IT БЕЗПЕКА ДЛЯ KYIV SMART CITY

Fortinet Security Day

24 квітня 2019 р

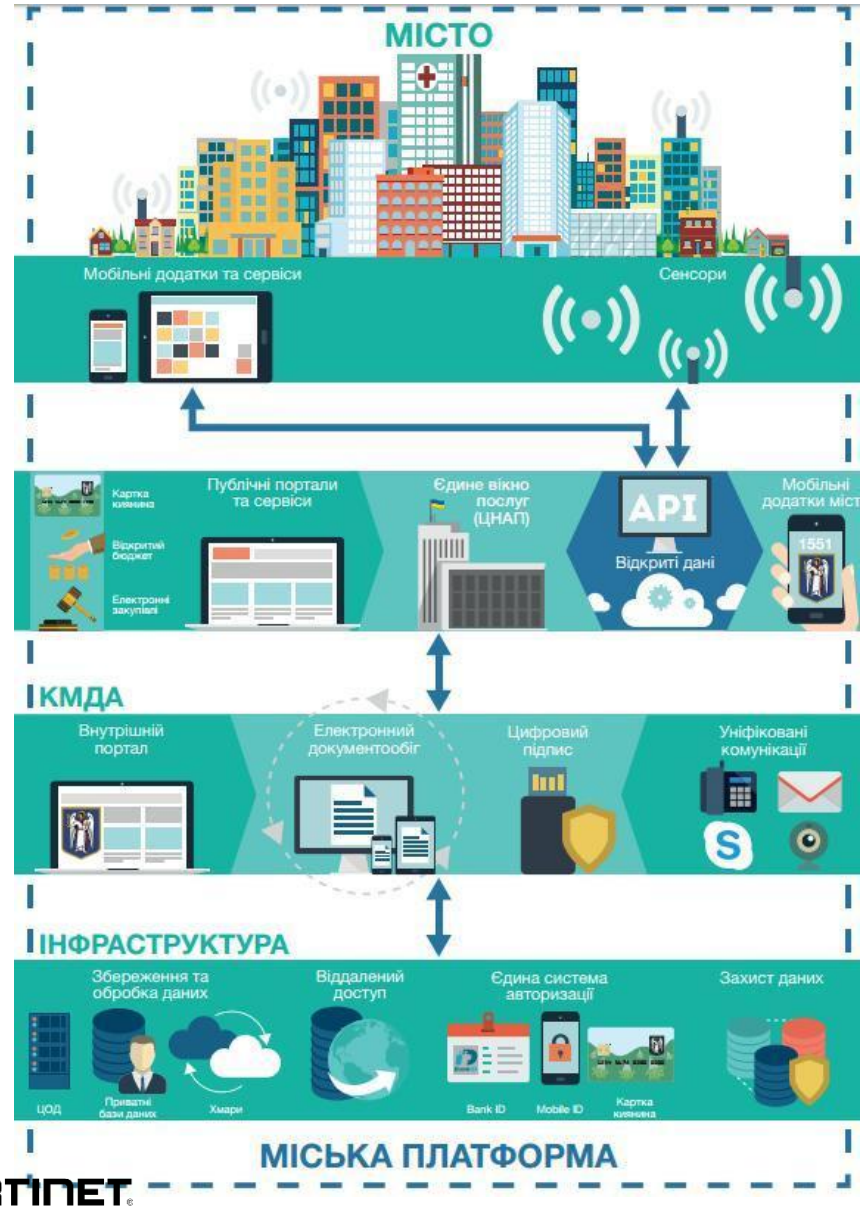
Костянтин Лєсніков

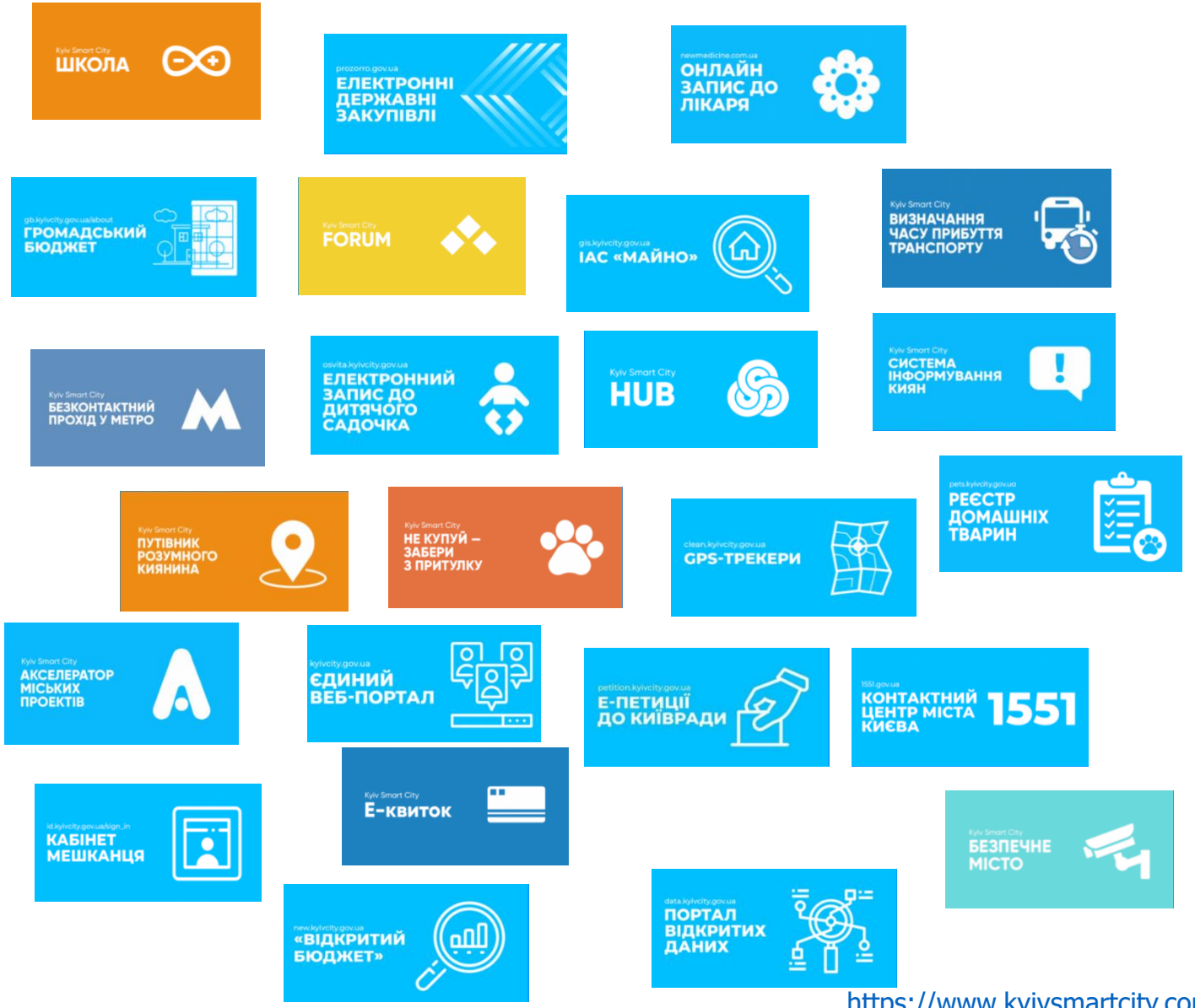
Технічний директор

Belintech UA

KYIV SMART CITY

Belintech UA

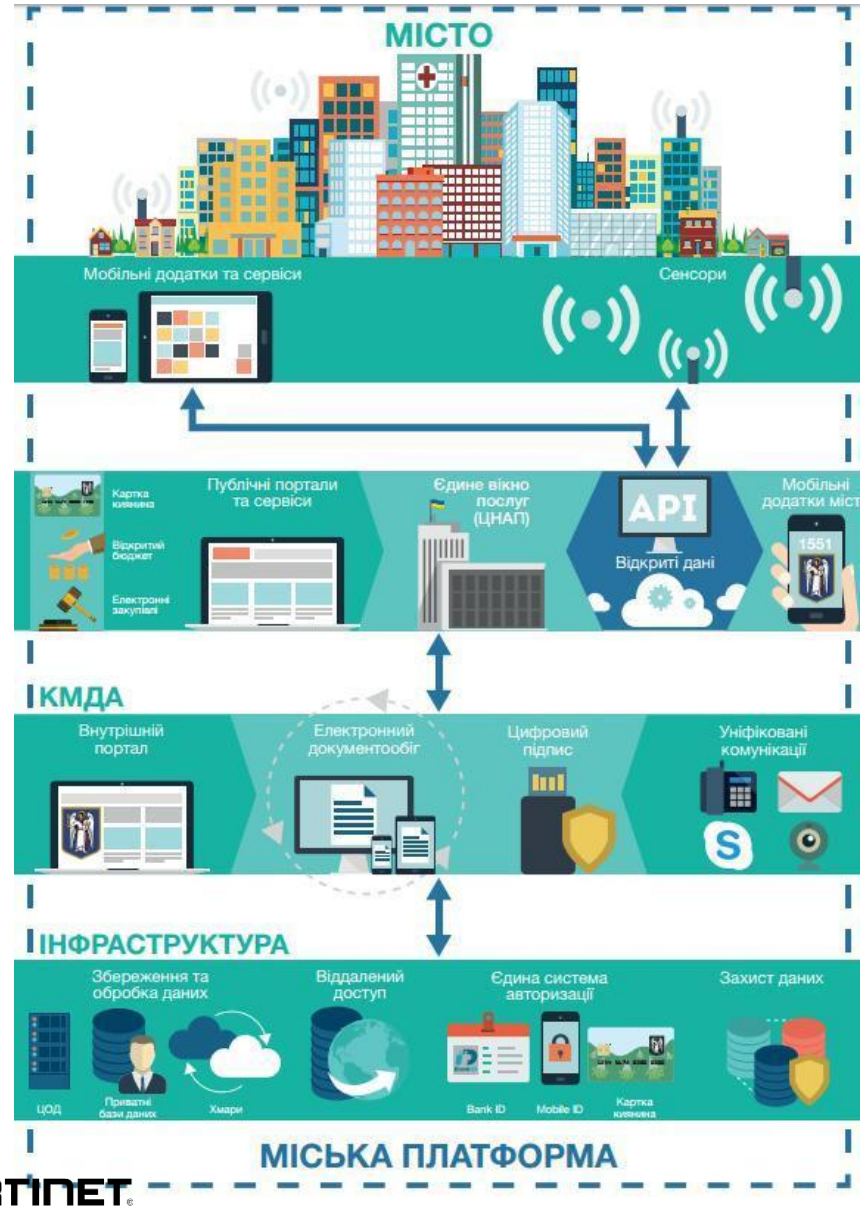


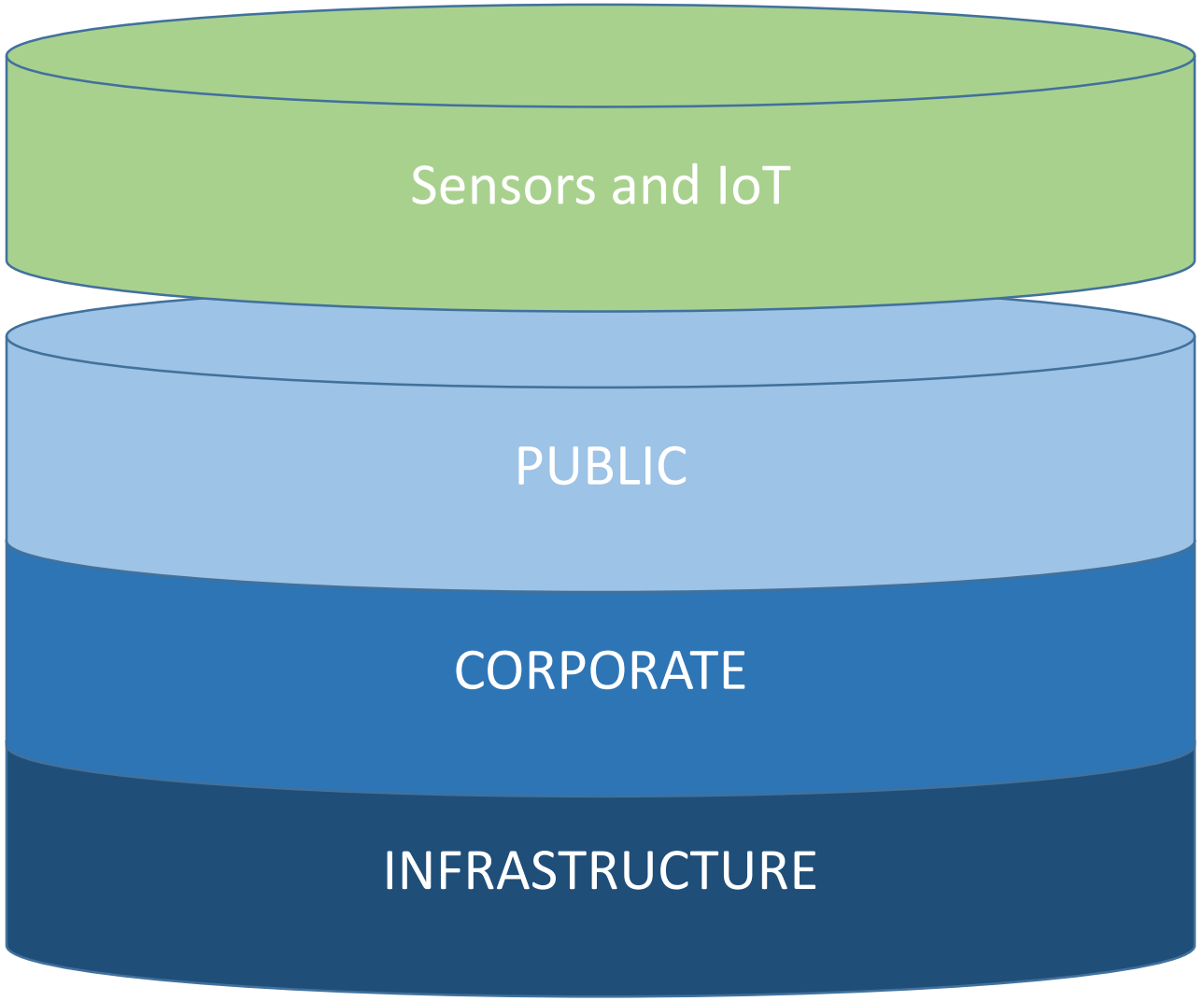


https://www.kyivsmartcity.com/

FORTINET

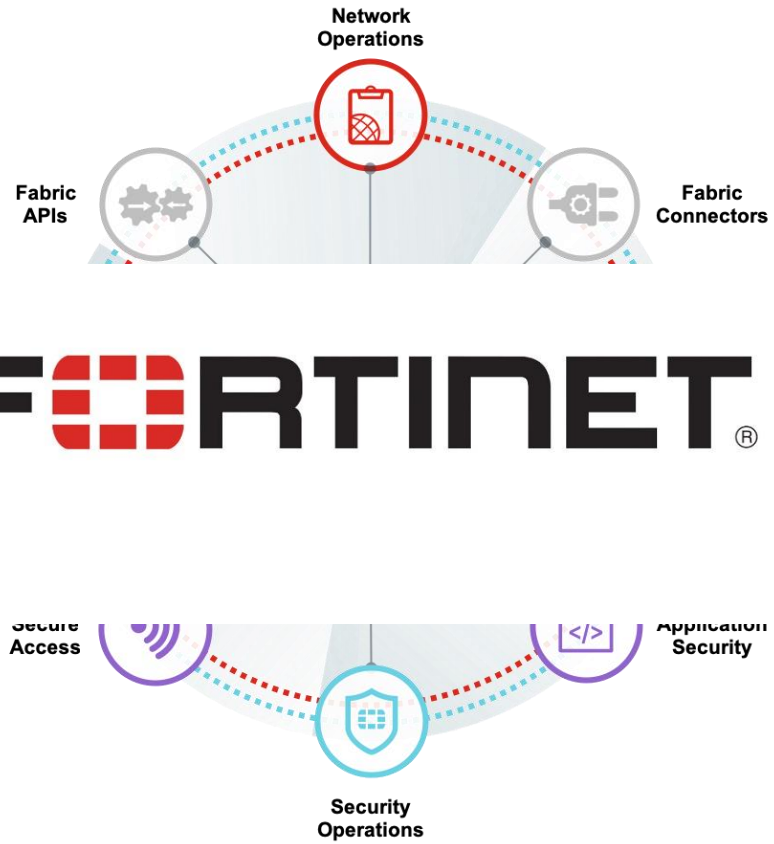
KYIV SMART CITY





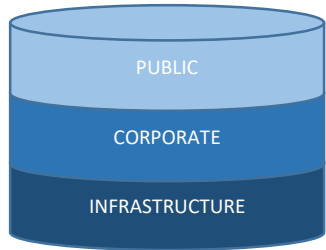
SECURITY

Belintech UA



FORTINET®

d



FORTINET

Belintech UA

FortiDDoS

FortiGate

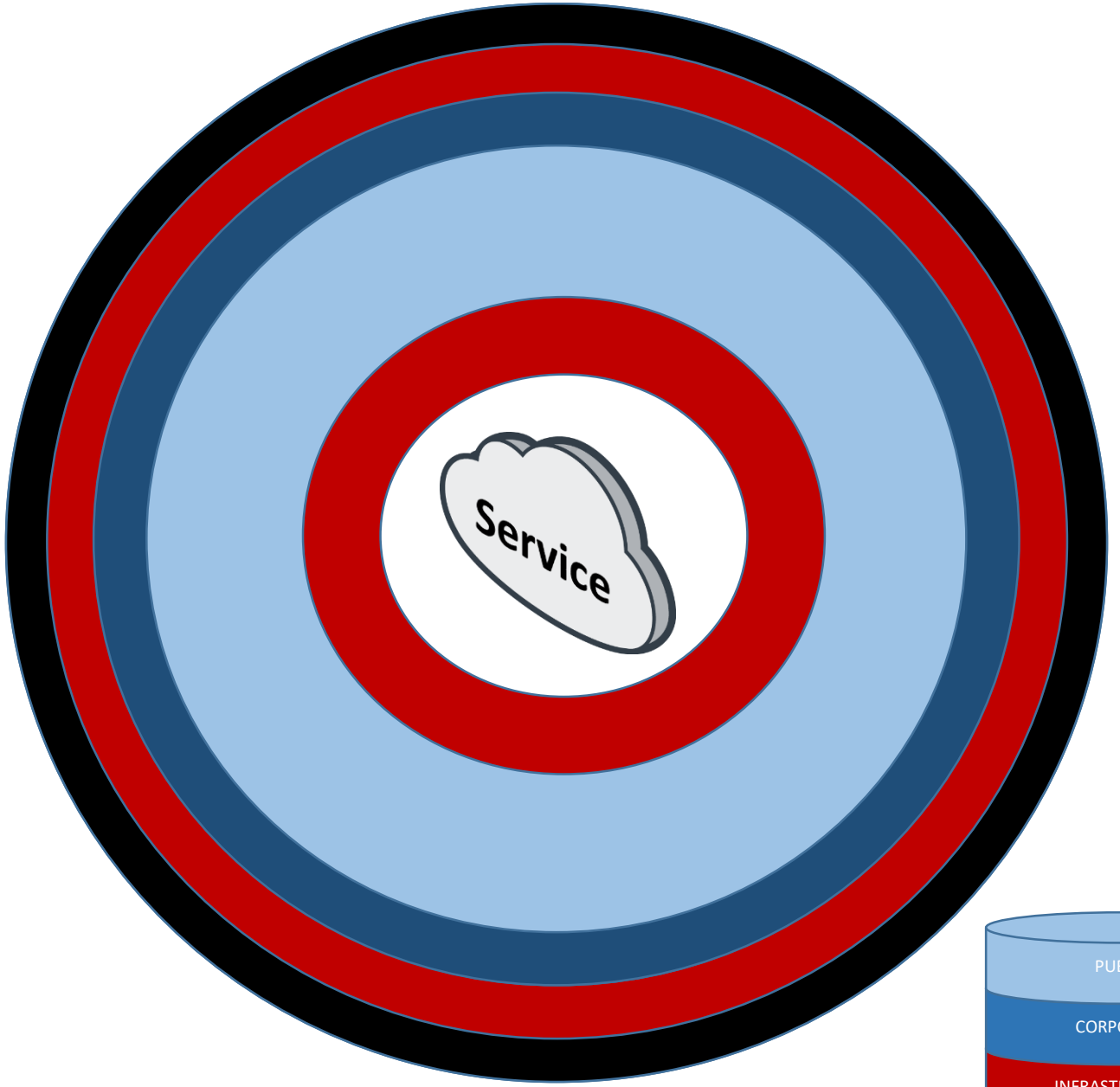
FortiADC

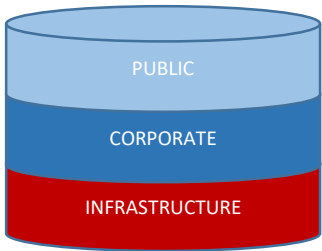
FortiGate

FortiClient

FortiAnalyzer

FortiManager





FORTINET

Belintech UA

FortiDDoS

FortiGate

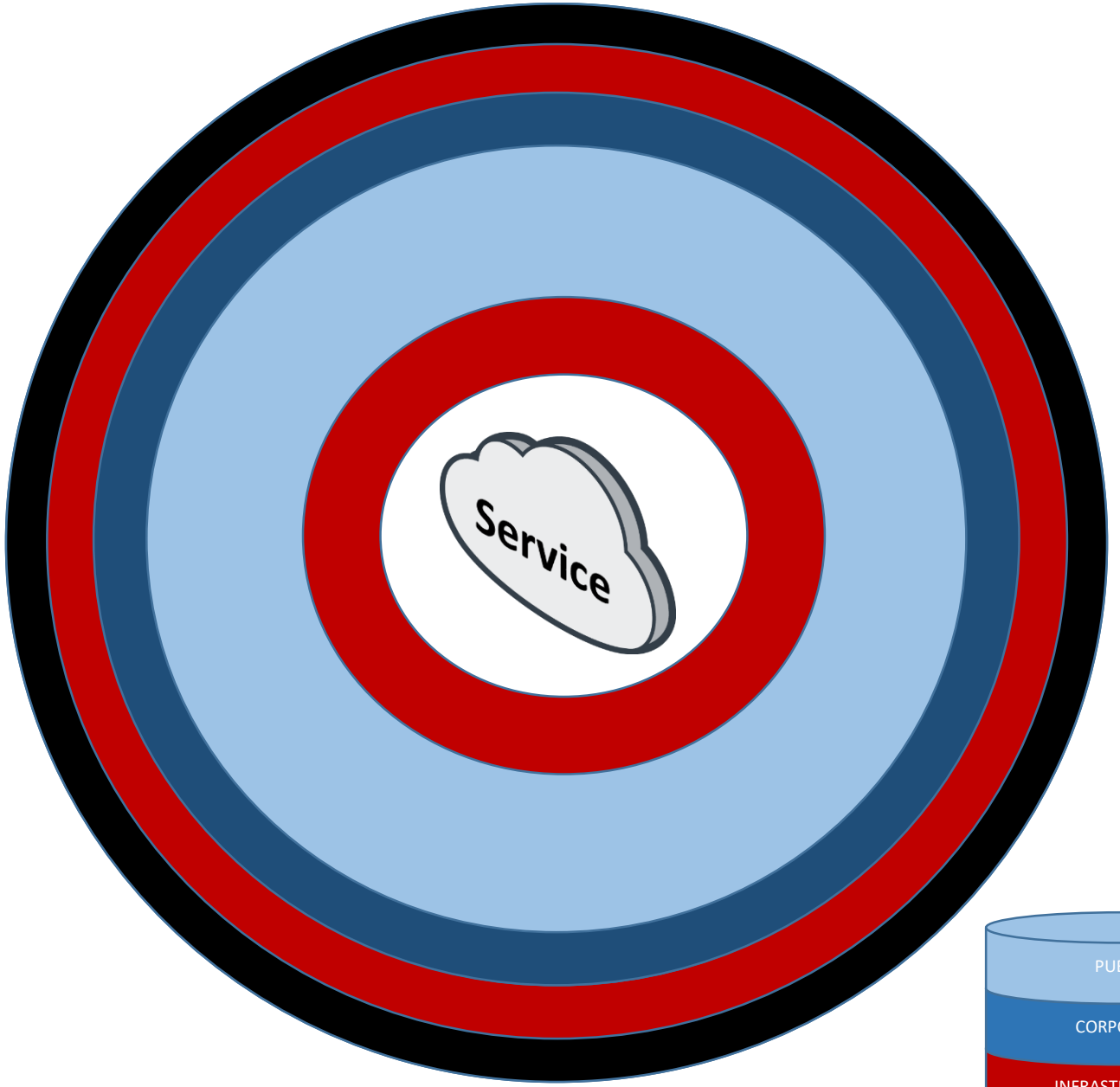
FortiADC

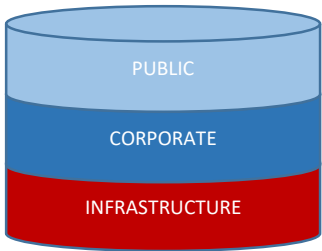
FortiGate

FortiClient

FortiAnalyzer

FortiManager





FORTINET

PUBLIC & CORPORATE

Belintech UA

FortiDDoS

FortiGate

FortiADC

FortiWeb

FortiMail

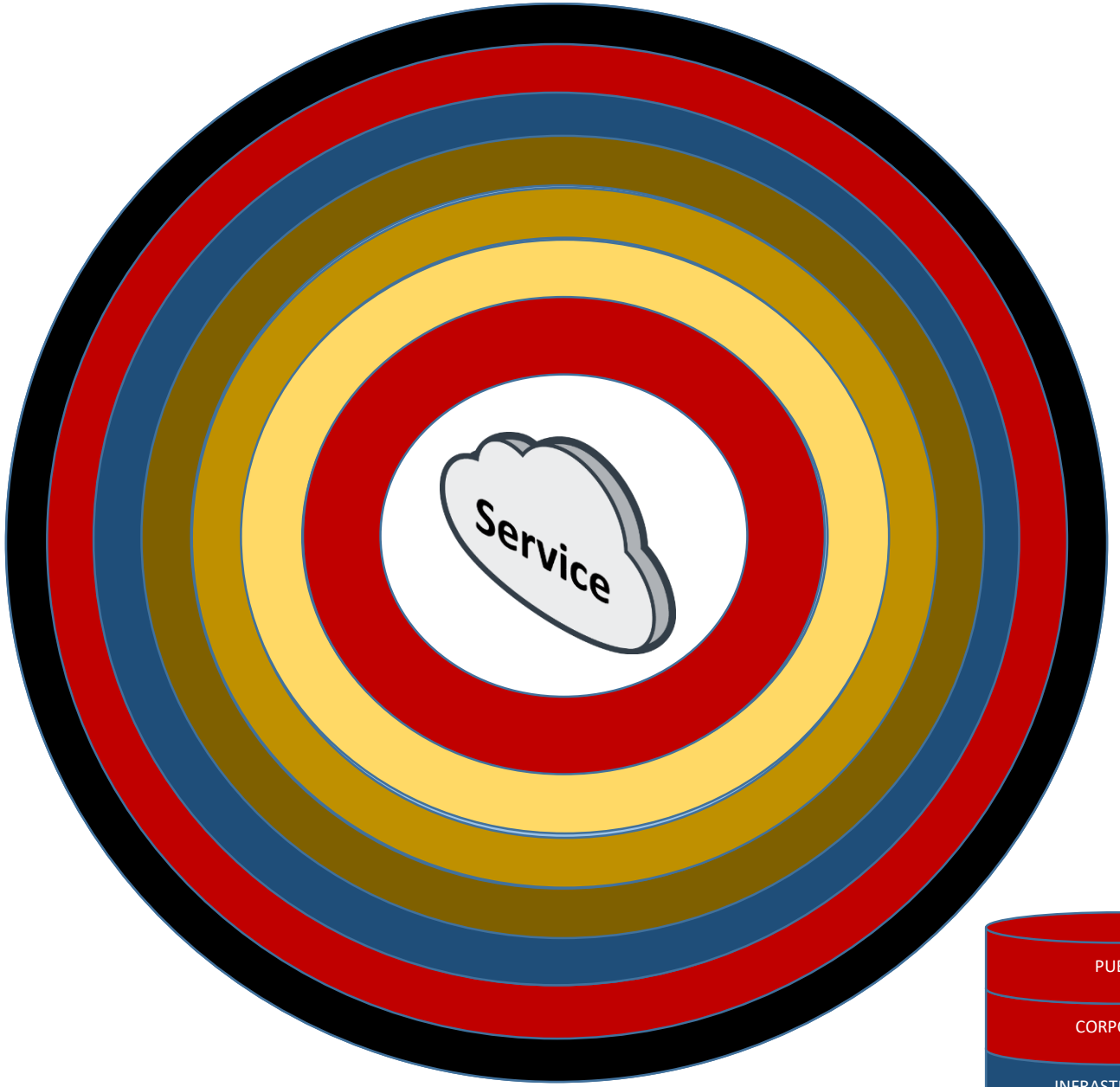
FortiSandbox

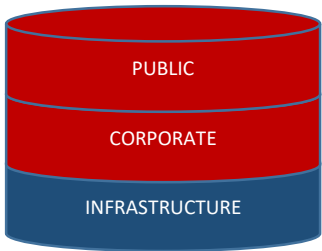
FortiGate

FortiClient

FortiAnalyzer

FortiManager





FORTINET

PUBLIC & CORPORATE

Belintech UA

FortiDDoS

FortiGate

FortiADC

FortiWeb

FortiMail

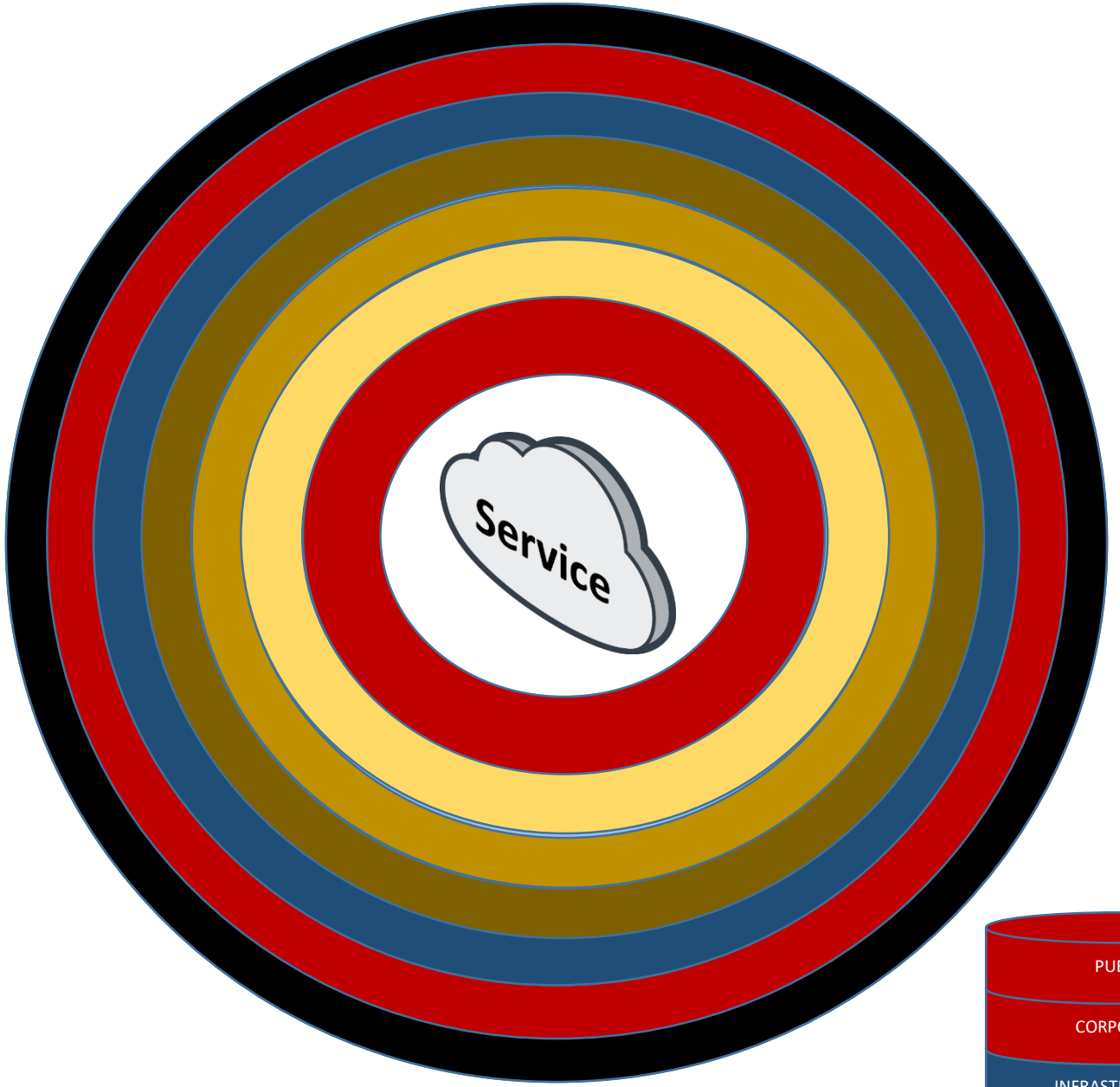
FortiSandbox

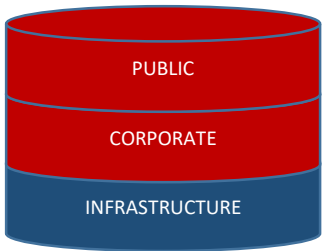
FortiGate

FortiClient

FortiAnalyzer

FortiManager





FORTINET

Belintech UA

FortiDDoS 1200B

IP Reputation

Packet Inspection

DNS Attack Mitigation

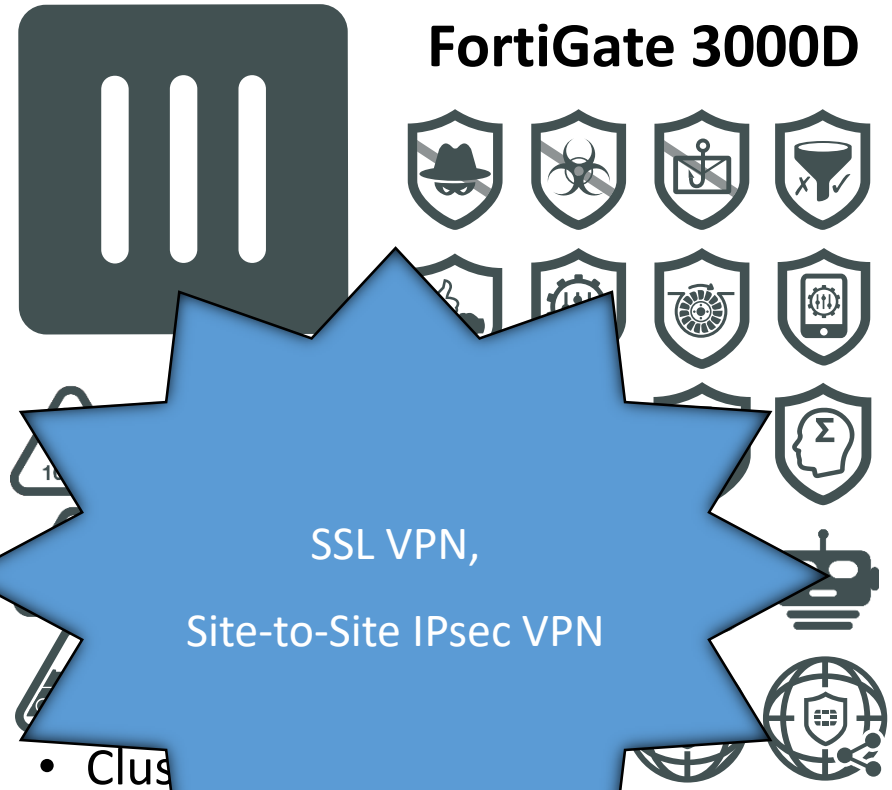
- ction
- tection
- Con
- Advanced D rotection
- Automated Learning Process
- Hybrid On-premise/Cloud Support

Thr t Ent rise
– 48 Mpps
<50 µs / <10 µs
Response Time <2 s
– 12M
SFP GE,
E/ SFP GE,
- n bypass 2 LAN and 2 WAN

FORTINET

Belintech UA

FortiGate 3000D



SSL VPN,

Site-to-Site IPsec VPN

Fortinet Single Sign-On (FSSO)

Web Filtering,

Application Control,

Antivirus,

Intrusion Prevention and

Denial of Service

Firewall

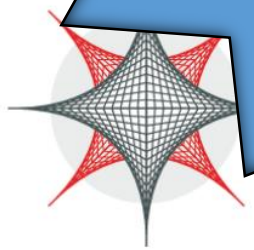
– 23 Gbps

– 22 Gbps

13 Gbps

5

- Clus
- Next Genera n Firewall
- Segmentation
- IPS
- Mobile Security for 4G, 5G, IOT



FORTINET

Belintech UA

FortiGate 1000D

Fortinet Single Sign-On (FSSO)

SSL VPN,
Site-to-Site IPsec VPN

Web Filtering,
Application Control,
Antivirus,
Intrusion Prevention and
Denial of Service

Firewall – 6 Gbps

– 5 Gbps

4 Gbps

and GE SFP+ slots

- Clus
- Next Genera n Firewall
- Segmentation
- IPS
- Mobile Security for 4G, 5G, IOT

FORTINET

Belintech UA

FortiADC 100F

Global Server Load Balancing

Web Filtering

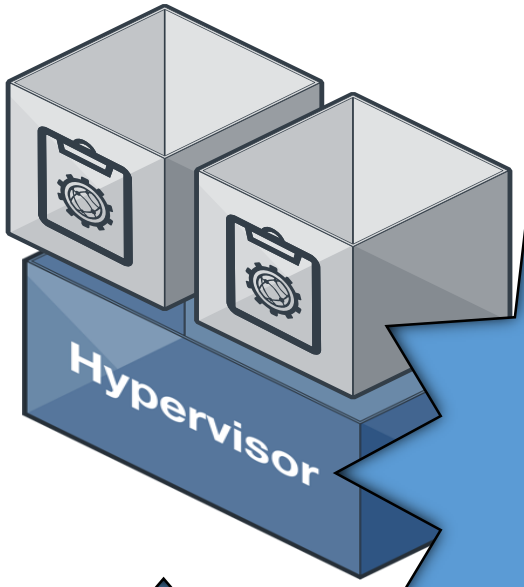
Web Application Firewall

- L4 [illegible] ough[illegible] Gbps
- [illegible] – 50 000
- [illegible] – 150 000
- Auth[illegible] [illegible]ion – 3M
- Global Server Load Balancing [illegible]3 000
- Link Load Balancing – 400 Mbps
- Health Check and Content Rewriting – 1 Gbps
- Web Application Firewall
- [illegible]RJ45

FORTINET

Belintech UA

FortiWeb-VM08



Built-in Load Balancer

OWASP Top 10,

PCI DSS 3.0

Web Application Firewall, Web Filtering

– 4

40 Gb

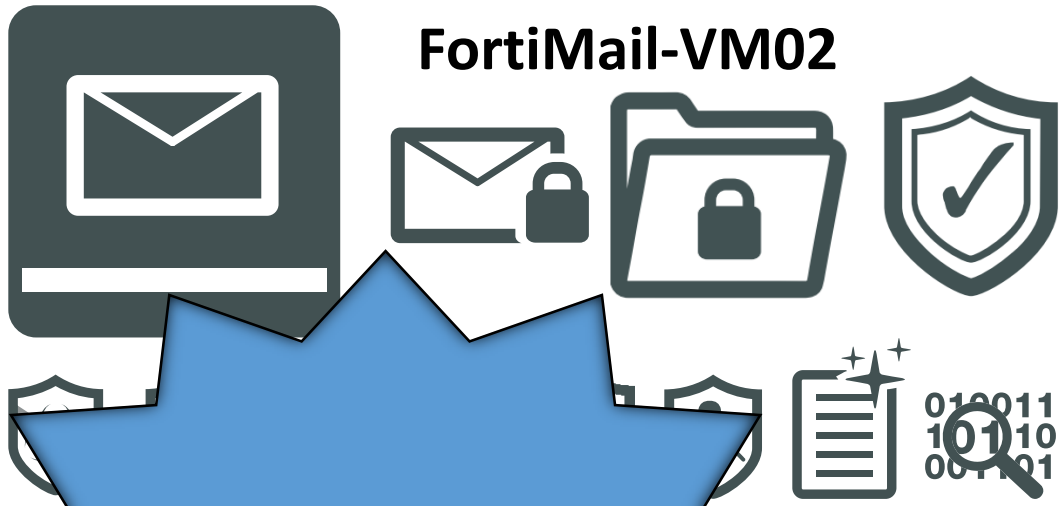
1 / 10

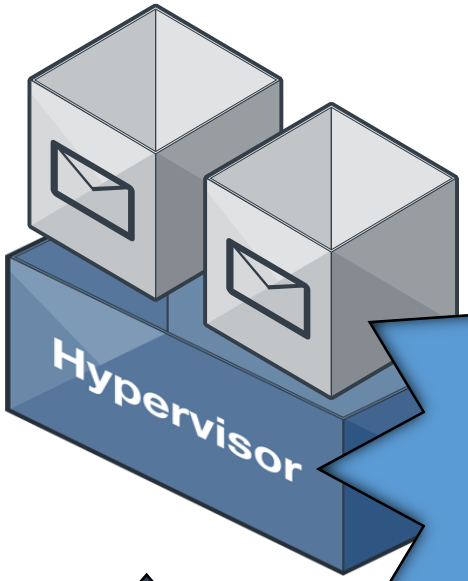
2 Gbps

erse Proxy

- App ction
- Security Serv s
- Authentication
- Management and Reporting

Belintech UA





Antivirus

Authentication Proxy

Antispam

- Inte on
- Content Disa and Neutralization
- Antispam
- Antivirus
- Recipient-based Policies

– 4

50 Gb / 2 TB

4

67 000 per hour

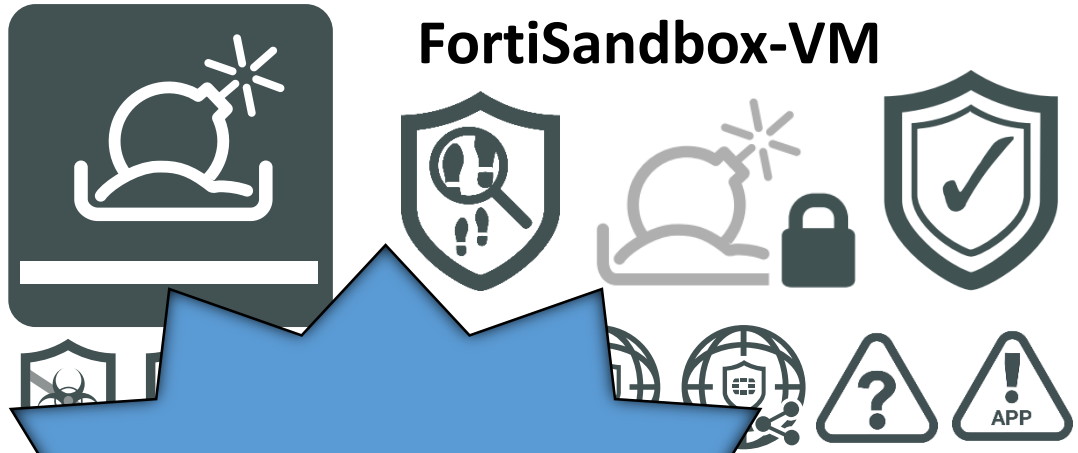
– 54 000 per hour

s – 52 000 per hour

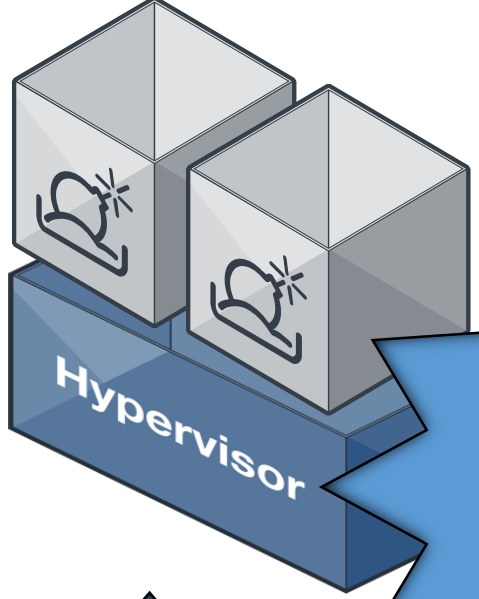
Gat ode

FORTISANDBOX

Belintech UA



FortiSandbox-VM



EDGE
(FortiGate)

Email Networks
(FortiMail)

Web Applications
(FortiWeb)

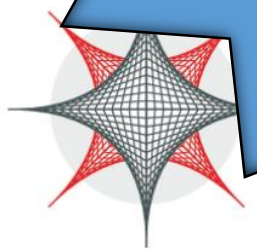
- vCP
- Malware – 48
- 30 Gb / 16 TB
- 6
- FortiADC
- FortiWeb
- FortiMail
- FortiClient (ATP Agent)
- FortiAnalyzer (Remote Logging)
- FortiManager (Update Database)

1 Gbps

8

– 140 000 per day

Dep t M – Integrated



FORTINET

Belintech UA

FortiAnalyzer 400E

- d Threat
- Gb/ Log
- – 6 000
- – 9 000
- Flexible Deploym
- 200
- Cen ized n an Reports
- – 30
- Seamless Integration with the Fortinet Security Fabric
- – 12 TB
- Automated IOC
- Real-time and Historical Views

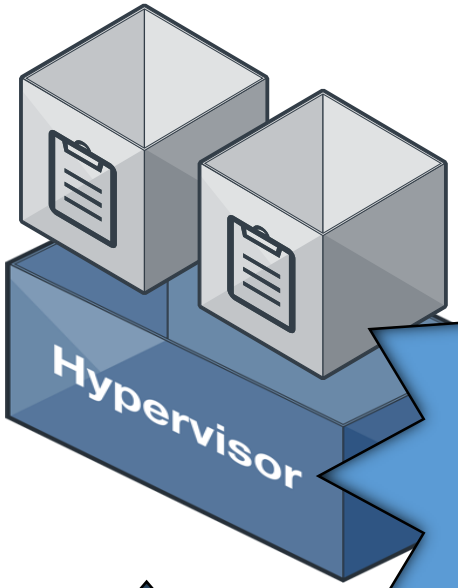
LOGS

CORRELATION

REPORTS

Belintech UA

FortiManager-VM



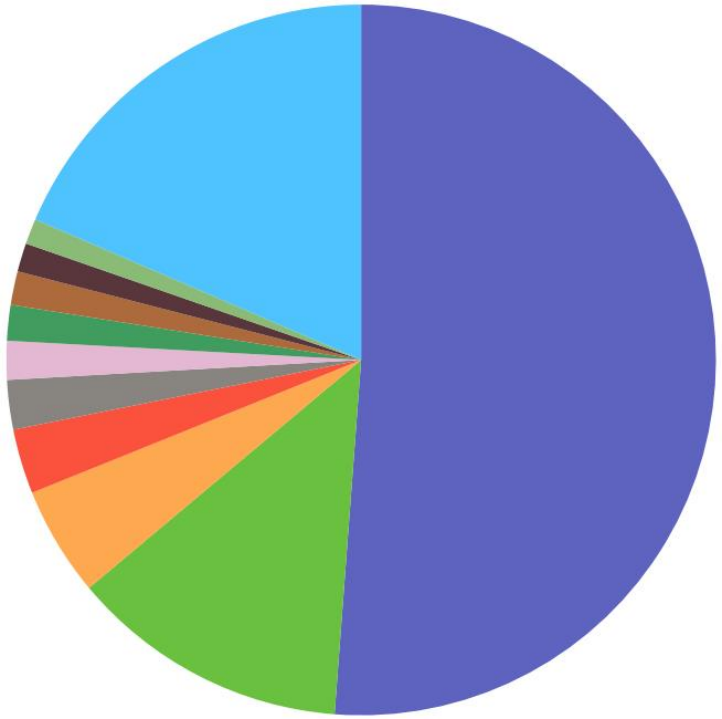
Software Upgrade

FortiGuard FQDN

Device and Policy Monitoring

- vCP
- – 4
- ts Manage
- 100 GB
- Cen grades
- 4
- Centralized S rity Updates
- 1
- Detailed Revision Tracking and Auditing
- 10
- Automation

Application Analysis



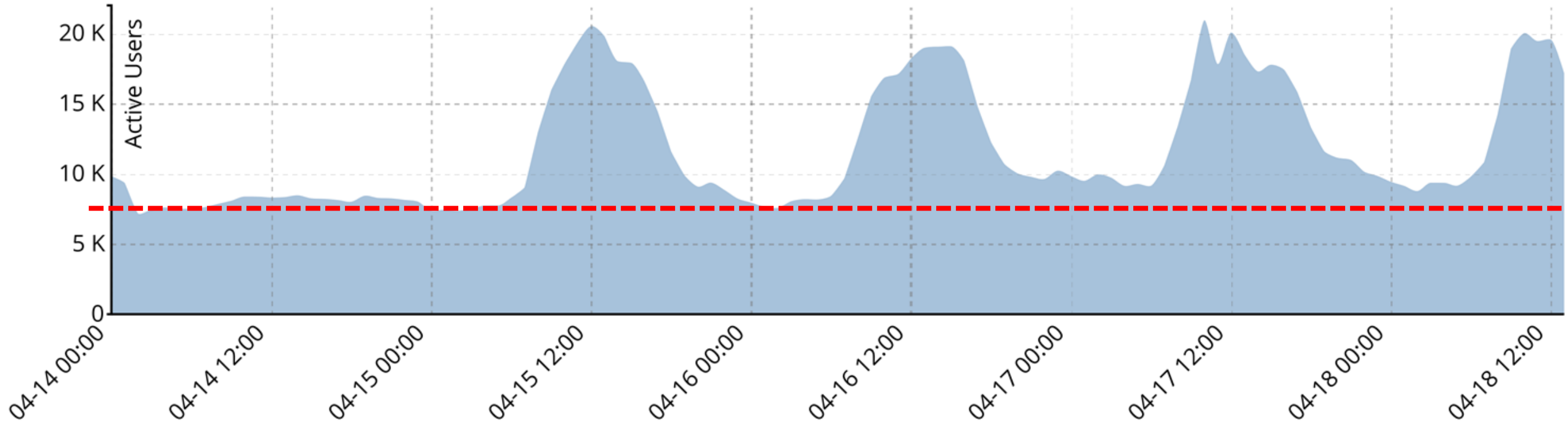
- 3,660,895 Microsoft Office/14.0 (Windows NT 6.1; Microsoft Outlook 14.0.7232; Pro)
- 909,693 Microsoft Office/15.0 (Windows NT 10.0; Microsoft Outlook 15.0.5127; Pro)
- 356,772 Microsoft Office/14.0 (Windows NT 6.2; Microsoft Outlook 14.0.7232; Pro)
- 210,956 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0
- 160,650 Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3
- 125,624 Microsoft Office/16.0 (Windows NT 10.0; Microsoft Outlook 16.0.4266; Pro)
- 115,823 Microsoft BITS/7.5
- 109,444 Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Saf
- 92,986 Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101 Firefox/66.0
- 83,079 Outlook-iOS-Android/1.0
- 1,324,688 Others

Top Virus Recipients and Senders

#	Recipient	Total Number
1	support.kyivcity@kmda.gov.ua	3
2	zvernen@kmda.gov.ua	3

#	Sender Virus	Total Number
1	cjorsi@email.cz	4
2	gpdx@mail.telepac.pt	2
3	service@vegatele.com	1

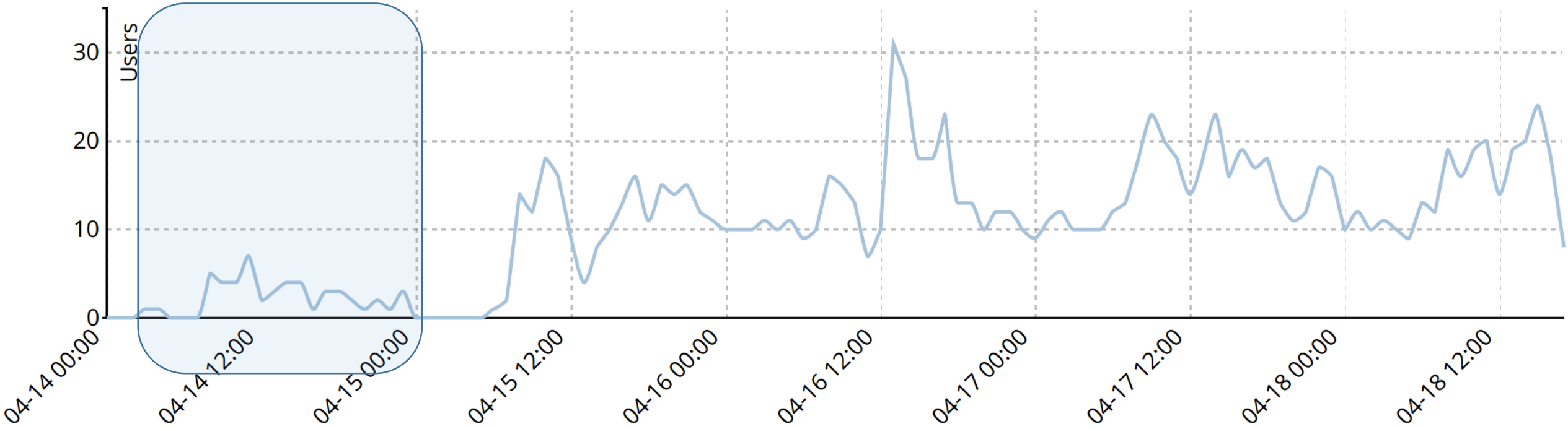
Traffic History by Number of Active Users



FORTIGATE 3000D

Belintech UA

VPN Users



FORTINET

Top 10 Blocked Web Categories

#	Category	Requests
1	Games	753,893
2	RESTRICTED_URLS	501,673
3	Gambling	59,049
4	Information and Computer Security	52,245
5	Content Servers	45,651
6	Malicious Websites	44,300
7	DEFAULT_URLS	36,817
8	Dating	15,720
9	Other Adult Materials	15,579
10	File Sharing and Storage	10,926

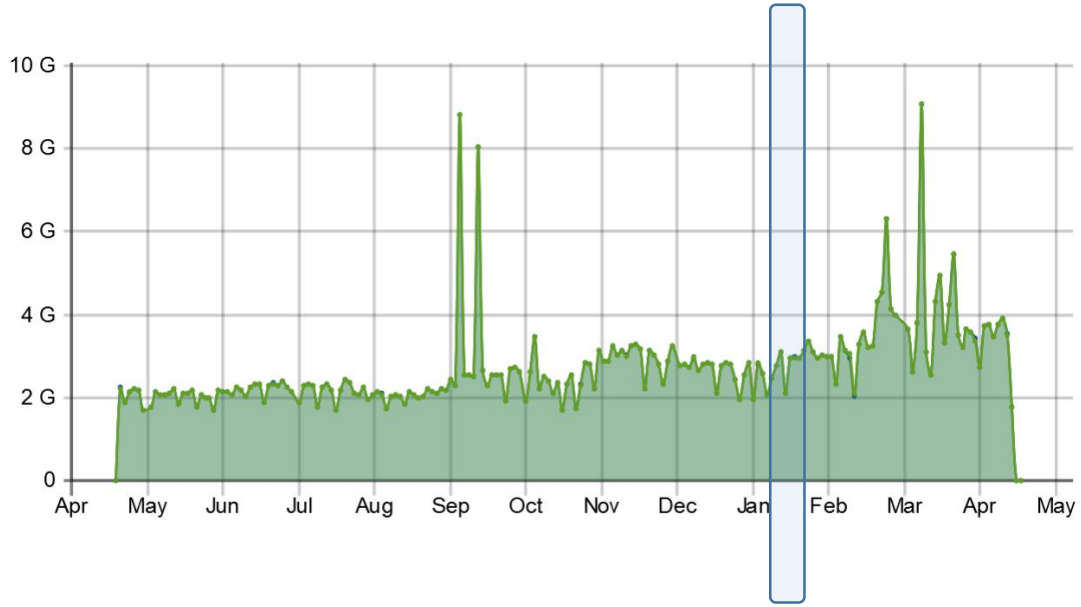
Top Users by Phishing Sites

User(or IP)	Phishing Site	Count	% of Subtotal
User(or IP)	http://pervogoaprela.ru/0942c3aad278ce5ea571a61712b4506a.php	1,247	50.02%
	http://etobylovjanvare.ru/0942c3aad278ce5ea571a61712b4506a.php	1,246	49.98%
	Subtotal	**2,493**	**6.15%**
User(or IP)	http://157.122.62.194/search?q=6737	1,103	48.98%
	http://38.102.150.27/search?q=6737	545	24.20%
	http://104.244.14.252/search?q=6737	535	23.76%
	http://46.101.128.59/search?q=6737	35	1.55%
	http://208.100.26.251/search?q=6737	34	1.51%
	Subtotal	**2,252**	**5.56%**
User(or IP)	http://ernesga.ru/i	567	38.70%
	http://z-req.ru/	567	38.70%
	https://eu.cssrvsync.com/	45	3.07%
	https://us.cssrvsync.com/	35	2.39%
	http://sdk.appsflyer.tk/op?platform=1&os_version=7.1.2&package_name=com.xrom.intl.appcenter&app_version_name=5.1.010-2018071915&app_version_code=500001010&orientation=1&image_size=1&model=M6%20Note&android_id=94471d378613683f&imei=866542035622087&mac=14169e1b8afd&mnc=06&mcc=255&network_type=-1&language=ru-RU&timezone=GMT%2B02:00&gp_version=14.3.18-all%20%5B0%5D%20%5BPR%5D%20241092342&gpsv=16.0.89%20(040408-239467275)&screen_size=1080x1920&app_id=9782-461	26	1.77%
	Others	**225**	**15.36%**
	Subtotal	**1,465**	**3.62%**
User(or IP)	http://go.onclasrv.com/apu.php?zoneid=1543391	39	4.28%
	http://adpays.net/serve/ads.js	33	3.62%
	https://uzwhi5fnd2.pshntf.com/	31	3.40%
	http://sax.peakonspot.com/dep.php?pid=8198&subid=%7Badx%7D	16	1.76%
	http://sax.peakonspot.com/dep.php?pid=8260&subid=%7Badx%7D	16	1.76%
	Others	**776**	**85.18%**

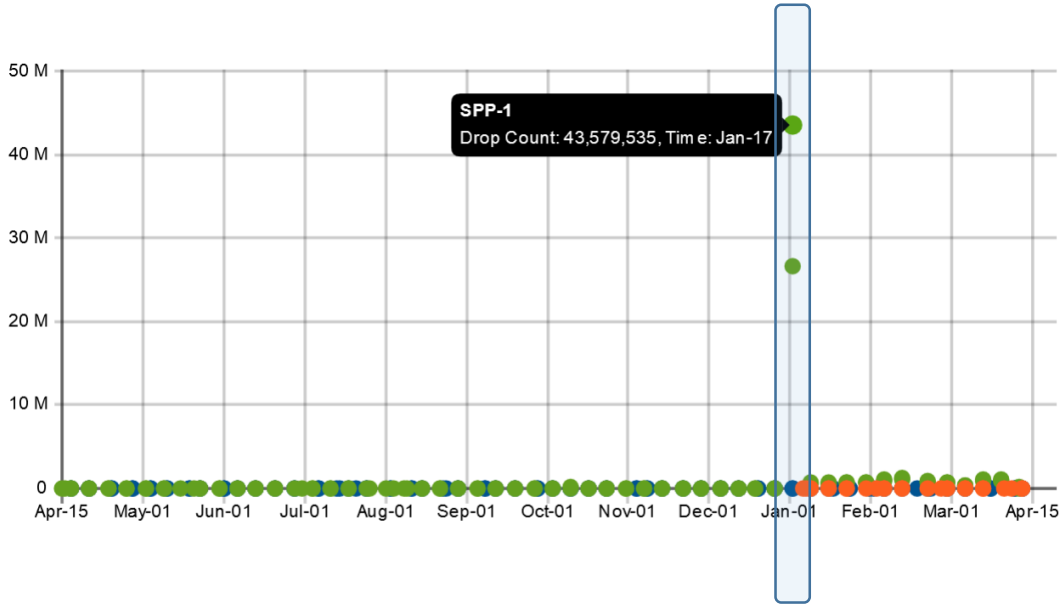
FORTIDDOS 1200B

Attack Mitigation 17-Jan-2019

Throughput (bits/sec)



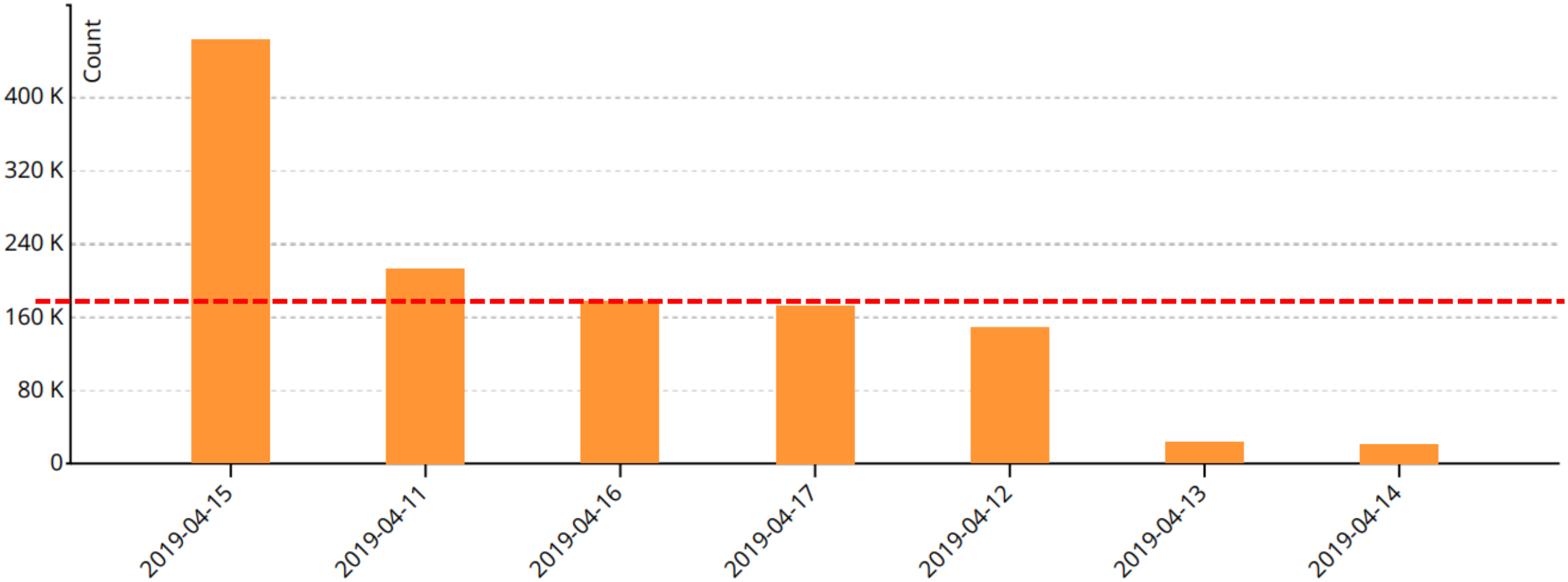
Drop Count: 43 579 535



FORTISANDBOX

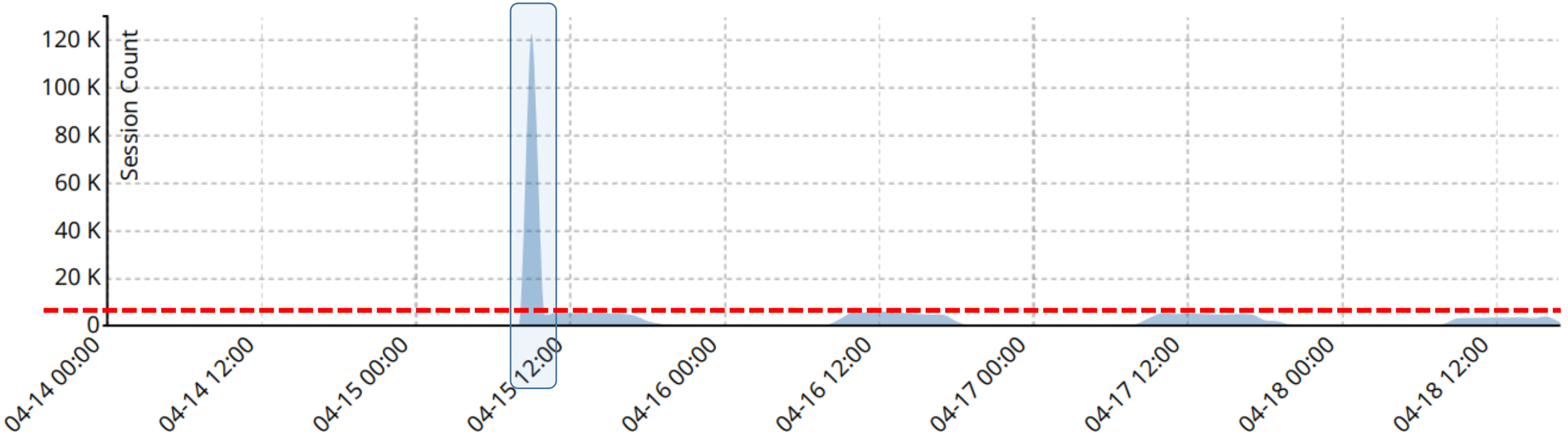
Belintech UA

Zero-day Malware Analyze



FORTINET

Proxy Avoidance

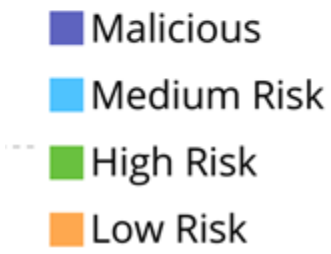


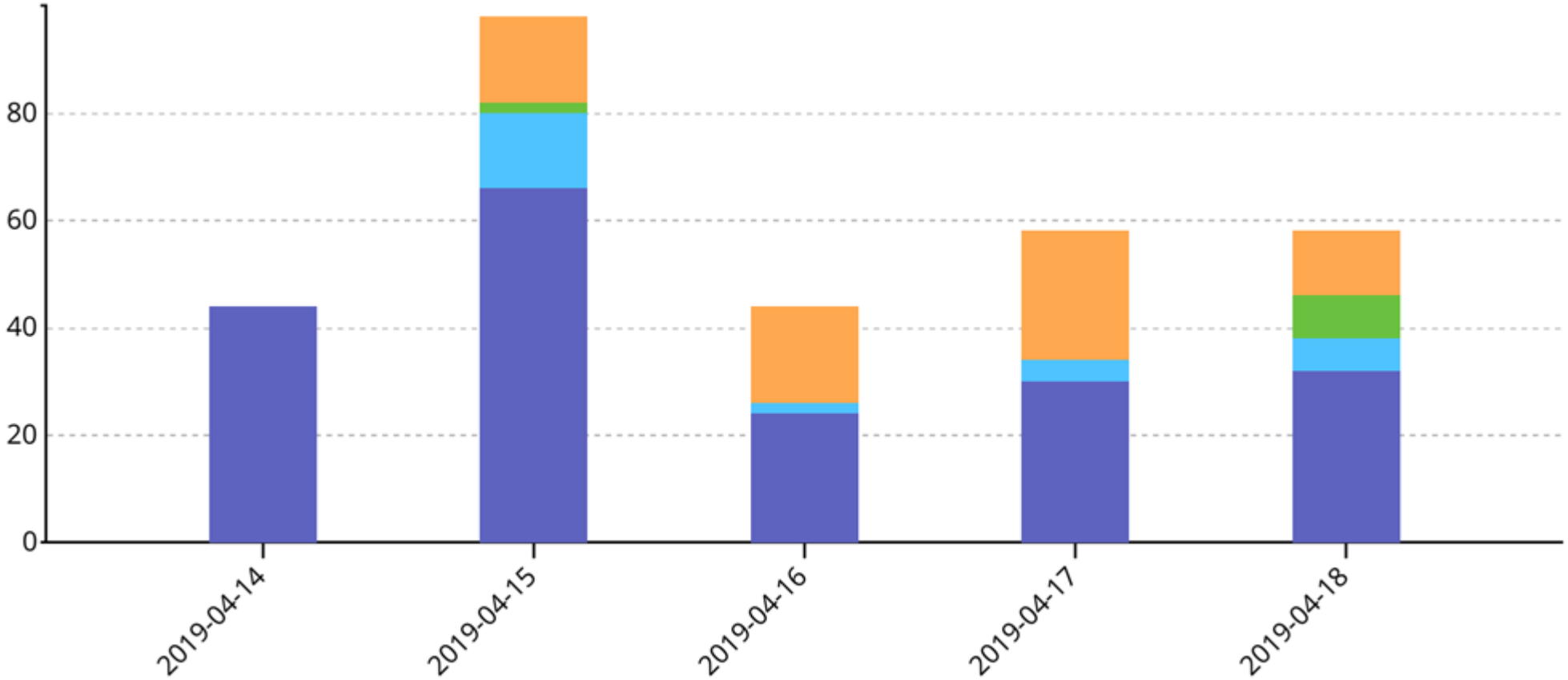
Threat Detection and Prevention

Malware Name	Malware Type	Victim	Source	Count
FSA/RISK_MALICIOUS	Virus	7	21	566
Locky	Virus	1	2	33
JS/Agent.DQGE!tr	Virus	1	1	19
JS/Agent.OAY!tr	Virus	3	8	14
AzorUlt	Virus	1	2	12
W32/Generic.AC.42BA8!tr	Virus	1	1	9
Malicious_Behavior.SB	Virus	2	4	7
W32/Install_Core	Virus	4	5	6
W32/FusionCore.AK	Virus	2	3	6
PHP/Mailfinder.AC!tr	Virus	1	2	4

Threat Rating Distribution

Malicious	196
Low Risk	70
Medium Risk	26
High Risk	10





Most At-Risk Devices and Hosts

Device	Scores
Device	2,214,087,660
Device	114,762,570
Device	63,591,355
Device	37,027,170
Device	31,717,570
Device	28,953,450
Device	16,171,090
Device	10,826,950
Device	9,406,175
Device	6,248,990

Костянтин Лєсніков

k.lyesnikov@bitech.com.ua

+38 067 235 61 66

САЙТ
bitech.com.ua

АДРЕСА
вул. Солом'янська, 3,
Київ, 01030, Україна

BELINTECH
Ukraine

ЕМЕЙЛ
office@bitech.com.ua

ТЕЛЕФОН
+38 (044) 222-82-93
+38 (044) 223-04-59