FAST. SECURE. GLOBAL.

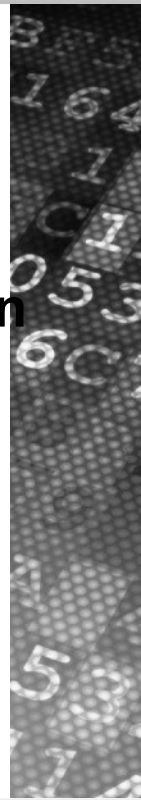
Bring your own Everything (ByoX) Threats, Visibility and Control

Mr.Pathom Suksathit
Regional SE Manager : Indo-China
CISSP, CISA, FCNSP

© Copyright Fortinet Inc. All rights reserved.

Today Agenda

- **Bring your own Everything (ByoX)**
- **Security Threats and Challenges & 2016 Threats Prediction**
- **Network Infrastructure Evolution & Internal Segmentation**
- **Internal Segmentation Security**



Survey Findings

The survey yielded responses from 214 IT practitioners, managers and directors in the UK from small, mid-size and enterprise companies.

- **BYOx is the emerging technology that is most disruptive to business**

  - **Mobility,**
  - **Cloud computing,**
  - **Data analytics and**
  - **Compliance,** round up the top five emerging technologies

Lawrence Garvin is a Head Geek and Technical Product Marketing Manager at SolarWinds.

The survey yielded responses from 214 IT practitioners, managers and directors in the UK from small, mid-size and enterprise companies.

Survey Findings

- **Over half (53%) of all IT departments now manage virtualization, mobility, compliance, data analytics, SDN/virtual networks, BYOx, cloud computing and self-service automation**

- **40% of respondents said increasing complexity has greatly affected their responsibilities** over the past 3-5 years, and an additional

- **49% said it has somewhat affected their role**

Lawrence Garvin is a Head Geek and Technical Product Marketing Manager at SolarWinds.

The survey yielded responses from 214 IT practitioners, managers and directors in the UK from small, mid-size and enterprise companies.

Bring Your Own 'x' (BYOx)

- Employee/students bring their own digital devices to Org/School, for the purposes of learning/working.
- So instead of using Org/school-owned ICT
- Employee/students use their own.

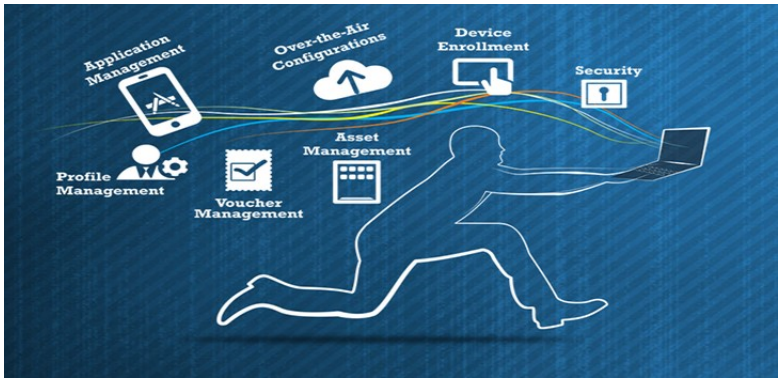
The BYOx movement includes

- bring your own device (BYOD)
- bring your own apps (BYOA)
- bring your own encryption (BYOE)
- bring your own identity (BYOI)

- bring your own technology (BYOT)
- bring your own network (BYON)
- bring your own wearables (BYOW)

The tidal surge of bring your own devices

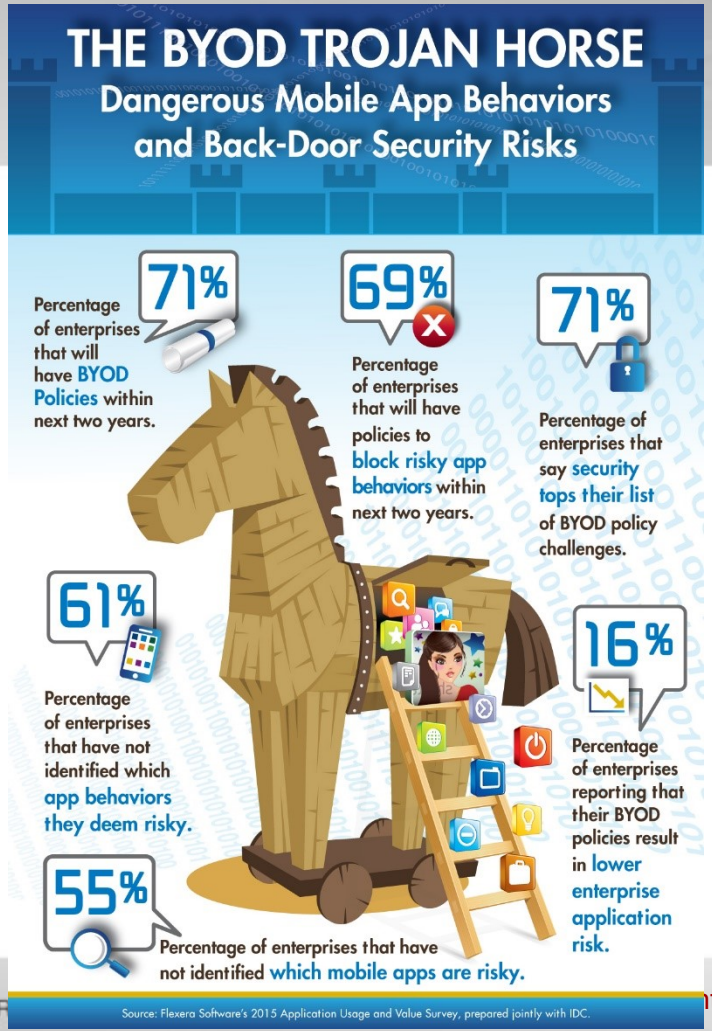
- **The benefits are significant**
- **Connected employees are happy employees.**
- Workers empowered by mobile devices and apps are more productive, collaborative, and innovative.



References : The State of Queensland (Department of Education and Training) 2015

Risk still out there..

- But risks have mounted rapidly as well.
- It is nearly **impossible to track and protect critical data**, provision appropriate infrastructure, and build effective defences against hackers.
- From a management point of view, **the percentage of organizations enabling BYOD is growing, A lot of BYOD activity is still going unmanaged**


THE BYOD TROJAN HORSE
Dangerous Mobile App Behaviors and Back-Door Security Risks
71%
Percentage of enterprises that will have BYOD Policies within next two years.
69%
Percentage of enterprises that will have policies to block risky app behaviors within next two years.
71%
Percentage of enterprises that say security tops their list of BYOD policy challenges.
61%
Percentage of enterprises that have not identified which app behaviors they deem risky.
16%
Percentage of enterprises reporting that their BYOD policies result in lower enterprise application risk.
55%
Percentage of enterprises that have not identified which mobile apps are risky.
Source: Flexera Software's 2015 Application Usage and Value Survey, prepared jointly with IDC.

Key Breach Report Trends - 2015

95%

FOUR OUT OF FIVE DIDN'T LAST BEYOND A WEEK.

50%

THE FIRST HOUR.

70–90%

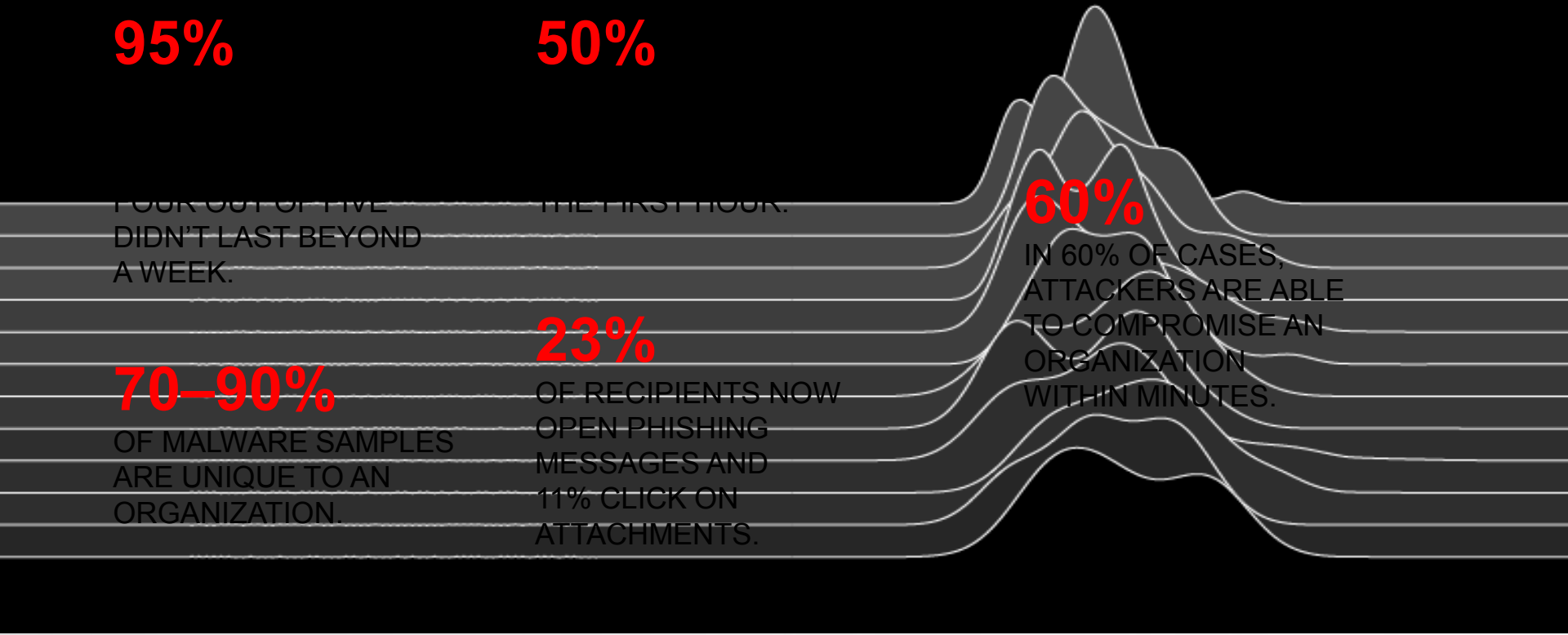
OF MALWARE SAMPLES ARE UNIQUE TO AN ORGANIZATION.

23%

OF RECIPIENTS NOW OPEN PHISHING MESSAGES AND 11% CLICK ON ATTACHMENTS.

60%

IN 60% OF CASES, ATTACKERS ARE ABLE TO COMPROMISE AN ORGANIZATION WITHIN MINUTES.

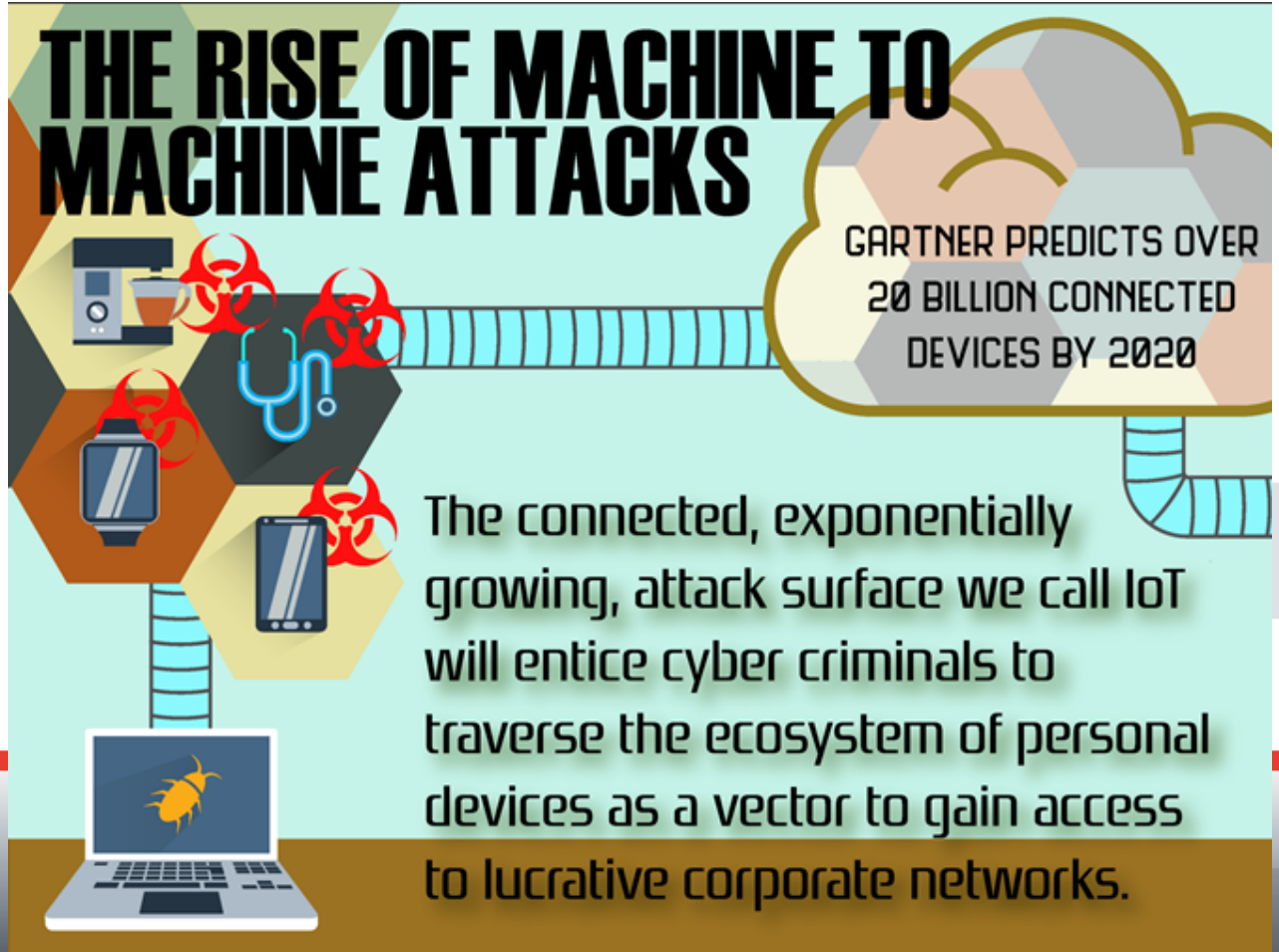


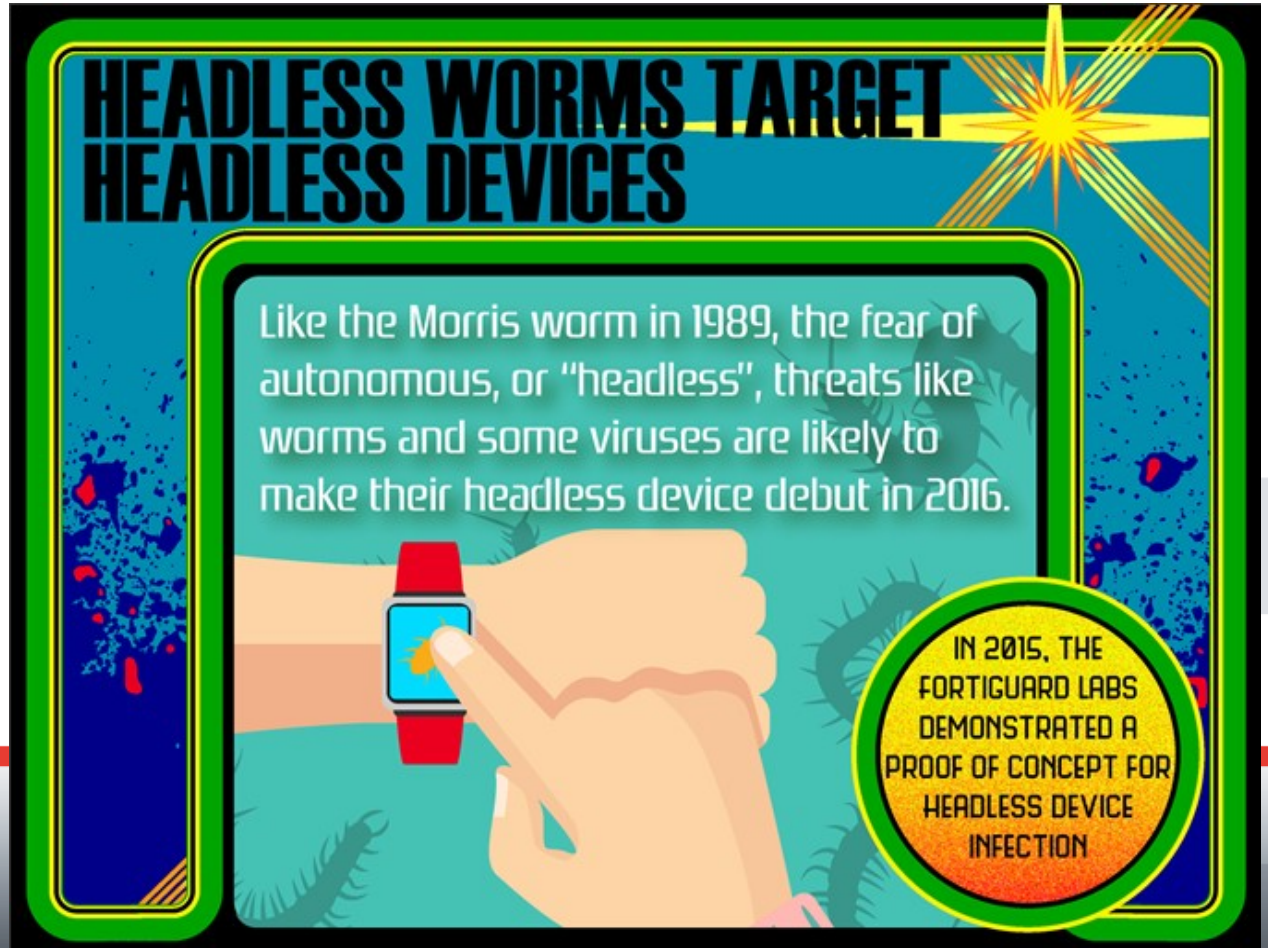
Fortinet Threat Predictions 2016

FORTINET®

THE EVOLVING THREAT LANDSCAPE

FORTINET®


THE RISE OF MACHINE TO MACHINE ATTACKS
GARTNER PREDICTS OVER 20 BILLION CONNECTED DEVICES BY 2020
The connected, exponentially growing, attack surface we call IoT will entice cyber criminals to traverse the ecosystem of personal devices as a vector to gain access to lucrative corporate networks.

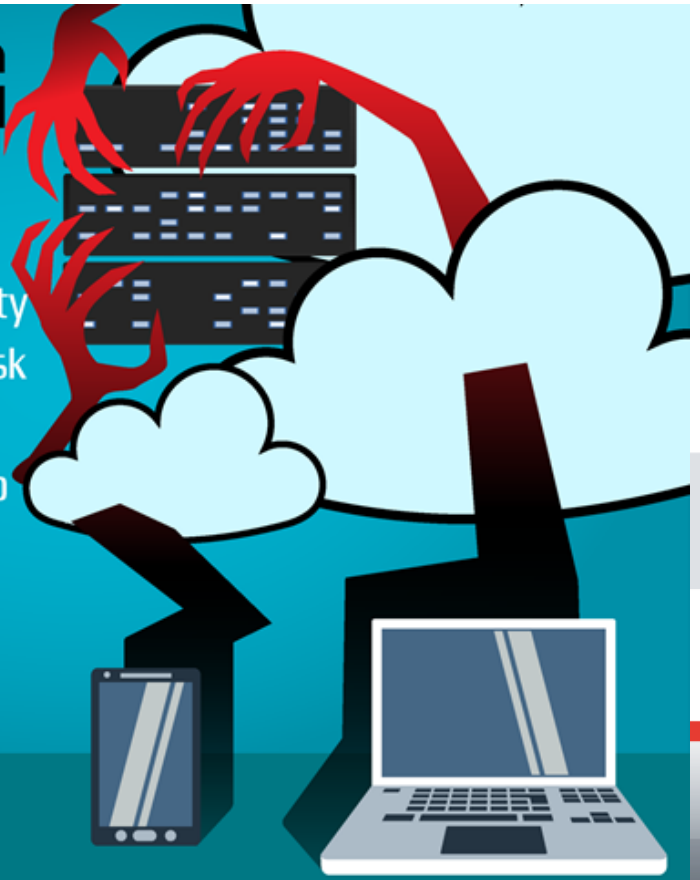

HEADLESS WORMS TARGET HEADLESS DEVICES
Like the Morris worm in 1989, the fear of autonomous, or "headless", threats like worms and some viruses are likely to make their headless device debut in 2016.
IN 2015, THE FORTIGUARD LABS DEMONSTRATED A PROOF OF CONCEPT FOR HEADLESS DEVICE INFECTION

FORTINET®

JAILBREAKING THE CLOUD

In 2015, the Venom vulnerability was used to exploit floppy disk drivers to break out of a hypervisor and gain access to a host operating system.

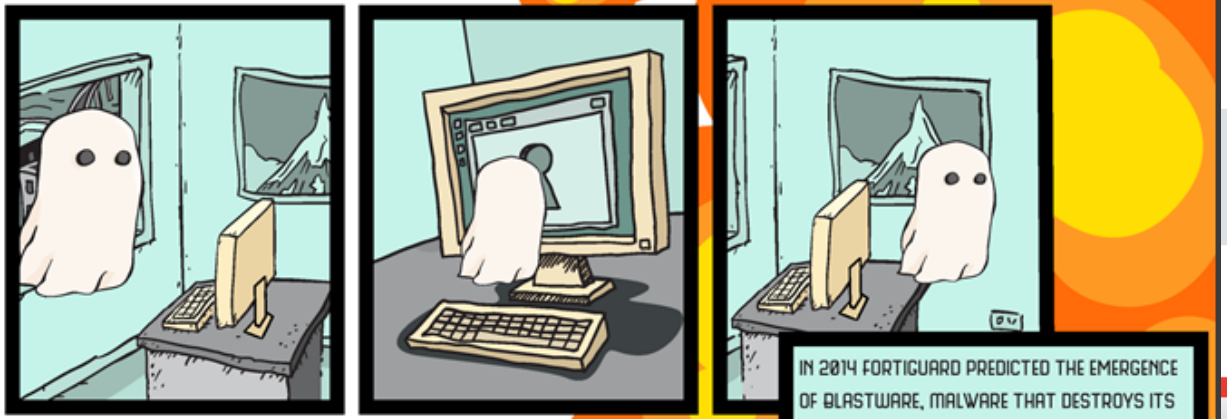
In 2016 we expect to see malware that is purpose-built to crack the hypervisor



FORTINET®

GHOSTWARE CONCEALS INDICATORS OF COMPROMISE

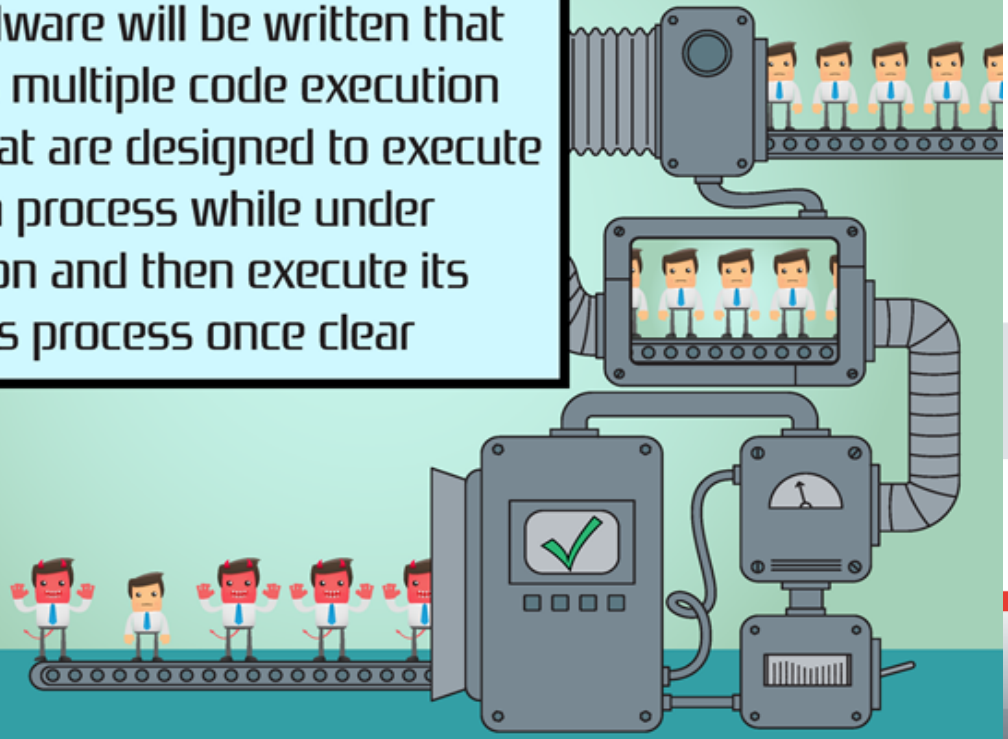
Malware specifically designed to infiltrate, steal, and then conceal its tracks is likely to make an appearance in 2016. As law enforcement bolsters their investigative capabilities, Hackers will need to clean up after themselves or face a justice system that is adjusting to cybercrime.



FORTINET®

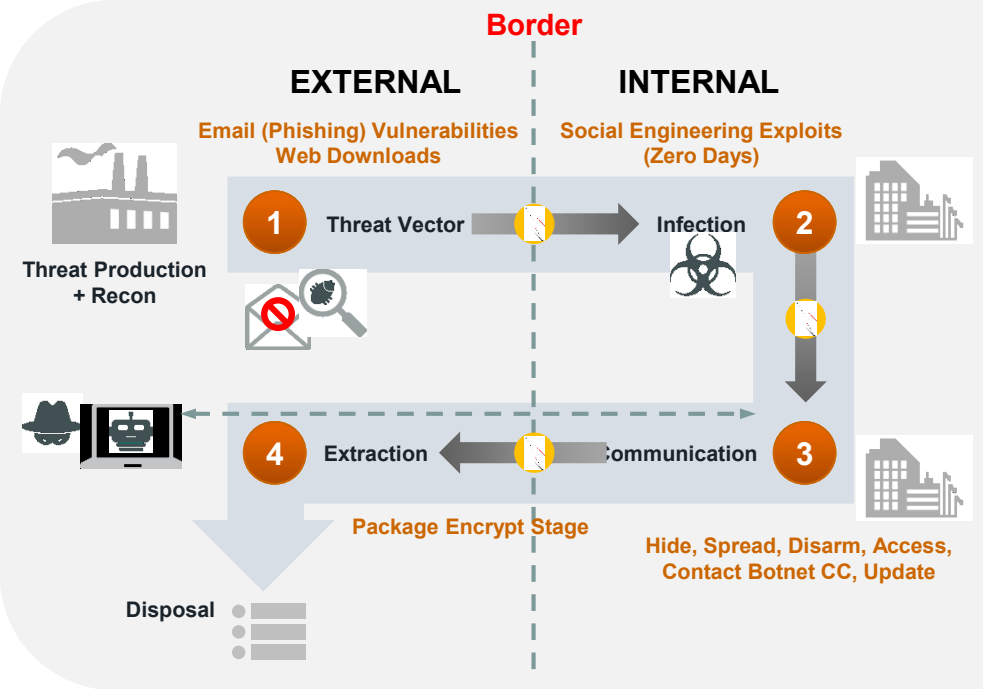
TWO-FACED MALWARE

New malware will be written that employs multiple code execution paths that are designed to execute a benign process while under inspection and then execute its malicious process once clear

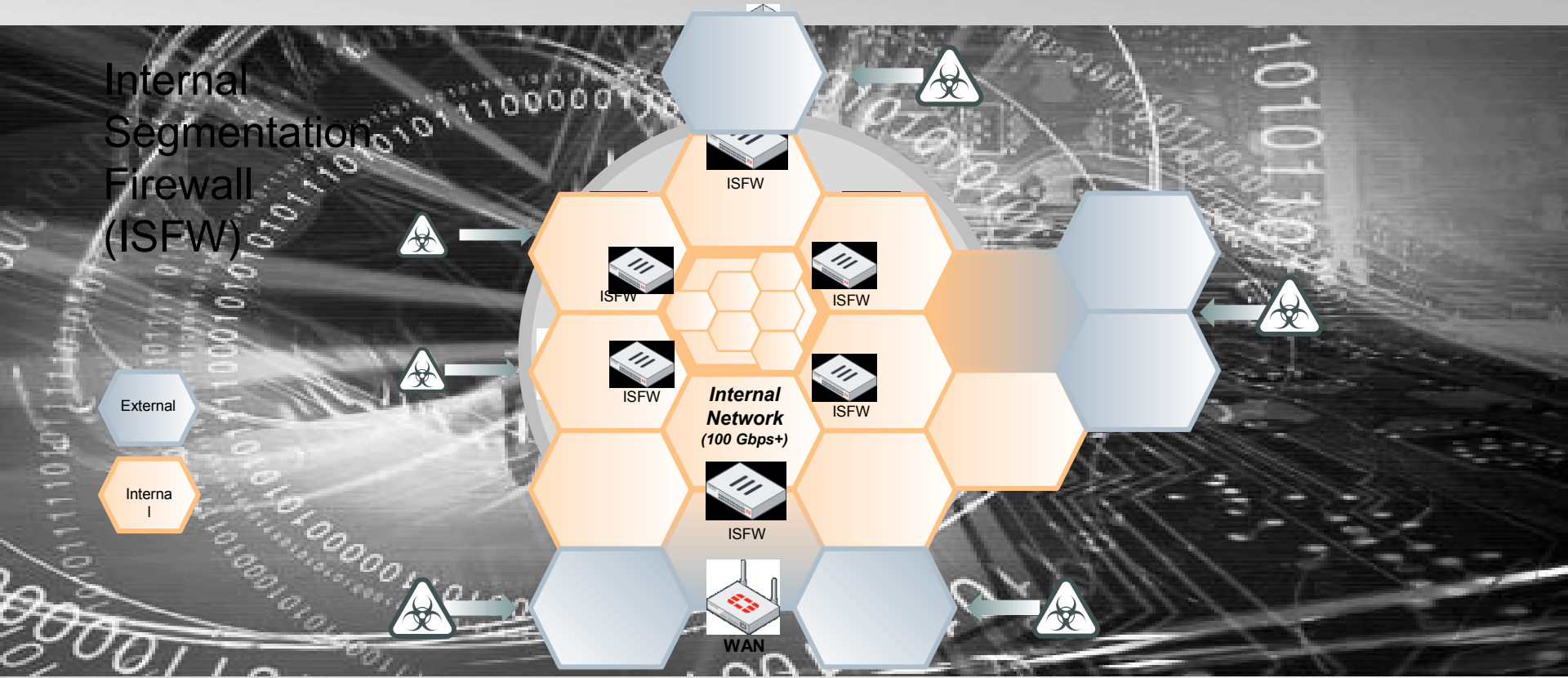


Advanced Threats Take Advantage of the “Flat Internal” Network

- Existing Firewalls focused on the **Border**
- Internal network no longer “trusted”
- Many ways into the network
- Once inside threats can spread quickly



Threat Landscape & Evolving IT Infrastructure



ISFW Requirement NO. 1 - PERFORMANCE

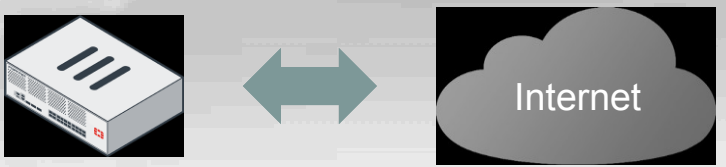
Internal Segmentation Firewall (ISFW)

Interfaces → 10G, 40G & 100G

No. of Ports → 8 to 48 Ge/10Ge

Throughput → 10Gps to 1Tbps

Border Firewall (NGFW)

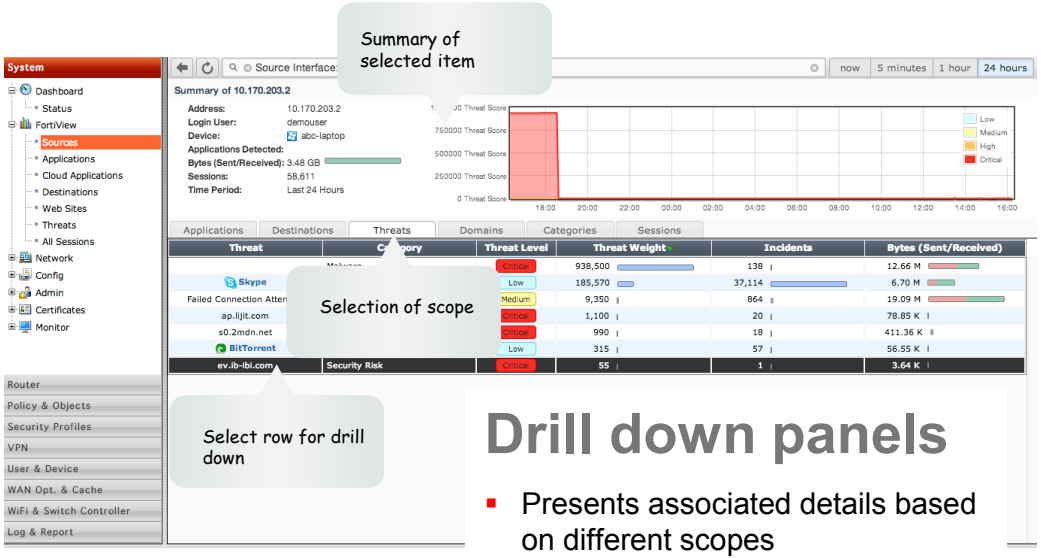


Ports Speeds → 1G, 10G

No. of Ports → 2 to 12

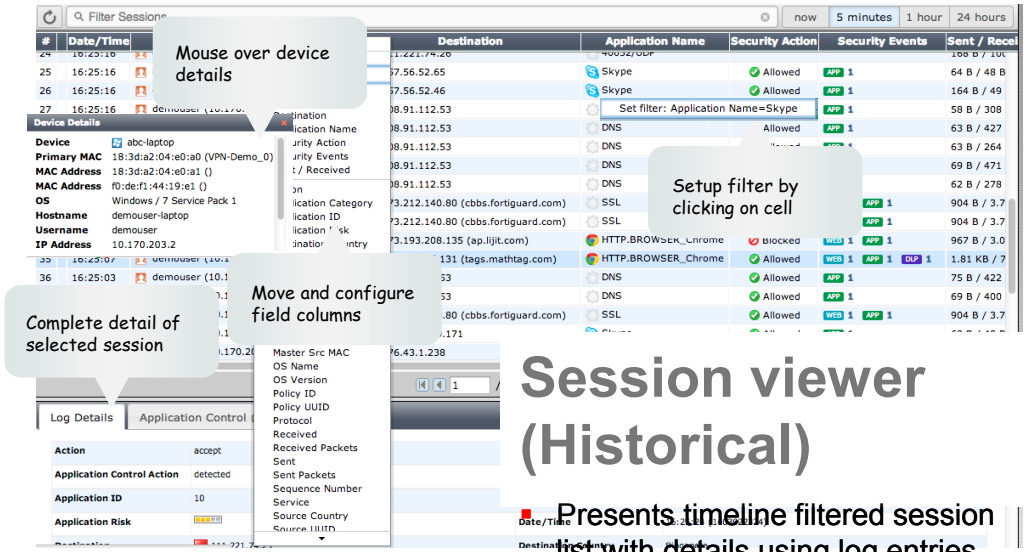
Throughput → Mbps to 1Gbps

ISFW Requirement No. 2 - VISIBILITY



Drill down panels

- Presents associated details based on different scopes
- Further drill down to filtered Session Viewer



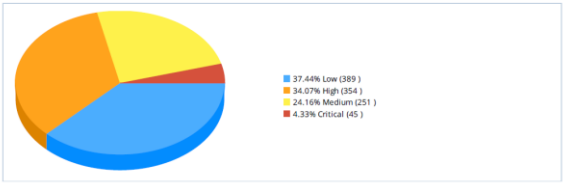
Session viewer (Historical)

- Presents timeline filtered session list with details using log entries

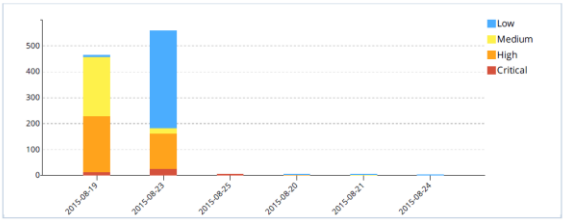
FORTINET

Summary

Intrusions By Severity



Intrusions Timeline



High Severity Intrusions

#	Attack Name	Intrusion Type	Counts
1	Back.Orifice.Traffic	Malware	34
2	FritzBox.Webcm.Unauthenticated.Command.Injection	OS Command Injection	27
3	HTTP.URI.SQL.Injection	SQL Injection	18
4	MobileCartly.Arbitrary.File.Creation	Permission/Priviledge/Access Control	7
5	PHP.Charts.PHP.Code.Execution	Code Injection	7
6	Open.Flash.Chart.PHP.File.Upload	Permission/Priviledge/Access Control	6
7	TWiki.Debugenableplugins.Remote.Code.Inje		
8	Spreecommerce.Arbitrary.Command.Executio		
9	XODA.Arbitrary.PHP.File.Upload		
10	WeBid.Converter.Remote.PHP.Code.Injection		
11	Gitorious.Arbitrary.Command.Execution		
12	PhpMoAdmin.moadmin.php.Unauthenticate on		
13	WordPress.RevSlider.Arbitrary.File.Upload		
14	CakePHP.Cache.Corruption.Code.Execution		
15	Auxilium.RateMyPet.Arbitrary.File.Upload		
16	DataLife.Engine.Catlist.Parameter.PHP.Code.I		
17	Adobe.ColdFusion.Administrator.Page.Direct		
18	Snortreport.PHP.Remote.Command.Executio		

FORTINET

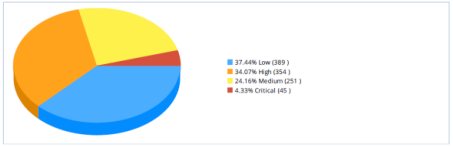
Intrusion Victims

#	Attack Victim	Counts (Critical / High / Medium)	Percent of Total Attacks
1	203.121.162.84	483	74.31%
2	203.121.162.87	116	17.85%
3	203.121.162.85	17	2.62%
4	203.121.162.72	4	0.62%
5	203.121.162.73	4	0.62%
6	203.121.162.76	2	0.31%
7	203.121.162.66	2	0.31%
8	203.121.162.93	2	0.31%
9	203.121.162.67	2	0.31%
10	106.10.199.11	2	0.31%
11	203.121.162.77	2	0.31%
12	203.121.162.86	2	0.31%
13	203.121.162.83	2	0.31%
14	203.121.162.68	2	0.31%
15	203.121.162.75	2	0.31%
16	203.121.162.71	2	0.31%
17	203.121.162.80	2	0.31%
18	203.121.162.90	2	0.31%

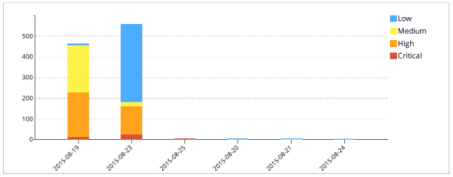
FORTINET

Summary

Intrusions By Severity



Intrusions Timeline



FORTINET

Intrusions Detected

Critical Severity Intrusions

#	Attack Name	Intrusion Type	Counts
1	OpenSSL.Heartbleed.Attack	Information Disclosure	9
2	Bash.Function.Definitions.Remote.Code.Execution	OS Command Injection	4
3	Adobe.ColdFusion.Multiple.Vulnerabilities	Information Disclosure	4
4	Symantec.Web.Gateway.Arbitrary.File.Upload	Permission/Priviledge/Access Control	3
5	HTTP.Negative.Data.Length	Buffer Errors	3
6	Pandora.v3.1.Default.Admin.Account.Access	Improper Authentication	3
7	Wordpress.Front-end.Editor.Unauthenticated.File.Upload		
8	WordPress.Foxypress.Plugin.Uploadify.Arbitrary.File.Upload		
9	Apache.Struts2.OGNL.Script.Injection		
10	Symantec.Web.Gateway.Ipchange.Command.Injection		
11	RedHat.Piranha.Command.Execution		
12	Adobe.ColdFusion.Scheduled.Task.Arbitrary.File.Upload		
13	CGI.Phf.Command.Execution		
14	ManageEngine.DesktopCentral.Arbitrary.File.Upload		
15	Ruby.On.Rails.XML.Processor.YAML.Deserialization.Code.Exe		
16	OpenSSL.TLS.Heartbeat.Information.Disclosure		

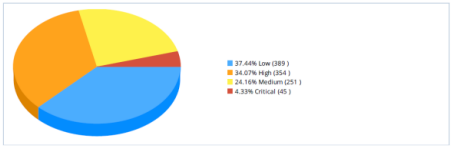
Intrusion Sources

#	Attack Source	Counts (Critical / High / Medium)	Percent of Total Attacks
1	101.108.23.80	303	46.62%
2	180.180.36.90	129	19.85%
3	124.120.20.119	87	13.38%
4	124.120.2.115	78	12.00%
5	101.108.31.249	13	2.00%
6	124.120.11.99	10	1.54%
7	124.120.7.82	8	1.23%
8	101.108.4.201	7	1.08%
9	101.108.31.60	4	0.62%
10	212.84.191.178	4	0.62%
11	119.63.94.11	2	0.31%
12	66.240.192.138	1	0.15%
13	141.212.121.152	1	0.15%
14	203.150.230.103	1	0.15%
15	101.108.18.182	1	0.15%
16	222.110.205.167	1	0.15%

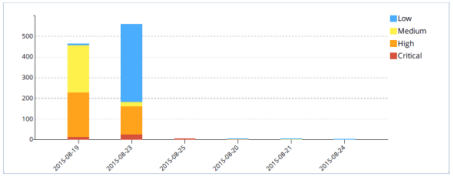
FORTINET

Summary

Intrusions By Severity



Intrusions Timeline



FORTINET

Intrusions Blocked

#	Intrusion Name	Intrusion Type	Severity	Counts
1	OpenSSL.Heartbleed.Attack	Information Disclosure	Critical	9
2	Bash.Function.Definitions.Remote.Code.Execution	OS Command Injection	Critical	4
3	HTTP.Negative.Data.Length	Buffer Errors	Critical	3
4	Apache.Struts2.OGNL.Script.Injection	Other	Critical	3
5	RedHat.Piranha.Command.Execution	Code Injection	Critical	2
6	Ruby.On.Rails.XML.Processor.YAML.Deserialization.Code.Execution	Other	Critical	1
7	ManageEngine.DesktopCentral.Arbitrary.File.Upload	Permission/Priviledge/Access Control	Critical	1
8	HTTP.URI.SQL.Injection	SQL Injection	High	18
9	Spreecommerce.Arbitrary.Command.Execution	OS Command Injection	High	4
10	UpTime.MS.Post2file.Arbitrary.File.Upload	Permission/Priviledge/Access Control	High	3

Application Usage By Category

As part of the traffic classification process, the FortiGate identifies and categorizes the applications crossing the network into different categories based on the number of sessions and

FORTINET

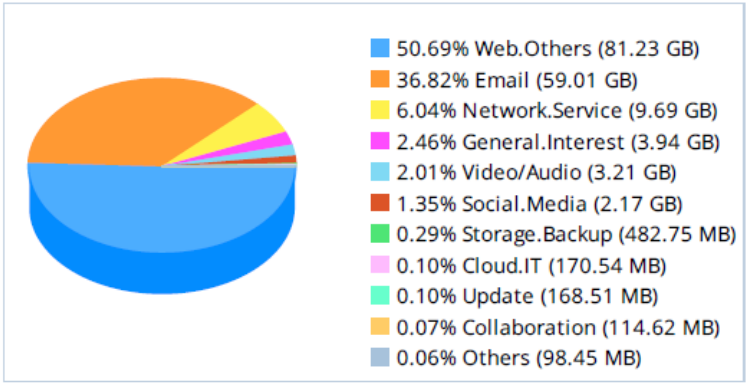
Top Application Users By Bandwidth

This chart provides information about the users who are creating the most network traffic in terms of bandwidth usage. It helps the network manager to identify users that are potentially abusing network usage or creating traffic that does not comply with internal security policies. The following chart displays the top 20 users by bandwidth usage.

Top Users By Bandwidth

#	User (or IP)	Source IP	Bandwidth (Sent / Received)
1	203.121.162.72	203.121.162.72	34.53 GB
2	203.121.162.77	203.121.162.77	33.18 GB
3	223.27.218.142	223.27.218.142	10.13 GB
4	119.63.94.11	119.63.94.11	7.39 GB
5	203.121.162.66	203.121.162.66	3.50 GB
6	119.63.94.19	119.63.94.19	1.41 GB
7	180.183.128.145	180.183.128.145	1.07 GB
8	203.121.162.90	203.121.162.90	581.76 MB
9	103.40.116.41	103.40.116.41	464.96 MB
10	49.49.251.214	49.49.251.214	344.46 MB

Top 10 Application Categories by Bandwidth Usage



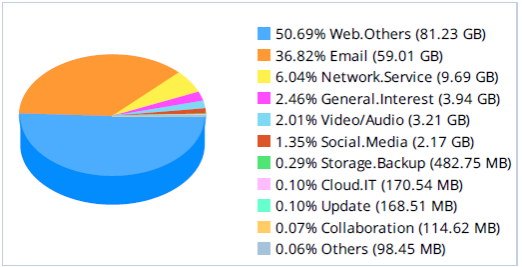
Application Categories By Bandwidth Usage

#	Application Category
1	Web.Others
2	Email
3	Network.Service
4	General.Interest
5	Video/Audio
6	Social.Media
7	Storage.Backup
8	Cloud.IT
9	Update
10	Collaboration
11	Remote.Access
12	Mobile
13	Business
14	VoIP
15	Game
16	P2P
17	Proxy
18	Botnet
19	unscanned

Application Usage By Category

As part of the traffic classification process, the FortiGate identifies and categorizes the applications crossing the network into different categories based on the number of sessions and bandwidth. This data complements the granular application threat data and provides a more complete summary of the types of applications in use on the network.

Top 10 Application Categories by Bandwidth Usage



Top Applications Running Over HTTP

#	Application	Sessions	Bandwidth
1	HTTPS.BROWSER	2,303,458	65.67 GB
2	HTTP.BROWSER	3,038,621	15.39 GB
3	SSL	118,037	5.19 GB
4	YouTube	43,335	3.15 GB
5	Google.Accounts	270,669	3.06 GB
6	Facebook	79,024	1.45 GB
7	Gmail	10,790	458.42 MB
8	HTTP.Download.Accelerator	320,308	430.05 MB
9	Twitter	44,780	414.82 MB
10	Hotmail	2,912	288.84 MB
11	Google.Translate	20,595	233.67 MB
12	4shared	7,174	192.20 MB
13	Amazon.AWS	76	166.47 MB
14	Dropbox	2,576	158.17 MB
15	HTTP.Segmented.Download	14,015	140.86 MB
16	Google.Plus	5,265	126.90 MB
17	SSLv2	26,309	119.41 MB
18	LinkedIn	8,715	94.98 MB
19	Photobucket	3,717	92.30 MB
20	Blogger	6,126	87.70 MB

Network Visibility

FORTINET FortiGate VM64

Wizard

System
- Dashboard
  - Status
- FortiView
  - Sources
  - Applications
  - Cloud Applications
  - Destinations
  - Web Sites
  - Threats
  - All Sessions
  - System Events
  - Admin Logins
  - VPN
- Network
- Config
  - HA
  - SNMP
  - Replacement Messages
  - FortiGuard
  - FortiSandbox
  - Advanced
  - Features
- Admin
  - Administrators
  - Admin Profiles
  - Settings

Router
Policy & Objects
Security Profiles
VPN
User & Device
Log & Report

Cloud Application: YouTube | Add Filter | Applications | Users | 5 minutes

Summary of YouTube

Sessions: 36
Time Period: Last 5 Minutes

Cloud Users | Files | Videos | Sessions

1	08:58:51	10.0.0.2	pathom (10.0.0.2)	ညီမင်းခိုင် - ဝဲငြိမ့် (Nyi Min Khine - Nwe Ni)	612.57 KB
2	08:58:14	10.0.0.2	pathom (10.0.0.2)	ညီမင်းခိုင် - ဝဲငြိမ့် (Nyi Min Khine - Nwe Ni)	155.04 KB
3	08:58:12	10.0.0.2	pathom (10.0.0.2)	ညီမင်းခိုင် - ဝဲငြိမ့် (Nyi Min Khine - Nwe Ni)	499 B
4	08:58:10	10.0.0.2	pathom (10.0.0.2)	ညီမင်းခိုင် - ဝဲငြိမ့် (Nyi Min Khine - Nwe Ni)	69.67 KB
5	08:58:02	10.0.0.2	pathom (10.0.0.2)	ညီမင်းခိုင် - ဝဲငြိမ့် (Nyi Min Khine - Nwe Ni)	65.54 KB
6	08:58:00	10.0.0.2	pathom (10.0.0.2)	ညီမင်းခိုင် - ဝဲငြိမ့် (Nyi Min Khine - Nwe Ni)	66.67 KB
7	08:58:00	10.0.0.2	pathom (10.0.0.2)	ညီမင်းခိုင် - ဝဲငြိမ့် (Nyi Min Khine - Nwe Ni)	65.54 KB
8	08:58:00	10.0.0.2	pathom (10.0.0.2)	ညီမင်းခိုင် - ဝဲငြိမ့် (Nyi Min Khine - Nwe Ni)	65.54 KB
9	08:57:59	10.0.0.2	pathom (10.0.0.2)	Lay Phyu Song with Lyrics ေလးျဖဴ တိမ္ဖူးတဲ့လ	156.78 KB
10	08:57:58	10.0.0.2	pathom (10.0.0.2)	Lay Phyu Song with Lyrics ေလးျဖဴ တိမ္ဖူးတဲ့လ	78.60 KB
11	08:57:58	10.0.0.2	pathom (10.0.0.2)	Lay Phyu Song with Lyrics ေလးျဖဴ တိမ္ဖူးတဲ့လ	65.54 KB
12	08:57:57	10.0.0.2	pathom (10.0.0.2)	Lay Phyu Song with Lyrics ေလးျဖဴ တိမ္ဖူးတဲ့လ	65.54 KB
13	08:57:57	10.0.0.2	pathom (10.0.0.2)	Lay Phyu Song with Lyrics ေလးျဖဴ တိမ္ဖူးတဲ့လ	65.54 KB
14	08:57:54	10.0.0.2	pathom (10.0.0.2)	Myanmar new love song - 2015 - အလြမ္းသေ - Bobby Soxer (with lyrics)	317.72 KB
15	08:57:54	10.0.0.2	pathom (10.0.0.2)	Myanmar new love song - 2015 - အလြမ္းသေ - Bobby Soxer (with lyrics)	158.79 KB
16	08:57:50	10.0.0.2	pathom (10.0.0.2)	ေမြကြာပ်ံကိုး htet mon myanmar music song	65.54 KB
17	08:57:40	10.0.0.2	pathom (10.0.0.2)	ေမြကြာပ်ံကိုး htet mon myanmar music song	1.25 KB
18	08:57:40	10.0.0.2	pathom (10.0.0.2)	ေမြကြာပ်ံကိုး htet mon myanmar music song	59.49 KB
19	08:57:32	10.0.0.2	pathom (10.0.0.2)	ေမြကြာပ်ံကိုး htet mon myanmar music song	65.54 KB
20	08:57:32	10.0.0.2	pathom (10.0.0.2)	ေမြကြာပ်ံကိုး htet mon myanmar music song	46.22 KB
21	08:57:32	10.0.0.2	pathom (10.0.0.2)	ေမြကြာပ်ံကိုး htet mon myanmar music song	65.54 KB
22	08:57:32	10.0.0.2	pathom (10.0.0.2)	ေမြကြာပ်ံကိုး htet mon myanmar music song	65.54 KB
23	08:57:32	10.0.0.2	pathom (10.0.0.2)	ေမြကြာပ်ံကိုး htet mon myanmar music song	65.54 KB
24	08:57:32	10.0.0.2	pathom (10.0.0.2)	ေမြကြာပ်ံကိုး htet mon myanmar music song	65.54 KB
25	08:57:17	10.0.0.2	pathom (10.0.0.2)	Myanmar new love song - 2015 - အလြမ္းသေ - Bobby Soxer (with lyrics)	1.03 MB
26	08:57:08	10.0.0.2	pathom (10.0.0.2)	Myanmar new love song - 2015 - အလြမ္းသေ - Bobby Soxer (with lyrics)	1.15 KB
27	08:57:08	10.0.0.2	pathom (10.0.0.2)	Myanmar new love song - 2015 - အလြမ္းသေ - Bobby Soxer (with lyrics)	115.86 KB
28	08:57:00	10.0.0.2	pathom (10.0.0.2)	Myanmar new love song - 2015 - အလြမ္းသေ - Bobby Soxer (with lyrics)	65.54 KB
			pathom (10.0.0.2)	Myanmar new love song - 2015 - အလြမ္းသေ - Bobby Soxer (with lyrics)	65.54 KB

1 / 2 [Total: 63]

Top 20 Viruses Crossing The Network

As the FortiGate scans the network, it provides information about the viruses that are crossing the network. The Fortigate is able to apply different strategies in order to detect malware: - Signatures: Fortinet's Compact Pattern Recognition Language (CPRL) - Heuristics: These are applied to: * file structure; * API call. The FortiGate's antivirus engine provides two main capabilities: Decompression allows embedded files to be extracted; Emulation allows the hidden layers of malicious file of be extracted.

Top Viruses By Name

#	Virus Name	Occurrences
1	WM/Agent!tr	190
2	W32/Waski.K!tr	82
3	JS/Nemucod.AA!tr.dldr	
4	HTML/PhishA.4BB1!tr	
5	Zeus	
6	W32/Injector.CGWH!tr	
7	W32/Injector.CFFN!tr	

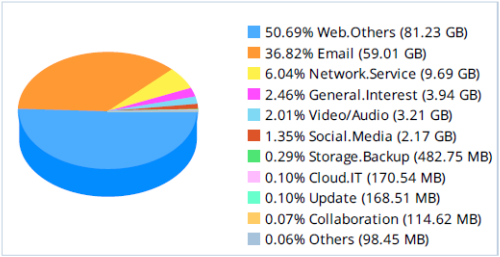
High Risk Applications

#	Risk	Application Name	Category	Technology	Bandwidth	Sessions
1	Botnet	Tiny.Botnet	Botnet	Client-Server	3.94 KB	5
2	Botnet	Torpig.Mebroot.Botnet	Botnet	Client-Server	529 B	2
3	Evasive	Twitter	Social.Media	Browser-Based	420.23 MB	48,506
4	Evasive	Photobucket_Share	Storage.Backup	Browser-Based	92.01 MB	3,571
5	Evasive	Google.Earth	General.Interest	Client-Server	31.68 MB	1,369
6	Evasive	Valve.Games	Game	Client-Server	14.50 KB	563
7	Evasive	Google.Hangouts	Collaboration	Browser-Based	37.27 MB	438
8	Evasive	Facebook_Plugins	Social.Media	Browser-Based	706.99 KB	366
9	Evasive	Facebook_Like.Button	Social.Media	Browser-Based	592.24 KB	292
10	Evasive	Google.Talk	Collaboration	Client-Server	504.52 KB	140
11	Evasive	EBay.Toolbar	General.Interest	Browser-Based	407.64 KB	108
12	Evasive	RTMPT	Video/Audio	Network-Protocol	42.40 KB	79
13	Evasive	Foursquare	Social.Media	Browser-Based	195.54 KB	64
14	Evasive	Computrace	General.Interest	Client-Server	13.56 KB	56
15	Evasive	Stumbleupon.Toolbar	General.Interest	Browser-Based	111.67 KB	47

Application Usage By Category

As part of the traffic classification process, the FortiGate identifies and categorizes the applications crossing the network into different categories based on the number of sessions and bandwidth. This data complements the granular application threat data and provides a more complete summary of the types of applications in use on the network.

Top 10 Application Categories by Bandwidth Usage



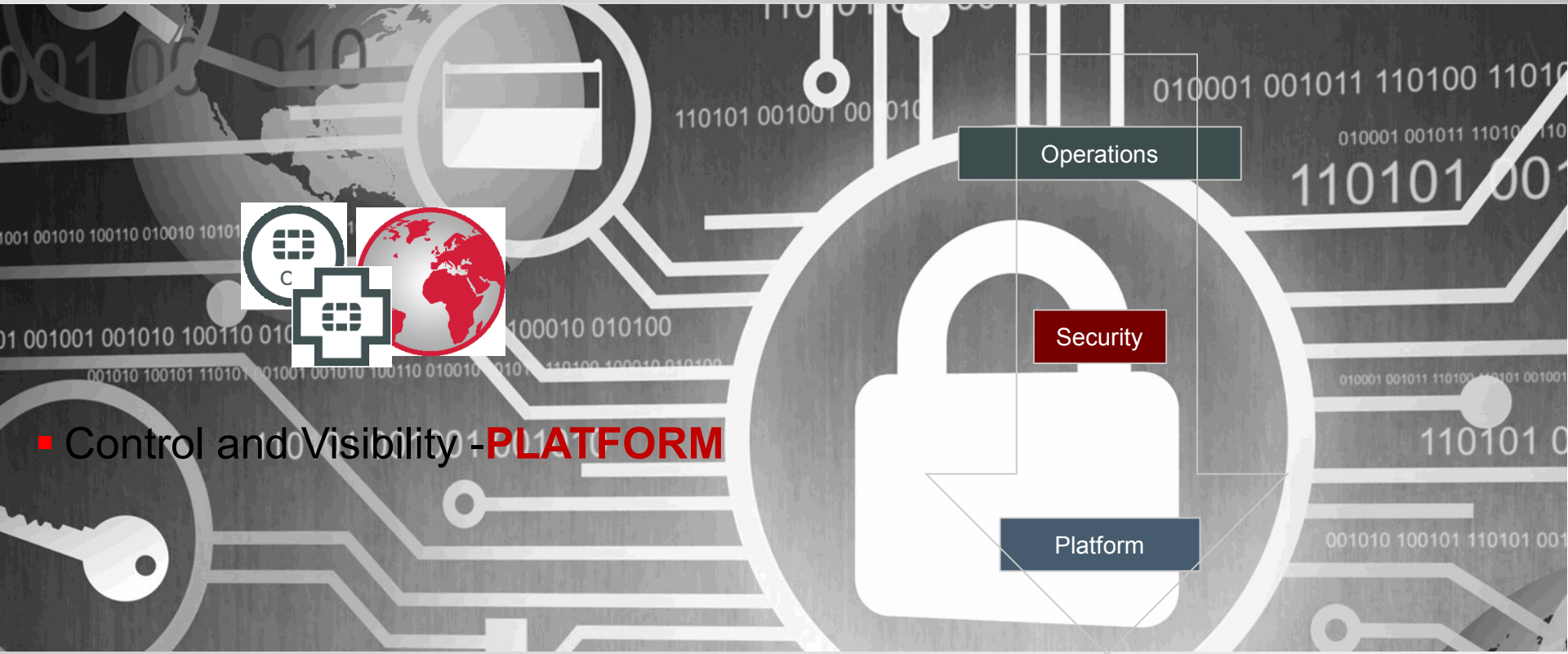
Top Web Sites By Browsing Time

The following chart shows the web sites that users visit for longer time. The administrator can then decide to create security policy to mitigate or block web sites access, accordingly to internal corporate policy.

Top Web Sites By Browsing Time

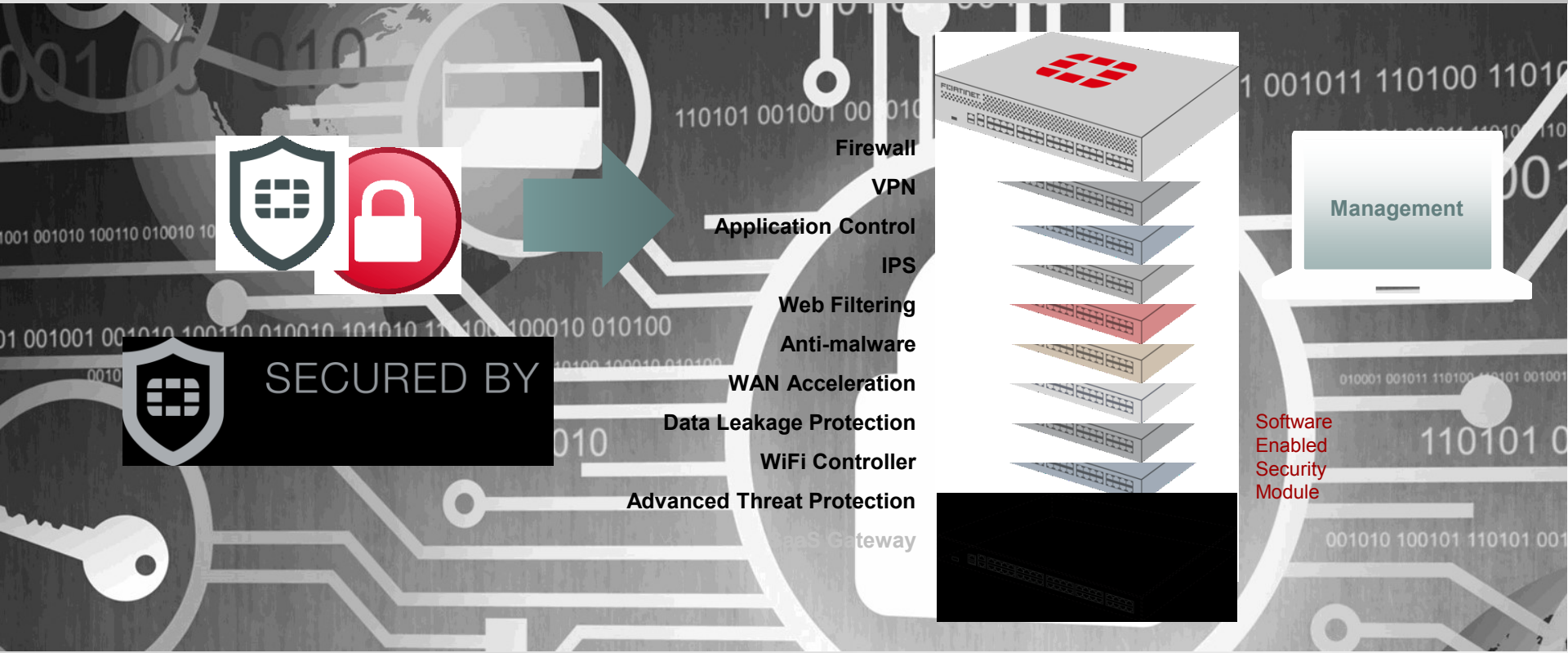
#	Website	Browsing Time(hh:mm:ss)	Bandwidth (Sent / Received)
1	www.bigc.co.th	89:59:52	871.59 MB
2	37.48.93.219	44:51:48	12.99 MB
3	tm300i.dhl.com	18:10:44	29.91 MB
4	crl.microsoft.com	13:46:11	2.98 MB
5	www.settrade.com	12:25:05	85.07 MB
6	www.microsoft.com	05:54:14	1.37 MB
7	188.172.204.20	05:41:24	1.25 MB
8	www.google-analytics.com	04:24:09	93.18 MB
9	download.mozilla.org	04:15:10	10.18 MB
10	info.music.metaservices.microsoft.com	04:05:43	59.47 MB
11	aqua.c1ub.net	03:11:34	2.95 MB
12	www.thscore.cc	03:05:18	15.12 MB
13	ocsp.digicert.com	02:33:47	11.30 MB
14	www.dida-semovci.com	02:33:03	1.29 MB
15	clients1.google.com	02:28:23	14.37 MB

ISFW Requirement NO. 4 – **POLICY & PROTECTION**

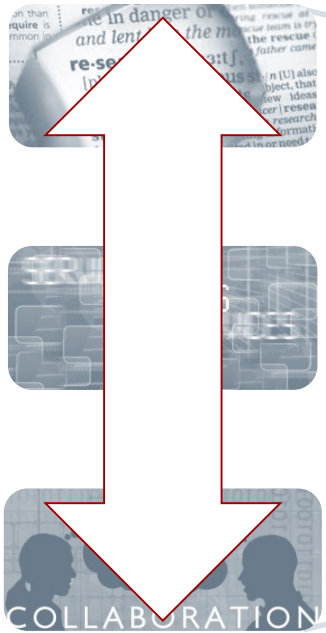


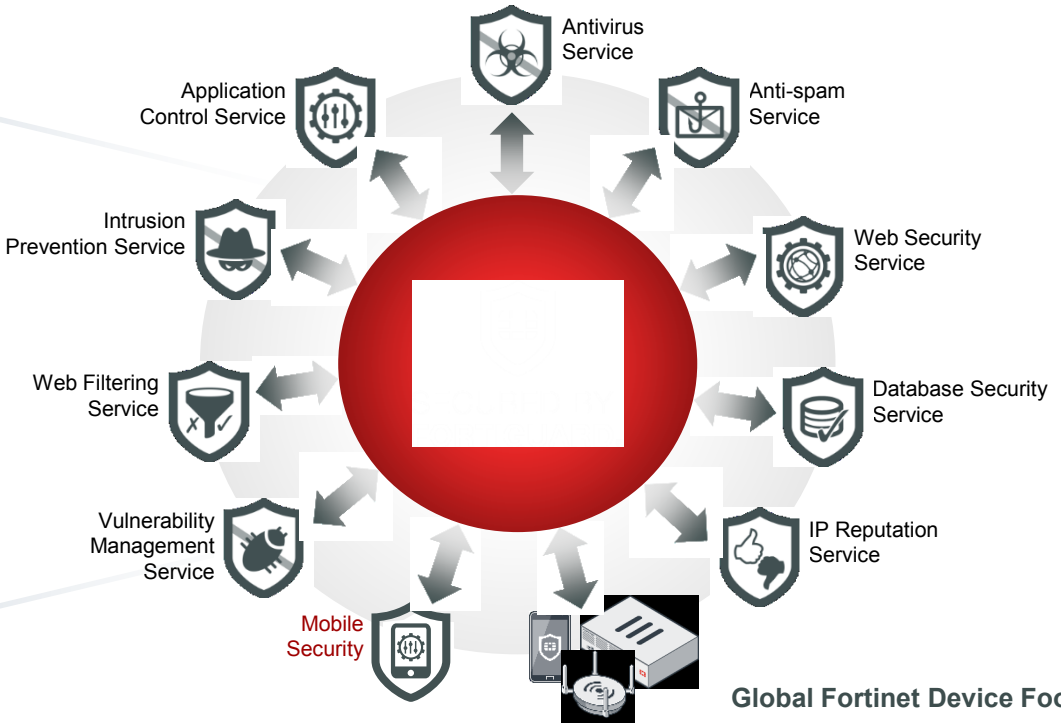
- Control and Visibility - **PLATFORM**

ISFW **PROTECTION**

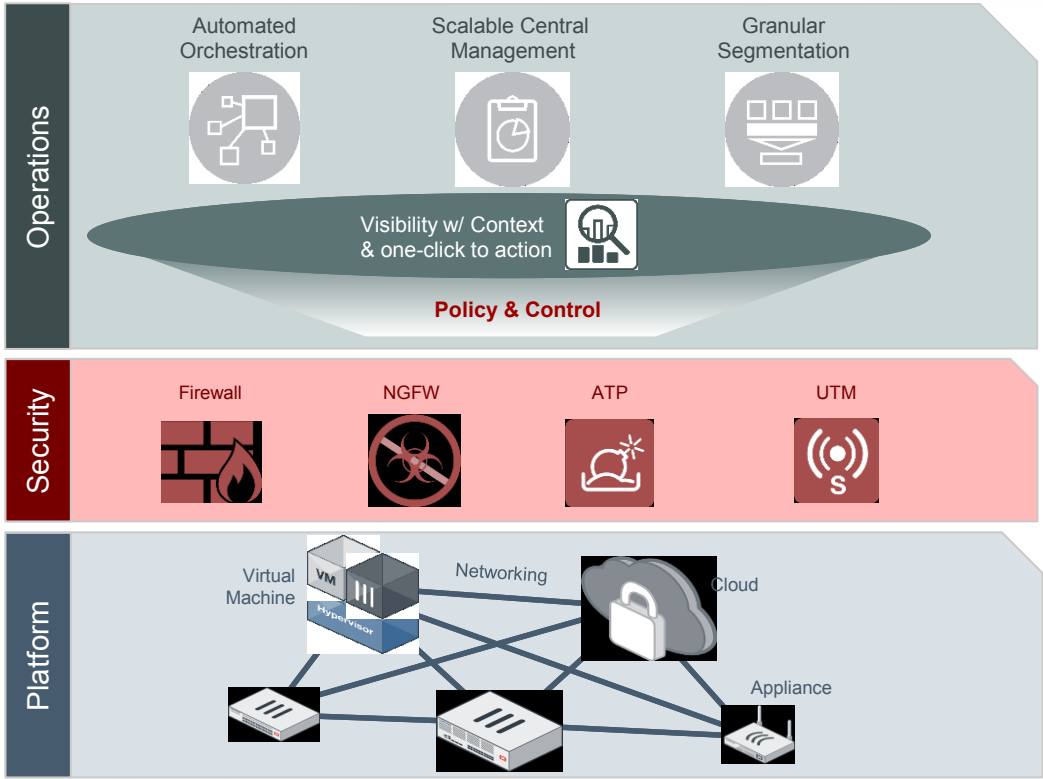


A Global Threat **Security** Service that Updates the Platform in Real time - FortiGuard





The Core of the Platform of Security



Time to Resolution

Protection & Intelligence

End to End Platform


DON’T GO UNPROTECTED
FORTINET®
FAST. SECURE. GLOBAL.