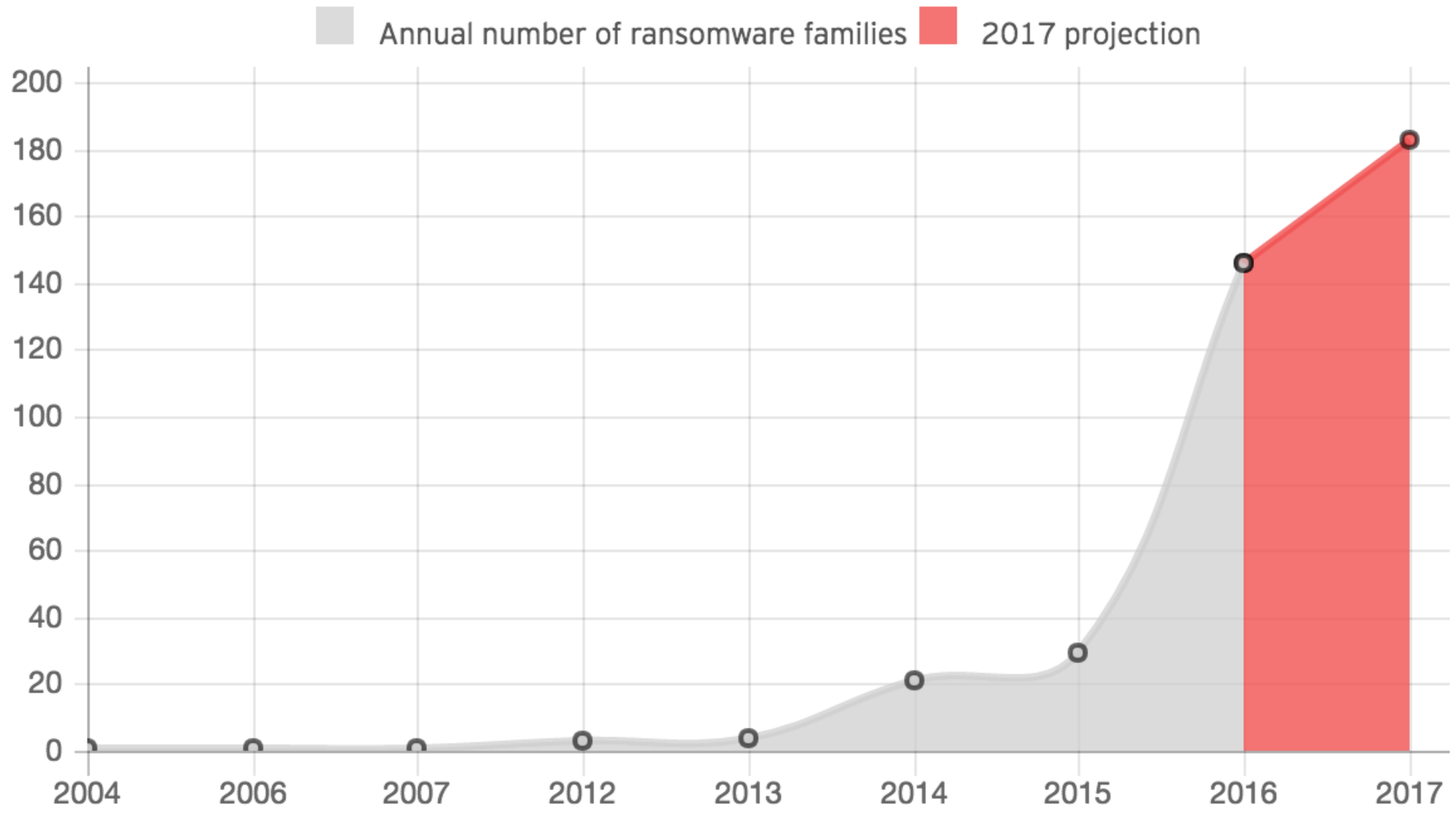
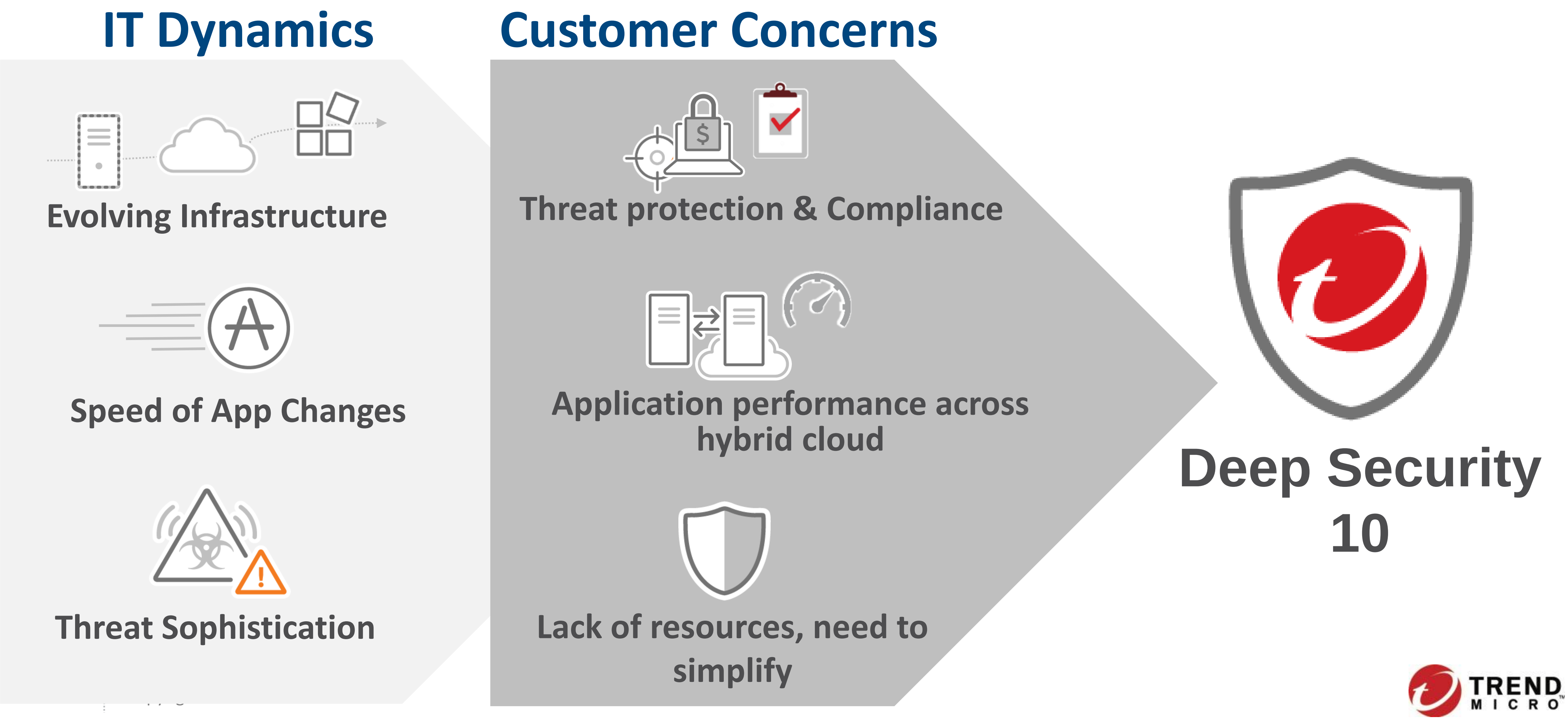


Figure 1: Annual number of ransomware families, including 2017 projection

Hybrid Cloud Security Challenges



IT Dynamics

Evolving Infrastructure

Speed of App Changes

Threat Sophistication

Customer Concerns

Threat protection & Compliance

Application performance across hybrid cloud

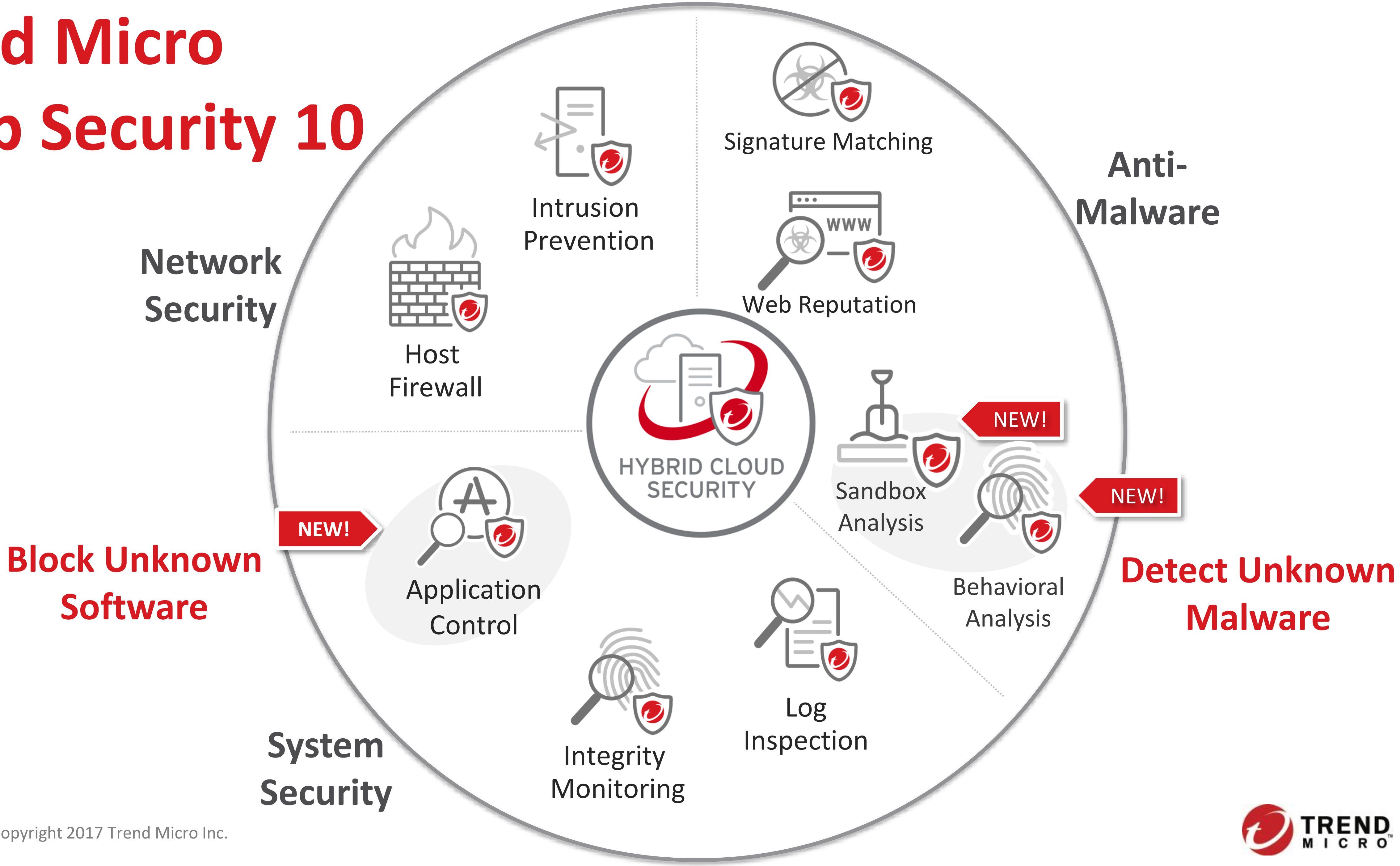
Lack of resources, need to simplify

Deep Security 10

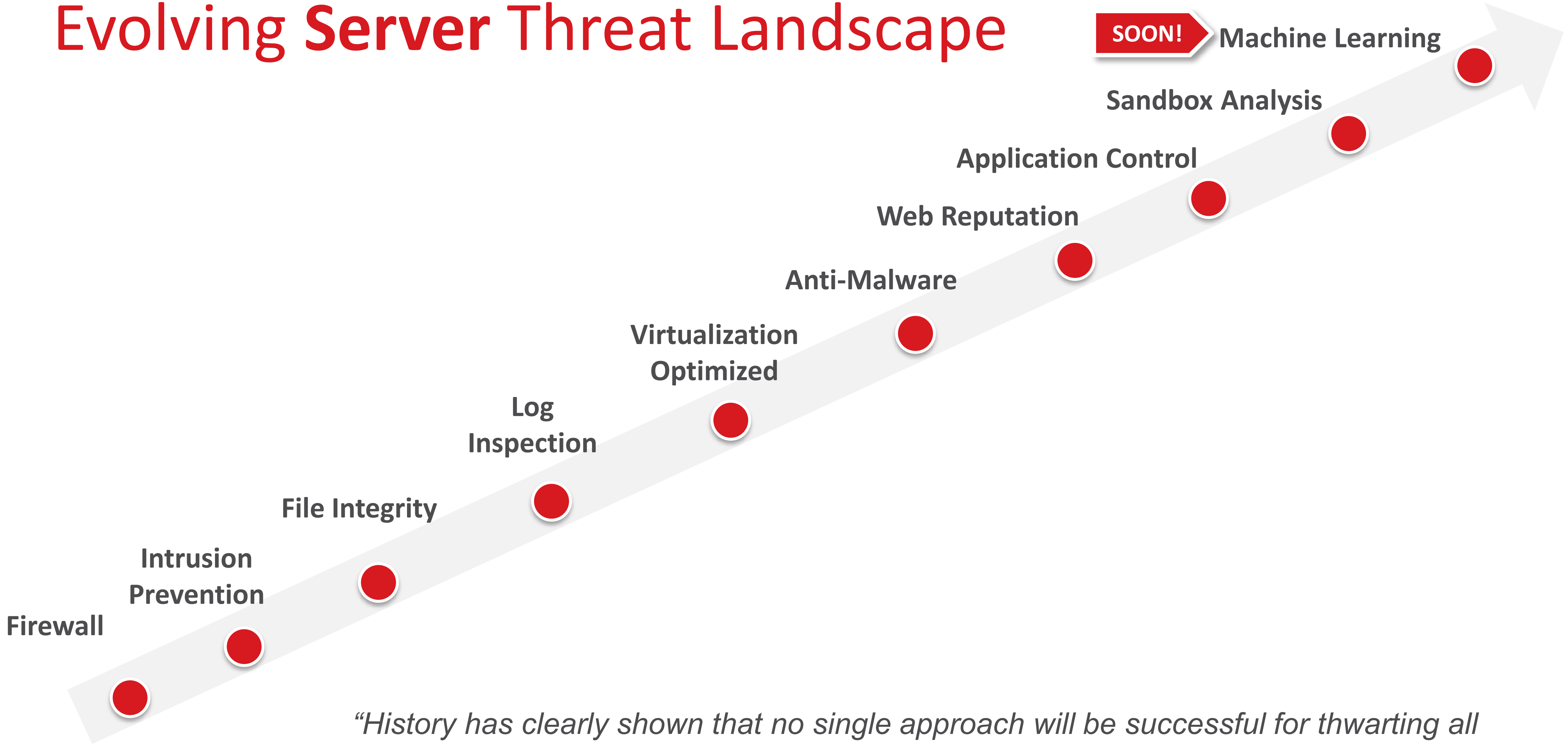
TREND MICRO

What’s new in Deep Security 10

Trend Micro Deep Security 10

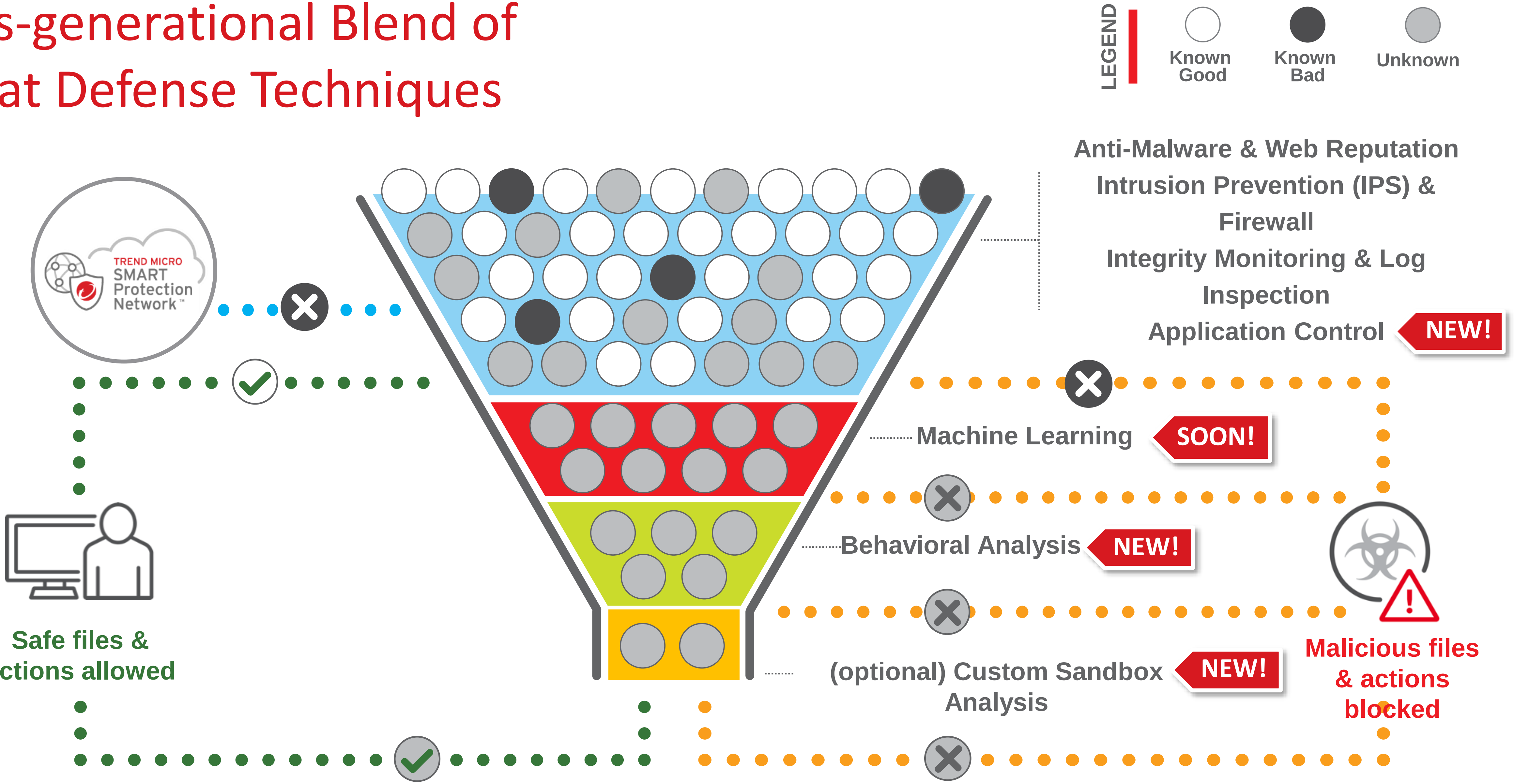


Deep Security vs. Point Solutions over the Evolving **Server** Threat Landscape



"History has clearly shown that no single approach will be successful for thwarting all types of malware attacks. Organizations and solution providers have to use an adaptive and strategic approach to malware protection." - Gartner EPP MQ 2016 quote

Cross-generational Blend of Threat Defense Techniques



Anti-Malware & Web Reputation

Intrusion Prevention (IPS) & Firewall

Integrity Monitoring & Log Inspection

Application Control NEW!

Machine Learning SOON!

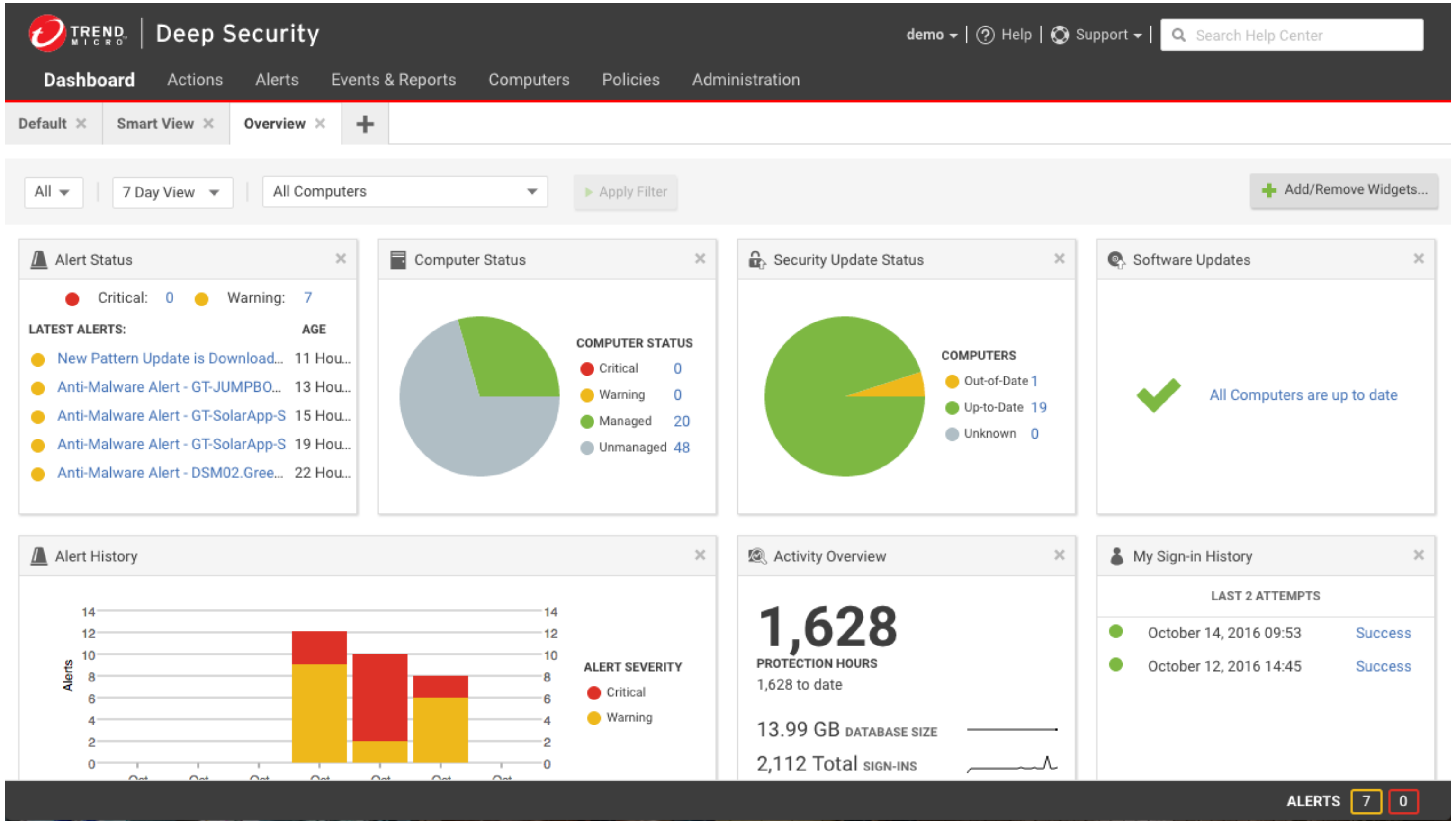
Behavioral Analysis NEW!

(optional) Custom Sandbox Analysis NEW!

Safe files & actions allowed

Malicious files & actions blocked

Visibility into Complex Environments



TREND MICRO | Deep Security

demo | Help | Support | Search Help Center

Dashboard · Actions · Alerts · Events & Reports · Computers · Policies · Administration

Default ✕ · Smart View ✕ · Overview ✕ · +

All · 7 Day View · All Computers · Apply Filter · Add/Remove Widgets...

Alert Status ✕

● Critical: 0 ● Warning: 7

LATEST ALERTS:	AGE
● New Pattern Update is Download...	11 Hou...
● Anti-Malware Alert - GT-JUMPBO...	13 Hou...
● Anti-Malware Alert - GT-SolarApp-S	15 Hou...
● Anti-Malware Alert - GT-SolarApp-S	19 Hou...
● Anti-Malware Alert - DSM02.Gree...	22 Hou...

Computer Status ✕

COMPUTER STATUS	
● Critical	0
● Warning	0
● Managed	20
● Unmanaged	48

Security Update Status ✕

COMPUTERS	
● Out-of-Date	1
● Up-to-Date	19
● Unknown	0

Software Updates ✕

✓ All Computers are up to date

Alert History ✕

Activity Overview ✕

1,628 PROTECTION HOURS
1,628 to date

13.99 GB DATABASE SIZE

2,112 Total SIGN-INS

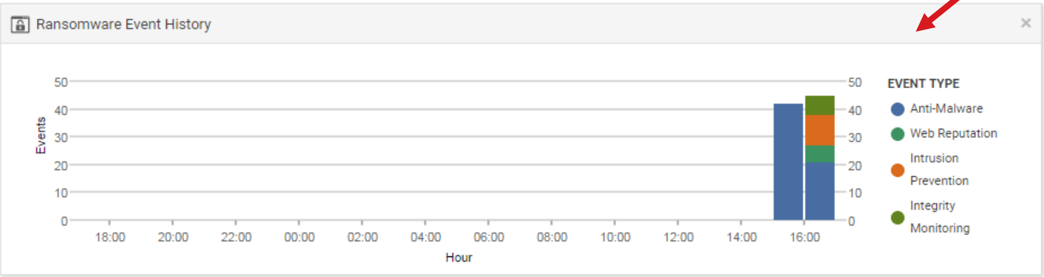
My Sign-in History ✕

LAST 2 ATTEMPTS

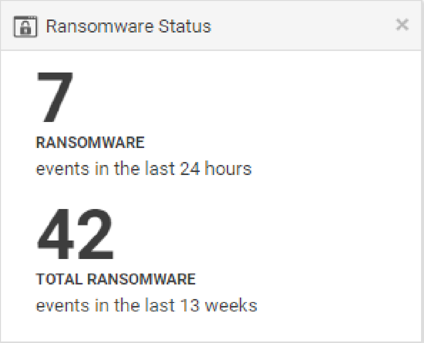
●	October 14, 2016 09:53	Success
●	October 12, 2016 14:45	Success

ALERTS 7 0

- Visual enhancements
  - Modern color palette
  - Updated graphics
- Carry-forward of familiar proven workflows
  - Intuitive multi-service configuration mgt
  - Customizable quick-view widgets
- New Ransomware widgets



Ransomware Event History ✕

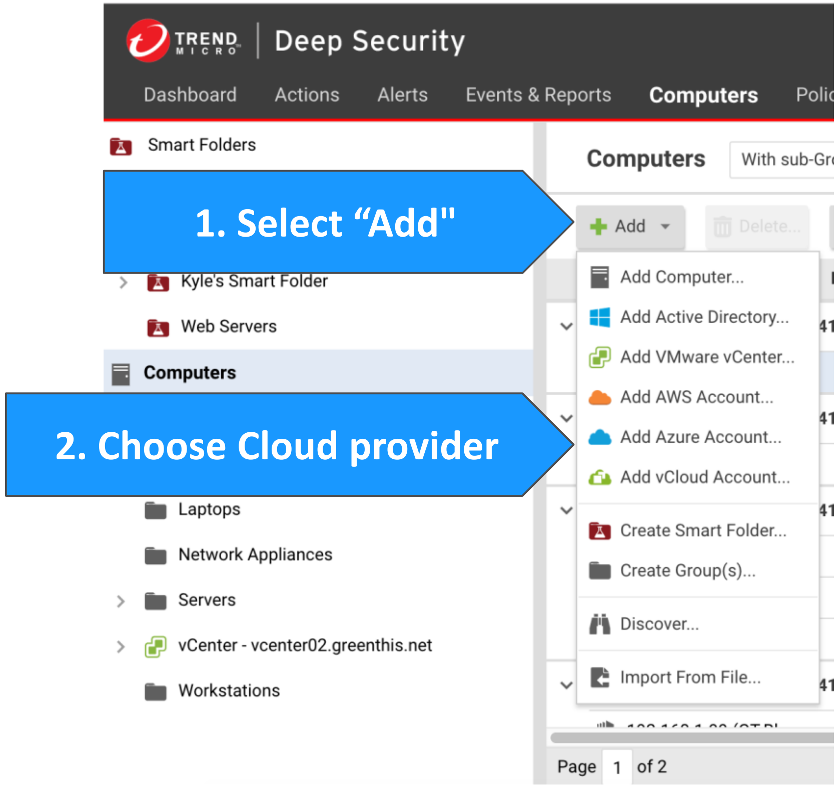


Ransomware Status ✕

7
RANSOMWARE
events in the last 24 hours

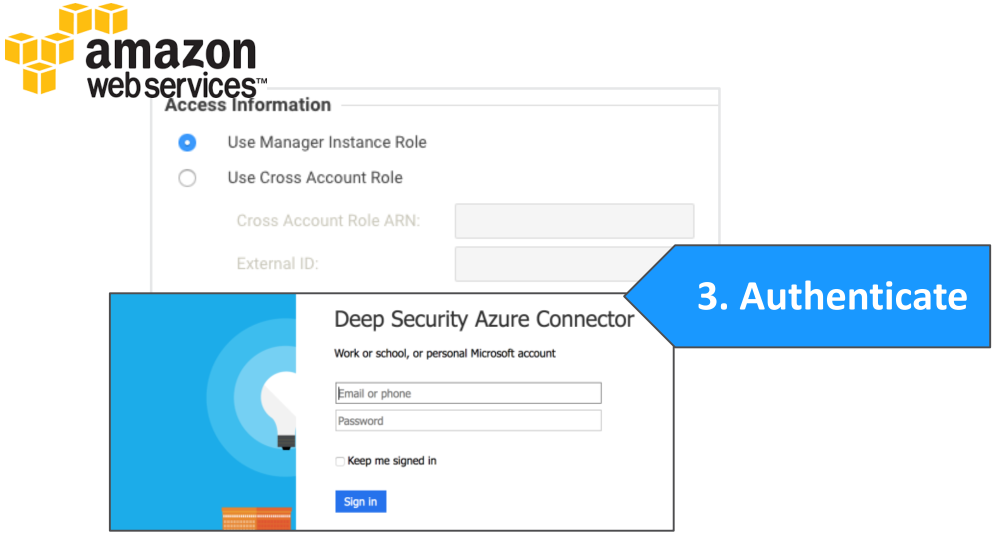
42
TOTAL RANSOMWARE
events in the last 13 weeks

Adding Cloud Accounts



1. Select “Add"

2. Choose Cloud provider



Access Information

● Use Manager Instance Role

○ Use Cross Account Role

Cross Account Role ARN:

External ID:

Deep Security Azure Connector

Work or school, or personal Microsoft account

Email or phone

Password

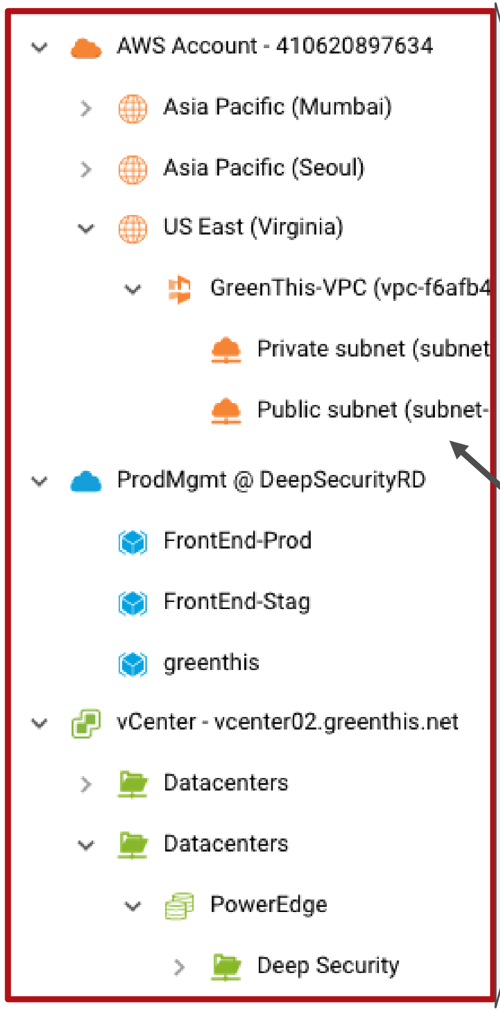
□ Keep me signed in

3. Authenticate

- Cloud Connector can be created even if Agents have already been deployed onto cloud workloads

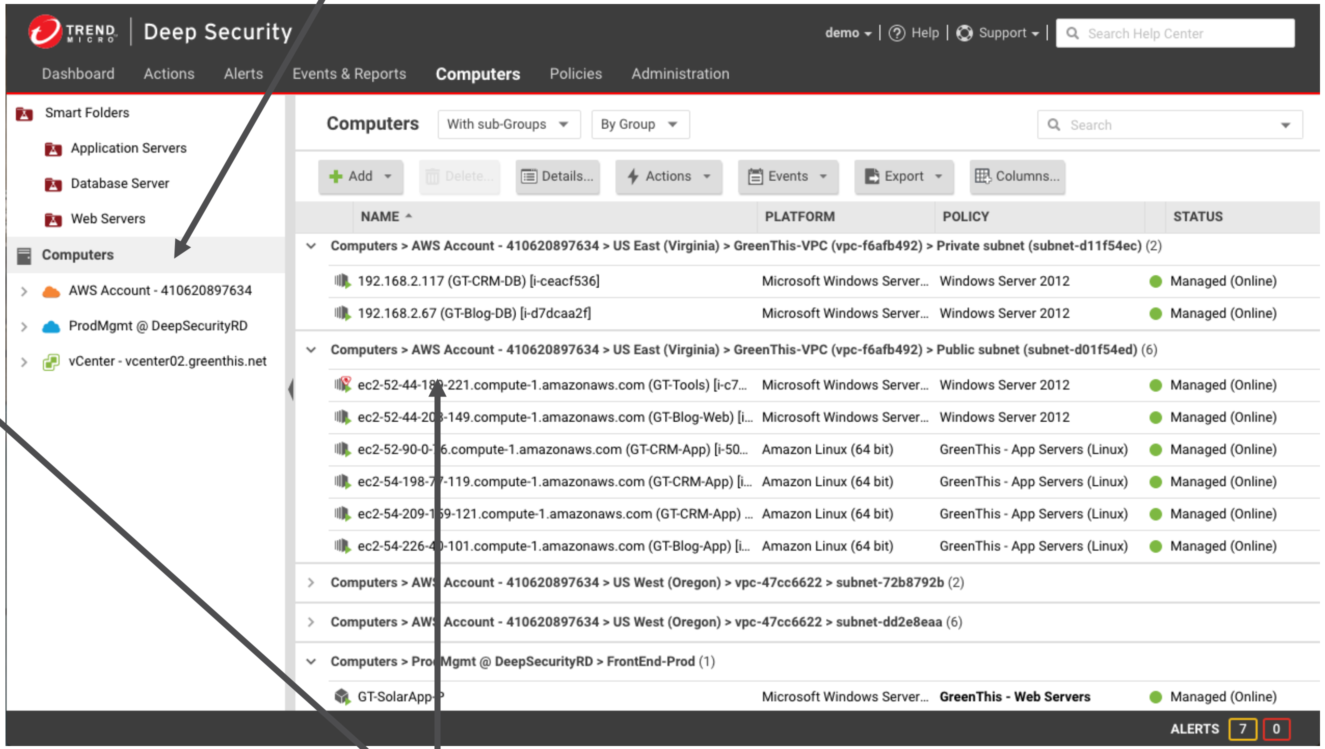
- Adding protection to new Cloud workloads
- Predefined ”Cloud Connectors” enable 3-click integration
- Connectors enable visibility and synchronization of all cloud workloads
  - Mitigates the need for manual administration of variable cloud workloads

Auto-organize Computers and Workloads



- AWS Account - 410620897634
  - Asia Pacific (Mumbai)
  - Asia Pacific (Seoul)
  - US East (Virginia)
    - GreenThis-VPC (vpc-f6afb4
      - Private subnet (subnet
      - Public subnet (subnet-
- ProdMgmt @ DeepSecurityRD
  - FrontEnd-Prod
  - FrontEnd-Stag
  - greenthis
- vCenter - vcenter02.greenthis.net
  - Datacenters
  - Datacenters
    - PowerEdge
      - Deep Security

Single-view for Data Center and Cloud



- Smart Folders
  - Application Servers
  - Database Server
  - Web Servers
- Computers
  - AWS Account - 410620897634
  - ProdMgmt @ DeepSecurityRD
  - vCenter - vcenter02.greenthis.net

Computers With sub-Groups ▾ By Group ▾ Search

NAME ▲	PLATFORM	POLICY	STATUS
Computers > AWS Account - 410620897634 > US East (Virginia) > GreenThis-VPC (vpc-f6afb492) > Private subnet (subnet-d11f54ec) (2)			
192.168.2.117 (GT-CRM-DB) [i-ceacf536]	Microsoft Windows Server...	Windows Server 2012	● Managed (Online)
192.168.2.67 (GT-Blog-DB) [i-d7dcaa2f]	Microsoft Windows Server...	Windows Server 2012	● Managed (Online)
Computers > AWS Account - 410620897634 > US East (Virginia) > GreenThis-VPC (vpc-f6afb492) > Public subnet (subnet-d01f54ed) (6)			
ec2-52-44-18[illegible]-221.compute-1.amazonaws.com (GT-Tools) [i-c7...	Microsoft Windows Server...	Windows Server 2012	● Managed (Online)
ec2-52-44-20[illegible]-149.compute-1.amazonaws.com (GT-Blog-Web) [i...	Microsoft Windows Server...	Windows Server 2012	● Managed (Online)
ec2-52-90-0-[illegible]6.compute-1.amazonaws.com (GT-CRM-App) [i-50...	Amazon Linux (64 bit)	GreenThis - App Servers (Linux)	● Managed (Online)
ec2-54-198-7[illegible]-119.compute-1.amazonaws.com (GT-CRM-App) [i...	Amazon Linux (64 bit)	GreenThis - App Servers (Linux)	● Managed (Online)
ec2-54-209-1[illegible]9-121.compute-1.amazonaws.com (GT-CRM-App) ...	Amazon Linux (64 bit)	GreenThis - App Servers (Linux)	● Managed (Online)
ec2-54-226-4[illegible]-101.compute-1.amazonaws.com (GT-Blog-App) [i...	Amazon Linux (64 bit)	GreenThis - App Servers (Linux)	● Managed (Online)
Computers > AW[illegible] Account - 410620897634 > US West (Oregon) > vpc-47cc6622 > subnet-72b8792b (2)			
Computers > AW[illegible] Account - 410620897634 > US West (Oregon) > vpc-47cc6622 > subnet-dd2e8eaa (6)			
Computers > Pro[illegible]Mgmt @ DeepSecurityRD > FrontEnd-Prod (1)			
GT-SolarApp-[illegible]	Microsoft Windows Server...	**GreenThis - Web Servers**	● Managed (Online)

ALERTS 7 0

Seamless inclusion of new Cloud Accounts and Workloads

Automatic placement of servers into infrastructure grouping

Customized views with Smart Folders

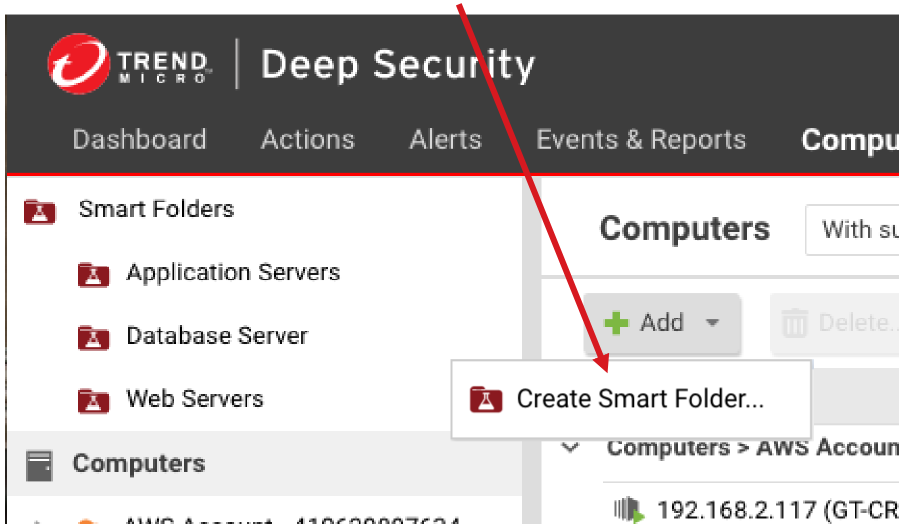
- Different teams have different requirements
- The infrastructure team is usually responsible for deploying computers and ensuring the infrastructure remains stable and reliable

- The security team is responsible for protecting the computers within that infrastructure

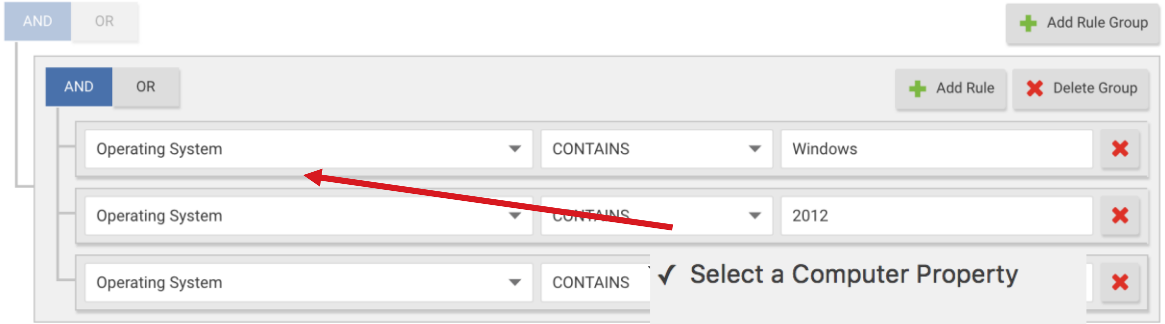
- Deep Security Smart Folders allow Security Administrators to arrange computers in a way that makes sense from a security perspective – regardless of where the infrastructure team has provisioned them
- Security Administrators can specify criteria that will dynamically populate the smart folder

Customized View of Computers and Workloads

1. Create your Smart Folder



2. Define filter rules based on Computer Properties

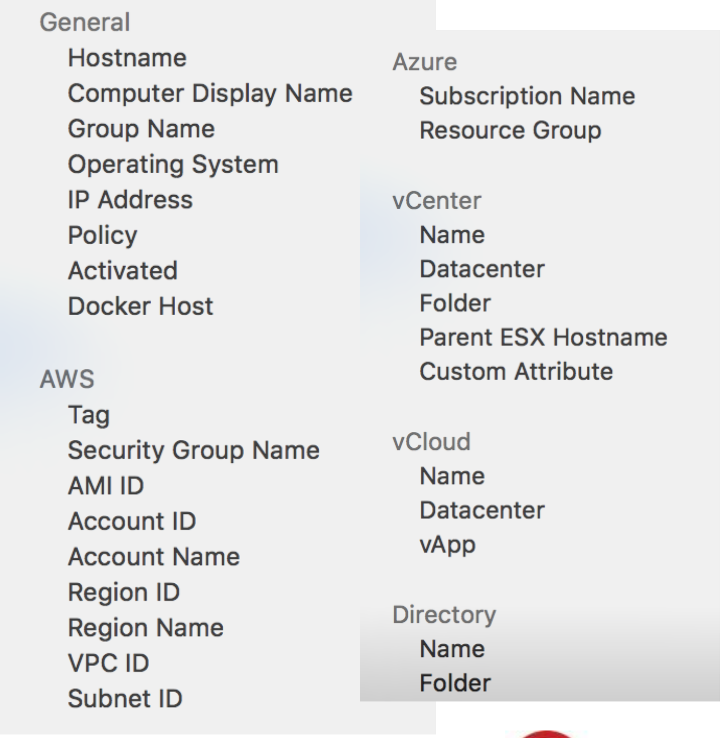


Operating System CONTAINS Windows

Operating System CONTAINS 2012

Operating System CONTAINS

✓ Select a Computer Property



General
- Hostname
- Computer Display Name
- Group Name
- Operating System
- IP Address
- Policy
- Activated
- Docker Host

AWS
- Tag
- Security Group Name
- AMI ID
- Account ID
- Account Name
- Region ID
- Region Name
- VPC ID
- Subnet ID

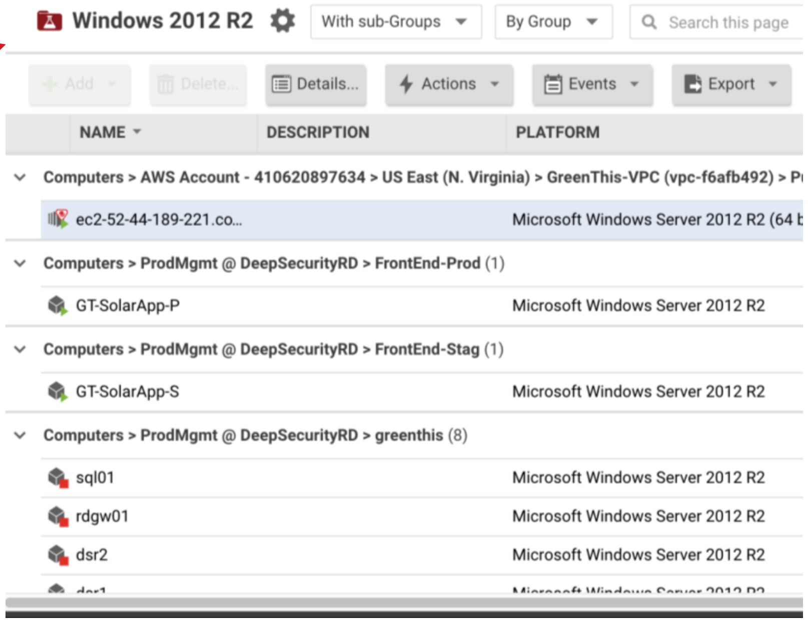
Azure
- Subscription Name
- Resource Group

vCenter
- Name
- Datacenter
- Folder
- Parent ESX Hostname
- Custom Attribute

vCloud
- Name
- Datacenter
- vApp

Directory
- Name
- Folder

3. Custom organized system-wide view of Data Center and Cloud workloads

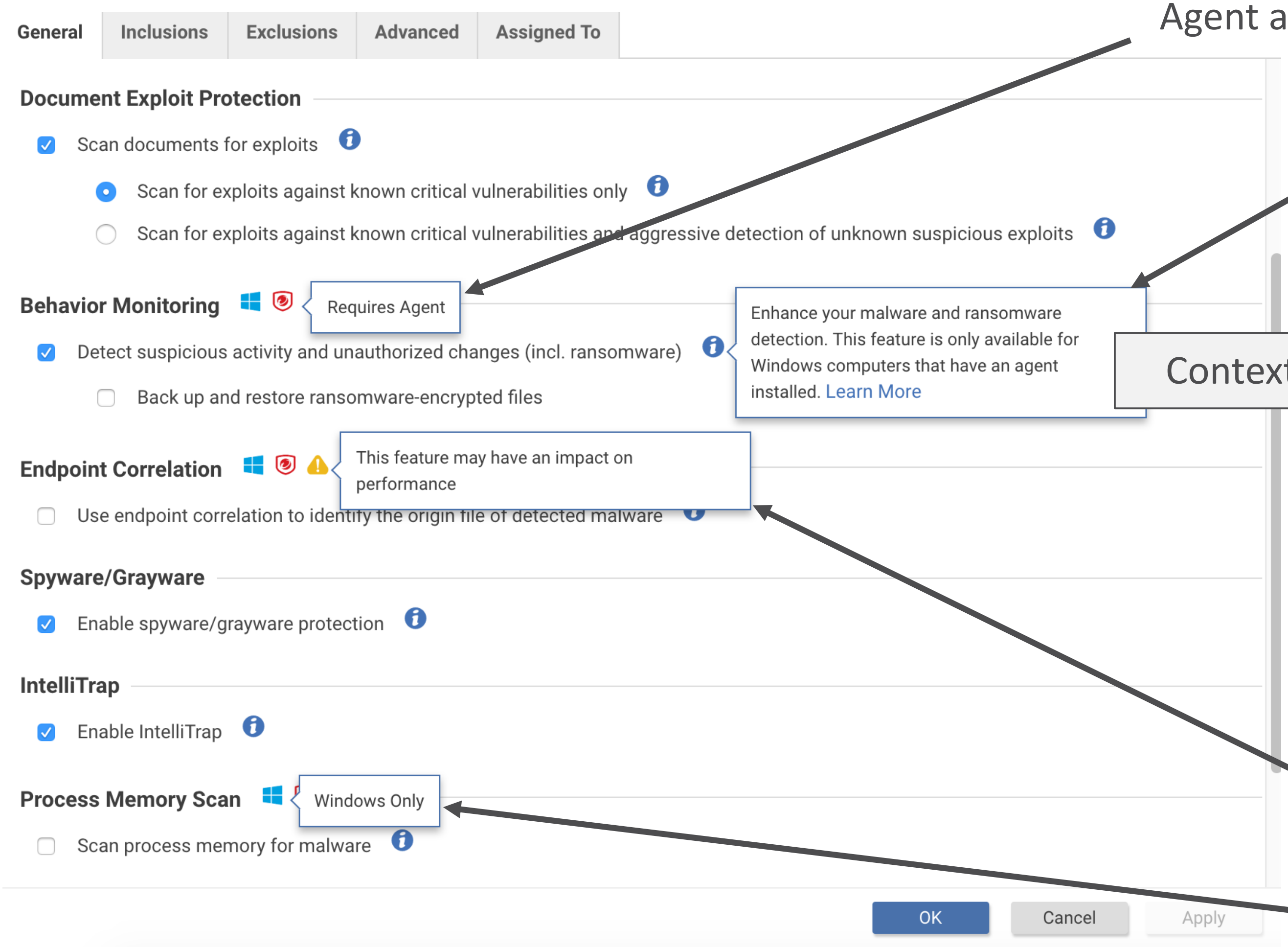


NAME	DESCRIPTION	PLATFORM
Computers > AWS Account - 410620897634 > US East (N. Virginia) > GreenThis-VPC (vpc-f6afb492) > P		
ec2-52-44-189-221.co...		Microsoft Windows Server 2012 R2 (64 b
Computers > ProdMgmt @ DeepSecurityRD > FrontEnd-Prod (1)		
GT-SolarApp-P		Microsoft Windows Server 2012 R2
Computers > ProdMgmt @ DeepSecurityRD > FrontEnd-Stag (1)		
GT-SolarApp-S		Microsoft Windows Server 2012 R2
Computers > ProdMgmt @ DeepSecurityRD > greenthis (8)		
sql01		Microsoft Windows Server 2012 R2
rdgw01		Microsoft Windows Server 2012 R2
dsr2		Microsoft Windows Server 2012 R2
dsr1		Microsoft Windows Server 2012 R2

Assistance when you need it

Is this feature or configuration supported on both Agent and Agentless?

What does this feature do? I'd like to learn more



Document Exploit Protection

☑ Scan documents for exploits

● Scan for exploits against known critical vulnerabilities only

○ Scan for exploits against known critical vulnerabilities and aggressive detection of unknown suspicious exploits

Behavior Monitoring

Requires Agent

Enhance your malware and ransomware detection. This feature is only available for Windows computers that have an agent installed. Learn More

☑ Detect suspicious activity and unauthorized changes (incl. ransomware)

□ Back up and restore ransomware-encrypted files

Endpoint Correlation

This feature may have an impact on performance

□ Use endpoint correlation to identify the origin file of detected malware

Spyware/Grayware

☑ Enable spyware/grayware protection

IntelliTrap

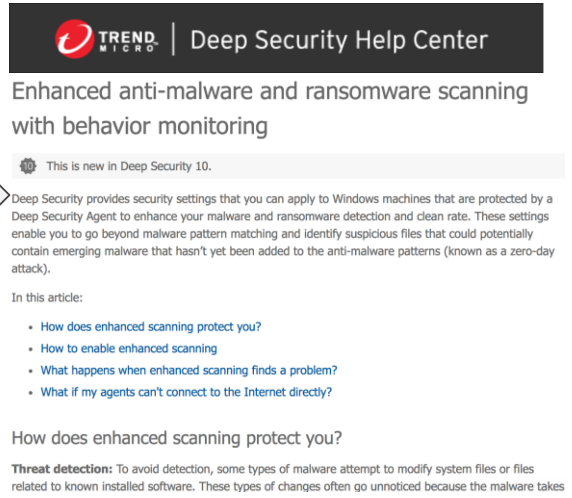
☑ Enable IntelliTrap

Process Memory Scan

Windows Only

□ Scan process memory for malware

Contextual



Enhanced anti-malware and ransomware scanning with behavior monitoring

This is new in Deep Security 10.

Deep Security provides security settings that you can apply to Windows machines that are protected by a Deep Security Agent to enhance your malware and ransomware detection and clean rate. These settings enable you to go beyond malware pattern matching and identify suspicious files that could potentially contain emerging malware that hasn't yet been added to the anti-malware patterns (known as a zero-day attack).

In this article:

- How does enhanced scanning protect you?
- How to enable enhanced scanning
- What happens when enhanced scanning finds a problem?
- What if my agents can't connect to the Internet directly?

How does enhanced scanning protect you?

Threat detection: To avoid detection, some types of malware attempt to modify system files or files related to known installed software. These types of changes often go unnoticed because the malware takes

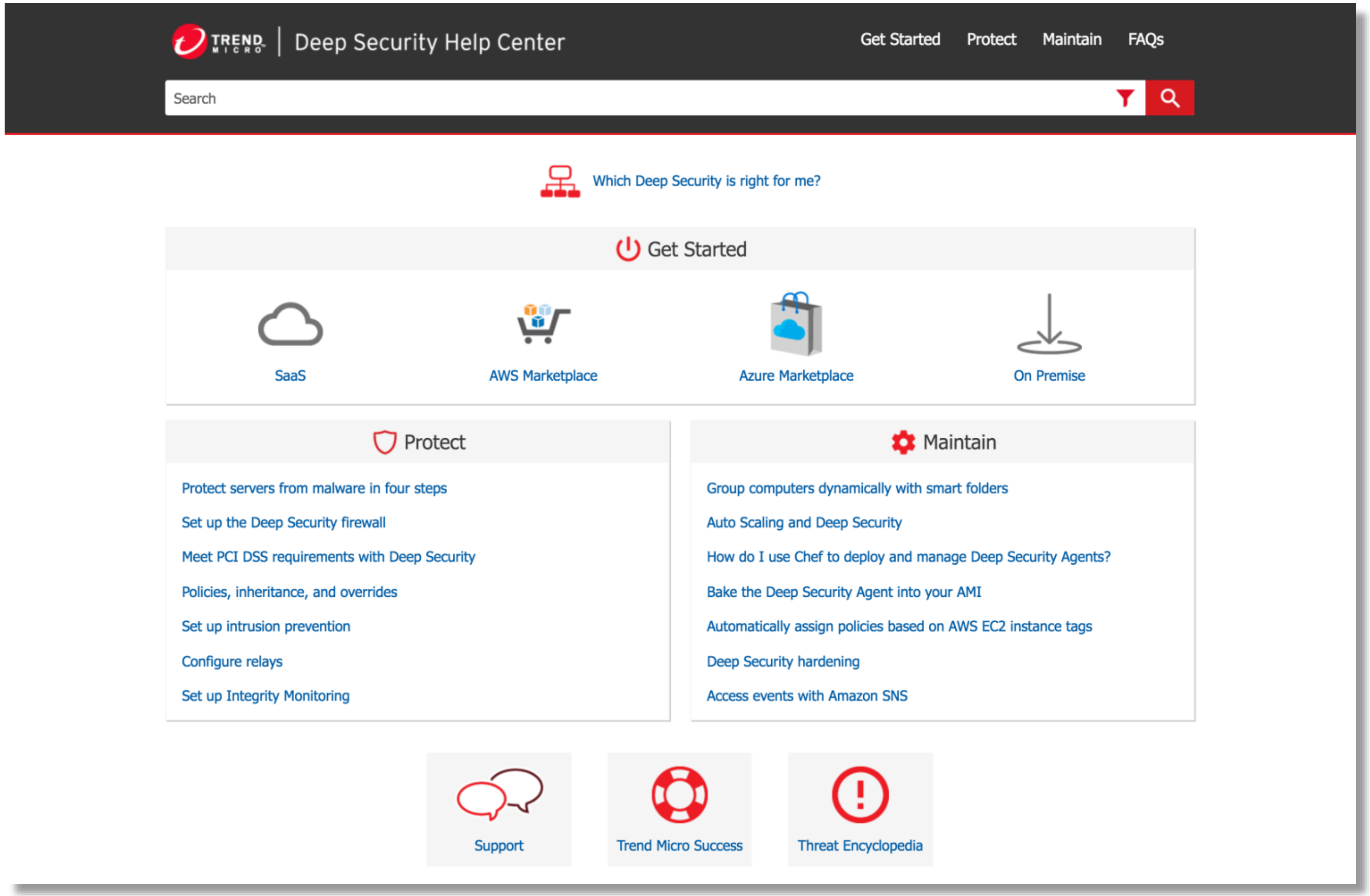
Do I need to consider resource impacts before I enable this feature?

Is this feature or configuration supported on both Windows and Linux?

Refreshed Help Center for Deep Security 10

Deep Security for Data Center, AWS, and Azure

- New Deep Security 10 Content
- Google-searchable
- Task-centric workflows
- New articles every week
- Contextual landing from DSM
- Installation, Administration and Best Practice Guides
- DSM Embedded version for air-gapped deployments



Deep Security Help Center

Which Deep Security is right for me?

Get Started

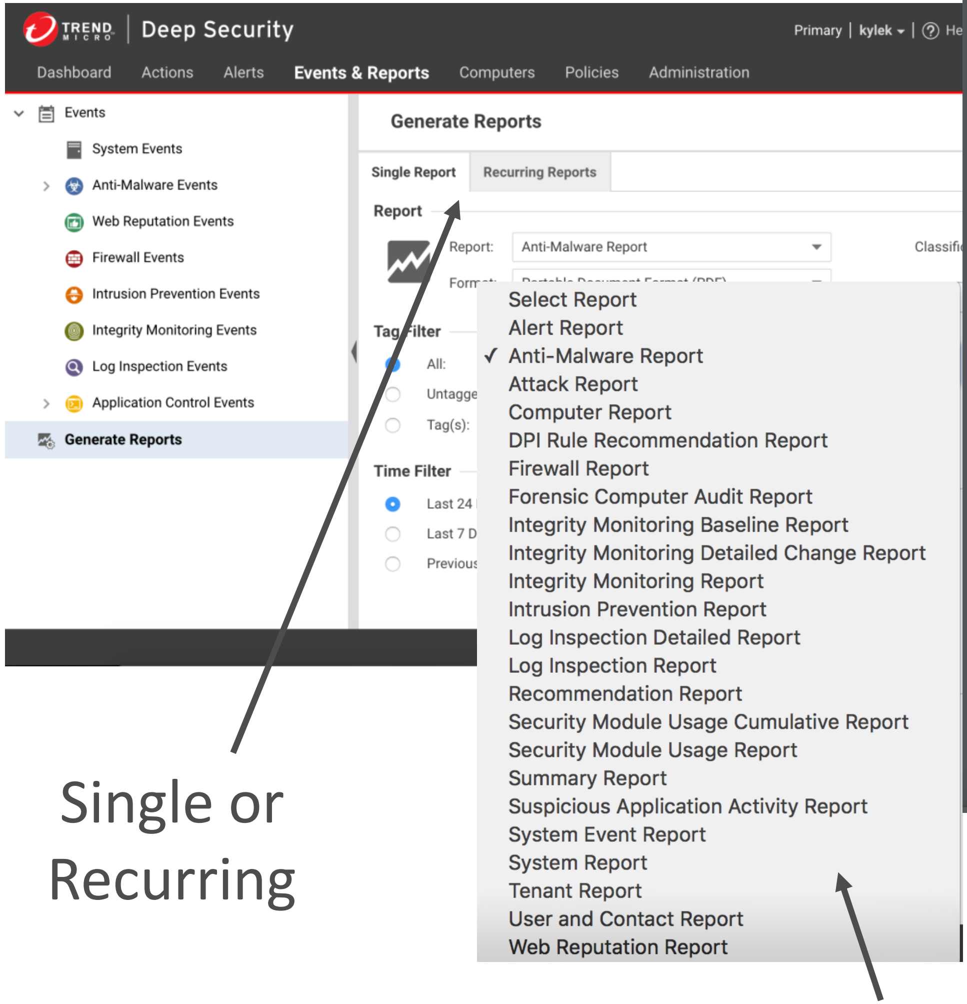
Protect

- Protect servers from malware in four steps
- Set up the Deep Security firewall
- Meet PCI DSS requirements with Deep Security
- Policies, inheritance, and overrides
- Set up intrusion prevention
- Configure relays
- Set up Integrity Monitoring

Maintain

- Group computers dynamically with smart folders
- Auto Scaling and Deep Security
- How do I use Chef to deploy and manage Deep Security Agents?
- Bake the Deep Security Agent into your AMI
- Automatically assign policies based on AWS EC2 instance tags
- Deep Security hardening
- Access events with Amazon SNS

Flexible Summary Report Generator



Generate Reports

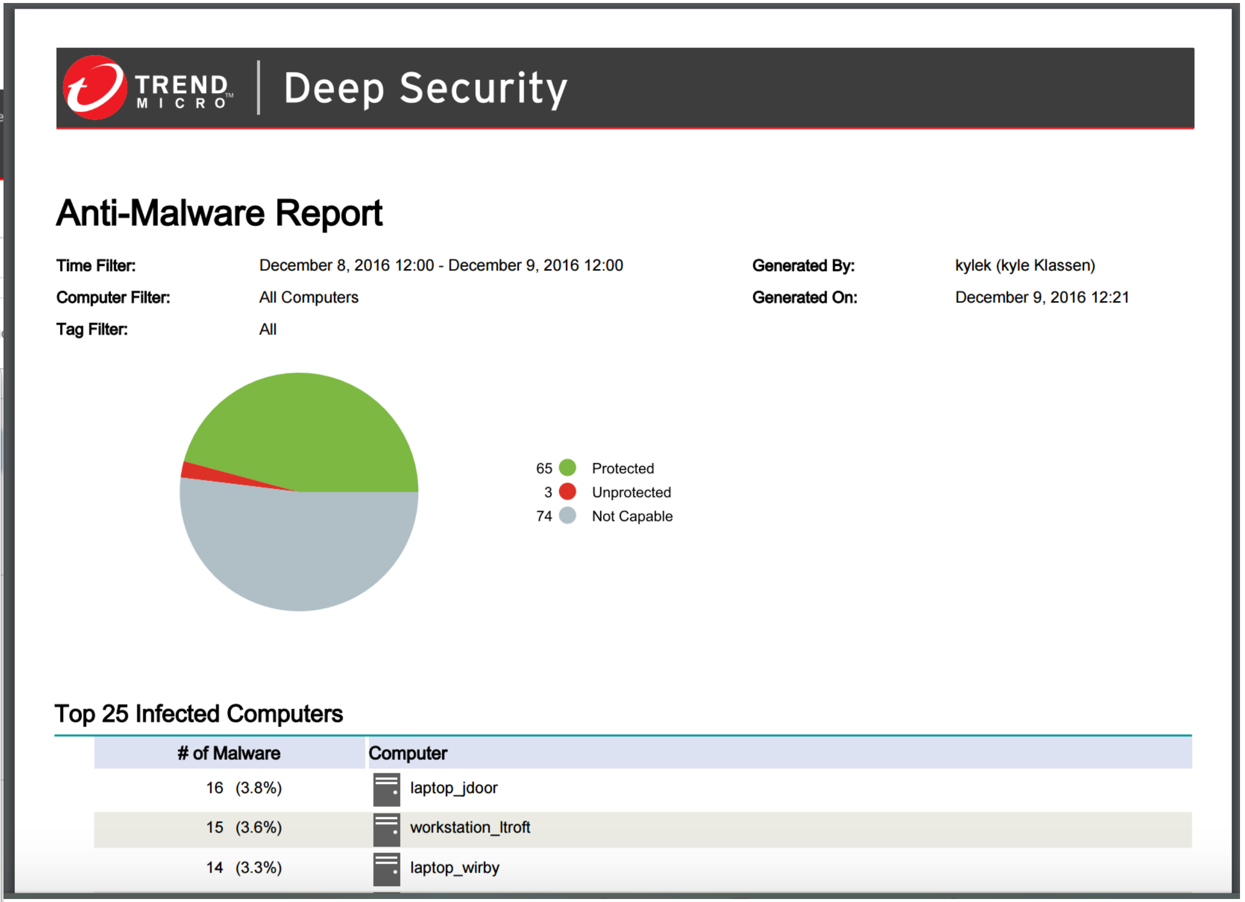
Report

Report: Anti-Malware Report

Format: Portable Document Format (PDF)

Single or Recurring

Predefined Reports



Anti-Malware Report

Time Filter:	December 8, 2016 12:00 - December 9, 2016 12:00	Generated By:	kylek (kyle Klassen)
Computer Filter:	All Computers	Generated On:	December 9, 2016 12:21
Tag Filter:	All		

Top 25 Infected Computers

# of Malware	Computer
16 (3.8%)	laptop_jdoor
15 (3.6%)	workstation_ltroft
14 (3.3%)	laptop_wirby

PDF or RTF report can be PW protected

Extend security to Docker containers

NEW!

Copyright 2017 Trend Micro Inc. 23

VMware continuity to NSX

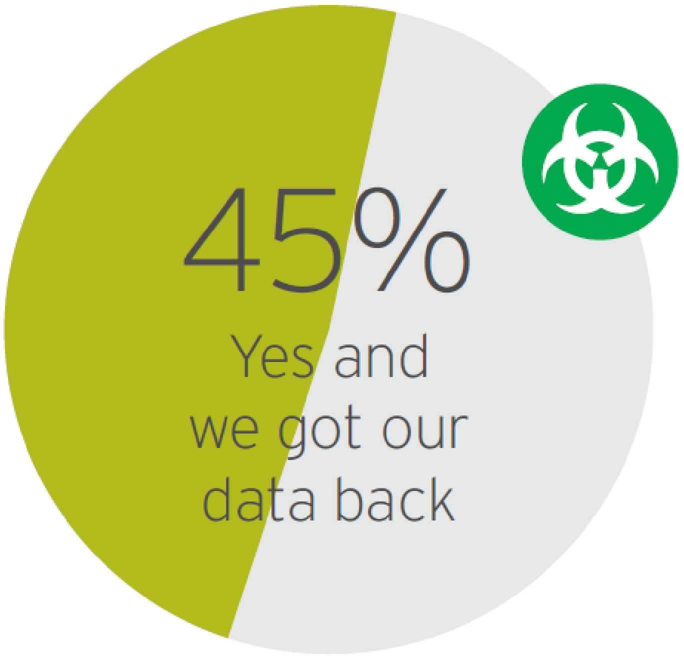
- DS 10 Supports Agentless deployments with NSX 6.2.4 or higher
  - Agentless AM-only requires
    - NSX for vShield Endpoint license, or
    - Standard license
  - Agentless ”All Controls” requires
    - NSX Advanced license, or
    - NSX Enterprise license
- Alternatively Agents can be deployed where “All Controls” are required
  - Agent deployments do not require NSX

Deep Security	vSphere with NSX (Agentless)			vSphere (Agent-based)
	NSX for vShield Endpoint (Free) or NSX Standard	NSX Advanced	NSX Enterprise	
Anti-Malware	✅	✅	✅	✅
Web Reputation	☑	✅	✅	✅
Firewall	☑	✅	✅	✅
IPS / VP	☑	✅	✅	✅
Integrity Monitoring	✅	✅	✅	✅
Log Inspection	☑			✅

1.With the built-in NSX firewall, the Deep Security firewall will normally not be used and should not be focused on for pure NSX deployments
2.Agent-based functionality in combined mode with Agentless

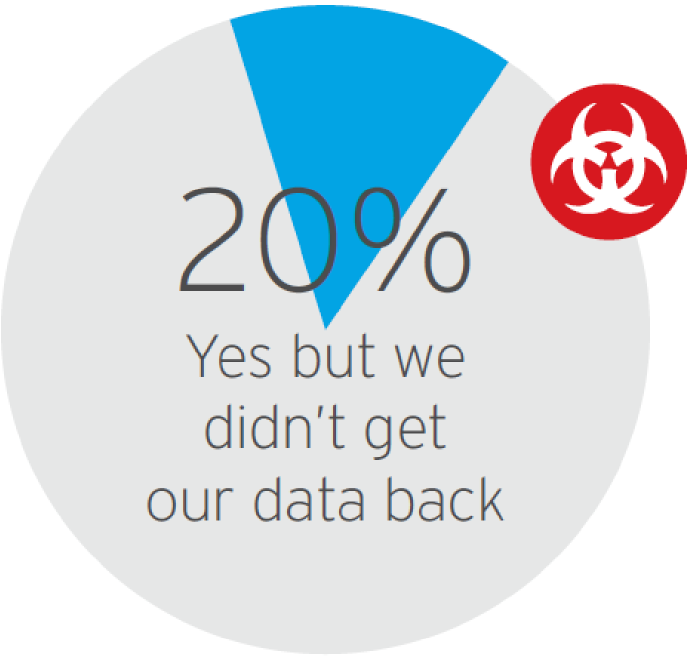
Solving Server zero-day Threats

To Pay or Not to Pay



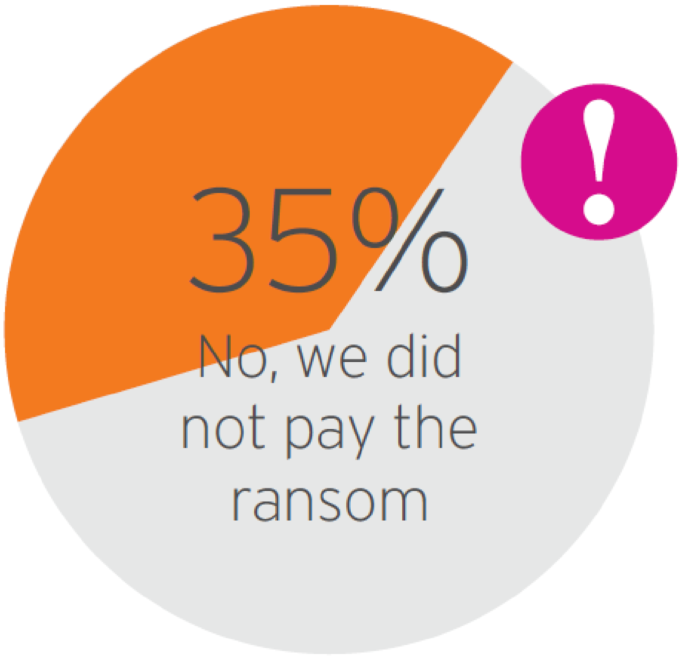
45%

Yes and we got our data back



20%

Yes but we didn't get our data back

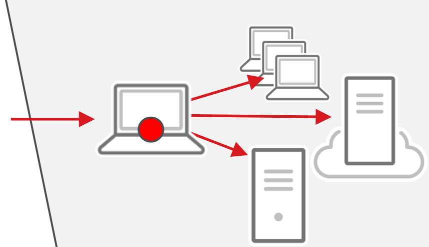


35%

No, we did not pay the ransom

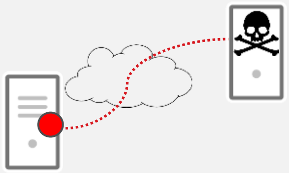
Ransomware Attack Sequence

Find Hosts



- Passive and Active techniques
- Multiple hosts
- Lateral movement
- Polymorphic propagation
- File shares and servers

Connect with Control Server

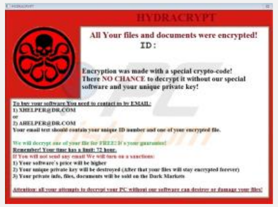


- Phone home
- Confirm success
- Create "Customer" ID
- Generate encryption keys
- Private key stored on control server

Modify (encrypt) files

- Public key used to encrypt local files
- Strong AES encryption
- File name hash
- Targeted file types
- Delete Backups

Present Ransom Note



HYDRACRYPT

All Your files and documents were encrypted!
ID :

Encryption was made with a special crypto-code!
There NO CHANCE to decrypt it without our special software and your unique private key!

To buy your software You need to contact us by EMAIL:
1) XHELPER@DR.COM
or
2) AHELPER@DR.COM
Your email text should contain your unique ID number and one of your encrypted file.

We will decrypt one of your file for FREE! It's your guarantee!
Remember! Your time has a limit: 72 hour.
If You will not send any email We will turn on a sanctions:
1) Your software's price will be higher
2) Your unique private key will be destroyed (After that your files will stay encrypted forever)
3) Your private info, files, documents will be sold on the Dark Markets

Attention: all your attempts to decrypt your PC without our software can destroy or damage your files!

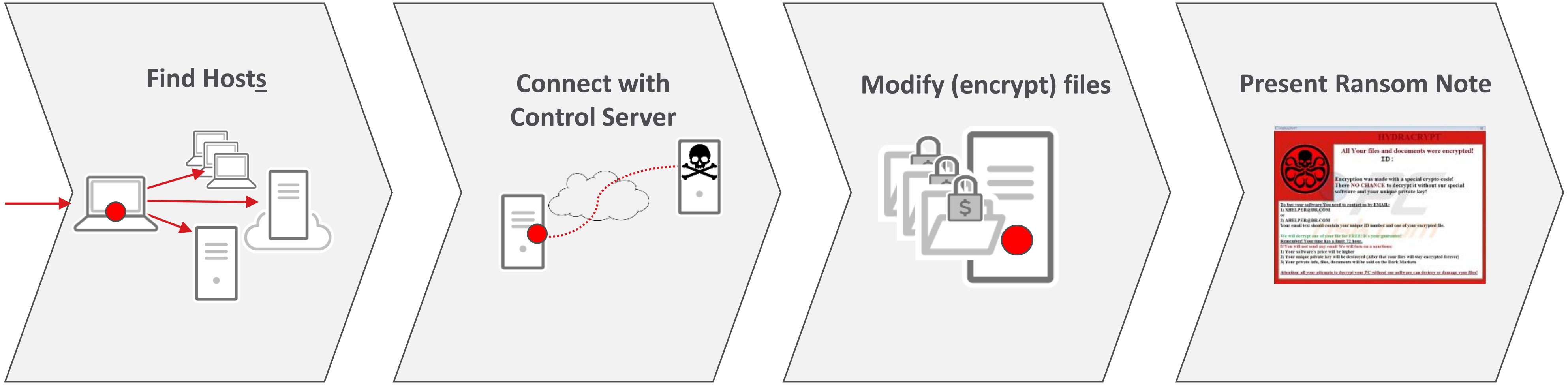
- Pay for decryption key?
- Restore from backup?
- Do nothing?

Deep Security 10: The Industry’s Most Comprehensive Server Protection against Ransomware Threats

✓ SPN Updates ✓ Anti-Malware ✓ Application Control ✓ Sandboxing

✓ Intrusion Prevention ✓ Behavior Monitoring ✓ File Recovery

✓ Firewall ✓ Intrusion Prevention (Heuristics) ✓ Connected Threat Defense



HYDRACRYPT

All Your files and documents were encrypted!
ID :

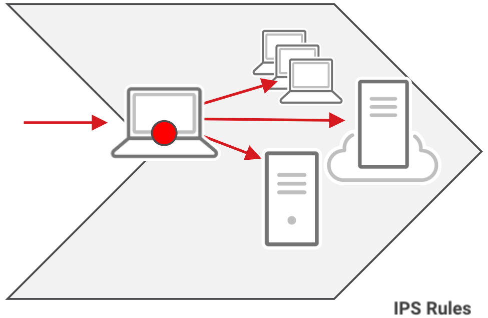
Encryption was made with a special crypto-code!
There NO CHANCE to decrypt it without our special software and your unique private key!

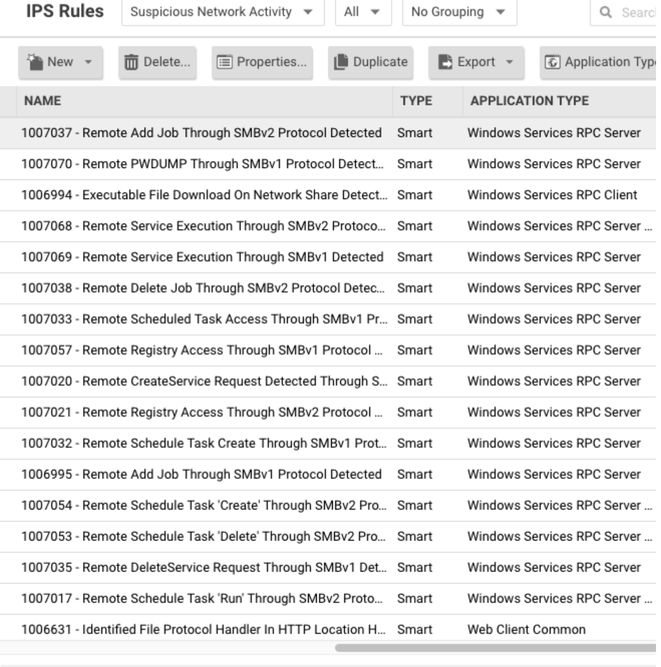
To buy your software You need to contact us by EMAIL:
1) XHELPER@DR.COM
or
2) AHELPER@DR.COM
Your email text should contain your unique ID number and one of your encrypted file.

We will decrypt one of your file for FREE! It's your guarantee!
Remember! Your time has a limit: 72 hour.
If You will not send any email We will turn on a sanctions:
1) Your software's price will be higher
2) Your unique private key will be destroyed (After that your files will stay encrypted forever)
3) Your private info, files, documents will be sold on the Dark Markets

Attention: all your attempts to decrypt your PC without our software can destroy or damage your files!

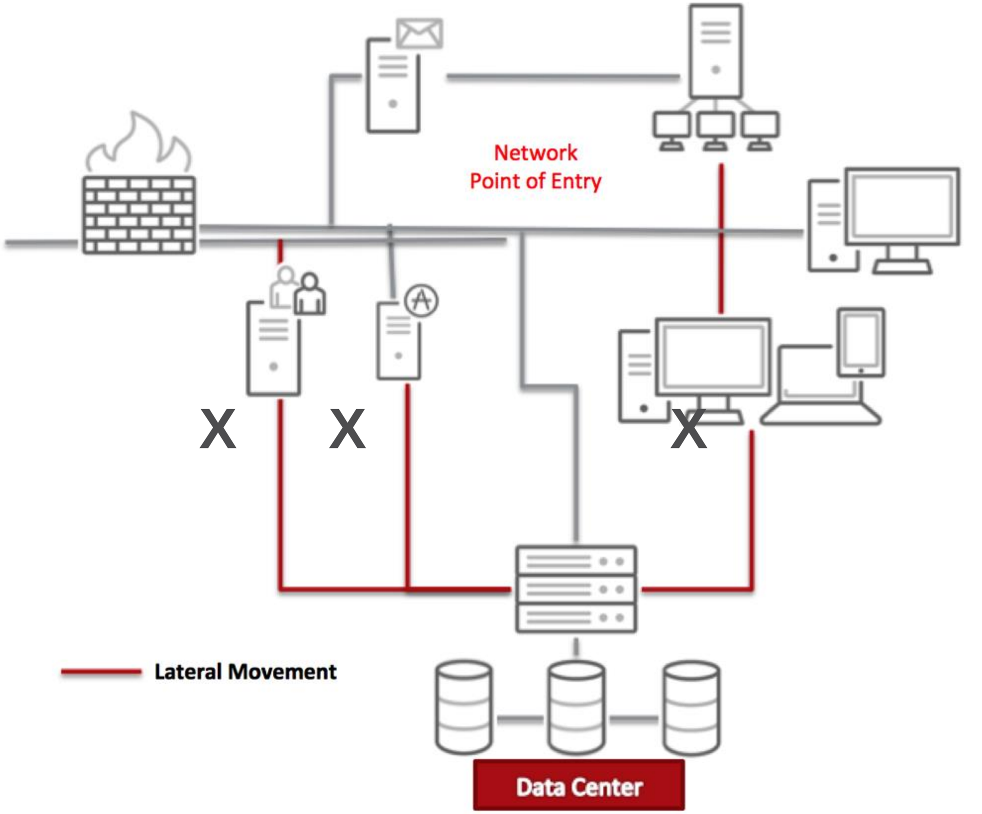
Stop Ransomware from moving to Protected Servers from an Infected Machine





IPS Rules

NAME	TYPE	APPLICATION TYPE
1007037 - Remote Add Job Through SMBv2 Protocol Detected	Smart	Windows Services RPC Server
1007070 - Remote PWDUMP Through SMBv1 Protocol Detect...	Smart	Windows Services RPC Server
1006994 - Executable File Download On Network Share Detect...	Smart	Windows Services RPC Client
1007068 - Remote Service Execution Through SMBv2 Protoco...	Smart	Windows Services RPC Server ...
1007069 - Remote Service Execution Through SMBv1 Detected	Smart	Windows Services RPC Server
1007038 - Remote Delete Job Through SMBv2 Protocol Detec...	Smart	Windows Services RPC Server
1007033 - Remote Scheduled Task Access Through SMBv1 Pr...	Smart	Windows Services RPC Server
1007057 - Remote Registry Access Through SMBv1 Protocol ...	Smart	Windows Services RPC Server
1007020 - Remote CreateService Request Detected Through S...	Smart	Windows Services RPC Server
1007021 - Remote Registry Access Through SMBv2 Protocol ...	Smart	Windows Services RPC Server
1007032 - Remote Schedule Task Create Through SMBv1 Prot...	Smart	Windows Services RPC Server
1006995 - Remote Add Job Through SMBv1 Protocol Detected	Smart	Windows Services RPC Server
1007054 - Remote Schedule Task 'Create' Through SMBv2 Pro...	Smart	Windows Services RPC Server ...
1007053 - Remote Schedule Task 'Delete' Through SMBv2 Pro...	Smart	Windows Services RPC Server ...
1007035 - Remote DeleteService Request Through SMBv1 Det...	Smart	Windows Services RPC Server
1007017 - Remote Schedule Task 'Run' Through SMBv2 Proto...	Smart	Windows Services RPC Server ...
1006631 - Identified File Protocol Handler In HTTP Location H...	Smart	Web Client Common



Intrusion Prevention

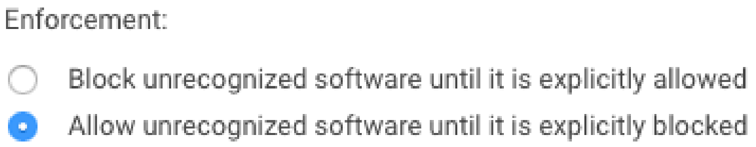
- Minimize server attack surface using IPS Vulnerability Shielding
- Smart rules monitor and prevent Lateral movement of threats including Ransomware
- Heuristic analysis catches unknown variants exhibiting characteristic Ransomware behavior

Block unknown software from running on Protected Servers

NEW!

Application Control

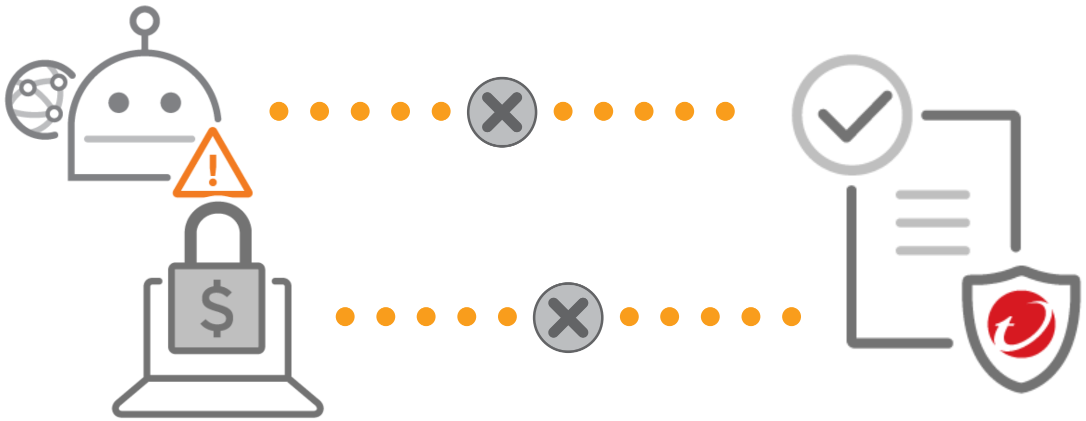
- When enabled, Application Control will scan servers and create a whitelist of approved software
- Administrator defined rules can block all unknown software (not included in the whitelist) until explicitly allowed
  - Effectively “locks down” servers to significantly reduce its attack surface
- Real-time protection against unknown software
- Included with the System Security License (along with Integrity Monitoring and Log Inspection)



Enforcement:

○ Block unrecognized software until it is explicitly allowed

● Allow unrecognized software until it is explicitly blocked



Many ways for malware to install on your servers
- Intrusions
- Lateral Movement
- Human Error
- Authorized users installing custom/personalized tools

Administrator Control

Lockdown Servers across the Hybrid Cloud even when workloads are elastic

Detailed view shows who changed the file

Share rulesets with other computers

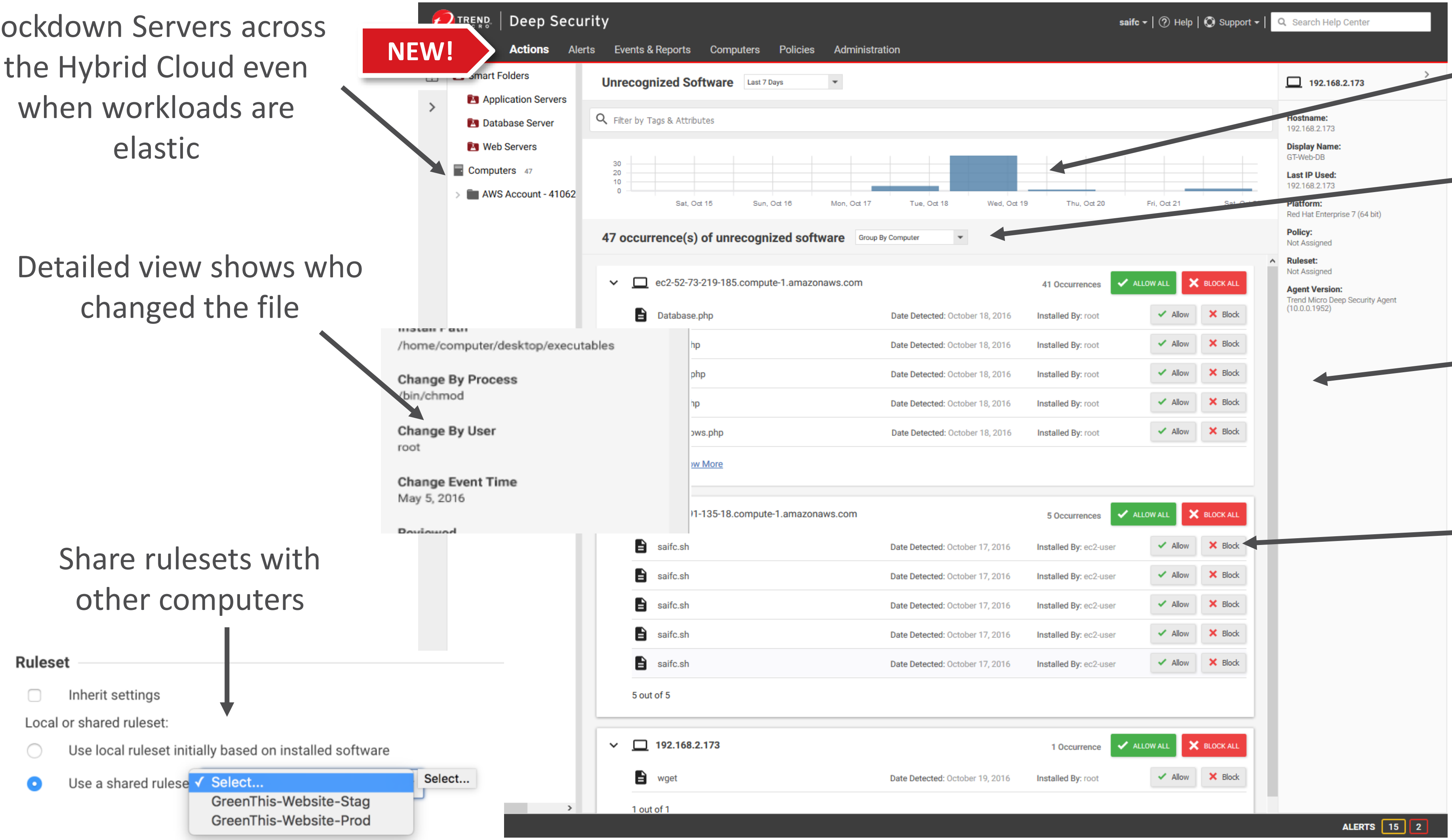
See how many unknown software events occurred hourly, daily, monthly or in total

Customize view by File or Computer

List view of all unknown software events

Choose ”Allow” to add software to whitelist

Choose ”Block” to exclude from whitelist



Unrecognized Software Last 7 Days

Filter by Tags & Attributes

47 occurrence(s) of unrecognized software Group By Computer

ec2-52-73-219-185.compute-1.amazonaws.com — 41 Occurrences — ✓ ALLOW ALL ✕ BLOCK ALL

Database.php	Date Detected: October 18, 2016	Installed By: root	✓ Allow ✕ Block
hp	Date Detected: October 18, 2016	Installed By: root	✓ Allow ✕ Block
php	Date Detected: October 18, 2016	Installed By: root	✓ Allow ✕ Block
hp	Date Detected: October 18, 2016	Installed By: root	✓ Allow ✕ Block
ws.php	Date Detected: October 18, 2016	Installed By: root	✓ Allow ✕ Block

w More

1-135-18.compute-1.amazonaws.com — 5 Occurrences — ✓ ALLOW ALL ✕ BLOCK ALL

saifc.sh	Date Detected: October 17, 2016	Installed By: ec2-user	✓ Allow ✕ Block
saifc.sh	Date Detected: October 17, 2016	Installed By: ec2-user	✓ Allow ✕ Block
saifc.sh	Date Detected: October 17, 2016	Installed By: ec2-user	✓ Allow ✕ Block
saifc.sh	Date Detected: October 17, 2016	Installed By: ec2-user	✓ Allow ✕ Block
saifc.sh	Date Detected: October 17, 2016	Installed By: ec2-user	✓ Allow ✕ Block

5 out of 5

192.168.2.173 — 1 Occurrence — ✓ ALLOW ALL ✕ BLOCK ALL

wget	Date Detected: October 19, 2016	Installed By: root	✓ Allow ✕ Block

1 out of 1

192.168.2.173

Hostname: 192.168.2.173

Display Name: GT-Web-DB

Last IP Used: 192.168.2.173

Platform: Red Hat Enterprise 7 (64 bit)

Policy: Not Assigned

Ruleset: Not Assigned

Agent Version: Trend Micro Deep Security Agent (10.0.0.1952)

Install Path
/home/computer/desktop/executables

Change By Process
/bin/chmod

Change By User
root

Change Event Time
May 5, 2016

Reviewed

Ruleset

□ Inherit settings

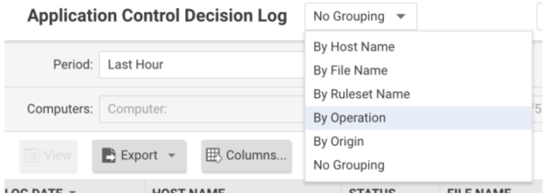
Local or shared ruleset:

○ Use local ruleset initially based on installed software

● Use a shared ruleset ✓ Select... | Select...

GreenThis-Website-Stag

GreenThis-Website-Prod



Application Control Decision Log No Grouping

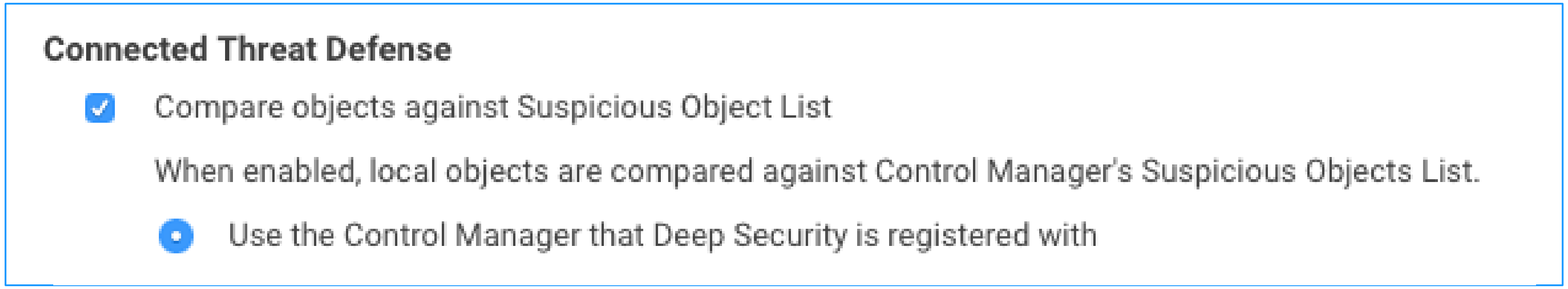
Period: Last Hour

Computers: Computer:

By Host Name
By File Name
By Ruleset Name
By Operation
By Origin
No Grouping

Turning Unknown threats into Known Threats!

NEW!



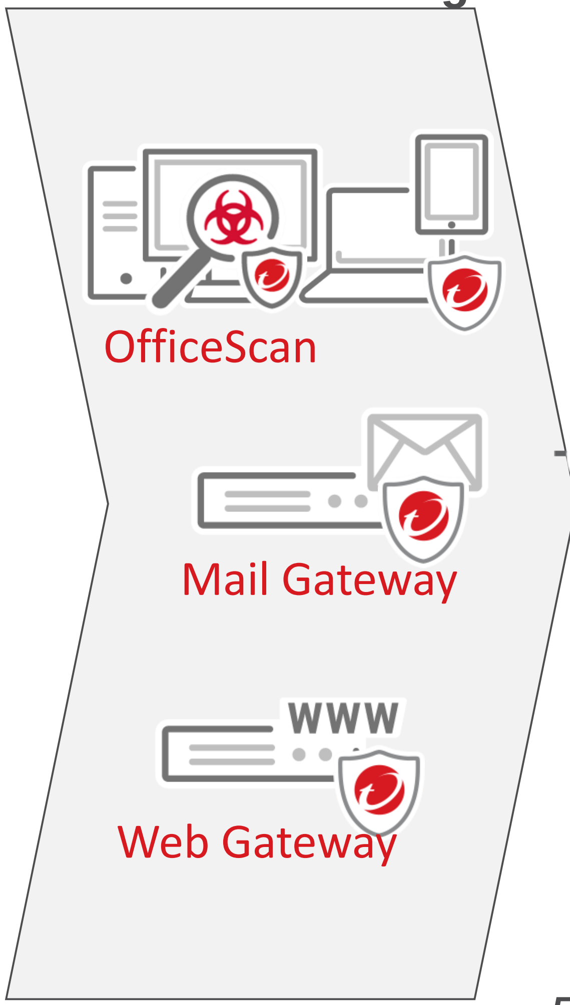
Connected Threat Defense

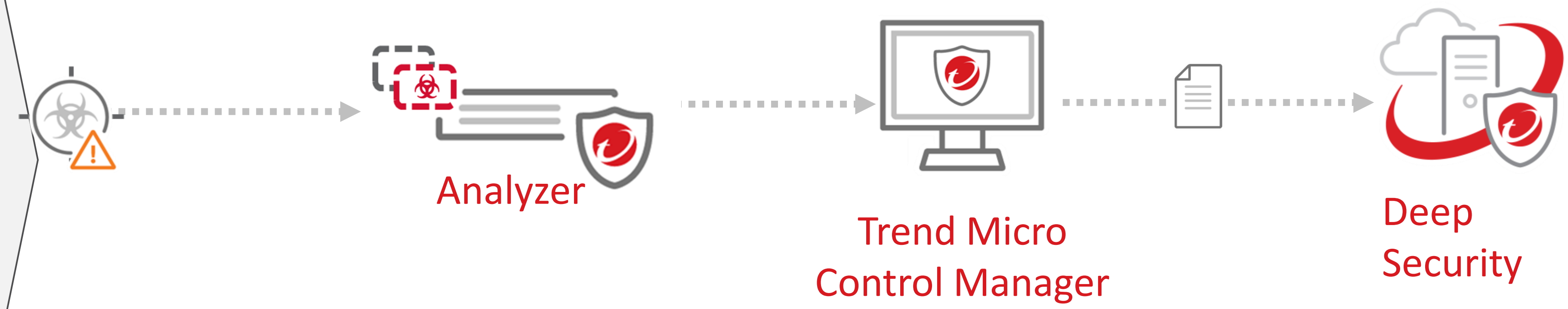
☑ Compare objects against Suspicious Object List

When enabled, local objects are compared against Control Manager's Suspicious Objects List.

● Use the Control Manager that Deep Security is registered with

Real-Time Scanning





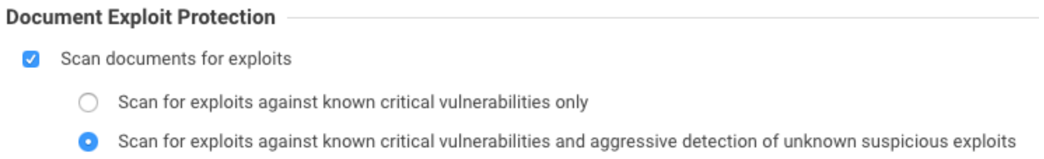
- Suspicious Object detected and sent to Deep Discovery Analyzer for confirmation

- TMCM notified of new malware and sends signature and policy to Deep Security

Full System Protection with Trend Micro Connected Threat Defense

Detect, analyze and contain suspicious document files

NEW!



Document Exploit Protection

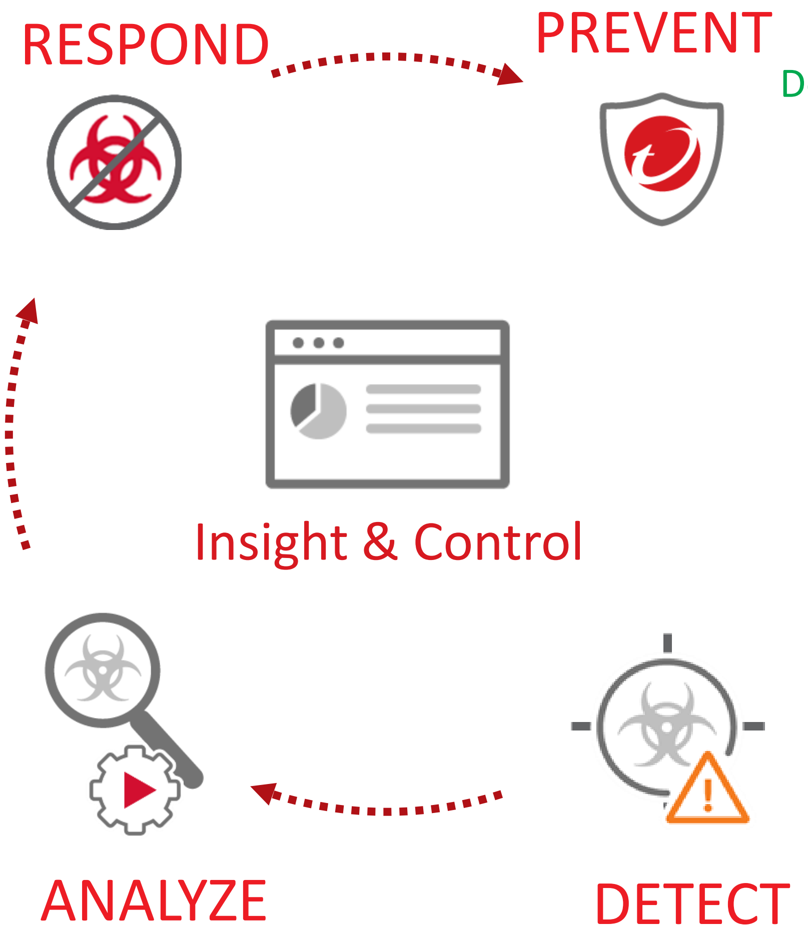
☑ Scan documents for exploits

○ Scan for exploits against known critical vulnerabilities only

● Scan for exploits against known critical vulnerabilities and aggressive detection of unknown suspicious exploits

Trend Micro Control Manager

Sandbox analysis results are sent to Trend Micro Control Manager where remediation actions are set



RESPOND

PREVENT

Insight & Control

ANALYZE

DETECT

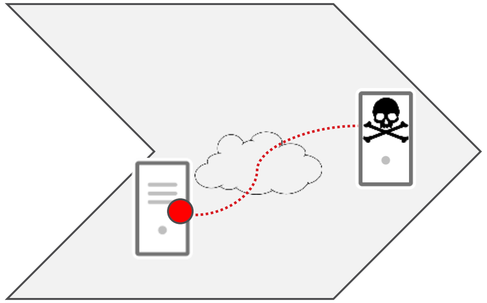
Deep Security receives updated signature and policy (eg. Quarantine)

Deep Security

Suspicious files are detected by Deep Security and submitted to Deep Discovery Analyzer

Deep Discovery Analyzer

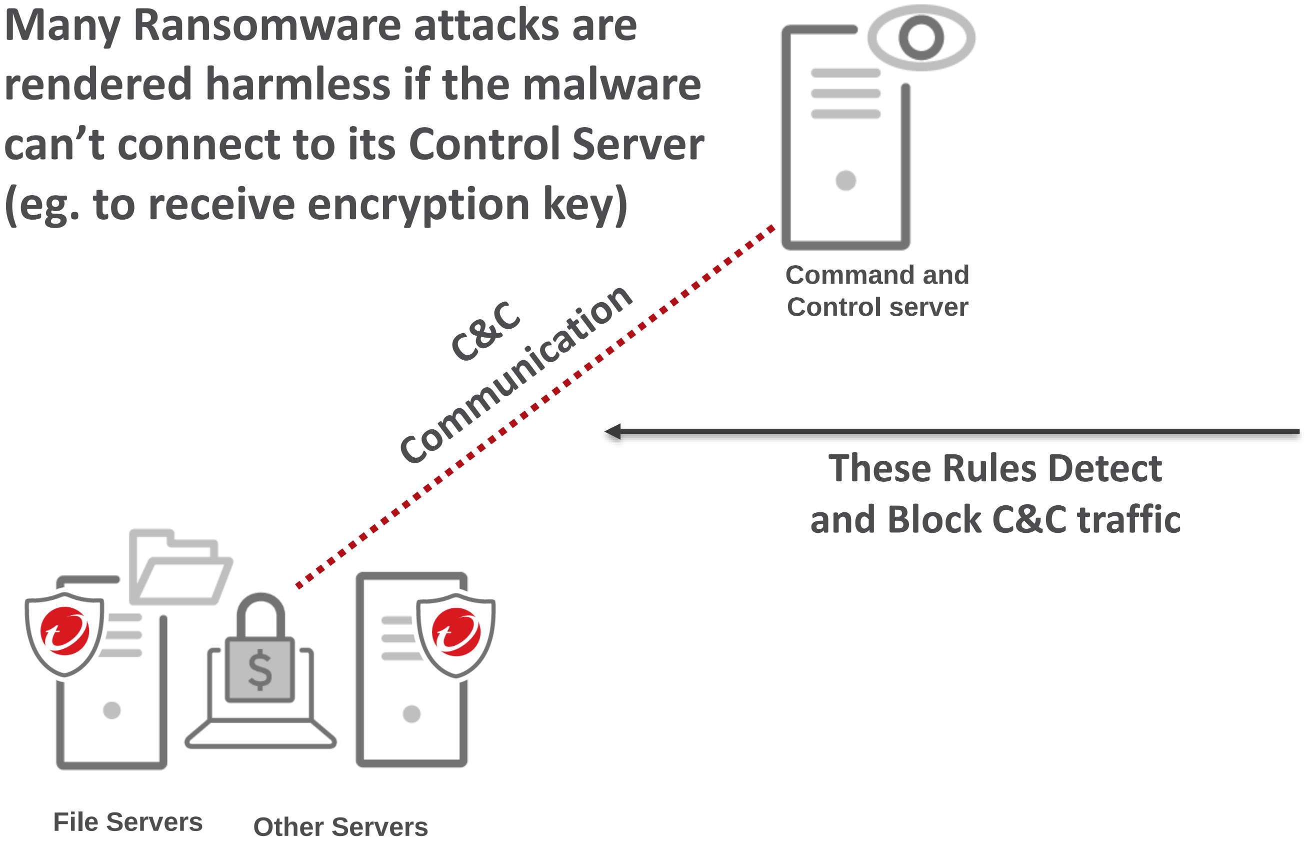
Suspicious objects are analyzed in a closed sandbox environment – to confirm Ransomware attack



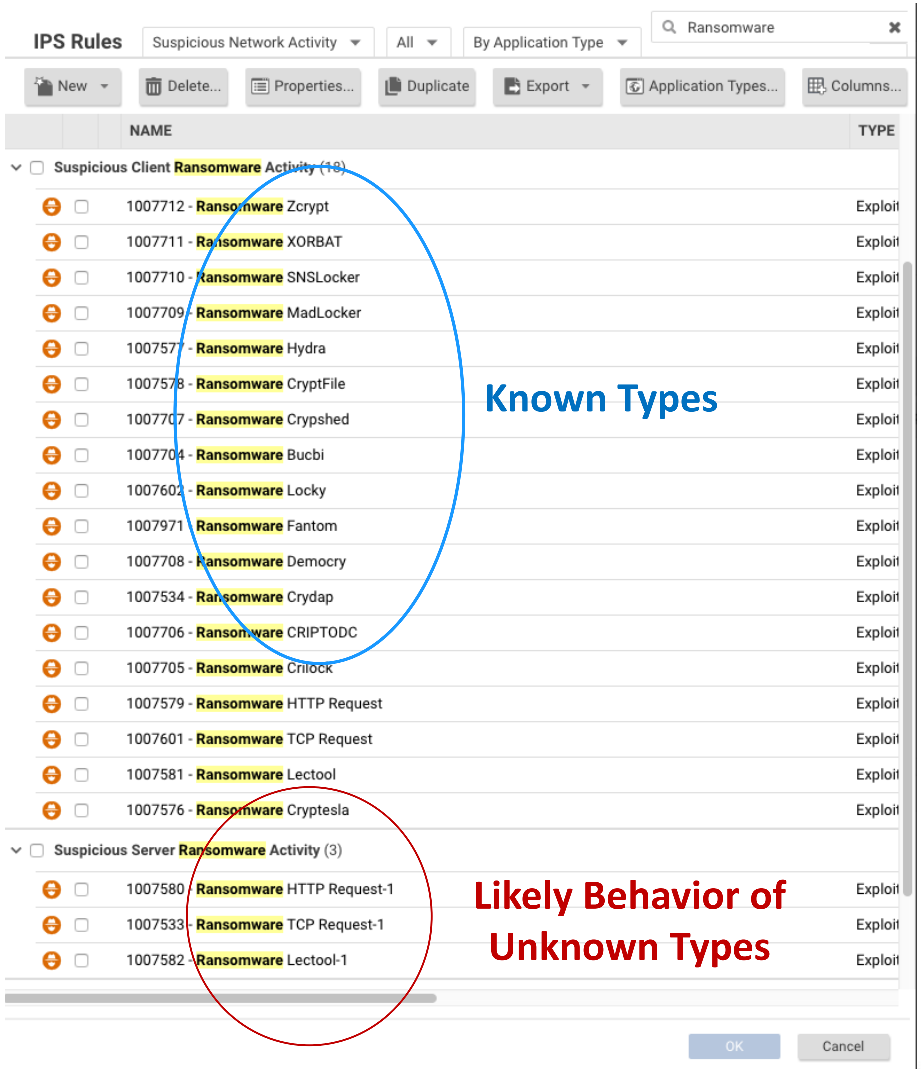
Stop Ransomware Attack by blocking Command and Control Traffic

Intrusion Prevention
Smart Rules

- **Many Ransomware attacks are rendered harmless if the malware can’t connect to its Control Server (eg. to receive encryption key)**



These Rules Detect and Block C&C traffic



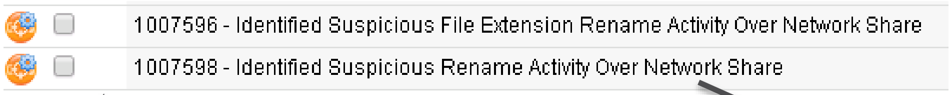
NAME	TYPE
Suspicious Client Ransomware Activity (18)	
1007712 - Ransomware Zcrypt	Exploit
1007711 - Ransomware XORBAT	Exploit
1007710 - Ransomware SNSLocker	Exploit
1007709 - Ransomware MadLocker	Exploit
1007577 - Ransomware Hydra	Exploit
1007578 - Ransomware CryptFile	Exploit
1007707 - Ransomware Crypshed	Exploit
1007704 - Ransomware Bucbi	Exploit
1007602 - Ransomware Locky	Exploit
1007971 - Ransomware Fantom	Exploit
1007708 - Ransomware Democry	Exploit
1007534 - Ransomware Crydap	Exploit
1007706 - Ransomware CRIPTODC	Exploit
1007705 - Ransomware Crilock	Exploit
1007579 - Ransomware HTTP Request	Exploit
1007601 - Ransomware TCP Request	Exploit
1007581 - Ransomware Lectool	Exploit
1007576 - Ransomware Cryptesla	Exploit
Suspicious Server Ransomware Activity (3)	
1007580 - Ransomware HTTP Request-1	Exploit
1007533 - Ransomware TCP Request-1	Exploit
1007582 - Ransomware Lectool-1	Exploit

Known Types

Likely Behavior of Unknown Types

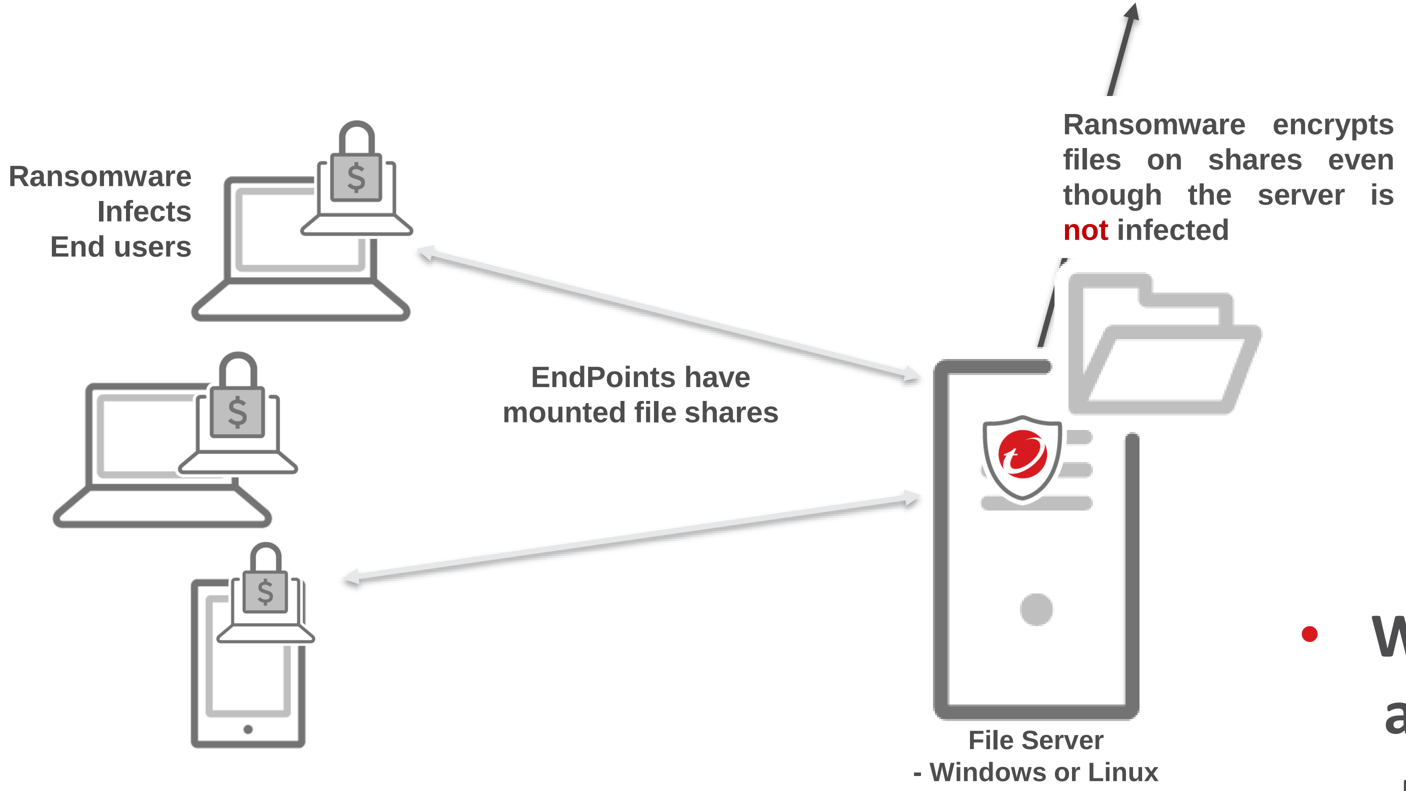
Detecting and Terminating Ransomware attacks with IPS Smart Rules

Intrusion Prevention
Smart Rules



☐ 1007596 - Identified Suspicious File Extension Rename Activity Over Network Share

☐ 1007598 - Identified Suspicious Rename Activity Over Network Share



Ransomware Infects End users
EndPoints have mounted file shares
Ransomware encrypts files on shares even though the server is not infected
File Server
- Windows or Linux

Rule 1007596 - Identified Suspicious File Extension Rename Activity Over Network Share:

- Detects renames to 50 ransomware related extensions.
- Provides early detection

Known Types

Rule 1007598 - Identified Suspicious Rename Activity

Likely Behavior of Unknown Types

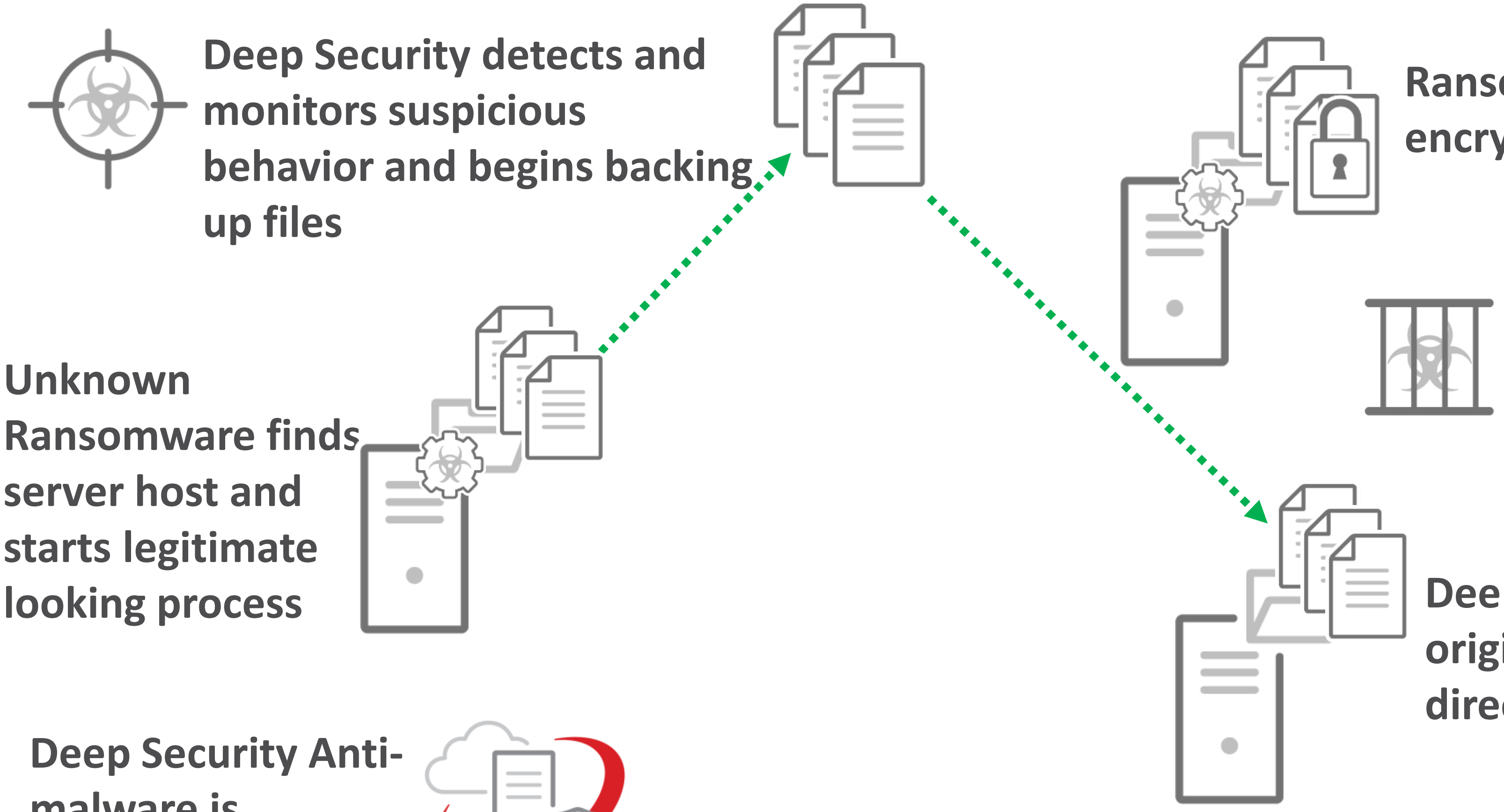
- **When Unknown Ransomware attempts to modify files, this rule will detect and prevent the attack**

Intelligent Detection and Protection against Ransomware attacks

NEW!

Anti-malware

Behavior Monitoring



Unknown Ransomware finds server host and starts legitimate looking process

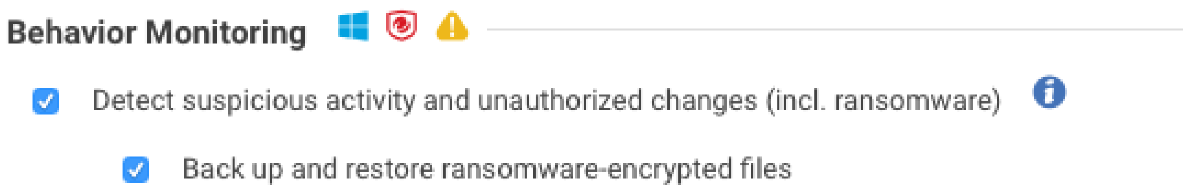
Deep Security detects and monitors suspicious behavior and begins backing up files

Ransomware begins encrypting files

Deep Security determines behavior to be a Ransomware Attack > Stops process and quarantines file

Deep Security restores original unencrypted files to directory and logs event

Deep Security Anti-malware is protecting server



Behavior Monitoring

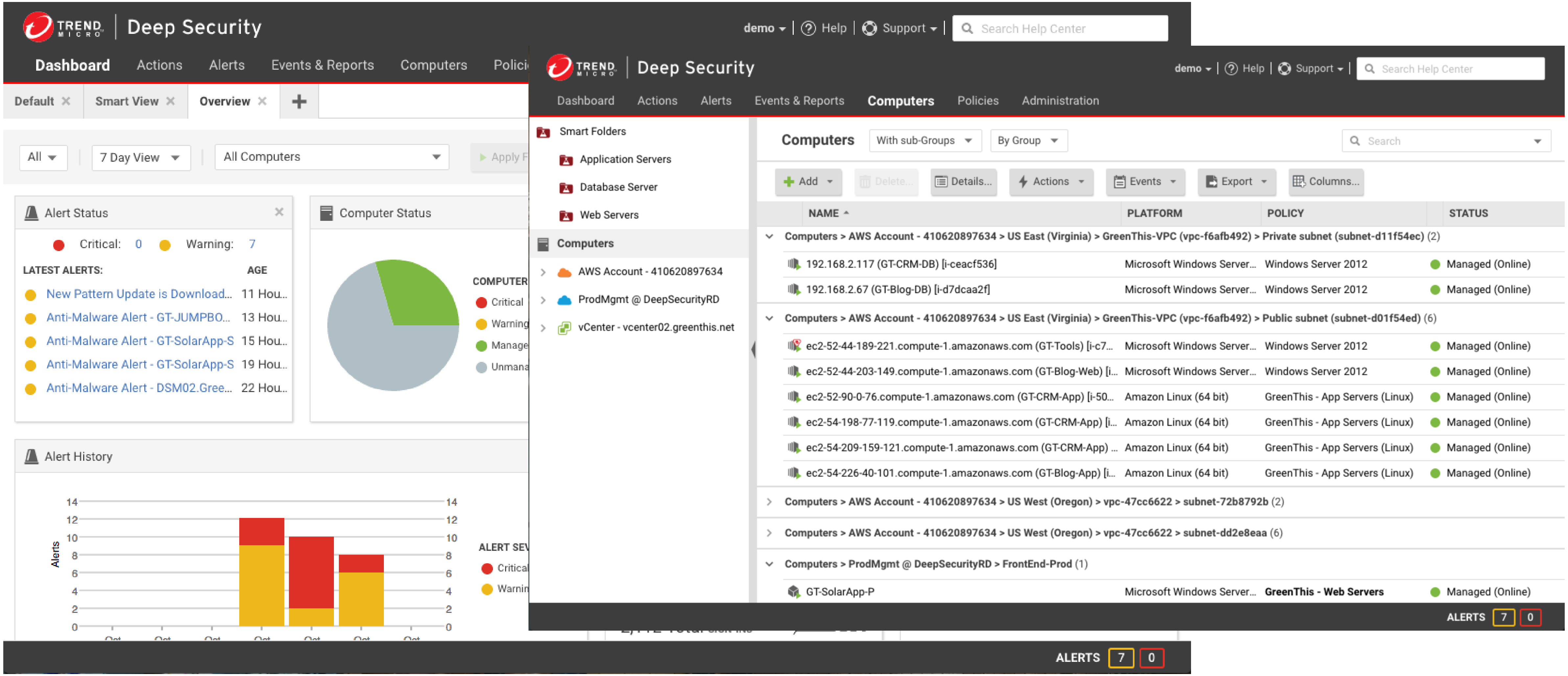
☑ Detect suspicious activity and unauthorized changes (incl. ransomware)

☑ Back up and restore ransomware-encrypted files

Ransomware Protection by Platform

Ransomware Protection	New in DS10?	Windows		Linux	
		Agent	Agentless	Agent	Agentless
IPS Smart Rules	9.x	Yes	Yes	Yes	Yes
Application Control	New 10.0	Planned	No	Yes	No
Connected Threat Defense	New 10.0	Yes	Yes	Yes	Yes
Anti-Malware Behavior Monitoring	New 10.0	Yes	No	No	No
Document Back-up and Restore	New 10.0	Yes	No	No	No

Eliminate security silos with central visibility



Deep Security

demo | Help | Support | Search Help Center

Dashboard | Actions | Alerts | Events & Reports | Computers | Polici

Default ✕ | Smart View ✕ | Overview ✕ | +

All | 7 Day View | All Computers | Apply F

Alert Status

● Critical: 0 ● Warning: 7

LATEST ALERTS:	AGE
● New Pattern Update is Download...	11 Hou...
● Anti-Malware Alert - GT-JUMPBO...	13 Hou...
● Anti-Malware Alert - GT-SolarApp-S	15 Hou...
● Anti-Malware Alert - GT-SolarApp-S	19 Hou...
● Anti-Malware Alert - DSM02.Gree...	22 Hou...

Computer Status

Alert History

ALERTS 7 0

Deep Security

demo | Help | Support | Search Help Center

Dashboard | Actions | Alerts | Events & Reports | Computers | Policies | Administration

Smart Folders
- Application Servers
- Database Server
- Web Servers

Computers
- AWS Account - 410620897634
- ProdMgmt @ DeepSecurityRD
- vCenter - vcenter02.greenthis.net

Computers | With sub-Groups | By Group | Search

Add | Delete... | Details... | Actions | Events | Export | Columns...

NAME ▲	PLATFORM	POLICY	STATUS
Computers > AWS Account - 410620897634 > US East (Virginia) > GreenThis-VPC (vpc-f6afb492) > Private subnet (subnet-d11f54ec) (2)			
192.168.2.117 (GT-CRM-DB) [i-ceacf536]	Microsoft Windows Server...	Windows Server 2012	● Managed (Online)
192.168.2.67 (GT-Blog-DB) [i-d7dcaa2f]	Microsoft Windows Server...	Windows Server 2012	● Managed (Online)
Computers > AWS Account - 410620897634 > US East (Virginia) > GreenThis-VPC (vpc-f6afb492) > Public subnet (subnet-d01f54ed) (6)			
ec2-52-44-189-221.compute-1.amazonaws.com (GT-Tools) [i-c7...	Microsoft Windows Server...	Windows Server 2012	● Managed (Online)
ec2-52-44-203-149.compute-1.amazonaws.com (GT-Blog-Web) [i...	Microsoft Windows Server...	Windows Server 2012	● Managed (Online)
ec2-52-90-0-76.compute-1.amazonaws.com (GT-CRM-App) [i-50...	Amazon Linux (64 bit)	GreenThis - App Servers (Linux)	● Managed (Online)
ec2-54-198-77-119.compute-1.amazonaws.com (GT-CRM-App) [i...	Amazon Linux (64 bit)	GreenThis - App Servers (Linux)	● Managed (Online)
ec2-54-209-159-121.compute-1.amazonaws.com (GT-CRM-App) ...	Amazon Linux (64 bit)	GreenThis - App Servers (Linux)	● Managed (Online)
ec2-54-226-40-101.compute-1.amazonaws.com (GT-Blog-App) [i...	Amazon Linux (64 bit)	GreenThis - App Servers (Linux)	● Managed (Online)
Computers > AWS Account - 410620897634 > US West (Oregon) > vpc-47cc6622 > subnet-72b8792b (2)			
Computers > AWS Account - 410620897634 > US West (Oregon) > vpc-47cc6622 > subnet-dd2e8eaa (6)			
Computers > ProdMgmt @ DeepSecurityRD > FrontEnd-Prod (1)			
GT-SolarApp-P	Microsoft Windows Server...	GreenThis - Web Servers	● Managed (Online)

ALERTS 7 0

Wrap up

Deep Security Protection Packages

Enterprise

Anti-malware (all)

Intrusion Prevention (IPS)

Firewall

NEW! Application Control

Integrity Monitoring

Log Inspection

Network

Intrusion Prevention (IPS)

Firewall

System

NEW! Application Control

Integrity Monitoring

Log Inspection

Anti-malware

Anti-malware

Web Reputation

NEW! Behavioral analysis

NEW! Sandbox integration

Deep Security for SAP

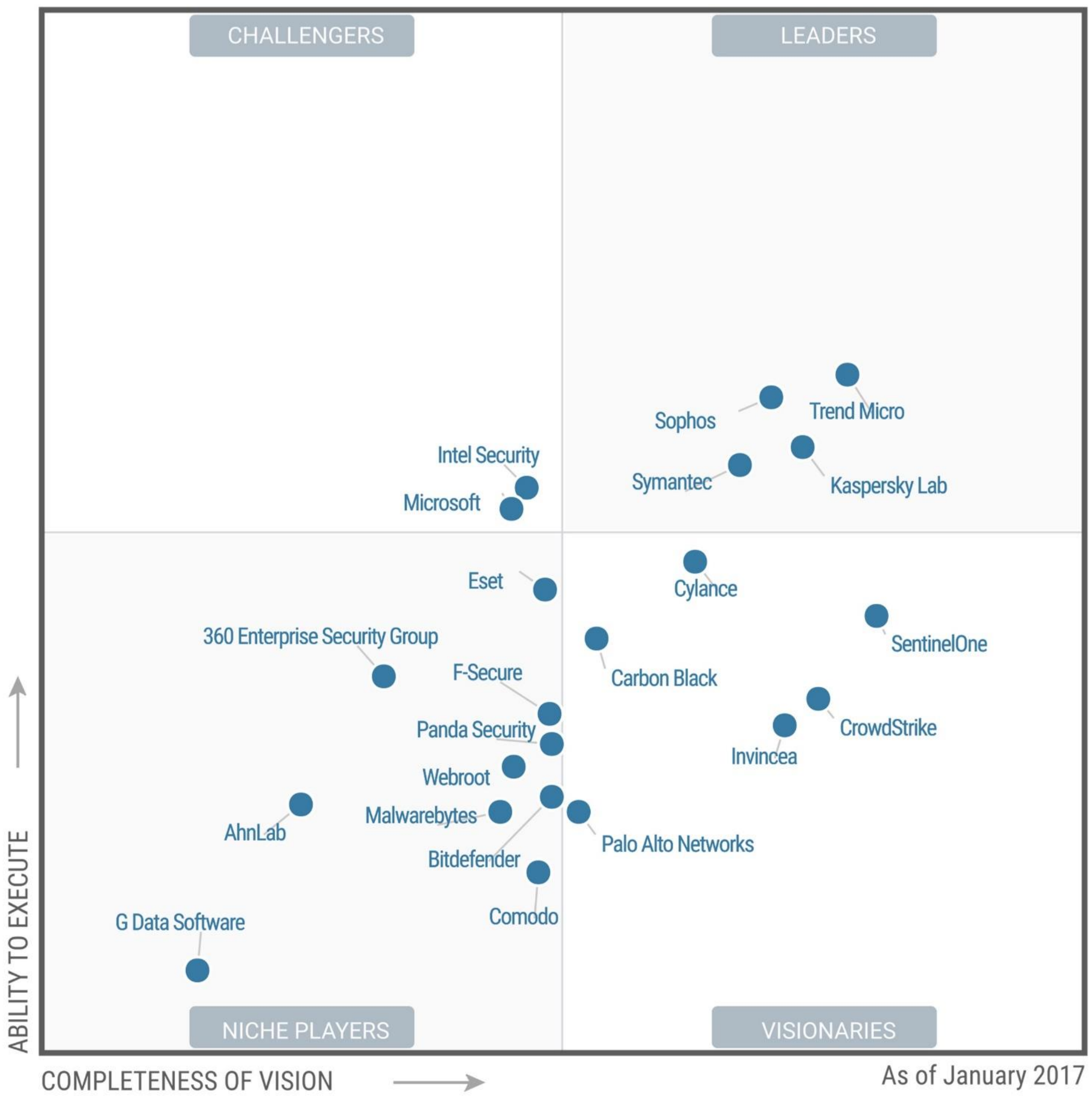
Gartner Magic Quadrant for Endpoint Protection Platforms

January 2017

"The breadth of coverage supplied by Deep Security across endpoints and the data center, with optimized support for VMware, Microsoft Azure and AWS, is appealing to organizations looking to consolidate vendors."

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from https://resources.trendmicro.com/Gartner-Magic-Quadrant-Endpoints.html

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organizati and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.



Source: Gartner (January 2017)

Deep Security 10

Thank You