Информационная безопасность в цифровом здравоохранении. Актуальные угрозы и методы защиты

3 марта 2022

Виталий Артемьев, директор департамента здравоохранения и ритейл

vartemiev@fortinet.com

Fortinet - мировой лидер в области кибербезопасности, предоставляющий широкую, интегрированную и автоматизированную **Security Fabric**

6.8 млн
Устройств безопасности
Крупнейший поставщик

35%+
Отгрузок Firewall в мире
Крупнейший поставщик

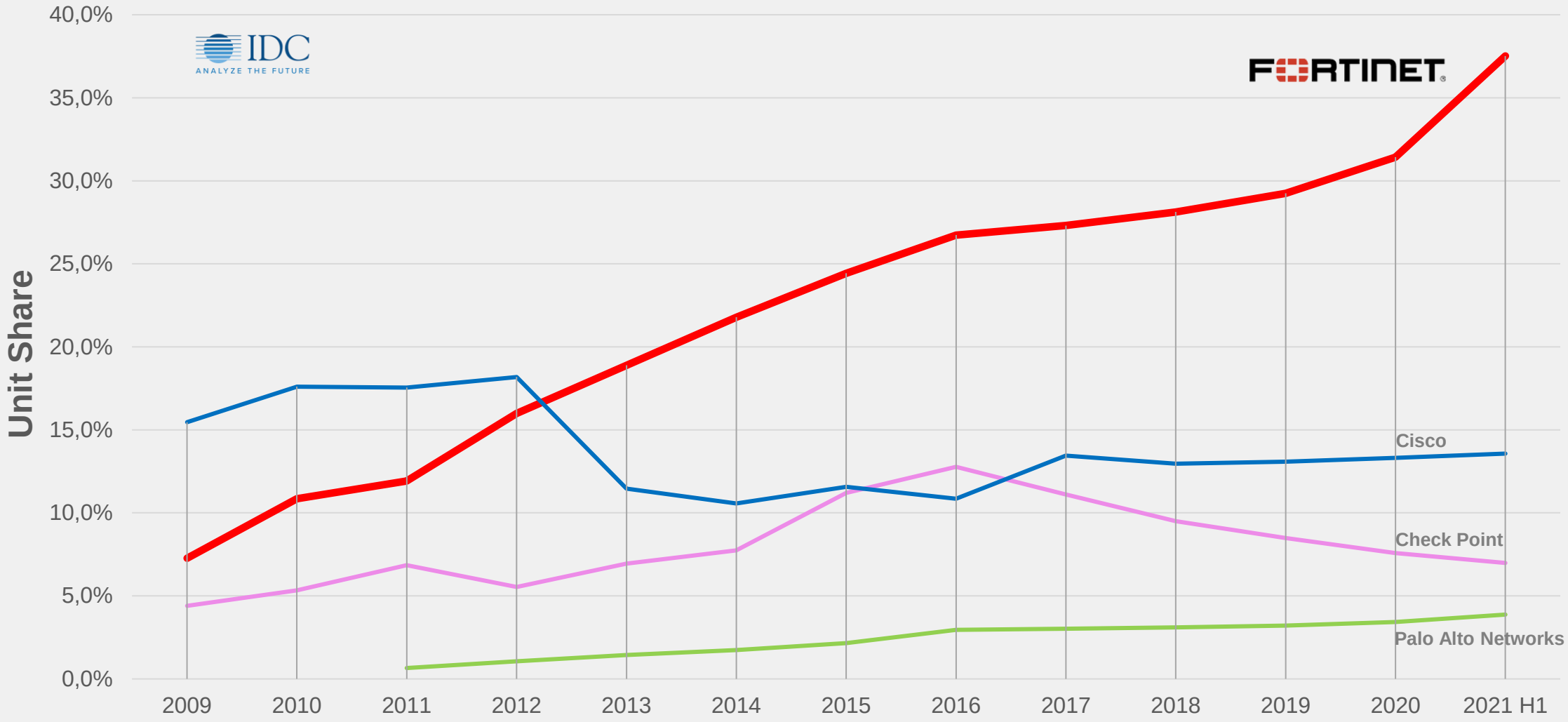
716+
Патентов
Инновационные разработки

50
Интегрированных продуктов
Широкий охват киберугроз

530 000+
Заказчиков по всему миру
Массивный клиентский опыт

660 000+
NSE Сертификатов
WEF Cybersecurity Founders

Fortinet # 1 Более 6.8 миллионов устройств!



FortiGuard Labs

ВИДИМОСТЬ → **ИННОВАЦИИ** → **ПРАКТИЧЕСКАЯ ИНФОРМАЦИЯ ОБ УГРОЗАХ**

Telemetry
Network
Web
Sandbox
Email
Endpoint

Enforcement Partnerships

OSINT

Trusted Partnerships

CERTs

Zero-Day

CTA feeds

FortiGuard Labs

- AI / Machine Learning
- Fortinet Distribution Network
- Detection and protection in milliseconds
- Federated Machine Learning

SECURITY FABRIC PROTECTIONS
- IPS
- Application Control
- Web Filtering
- Anti-Virus
- Anti-Spam
- Endpoint Vulnerability
- Indicators of Compromise (IoCs)

PROACTIVE RESEARCH
- Adversary Playbooks
- Security Blogs
- Threat Intel Briefs
- Threat Signals
- Virtual Patches

THREAT INTELLIGENCE SERVICES
- Penetration Testing
- Phishing Service
- Incident Response

Цифровизация здравоохранения

Цифровые инновации в здравоохранении активно развиваются и предоставляют новые возможности пациентам.

Однако эти жизненно важные усилия также увеличивают площадь цифровых атак и риски кибер-безопасности.

Клиники и лаборатории обеспечены каналами связи

Внедряются медицинские информационные системы

Рабочие места компьютеризованы

Цифровые личные кабинеты для пациентов

Расширяется интернет вещей

Хранение конфиденциальных медицинских данных

Удаленный доступ из любой точки

Нехватка ИТ и ИБ специалистов

ИТ-инфраструктура здравоохранения имеет прямое влияние на здоровье и качество жизни пациентов

Здравоохранение становится мишенью для атак

Объем только фармацевтического рынка в 2021 году превысил 1170 млрд USD

89% фарма компаний

Сталкивались с утечкой данных

$3.86 млн

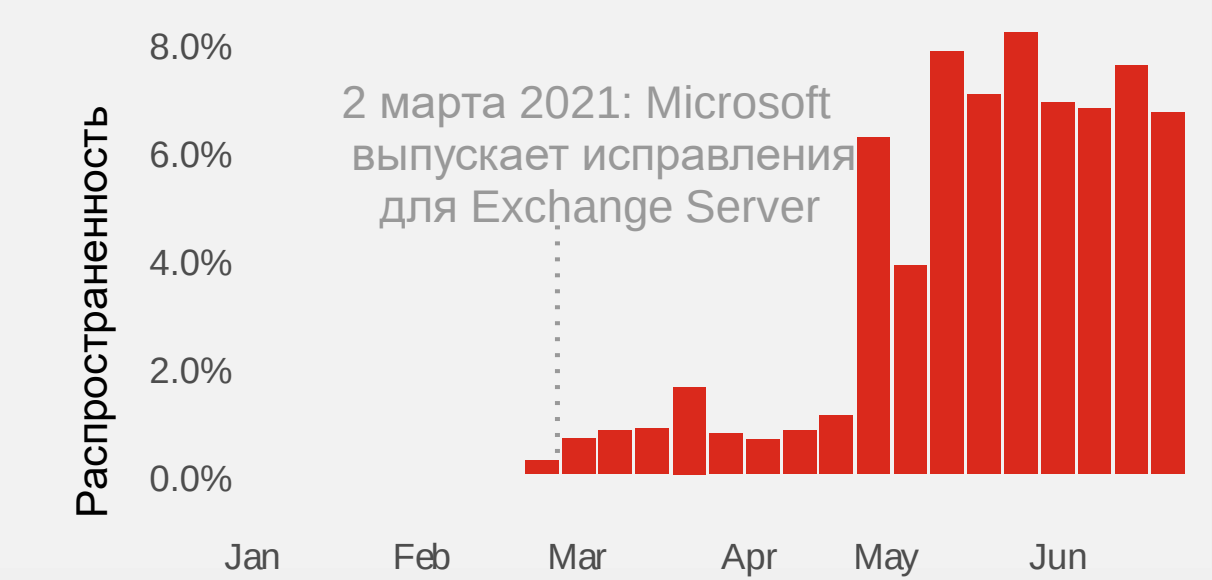
Средний ущерб от утечки данных в 2020 году

203 дня

Среднее время обнаружения уязвимости

Критичные уязвимости приложений

Рост числа, массовая эксплуатация в короткие сроки



Массовые критичные уязвимости:

- **ProxyLogon/ProxyShell**
  - **сотни тысяч уязвимых серверов Exchange**
- **Log4j**
  - **82 минуты от PoC до массовой эксплуатации**

Риски:

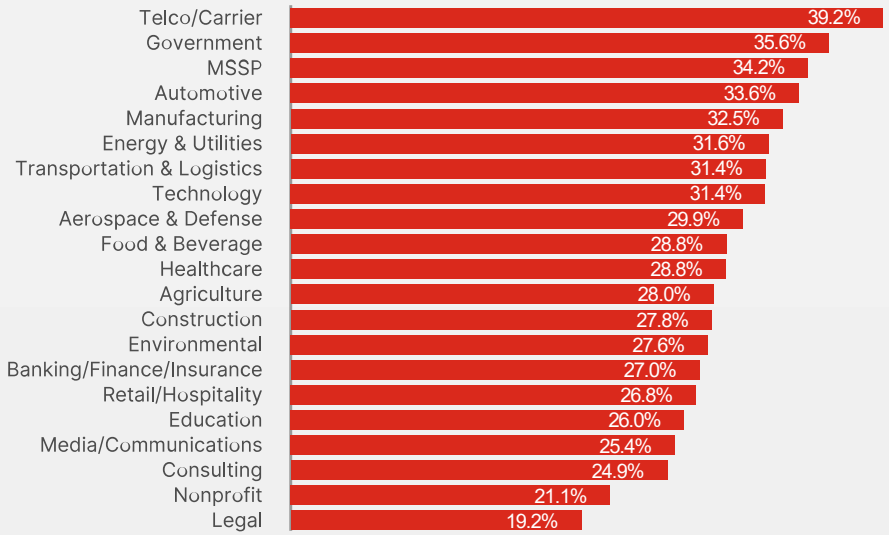
- **Доставка вредоносного кода**
- **Проникновение в инфраструктуру**

Угрозы:

- **Программы-вымогатели**
- **Крипто майнинг**
- **Бот-сети**

Программы-вымогатели (Ransomware)

Безудержный рост активности



>10x — **Рост активности за год (07.2020-07.2021)**

20-40% — **Распространенность по секторам экономики**

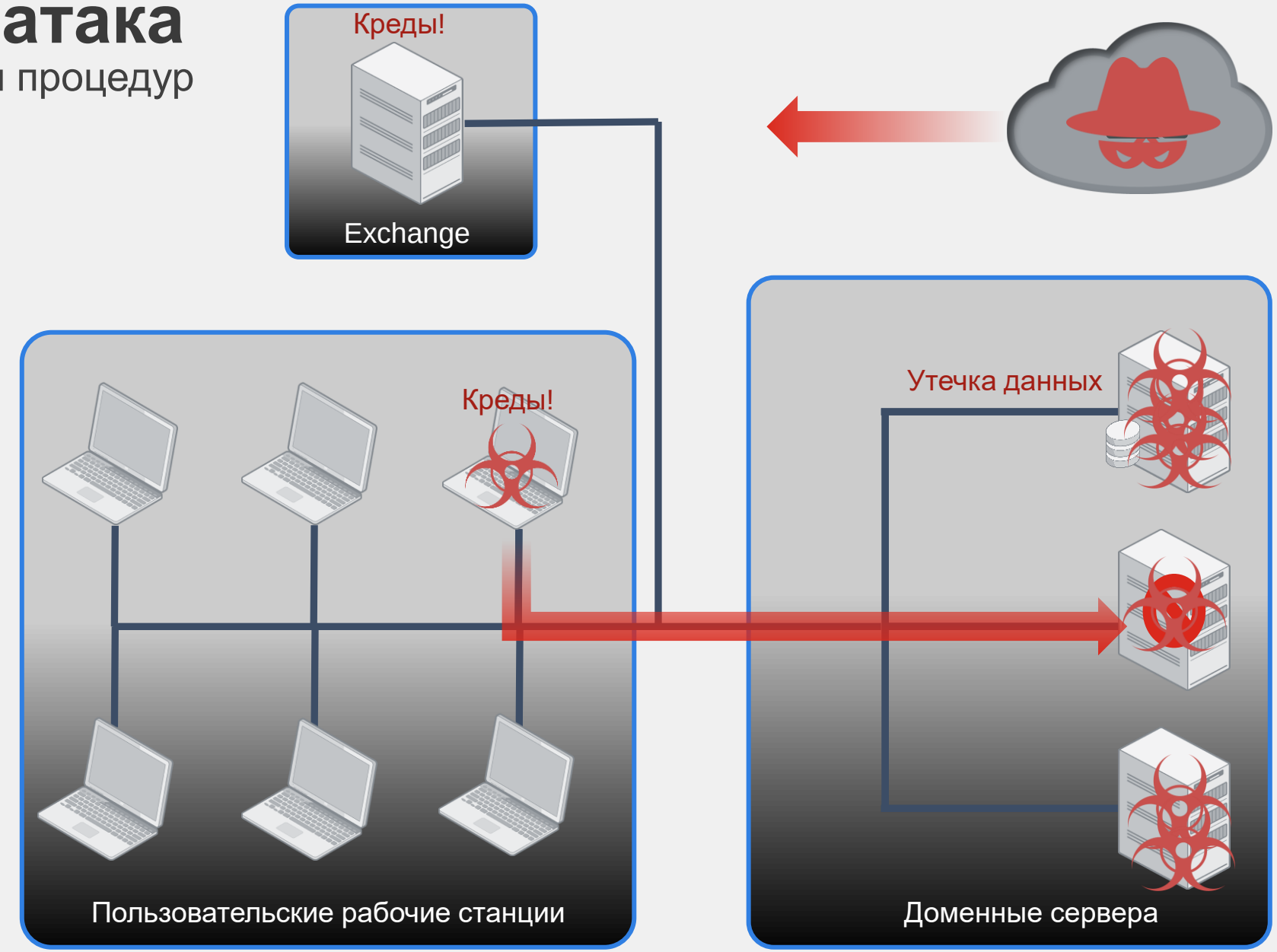
16 дней — **В среднем на устранение инцидента от шифровальщика**

5-10 раз — **Стоимость простоя превышает выкуп**

Как происходит атака

С примерами тактик, техник и процедур

1. **Доставка** – эксплуатация уязвимостей или фишинг (бэкдор)
2. **Похищение учетных записей** – память LSASS
3. **Дальнейшее распространение** – PSEXEC (разведка и распространение ВПО/бэкдоров)
4. **Подавление средств защиты** – Отключение MS Defender, установка ВПО
5. **Хищение данных** – хищение, либо другие цели (резервное копирование отключается)
6. **Доставка программ-вымогателей** –установка в групповых политиках сценария входа или авто-запуска



Остерегайтесь первичного заражения!

Первичное заражение возможно даже путем эксплуатации систем, являющихся основой вашей инфраструктуры!

*Арсенал уязвимостей, которые используют группы ransomware-вымогателей для обеспечения первичного доступа к целевым системам.

Постоянно отслеживайте рекомендации производителей по исправлению обнаруженных уязвимостей!

Комплексная защита

Архитектура решения

Технологии предотвращения доставки

Технологии выявления и подавления подозрительной активности

FortiGate/FortiSASE

Шлюз безопасности (Network Firewall)

- Снижение поверхности атаки
- Предотвращение распространения вредоносного кода и эксплуатации уязвимостей

FortiWeb

Межсетевой экран веб-приложений (WAF)

- Предотвращение эксплуатации уязвимостей приложений
- Защита от загрузки вредоносного кода

FortiMail

Шлюз электронной почты (SEG)

- Предотвращение доставки вредоносного кода
- Предотвращение фишинга
- Защита от мошенничества

FortiSandbox

Сетевая песочница

- Анализ поведения файлов и ссылок
- Формирование индикаторов

FortiAI

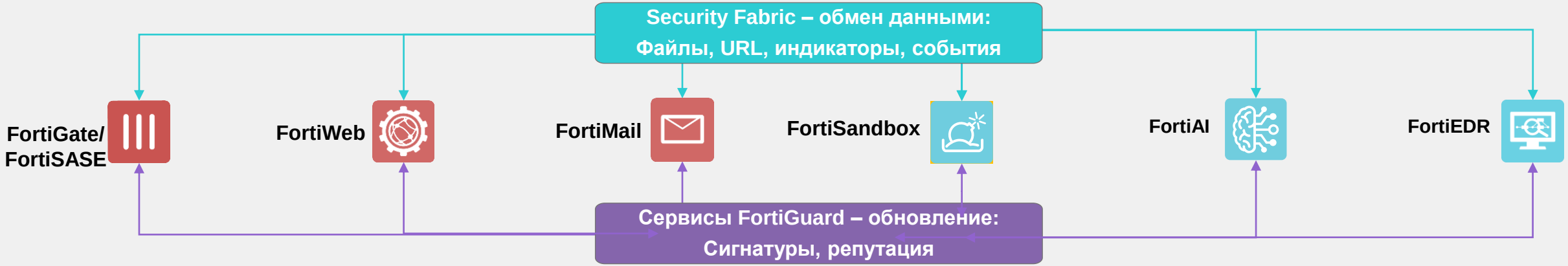
Локальный искусственный интеллект

- Исследование файлов с помощью нейронной сети
- Мгновенная реакция, высочайшая производительность

FortiEDR

Продвинутая защита конечных точек

- Предотвращение заражения
- Обнаружение и подавление действий злоумышленника



ПАК | Виртуальная Машина | Облако | Безопасность -как-Сервис | Программное Обеспечение

Единая экосистема продуктов Fortinet Security Fabric

Generic Known Threat

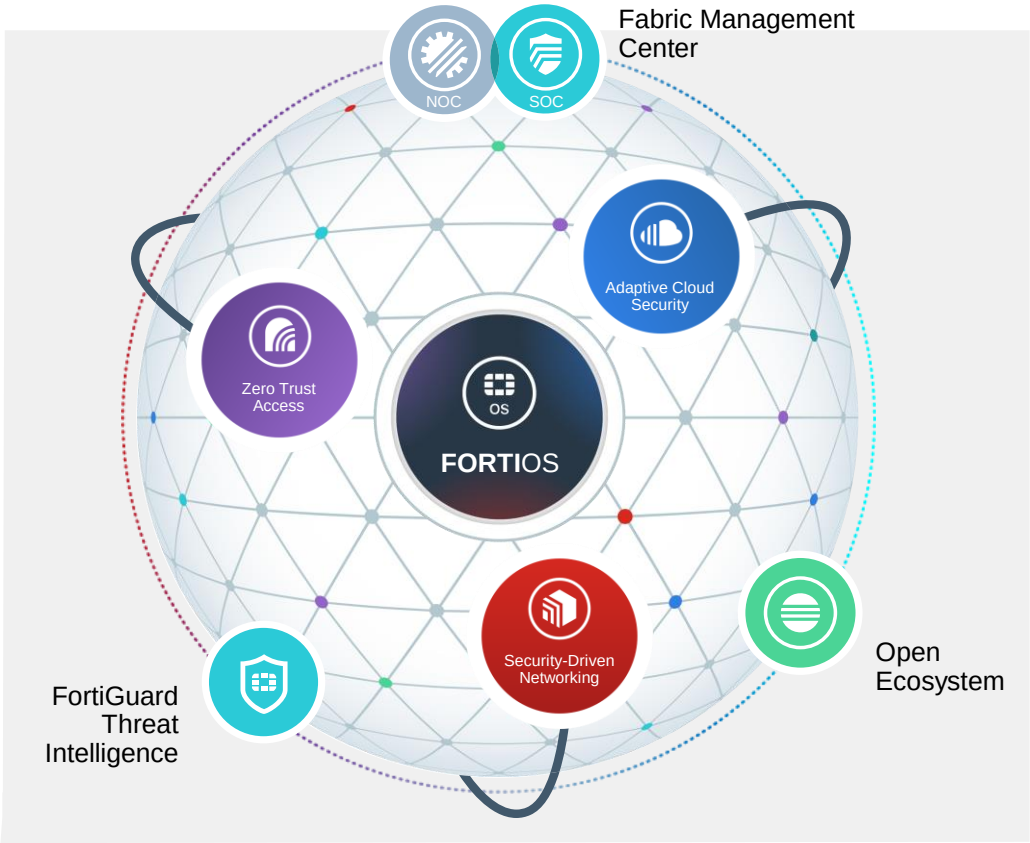
Generic Unknown Threat

Ransomware

Advanced Threat

Worms

Machine to Machine Attack



DearCry Ransomware

Artificial Intelligence

Flood/DDoS Attack

Bitcoin Mining

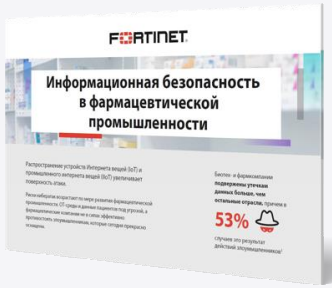
Hacker Group

Machine Learning Poisoning

Malicious Code

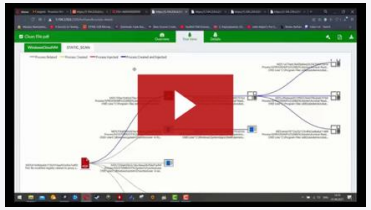
emea.fortinet.com/pharma-ru

Отрасль здравоохранения состоит из нескольких высокотехнологичных сегментов (медицинские услуги, исследования и производство, реализация), каждый из которых, - это свой набор технологии, бизнес-моделей и задач. Многие компании находятся сейчас в процессе цифровой трансформации, в рамках которой происходит автоматизация коммерческих, хозяйственных и промышленных процессов предприятия. Таким образом к уже существующим и понятным угрозам добавляются новые - угрозы, связанные с автономностью, новыми данными и онлайн-приложениями.



СКАЧАТЬ БРОШЮРУ

Демонстрация возможностей Fortinet Security Fabric



СМОТРЕТЬ ВЕБИНАР

Компания Fortinet присутствует на рынке информационной безопасности и инфраструктурных решений более 20-ти лет. Весь опыт компании сегодня представлен в виде уникальной в отрасли платформе информационной безопасности Fortinet Security Fabric. Fortinet Security Fabric состоит из множества функциональных модулей, каждый из которых представляет собой специализированное решение для защиты определенной части предприятия: инфраструктуры, процесса, приложения или актива. Выделенные элементы централизованного управления и аналитики синхронизируют действия всех модулей, заставляя их работать комплексно, усиливая друг друга. Комбинируя состав решения Fortinet Security Fabric можно получить эффективный набор средств противодействия, четко соответствующий структуре вашего предприятия.

Клиники, лаборатории и удаленные филиалы

УЗНАТЬ БОЛЬШЕ

Защищенный периметр

УЗНАТЬ БОЛЬШЕ

Проводной и беспроводной доступ

УЗНАТЬ БОЛЬШЕ

Защита web-порталов и мобильных приложений

УЗНАТЬ БОЛЬШЕ

Безопасность работы удаленных сотрудников

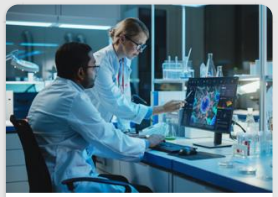
УЗНАТЬ БОЛЬШЕ

Экономическая эффективность

УЗНАТЬ БОЛЬШЕ

Телемедицина и защита персональных данных

УЗНАТЬ БОЛЬШЕ



Видеонаблюдение

УЗНАТЬ БОЛЬШЕ

Телефония

УЗНАТЬ БОЛЬШЕ

Создание надежного и защищённого цифрового мира

Миссия Fortinet - защита людей, устройств и данных повсюду!