Решения Fortinet для защиты от угроз в 2018 году

Андрей Терехов, инженер
aterekhov@fortinet.com

20 марта 2018

Лаборатория FortiGuard

- ~215 исследователей, аналитиков и инженеров в 31 стране
- Исследования | Разработка | Инновации
- Ответные меры | Обучение

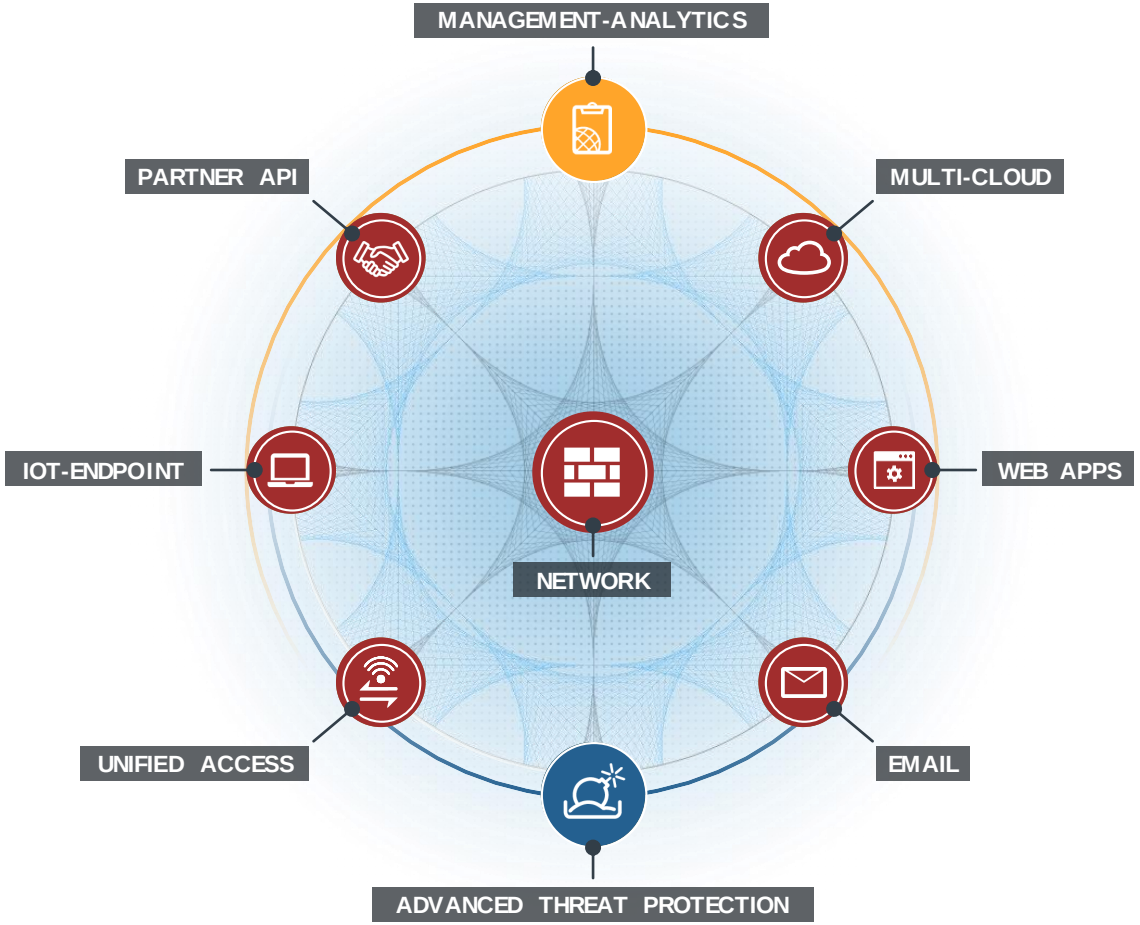
BURNABY (CANADA)

- 200+ Партнёров (e.g. Interpol, Certs, CTA, etc.)
- ~450,000 часов исследований в год

OTTAWA, CANADA

FortiGuard лаборатория - подписки

Лаборатория FortiGuard предоставляет сервисы, защищающие от эволюциюнирующих угроз



- ✓ Delivering Real-Time Updates & Proactive Protection
- ✓ At Machine Speed, Scale, with Extreme Accuracy
- ✓ Unparalleled Third-Party Certification and Validation

Недостаток кадров в ИБ

The Fast-Growing Job With A H
Gap: Cyber Security

Save

Shutterstock

Some experts predict there will be a global shortage of two million cyber security professionals [+]

Behind every new hack or data breach, there's a company scrambling to put out the fire. That's good news for job

Объём, скорость изменения и сложность угроз

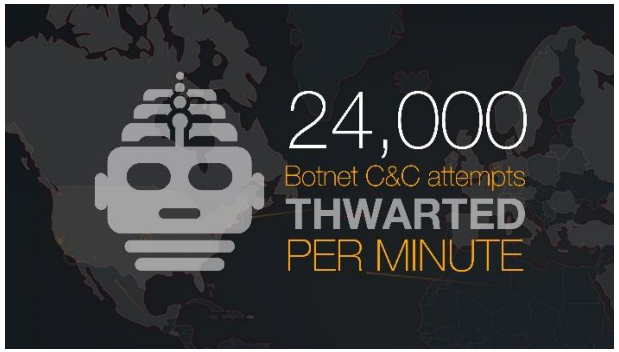
- 50 Billion Events Ingested Per Day
- ^ 1.3 Million Malware Samples Processed Per Day
- 17,671 Unique Malware Variants Detected In One Quarter

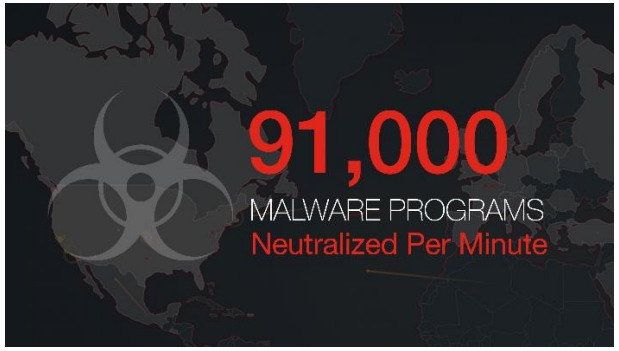
21 миллиард IOT устройств к 2020

Анализ, Выявление, Исследование – необходима автоматизация!

Source: Forbes.com

FortiGuard в числах

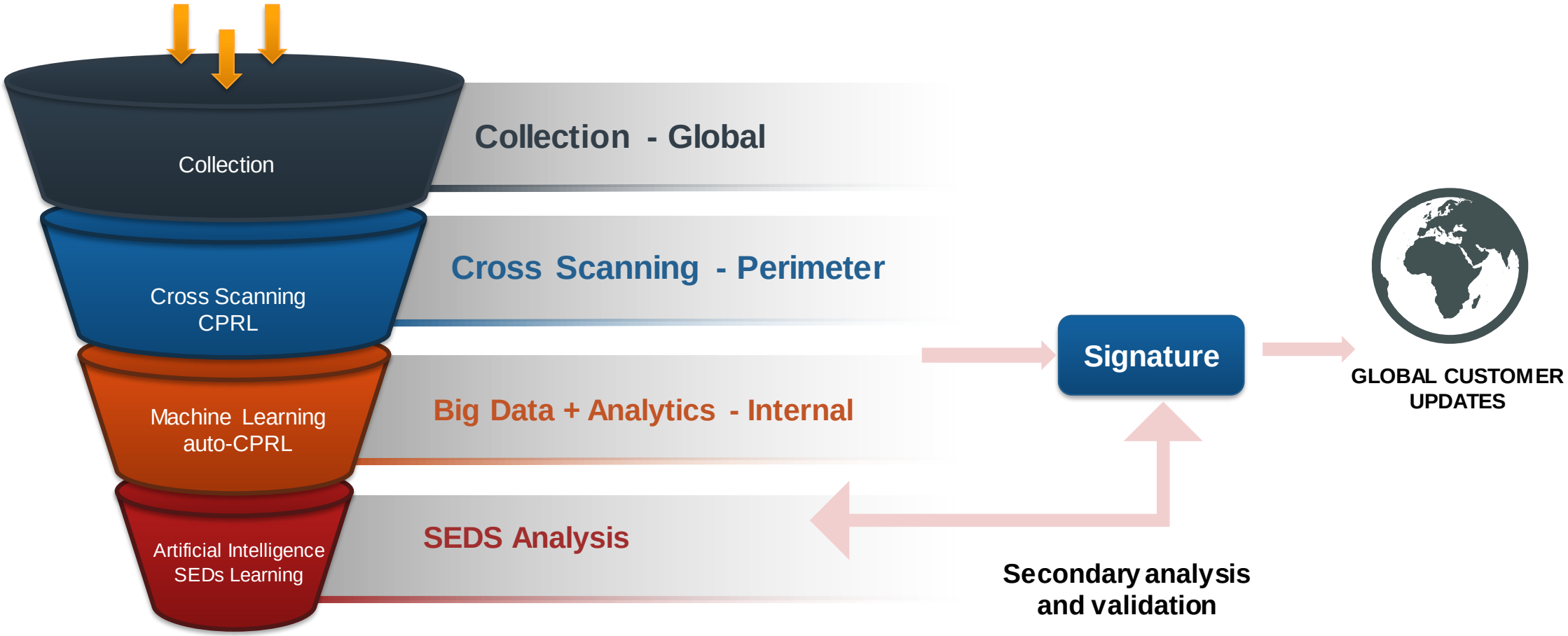




Архитектура реагирования на новые образцы

Применение машинного обучения и искусственного интеллекта

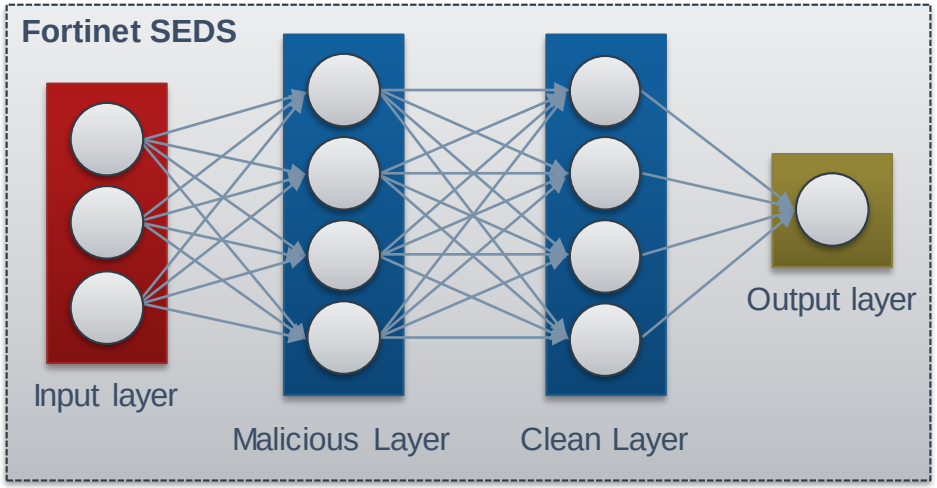
- Augmenting pattern recognition and automatic signature creation technology
- Continued learning and feature improvement – higher accuracy of the system



FortiGuard AI – Нейронная сеть

4-слойная архитектура

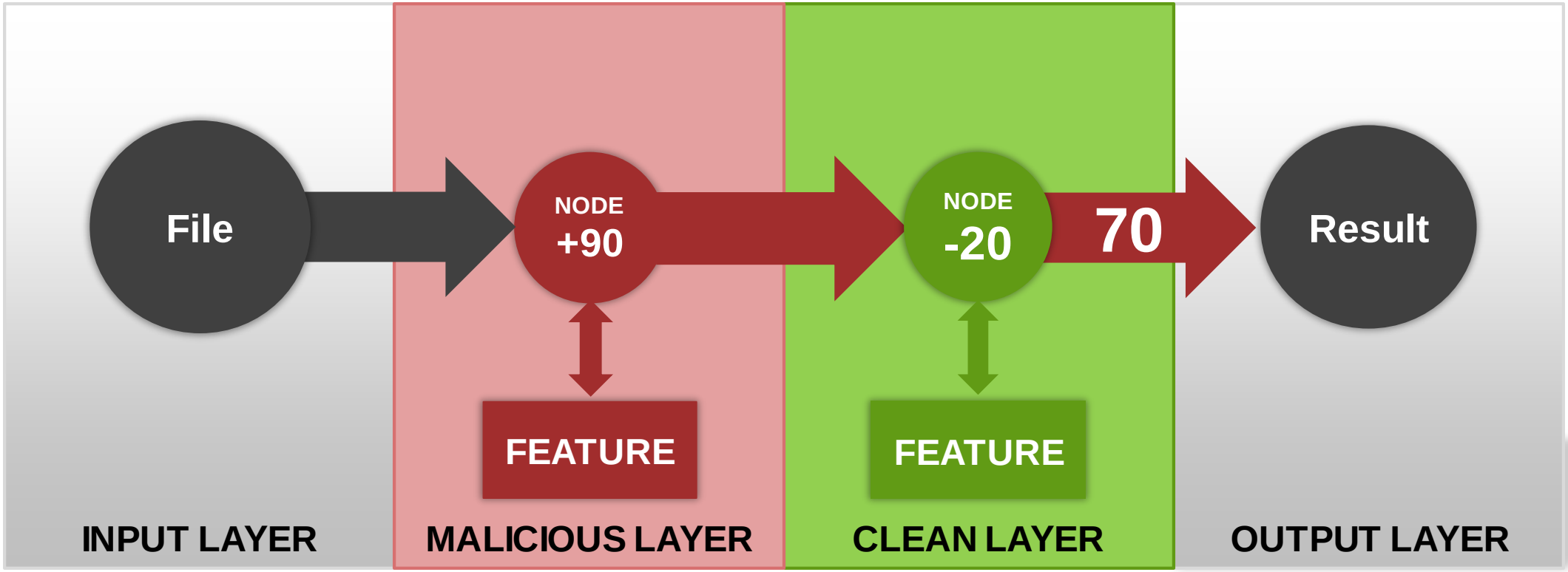
1) Input layer – submit files for analysis
2) Hidden layers (one or more) – computation
   - Connected to every node in the previous subsequent layer
   - Produces an output value based on inputs, function, and weighted valuation
     - 1 hidden layer scans 2.3 billion nodes analyzing for potential malicious features
     - 1 hidden layer scans for 3.2 billion nodes analyzing for clean features
3) Output layer – results of analysis - clean or dirty



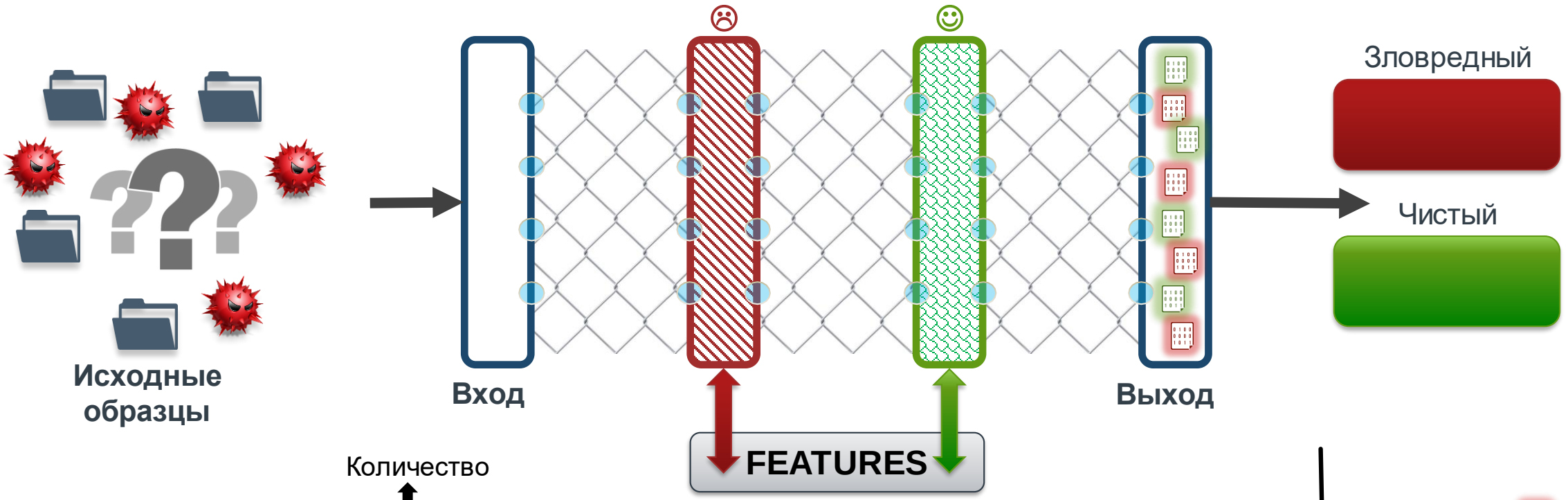
Consists of separate layers for either malicious or clean feature processing
Mathematical models compare samples and features to decide output

Features, Nodes & Weights – Пример обработки

1. We start with an input file – malicious or clean
2. Feature presence is calculated, re-weighted and passed forward to the next node
3. The analysis is repeated using the next layer feature, then passed to the next node
4. Result – the overall probability based on a score of feature presence

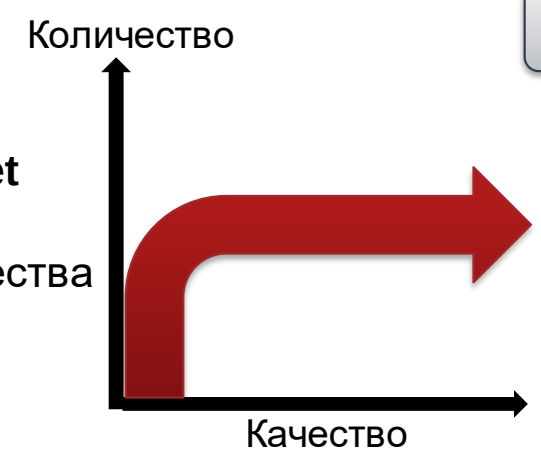


FortiGuard AI в действии

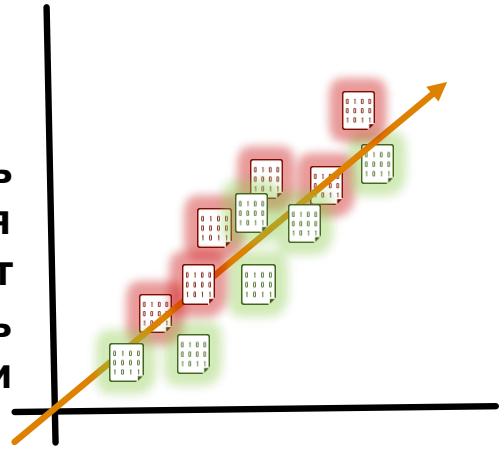


Улучшения Feature Set

- Качество
- Стабилизация количества features
- Взвешенная достоверность

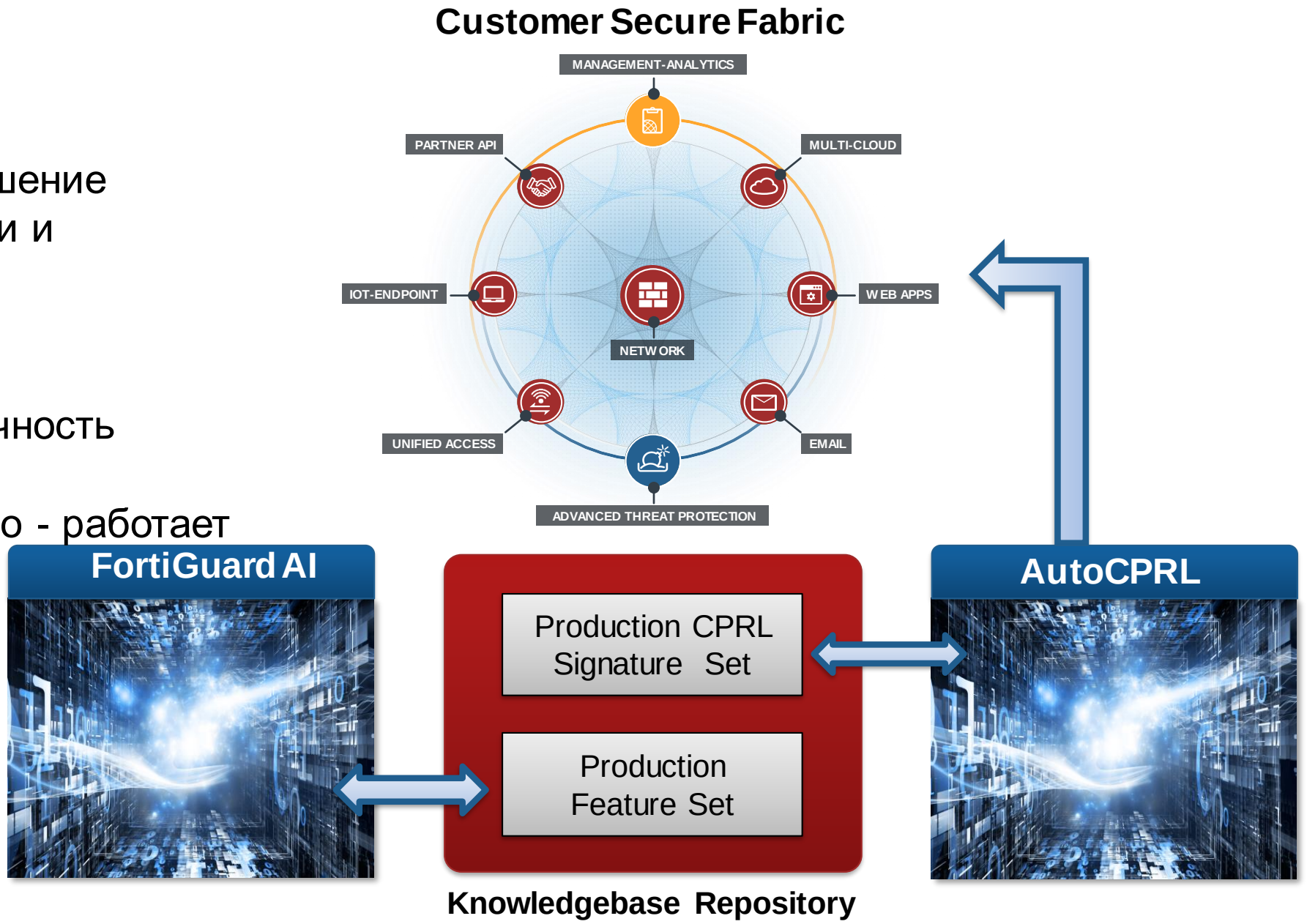


Точность срабатывания обеспечивает высокую степень достоверности

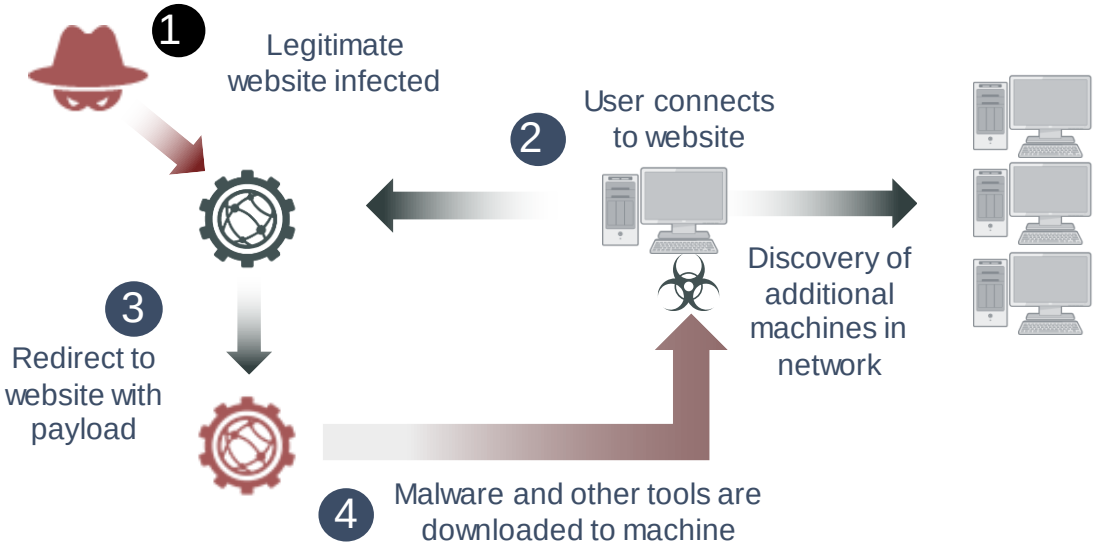


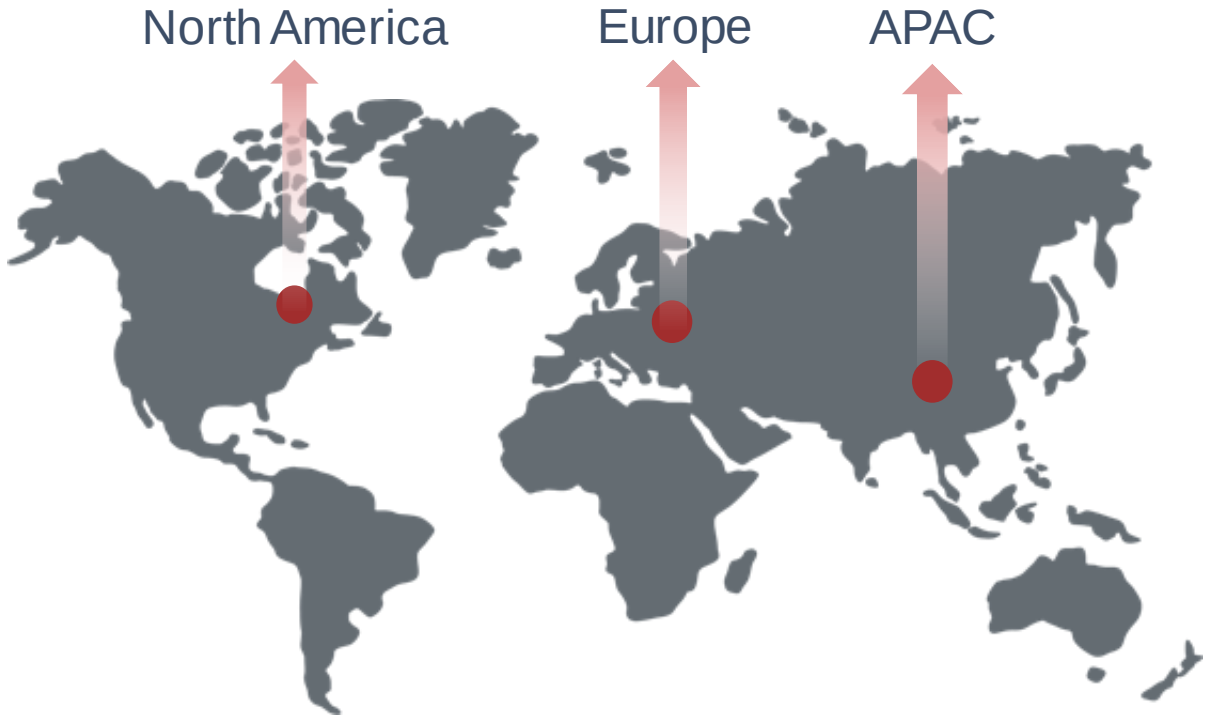
Результат

- Существенное повышение стоимости разработки и обновления для киберпреступников
- Непревзойденная точность
- Доказано и проверено - работает
- Адаптивно



Пример кампании - RATANKBA Malware





Fortinet's Machine-Learning methods analyze millions of files thru a sophisticated neural-network discovering new zero-days and malware variants.

Fortinet's machine-to-machine defensive system releases dynamic algorithm (W32/Generic.AC.39AB6D!tr)

Trend Micro discloses RATANKBA malware. Fortinet customers are proactively protected based algorithm 4 months prior

Symantec releases additional hash information on RATANKBA which Fortinet is already blocking based on algorithm created 4 months prior

Fortinet discovers several malicious domains. Customers are protected through web filtering and DNS engines.

Several additional domains are published and determined to be part of RATANKBA malware which Fortinet had protection

Prior Dates ***- 100 day*** **Day 0** ***Day 1*** ***Day 2*** ***Day 6***

Результаты Fortinet в тестах NSS за последние 6 лет

	Product	2012	2013	2014	2015	2016	2017
Data Center	Data Center Firewall		Recommended			Recommended	Passed
	Data Center IPS			Neutral		Recommended	
	Data Center Security Gateway						Recommended
	WAF			Recommended			Recommended
Virtual Security	vFW						
	vSG						
Endpoint	Endpoint Protection				Recommended		Recommended
Enterprise/ Perimeter Security	Breach Detection			Recommended	Recommended	Recommended	Recommended
	Breach Prevention						Recommended
	NGFW	Neutral	Recommended	Recommended		Recommended	Recommended
	NGIPS				Recommended	Recommended / Caution	Recommended
	SSL						

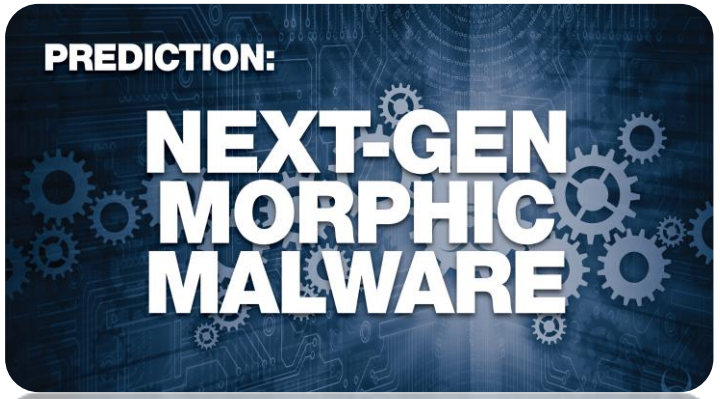
Это позволяет нам выявлять уязвимости нулевого дня

Список уязвимостей нулевого дня, анонсированных лабораторие FortiGuard в Q3 2017.
Уровни риска согласованы с общей методикой CVSS

Detection	Name/Description	Product	Vulnerability	Risk
JULY ANNOUNCEMENTS				
FG-VD-17-107	Multi-byte Character Filtering Cross-Site Scripting Vulnerability II	Joomla	CVE-2017-7985	High
FG-VD-17-108	Core Line Feed Character Cross-Site Scripting Vulnerability I	Joomla	CVE-2017-7985	High
FG-VD-17-109	Core Line Feed Character Cross-Site Scripting Vulnerability II	Joomla	CVE-2017-7985	High
AUGUST ANNOUNCEMENTS				
FG-VD-17-142	Embedded Open Type Font File Handling Memory Corruption	Microsoft	CVE-2017-8691	High
FG-VD-16-062	AVG Self-protection Bypass by disabling AV update	AVG	N/A	Med
FG-VD-17-018	Bitdefender AVC3 Driver Local Privilege Escalation	Bitdefender	N/A	High
SEPTEMBER ANNOUNCEMENTS				
FG-VD-17-019	Bitdefender Kernel Driver Self-Protection Bypass	Bitdefender	N/A	Med
FG-VD-16-043	Cisco Web Security Appliance Cross-Site Scripting Vulnerability	Cisco	N/A	Med

Подробнее: https://fortiguard.com/zeroday

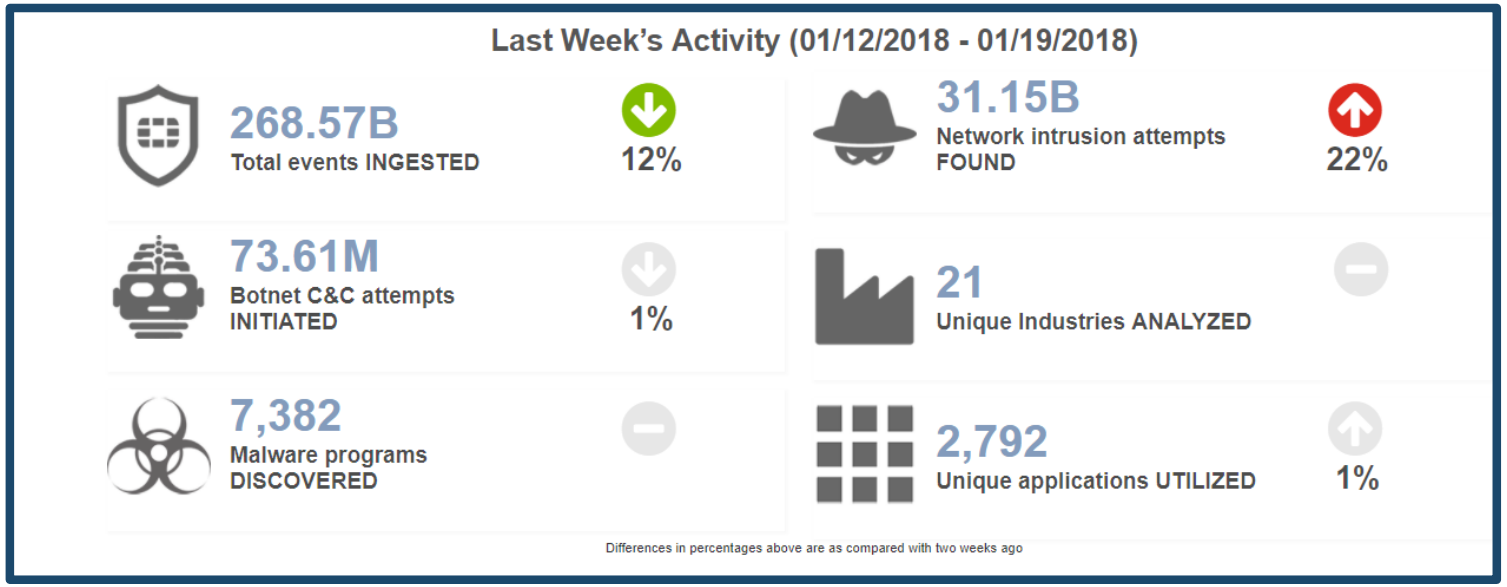
И понимать тренды – предсказания на 2018 год



Подробнее : https://blog.fortinet.com/2017/11/14/fortinet-fortiguard-2018-threat-landscape-predictions

Новый сервис - FortiGuard Threat Intelligence Service (TIS) https://tis.fortiguard.com/

Detection Metrics



Trending Determination

Threat Research Commentary

Profile-based Visualizations

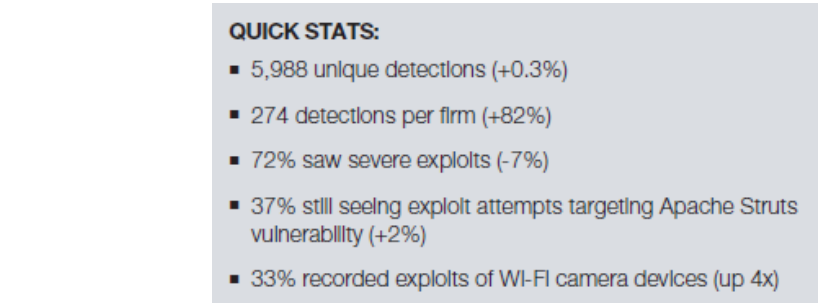
https://tis.fortiguard.com/

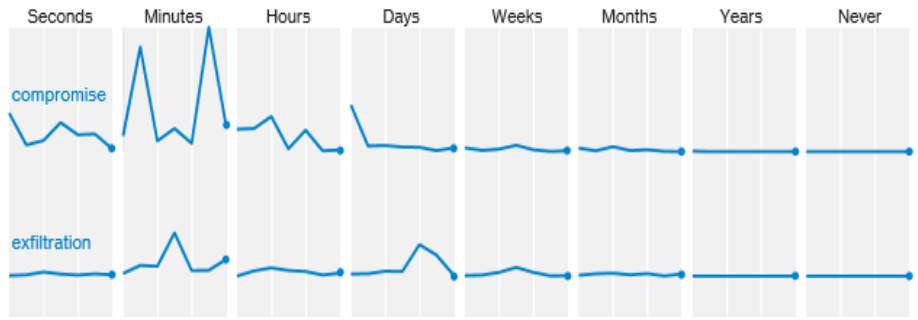
Потребность в новых сервисах - драйверы

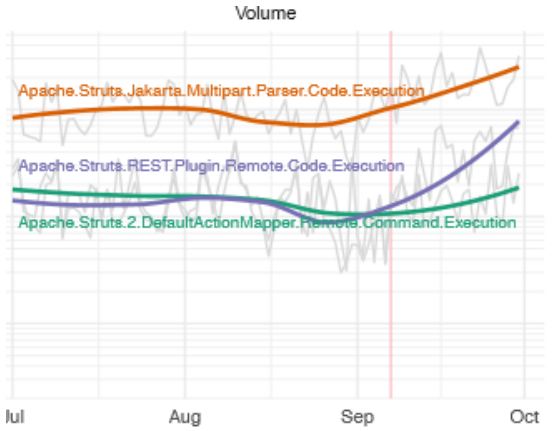
- Отчёт Fortinet - Threat Landscape Report

- Verizon Data Breach Investigation Report
  - » Компрометация происходит за минуты в большинстве случаев

- Техническое развитие злоумышленников
  - » Использование автоматизации и распределенных систем
  - » Эволюция тактик и техник для сокрытия активности
  - » Рынок услуг киберпреступности







Q42017 Threat Landscape Report: Основные выводы и рекомендации

Botnets

Firms typically have one or two different botnets active at any given time – some 10 or more!	Firms need to eradicate the underlying issues causing infections – find and fix root cause

Mobile Malware

Mobile is increasingly becoming a target – Q4 saw 14% firms reporting	Ensure mobile devices have appropriate security controls in place and are being monitored

IOT Exploits on the Rise

Exploit activity against IOT devices (like WiFi cameras) quadrupled in Q4	Identify ALL devices connected to your n/w. Segment IOT devices into secured n/w zones with customized policies

Ransomware

22% of firms detected some type of ransomware in Q4	Minimize impact by ensuring you have a good offline backup. Define pay or not-pay policies and process ahead of time

Q42017 Threat Landscape Report: Основные выводы и рекомендации (2)

Cryptojacking

Sharp increase in cryptomining malware – systems infected so they can be leveraged to mine cryptocurrencies → Regularly review system processes running on computers to find/kill culprits

Steganography

Top reported exploit in December used steganography to conceal hidden information with graphics file – distributes ransomware → Utilize a data sanitation service – like Content Disarm and Reconstruction that removes active content from files in real-time

P2P Proxy Target

Firms with high utilization of P2P and proxy apps have up to 9x higher rates of botnets and malware → Firms need to review policies, update software inventory, and scan for rogue applications

Vulnerability Swarm

37% of firms STILL seeing exploits targeting Apache Struts vulnerability – Attackers smell blood and swam. → Utilize a security audit service that can identify vulnerabilities and configuration weaknesses and help implement best practices

Новые сервисы

Virus Outbreak Services

» Репутационный антивирус – выявление новейшего вредоносного ПО, для которого ещё нет сигнатур

» На практике, обновление сигнатур проводится в среднем один раз в день – *VOS позволяет решить эту проблему*

Content Disarm & Reconstruction

» Удаляет весь активный контент из файлов в режиме реального времени, создаёт «плоский» файл

» Весь активный контент (скрипты, макросы и т.п.) воспринимается как пододрительный и требует подробной проверки

Security Audit Update Services

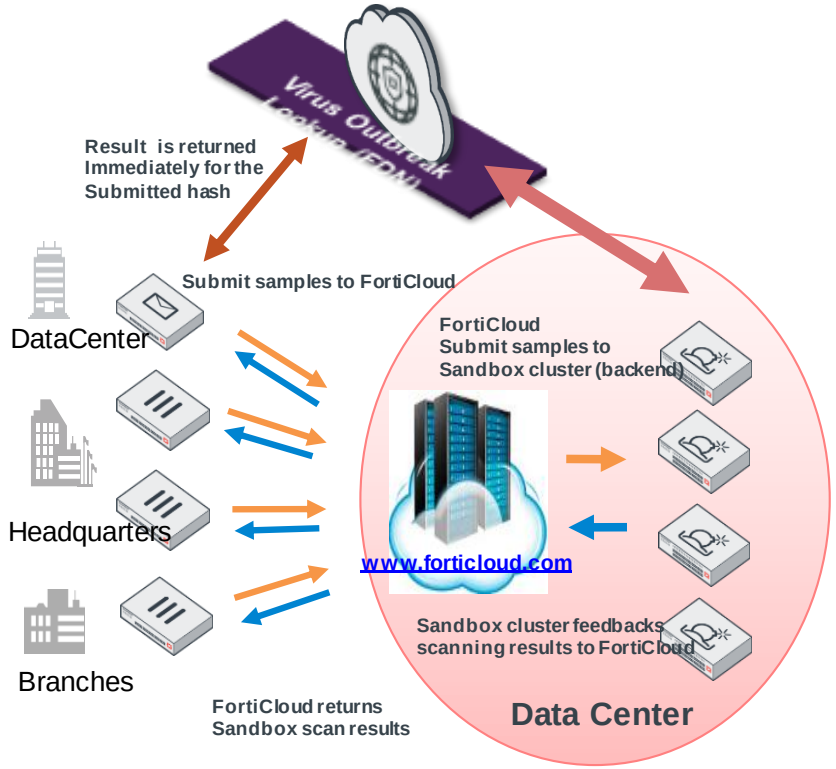
» Предоставляет рекомендации по дизайну, внедрению и поддержанию целевой архитектуры системы обеспечения ИБ

» Идентифицирует критические уязвимости и слабости конфигурации в Security Fabric, позволяет применить рекомендации, основанные на лучших практиках

FortiGuard Virus Outbreak Protection Service (VOS)

- Предоставляет возможности блокирования новейшего вредоносного ПО, выявленного в интервале между обновлениями сигнатур

- ✓ Закрывает нишу, образующуюся между сигнатурным антивирусом и «песочницей»
- ✓ Если сигнатурный подход не выявляет вредоносного ПО, то производится поиск по базе Global Threat Intelligence DB
- ✓ Global Threat Intelligence DB содержит информацию о новейшем вредоносном ПО, полученную как из внутренних, так и из сторонних источников

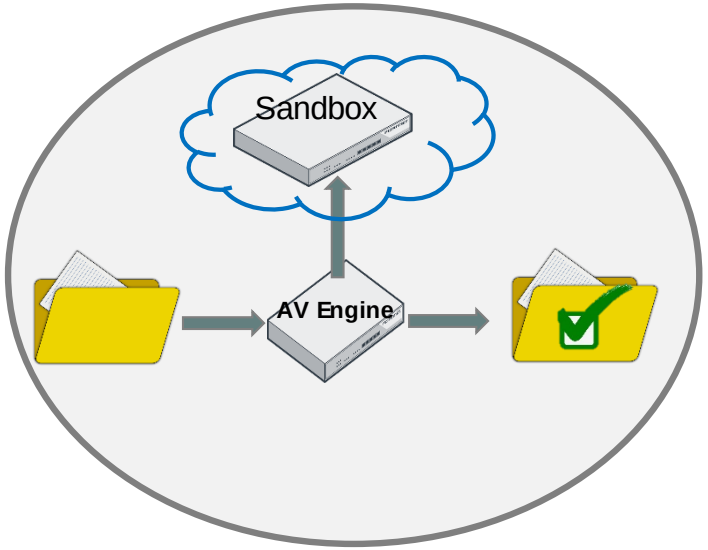


FortiGuard Content Disarm and Reconstruction (CDR)

Сервис санации данных

Удаляет весь активный контент из файлов в режиме реального времени, создаёт «плоский» файл

- ✓ Весь активный контент (скрипты, макросы и т.п.) воспринимается как подозрительный и требует подробной проверки
- ✓ На сегодняшний день поддерживаются файлы форматов Microsoft Office и Adobe – наиболее популярные у злоумышленников форматы
- ✓ CDR является частью политики МЭ– Администратор может включить функцию только для отдельных пользователей/групп/узлов
- ✓ Исходный контент можно загрузить по запросу при наличии локального FortiSandbox (если проверка покажет, что он чистый)



Security Rating Service

Усовершенствованный механизм реализации лучших практик

Организациям сложно своевременно исправлять новые уязвимости. Недостаток ресурсов на администрирование часто приводит к повторным заражениям

- ✓ Предоставляет рекомендации по дизайну, внедрению и поддержанию целевой архитектуры системы обеспечения ИБ
- ✓ Идентифицирует критические уязвимости и слабости конфигурации в Security Fabric, позволяет применить рекомендации, основанные на лучших практикахGuides customers to design, implement and maintain a target security fabric posture
- ✓ Оценивает степень зрелости архитектуре по шкале 1-5
- ✓ Возможность сравнить со схожими организациями

Опции комплектов подписок FortiGate (Bundle)

Ценовая оптимизация стоимости вложений и высокая гибкость в выборе подходящих подписок

Базовая защита инфраструктуры от угроз

Threat Protection
Antivirus + Botnet + Mobile
IPS
FortiCare + App Control

Традиционный комплект подписок «всё в одном»

UTM Protection
Antivirus + Botnet + Mobile
Web Filtering
Anti-spam
IPS
FortiCare + App Control

Автоматизация защиты от современных угроз

Enterprise Protection
FortiSandbox Cloud (incl. VOS + CDR)
Web Filtering
Anti-spam
Antivirus + Botnet + Mobile
IPS
FortiCare + App Control

Матрица комплектов подписок FortiGuard

Bundles	Threat Protection	UTM	Enterprise Protection
FortiGuard Security Rating Service *			•
FortiSandbox Cloud (plus FortiGuard CDR* and VOP* service)			•
FortiGuard Anti-Spam		•	•
FortiGuard Web Filtering		•	•
FortiGuard Antivirus + Botnet + Mobile AV Service	•	•	•
FortiGuard IPS Service	•	•	•
FortiCare + FortiGuard App Control Service	•	•	•

* Available when running FortiOS 6.0 and above

Напоминание - ФСТЭК по новым требованиям

- Новейший сертификат (от 16-го марта 2017)
- Требования к межсетевым экранам ” ФСТЭК России 2016”
- Профиль защиты межсетевых экранов типа А четвёртого класса защиты (ФСТЭК России 2016)
- Профиль защиты межсетевых экранов типа Б четвёртого класса защиты (ФСТЭК России 2016)
- Профиль защиты систем систем обнаружения вторжений уровня сети четвертого класса защиты (ФСТЭК России 2012)
- Требования к системам обнаружения вторжений (ФСТЭК России 2011)
- Классификация по уровню контроля отсутствия недекларированных возможностей – по 4 уровню контроля (Гостехкомиссия России)

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3720

Выдан 16 марта 2017 г.
Действителен до 16 марта 2020 г.

Настоящий сертификат удостоверяет, что **программно-аппаратный комплекс «FortiGate», функционирующий под управлением операционной системы FortiOS 5.4.1**, разработанный компанией Fortinet и производимый ЗАО «Национальный Инновационный Центр» в соответствии с техническими условиями ТУ 5015-003-95561296-15, является программно-техническим средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, соответствует требованиям руководящих документов «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевого экрана типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевого экрана типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011) и «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012).

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ЗАО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ» (аттестат аккредитации от 15.09.2016 № СЗИ.RU.0001.01БИ00.Б010) – техническое заключение от 23.12.2016, и экспертного заключения от 03.02.2017 органа по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: ЗАО «Национальный Инновационный Центр»
Адрес: 121471, г. Москва, Земледельческий пер., д.12
Телефон: (495) 204-2086

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям руководящих документов, указанных в настоящем сертификате, осуществляется испытательной лабораторией ЗАО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации
16 марта 2017 г.

FORTIOS 6.0


Fabric Integration
Tagging
SD-WAN
Certs
Fabric Ready Partners
Automation
Connectors
OS
Developers Network API
CASB
Fabric Agent
FortiGuard
SecurityRating

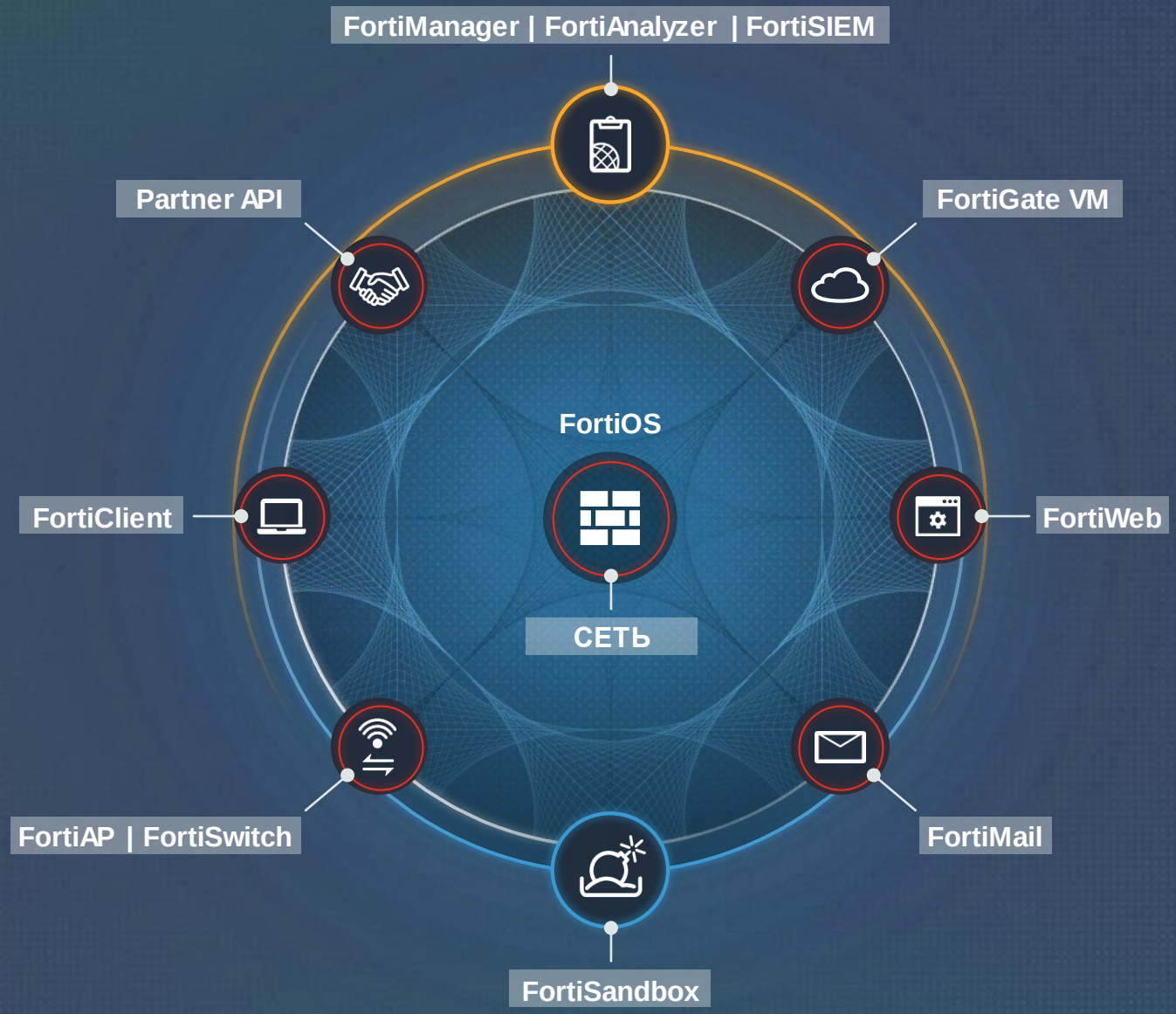
ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ЗНАЧИТЕЛЬНО РАСШИРЯЕТ ПОВЕРХНОСТЬ АТАКИ

2018 FORTINET SECURITY FABRIC

ШИРОТА

ИНТЕГРАЦИЯ

АВТОМАТИЗАЦИЯ



АРХИТЕКТУРА АДАПТИВНОЙ БЕЗОПАСНОСТИ

ОБОРУДОВАНИЕ + ПО + СЕРВИСЫ

ВСЕОБЪЕМЛЮЩАЯ ЗАЩИТА ИНФРАСТРУКТУРЫ

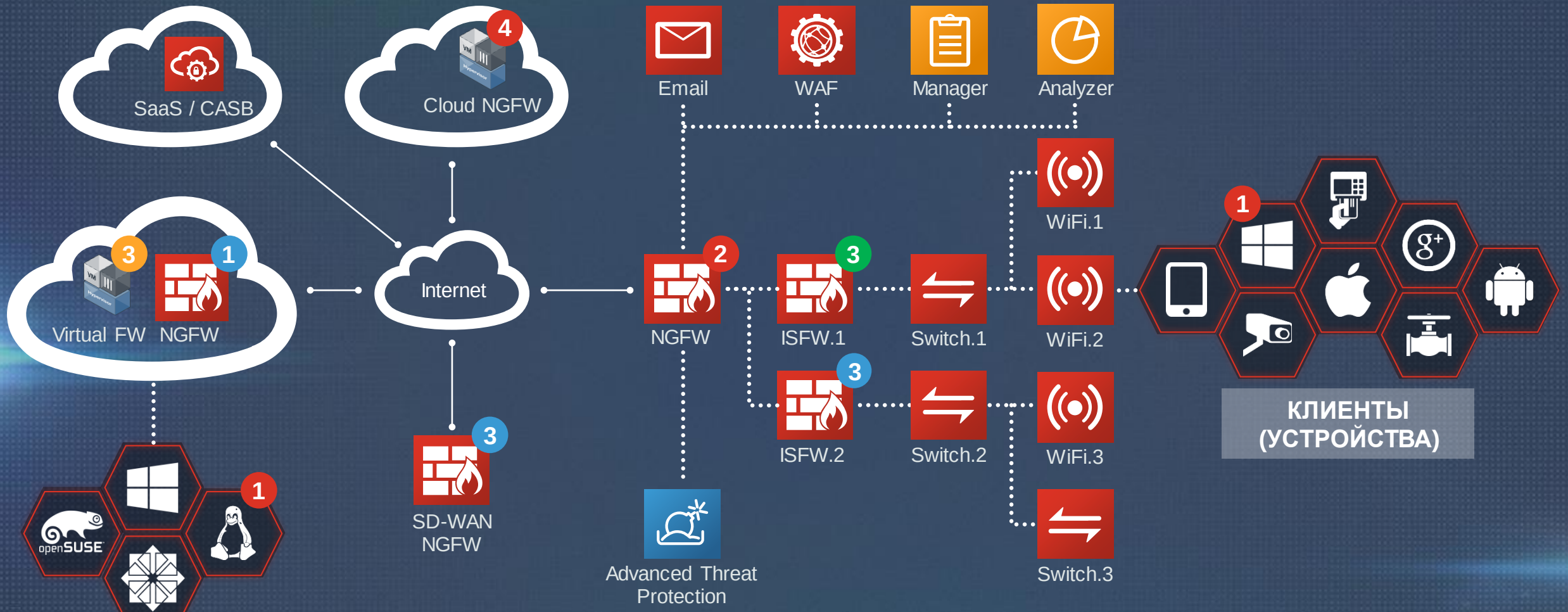
КОНТРОЛЬНЫЙ СПИСОК ИНТЕГРАЦИЙ SECURITY FABRIC

Fabric Integration

	NETWORK	ENDPOINT	UNIFIED ACCESS		EMAIL	WEB APPS		MULTICLOUD
	FORTIGATE	FORTICLIENT	FORTISWITCH	FORTIAP	FORTIMAIL	FORTIWEB	FORTIADC	FORTICASB
TELEMETRY DEVICE LEVEL API	✓	✓	✓	✓	✓	✓	✓	2018
FORTIVIEW TOPOLOGY MAP	✓	✓	✓	✓	2018	✓	✓	
FORTIMANAGER	✓	✓	✓	✓		✓		
FORTIANALYZER	✓	✓		✓	✓	✓	2019	Q1 2018
SECURITY RATING AUDIT	✓			✓	2019	2018		
AUTOMATION STITCHES	✓	✓	✓	2018	2018	✓		
VULNERABILITY SCAN		✓				✓		
ADVANCED THREAT PROTECTION SANDBOX	✓	✓			✓	✓	✓	
FORTISIEM	✓	✓	2018	✓	✓	✓	2018	

FORTINET SECURITY FABRIC - ТОПОЛОГИЯ

Fabric Integration



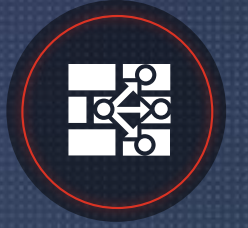
ДИЛЕММА РЫНКА SD-WAN

SD-WAN

Features	SD-WAN Vendors	Security Vendors	Combinations	Fortinet
SD-WAN	✓	⊘	✓	✓
Security	⊘	✓	✓	✓
Cost	=	=	⊘	✓

FORTINET SD-WAN – ЛУЧШЕЕ СОЧЕТАНИЕ ФУНКЦИЙ, ЗАЩИТЫ И СТОИМОСТИ

SD-WAN



Application Aware

Visibility into more than 3500 applications

Application-level transaction for better SLA

Multi-Path Intelligence

Dynamic WAN link selection using Performance SLA

Automated fail-over capabilities

Multi Broadband Supported

Transport independent with support for Ethernet, 3G/4G

Aggregate multiple interfaces into single SD-WAN interface

Simplified Provisioning

One-click VPN to connect multiple branches to the datacenter

Zero-touch provisioning to bring up WAN at a new branch

Certified Security

Most Certified Security such as NSS Labs

High Performance powered by Security Processor technology

КОЛИЧЕСТВО РЕКОМЕНДАЦИЙ ОТ NSS LABS

Certs

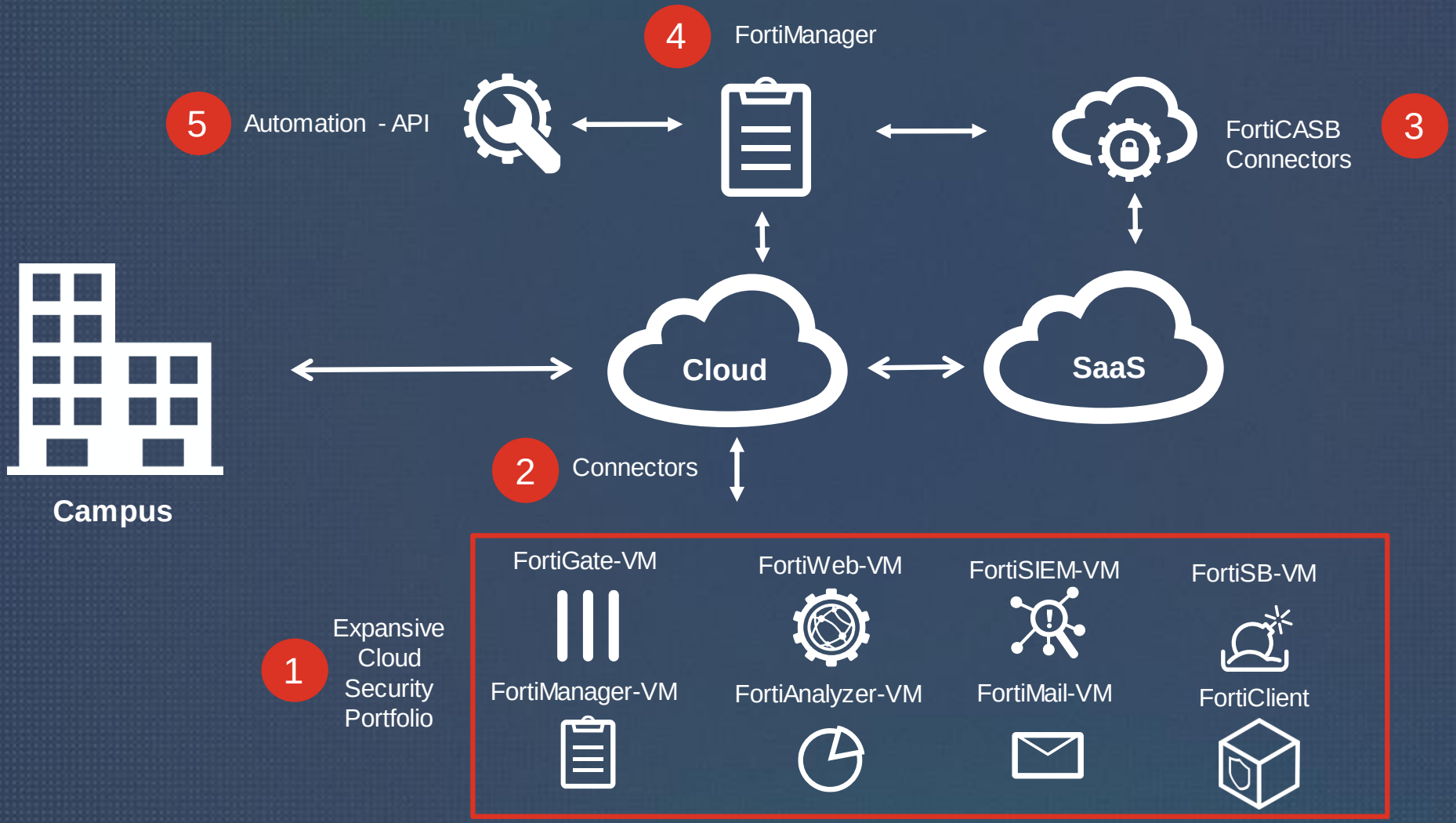
2017 & 2018

11

Рекомендаций

ПОРТФЕЛЬ FORTINET ДЛЯ ЗАЩИТЫ ОБЛАКОВ

Connectors

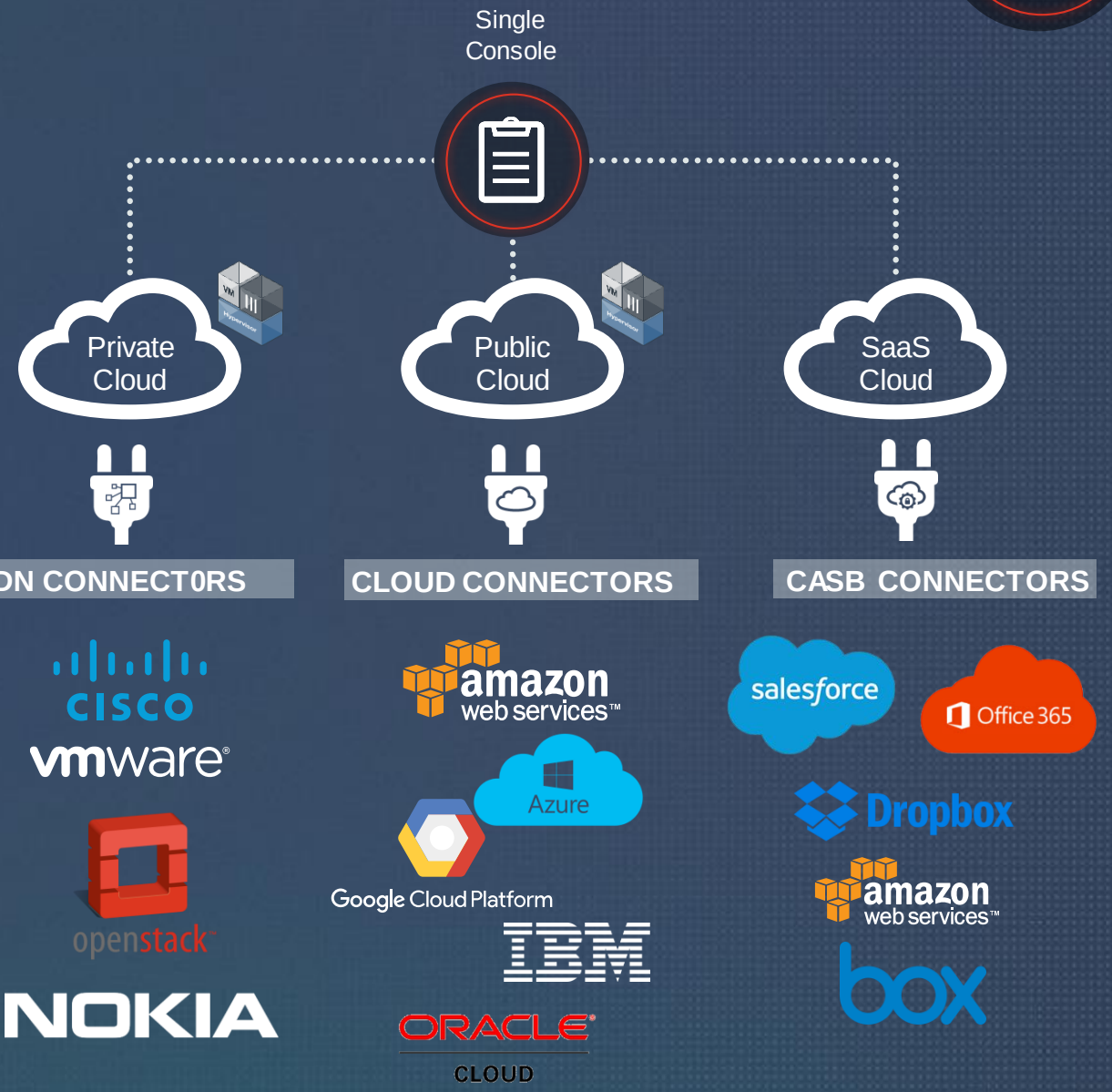


КОННЕКТОРЫ ДЛЯ РАСПРОСТРАНЕННЫХ ОБЛАКОВ И СЕРВИСОВ

Connectors

Private | Public | SaaS

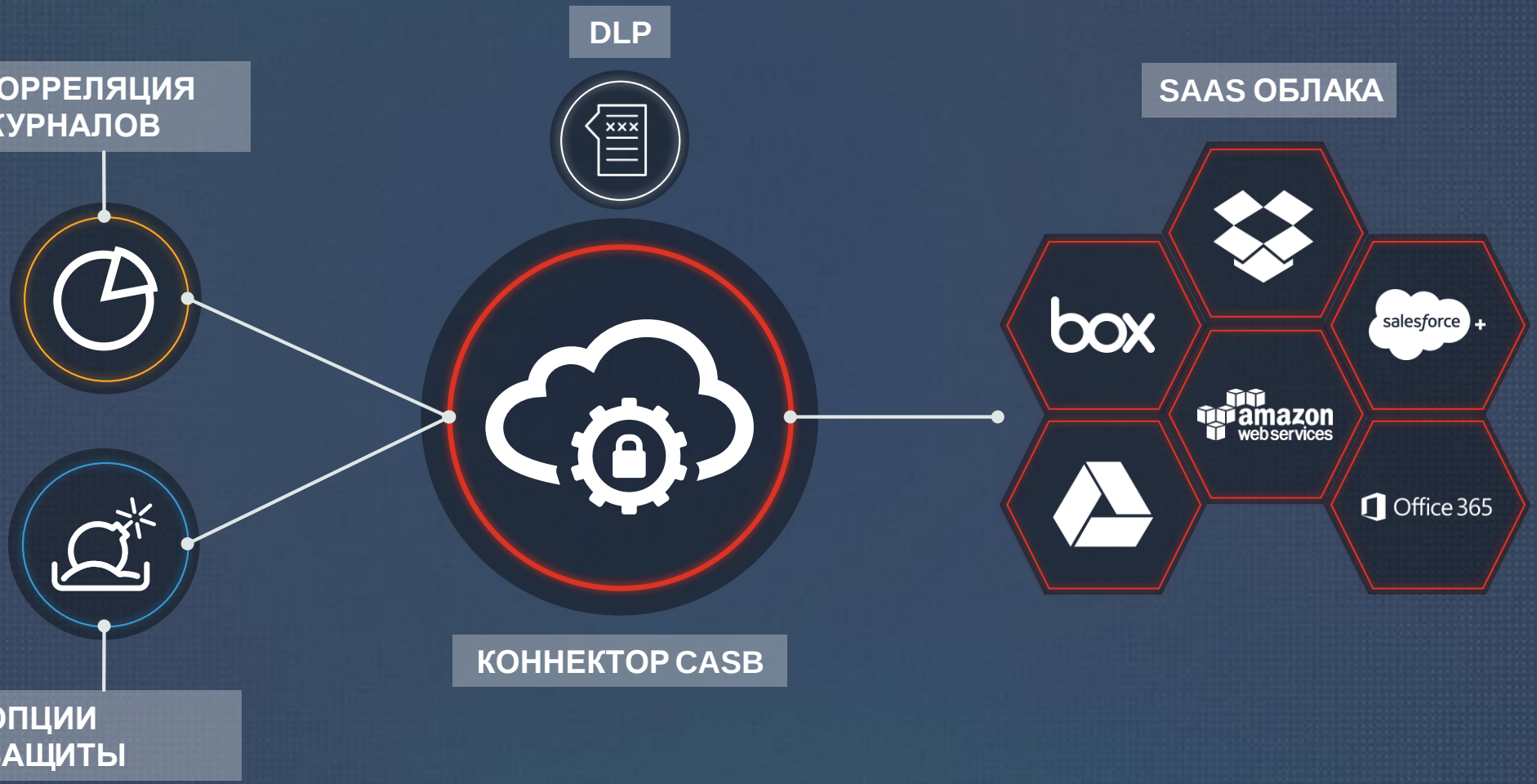
Virtual Security	Cloud Security	API
Applications	Applications	Applications
Data	Data	Data
O/S	O/S	O/S
Virtualization	Virtualization	Virtualization
Servers	Servers	Servers
Networking	Networking	Networking



CASB – КРИТИЧЕСКИЙ КОМПОНЕНТ ЗАЩИТЫ СЕТИ

FORTICASB 1.2

CASB



СЕРВИСЫ ЗАЩИТЫ FORTIGUARD

FortiGuard

Baseline Protection

- IP Reputation
- Internet service DB
- Certificate & Domain white list
- Application Control
- Anti-Spam

+

Threat Protection

- Antivirus
- Intrusion Prevention

Unified Protection

- Web Filtering
- Antivirus
- Intrusion Prevention

Enterprise Protection

- Virus Outbreak Service
- Content Disarm & Reconstruction
- FortiSandbox Cloud
- Web Filtering
- Antivirus
- Intrusion Prevention

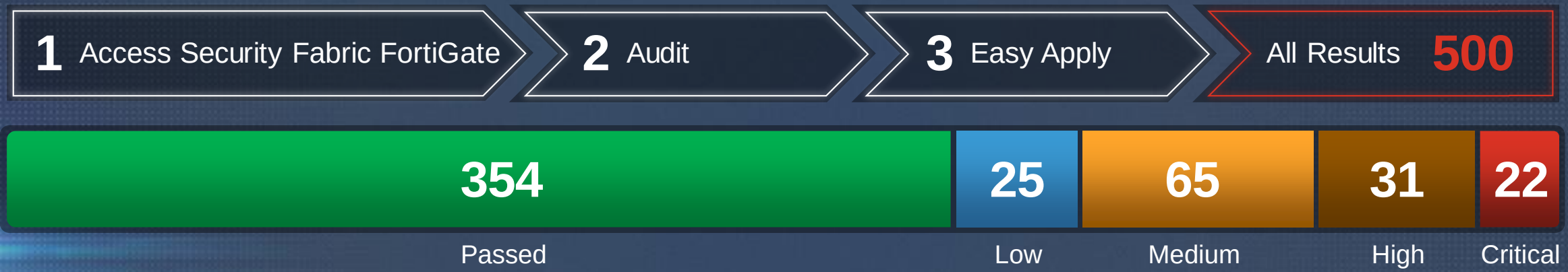
Industrial Security Service

Security Audit Service

SECURITY RATING SERVICE

VULNERABILITY SCAN

Security Rating



9,564	569	126	27	6
Passed	Low	Medium	High	Critical

FABRIC АГЕНТ И ЗАЩИТА УЗЛОВ

ПОДДЕРЖКА СЕРВЕРОВ И АРМ

Fabric Agent

Защита от угроз

Агент VPN

Агент фабрики – сетевая телеметрия

БД Устройств

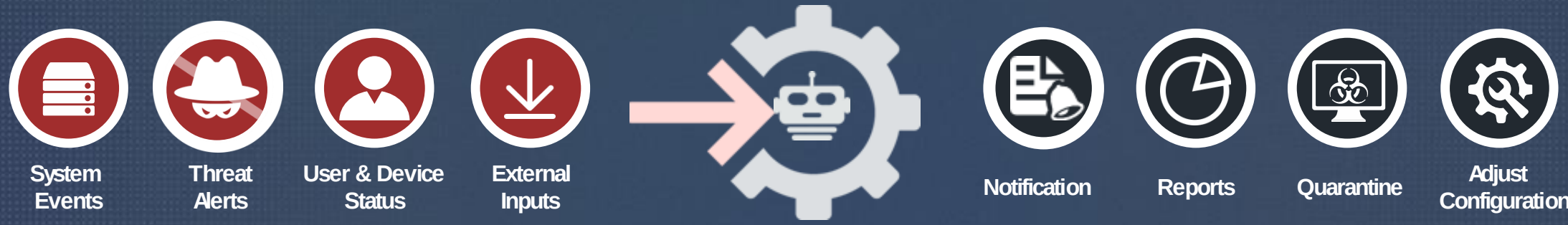
HOSTS (APPS)

ENDPOINT (DEVICES)

IOT (DEVICES)

WORKFLOW - АВТОМАТИЗАЦИЯ

Automation



Триггеры | **Автоматизация реагирования** | **Действия**

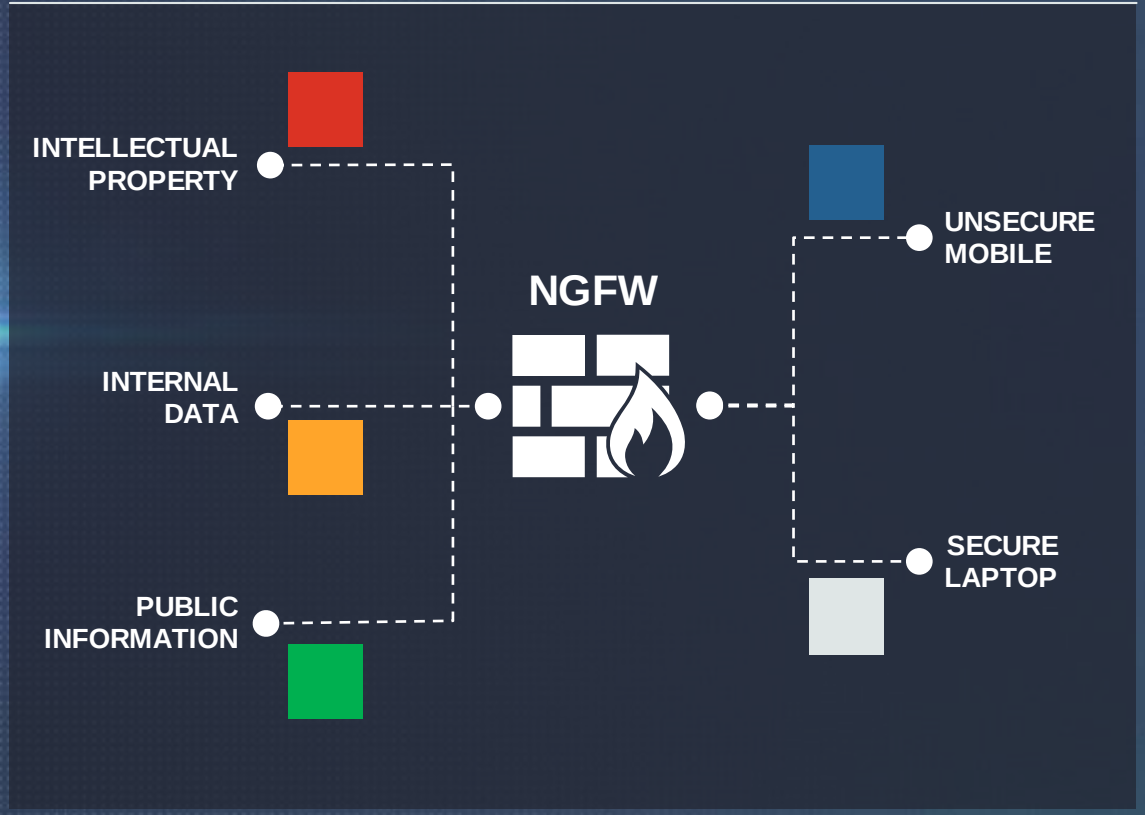
Автоматизация позволяет предпринять соответствующие действия без вовлечения администраторов (например, помещение в карантин)

ЗАЩИТА СЕТИ НА ОСНОВЕ НАМЕРЕНИЙ

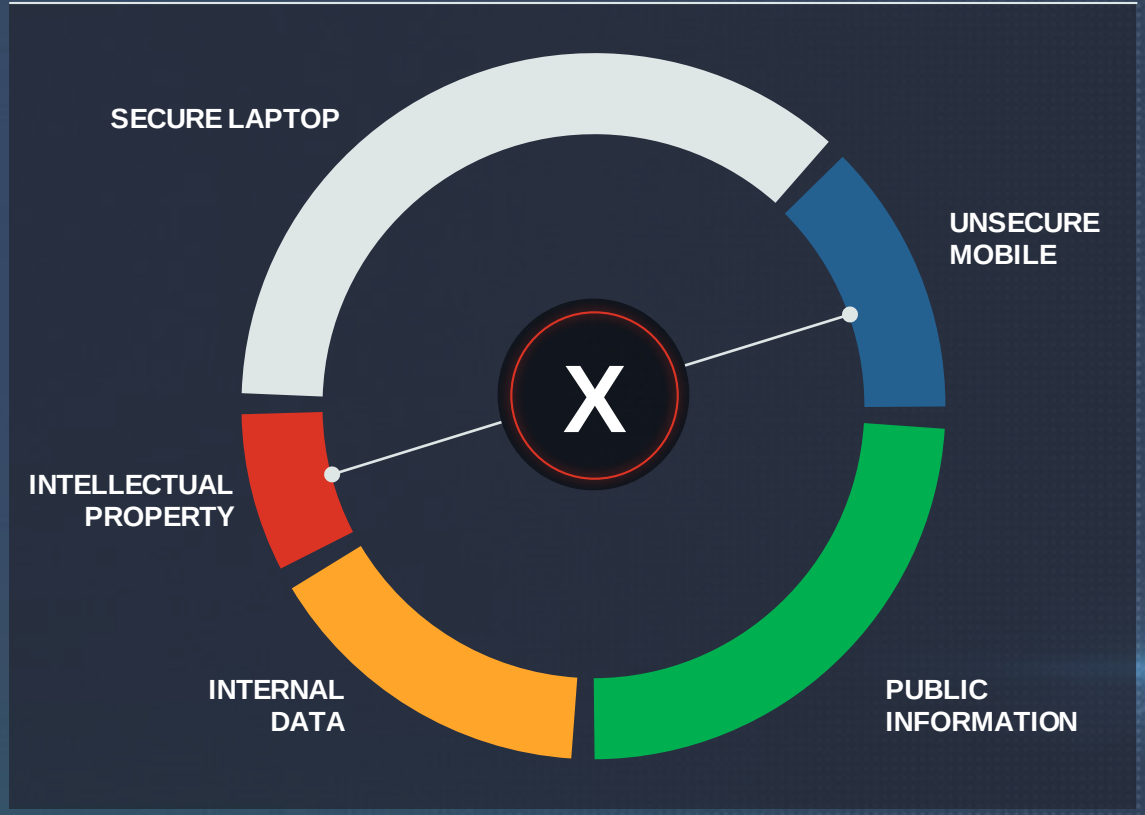
ТЕГИРОВАНИЕ АКТИВОВ

Tagging

TAGGING (DEVICES, INTERFACES, OBJECTS)



GLOBAL POLICY



ПРОГРАММА FABRIC READY

:: WE CONTINUE TO ADD NEW TECHNOLOGY ALLIANCE PARTNERS

Fabric Ready Partners

IBM Security

NEC

vmware®

McAfee™
Together is power.

servicenow

HUGHES®
An EchoStar Company

CYBERARK®

Phantom®

BACKBOX | BACKUP RECOVERY AUTOMATION

MICRO FOCUS®

cyglass

FABRIC READY - ЭКОСИСТЕМА

Fabric Ready Partners

CLOUD

- amazon web services™
- Google Cloud Platform
- ORACLE
- Microsoft Azure
- IBM

SDN

- BROCADE
- cisco
- nuagenetworks
- NEC
- openstack.
- vmware

ENDPOINT

- Attivo NETWORKS
- CARBON BLACK ARM YOUR ENDPOINTS
- McAfee Together is power.
- SentinelOne
- Symantec.
- ziften

MANAGEMENT

- algosec
- FIREMON
- servicenow
- tufin
- BACKBOX

Security/SIEM

- QUALYS Continuous Security
- IBM Security
- Hewlett Packard Enterprise
- CYBERARK
- MICRO FOCUS
- cyglass
- WhiteHat SECURITY.
- Phantom

IOT/OT/NAC

- BRADFORD NETWORKS
- ForeScout
- NOZOMI NETWORKS
- Pulse Secure

IDENTITY

- Centrify
- CLOUDIFY
- CYBERARK

TECHNOLOGY

- ADVA Optical Networking
- HUGHES
- intel
- Sonus Cloud communications made smarter
- VERISIGN

В ЗАКЛЮЧЕНИЕ – СУММАРНЫЙ РЫНОК ИБ - $83B

ЧЕТЫРЕ ОБЛАСТИ РОСТА

Google Cloud Platform Live · amazon web services · vmware · Office · Microsoft Azure · Dropbox · salesforce · cisco

ЗАЩИТА ИНФРАСТРУКТУРЫ

$47B

ЗАЩИТА ОБЛАКОВ

$2B

ЗАЩИТА СЕТИ

$25B

ЗАЩИТА IOT & OT

$9B


FORTINET