

**FORTINET®**

# Active Defense Security Fabric 2020



*<name>  
System Engineer*



# DX

**Интеграция цифровых технологий во все аспекты  
бизнеса, приводящая к фундаментальным изменениям  
в работе бизнеса и в способах донесения ценности до  
потребителя.**

## **[Digital Transformation]**



# SX

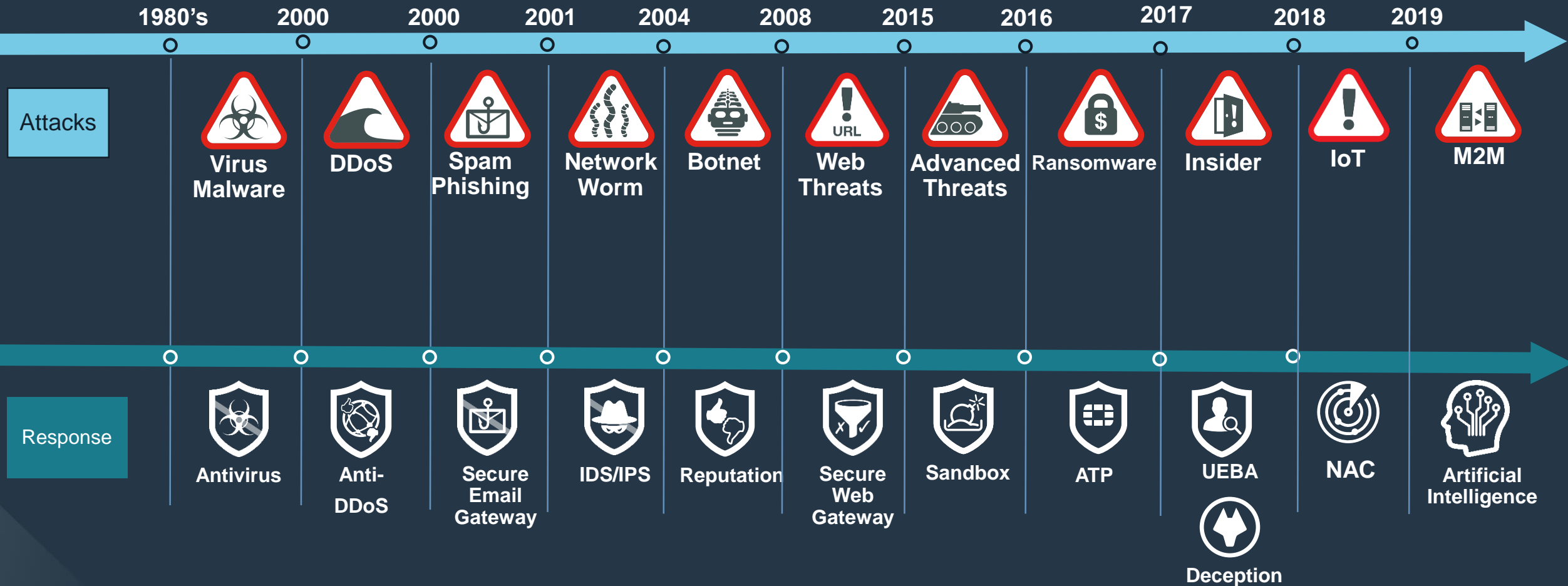
Интеграция безопасности во все аспекты цифровых технологий, приводящая к появлению **Архитектуры Безопасности**, которая обеспечивает **Непрерывную Оценку Доверия**.

[Security Transformation]

# Ландшафт угроз постоянно меняется



Расширение плоскости атак создает новые вызовы





# Fortinet Security Fabric

## Комплексная

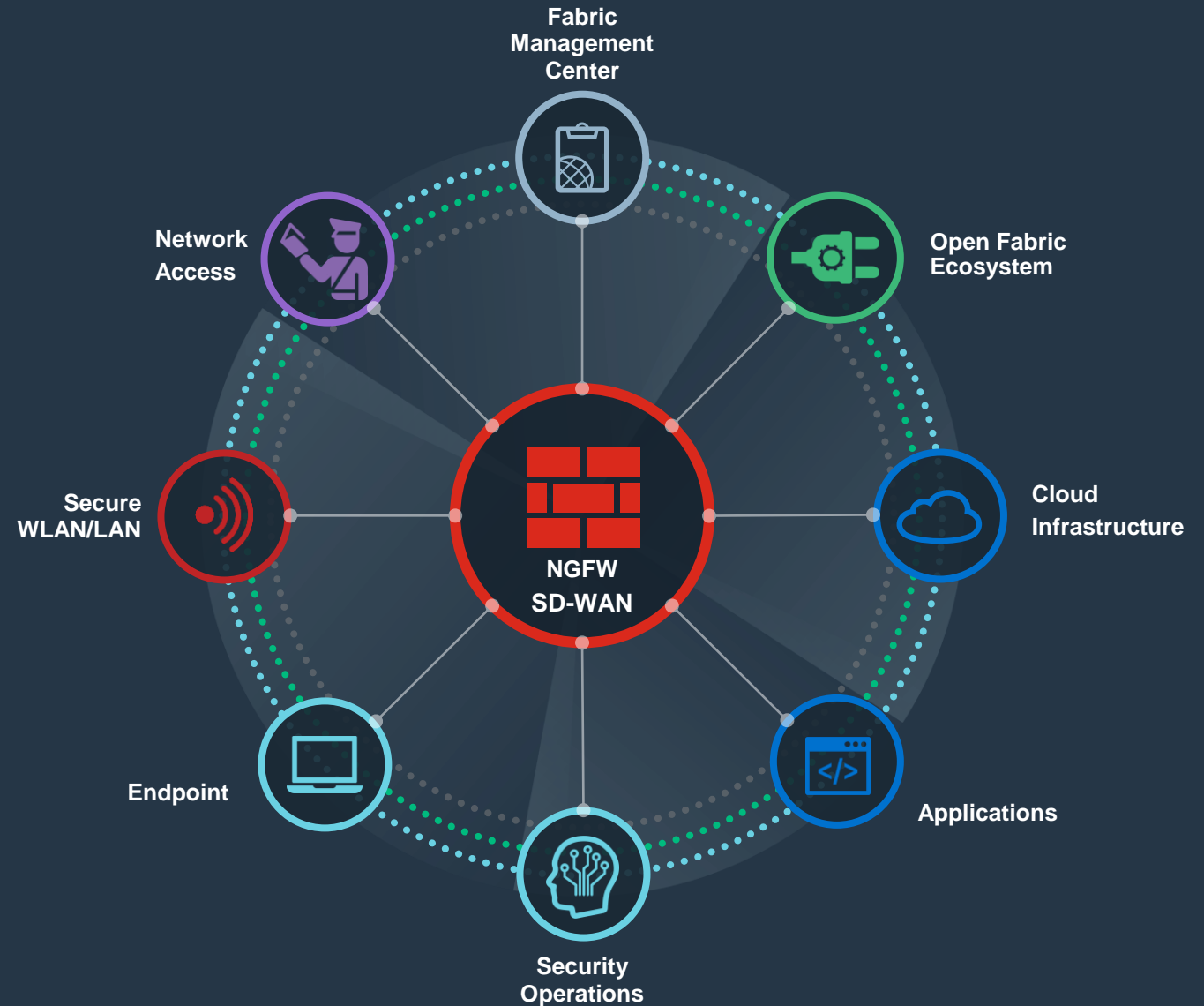
видимость всей поверхности атаки  
для лучшего управления рисками

## Интегрированное

решение, упрощающее поддержку  
нескольких точечных продуктов

## Автоматизированные

рабочие процессы,  
увеличивающие скорость  
управления и реагирования



### FortiGate Cloud

- FortiGate Mgmt., Log Analysis and Retention
- Bulk Provisioning
- IoC Service

### FortiSandbox Cloud

### FortiMail Cloud

### FortiWeb Cloud

### FortiAP Cloud

### FortiSwitch Cloud

### FortiToken Cloud

### FortiVoice Cloud



### FortiPresence

### FortiCASB

### FortiCWP

FTNT Hosted Services



Public Cloud Instances

## SECURITY/NETWORK OPERATING CENTER

### FortiAnalyzer

Central Log & report



Central Device Mgmt.



FortiManager

### FortiNAC

IoT Access Control



User Access Mgmt.



FortiAuthenticator

### FortiSandBox

File Analysis



Network Tester



FortiTester

### FortiWLC

Wireless Controller



Wireless Manager



FortiWLM

### FortiDeceptor

Honeypot



SIEM



FortiSIEM

### FortiSOAR

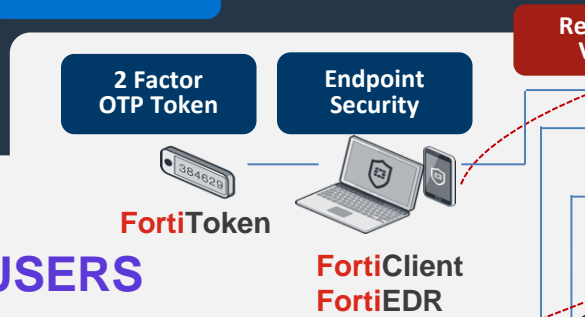
SOAR



Client Mgmt. System



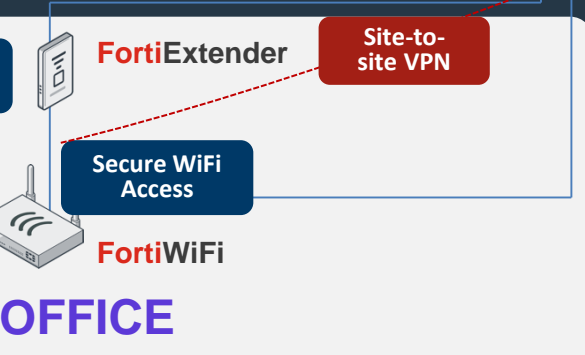
FortiClient EMS



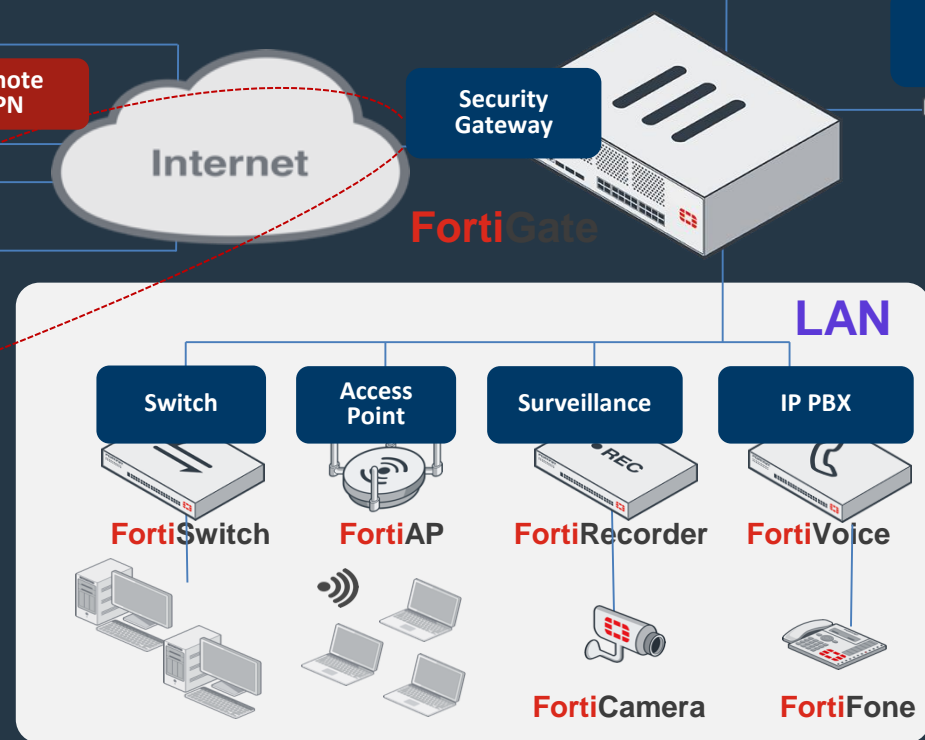
## MOBILE USERS

FortiToken

FortiClient  
FortiEDR



## REMOTE OFFICE



## LAN

Switch



FortiSwitch

Access Point



FortiAP

Surveillance



FortiRecorder

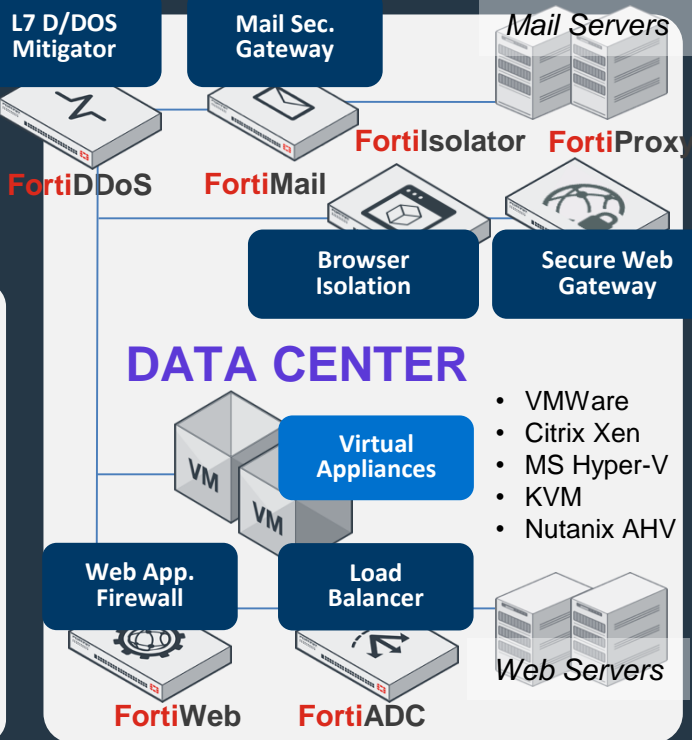
IP PBX



FortiVoice

FortiCamera

FortiFone



## DATA CENTER

L7 D/DOS Mitigator



FortiDDoS

Mail Sec. Gateway



FortiMail

FortiIsolator



Browser Isolation

Mail Servers



FortiProxy



Secure Web Gateway



FortiWeb

Virtual Appliances



Load Balancer



FortiADC

- VMWare
- Citrix Xen
- MS Hyper-V
- KVM
- Nutanix AHV



Web Servers



# Fortinet Security Fabric – основа цифровых инноваций



Защита каждого элемента инфраструктуры

## Zero-trust Network Access



Идентификация и обеспечение безопасности пользователей и устройств внутри и вовне сети

## Security-driven Networking



Обеспечение сетевой безопасности без ущерба производительности

## Dynamic Cloud Security



Безопасность и контроль облачной инфраструктуры и приложений

## AI-driven Security Operations



Автоматическое обнаружение, предотвращение, и реагирование на киберугрозы

# Security Fabric Products

Доступны различные модели развертывания



-  Appliance
-  Virtual Machine
-  Cloud
-  Security-as-a-Service
-  Software

FortiNAC	FortiAP	FortiGate	FortiGate VM	FortiWeb	FortiClient	FortiAnalyzer	FortiManager
FortiClient Fabric Agent	FortiSwitch		FortiCWP	FortiMail	FortiEDR	FortiSIEM	FortiGate Cloud
FortiAuthenticator				FortiCASB		FortiSandbox	FortiCloud
				FortiADC		FortiSOAR	

 FortiGuard Services





# Сетевая безопасность

## Next-generation Firewall

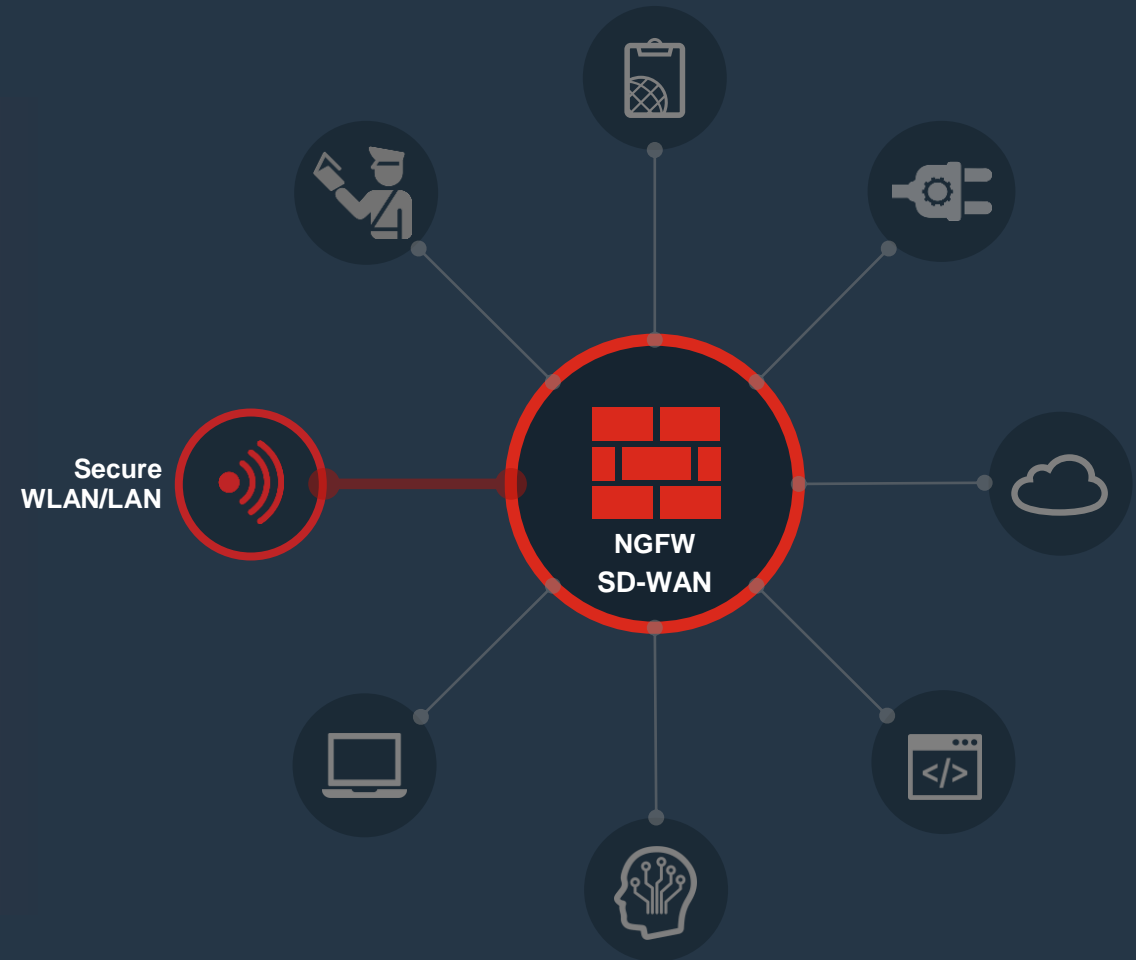
Управление всеми рисками безопасности и гипермасштабируемая защита

## SD-WAN

Улучшенное взаимодействие пользователя и приложения

## Secure Web Gateway

Блокирование угроз



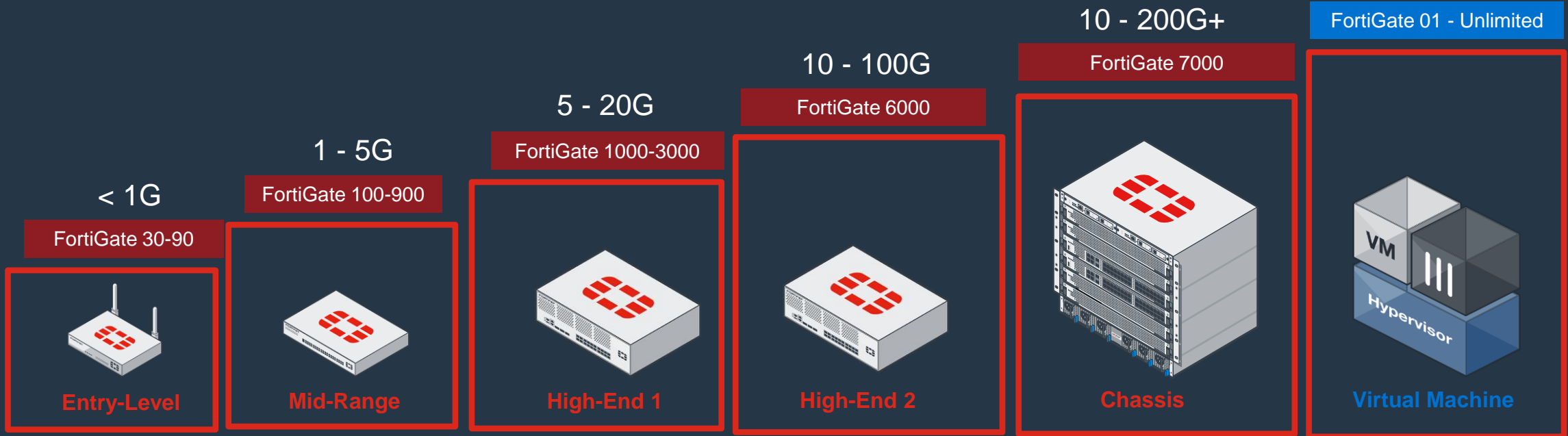
# Модельный ряд Fortinet Network Security Appliance



Up to 110Gbps SSL Inspection



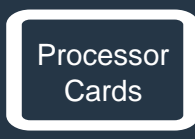
Up to 100Gbps Threat Protection



N x



N x



N x



N x



N x



N x



N x



Hardware  
Dependent

# Сетевая безопасность: Next Generation Firewall (NGFW)



## NGFW

Источники кибератак могут находиться как во внешней, так и во внутренней сети. Они могут нарушить работу бизнес-служб. Управление рисками безопасности с большим охватом и на высокой производительности необходимы для непрерывности бизнеса.



FortiGate



NGFW



Segmentation

- Управление внешними и внутренними рисками
- Удаление «слепых» зон с помощью проверки SSL
- Защита гипермасштабируемой инфраструктуры



# Сетевая безопасность: Next Generation Firewall (NGFW)



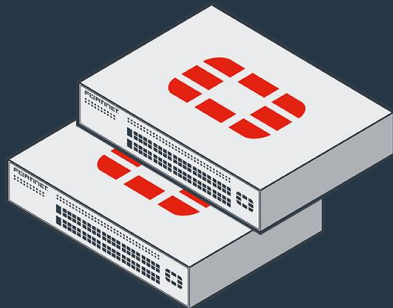
Segmentation



FortiGate

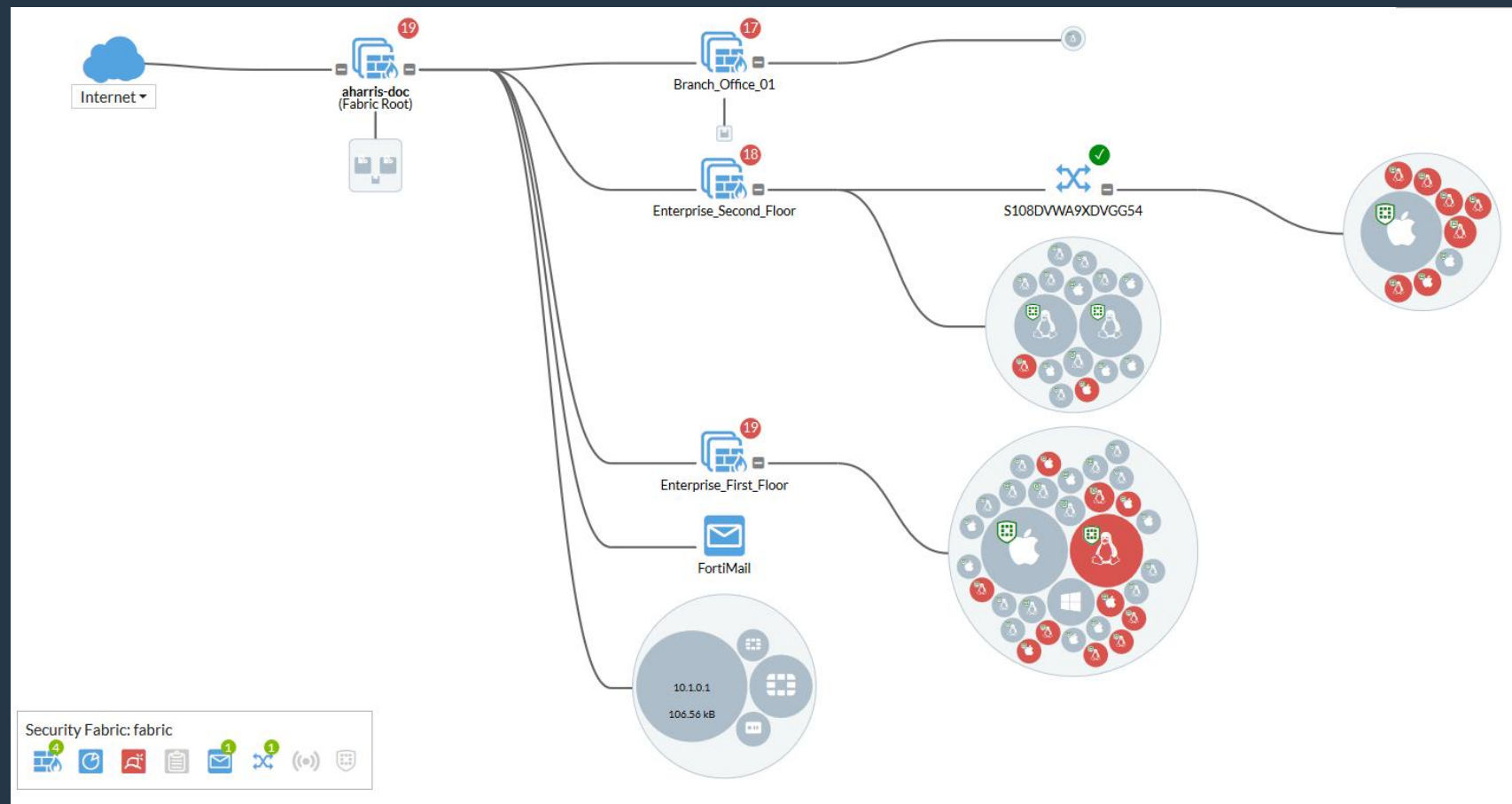


NGFW



Устройство **FortiGate** обеспечивает возможности межсетевого экрана нового поколения для средних и крупных предприятий с возможностью гибкого развертывания в кампусе или на филиале предприятия. Защищите инфраструктуру от киберугроз с помощью процессора безопасности, обеспечивающего высокую производительность, эффективность безопасности и глубокую видимость.

## Security Fabric Topology





# Сетевая безопасность: Secure SD-WAN

## SD-WAN

Быстро увеличивающееся потребление полосы пропускания и внедрение облачных технологий приводят к ухудшению взаимодействия с пользователем и увеличению затрат на WAN. Компаниям необходимо упростить операции, снизить затраты и обеспечить безопасный переход в «облако».



FortiGate



SD-WAN



- Снижение стоимости WAN
- Улучшение работы с приложениями
- Поддержка перехода в «облако»



# Что значит **SD-WAN** с точки зрения Fortinet?

○ It is not a product.  
It is included into FortiOS.

○ Whatever WAN-Interface type.  
WAN Path Control  
Real-time SLA.  
Quality parameters like jitter or latency.

It's a **feature** which allows FortiGate to use the **best paths** in order to reach an **application** applying **QoS** **overlay networking** and **NGFW** security.

○ Application awareness  
Internet DB  
Service

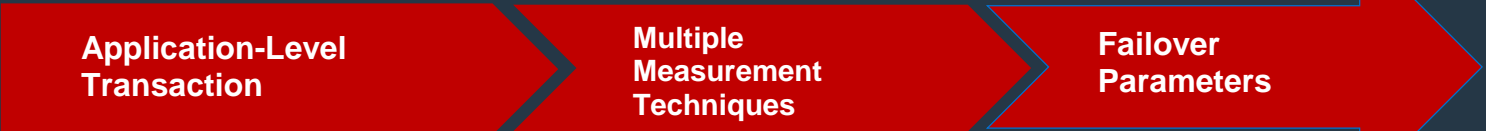
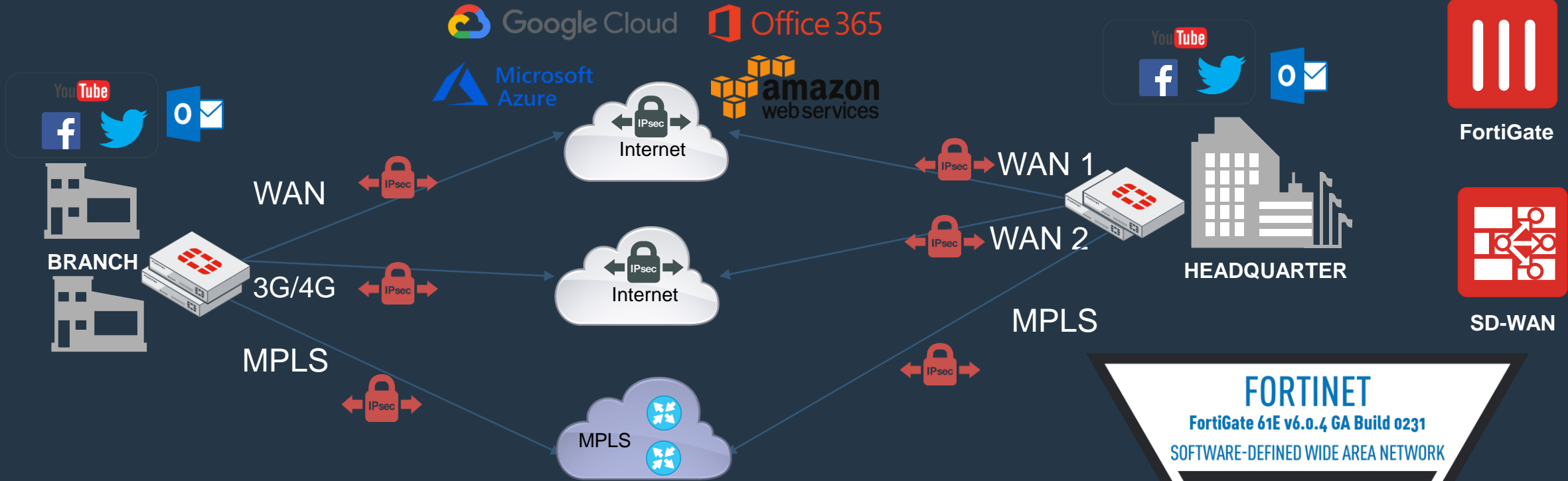
Traffic shaping w/ queues  
Guarantee, maximum, %

○ SPU accelerated  
VPN tunnels

○ Based on FortiGate  
NGFW Features and  
SSL Inspection



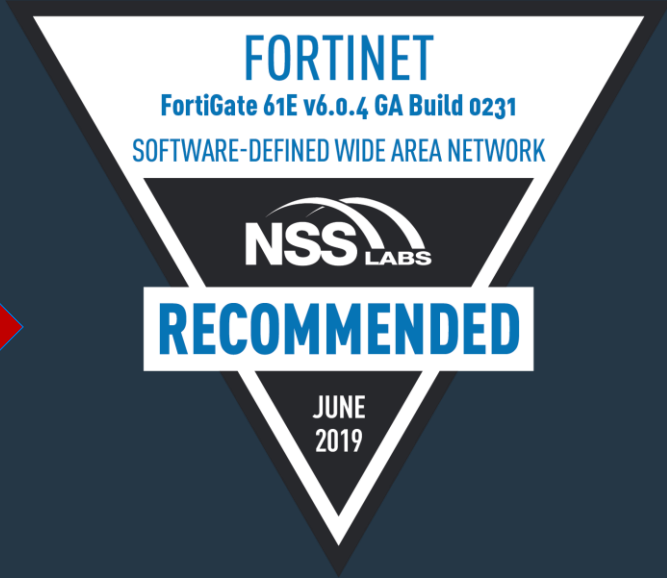
# SD-WAN Multi-Path Intelligence



Latency < 200ms  
 Latency < 100ms  
 AND  
 Packet Loss < 1%  
 AND  
 Jitter < 30ms

- Ping
- HTTP
- TCP Echo
- UDP Echo
- TWAMP

- Check Interval
- Failure before inactive
- Success before restore



# FortiGate NGFW с встроенным SD-WAN



SD-WAN требует прямого доступа в Интернет, что требует большей безопасности в каждом филиале.

90% поставщиков SD-WAN предлагают только брандмауэры с отслеживанием состояния, что недостаточно.

## Secure SD-WAN

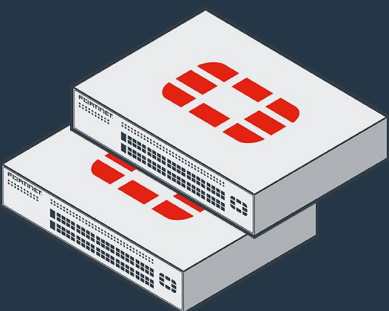
## NGFW

## SD-WAN



Масштабируемость и простота развертывания

Беспрецедентная интеграция и видимость



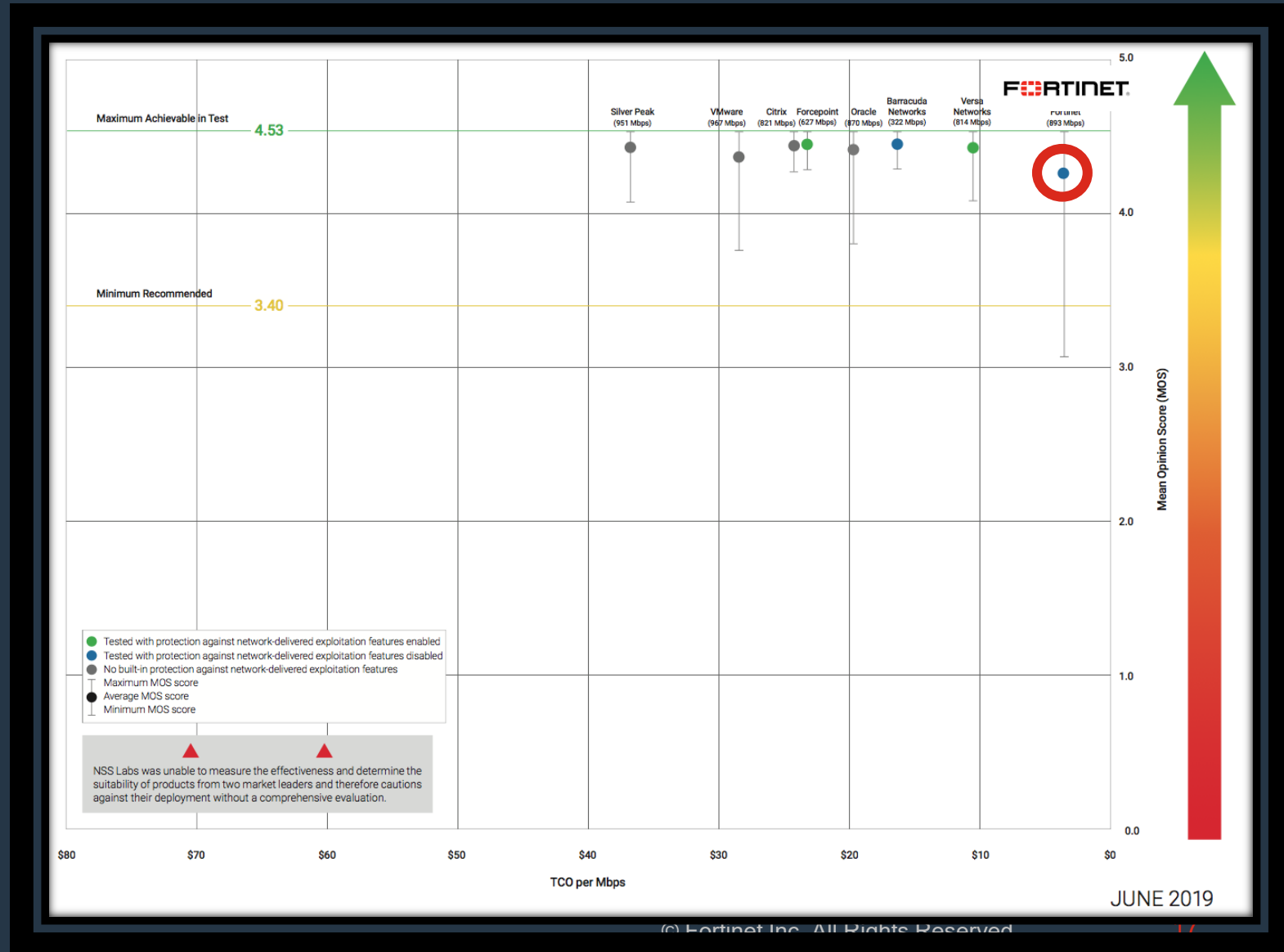


# NSS Labs Карта эффективности SD-WAN 2019



## Результаты FortiGate SD-WAN

- ✓ Второй в рейтинге SD-WAN **Recommended**
- ✓ Лучшее TCO среди 8 вендоров (\$3.5)
- ✓ Zero Touch Deployment за 6 минут
- ✓ Надежный показатель QoE



# Сетевая безопасность: Secure Web Gateway (SWG)



## Secure Web Gateway (SWG)

Вредоносные URL-адреса являются источником угроз, которые могут привести к заражению вредоносными программами и краже данных. С более чем 70% зашифрованного трафика в сети остается больше «слепых» зон. Для защиты от растущих интернет-угроз в NGFW встроена Веб-фильтрация.



FortiGate



SWG



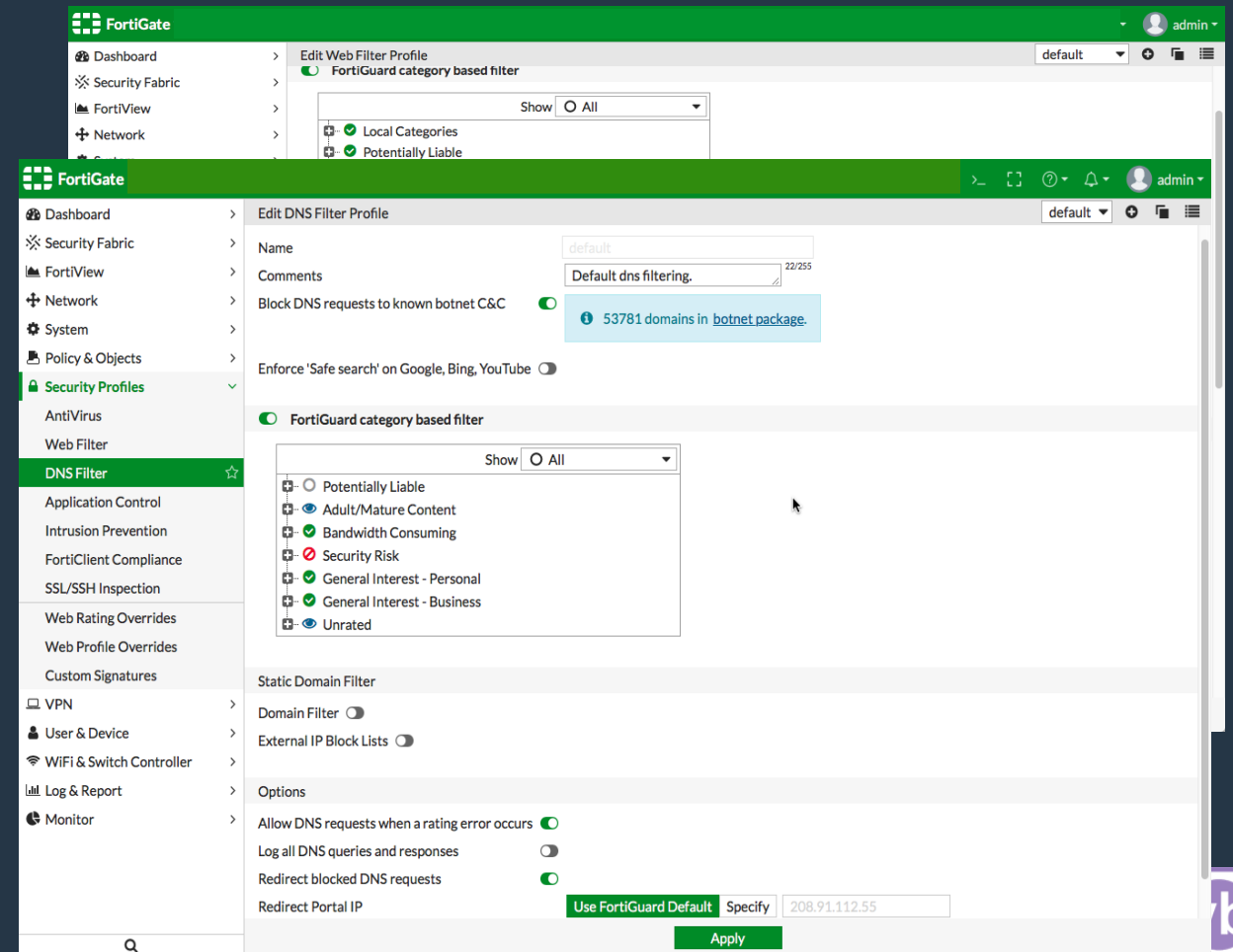
- Защита пользователей от вредоносных URL
- Удаление «слепых» зон с помощью проверки SSL
- Уменьшение разнообразия продуктов и их сложности

# Сетевая безопасность: Secure Web Gateway (SWG)



- Защитите свою организацию, заблокировав доступ к вредоносным, взломанным или неприемлемым веб-сайтам с помощью FortiGuard Web Filtering.
- Веб-фильтрация – это первая линия защиты от сетевых атак.
- Вредоносные или взломанные веб-сайты, основной вектор для инициирования атак, запускают загрузку вредоносных программ, шпионского ПО или опасного контента.
- FortiGate Web Filtering - единственная служба веб-фильтрации в отрасли, которая сертифицирована VBWeb на предмет эффективности безопасности Virus Bulletin.
- Было заблокировано 97,7% прямых загрузок вредоносных программ и остановлено 83,5% вредоносных программ, направленных с помощью всех методов, протестированных в рамках тестирования безопасности VBWeb Virus Bulletin.
- Служба веб-фильтрации доступна с использованием NGFW FortiGate, что позволяет Вам легко видеть и контролировать, какие веб-сайты посещают Ваши пользователи.

**FORTINET**



## TOP-RATED SECURITY EFFECTIVENESS

- VBWeb certified for security effectiveness by Virus Bulletin





# Fortinet 2020 Security Bundles

1. 24x7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 6.2

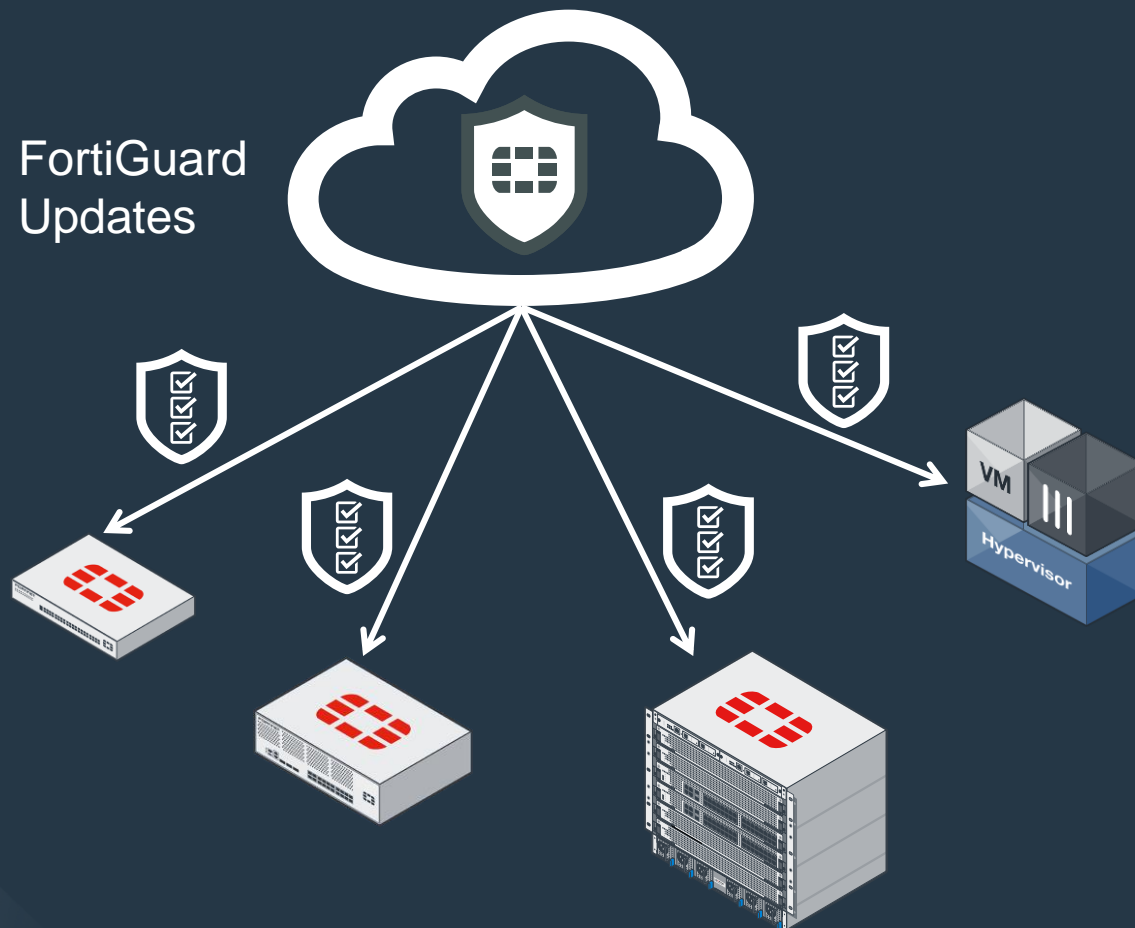
FortiManager Cloud <sup>2</sup>				✓
FortiAnalyzer Cloud <sup>2</sup>				✓
SD-WAN Overlay Controller VPN Service <sup>2</sup>				✓
SD-WAN Cloud Assisted Monitoring <sup>2</sup>				✓
FortiConverter Service				✓
FortiCASB SaaS-only Service			✓	✓
FortiGuard Industrial Service			✓	✓
FortiGuard Security Rating Service			✓	✓
FortiGuard Anti-Spam Service		✓	✓	✓
FortiGuard Web Filtering Service		✓	✓	✓
FortiGuard Advanced Malware Protection (AMP) - Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	✓	✓	✓	✓
FortiGuard IPS Service	✓	✓	✓	✓
FortiGuard App Control Service	✓	✓	✓	✓
FortiCare (incl. Internet Service DB, Client ID DB, IP Geography DB, Malicious URL DB, URL Whitelist DB)	24x7	24x7	24x7	ASE <sup>1</sup>
<b>Bundles</b>	<b>Threat Protection</b>	<b>UTP</b>	<b>Enterprise Protection</b>	<b>360</b>



# Security Rating Service

ЛУЧШИЕ МИРОВЫЕ ПРАКТИКИ ПО ИНДУСТРИИ

FortiGuard  
Threat  
Intelligence



- Коллекция лучших практик от заказчиков
- Примеры
  - Безопасность паролей
  - Пороги срабатывания попыток входа
  - Логирование на FortiAnalyzer
  - Использование 2-х факторной аутентификации
- Система сравнивается на соответствие всем лучшим практикам
- Приоритезирует найденное по уровню важности от критической до низкой
- Доступны быстрые пресеты для исправления

354

Passed

25

Low

65

Medium

31

High

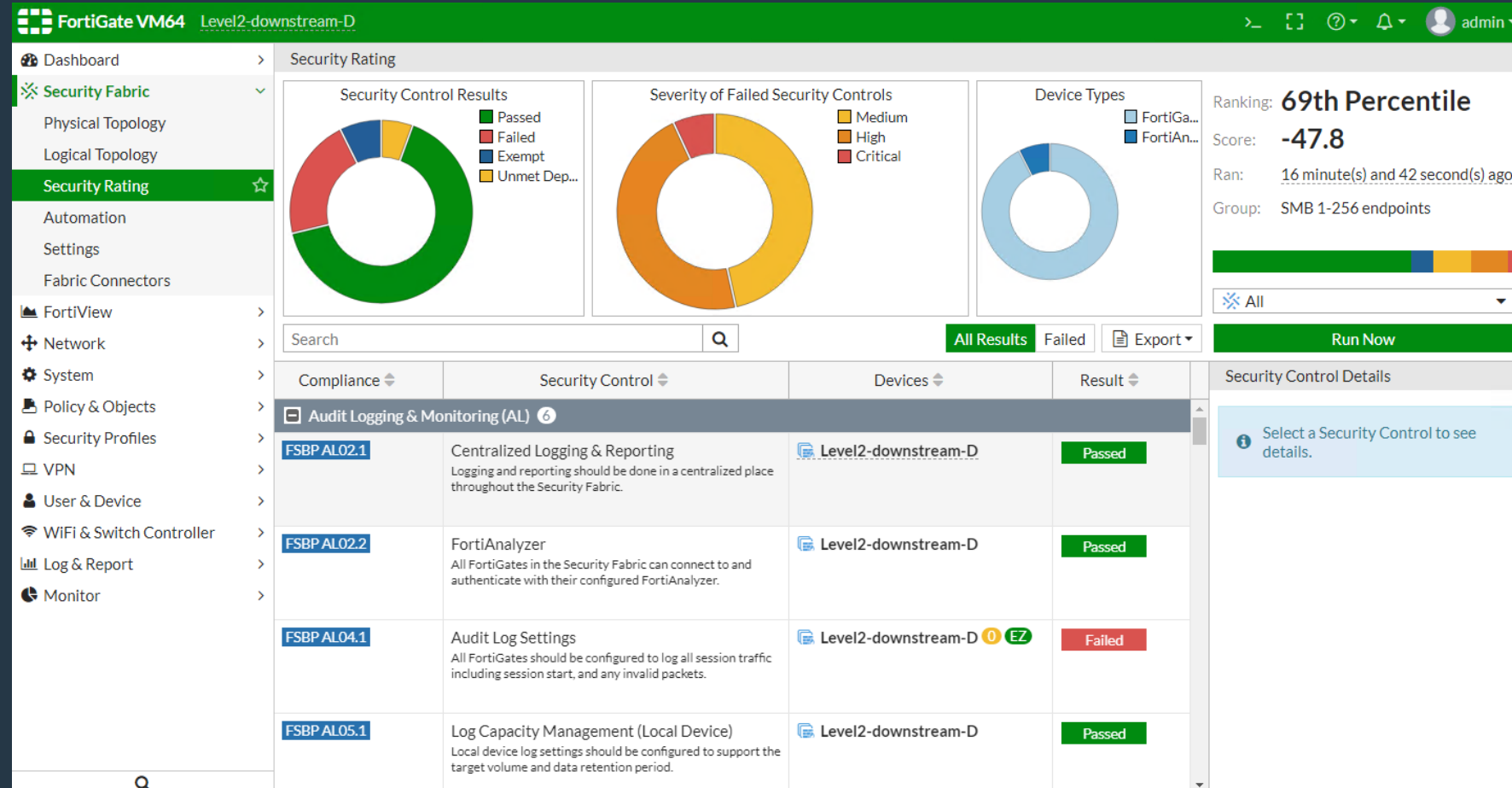
22

Critical

# Рейтинг безопасности позволяет проводить сравнительный анализ

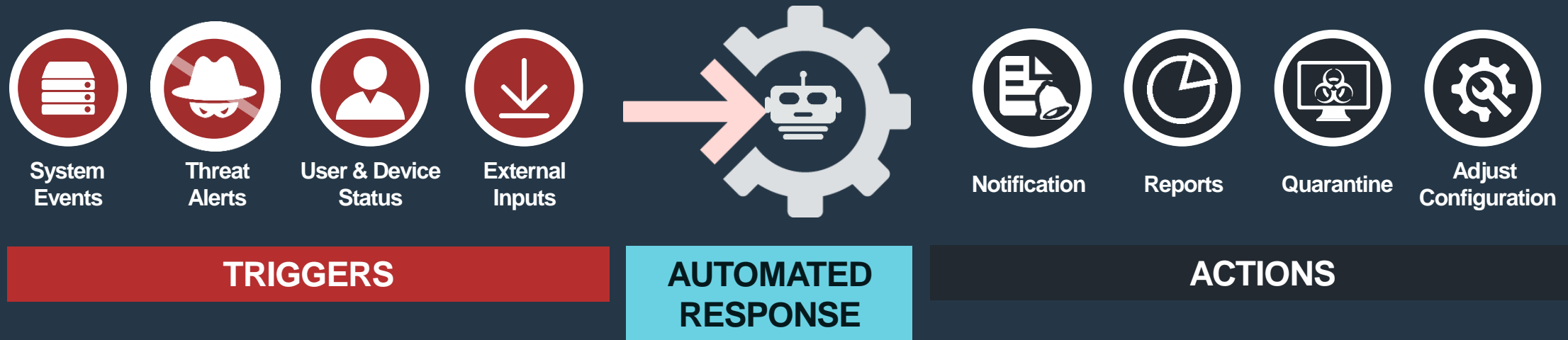


- Сравнительный анализ по рейтингу безопасности
  - » Сравнение с аналогичными организациями по размеру и индустрии в процентах
- Представление графика трендов
  - » Путем получения исторических данных из FortiAnalyzer





# Автоматизация процессов



- Автоматизированные операции (stitches) используют триггеры для выполнения действий
  - » Легко создаются с помощью графических помощников (wizard)
  - » Работают с компонентами внутри Security Fabric



# Автоматизация процессов

- Автоматизированные операции (stitches) используют триггеры для выполнения действий:

- » Легко создаются с помощью графических помощников (wizard)
- » Работают с компонентами внутри Security Fabric

The screenshot displays the configuration page for an automated process named "Compromised-IP-Banned".

- Name:** Compromised-IP-Banned
- Status:** Enabled (indicated by a green up arrow icon)
- FortiGate:** All FortiGates (with a plus sign to add more)

**Trigger Section:**

- Compromised Host (selected with a green checkmark)
- Event Log
- Reboot
- Conserve Mode
- High CPU
- License Expiry
- HA Failover (selected with a green checkmark)
- Configuration Change

**IOC level threshold:** High (selected)

**Action Section:**

- Email
- FortiExplorer Notification
- Access Layer Quarantine
- Quarantine FortiClient via EMS
- IP Ban (selected with a green checkmark)
- AWS Lambda
- Webhook

**Minimum interval (seconds):** 0



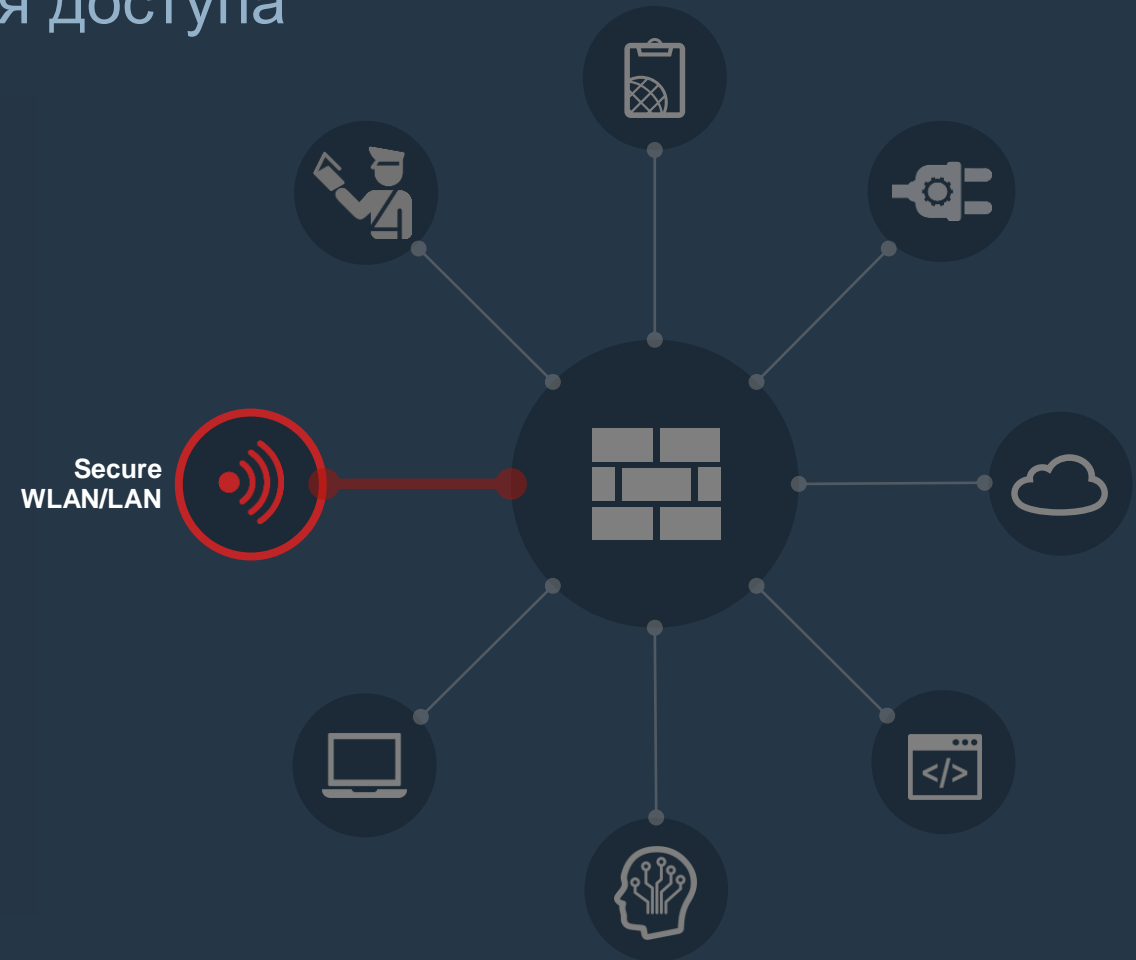


# Безопасная инфраструктура : **Secure Access**

Расширение безопасности до уровня доступа

## Secure WLAN/LAN

Расширение безопасности до уровня доступа





# Безопасная инфраструктура : **Secure Access**

Расширение безопасности до уровня доступа

Большинству продуктов уровня доступа не хватает интеграции с решениями безопасности и инструментов управления. Защиту FortiGate можно распространить на сеть доступа, чтобы обеспечить более глубокую интеграцию и постоянную безопасность.



FortiGate



FortiAP



FortiSwitch

- Расширение безопасности до уровня доступа
- Упрощение операций
- Применение решения SD-Branch



# Безопасная инфраструктура : **Secure Access**



Расширение безопасности до уровня доступа

## FortiGate Appliances



- 17+ моделей
- Next Generation Firewall
- WLAN Controller
- Switch Controller

## Access Points



- 30+ моделей
  - 11ac wave 1 & 2, Wi-Fi 6
- Indoor/Outdoor/Wall jack
- Не требует лицензий

## Switches



- 20+ моделей
  - Edge Switches
  - ToR Switches
- FortiLink integration to FGT
- L2/L3 & Advanced Services



# Безопасная инфраструктура : **Secure Access**

Расширение безопасности до уровня доступа

## Упрощение

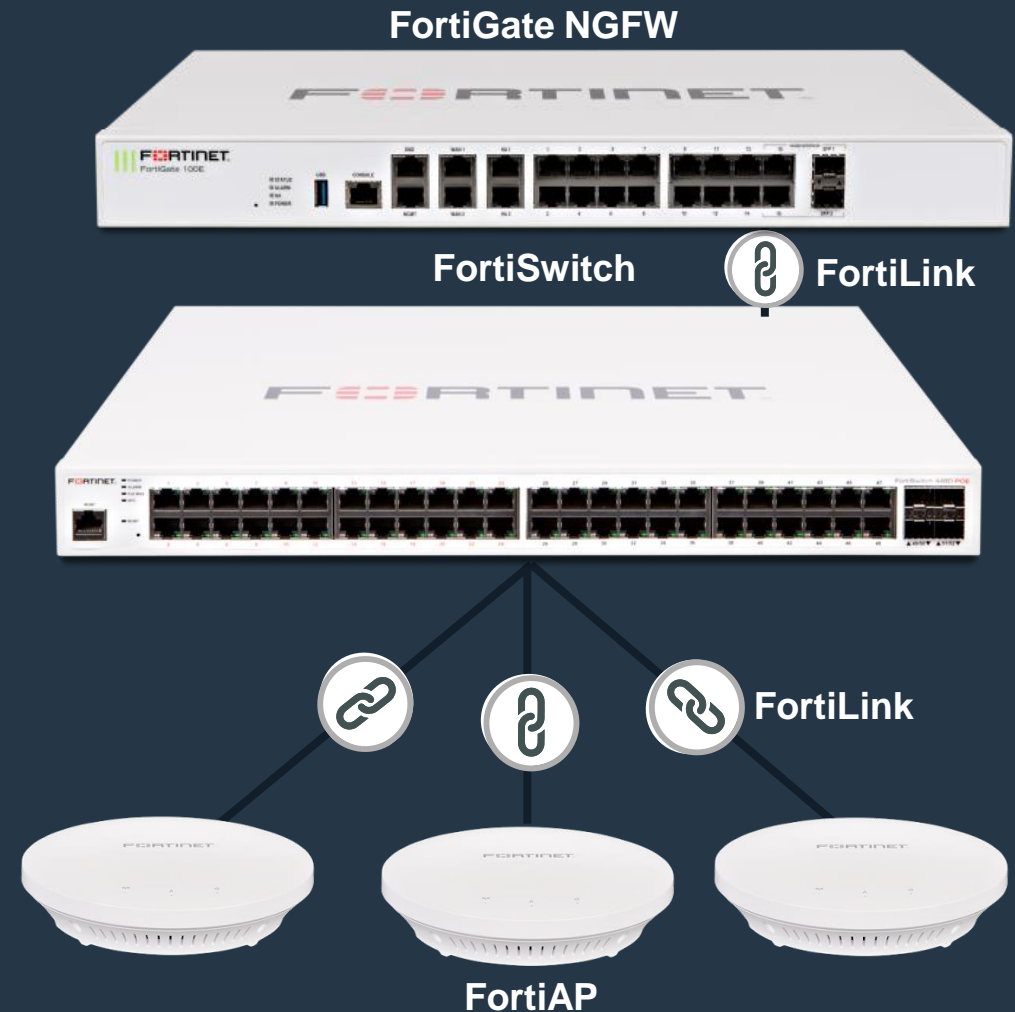
- Гибкая архитектура, масштабируемая по мере изменения потребностей
- Управление, видимость и аналитика между проводной, беспроводной сетью и безопасностью

## Безопасность

- Порты МЭ и коммутатора одинаково безопасны, SSID напрямую привязаны к политикам МЭ
- Политики Global Security контролируют уровень портов и WLAN

## Уменьшение стоимости владения

- Управление доступом включено в SD-Branch. Не требует лицензии

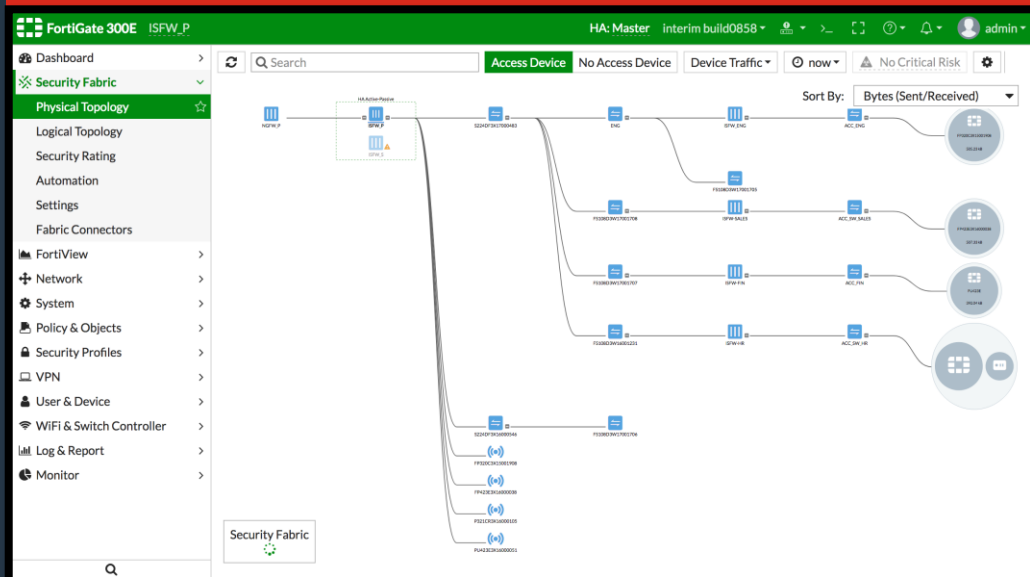


# Безопасная инфраструктура : **Secure Access**

Расширение безопасности до уровня доступа



## FortiGate Interface



- Идеально подходит для развертывания на небольшом или одном объекте
- Поддерживает настройку и управление SD-WAN
- Управление безопасностью, доступом к сети и WAN из одного интерфейса

## FortiManager

Access Point	Connected Via	SSIDs	Channel	Clients	OS Version	AP Profile
FP320C3X140078	192.168.10.101	Radio 1: 1 Radio 2: 136	Radio 1: 1 Radio 2: 136	Radio 1: 0 Radio 2: 1	FP320C-v5.6-build04	
PS323C3U150004	192.168.4.100	Radio 1: 1 Radio 2: 165	Radio 1: 1 Radio 2: 165	Radio 1: 0 Radio 2: 0	PS323C-v5.6-build03	
FP320C3X140120	192.168.107.100	Radio 1: 1 Radio 2: 132	Radio 1: 11 Radio 2: 132	Radio 1: 0 Radio 2: 1	FP320C-v5.6-build04	
FP320C3X150019	192.168.101.2	Radio 1: 0 Radio 2: 20	Radio 1: 0 Radio 2: 20	Radio 1: 0 Radio 2: 0	FP320C-v6.0-build00	
FP423E3X160000	192.168.103.2	Radio 1: 1 Radio 2: 144	Radio 1: 1 Radio 2: 144	Radio 1: 0 Radio 2: 0	FP423E-v6.0-build00	
P321CR3X160001	192.168.104.3	Radio 1: 0 Radio 2: 0	Radio 1: 0 Radio 2: 0	Radio 1: 0 Radio 2: 0	P321CR-v5.4-build01	
PU423E3X160000	192.168.102.1	Radio 1: 1 Radio 2: 149	Radio 1: 1 Radio 2: 149	Radio 1: 0 Radio 2: 0	PU423E-v5.4-build00	
FP221B3X130102	20.20.20.22	Radio 1: 36 Radio 2: 11	Radio 1: 36 Radio 2: 11	Radio 1: 0 Radio 2: 0	FP221B-v5.4-build03	
FP320B3X130031	20.20.20.23	Radio 1: 0 Radio 2: 1	Radio 1: 0 Radio 2: 1	Radio 1: 0 Radio 2: 1	FP320B-v5.0-build06	
FP320C3X140098	20.20.20.21	Radio 1: 11 Radio 2: 149	Radio 1: 11 Radio 2: 149	Radio 1: 0 Radio 2: 1	FP320C-v5.6-build04	

- Масштабируемое управление
- Поддерживает настройку и управление SD-WAN
- Поддержка zero touch deployment
- Управление SD-WAN, безопасностью и доступом из единого интерфейса



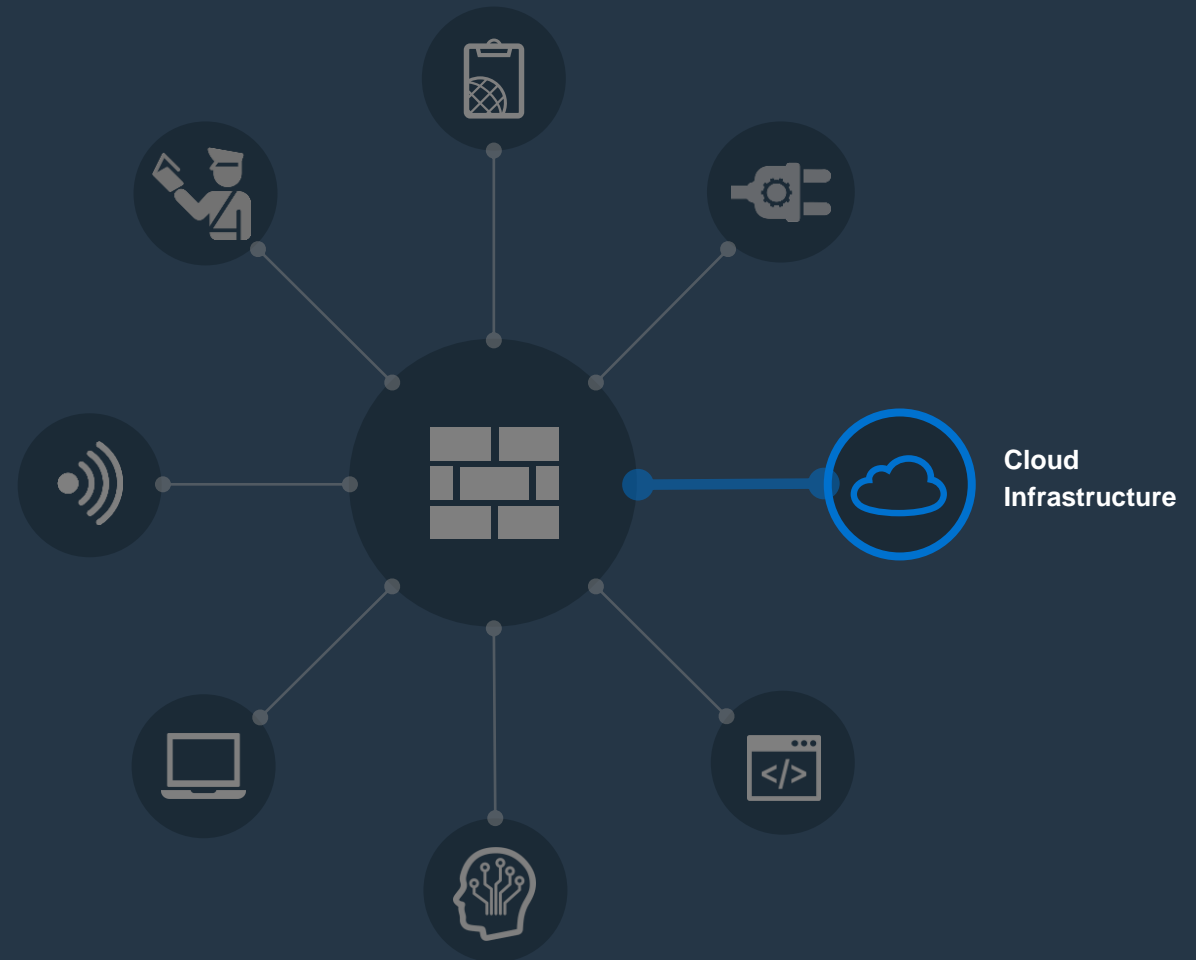
# Dynamic Cloud Security

## Public Cloud Infrastructure

Безопасность вычислений и приложений, построенных в облаке

## Private Cloud & SDN

Безопасность, автоматизация и интеграция для частного облака





# Dynamic Cloud Security

	VMWare vSphere	Citrix Xen Server	Xen	KVM	Microsoft Hyper-V	Nutanix AHV	Amazon AWS	Microsoft Azure	Oracle OPC	Google GCP	Aliyun
FortiGate-VM*	✓	✓	✓	✓	✓	✓	B P	B P	B P	B P	B P
FortiManager-VM	✓	✓	✓	✓	✓	✓	B P	B	B	B	B
FortiAnalyzer-VM	✓	✓	✓	✓	✓	✓	B P	B	B	B	B
FortiWeb-VM	✓	✓	✓	✓	✓		B P	B P	B	B	
FortiWeb Manager-VM	✓						B				
FortiMail-VM	✓	✓		✓	✓	✓	B	B			
FortiAuthenticator-VM	✓		✓	✓	✓		B	B			
FortiADC-VM	✓	✓	✓	✓	✓	✓	B P	B P	B P	B P	
FortiVoice-VM	✓	✓		✓	✓		B	B			
FortiRecorder-VM	✓	✓		✓	✓		P				
FortiSandbox-VM	✓			✓	✓	✓	B P	P			
FortiSIEM	✓			✓			B				
FortiProxy-VM	✓			✓			B	B			

\* Also support AzureStack and RackSpace (PAYG)

**B** BYOL **P** PAYG



# Dynamic Cloud Security

## Public cloud infrastructure

Облачные приложения требуют такой же сетевой безопасности, как и локальные, но при этом необходим непрерывный мониторинг активности и конфигурации облачной платформы.



FortiGate VM



FortiCWP

### Сетевая безопасность

- VPN-подключение
- Сетевая сегментация
- Предотвращение вторжений
- Secure Web Gateway

### Видимость и контроль

- Неправильная конфигурация
- Безопасность данных
- Соответствие требованиям
- Управление угрозами



Microsoft Azure



Cloud Infrastructure

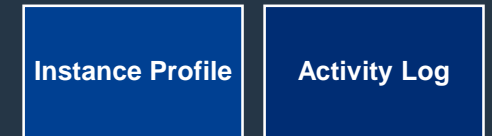
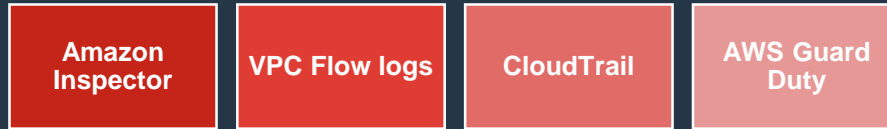




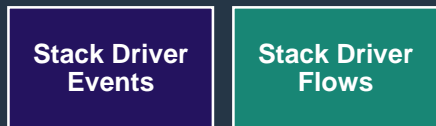
# Dynamic Cloud Security: Как FortiCWP взаимодействует с Облаком?



Cloud Infrastructure



Azure Security Center



Google Cloud Security Command Center



Security Architect

Malware  Sensitive data  Clean data

PUBLIC  EXTERNAL  INTERNAL  PRIVATE

- Dashboard
- Alert
- Resource
- Documents
- Activity
- Policy
- Report
- Admin

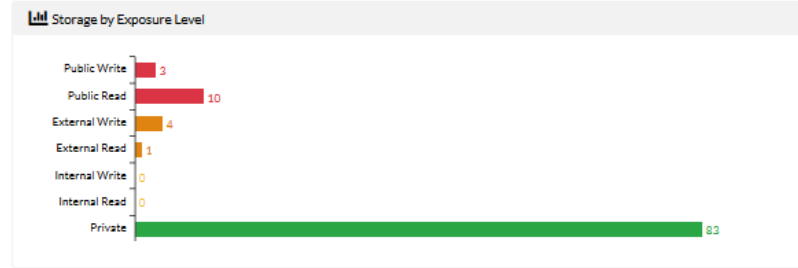
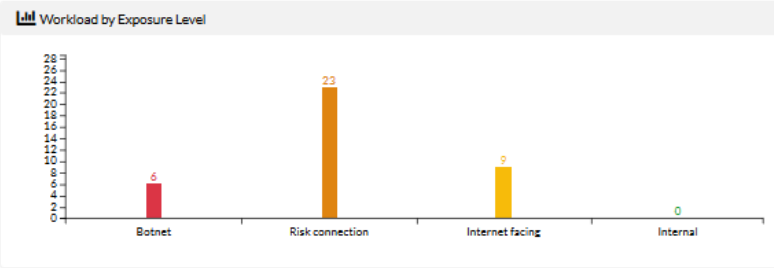
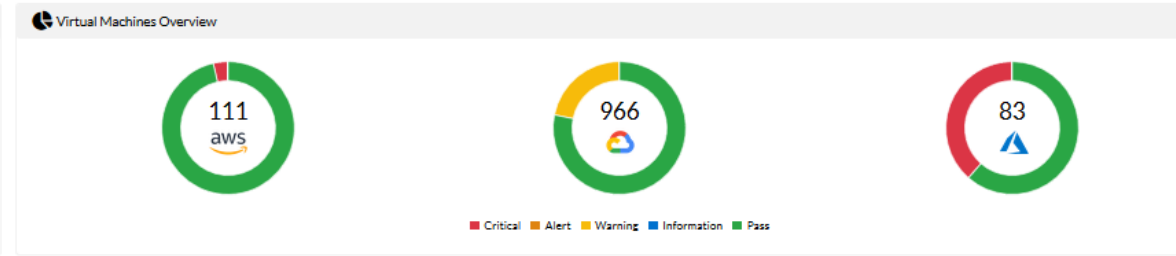
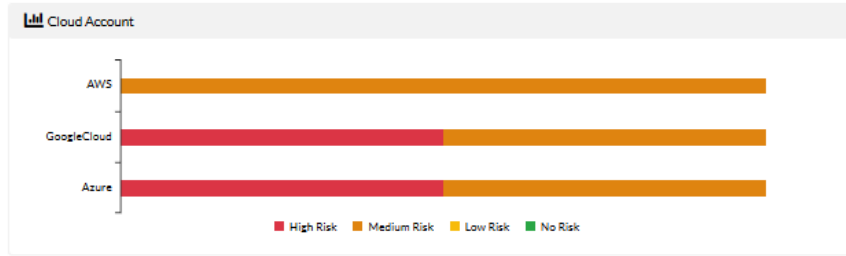
**Service Info**

**FortiCWP**  
Version 4.4.0

REGISTERED TO  
fcasbdemo@gmail.com

WORKLOAD GUARDIAN  
In use: 10/20 VM

STORAGE GUARDIAN ADV  
In use: 3.43 GB / 2 TB



**Malware Scan**

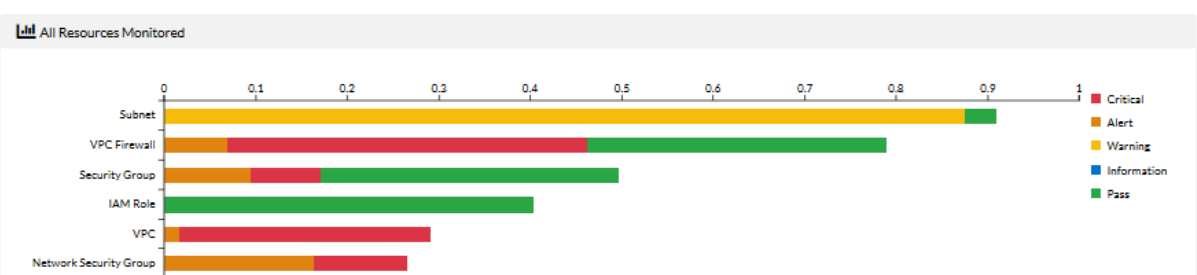
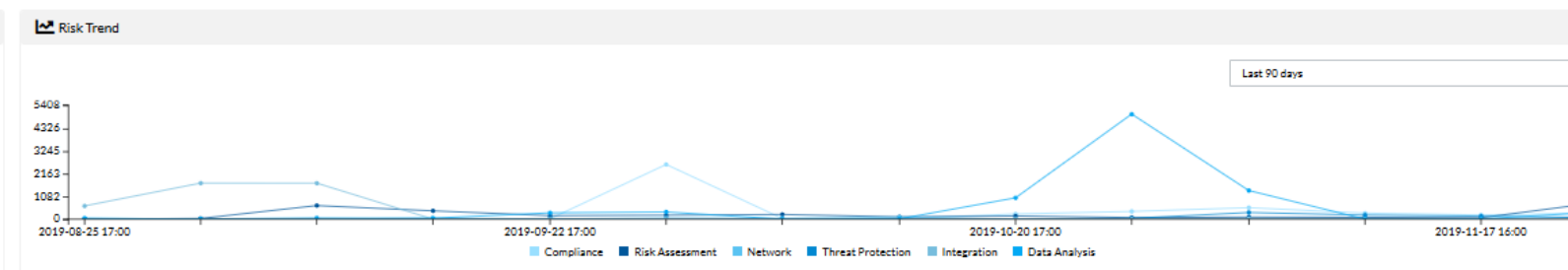
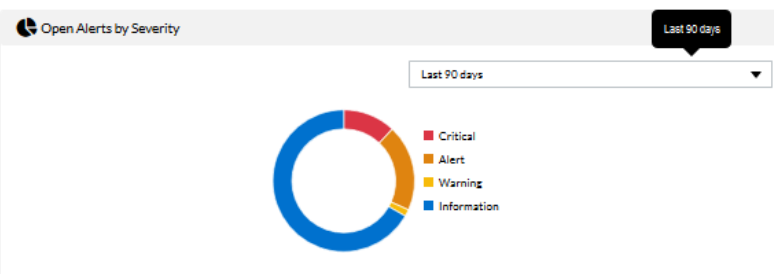
9 Malware Found

[View All](#)

**DLP Scan**

351 Sensitive Document

[View All](#)



**Top Policy Violation**

Last 90 days

- Import AWS Inspector alerts
- PCI - Privileged Account Activity
- Suspicious Location
- DLP USA/Germany Passport Number Policy
- DLP SSN Policy
- MIRAA - Login



# Dynamic Cloud Security

## Web Application & API Security

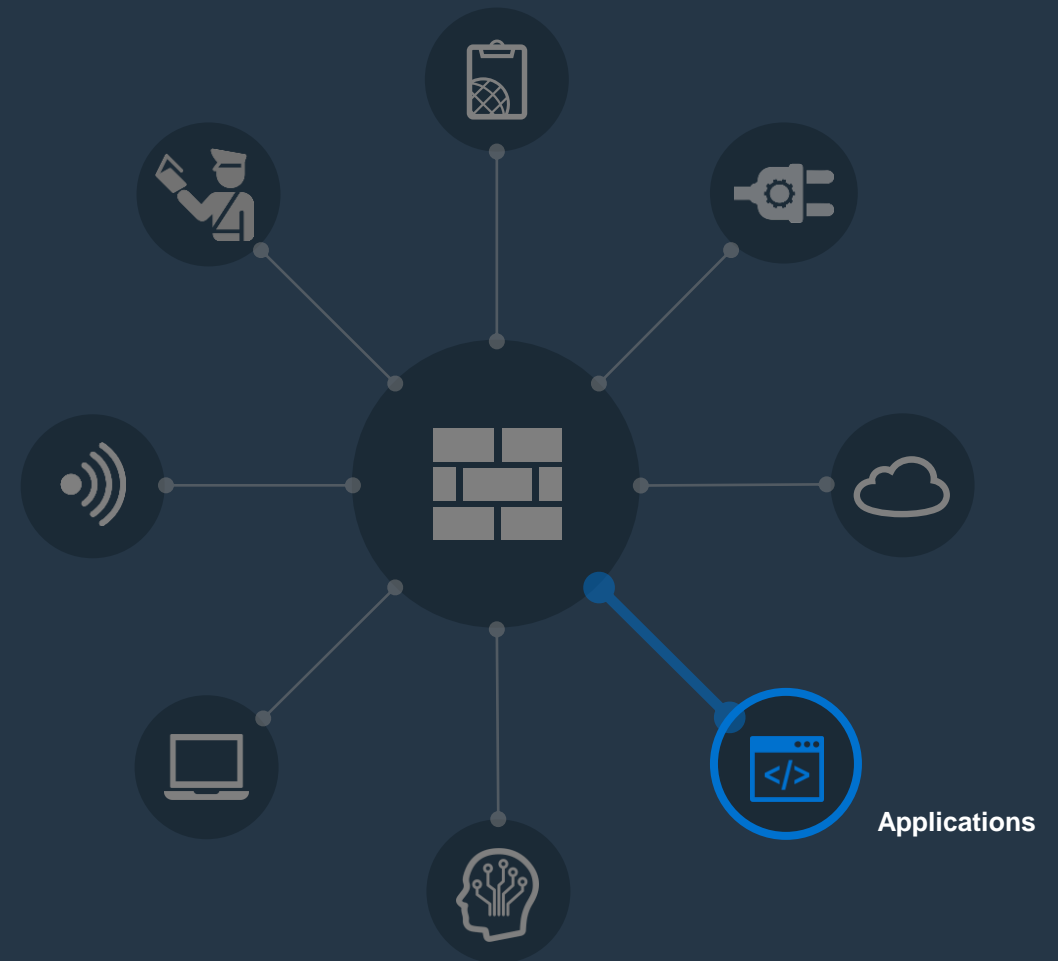
Защита веб-приложений и API от атак на уровне приложений

## Email Security

Обеспечение безопасного и подходящего обмена электронной почтой через облачные и локальные сети

## SaaS Security

Защита приложений SaaS от угроз и рисков





# Dynamic Cloud Security

## SaaS security

Риск неправильной конфигурации и отсутствия видимости быстро растет по мере ускорения внедрения SaaS.



FortiCASB

- Управление рисками неправильной конфигурации
- Видимость и контроль активности администраторов и пользователей SaaS
- Безопасность данных для файлов, хранящихся в SaaS-приложениях
- Комплаенс конфигураций SaaS-приложений



box



Office 365



Dropbox



salesforce

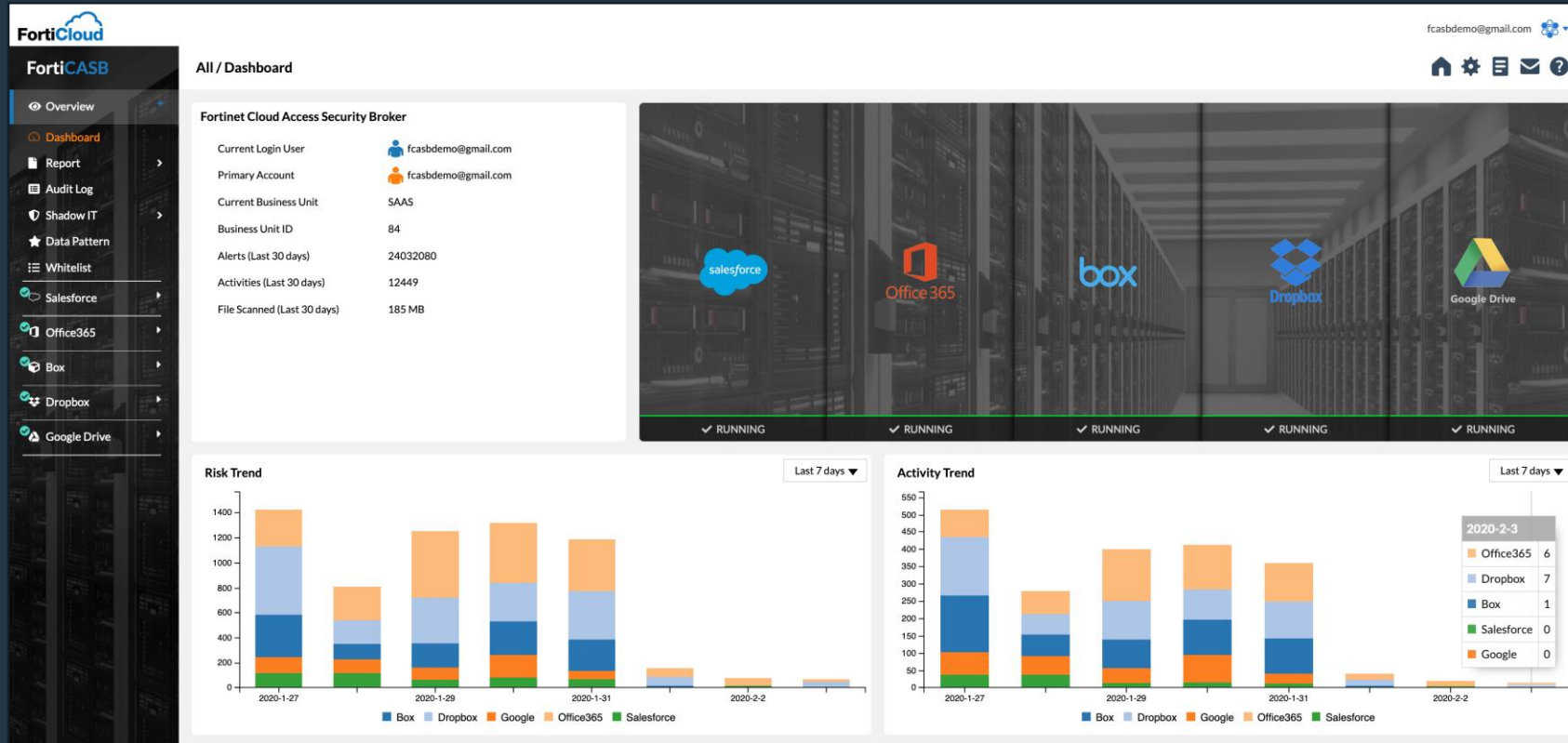


Applications

# Dynamic Cloud Security: FortiCASB GUI



## SaaS security

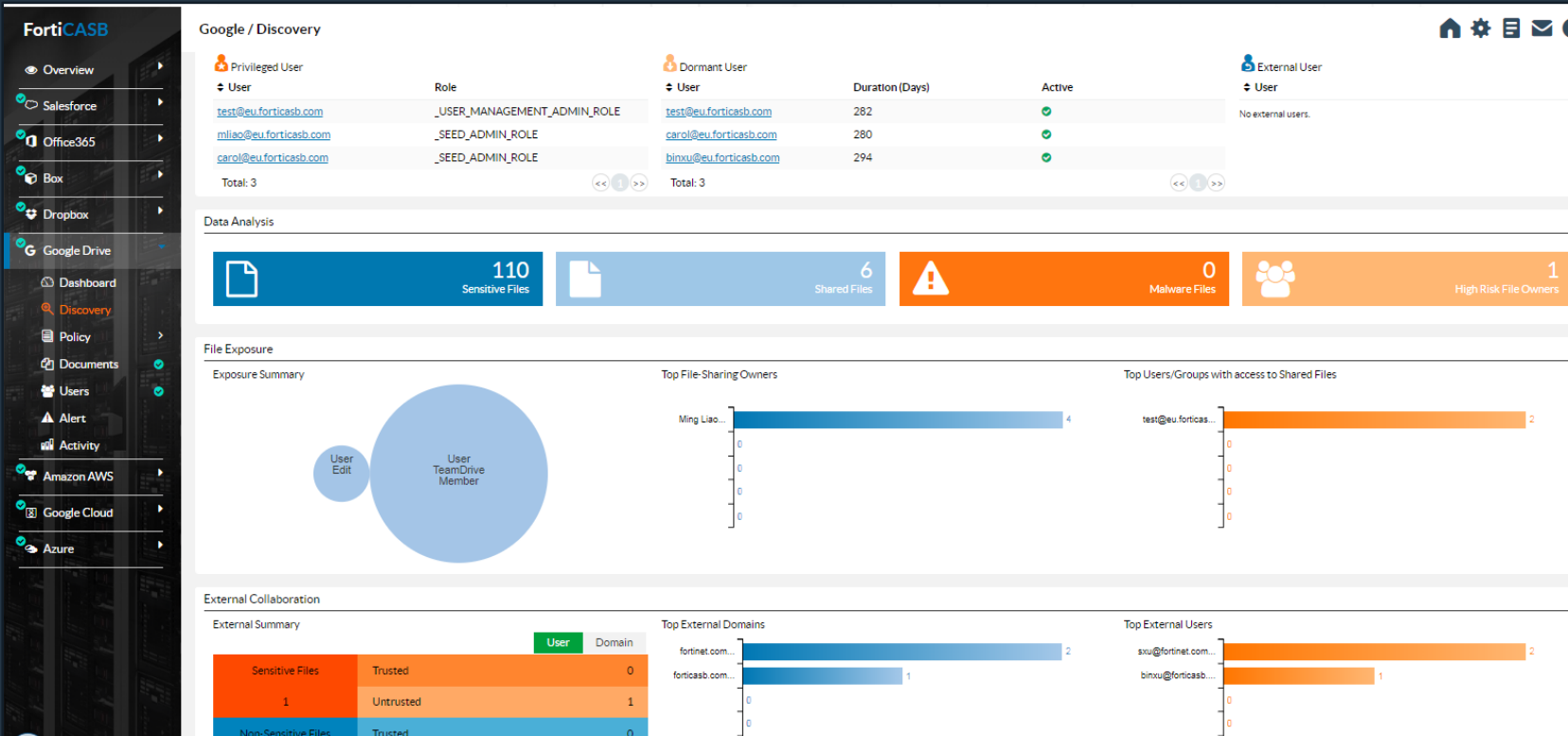


- Веб-портал управления
- Элементы управления для каждого поддерживаемого приложения SaaS
- Панели мониторинга помогают быстро определять риски
- Расширенная отчетность и показатели
- Упрощенное, «за считанные минуты» развертывание

# Dynamic Cloud Security: FortiCASB GUI



- DLP-сканирование
- Анализ вредоносных программ с антивирусным сканированием
- Анализ использования и разрешений для документов и пользователей
- Видимость и контроль совместной работы с файлами
- Политики защиты от угроз, подозрительная активность - кто, когда, где
- И не только



# Dynamic Cloud Security: отчет Shadow IT



FortiGate



FortiCASB

- Импорт и объединение Санкционированных и Несанкционированных SaaS-данных **FortiAnalyzer** и **FortiGate** с **FortiCASB**
- Консолидированная панель управления **FortiCASB** с расширенными инструментами анализа и отчетностью
- Полный отчет **Shadow IT** с обзором рисков и дашбордами
- Расширение инструментария **FortiAnalyzer** путем добавления обширной базы данных приложений в **FortiCASB**
- Автоматическое или «по запросу» получение feed-данных от **FortiAnalyzer** и **FortiGate**





# Dynamic Cloud Security

## Web application and API Security

Поскольку для работы предприятия все больше полагаются на веб-приложения, потребность в защите бизнес-приложений продолжает расти.



FortiWeb

### Защита веб-приложения от:

- Уязвимости и известные угрозы
- Гарантии безопасности с поддержкой ML

### Безопасность API

- Проверка схемы, безопасность OpenAPI
- Предотвращение активности ботов (scraping, analytics)



WORDPRESS



django



Joomla!



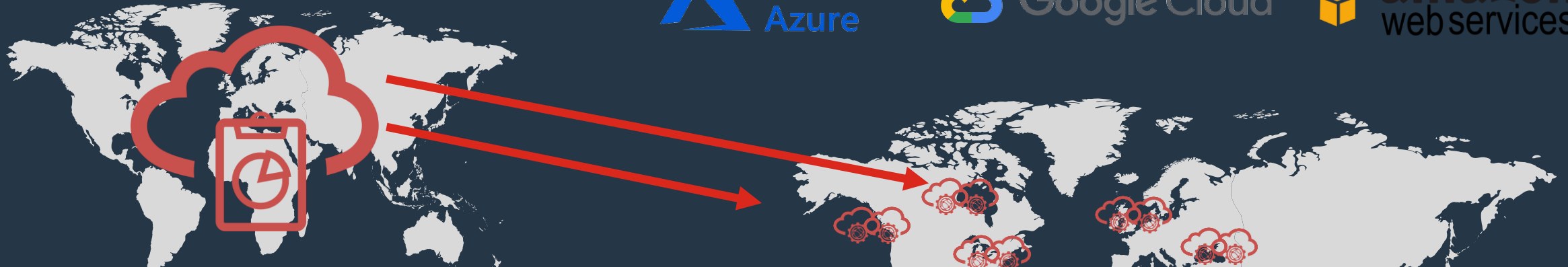
Applications



# Dynamic Cloud Security: FortiWeb as a Service



Web application and API Security



**FORTINET**  
FortiWeb Cloud

Applications

+ Add Filter

+ ADD APPLICATION

Name	Domain Name	Platform	Region	DNS Status	Blocked Requests	Requests	Data	Block Mode	Action
WAAS Demo on Microsoft Azure	azure.fortiwelclouddemo.com	Azure	CDN	✓ OK	268	216 k	797 MB	ON	
WAAS Demo	www.fortiwelclouddemo.com	AWS	US East (N. Virginia)	✓ OK	249	123 k	197 MB	ON	
Total this month					517	339 k	994 MB		

Showing 1 to 2 of 2 entries

20 FIRST PREVIOUS 1 NEXT

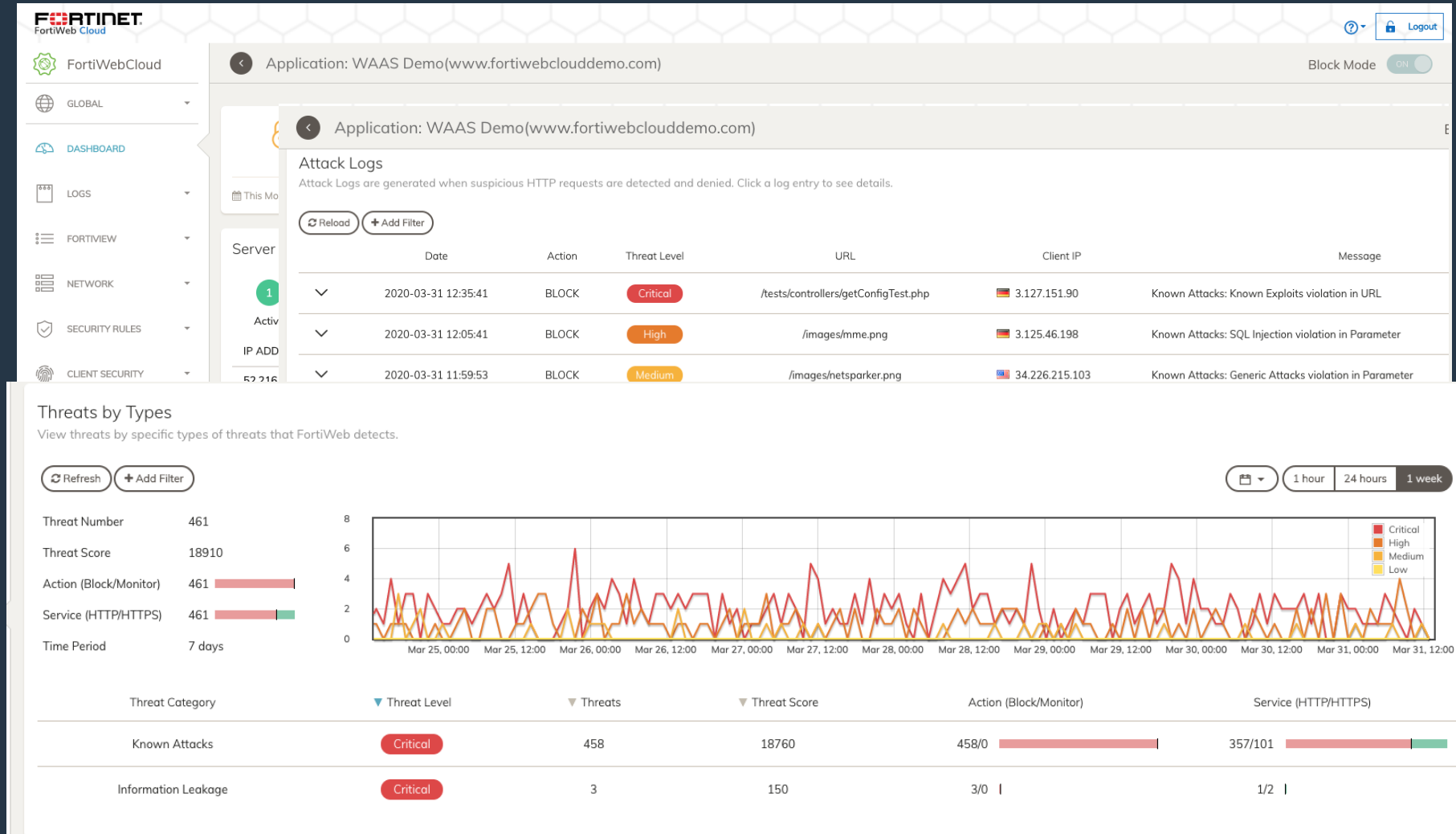
# Dynamic Cloud Security: FortiWeb as a Service



## Web application and API Security

Защитите свои размещенные веб-приложения без развертывания инфраструктуры и управления ею – позвольте Fortinet защитить ваши приложения, а Вы сосредоточитесь на предоставлении бизнес-ценности с помощью своих веб-приложений.

Решение требует минимальной настройки и управления, и его можно развернуть перед Вашими приложениями, подписавшись на AWS Marketplace. В решении используются несколько методов защиты для быстрого и точного устранения угроз, позволяя при этом проходить обычному трафику.





# Dynamic Cloud Security: FortiMail

## Email security

Электронная почта остается критически важной функцией для бизнеса и, к сожалению, предпочтительным способом доставки для киберпреступников. Организации должны усилить контроль как локально, так и в облаке.



FortiMail

- Предотвращение доставки традиционных и сложных угроз
- Недопущение потери конфиденциальной информации
- Поддержка перехода на облачную электронную почту



Applications

# Dynamic Cloud Security

Email security



Cloud



Appliance



Virtual  
Machine



Hosted



Усовершенствованное решение для защиты от нежелательной почты и вирусов с обширными возможностями карантина и архивирования



Антиспам и антифишинг с самым высоким рейтингом



Независимо сертифицированная защита от расширенных угроз



Интегрированная защита данных



Управление корпоративного уровня



Высокопроизводительная обработка почты





# Zero-trust Network Access

## NAC

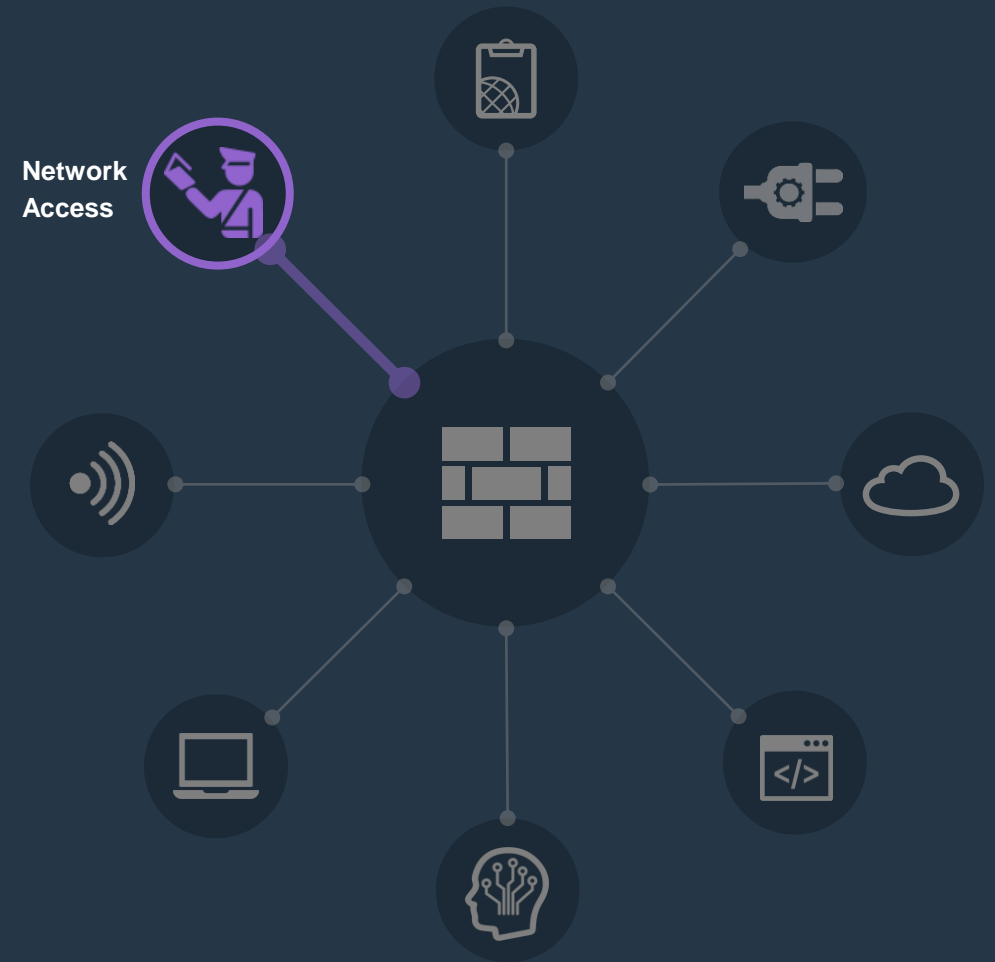
Знайте и контролируйте, что находится в Вашей сети

## Identity

Знайте и контролируйте, кто находится в Вашей сети

## Endpoint

Отслеживайте пользователей и устройства внутри и вне сети





# Zero-trust Network Access

Определите, *Что* находится в вашей сети

Быстрый рост устройств и IoT порождает угрозы. Организации развертывают NAC, чтобы снова обрести видимость.



FortiNAC

- Обнаружение всех устройств в сети
- Идентификация устройств
- Контроль на основе политик
- Непрерывный мониторинг и обнаружение аномалий



NAC

# Zero-trust Network Access: FortiNAC



Appliance



Virtual Machine



Определите, *Что* находится в вашей сети



Обеспечивает видимость пользователей и конечных точек для корпоративных сетей и автоматизирует реагирование на угрозы



Идентификация устройства и профилирование

Непрерывное профилирование устройства



Упрощенный гостевой доступ с самостоятельной регистрацией



Постоянная оценка рисков



Микросегментация конечных точек



Автоматизированное реагирование на выявленные риски



Оркестрация сторонних устройств

Add Filter: Select Update

Ports - Displayed: 26 Total: 26

<< first < prev 1 next > last >> 300

Status	Device	Label	Name	IP Address	Connection State	Default VLAN	Cu
	SwitchBuilding-1	F0/1	SwitchBuilding-1 Fa0/1	172.27.2.2	Rogue Host	502	504
	SwitchBuilding-1	F0/2	SwitchBuilding-1 Fa0/2	172.27.2.2	Not Connected	502	502
	SwitchBuildino-1	F0/3	SwitchBuildino-1 Fa0/3	172.27.2.2	Not Connected	502	502

Export to:

Options Hide Details Panel

Adapters Port Changes

Adapters - Total: 1

Status	Host Status	IP Address	Physical Address	All IPs	Location	Media	Access Value	D
		172.27.2.4	34:E6:D7:3D:3A:6E	172.27.2.4 (IPv4)	SwitchBuilding-1 Fa0/4		504	D

1. Пользователь приносит на работу зараженный ноутбук

2. FG1 отправляет событие на FortiNAC

3. FortiNAC помещает ноутбук в карантин на уровне доступа

4. Virus contained at switch node

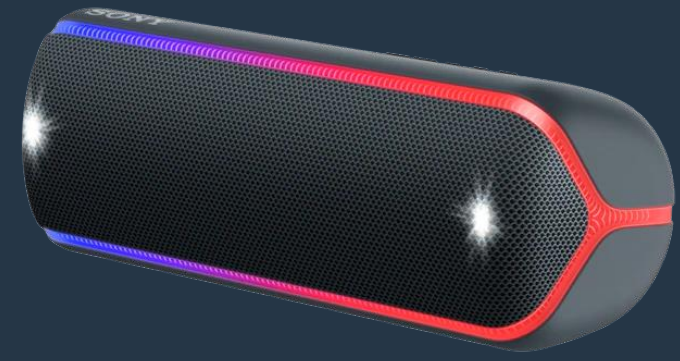
# Zero-trust Network Access: FortiNAC



Определите, *Что* находится в вашей сети

- **Kash's Sony Speaker**

- (у которого, как он даже не подозревал, есть беспроводной интерфейс)



- FortiOS

Device List	Windows Phone (1)			
Custom Devices & Groups	Offline	Windows-Phone	10.1.2.54	Windows Phone
Device List	Unknown OS (8)			
Single Sign-On	Online	RingPro-e9	10.1.2.69	
LDAP Servers	Offline	50:33:8b:fa:d0:26	10.1.2.70	
RADIUS Servers				

- FortiNAC

» Узнал только через DHCP Fingerprint

Status	IP Address	Physical Address	Media Type	Location	Actions
	10.1.2.70	50:33:8B:FA:D0:26		NAC-Default	

Wireless Access Point  
Sony embedded|Planet embedded|Bose embedded|USRobotics embedded|Denon embedded|Virdi embedded|D-Link embedded|Yamaha embedded|KCorp embedded

07/15/18 11:43 PM GMT+0100





# Zero-trust Network Access

Определите, *Кто* находится в вашей сети

Слабые пароли и украденные учетные данные делают сети уязвимыми. Требуются строгая проверка подлинности и доступа на основе ролей.



FortiAuthenticator



FortiToken

- Аутентификация пользователя
- Доступ и контроль на основе ролей (RBAC)

Двухфакторная аутентификация



Identity

# Zero-trust Network Access: FortiAuthenticator



Определите, *Кто* находится в вашей сети



## Управление идентификацией, контроль доступа пользователей и многофакторная идентификация



Прозрачная идентификация пользователей сети и применение политик на основе идентификации в корпоративной сети с поддержкой Fortinet



Бесшовная двухфакторная аутентификация / OTP в рамках всей организации в сочетании с FortiToken



Управление сертификатами для развертывания корпоративной беспроводной сети и VPN



Управление гостевым доступом для обеспечения безопасности проводных и беспроводных сетей



Возможности единого входа (SSO) для внутренних и облачных сетей



Add RADIUS client

Name: FortiGate-1

Client address:  IP/Hostname  Subnet  Range  
172.20.120.142

Secret:

First profile name: Default

Description:

Apply this profile based on RADIUS attributes.

EAP types:  EAP-GTC  EAP-TLS  PEAP  EAP-TTLS

Device Authentication

MAC Authentication Bypass(MAB)

AD machine authentication

MAC device filtering

User Authentication

Authentication method:  Enforce two-factor authentication  Apply two-factor authentication if available (authenticate any user)  Password-only authentication (exclude users without a password)  FortiToken-only authentication (exclude users without a FortiToken)

Enable Token Mobile push notifications authentication

Username input format:  username@realm  realm\username  realm/username

Realms:

Default	Realm	Allow local users to override remote users	Use Windows AD domain authentication	Groups	Delete
<input checked="" type="radio"/>	local   Local users	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> Filter: employees [Edit] <input type="checkbox"/> Filter: local users: [Edit]	<input type="checkbox"/>

[Add a realm](#)



# Zero-trust Network Access: FortiToken

Определите, *Кто* находится в вашей сети

384629

## Oath Compliant Time Based One Time Password Token



Масштабируемое решение для строгой аутентификации с низкими начальными затратами и низкой совокупной стоимостью владения (TCO)



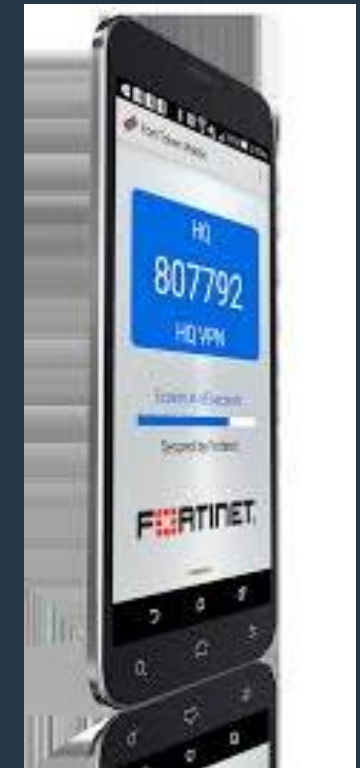
Уникальный упрощенный вариант онлайн-активации



Снижение эксплуатационных расходов за счет использования существующего FortiGate в качестве сервера аутентификации



Большой, легко читаемый ЖК-дисплей





# Zero-trust Network Access

Отслеживайте пользователей и устройства внутри и вне сети

Современный цифровой бизнес требует, чтобы сотрудники работали в любое время, в любом месте и практически на любом устройстве. Endpoint agent должен обеспечивать видимость и контроль.



- Видимость конечной точки
- Динамический контроль доступа

# Zero-trust Network Access: FortiClient



Отслеживайте пользователей и устройства внутри и вне сети



**Комплексная защита конечных точек и обеспечение безопасности**



Широкая видимость конечных точек



Соответствие конечных точек и управление уязвимостями



Проактивная защита конечных точек



Автоматическое сдерживание угроз



Безопасный удаленный доступ



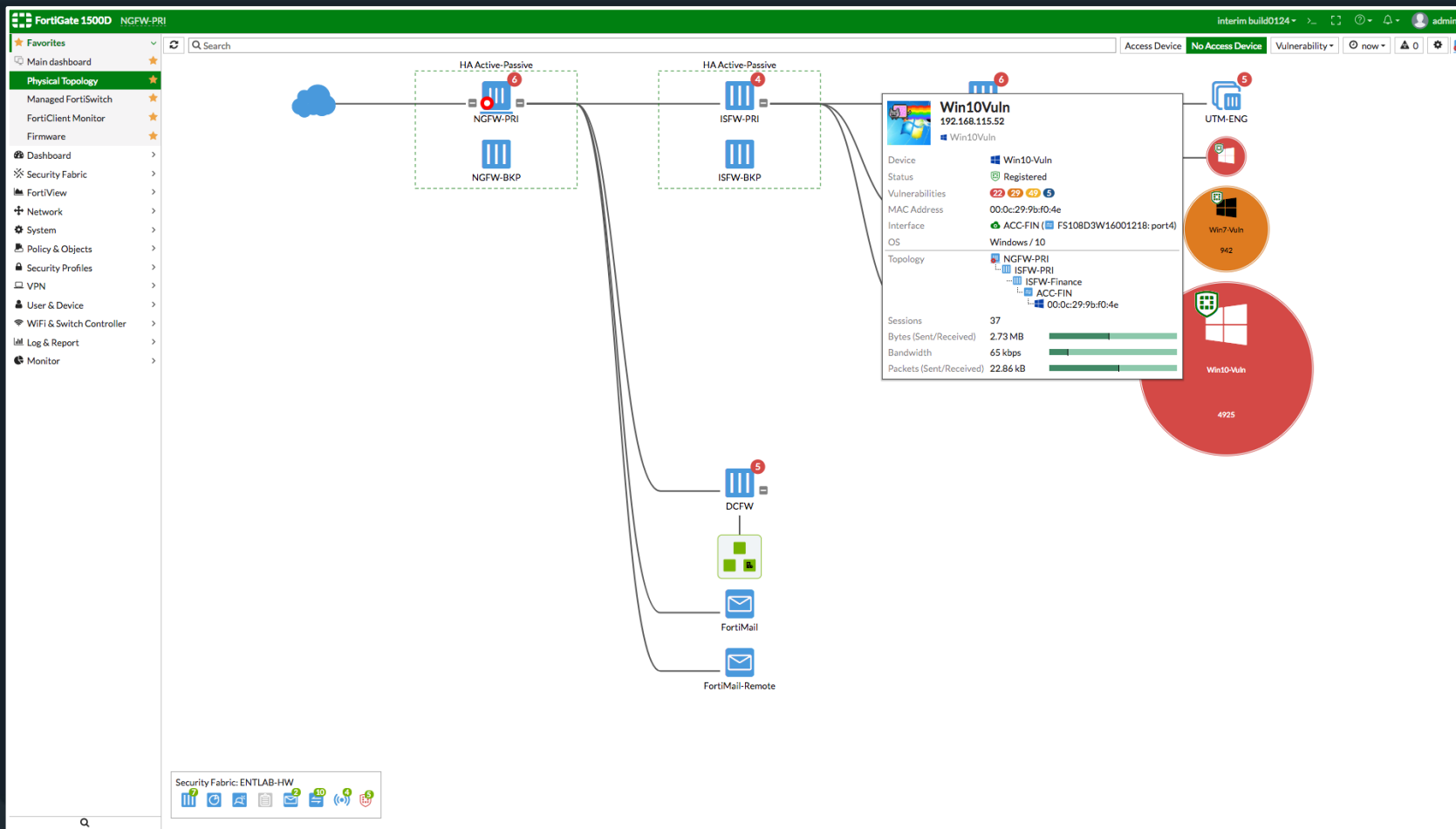
Легко развернуть и управлять



# Zero-trust Network Access: FortiClient



Отслеживайте пользователей и устройства внутри и вне сети



- Device information
  - OS
  - Co-relate multiple MAC
- FortiClient Status
- Endpoint Vulnerabilities
- Logged-in User
- User Avatar
- Social IDs
- Online/Off-line
- Endpoint events and logs

Видимость рисков в контексте сети  
Сбор данных о конечной точке



# AI-driven Security Operations

## Прогнозирование и предотвращение атак

Глобальное машинное обучение для проактивной защиты

## Обнаружение неизвестных и внутренних угроз

Специальное машинное обучение для раннего предупреждения

## Оркестрация и автоматизация реагирования

Экспертные системы для более быстрого сдерживания





# Прогнозирование и предотвращение атак

Глобальное машинное обучение для проактивной защиты

Устаревшие продукты безопасности отстают от постоянно меняющегося ландшафта угроз. Требуются технологии нового поколения, глобальный интеллект и аналитика, а также защита на основе искусственного интеллекта.



FortiGuard  
Services



Advanced  
Threats



Intrusion  
Prevention



Application  
Control



Cloud  
Sandbox



Security  
Rating



Antispam



Web  
Filtering



Botnet  
Protection



UEBA



Indicators of  
Compromise

Zero Trust Network  
Access

Two-Factor  
Authentication

Dynamic Cloud  
Security







# Прогнозирование и предотвращение атак : FortiGuard

Глобальное машинное обучение для проактивной защиты

## Fortinet Threat Research

- Анализ вредоносного ПО и URL
- Анализ текущих угроз
- Исследование нулевого дня

## Development

- Антивирусный движок
- Механизм предотвращения вторжений
- Разработка сигнатур

## Innovation

- Автоматизация аналитических задач
- Отслеживание новшеств
- Использование новых технологий



SECURED BY  
**FORTIGUARD**®

## Customer Service

- Создание сигнатур
- Категоризация URL
- Первоклассный сервис

# Прогнозирование и предотвращение атак : FortiGuard



Глобальное машинное обучение для проактивной защиты

Остановка угроз  
«на лету»

Advanced Malware Protection



- Advanced Threat Protection
- Antivirus
- Intrusion Prevention

Устранение атак  
на общих точках  
входа

Content Security



- Web Filtering
- AntiSpam
- Content Disarm & Reconstruct

Проактивное  
предотвращение и  
обнаружение  
нарушений  
Advanced Detection



- Security Rating
- Vulnerability Management
- Indicators of Compromise

Безопасность  
расширенной  
поверхности атаки  
Application & IoT Security



- Application Control
- Web Application
- Industrial Security

## FortiGuard AI-Driven Protection and Intelligence

Обеспечение Security Fabric лучшей защитой, доступной в FortiGuard Services

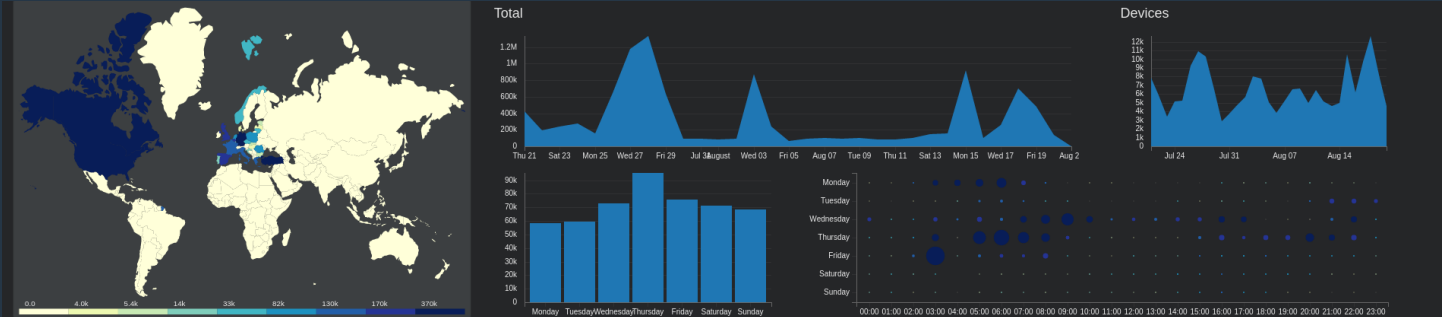


# Прогнозирование и предотвращение атак : FortiGuard

## Глобальное машинное обучение для проактивной защиты

### Видимость

- Глобальная сеть сенсоров
- 4,4 миллиона устройств отправляют отчеты ежедневно
- Согласованная сеть раннего предупреждения

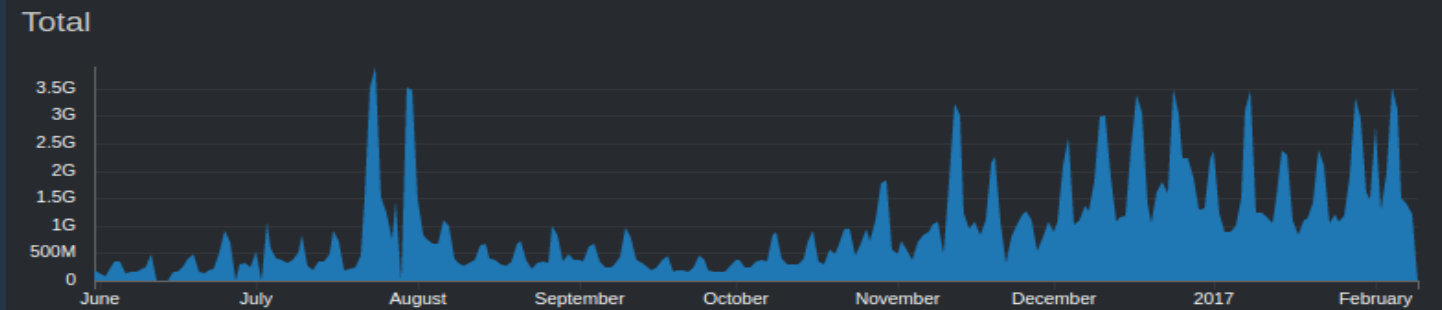
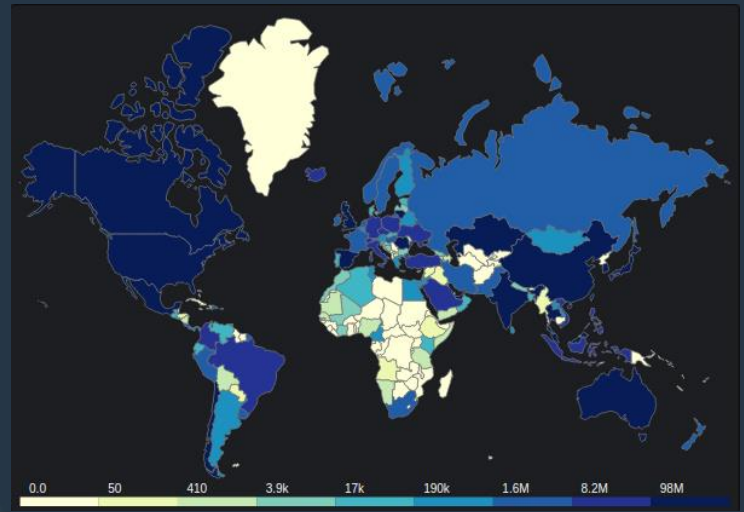


Region Name	FG Count	Total
Asia	4,400,000	4,400,000
North America	38,388	8,070,291
Europe	11,471	3,187,615
Africa	521	461,738
South America	1,487	305,924
Oceania	802	177,982
Region 1	759	169,107

Country Code	Country	FG Count	Total
US	United States	38,156	7,165,008
TR	Turkey	1,183	611,004
CA	Canada	1,375	409,926
DE	Germany	1,558	365,218
ES	Spain	736	261,270
BE	Belgium	556	231,435
GB	United Kingdom	802	172,319
GR	Greece	109	161,592
IT	Italy	733	130,122
FR	France	1,145	129,444

Name	FG Count	Total
JS/Nemucod.AN0!tr	4,229	1,222,870
JS/Nemucod.AOT!tr	6,873	854,760
WM/Agent.BJ3Ctr.dldr	10,340	851,746
WM/Agent.BOJ!tr.dldr	6,945	765,617
HTML/Refresh.BC!tr	6,917	670,939
JS/Nemucod.DRY!tr.dldr	4,845	610,478
JS/Nemucod.25A0!tr.dldr	5,525	552,970
WM/Agent!tr	5,731	518,566
JS/Nemucod.0971!tr	2,548	367,988
Adware/AdExchange	7,893	230,832

Serial ID	Unique Names	Total
11914	288	158,740
16851	30	150,688
44597	6	112,456
1683036	21	110,820
16741	8	108,568
220740	7	106,719
686	17	103,348
1712873	8	101,867
13025	12	101,853
13922	9	100,723



# Прогнозирование и предотвращение атак : FortiGuard



Глобальное машинное обучение для проактивной защиты



Antivirus



Intrusion Prevention



Web Filtering



Anti-spam



Anti-Botnet



FortiGate



FortiMail

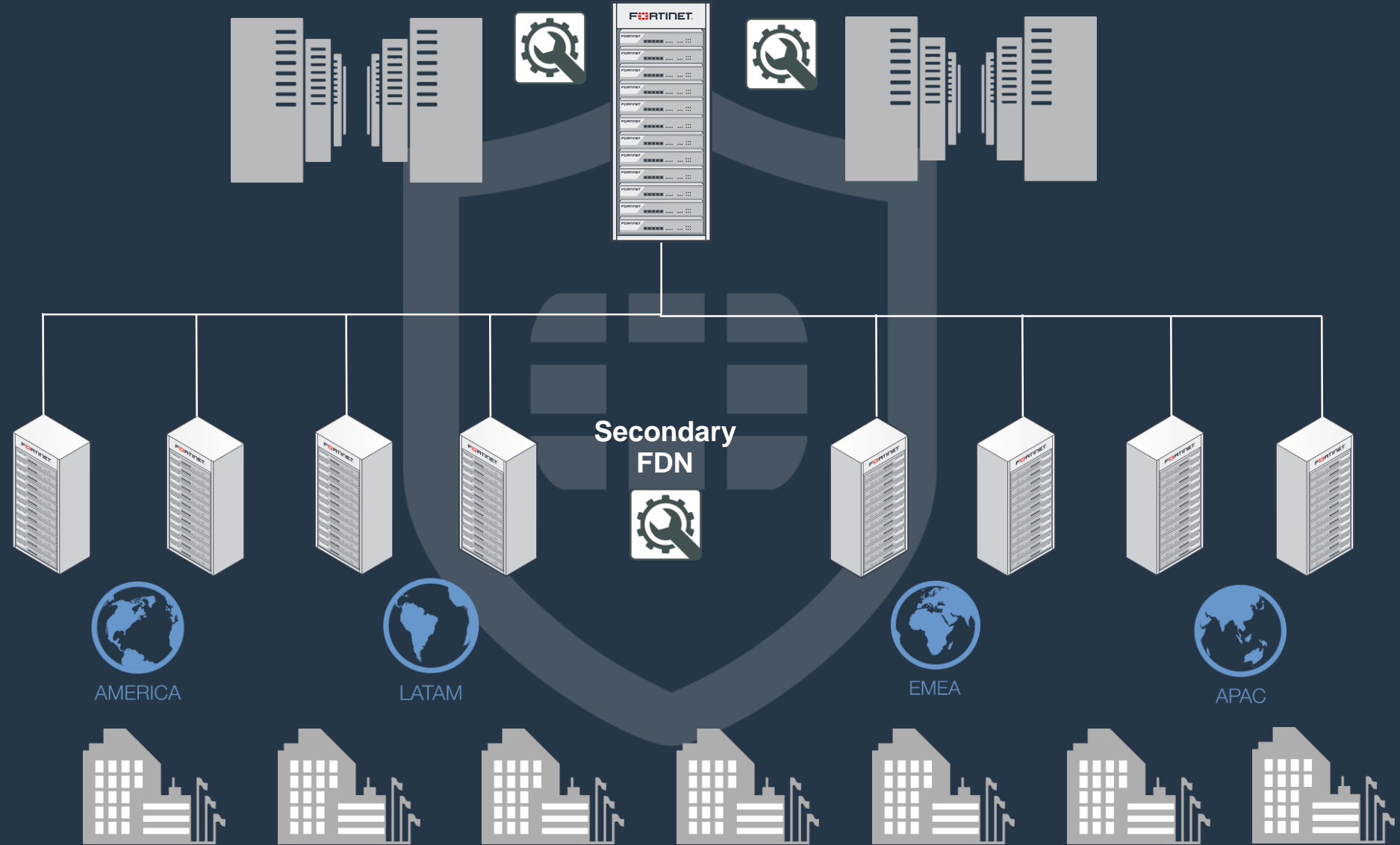


FortiClient



FortiSIEM

FORTINET



# Прогнозирование и предотвращение атак : FortiGuard



Глобальное машинное обучение для проактивной защиты

## NGFW IPS Signatures

- MS.SMB.Server.SMB1.Trans2.Secondary.Handling.Code.Execution (CVE-2017-0144)
- Backdoor.DoublePulsar (Application Control)

## NGFW AV Signatures

- W32/GenKryptik.1C25!tr
- W32/Filecoder\_WannaCryptor.B!tr
- W32/Wanna.A!tr
- W32/WannaCryptor.B!tr
- и другие варианты открывались каждый час

## NGFW Web Filtering & IOC

- Против динамических вредоносных сайтов

## NGFW Botnet C&C & DNS

- Detect/Block, Report and Protect

## Example - WannaCry Protection

**28C25239\_cry.v9a**

Job ID	3345054712729979237
Reclved	May 13 2017 13:36:48
Status	Done
Rating	High Risk
Suspicious Type	Unknown
Rated By	VM Engine
Submit Type	On-Demand
Scan Bypass	Static Scan,AV Scan,Cloud Query
Packers	Microsoft Visual C++ v6.0
File Type	exe
File Size(Bytes)	3514368
Download From	28C25239_cry.v9a
MD5	509c41ec97bb81b0567b059aa2f50fe8
SHA1	87420a2791d18dad3f18be436045280a4cc16fc4
SHA256	09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
Submitted By	eNpLTMnNzAMABgECCg==
Submitted Filename	28C25239_cry.v9a
Filename	28C25239_cry.v9a
Start Time	May 13 2017 13:36:51
Detection Time	May 13 2017 13:43:15
Scan Time(Sec)	384
Detection OS	WIN7X64VM
Infected OS	WIN7X64VM
Comments	wantacry

**Behaviors for WIN7X64VM**

**Behavior Summary**

- This file rated by Cloud-based Threat Intelligence
- This file dropped files
- This file modified files
- This file deleted files
- This file spawned process(es)

**Behavior Details**

**Suspicious Behaviors(5)**

- ⚠ Virus detected
- ⚠ Ransomware like behaviors were detected
- ⚠ Threat\_Intelligence
- ⚠ The executable tried to hide a file/directory
- ⚠ The executable create files in sensitive directories

Threat_Intelligence	%currentpath%\t.wnry	1c4bfd877e58eae3ac4d35109a9b13	5dcaac857e695a65f5c3ef1441a73a8f	Threat_Intelligence
W32/Agent.AAPW!tr	%currentpath%\taskld.exe	e09ade083b0e2fa162e09d0001cbbdcc	4fe5e34143e646dbf9907c4374276f5	Virus detected
W32/Zapchast.D!tr	%currentpath%\taskse.exe	cf24beb30086a6ba1b0dd5f6141ff043	8495400f199ac77853c53b5a3f278f3e	Virus detected
N/A	%currentpath%\u.wnry	1f219d338687d32c99c34bc1ce61b02d	7bf2b57f2a205768755c071238fb32cc	
N/A	%currentpath%\00000000.pky	e9b01fca24128afa6d6798d01f1133c26	03f1cb1545e07eabfd6318a882e4af0a	
N/A	%currentpath%\00000000.eky	N/A	N/A	
N/A	%currentpath%\00000000.res	46a7232072df7882df979cc9483e3b34	d699b921acffa6e06bb51ccd7ba1acd	
N/A	%currentpath%\@wanadecryptor@.exe	e3a0dfbd000b091d6f05bd3472837d08	7bf2b57f2a205768755c071238fb32cc	



# Обнаружение неизвестных и внутренних угроз

Специальное машинное обучение для раннего предупреждения

Растет понимание того, что 100%-ное предотвращение невозможно с учетом современных сложных угроз. Чтобы избежать взломов, организации вкладывают средства в расширенные возможности обнаружения.



FortiDeceptor



FortiSandbox



FortiInsight

Выявление неизвестных противников

Обнаружение неизвестного вредоносного ПО

Раскрытие риска инсайдера





# Обнаружение неизвестных и внутренних угроз : FortiDeceptor

Специальное машинное обучение для раннего предупреждения



## Автоматическое обнаружение внешних и внутренних угроз и реагирование на них



Карта угроз на основ интерфейса позволя обнаружить кампани нацеленные на вашу



Интеграция безопас инфраструктуру обес блокировку злоумыш реальном времени д будет нанесен реаль



Централизованное у автоматизация разв ловушек

The screenshot displays the FortiDeceptor 1000F web interface. The top navigation bar includes 'Dashboard', 'Decoy & Lure Status', 'Analysis', and 'Decoy Map'. A sidebar menu on the left lists various sections: Deception, Incident, Analysis, Campaign, Attack Map, Fabric, Network, System, and Log. The 'Decoy Map' view is active, showing a network diagram with nodes labeled 'Finance-Scada', 'Finance-Win10', 'Finance-Linux', 'Ubuntu', and 'Engineering'. The interface also features a search bar and a 'FILTER CURRENT VIEW' section.

# Обнаружение неизвестных и внутренних угроз : FortiSandbox



## Специальное машинное обучение для раннего предупреждения

**Автоматизированное обнаружение и устранение вредоносных программ нулевого дня с расширенными возможностями**

FortiSandbox, инструмент исследования и отчетности, основанный на Mitre ATT&CK, предоставляет подробный отчет об анализе, в котором методы обнаруженных вредоносных программ сопоставляются с платформой Mitre ATT&CK, со встроенными мощными инструментами расследования, которые позволяют группе Security Operations (SecOps) загружать захваченные пакеты, исходный файл, журнал трассировки, скриншот вредоносной программы и IOС, совместимые с STIX 2.0, которые не только предоставляют подробные сведения об угрозах, но и дают полезные сведения после проверки файлов

The screenshot displays the FortiSandbox dashboard for a device named '3000D'. It includes sections for System Information, Threats Distribution (Last 7 Days), and Scanning Statistics (Last 7 Days). A prominent red alert banner indicates a 'High Risk Dropper' (WIN7X86VM) with various indicators and a MITRE ATT&CK Matrix.

Rating	Sniffer	Device(s)	On Demand	Network	Adapter	URL	All
Malicious	0	1,264	0	0	0	0	1,264
Suspicious - High Risk	0	439	0	0	0	0	441
Suspicious - Medium Risk	0	105	0	0	0	0	105
Suspicious - Low Risk	0	209	9	0	0	0	218

**High Risk Dropper Indicators (14):**

- This file prevented autostart registry from being deleted
- The executable tried to create a process with critical flag which might cause BSOD when process is terminated
- The file tries to bypass firewall
- Executable dropped a copy of itself in high risk path
- The file dropped suspicious file(s) to the startup folder
- This file applied low suspicious autostart registry modifications to start itself automatically
- Executable dropped a copy of itself
- Suspicious file, %appdata%\microsoft.exe installed in system folder
- This file writes data which contains an executable to process memory
- The executable had no visible window
- The executable tries to spawn process of itself
- The file escalated the privilege to SeDebugPrivilege
- The file escalated the privilege to SeDebugPrivilege
- The file escalated the privilege to SeDebugPrivilege

**MITRE ATT&CK Matrix (16):**

Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement
				Hidden Window (1)			
				Disabling Security Tools (2)			
				Masquerading (1)			
	Execution through API (2)	Registry Run Keys / Start Folder (3)	Hooking (3)	Process Injection (2)			Replication Through Removable Media (2)

**FSA** будет иметь возможность выявлять и анализировать угрозы с использованием виртуальных машин для запуска кода эмуляции на основе платформы MITRE ATT&CK.







# Обнаружение неизвестных и внутренних угроз : FortiInsight

## Специальное машинное обучение для раннего предупреждения

**AI Alerts**

Policy Alerts AI Alerts

From: 2018-04-05 14:12:16 To: 2018-04-12 14:12:16

Users

acm

acm

acm

Show:  Expand  Severity  Time (UTC)  Tags  User Name  Application  Activity

Previous 1 Next

Expand	Severity	Time (UTC)	Tags
	42	09/04/2018 17:17:11	
	30	11/04/2018 14:38:54	
	44	11/04/2018 21:11:47	NFS READ
	30	11/04/2018 06:24:01	
	34	12/04/2018 08:43:23	

**Policy Alerts**

Policy Alerts AI Alerts

From: 2018-04-05 14:03:55 To: 2018-04-12 14:03:55

Export to CSV

Users Entities Labels Policies

Username	Alerts
acmeltd_temp1	68
acmeltd_engineer2	39
acmeltd_contractor1	22
acmeltd_engineer3	5

Show:  Expand  Severity  Time (UTC)  Labels  Framework  Policy Name  Endpoint  User  Application  Resource

Search returns: 138 Alerts

Previous 1 2 Next

Expand	Severity	Time (UTC)	Labels	Framework	Policy Name	Endpoint	User	Application	Resource
	10	12/04/2018 13:02:40	Removable Media Use	ISO27001	Removable Media Audit	uqP	acmeltd_engineer2	bbackup.exe	rm:\\e
	10	12/04/2018 13:02:35	Removable Media Use	ISO27001	Removable Media Audit	uqP	acmeltd_engineer2	bbackup.exe	rm:\\e
1 more	10	12/04/2018 13:01:52	Removable Media Use	ISO27001	Removable Media Audit	uqP	acmeltd_engineer2	bbackup.exe	rm:\\e
1 more	10	12/04/2018 09:11:13	<none>	GDPR	Uploads of sensitive data to non -EEA countries	uqP	acmeltd_engineer2	chrome.exe	c:\\use
1 more	50	12/04/2018 09:02:27	Sensitive Data	GDPR ISO27001	Demo Policy	z99	acmeltd_temp1	explorer.exe	c:\\use



# Оркестрация и автоматизация реагирования

Экспертные системы для более быстрого сдерживания

Учитывая нехватку навыков кибербезопасности, организации стремятся координировать и все более автоматизировать усилия по расследованию / реагированию.



FortiAnalyzer

Аналитика  
Security Fabric



FortiSIEM

Мультивендорная  
видимость



FortiSOAR

Управляемый  
ответ



FortiAI

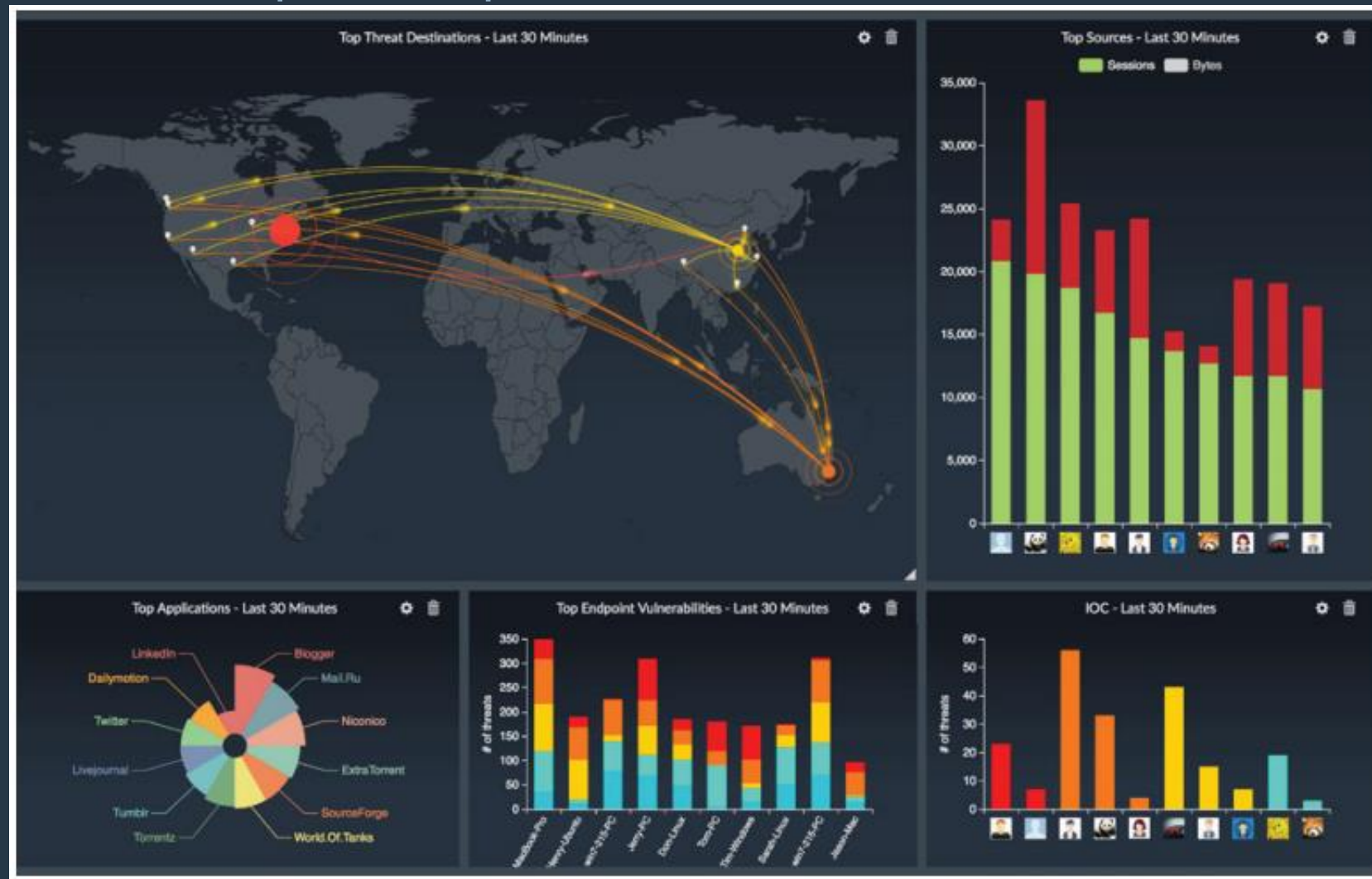
Виртуальный  
аналитик





Экспертные системы для более быстрого сдерживания

- Автоматизированное управление журналами и анализ угроз в реальном времени
- Непрерывная отчетность для предприятий
- Упрощенная форензика и быстрое реагирование

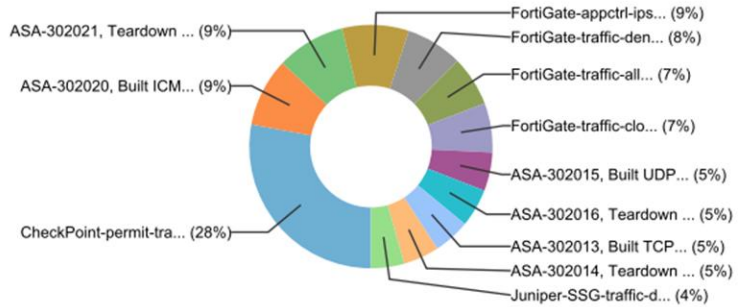


# Оркестрация и автоматизация реагирования : FortiSIEM

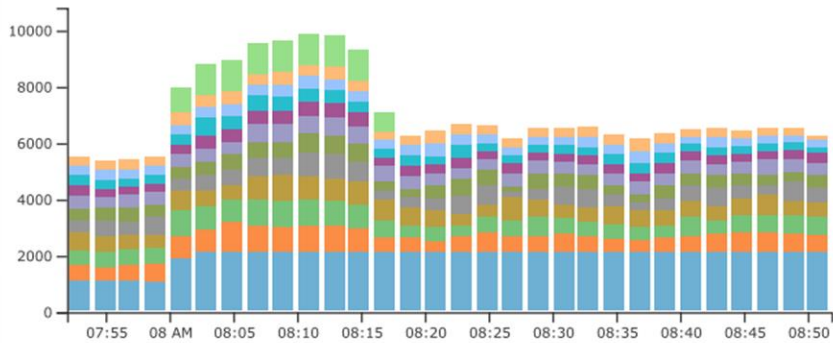


## Экспертные системы для более быстрого сдерживания

Donut Chart - Firewall Event Types



Trend Bar Chart - Firewall Event Types



- CheckPoint-permit-traffic, Permitted IP traffic by policy
- ASA-302020, Built ICMP connection
- ASA-302021, Teardown ICMP connection
- FortiGate-appctrl-ips-pass, FortiGate appctrl ips pass
- FortiGate-traffic-denied, Denied traffic
- FortiGate-traffic-allowed, Permitted traffic
- FortiGate-traffic-close, Session closed
- ASA-302015, Built UDP connection
- ASA-302016, Teardown UDP connection
- ASA-302013, Built TCP connection
- ASA-302014, Teardown TCP connection
- Juniper-SSG-traffic-deny, Denied network traffic

ция

ы

**FortiSIEM** DASHBOARD | ANALYTICS | INCIDENT | CASE | CMDB | RESOL

Security Dashboard | Perimeter | Access | Malware | Vulnerability | Exploits | Policy Violation

### Permitted Outbound Ports By Bytes

Last 1 hour@11:46

IP Protocol, Destination TCP / UDP Port	AVG(Total Bytes)	Trend
17 (UDP), 8888	30.61 KB	[Trend Line]
17 (UDP), 123 (NTP)	17.66 KB	[Trend Line]
6 (TCP), 443 (HTTPS)	1.87 KB	[Trend Line]
17 (UDP), 53 (DOMA...)	1.31 KB	[Trend Line]
6 (TCP), 80 (HTTP)	606.43 B	[Trend Line]
6 (TCP), 5587	131 B	[Trend Line]
6 (TCP), 3186	129 B	[Trend Line]
6 (TCP), 6100	129 B	[Trend Line]

### Permitted Inbound Ports By Bytes

Last 1 hour@11:46

IP Protocol, Destination TCP / UDP Port	AVG(Total Bytes)	Trend
6 (TCP), 45270	219.21 KB	[Trend Line]
6 (TCP), 45119	126.28 KB	[Trend Line]
6 (TCP), 45115	124.92 KB	[Trend Line]
6 (TCP), 45174	39.21 KB	[Trend Line]
6 (TCP), 16389	32.47 KB	[Trend Line]
6 (TCP), 16403	32.47 KB	[Trend Line]
6 (TCP), 16376	29.72 KB	[Trend Line]
17 (UDP), 4500 (IPS...)	19.02 KB	[Trend Line]

### Denied Internal Sources By Connections

Last 1 hour@11:46

192.168.200.12, HO...	[Bar]
172.16.22.137, HOS...	[Bar]
192.168.19.2, HOST...	[Bar]
192.168.88.16, HOS...	[Bar]
172.16.3.9, HOST-1...	[Bar]
192.168.89.2, HOST...	[Bar]
192.168.19.1, ph-n...	[Bar]
192.168.19.1, HOST...	[Bar]
172.16.22.100, HOS...	[Bar]
192.168.64.115, HO...	[Bar]

### Firewall Deny: Top Countries By Inbound Denies

Last 1 hour@11:48

Source Country	COUNT(Matched Events)
China	43
United States	42
Hong Kong	12
Vietnam	4
Seychelles	3
Chile	2
Russian Federation	2
Spain	1



# Оркестрация и автоматизация реагирования : FortiAI

Экспертные системы для более быстрого сдерживания угроз

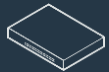
Хост, который был заражен в дату обнаружения (Detection Date), с указанием того, какое заражение произошло первым



Virtual Security Analyst™ на базе Neural Networks выявляет и классифицирует угрозы и обнаруживает вспышки вредоносных программ за доли секунды.



FortiAI  
Virtual Security Analyst™



Appliance

Integrates with



FortiGate

FortiAI 3500F FK-SVM0000000000

- Dashboard
- Security Fabric
- Attack Scenario
- Host Story

View All Host Story

10.10.10.23	342	2522	1186
10.10.10.53	13	22	24
172.16.92.175	11	10	9
10.10.10.51	7	19	25
10.10.10.56	6	21	19
10.10.10.54	5	15	17
172.17.45.105	5	1	3
10.10.10.55	4	20	14
10.10.10.70	4	10	9
10.10.10.37	4	10	2
10.10.10.63	4	3	3
10.10.10.52	3	27	16
10.10.10.43	3	10	6
10.10.10.35	3	8	3
10.10.10.49	3	4	5
10.10.10.36	3	3	5
10.10.10.57	2	15	10
10.10.10.77	2	11	6
10.10.10.75	2	9	7
10.10.10.80	2	9	3

Threat Investigation

Host story 10.10.10.70

Threat Level: High Risk, Medium Risk, Critical Risk

Scenario Type: Generic Trojan, Banking Trojan, Backdoor, Worm Activity, Ransomware, Data Leak

Device Type: Sniffer

Detection Date	Scenario Type	Virus Family	Device Type	Threat Level	Attack Chain
2020/02/21 05:15:32	Worm Activity	Generic	Sniffer	Critical Risk	PE/Worm/Generic
2020/02/21 05:15:23	Backdoor	Curioso	Sniffer	High Risk	PE/BackDoor/Curioso
2020/02/21 05:15:18	Generic Trojan	Downeks	Sniffer	Medium Risk	PE/Trojan/Downeks
2020/02/21 05:15:15	Generic Trojan	General	Sniffer	Medium Risk	PE/Trojan/General
2020/02/21 05:15:12	Backdoor	Hupigon	Sniffer	High Risk	PE/BackDoor/Hupigon
2020/02/21 05:15:08	Ransomware	Qukart	Sniffer	Critical Risk	PE/Ransomware/Qukart
2020/02/21 05:15:07	Generic Trojan	General	Sniffer	Medium Risk	PE/Trojan/General
2020/02/21 05:15:04	Banking Trojan	General	Sniffer	High Risk	PE/Banking Trojan/General
2020/02/21 05:15:00	Banking Trojan	General	Sniffer	High Risk	PE/Banking Trojan/General
2020/02/21 05:14:51	Generic Trojan	Scar	Sniffer	Medium Risk	PE/Trojan/Scar
2020/02/21 05:14:44	Banking Trojan	General	Sniffer	High Risk	PE/Banking Trojan/General
2020/02/21 05:14:42	Worm Activity	Ardurk	Sniffer	Critical Risk	PE/Worm/Ardurk
2020/02/21 05:14:41	Generic Trojan	General	Sniffer	Medium Risk	PE/Trojan/General
2020/02/21 05:14:40	Generic Trojan	General	Sniffer	Medium Risk	PE/Trojan/General

Details

Date: 2020/02/21 05:15:32  
Event Type: Worm Activity  
Attack Chain: PE/Worm/Generic  
MD5: afb32a5ed6ddb156dc7c886ae0d1f41  
Entry Date: 2020/02/21 05:15:32



# Оркестрация и автоматизация реагирования: FortiSOAR

Экспертные системы для более быстрого сдерживания

## SOC Management Platform

- Enterprise Case Management
- Role based Access
- Multi-Tenant



## Orchestration & Automation

- Playbooks
- Connectors/Integrations

### Управление кейсами

- OOB modules for Incident Response, Vulnerability Response and Fraud
- Build your own Modules (Ex, GDPR, Legal)
- Contextual Visualizations

### Упорядоченное реагирование

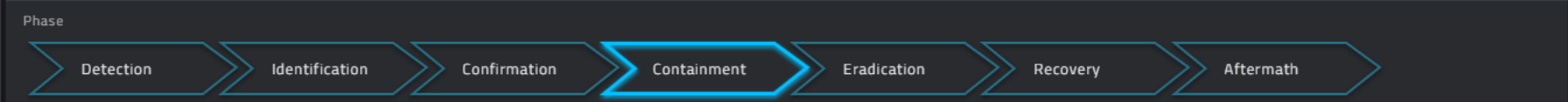
- Visual Playbook Designer
- 250+ Connectors for automated actions
- Real Life Use Case's Reference Content

### Мультитенантность

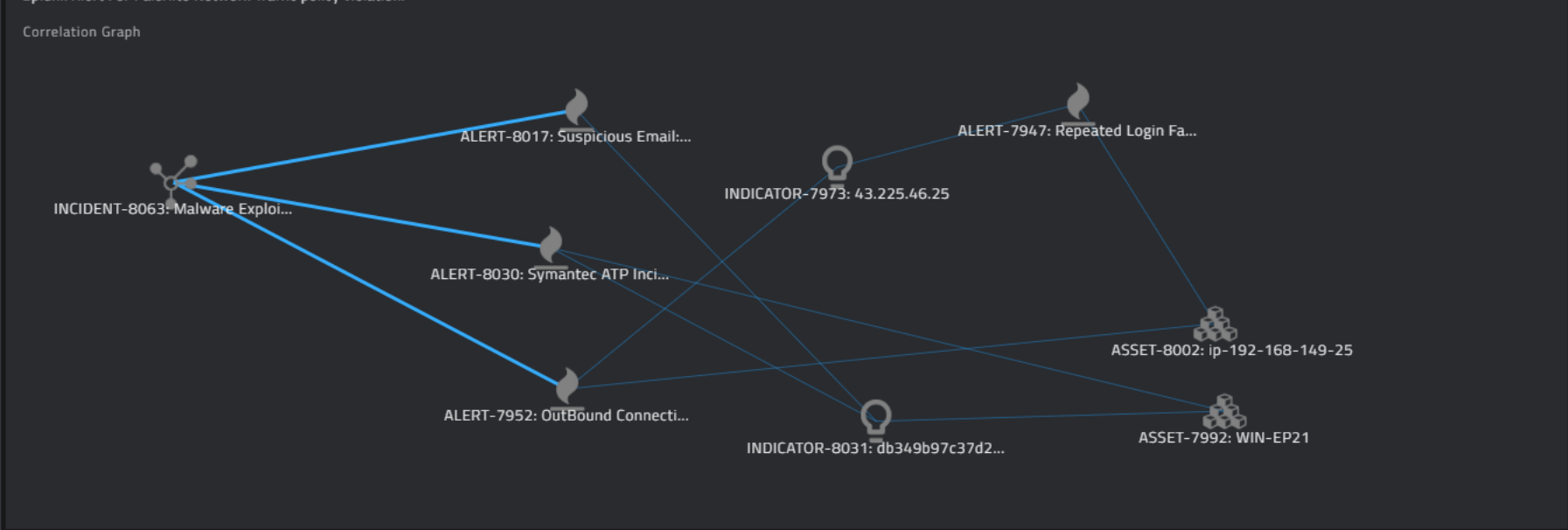
- Distributed/Federated Architecture
- Control Access to Data and Playbooks

Workbench > Incident

**HIGH** INCIDENT-8063 Malware Exploited Last Modified by Playbook on 03/11/2019 11:35 PM



Description  
Splunk Alert For PaloAlto Network Traffic policy violation.



Incident Lead <b>CS Admin</b>	Status <b>Open</b>	Source Paloalto	SLA
Campaign <b>Dummy Campaign</b>	Phase <b>Containment</b>		Created On 03/11/2019 11:22 PM
			Date Of Incident 03/10/2019 12:00 AM
			Discovered Date 03/12/2019 12:00 AM
			Resolved Date --

TYPE DETAILS  
Type: **Other**

OBSERVABLES | RELATED RECORDS | TASKS | ATTACHMENTS | ACCESS CONTROL | AUDIT LOG

EXECUTE ACTIONS

GENERATE INCIDENT SUMMARY REPORT
EXECUTE
EDIT RECORD
EXPORT
DELETE

**Visual Correlation:**  
full view of Incident to Alerts to Assets to Vulnerabilities to Users

**CS ADMIN**  
Requesting Block IP for 43.225.46.25  
LESS THAN A MINUTE AGO

Rich text editor toolbar with icons for Bold, Italic, Underline, Strikethrough, Bulleted List, Numbered List, Link, and Unlink.

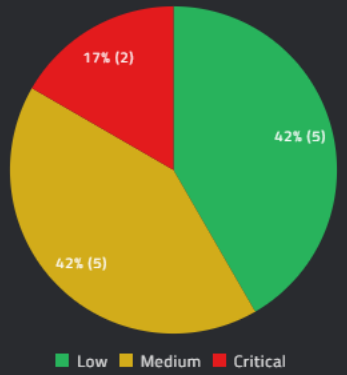
Workbench > Alerts List

- DASHBOARD
- QUEUE MANAGEMENT
- SECURITY ANALYTICS
- INCIDENT RESPONSE
  - ALERTS
  - INCIDENTS
  - TASKS
  - INDICATORS
  - CAMPAIGNS
  - HUNTS
- VULNERABILITY MANAGEMENT
- AUTOMATION
- RESOURCES
- REPORTS
- HELP

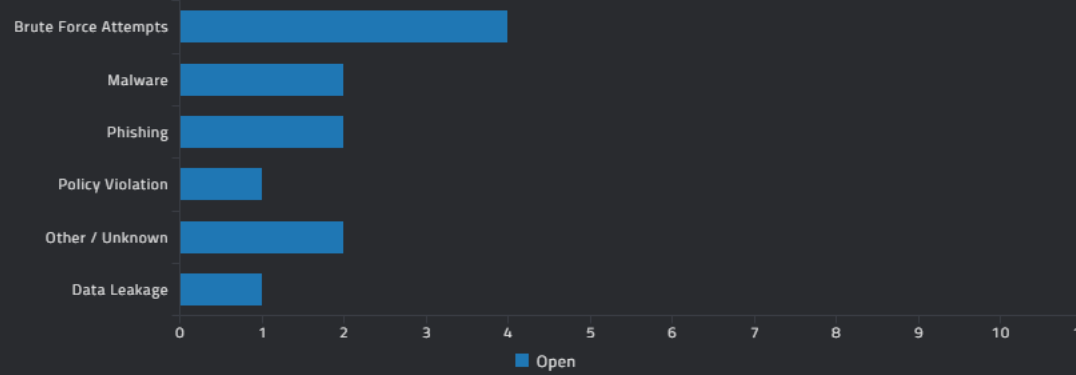
# ALERTS

EDIT TEMPLATE

## OPEN ALERTS BY SEVERITY



## ALERTS BY TYPE



12 Items

+ ADD ALERT EXECUTE ACTIONS EXECUTE

Search

ID	SEVERITY	NAME	SOURCE	DUE DATE	TYPE	STATUS	ASSIGNED TO	ESCALATED	KILL CHAIN ...
7947	CRITICAL	Repeated Login Failures on 192.168.50.19	Splunk	03/13/2019 09:...	Brute Force A...	Open	CS Admin	NO	
8049	MEDIUM	AIE: CyberSponse Login Failure	LogRhythm	03/16/2019 09:...	Other / Unkn...	Open	CS Admin		
8037	CRITICAL	Symantec Cloud.SOC -> Policy Violation -> External File Sharing	Symantec Cloud.SOC	03/16/2019 09:...	Data Leakage	Open	CS Admin		
8030	MEDIUM	Symantec ATP Incident :epmp_incident-2018-04-17/incident	Symantec ATP	03/16/2019 09:...	Malware	Open	CS Admin		Exploitation
8017	MEDIUM	Suspicious Email:Urgent: Requesting CEO Level Demo Environment	User Reported	03/16/2019 06:...	Phishing	Open	CS Admin		Delivery
7952	LOW	OutBound Connection - PaloAlto Network Traffic Alert	Splunk	03/13/2019 09:...	Policy Violati...	Open	CS Admin		
7951	LOW	IMAP -WIN-EXCH.cyops.local	Splunk - IMAP	03/13/2019 09:...	Phishing	Open	CS Admin		Delivery
7950	MEDIUM	WIN-EP2 - XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	Splunk	03/12/2019 09:...	Other / Unkn...	Open	CS Admin		
7949	LOW	Repeated Login Failure on Win-EP2	Splunk	03/13/2019 09:...	Brute Force A...	Open	CS Admin		
7948	MEDIUM	Malware Detected on WIN-EP2	Splunk	03/12/2019 09:...	Malware	Open	CS Admin	NO	




SAVE CANCEL REMOVE STEP

### VIRUSTOTAL 1.0.1

Step Name: Get Source IP Reputation

Step Description: Add information about the step here.



**VirusTotal**  
CyOPs Connector | Version 1.0.1  
CyberSponse Certified: Yes

[DOCUMENTATION](#)

Configuration: demo

Action: Get IP Reputation

Get IP Reputation from VirusTotal

Inputs: IP: {{vars.source\_ip}}

Advanced Configurations

Mock Output

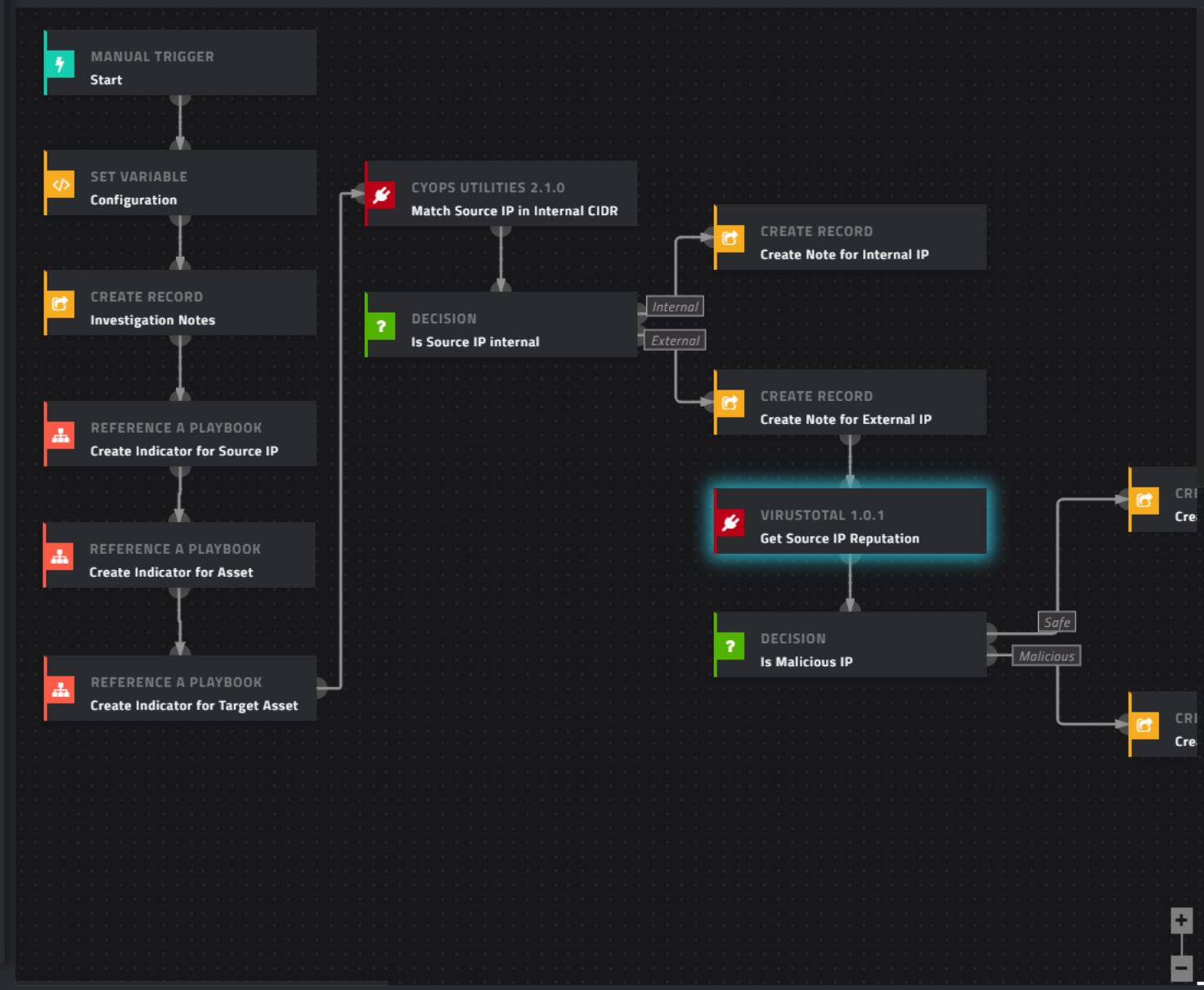
```
{
  "data": {
    "undetected_urls": [],
    "verbose_msg": "IP address in dataset",
    "aggregate": 11,
    "response_code": 1,
    "detected_urls": [
      {

```

+ Add Condition Variables Loop Message Mock Output Ignore Error

Description: Investigate Login Failures and also identify other impacted assets  
#ManualAction

OPTIONS TAKE SNAPSHOT SAVE PLAYBOOK





# AI-driven Security Operations - Endpoint

## Прогнозирование и предотвращение атак

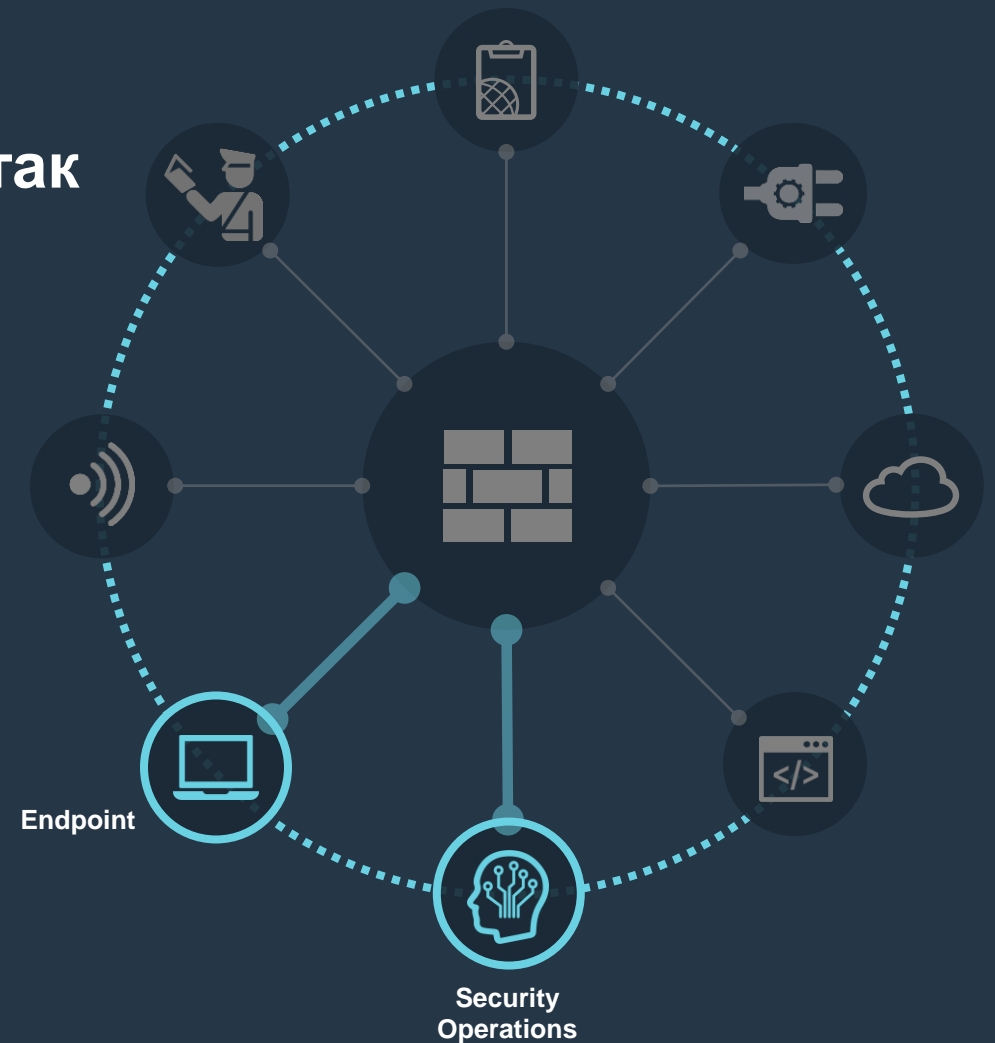
Уменьшение поверхности атаки, предотвращение активности вредоносного ПО

## Обнаружение и обезвреживание угроз

Предотвращение брешей безопасности с помощью обнаружения и разоружения в реальном времени

## Реагирование, расследование и охота

Организованное восстановление и форензика





# Прогнозирование и предотвращение

Уменьшение поверхности атаки, предотвращение активности вредоносного ПО

По многим причинам устройства ИТ и ОТ не всегда соответствуют корпоративным стандартам безопасности в части обновлений ОС, исправлений и других конфигураций. Такие системы становятся легкой добычей для злоумышленников.



FortiClient



FortiEDR



- Сканирование уязвимостей и установка патчей
- Предотвращение выполнения эксплойтов
- Анти-вирусное машинное обучение
- Поддержка изолированных сред

# Прогнозирование и предотвращение: FortiClient



Уменьшение поверхности атаки, предотвращение активности вредоносного ПО



## Комплексная защита конечных точек и обеспечение безопасности



Широкая видимость конечных точек



Комплаенс конечных точек и управление уязвимостями



Проактивная защита конечных точек



Автоматическое сдерживание угроз



Безопасный удаленный доступ



Легко развернуть и управлять



# Прогнозирование и предотвращение: FortiClient



Уменьшение поверхности атаки, предотвращение активности вредоносного ПО

FortiClient Enterprise Management Server

26 Total Applications

- Adobe Systems Incorporated (4)
  - Adobe Acrobat Reader DC
  - Adobe Flash Player 10 Plugin
  - Adobe Reader 9.3
  - Adobe Refresh Manager
- Bit9, Inc. (1)
  - Bit9 Agent
- Fortinet Technologies Inc (1)
  - FortiClient
- Google Inc. (1)
  - Google Chrome
- Igor Pavlov (1)
  - 7-Zip 17.00 beta (x64)
- Macromedia (5)
  - Macromedia Flash 8
  - Macromedia Flash 8 Video Encoder
  - Macromedia Flash MX 2004
  - Macromedia Flash Player 8
  - Macromedia Flash Player 8 Plugin
- Macromedia, Inc. (1)
  - Macromedia Extension Manager
- McAfee, Inc. (1)
  - McAfee Agent
- McAfee, LLC. (2)
  - McAfee Endpoint Security Firewall

26 of 26 applications loaded

FortiClient Enterprise Management Server

6666xp.exe (High Risk)

Threat Detected → Sandbox Analysis → File Blocked on 08-28-2018 at 12:45:22 → Send Dynamic Signature Updated to all FortiClient

Malware W32/Filecoder\_GandCrab.B!tr

Endpoint: Andrew (172.18.72.40, Burnaby, Canada)

Indicators (3):

- Executable dropped dll/sys files (s) to system directory
- The executable listened to local ports
- The file escalated the privilege to SeShutdown Privilege

Process Tree

6666xp.exe → svchost.exe → AcroRd32.exe → services.exe → mscoree.exe → mscoree.exe → mscoree.exe → mscoree.exe → mscoree.exe → mscoree.exe

Details

Process Information		Memory Operation	Network Operation
PID	3844		
File Path	%CURRENTPATH%\loader.exe		
File Type	pdf		
CMD Line	c:\work\loader.exe*c:\work\4035302442377709471.pdf* 55000		
MDS	494c087a144d3cc4c4a661ed1244039		
Detail	Executable dropped dll/sys file(s) to system directory		

3

2

1

# Обнаружение и обезвреживание

Предотвращение брешей безопасности с помощью обнаружения и разоружения в реальном времени

Предотвращение возможно не на 100% из-за все более изощренных угроз и методов атак, бесфайловых вредоносных программ, маскирующихся программ-вымогателей и концепции «living off the land attacks».



FortiEDR

- Обнаружение в реальном времени и защита после взлома
- Предотвращение взлома файлов и шифрования программами-вымогателями
- Противодействие краже данных, обмену данными с C&C и lateral movement



# Реагирование, расследование и охота

## Организованное восстановление и форензика

Нехватка навыков кибербезопасности. Реагирование на инциденты часто осуществляется вручную, требует дорогостоящих процессов и может повлиять на бизнес-операции или производительность сотрудников.



FortiEDR

- Восстановление без отключения машины
- Реагирование на угрозы на основе рисков
- Рекомендации по восстановлению для ИТ – не нужно перезабивать образ
- Дополнительный MDR для мониторинга угроз, упорядочивания предупреждений и реагирования



# AI-driven Security Operations Endpoint: FortiEDR



## Экспертные системы реагирования на инциденты

The screenshot displays the FortiEDR interface with the 'EVENT VIEWER' tab selected. The event details for 'taskeng.exe' (Event ID: 469778) are shown. The event is classified as 'Malicious' and occurred on 'andy-WIN7-PC' running 'Windows 7 Ultimate'. The process path is '\Device\HarddiskVolume2\Windows\System32\taskeng.exe'. The event details include a process creation diagram and a table of loaded DLLs.

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN	
andy-WIN7-PC	Windows 7 Ultimate	taskeng.exe	Malicious	File Service Access	27-Mar-2020, 08:50:21	27-Mar-2020, 08:50:20	

RAW ID: 1731790478    Process Type: 64 bit    Certificate: Unsigned    Process Path: \Device\HarddiskVolume2\Windows\System32\taskeng.exe    User: andy-WIN7-PC\andy    Count: 2

PARENT PROCESS CREATION    **SERVICES ACCESS ATTEMPT**

**SERVICES ACCESS ATTEMPT**

Process ID: 3480    Company: Microsoft Corporation    Product: Microsoft® Windows® Operating System    Process Hash (SHA-1): 09FAFEB1B8404124B33C44440BE7E3FDB6105F8A  
Source Process: \Device\HarddiskVolume2\Windows\System32\vssadmin.exe    Description: Command Line Interface for Microsoft® Volume Shadow Copy Service    Comments:    Process Owner: NT AUTHORITY\SYSTEM  
Target: SHADOW COPY ACCESS    Version: 6.1.7600.16385 (win7\_rtm.090713-1255)    Command Line: Delete Shadows /Quiet /All

EXECUTABLE FILE NAME	WRITABLE	CERTIFICATE	REPETITIONS	BASE ADDRESS	END ADDRESS	HASH
Main -\Device\HarddiskVolume2\Windows\System32\vssadmin.exe	No	Unsigned				09FAFEB1B8404124B33C44440B...
\Device\HarddiskVolume2\Windows\System32\kernel32.dll	No	Unsigned	3	0x76e10000	0x76f2f000	D48370...
\Device\HarddiskVolume2\Windows\System32\ole32.dll	No	Unsigned	2	0x7efeaa0000	0x77efeca1000	E06FBA...
\Device\HarddiskVolume2\Windows\System32\ntdll.dll	No	Signed	1	0x76f30000	0x770db000	3D62555687087F3DD8C628752A...
\Device\HarddiskVolume2\Windows\System32\ole32.dll	No	Unsigned	14	0x7efeaa0000	0x77efeca1000	31BB9C5389A91733A101E06FBA...
\Device\HarddiskVolume2\Windows\System32\ntdll.dll	No	Signed	1	0x76f30000	0x770db000	3D62555687087F3DD8C628752A...





# Fabric Management Center

## Централизованное управление сетью

Управление из единой консоли

## Единое управление приложениями

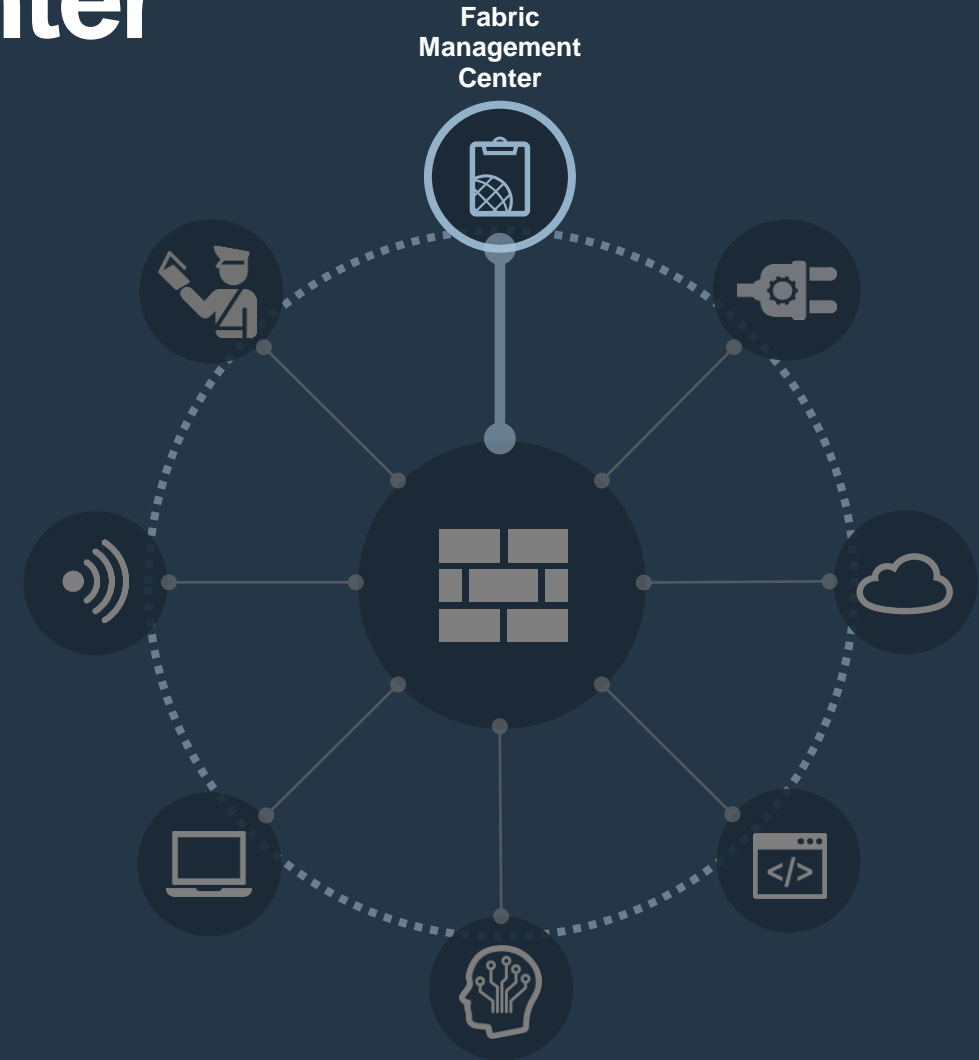
Единый вход (SSO) в приложениях Security Fabric

## Автоматизация и оркестрация

Интеграция рабочих процессов в Security Fabric

## Сетевая аналитика и отчетность

Аналитика сети и отчеты в режиме реального времени





# Fabric Management Center

Трудно достичь аналитики состояния сети в реальном времени, если она не является неотъемлемой частью Security Fabric. Для сетевой аналитики в реальном времени требуется интегрированная аналитика.



FortiAnalyzer



FortiGate Cloud



FortiManager

Единая консоль управления сетью  
Автоматизация и оркестрация  
Сетевая аналитика и отчетность



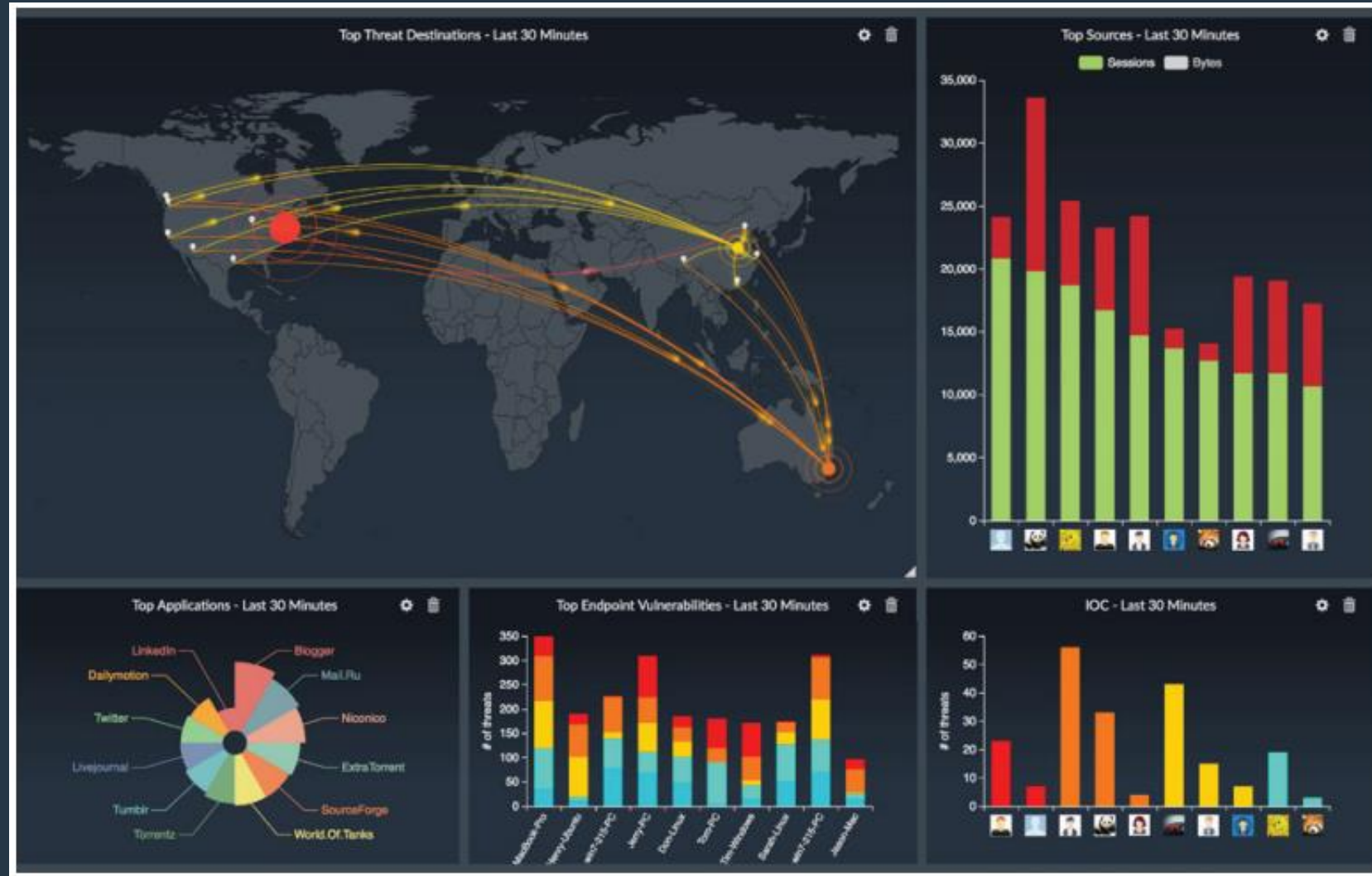
- Анализ состояния сети в реальном времени
- Управление сетевыми журналами
- Отчетность о соответствии требованиям

# Fabric Management Center: FortiAnalyzer



Сетевая аналитика и отчетность

- Автоматизированное управление журналами и анализ угроз в реальном времени
- Непрерывная отчетность для предприятий
- Упрощенная форензика и быстрое реагирование



# Fabric Management Center: FortiManager

Единая консоль управления сетью



Device Manager | Device & Groups | Firmware | License | Provisioning Templates | Scripts | SD-WAN | ADOM: fgt62 | admin

Install Wizard | Per-device Management

SD-WAN | Edit SD-WAN

Monitor | Device: FGVMO20000155864 (root)

SD-WAN Status: ON

---

Device Manager | Device & Groups | Firmware | License | Provisioning Templates | Scripts | SD-WAN | ADOM: adom60 | admin

Add Device | Device Group | Install Wizard | Tools | Table View

Managed Devices | 21 Devices | 2 Devices | 1 Devices | 0 Devices

---

Policy & Objects | Policy Packages | Object Configurations | ADOM: FG60 | admin

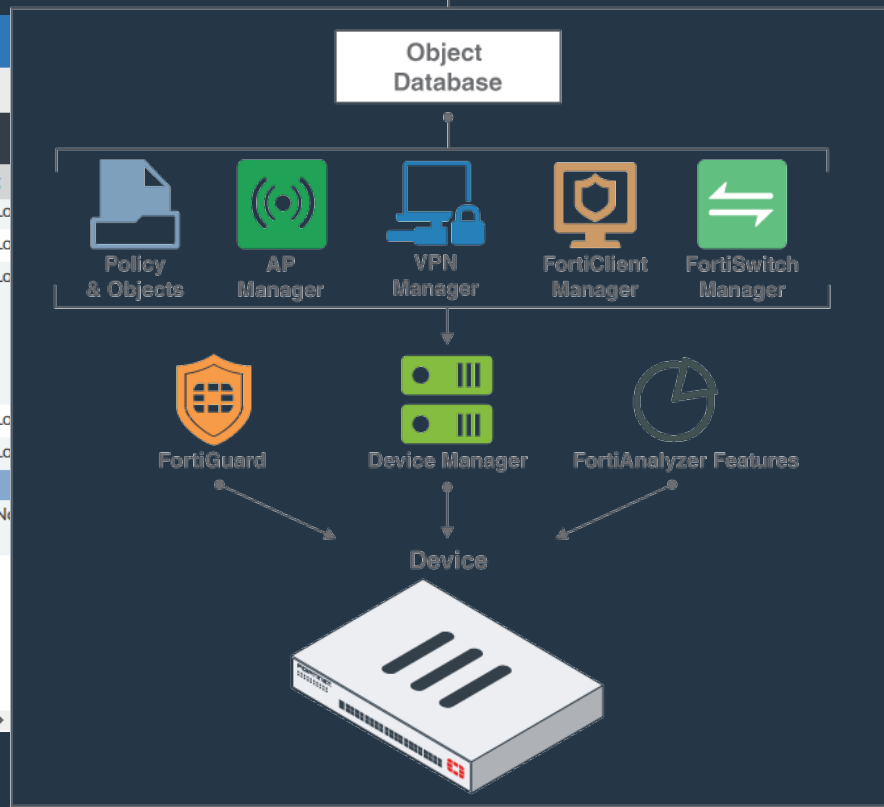
Policy Package | Install | ADOM Revisions | Tools | Collapse All | Object Selector

Search...

Seq.#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profiles	Log
1	test	any	port9	all	all	always	ALL		Deny		Lo
2	badbuild	port8	port9	auth.gfx.ms	all	always	ALL		Deny		Lo
3	shadowing	port7	port6	auth.gfx.ms	google-play	always	ALL_ICMP		Accept	certificate-inspection	Lo
		port6	port7	google-play	swscan.apple.com		ALL_TCP				
							ALL_ICMP6				
							ALL_UDP				
							FTP				
4	matching	any	port5	all	all	always	ALL		Deny		Lo
5	malade	any	port3	all	all	always	ALL		Accept	certificate-inspection	Lo
Implicit (6-6 / Total:1)											
6	Implicit Deny	any	any	all	all	always	ALL		Deny		No

default | Packages | 149\_root | IPv4 Header Policy | IPv4 Policy | IPv4 Footer Policy | IPv4 Virtual Wire Pair Policy | IPv6 Policy | NAT46 Policy | NAT64 Policy | Proxy Policy | IPv4 DoS Policy | IPv6 DoS Policy | IPv4 Interface Policy | IPv6 Interface Policy | Multicast Policy | IPv4 Local In Policy | IPv6 Local In Policy | Traffic Shaping Policy | Installation Targets | FortiGate-VM64 | Root | zCDOMm

FortiManager



# Open Fabric Ecosystem

## Fabric Connectors

Разработанная Fortinet глубокая интеграция, автоматизирующая операции и политики безопасности

## Fabric API

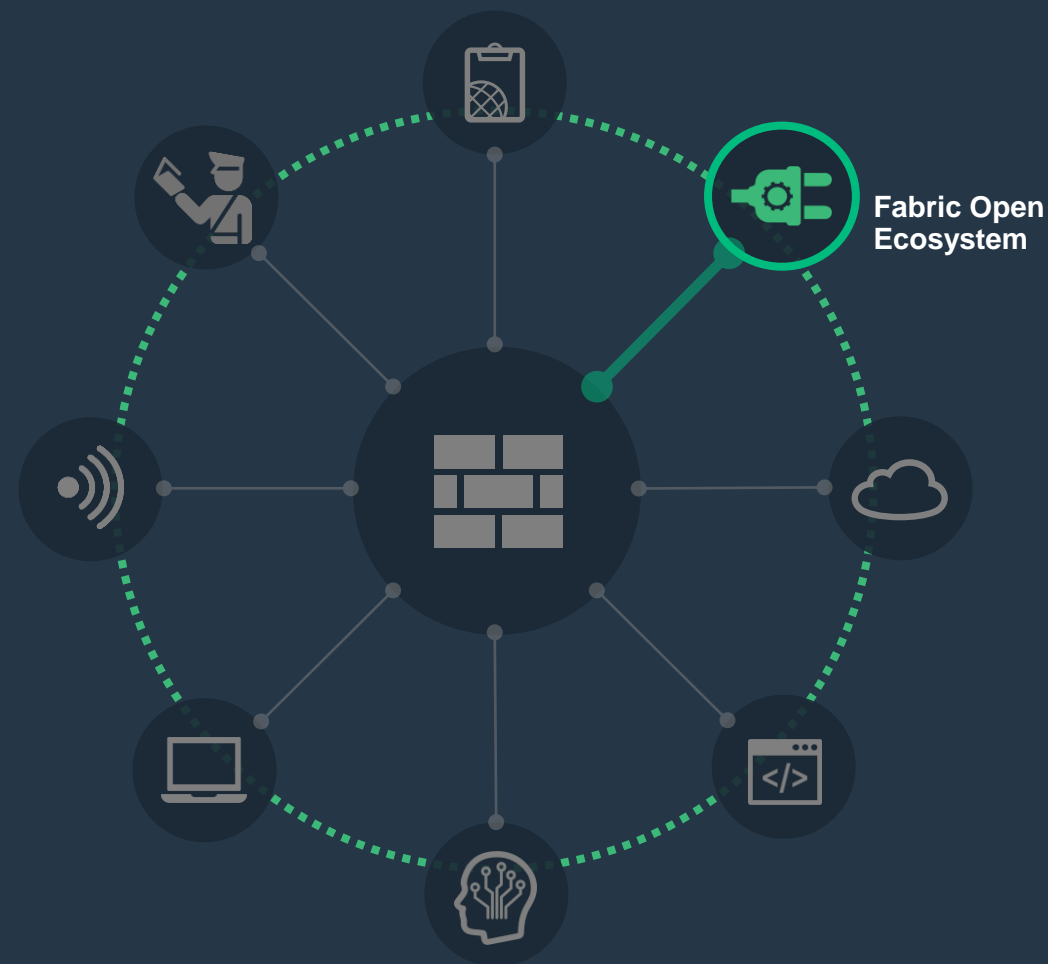
Разработанная партнерами интеграция с использованием API-интерфейсов Fabric, обеспечивающая широкую end-to-end видимость

## Fabric DevOps

Создаваемые сообществом сценарии DevOps, автоматизирующие развертывание, настройку и оркестрацию сети и безопасности

## Extended Fabric Ecosystem

Сотрудничество с инициативами по обмену угрозами и интеграцией с технологиями других поставщиков





# Обширная отраслевая экосистема кибербезопасности

## 250+ интеграций с экосистемой Security Fabric



### Fabric Connectors (12)

Разработанная Fortinet глубокая интеграция, автоматизирующая операции и политики безопасности



### Fabric APIs (135+)

Разработанная партнерами интеграция с использованием API-интерфейсов Fabric, обеспечивающая широкую end-to-end видимость



### Fabric DevOps (9)

Создаваемые сообществом сценарии DevOps, автоматизирующие развертывание, настройку и оркестрацию сети и безопасности



### Extended Security Fabric Ecosystem (130+)

Сотрудничество с организациями по обмену угрозами (30+) и интеграция с продуктами других поставщиков (100+)



Note: Logos are a representative subset of the Security Fabric Ecosystem

# Экосистема сетевых операций

## Fabric API Partnerships с FortiGate & FortiManager



### Fabric API



# SCADA / Промышленное управление

Fabric API Partnerships в ОТ-вертикали

## Fabric API



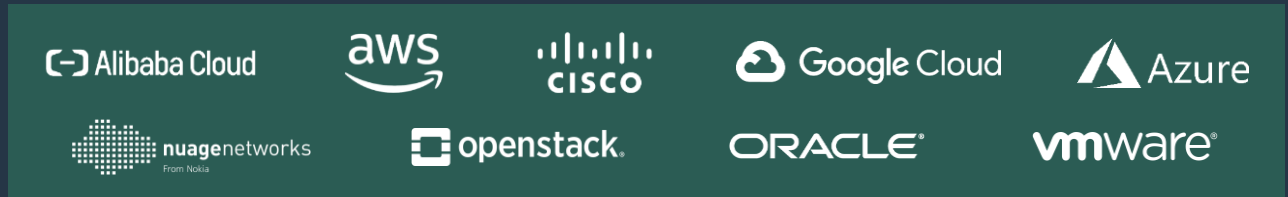


# Экосистема мультиоблачной безопасности

Public & private cloud partnerships



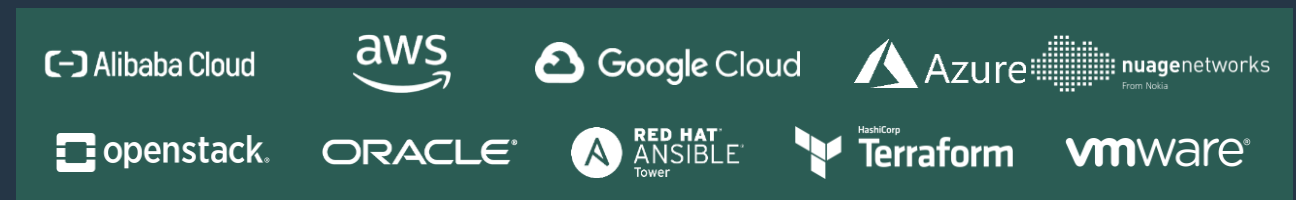
## Fabric Connector



## Fabric API



## Fabric DevOps



# Экосистема безопасности приложений

Fabric API Partnerships с FortiWeb и FortiMail



## Fabric API



# Экосистема безопасности операций

Fabric API Partnerships с FortiSandbox, FortiAnalyzer, и FortiSIEM



## Fabric Connector

**servicenow**

## Fabric API

**Attivo**  
NETWORKS

**BROCADE**

**CITRIX**

**CYBERARK**

**DB SECURITY**

**graylog**

**INTSIGHTS**

**METTCARE**  
Technologies

**rubrik**

**SAFE-T**  
Smart Security Made Simple.

**safetica**

**SECLYTICS**  
ACCURATE · VERIFIABLE · ATTACK PREDICTIONS

**Siemplify**

**splunk**

**spirent**  
Promise. Assured.

**STRATOZEN**

**SWIMLANE**

**ThreatConnect**

**TRAPX**  
SECURITY

**vijilan**  
IT Security. Enabled.

# Экосистема конечных точек

## Fabric API Partnerships с FortiClient



### Fabric Connector



### Fabric API



# Экосистема безопасного доступа

Fabric API Partnerships с FortiNAC and FortiAuthenticator



## Fabric Connector

**aruba**  
a Hewlett Packard  
Enterprise company

**CISCO**

## Fabric API



# Fabric Connectors

Разработанная Fortinet глубокая интеграция с платформами клиентской экосистемы



# Fabric APIs

Решения для комплексной безопасности с дополнительной интеграцией



# Fabric DevOps

Готовые сценарии автоматизации





# Расширенная экосистема Security Fabric

Партнерство по обмену сведениями об угрозах и технологическая интеграция с другими поставщиками

## CYBER THREAT ALLIANCE

Co-founded by Fortinet



Для обеспечения высококачественного обмена информацией о киберугрозах между компаниями и организациями, занимающимися кибербезопасностью, в режиме, близком к реальному времени.

## COMMUNITY-SUPPORTED STANDARD



OASIS



MITRE

Определение отраслевых стандартов и протоколов для автоматизации обмена информацией, комплексного анализа и защиты в реальном времени

## ENTERPRISE TECHNOLOGY LEADERS



Microsoft

verizon

Для своевременного реагирования на уязвимости приложений, угрозы и тренды

## COMPUTER EMERGENCY RESPONSE TEAMS



Для своевременного прерывания кибер-кампаний и злоумышленников

## LAW ENFORCEMENT AND GOVERNMENT



Обмен кибер-данными для подрыва действий национальных и продвинутых киберпреступников с целью улучшения и повышения эффективности безопасности цифровой экосистемы

Интеграция с более чем 100 технологиями других поставщиков

- Firewall
- Endpoint Security
- Switching
- Wireless
- Mobile Device

... and more

Интеграция, обеспечивающая хорошую работу решений Fortinet с продуктами других поставщиков в вашей инфраструктуре.

# Обширная экосистема Fabric

## Интеграция с другими ИТ-поставщиками

### TECHNOLOGY VENDORS

- 3Com
- Access Credentials
- Adtran
- Aerohive
- AirWatch
- Alert Logic
- Allied Telesis
- Alteon
- Apache Tomcat
- APC NetBotz
- Apple
- Authentium
- Avast
- Avaya
- AVG
- Avira
- Barracuda Networks
- Bit9
- Blink
- Box.com
- BullGuard
- CA
- Check Point
- ClamAV
- CloudPassage
- Colubris
- CrowdStrike
- Cylance
- Cyphort
- Cxterta AppGuard
- Damballa
- Dell SonicWall
- Digital Guardian
- Dropbox
- D-Link
- Dr. Web
- EMC
- Enigma
- Enterasys
- F5
- FireEye
- Foundry Networks
- F-PROT
- F-Secure
- G DATA
- GitHub
- Green League
- H3C
- Imperva
- Intego
- Javacool
- Juniper Networks
- Lantronix
- Lastline
- Lavasoft
- Open LDAP
- Liebert
- Lightspeed
- Linux Server
- LiveAction
- MaaS360
- Malwarebytes
- Medigate
- MicroWorld
- MikroTik
- MobileIron
- Motorola
- MySQL
- Nessus
- NetApp
- Nginx
- Nimble
- Norman
- Nortel
- Norton
- Okta
- One Identity
- PacketFence
- Palo Alto Networks
- PC Tools
- QNAP Turbo NAS
- Radiflow
- Radius
- Radware
- Rapid7
- Rising
- Riverbed Accelerator
- Ruckus
- Smart Hive
- Snort
- Softwin
- Sophos
- Spyware Bot
- SSH Comm Security
- StackRox
- Sun Solaris
- Sunbelt
- Tenable
- Trend Micro
- VASCO DIGIPASS
- Vexira
- Webroot
- WatchGuard
- Websense
- ZoneAlarm
- XenMobile
- Xirrus
- XYLink

*...и другие ИТ-поставщики и группы стандартов*

**FORTINET**<sup>®</sup>