FORTINET

Информационная безопасность как основа Цифрового Лидерства

Назим Латыпаев

nlatypayev@fortinet.com

Вопросы доверия

„У тебя не может быть лучшего завтра, если ты все время думаешь о вчерашнем дне.“

Чарльз Франклин Кеттеринг

© Fortinet Inc. All Rights Reserved.

Предположения о Кибербезопасности

© Fortinet Inc. All Rights Reserved.

Осознанность в ИБ или как быть в потоке ИБ?

© Fortinet Inc. All Rights Reserved.

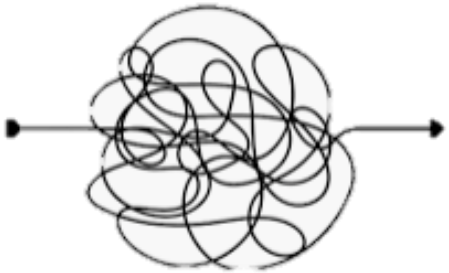
Историческая перспектива кибербезопасности

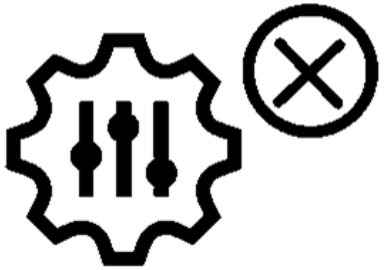
	2000 - 2010	2011-2020	2020+
Технологии кибербезопасности	Защита на Основе Сигнатур	Обнаружение и реагирование	ИИ и Автоматизация
	Antivirus, Antispam, URL Filtering	EDR, Sandbox, NDR	ML/AI, Operations
Инфраструктура	Новые Векторы Угроз	Расширенная Поверхность Атаки	Распределенная Поверхность Атаки
	Files, Email, Web	WFA, Mobile, Cloud	OT/IoT, 5G, Edge
Предложения в Индустрии	Защита конечных станций	Сетевая Защита	Защита Платформ
	Endpoint	Network	Endpoint, identity, Network, Native

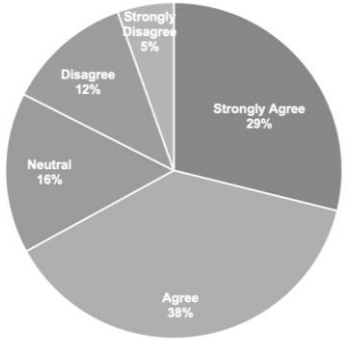
© Fortinet Inc. All Rights Reserved.

Текущее состояние – Отсутствие Синергии

Отсутствие основы для использования современных передовых технологий, обеспечивающих централизованное и автоматизированное обнаружение и реагирование со скоростью машины.







Сложность

Сложность продуктов по ИБ и Сетевой Инфраструктуры

Много «Уникальных» решений

Трудно сбалансировать лучшее в своем классе с интегрированной и синергетической безопасностью

Изоляция

Инструменты безопасности и команды, которые работают изолированно и требуют ручной работы

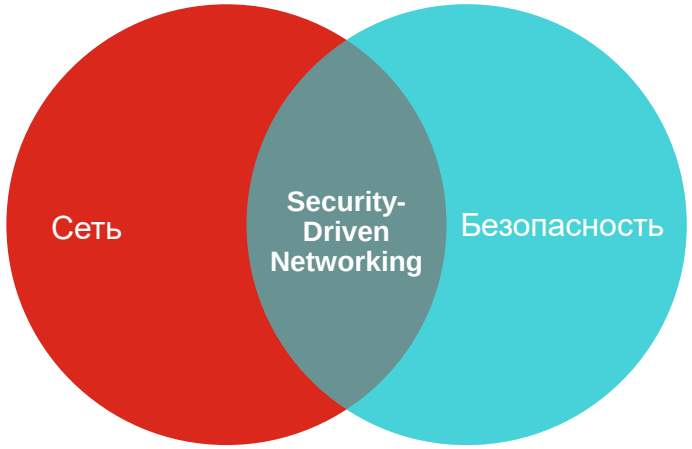
Перегруженные люди

Недостаток навыков + большой объем угроз = перегруженные службы безопасности

© Fortinet Inc. All Rights Reserved.

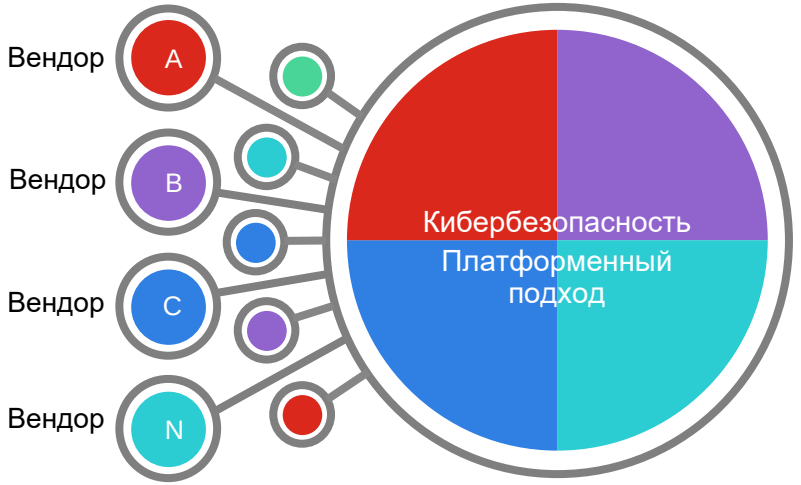
Стратегические тренды и технологии кибербезопасности

Уменьшение сложности



Конвергенция сети и безопасности

Достижение Синергии



Консолидация поставщиков продуктов ИБ

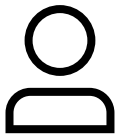
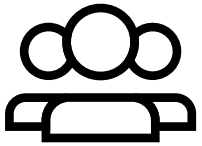
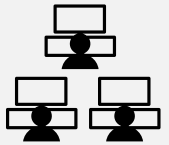
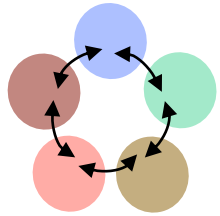
Централизация и Автоматизация

Сеть и SOC под управлением ИИ

© Fortinet Inc. All Rights Reserved.

Конвергенция vs. Консолидация

В чём разница?

	Конвергенция	Консолидация
Вендор	1	1-3
Рабочих групп	 Один	 Несколько
Система управления	 Один	 Несколько
Продукт	 Один	 Несколько

© Fortinet Inc. All Rights Reserved.

Действуйте заранее

Не показывайте слабости

начиная с этапа разведки

Снижение рисков на раннем этапе

- Управление внешней поверхностью атаки
- Защита бренда
- EDR

Всегда Ищите

потенциальные пробелы – и исправляйте их

Оценки кибербезопасности

- Уязвимость
- Оценка готовности к целевым атакам - (ransomware, phishing, email)

Люди - ваша уязвимость

– оценивайте и «патчите» их

Обучение кибербезопасности

- Гигиена кибербезопасности
- Социальная инженерия
- Анти-Фишинг

Стремитесь Узнать Больше– Разведка Ориентированная на Противника (ACI)

Работайте умнее

Инвестируйте в Threat Intelligence

- Создавайте общую картину
- Нормализуйте и централизуйте данные безопасности
- Каналы информации о глобальных угрозах
- Активируйте функции безопасности
- Убедитесь, что в ваших логах есть значимые данные.

Замедляйте противника

- Возможности расшифровки
- Нулевое доверие и сегментация
- Технологии приманки (Honeypot)
- Обнаружение и ответ в сетевых технологиях

Конвертируйте информацию в интеллектуальные данные

Сопоставляйте и используйте несколько форм машинного обучения (централизованного, распределенного и федеративного) для создания упреждающей, предиктивной и централизованной аналитики.

Побеждайте быстрее

Автоматизируйте

- Машинное Обучение (локальная и облачная доставка)
- Проактивная и единая политика
- Думаете о Гибридной системе
- Инвестируйте в сборники сценариев атак
- Обнаружение эпидемий ИБ

Дополняйте SOC

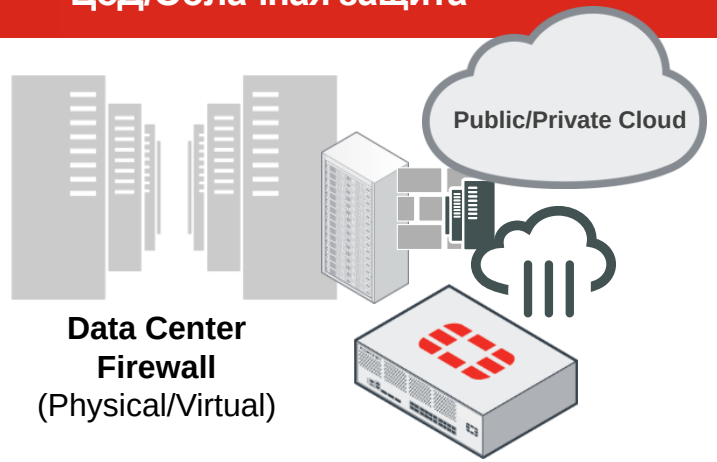
- SOC как Service
- Криминалистика на уровне клиента
- MDR
- Реагирование на инцидент
- Оповещения о вспышках похожих инцидентов

Практика делает вас Лучше (и Быстрее)

- Постоянное обучение
- Обучение сотрудников в рабочей инфраструктуре
- Разработка и улучшение сборников сценариев атак
- Моделирование атак

Fortinet решает задачи вашего бизнеса

ЦоД/Облачная защита

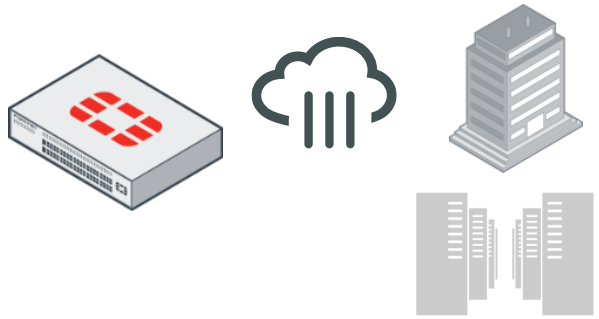


Data Center Firewall
(Physical/Virtual)

SOC

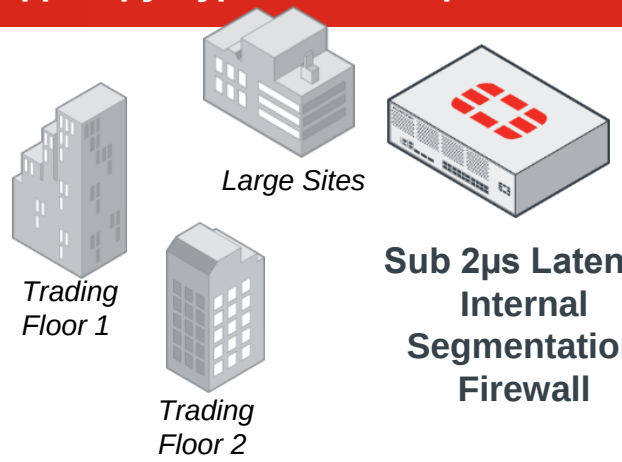
SOAR / SIEM / Correlation / Risk Analysis / Compliance
FortiGuard Threat Intelligence

Инспекция Контента



Next Gen Firewall

Ифраструктура для электронных площадок

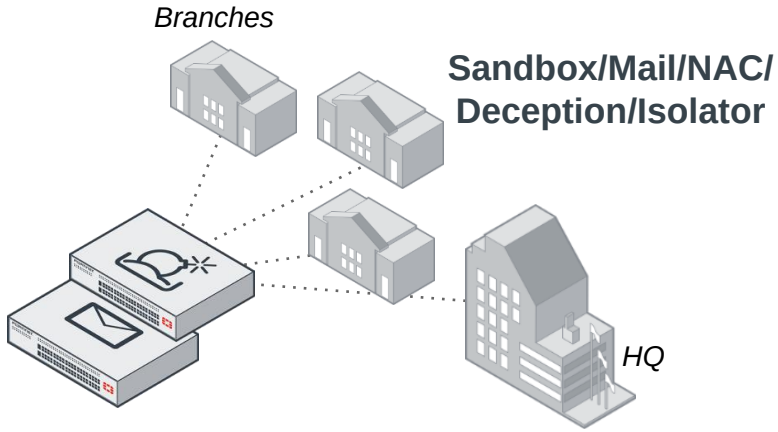


Sub 2µs Latency Internal Segmentation Firewall

Защищенный Филиал

SD-WAN / SD-Branch / End Point Protection

Общая Защита Бизнеса



© Fortinet Inc. All Rights Reserved.

Fortinet Security Fabric

Масштабируемая

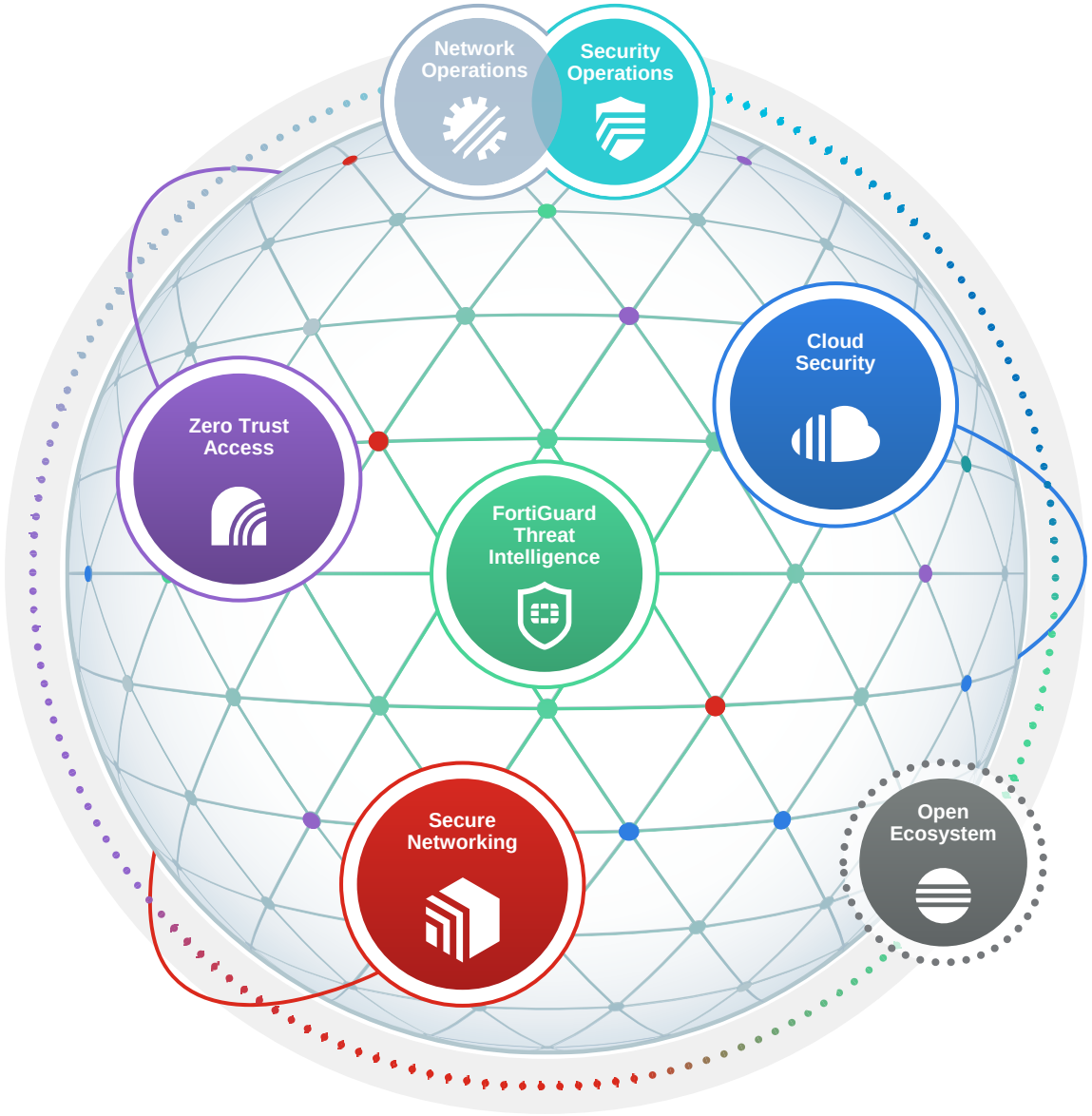
видимость и защита всей поверхности цифровых атак для лучшего управления рисками

Встроенная

решение, упрощающее управление и предоставляющее доступ к сведениям об угрозах

Автоматизированная

самовосстанавливающиеся сети с безопасностью на основе ИИ для быстрой и эффективной работы



Appliance

Virtual

Hosted

Cloud

Agent

Container

© Fortinet Inc. All Rights Reserved.

Назим Латыпаев
nlatypayev@fortinet.com