«Сетевая безопасность: проблематика, обзор NGFW-решений»

Верещагин Виктор

Менеджер по развитию бизнеса в ЦФО

Угрозы сетевой безопасности

Черви, вирусы, трояны, backdoors и вымогатели – наиболее распространённые типы вредоносов

- **Вирусы** и черви (Viruses & worms)

(WannaCry, Petya, Xafecopy Trojan, Kedi RAT, Thanatos, Titanium)

- Теневые **загрузки** (Drive-by Download)

(LoadPCBanker, YoukuTudou и другие вредоносные сайты)

- **Бот**-сети (Botnets)

(Emotet, Trickbot, Dridex, Roboto)

- **Фишинг** и социальная инженерия (Phishing)

(email, business email compromise (BEC), company impersonation, websites)

- Эксплойты, **уязвимости** (Exploit Kits)

(EK: Spelevo, Fallout, Magnitude, RIG, GrandSoft, Underminer, KaiXin, Purplefox, Capesand)

- **Отказ** в обслуживании (Denial of Service)

(LDAP amplification, DNS-service Router 53, Flood: ICMP, HTTP, TCP, UDP)

- **Шифровальщики** (Ransomware)

(STOP (DJVU), Dharma, Phobos, GlobeImposter, REvil, GandCrab, Magniber, Scarab, Rapid, Troldesh)

- **Криптомайнинг** (Cryptojacking)

(in-browser (websites, cryptomining scripts), Coinhive (JavaScript miner), Cryptoloot)

- Целенаправленные **угрозы** (APT)

(Угрозы «нулевого» дня, бесфайловые атаки, незаметное присутствие злоумышленника, горизонтальное перемещение и т.д.)

KILL CHAIN

Процесс, описывающий продвижение злоумышленника внутри сети

LOCKHEED MARTIN

ЦЕЛЬ АТАКИ

- Разведка (Reconnaissance)
- Подготовка (Weaponization)
- Доставка (Delivery)

ЗАРАЖЕНИЕ

- Исполнение (Exploitation)
- Установка (Installation)

ВЗЛОМ

- Управление (Command & Control)
- Действия (Actions on Objectives)






Каналы распространения угроз

Электронная почта и Интернет-трафик – наиболее доступные и распространённые векторы атак

- Электронная почта (POP3, IMAP, SMTP)

- Мобильные устройства (ОС, фишинг, файлы, ПО, Wi-Fi)

- Интернет-трафик (HTTP, HTTPS)

- Облачные сервисы (Office 365, Dropbox, AWS, гибридные и частные облака)

- Конечные станции (USB, файлы, ОС, ПО)

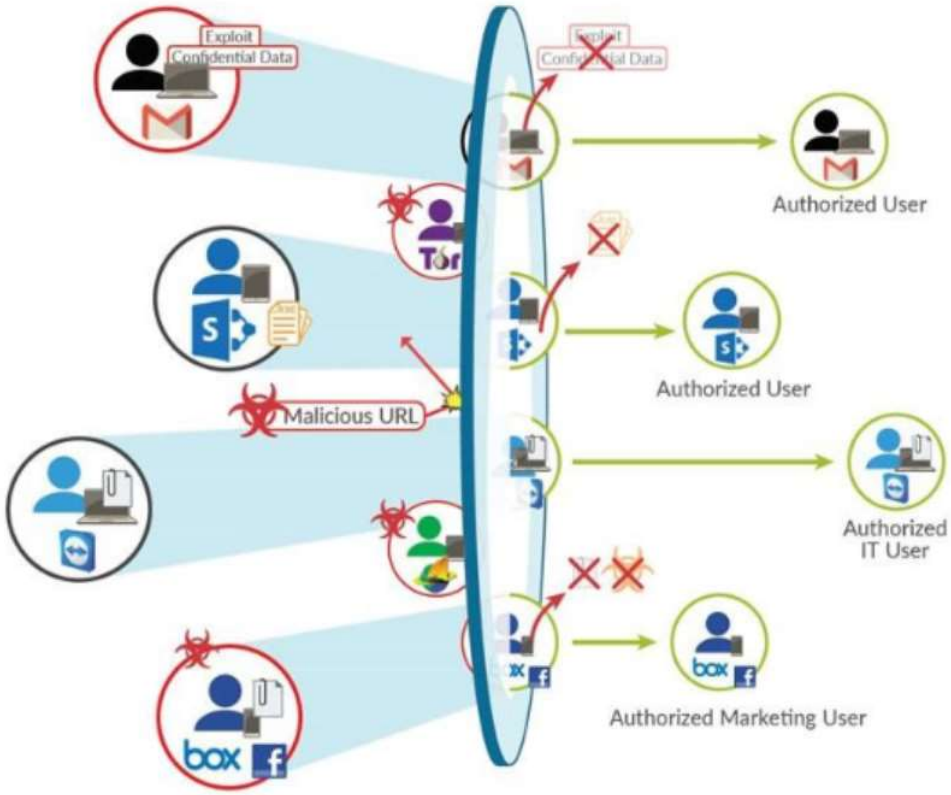
- Файловые хранилища (CIFS, SMB, NFS, FTP, Облако)

- Другие каналы распространения (DNS, веб-приложения, мессенджеры, внутрикорпоративная сетевая активность, аномальное поведение сотрудников)

Ключевые возможности решения

Технологии по анализу сетевого трафика

- Встроенная глубокая проверка пакетов (Deep Packet Inspection, DPI)
- Предотвращение вторжений (Intrusion Prevention System, IPS)
- Проверка трафика на уровне Приложений (Application Control, AC)
- Потоковая антивирусная проверка (Stream Antivirus, SA)
- Проверка зашифрованного трафика SSL/TLS и Веб-фильтрация (URL-Filtering)
- Интеграция с Active Directory (AD) и Песочницей

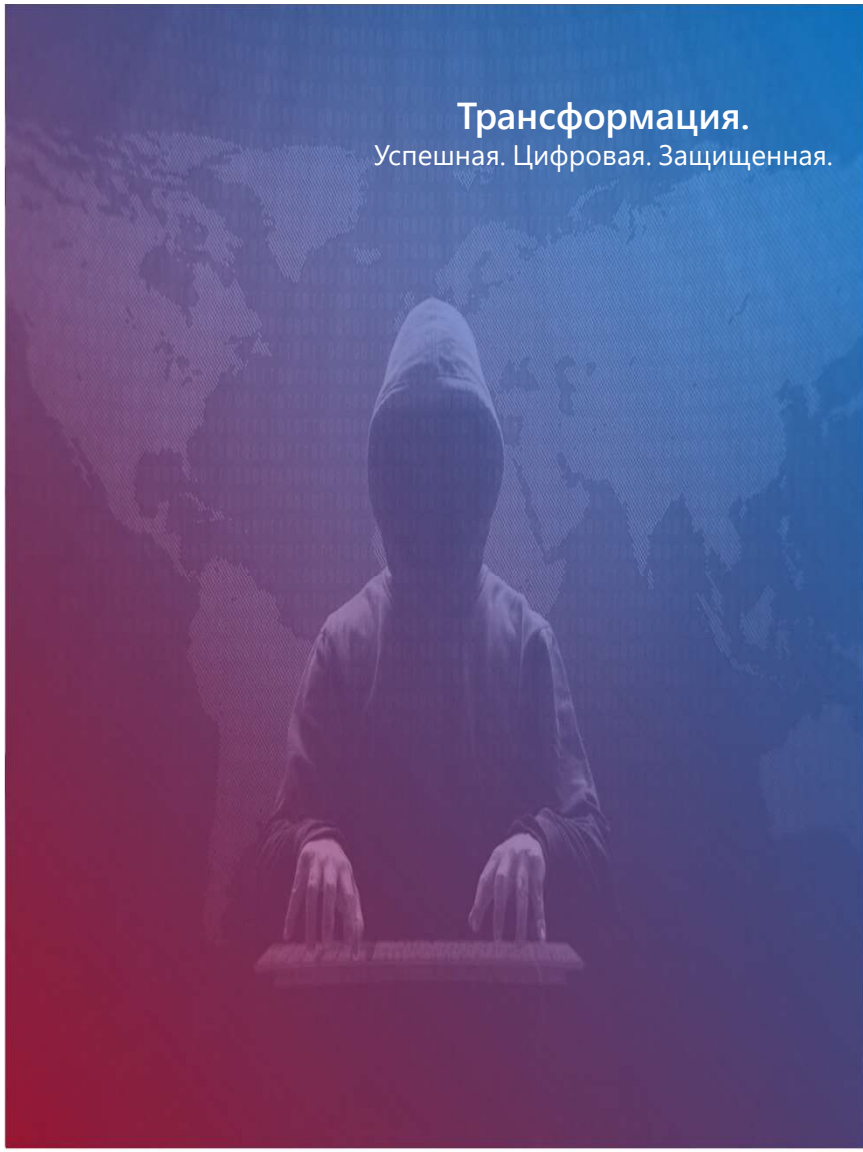


Угрозы кибербезопасности в РФ

Статистика на территории Российской Федерации

Кратный рост числа DDoS-атак:
- Государственные организации
- Банки
- Сайты СМИ

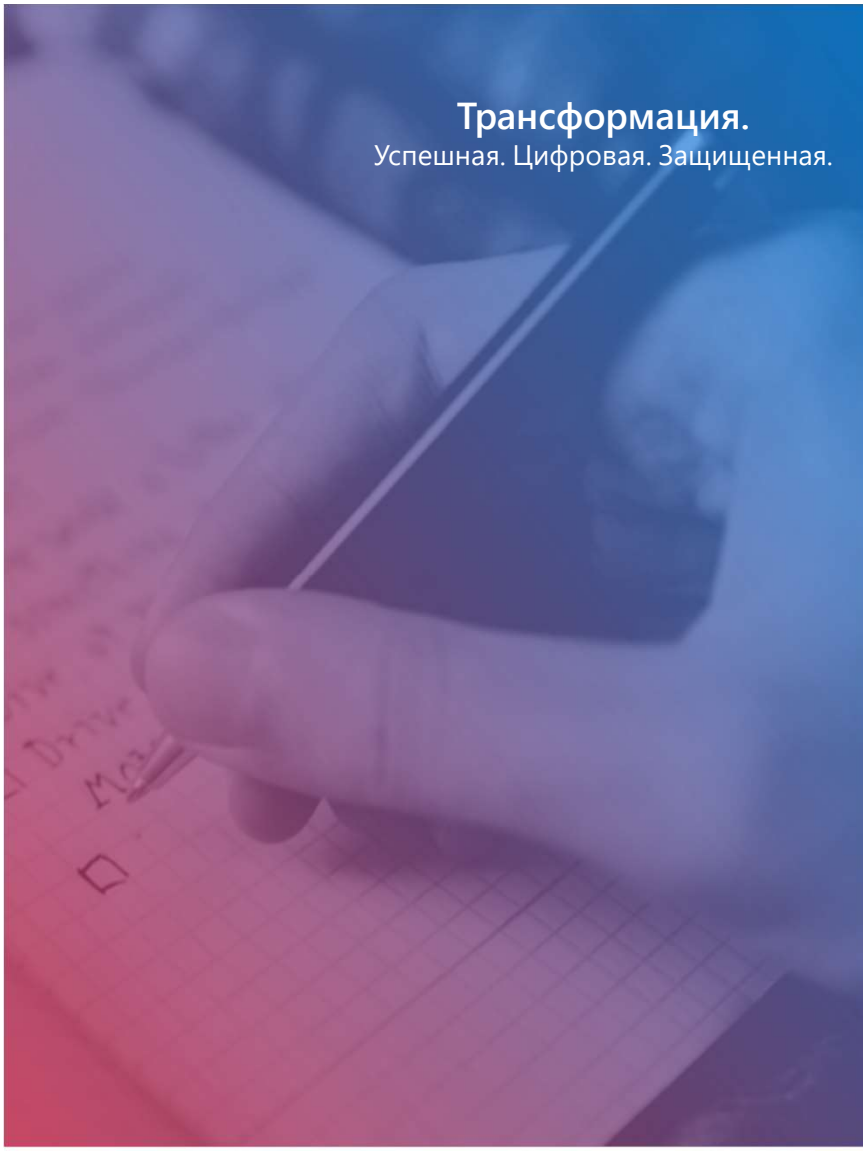
Векторы атак:
RUS, РУС, РОС, .ru, .рф и др.



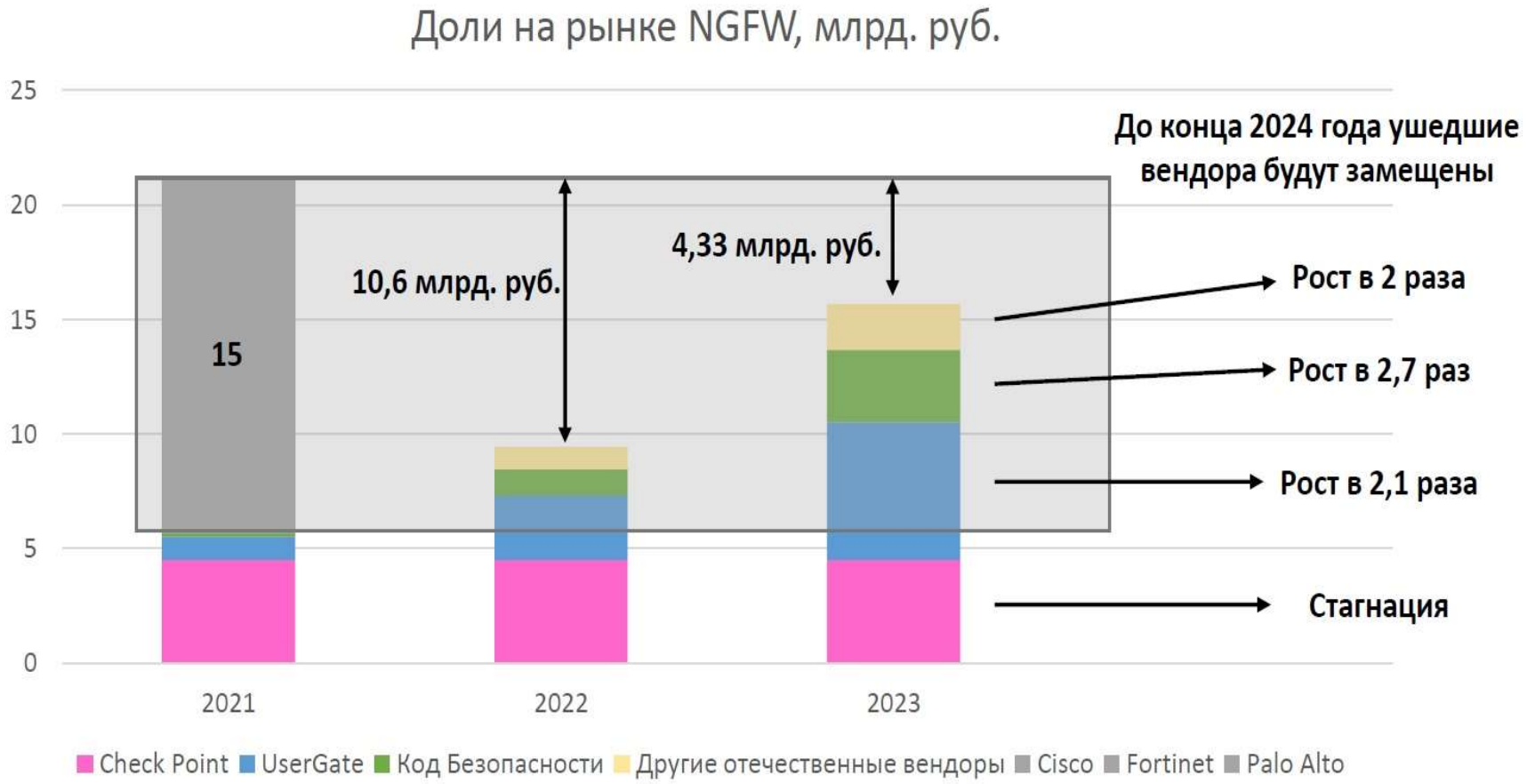
Проблематика

Риски при отсутствии функционального решения

- **Проникновение** и свободное перемещение **злоумышленника** по сетевой инфраструктуре
- **Распространение вредоносного ПО** и Фишинга
- **Неконтролируемый доступ** к обрабатываемой информации
- **Риск утечек** чувствительных данных
- **Несоблюдение требований** стандартов и нормативных правовых актов в области защиты информации



Рынок NGFW до и после 2022 г.



Партнёры-производители

Поставка средств межсетевого экранирования следующего поколения

КОД БЕЗОПАСНОСТИ

UserGate

infotecs®

Check Point
SOFTWARE TECHNOLOGIES LTD.

INFOWATCH®

*PT POSITIVE TECHNOLOGIES

*kaspersky


softline®
SO
FL
Цифровая Трансформация.
Успешная. Эффективная.