Безопасность без компромиссов

Алексей Андрияшин
+79859996477
aandriyashin@fortinet.com

Безопасность ИЗМЕНИЛАСЬ

3.2 МИЛЛИАРДА ПОЛЬЗОВАТЕЛЕЙ ИНТЕРНЕТ

1.3 МИЛЛИАРДА СМАРТФОНОВ В МИРЕ

3 МИЛЛИАРДА УСТРОЙСТВ ЕЖЕГОДНО ДО 2020

10,000x
РОСТ КИБЕР УГРОЗ

РЫНОК ОБЛАЧНЫХ УСЛУГ ДОСТИГНЕТ
$191 МИЛЛИАРДА

Ключевые факторы оценки рисков

67 %

ЖЕРТВ ПОЛУЧИЛИ УВЕДОМЛЕНИЕ О НАРУШЕНИИ ИЗ ВНЕШНЕГО ИСТОЧНИКА

50%

50% АБОНЕНТОВ НАЖИМАЮТ НА ФИШИНГОВЫЕ ССЫЛКИ В ТЕЧЕНИЕ ОДНОГО ЧАСА

70–90%

ЗЛОВРЕДНЫХ ВЛОЖЕНИЙ УНИКАЛЬНЫ ДЛЯ КАЖДОЙ ОРГАНИЗАЦИИ

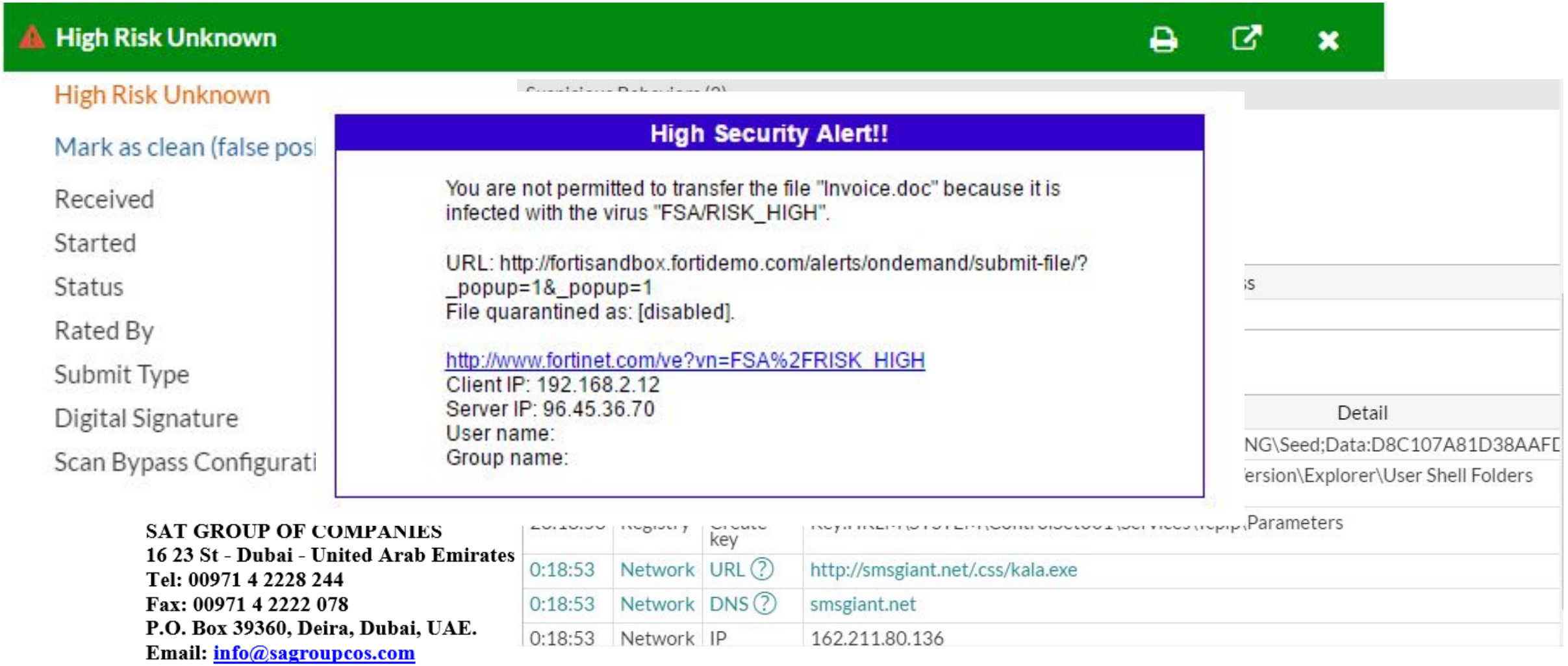
23%

АБОНЕНТОВ ОТКРЫВАЮТ ФИШИНГОВЫЕ СООБЩЕНИЯ
11% ОТКРЫВАЮТ ВЛОЖЕНИЯ

60%

В 60% СЛУЧАЕ ЗЛОУМЫШЛЕННИКИ СМОГЛИ ПРОВЕСТИ АТАКУ НА ЖЕРТВУ В ТЕЧЕНИЕ ОДНОЙ МИНУТЫ

APT в действии



SAT GROUP OF COMPANIES
16 23 St - Dubai - United Arab Emirates
Tel: 00971 4 2228 244
Fax: 00971 4 2222 078
P.O. Box 39360, Deira, Dubai, UAE.
Email: info@sagroupcos.com

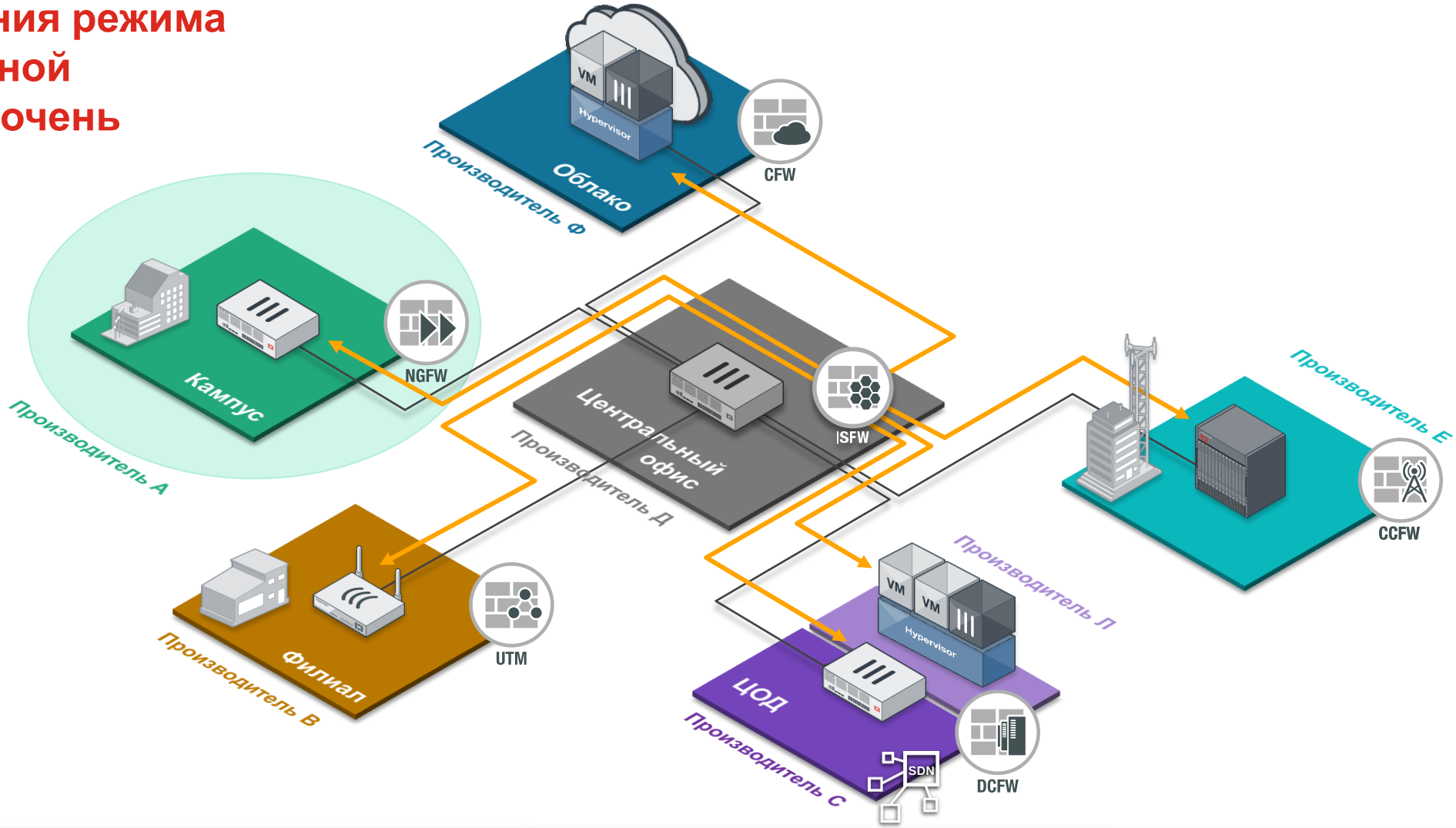
Возможностей для кибератак стало больше

Современная безопасность не имеет границ

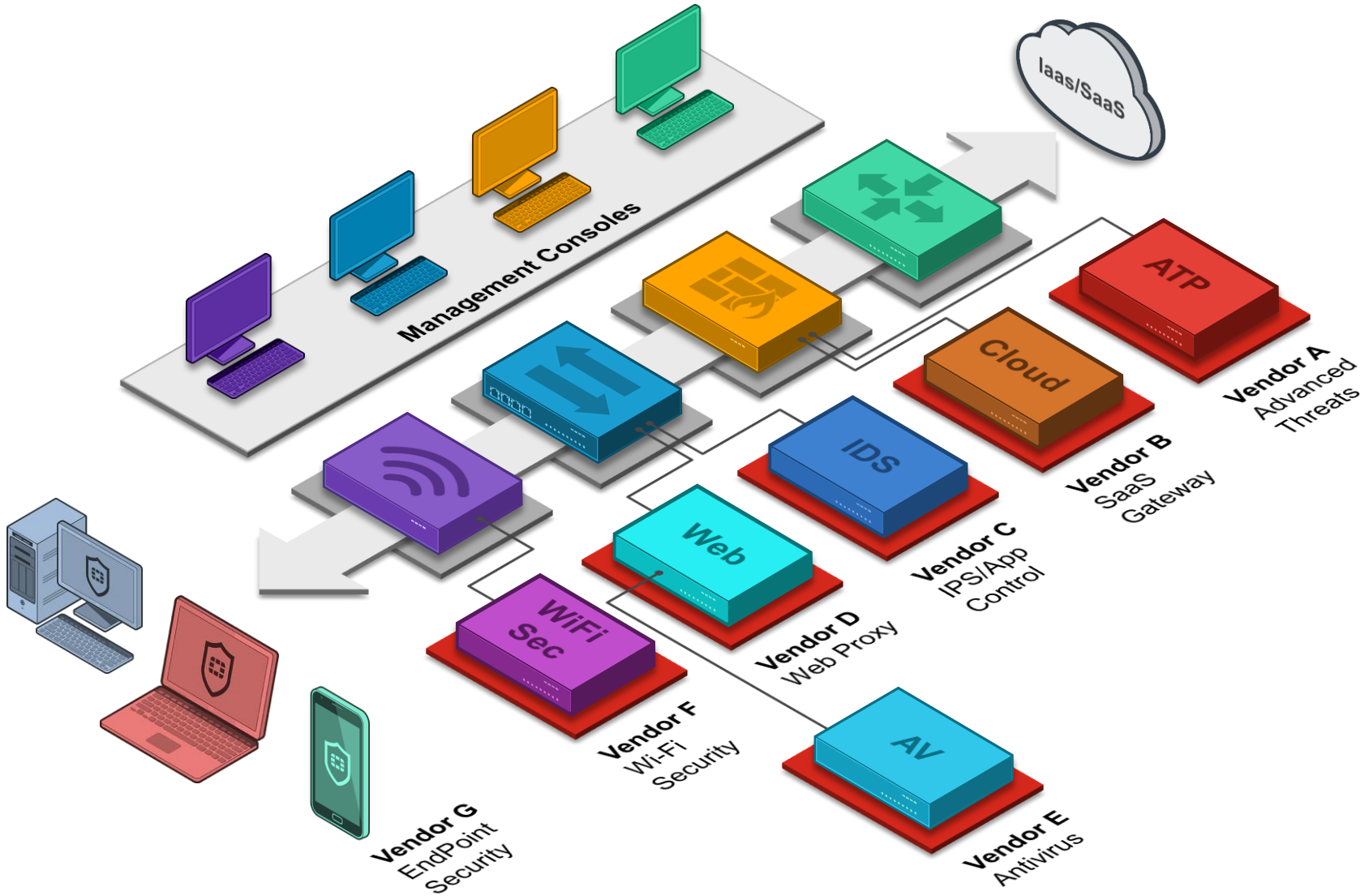
- Сети
- Приложения
- Данные
- Персонал

Разные Производители обеспечивают безопасность

Соблюдение комплекса мер обеспечения режима информационной безопасности очень критично

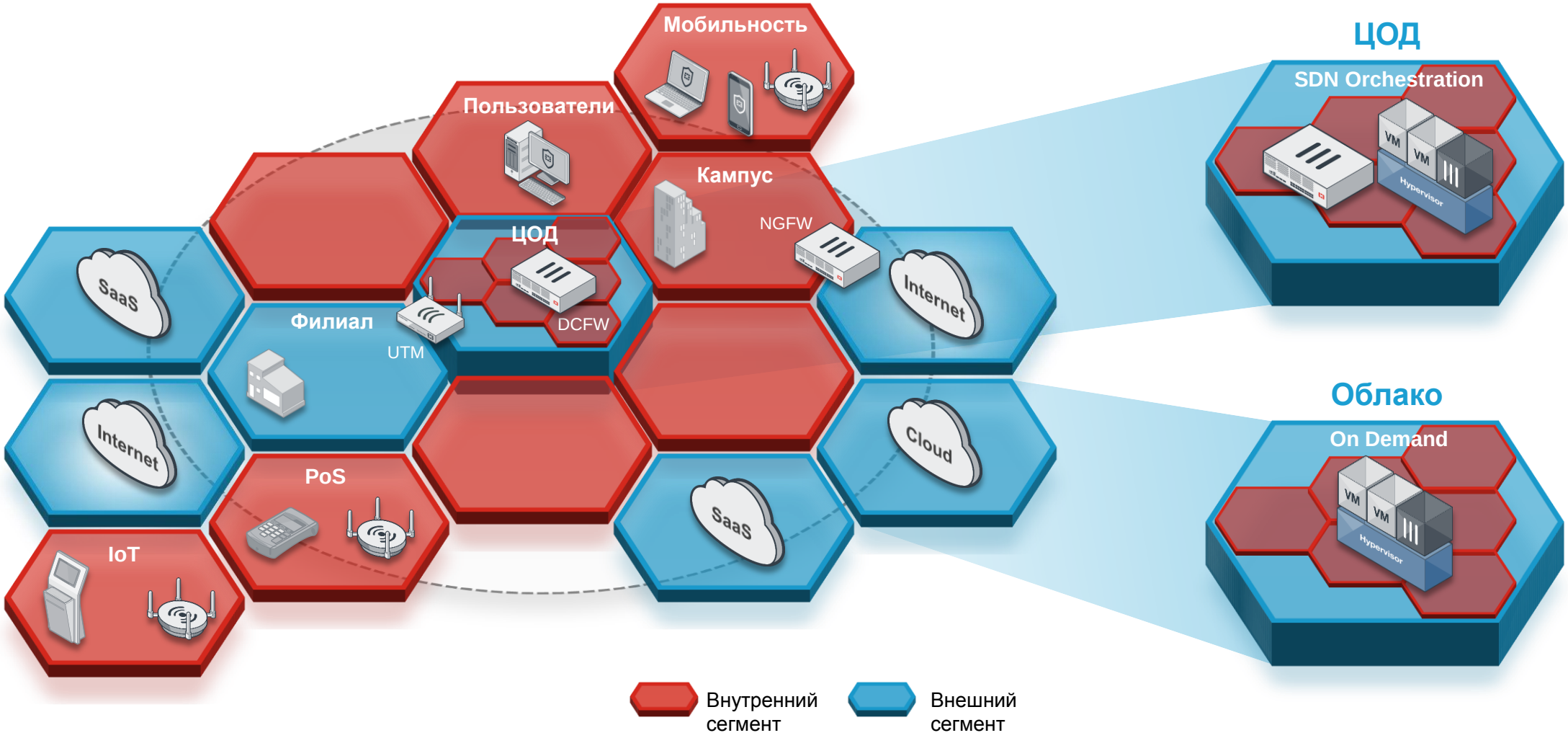


Слишком много "Точечных Решений"

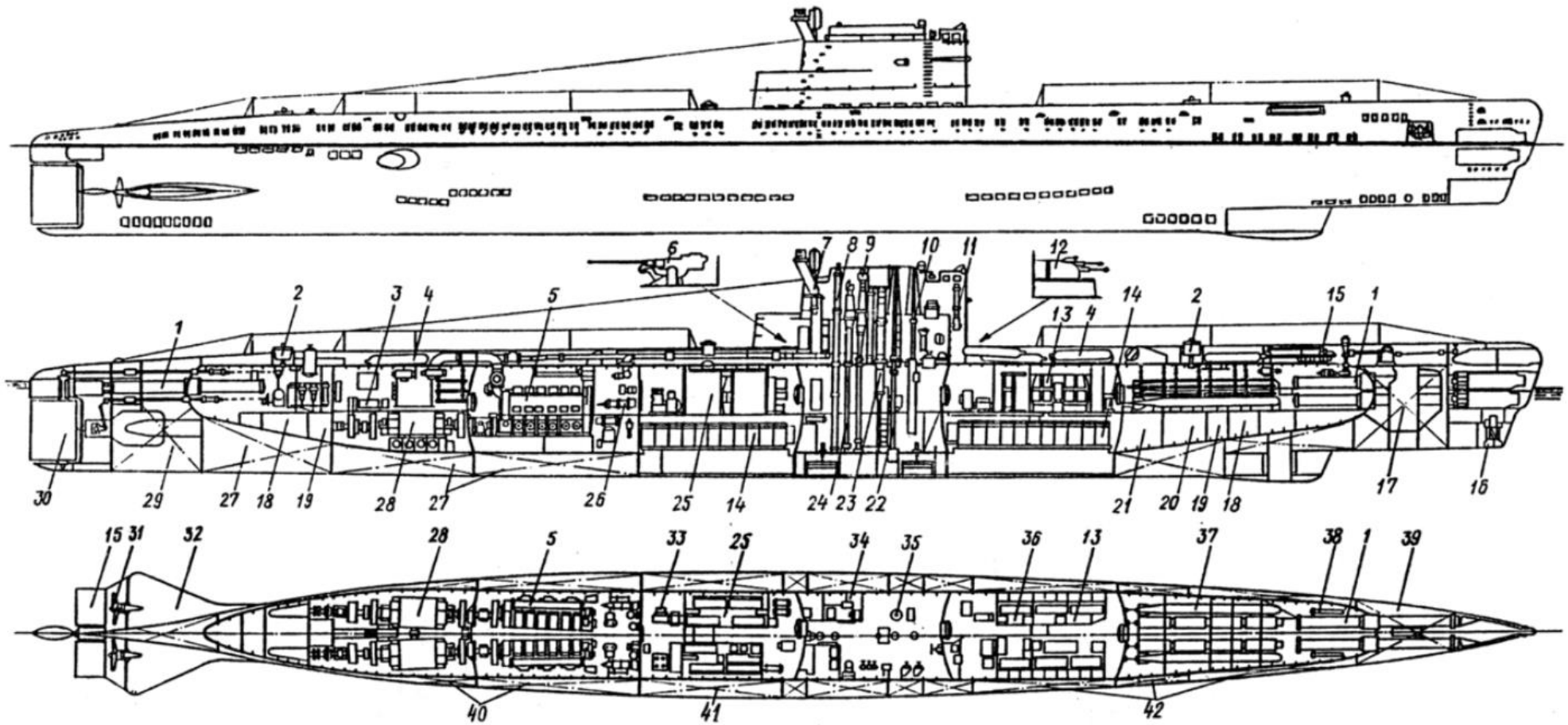


Networking	Routing
	Switching
	Wi-Fi Controller
Basic Security	Firewall
	VPN
Advanced Security	IPS/ App Control
	Web Filtering
	Antivirus
	Advanced Threat Protection
	Cloud Application Control

Концепция непрерывной сегментации или фабрики

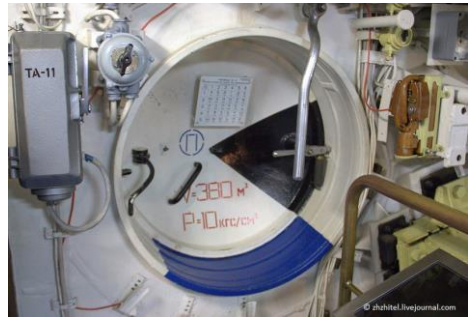


Слушать в отсеках!



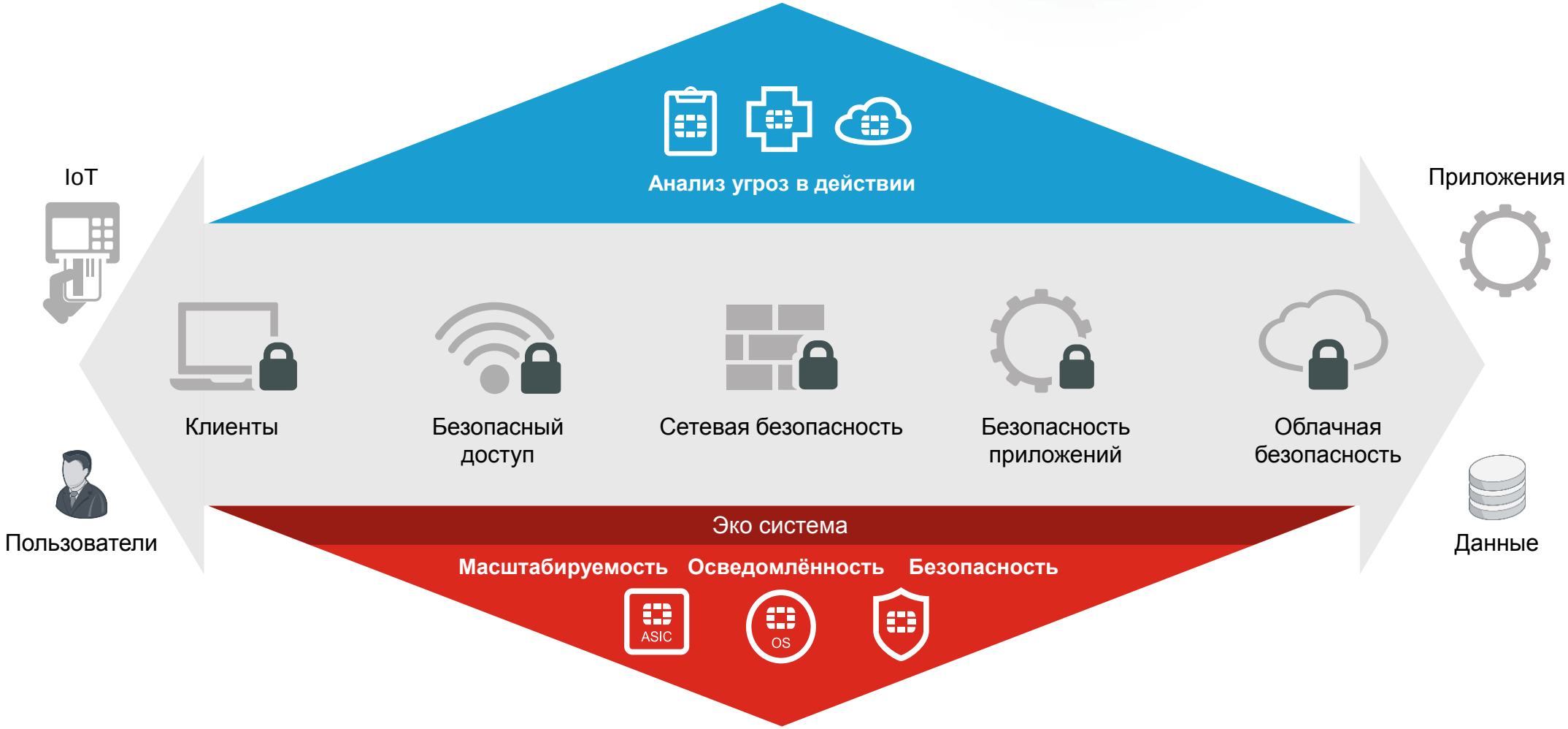
Подводная лодка проекта 613. Продольный разрез, план:

1 — торпедный аппарат; *2* — аварийный телефонный буй; *3* — электродвигатель экономического хода; *4* — баллон сжатого воздуха; *5* — дизельный двигатель 37Д; *6* — артиллерийская установка СМ-24-ЗИФ; *7* — газоотвод двигателя 37Д; *8* — антенна «ВАН»; *9* — антенна «Накат»; *10* — перископ атаки; *11* — магнитный компас ГОН-23М; *12* — артиллерийская установка 2М-8; *13* — 4-местная каюта офицеров; *14* — аккумуляторная батарея; *15* — горизонтальный руль; *16* — гидролокационная станция «Тамир-5Л»; *17* — цепной ящик; *18* — дифферентная цистерна; *19* — цистерна пресной воды; *20* — торпедозаместительная цистерна; *21* — топливная цистерна внутри прочного корпуса; *22* — зенитный перископ; *23* — неподвижная воздушная шахта РДП; *24* — антенна «Флаг»; *25* — жилое помещение старшин; *26* — дизель-компрессор ДК-2; *27* — топливная цистерна вне прочного корпуса; *28* — гребной электродвигатель ПГ-101; *29, 39, 40, 41, 42* — цистерны главного балласта; *30* — вертикальный руль; *31* — гребной винт; *32* — стабилизатор; *33* — электрокомпрессор воздуха высокого давления; *34* — рубка радиолокации; *35* — основной компас;



Fortinet “Фабрика Безопасности”

Фабрика безопасности защищает от атак на всех участках



Фабрика безопасности

Составные части фабрики:

Масштабируемость

Безопасность

Осведомлённость

Действия

Масштабируемая фабрика от IoT до Cloud

Единая панель управления

Единый источник обновлений безопасности

Единая операционная система

Устройства	Сегмент доступа	Сеть	Облака
IoT, BYOD, Endpoint	WLAN, LAN	Enterprise Edge, AppSec, Segmentation; WAN, Data Center & SDN, ATP	On Demand; IPsec, Hybrid Cloud, Public Cloud
		UTM, NGFW, ISFW, FW, DCFW, CCFW	VFW, CFW

Сетевая безопасность для всех сегментов

Единая панель управления

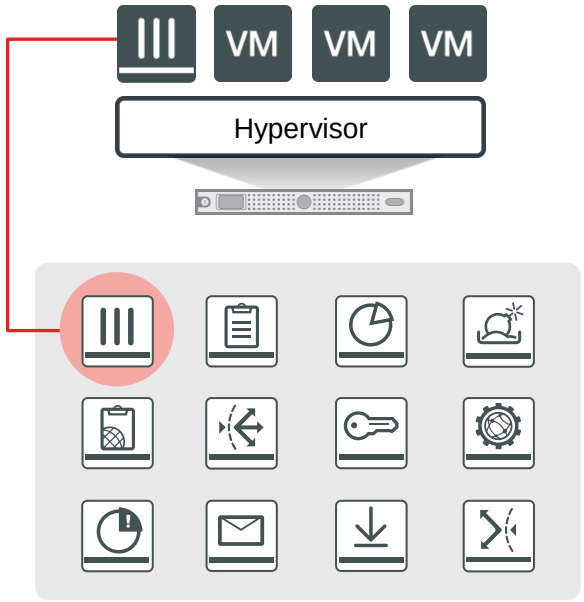
Единый источник обновлений безопасности

Единая операционная система

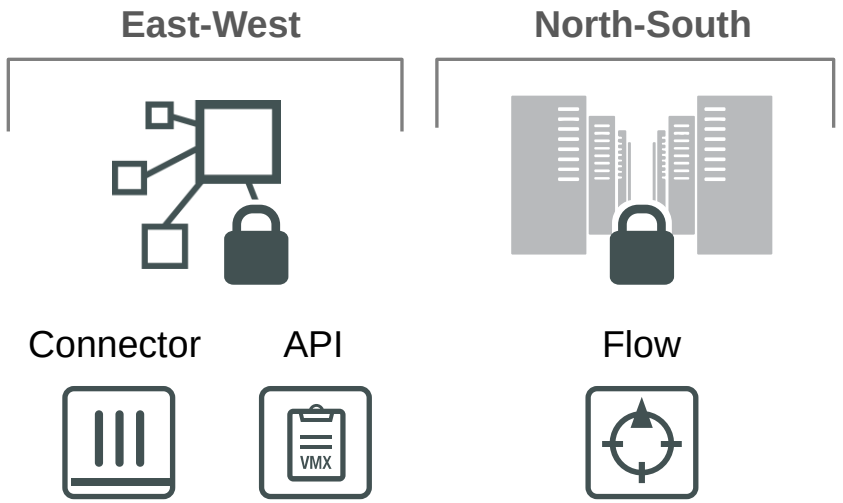
Устройства	Сегмент доступа	Сеть				Облако	
Endpoint	WLAN / LAN Rugged	Distributed Enterprise	Edge Segmentation Branch	Data Center North-South	Carrier	Private Cloud	IaaS/SaaS
	Device >1G	Appliance >5G	Appliance >30G	Appliance >300G	Chassis >Terabit	Virtual Machine SDN/NFV	Virtual Machine On Demand
Client	Embedded	System on a Chips	Content Processor ASIC	Packet Processor ASIC		Hardware Dependent	

Безопасность для Облаков и Центров Обработки данных

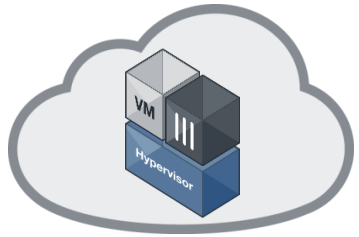
Virtualization
Hypervisor Port



Private Cloud
SDN - Orchestration Integration

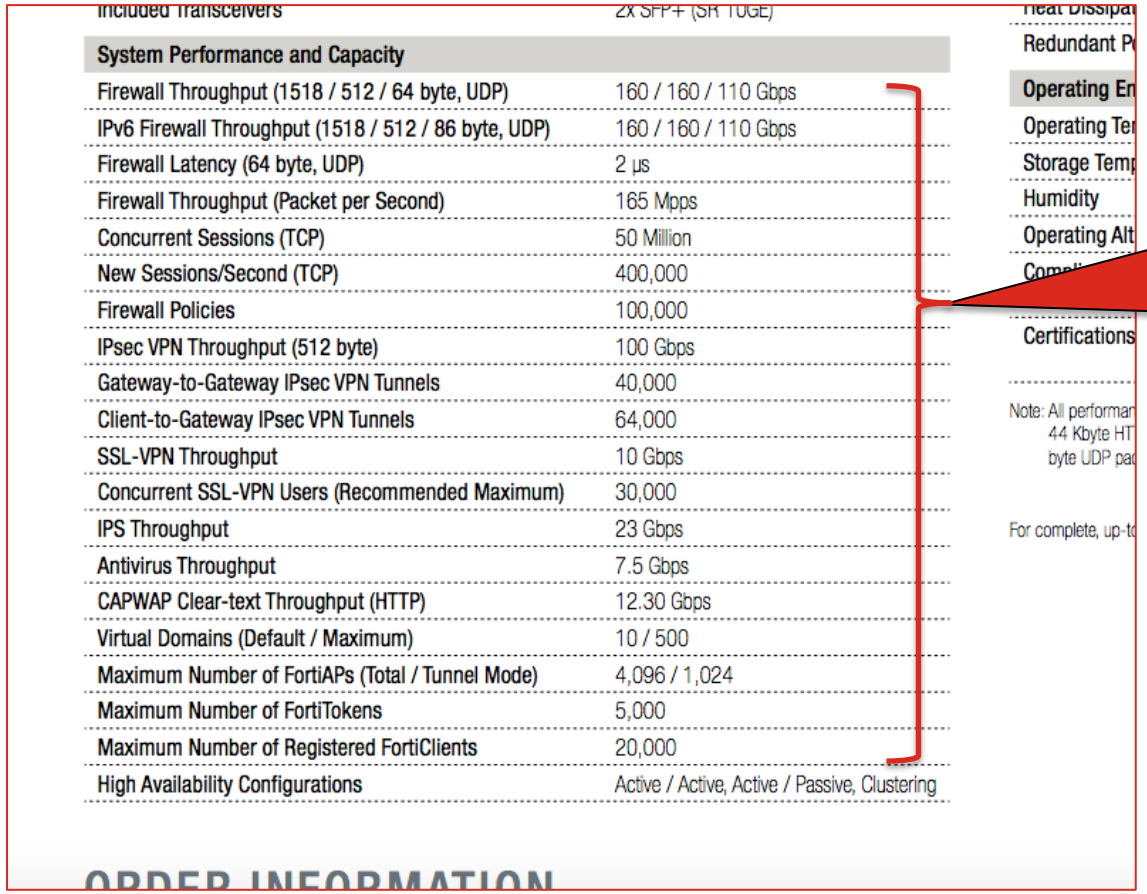


Cloud
On-Demand (Pay-as-you-Go)



Cloud

Многократный рост скорости передачи данных



Included Transceivers	2x SFP+ (SR 10GE)
System Performance and Capacity	
Firewall Throughput (1518 / 512 / 64 byte, UDP)	160 / 160 / 110 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	160 / 160 / 110 Gbps
Firewall Latency (64 byte, UDP)	2 µs
Firewall Throughput (Packet per Second)	165 Mpps
Concurrent Sessions (TCP)	50 Million
New Sessions/Second (TCP)	400,000
Firewall Policies	100,000
IPsec VPN Throughput (512 byte)	100 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	40,000
Client-to-Gateway IPsec VPN Tunnels	64,000
SSL-VPN Throughput	10 Gbps
Concurrent SSL-VPN Users (Recommended Maximum)	30,000
IPS Throughput	23 Gbps
Antivirus Throughput	7.5 Gbps
CAPWAP Clear-text Throughput (HTTP)	12.30 Gbps
Virtual Domains (Default / Maximum)	10 / 500
Maximum Number of FortiAPs (Total / Tunnel Mode)	4,096 / 1,024
Maximum Number of FortiTokens	5,000
Maximum Number of Registered FortiClients	20,000
High Availability Configurations	Active / Active, Active / Passive, Clustering

Redundant P
Operating En
Operating Te
Storage Temp
Humidity
Operating Alt
Certifications
Note: All performan
44 Kbyte HT
byte UDP pac
For complete, up-t
ORDER INFORMATION

Достаточно для 5-летнего роста?

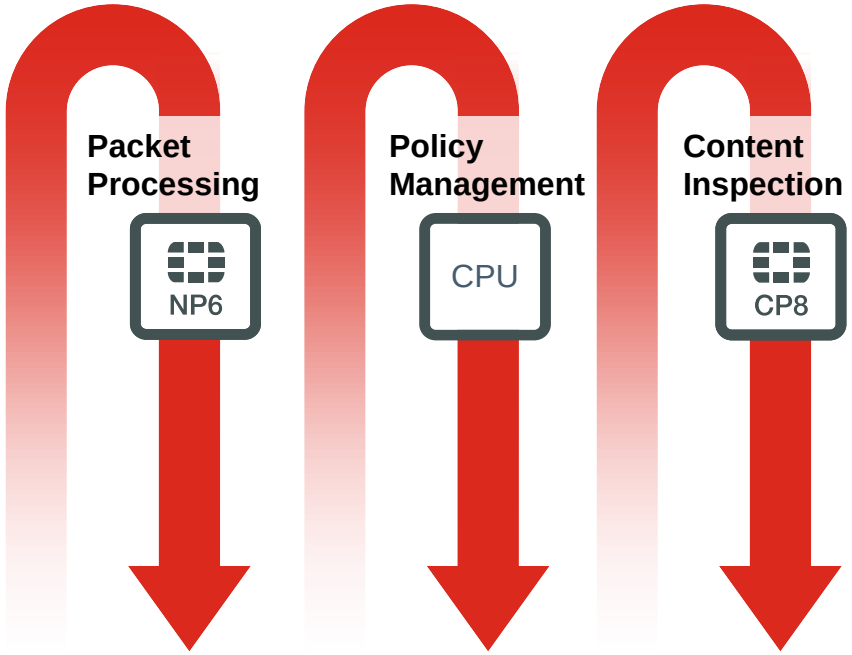
- Некоторые операторы ожидают 500%+ роста трафика в мобильных сетях в течение 5 лет
- Рост числа мобильных устройств и IoT продолжается
- Применение 4K потокового видео приведет четырехкратному увеличению загрузки
- Переход к 5G с > 1Gbps на устройство
- **Сетевые решения безопасности должны масштабироваться для соответствия производительности сетевой архитектуры**

Безопасность для современных Сетей

Медленный значит взломанный

CPU Only Традиционное решение

Parallel Path Processing (PPP) Fortinet



Использование Fortinet ASIC

- Больше производительность
- Меньше задержка
- Энергоэффективность
- Меньше места в стойках

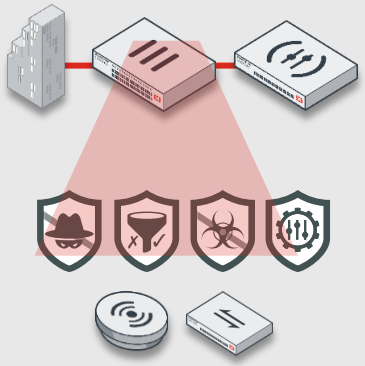
Безопасность для Сегмента Доступа

WLAN

1

Infrastructure

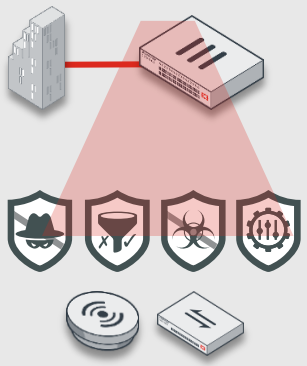
On Premise Management



2

Integrated

On Premise Management

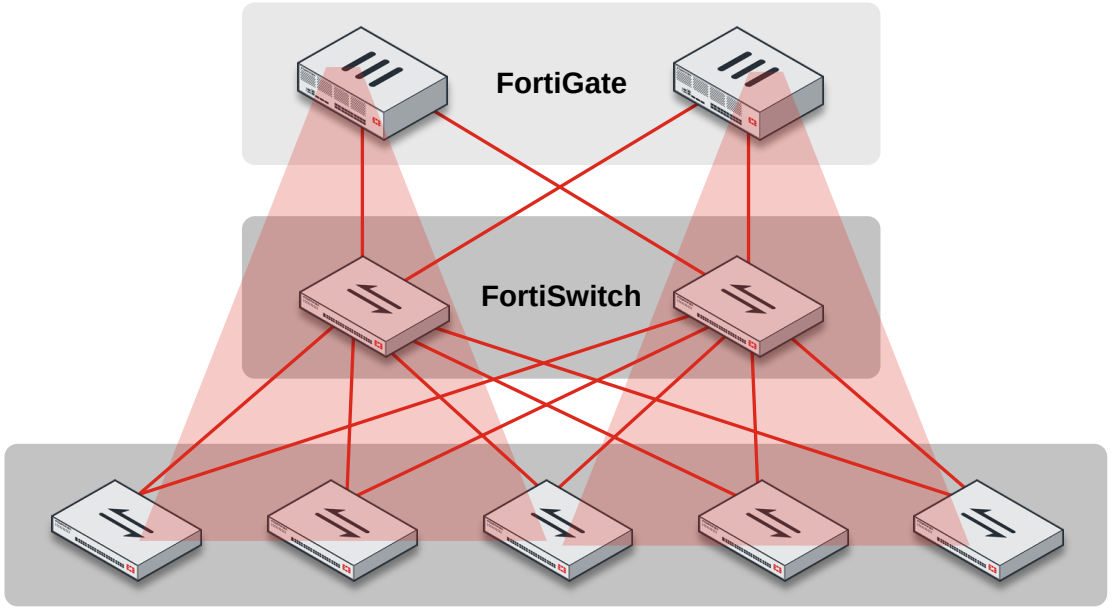


3

Cloud

Cloud Management

LAN



Фабрика безопасности

Составные части фабрики:

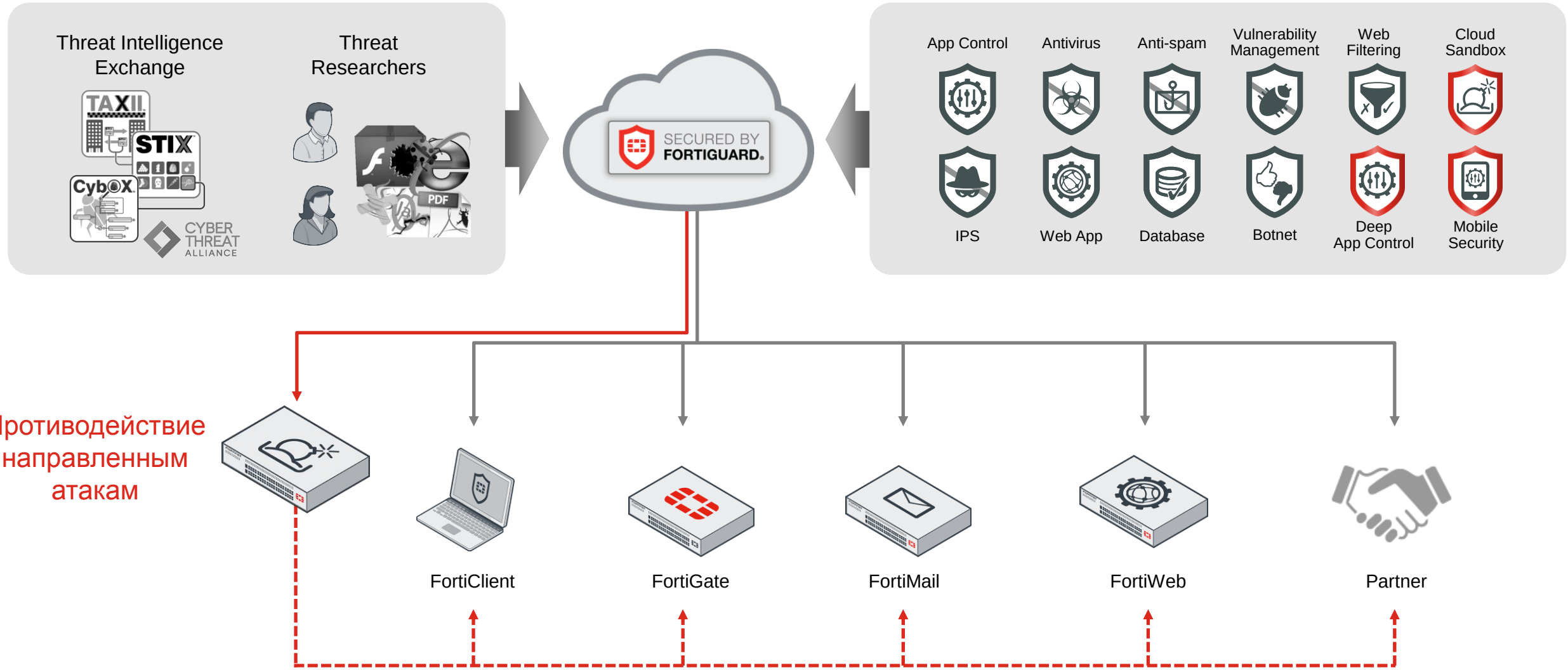
Масштабируемость

Безопасность

Осведомлённость

Действия

Глобальная и локальная Безопасность



Фабрика безопасности

Составные части фабрики:

Масштабируемость

Безопасность

Осведомлённость

Действия

Режим изучения

Сложность это враг безопасности

Идентификация пользователей

Кто подключен?

Идентификация устройств

Какие устройства подключены?

Физическая топология сети

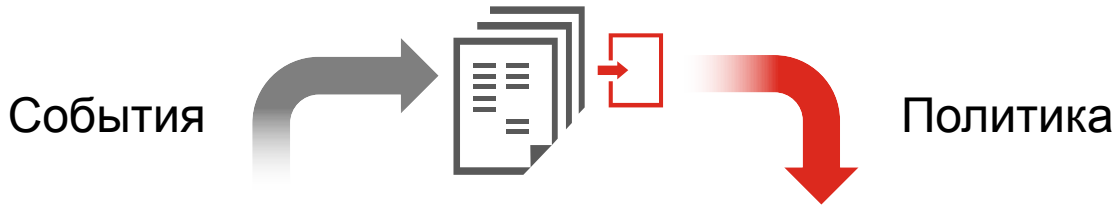
Как они подключены?

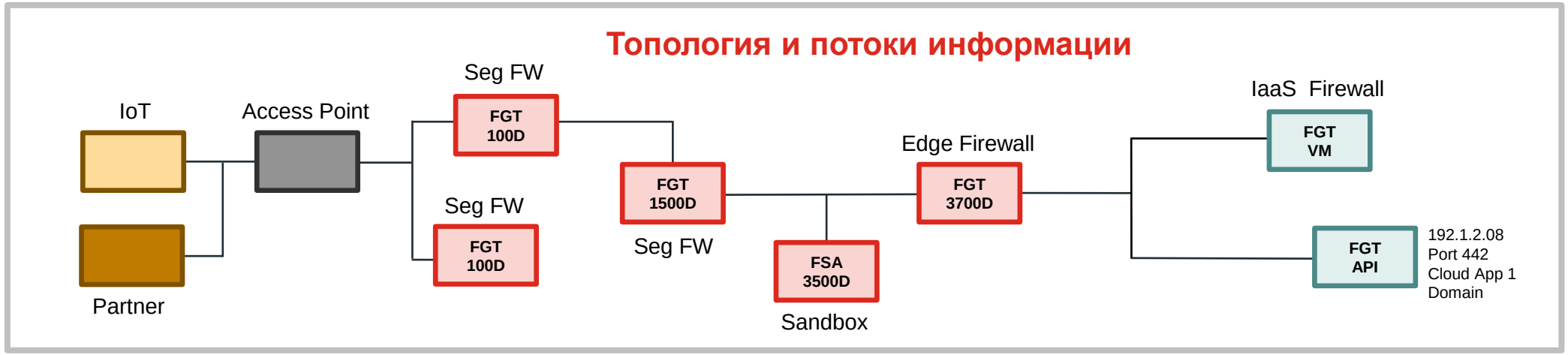
Топология приложений

Какие политики необходимы?

МОНИТОРИНГ И ИЗУЧЕНИЕ

Осведомлённость Фабрики Безопасности





Фабрика безопасности

Составные части фабрики:

Масштабируемость

Безопасность

Осведомлённость

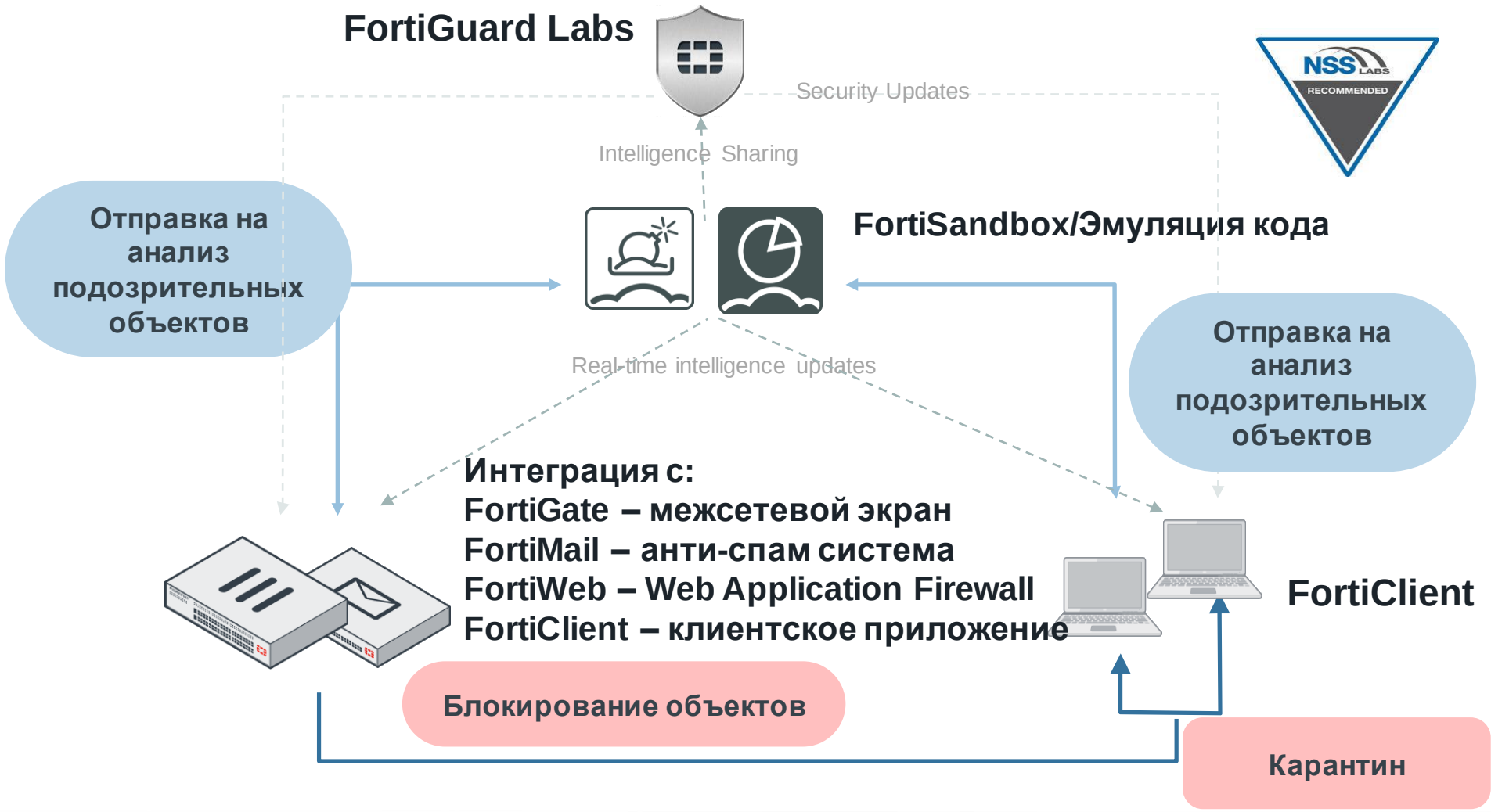
Действия

Анализ Угроз в действии

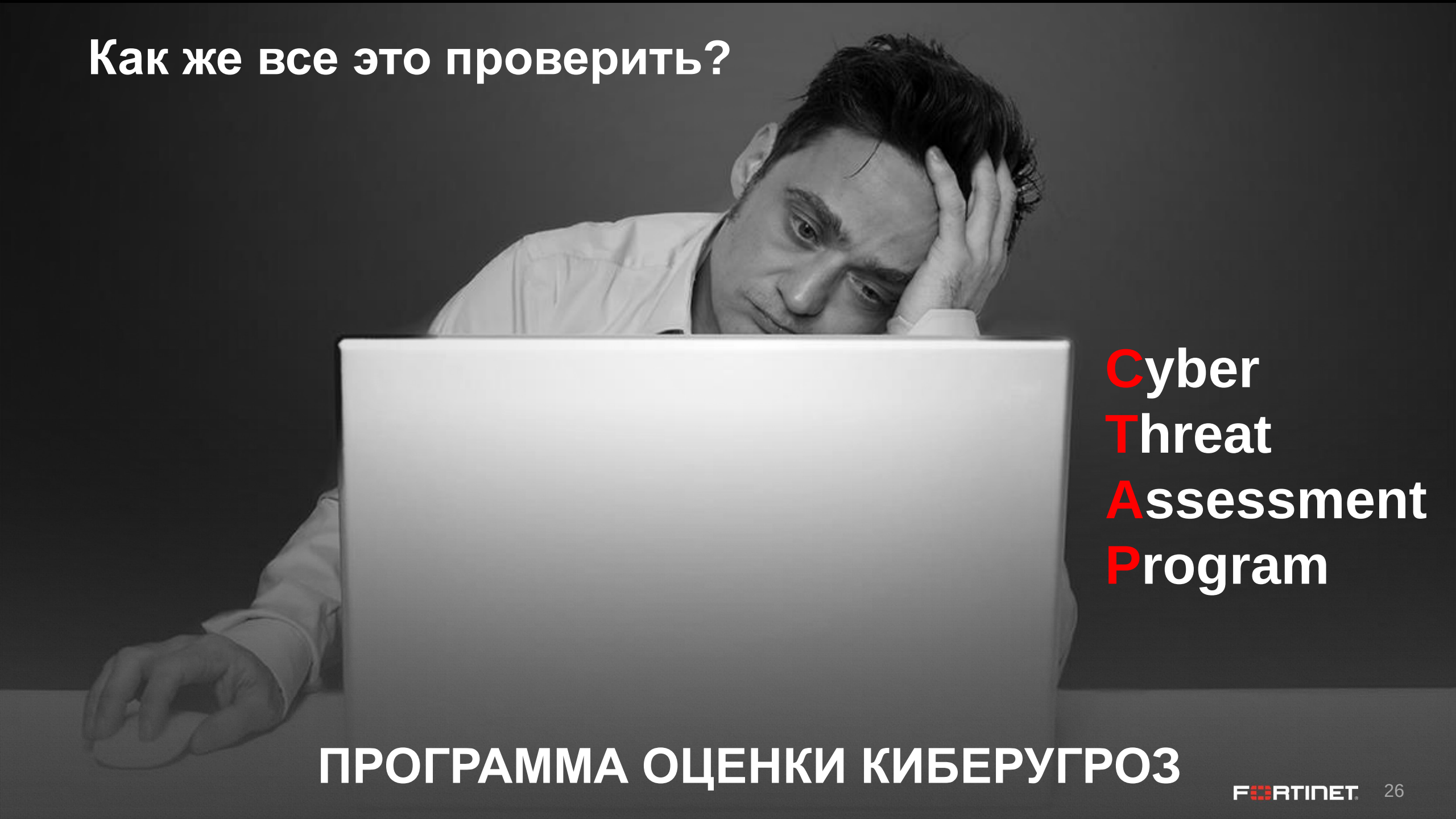
Реагирование на угрозы	Единое управление	Миграция в облака		
FortiCare	**FortiManager**	**FortiCloud**	**FortiGuard+**	**Cloud FortiSanbox**
Cloud Based Management of NGFW + Access Point	Cloud Based Management of NGFW + Access Point	Cloud Based Management of NGFW + Access Point	Threat Intelligence	Advanced Threat Protection

Безопасность без компромиссов

✓ Как противодействовать таргетированным атакам?



Как же все это проверить?



Cyber
Threat
Assessment
Program

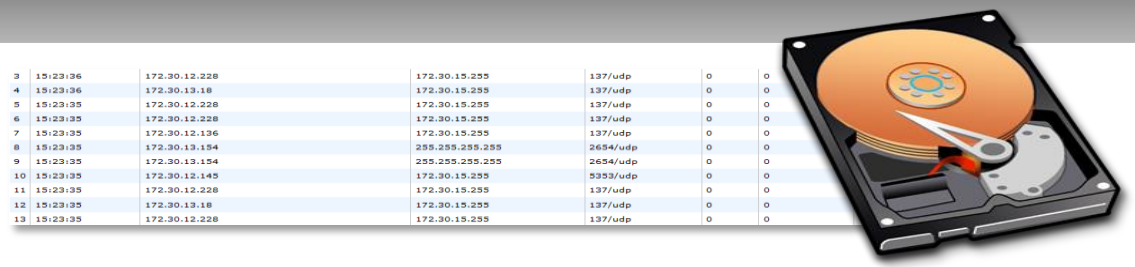
ПРОГРАММА ОЦЕНКИ КИБЕРУГРОЗ

Будем рады Вам помочь!
Программа оценки киберугроз (CTAP)

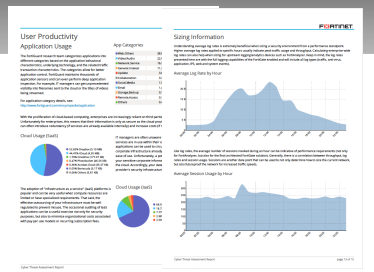
1 Свободная регистрация на fortinet.com/assessment

2 Наши эксперты внедрят FortiGate для мониторинга вашей сети

3 FortiGate соберет необходимую для оценки уровня угроз



4 Мы вместе с Вами анализируем отчет об угрозах



FortiConverter

Возможность адаптировать действующую политику ИБ

CTAP отчет (пример)

FORTINET

Executive Summary

Security and Threat Prevention

IPS Attacks Detected: 11,027
Malware/Botnets Detected: 7
High-Risk Applications Used: 13
Malicious Websites Detected: 125

Last year, over 2,100 enterprises were breached as a result of poor internal security practices and latent vendor content security. The average cost of a corporate security breach is estimated at $3.5 million USD and is rising at 15% year over year. Intrusions, malware/botnets and malicious applications collectively comprise a massive risk to your enterprise network. These attack mechanisms can give attackers access to your most sensitive files and database information. FortiGuard Labs mitigates these risks by providing award-winning content security and is consistently rated among industry leaders by objective third parties such as NSS Labs, VB 100 and AV Comparatives.

User Productivity

Applications Detected: 242
Top Used Application: Google.Search_Image
Top Application Category: Network.Service
Websites Visited: 515
Top Website: ca.archive.ubuntu.com
Top Web Category: Information Technology

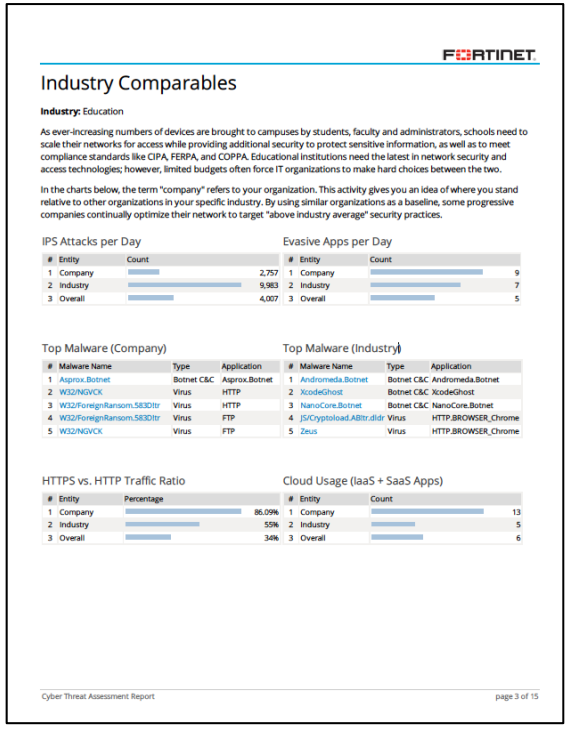
User application usage and browsing habits can not only be indicative of inefficient use of corporate resources, but can also indicate a lack of proper enforcement of corporate usage policies. Most enterprises recognize that personal use of corporate resources is acceptable. But there are many grey areas that businesses must keep a close eye on including: use of proxy avoidance/peer to peer applications, inappropriate web browsing, phishing websites, and potentially illegal activity - all of which expose your company to undue liability and potential damages. With over 5,800 application control rules and 250 million categorized websites, FortiGuard Labs provides telemetry that FortiOS uses to keep your business running effectively.

Network Utilization

Total Bandwidth: 23.94 GB
Top Host by Bandwidth: 192.168.1.119
Highest Session Host: 10.2.60.117
Average Log Rate/Sec: 10.65

Performance effectiveness is an often undervalued aspect of security devices, but firewalls must keep up with the line speeds that today's next generation switches operate at. A recent survey by Infonetics indicates that 77% of decision-makers at large organizations feel that they must upgrade their network security performance (100+ Gbps aggregate throughput) in the coming year. FortiGates leverage FortiASICs to accelerate CPU intensive functions such as packet forwarding and pattern matching. This offloading typically results in a 5-10X performance increase when measured against competitive solutions.

Cyber Threat Assessment Report page 2 of 15



FORTINET

Industry Comparables

Industry: Education

As ever-increasing numbers of devices are brought to campuses by students, faculty and administrators, schools need to scale their networks for access while providing additional security to protect sensitive information, as well as to meet compliance standards like CIPA, FERPA, and COPPA. Educational institutions need the latest in network security and access technologies; however, limited budgets often force IT organizations to make hard choices between the two.

In the charts below, the term "company" refers to your organization. This activity gives you an idea of where you stand relative to other organizations in your specific industry. By using similar organizations as a baseline, some progressive companies continually optimize their network to target "above industry average" security practices.

IPS Attacks per Day

#	Entity	Count
1	Company	2,757
2	Industry	9,983
3	Overall	4,007

Evasive Apps per Day

#	Entity	Count
1	Company	9
2	Industry	7
3	Overall	5

Top Malware (Company)

#	Malware Name	Type	Application
1	Asprox.Botnet	Botnet C&C	Asprox.Botnet
2	W32/NGVCK	Virus	HTTP
3	W32/ForeignRansom.583Dltr	Virus	HTTP
4	W32/ForeignRansom.583Dltr	Virus	FTP
5	W32/NGVCK	Virus	FTP

Top Malware (Industry)

#	Malware Name	Type	Application
1	Andromeda.Botnet	Botnet C&C	Andromeda.Botnet
2	XcodeGhost	Botnet C&C	XcodeGhost
3	NanoCore.Botnet	Botnet C&C	NanoCore.Botnet
4	JS/Cryptoload.ABltr.dldr	Virus	HTTP.BROWSER_Chrome
5	Zeus	Virus	HTTP.BROWSER_Chrome

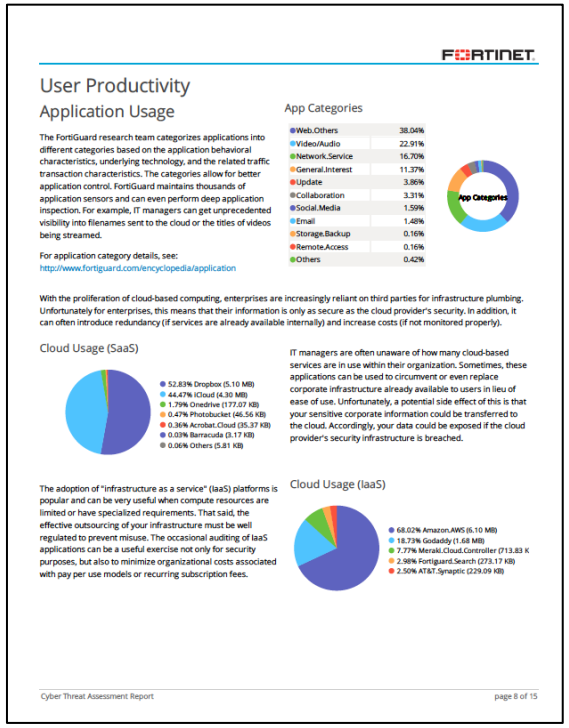
HTTPS vs. HTTP Traffic Ratio

#	Entity	Percentage
1	Company	86.09%
2	Industry	55%
3	Overall	34%

Cloud Usage (IaaS + SaaS Apps)

#	Entity	Count
1	Company	13
2	Industry	5
3	Overall	6

Cyber Threat Assessment Report page 3 of 15



FORTINET

User Productivity

Application Usage

The FortiGuard research team categorizes applications into different categories based on the application behavioral characteristics, underlying technology, and the related traffic transaction characteristics. The categories allow for better application control. FortiGuard maintains thousands of application sensors and can even perform deep application inspection. For example, IT managers can get unprecedented visibility into filenames sent to the cloud or the titles of videos being streamed.

For application category details, see:
http://www.fortiguard.com/encyclopedia/application

App Categories

Web.Others	38.04%
Video/Audio	22.91%
Network.Service	16.70%
General.Interest	11.37%
Update	3.86%
Collaboration	3.31%
Social.Media	1.59%
Email	1.48%
Storage.Backup	0.16%
Remote.Access	0.16%
Others	0.42%

With the proliferation of cloud-based computing, enterprises are increasingly reliant on third parties for infrastructure plumbing. Unfortunately for enterprises, this means that their information is only as secure as the cloud provider's security. In addition, it can often introduce redundancy (if services are already available internally) and increase costs (if not monitored properly).

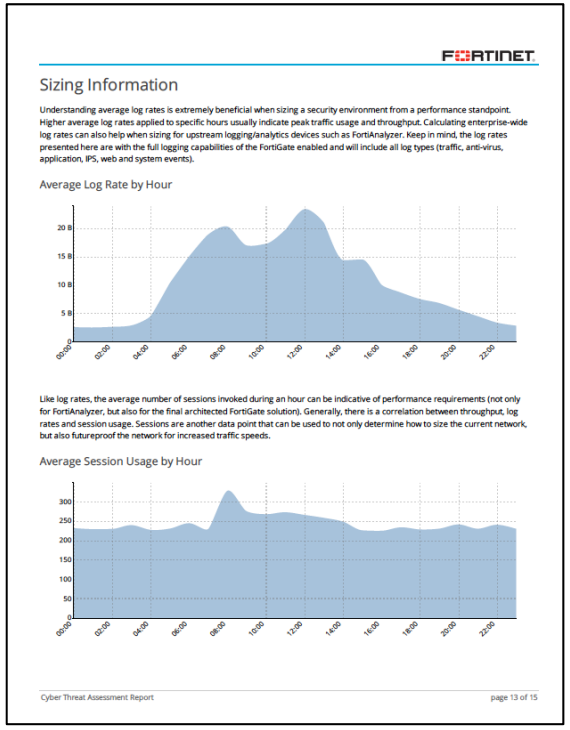
Cloud Usage (SaaS)

IT managers are often unaware of how many cloud-based services are in use within their organization. Sometimes, these applications can be used to circumvent or even replace corporate infrastructure already available to users in lieu of ease of use. Unfortunately, a potential side effect of this is that your sensitive corporate information could be transferred to the cloud. Accordingly, your data could be exposed if the cloud provider's security infrastructure is breached.

The adoption of "infrastructure as a service" (IaaS) platforms is popular and can be very useful when compute resources are limited or have specialized requirements. That said, the effective outsourcing of your infrastructure must be well regulated to prevent misuse. The occasional auditing of IaaS applications can be a useful exercise not only for security purposes, but also to minimize organizational costs associated with pay per use models or recurring subscription fees.

Cloud Usage (IaaS)

Cyber Threat Assessment Report page 8 of 15



FORTINET

Sizing Information

Understanding average log rates is extremely beneficial when sizing a security environment from a performance standpoint. Higher average log rates applied to specific hours usually indicate peak traffic usage and throughput. Calculating enterprise-wide log rates can also help when sizing for upstream logging/analytics devices such as FortiAnalyzer. Keep in mind, the log rates presented here are with the full logging capabilities of the FortiGate enabled and will include all log types (traffic, anti-virus, application, IPS, web and system events).

Average Log Rate by Hour

Like log rates, the average number of sessions invoked during an hour can be indicative of performance requirements (not only for FortiAnalyzer, but also for the final architected FortiGate solution). Generally, there is a correlation between throughput, log rates and session usage. Sessions are another data point that can be used to not only determine how to size the current network, but also futureproof the network for increased traffic speeds.

Average Session Usage by Hour

Cyber Threat Assessment Report page 13 of 15

Программа оценки киберугроз

- CTAP отчет обеспечивает детальный уровень анализа Вашей сети по ключевым направлениям:
  - » *Угрозы безопасности* – Обнаружение уязвимостей, вредоносного ПО, ботнет...
  - » *Продуктивность* – Анализ приложений и Интернет-активности
  - » *Производительность* – анализ загрузки каналов связи

- **БЫСТРО** – не более 7 дней мониторинга
- **ЛЕГКО** – без влияния на инфраструктуру
- **БЕСПЛАТНО** – никаких обязательств с Вашей стороны

Ключевые элементы фабрики

Партнеры экосистемы

Партнёры эко системы безопасности Fortinet

Cloud

- IBM Cloud
- Microsoft Azure
- amazon web services
- HP Cloud Services
- NTT

SDN

- vmware NSX
- big switch networks
- ARISTA
- openstack
- PLUMgrid
- Microsoft Hyper-V
- CISCO
- KVM
- PLURIBUS NETWORKS
- CITRIX
- nuagenetworks

Sandbox

- Bit9 + CARBON BLACK

Test/SSO

- ixia
- Centrify

System Integrator

- Hewlett Packard Enterprise
- IBM
- Capgemini CONSULTING.TECHNOLOGY.OUTSOURCING

SIEM

- splunk>
- ArcSight An HP Company
- IBM Radar
- LogRhythm
- ALIEN VAULT

Management

- REDSEAL
- skybox Security
- tufin
- algosec
- FIREMON
- Gigamon

Решения Fortinet для всех сегментов

1	2	3	4	5	6
Enterprise Firewall	**ATP Framework**	**Data Center Security**	**Cloud Security**	**Secure Access Architecture**	**Connected UTM** (SMB)
					
▪ Extensive Range of NetSec Hardware, Virtual and Cloud options ▪ Different perrsonalities for each Deployment mode	▪ Advanced Threat Protection – Sandbox ▪ Network+Email+Web+Client Security	▪ North - South (High Speed Appliance) + East West (Virtual & SDN) ▪ Application Security	▪ Public Cloud Security (AWS, Azure …) ▪ Hybrid Cloud	▪ WLAN Access ▪ LAN Access	▪ All In One Security ▪ Cloud Management

Management, Analytics & APIs (Appliance, Virtual machine & Cloud)

russia@fortinet.com