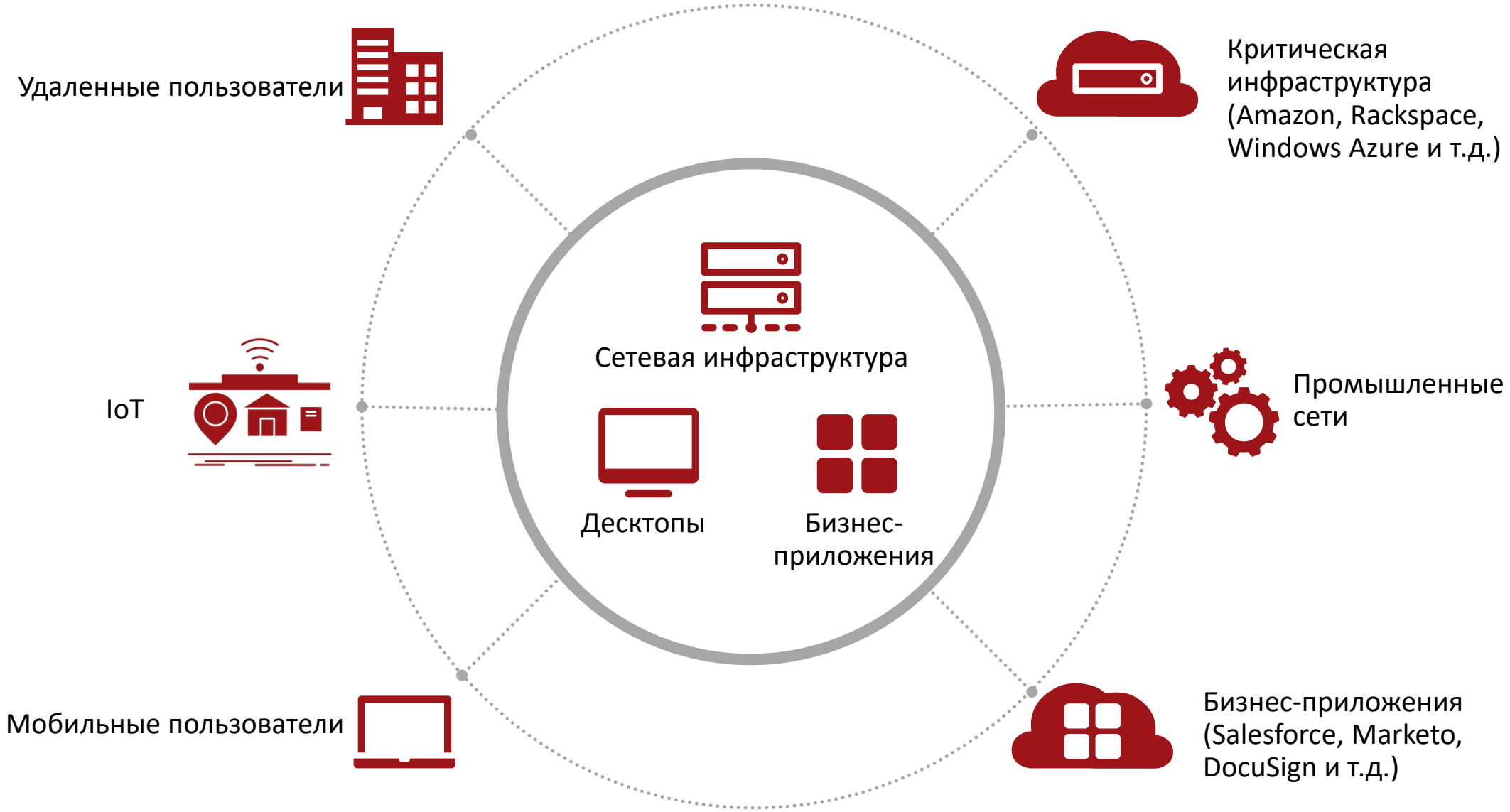
Вы уверены в безопасности вашей сети?

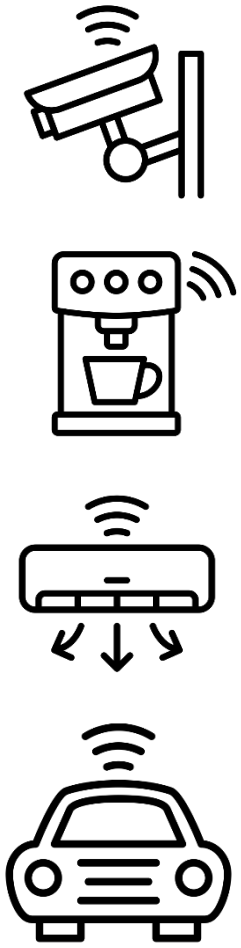
Дмитрий Казаков

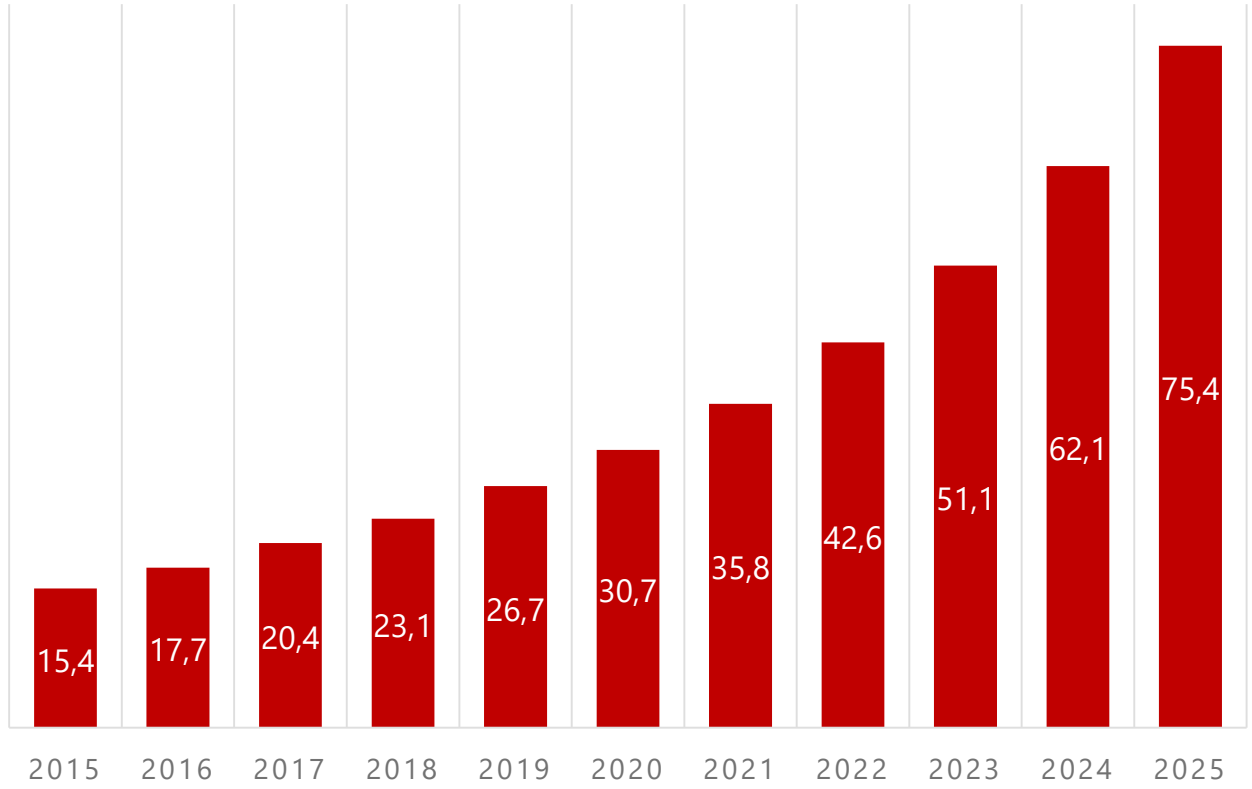
Менеджер по развитию бизнеса Cisco Security
D.Kazakov@softline.com

Что сегодня и завтра?

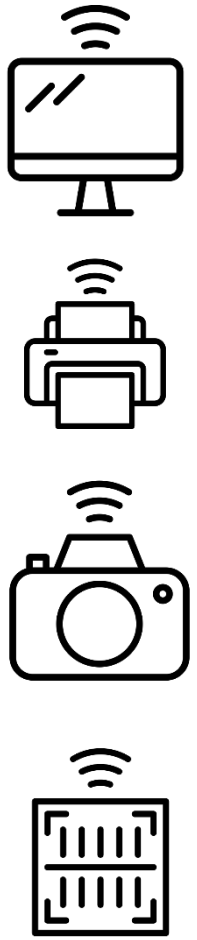


Количество IoT устройств





По данным статистического портала Statista



Рост угроз

На 89% выросло количество атак	**50 000 000 $**
Скрытый майнинг	до **18 000 000 $**
Шифровальщики	**60 000 000 $**


Talos

Это почти 3 блокировки на каждого человека

Самый широкий портфель в индустрии

TALOS

Сеть

- Межсетевые экраны
- Система обнаружения вторжений
- Прокси сервер
- Программная сегментация
- Поведенческая аналитика

Оконечные устройства

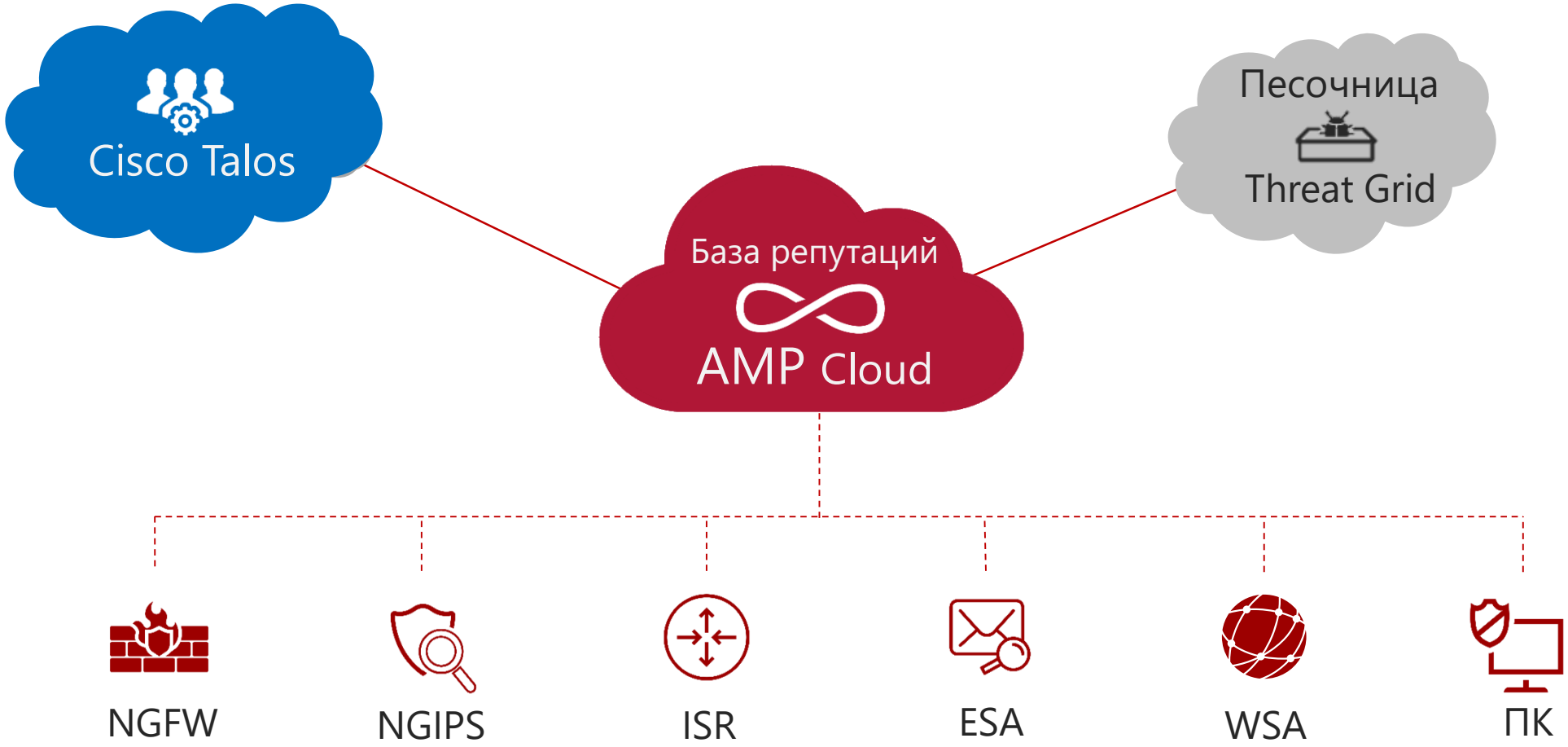
- Endpoint detection & response
- Защита мобильных устройств
- VPN
- Мультифакторная аутентификация

Облака

- Security Internet Gateway
- Защита публичных облаков
- Workload Security
- Защита доступа к облачным сервисам
- Защита почты

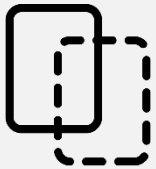

Advance Malware Protection
DEFENDING

AMP уже реализует безопасность будущего



Алгоритмы обнаружения вредоносной активности

Фильтрация по репутации



Сравнение сигнатур

Нечеткие идентифицирующие метки

Машинное обучение

Поведенческое обнаружение

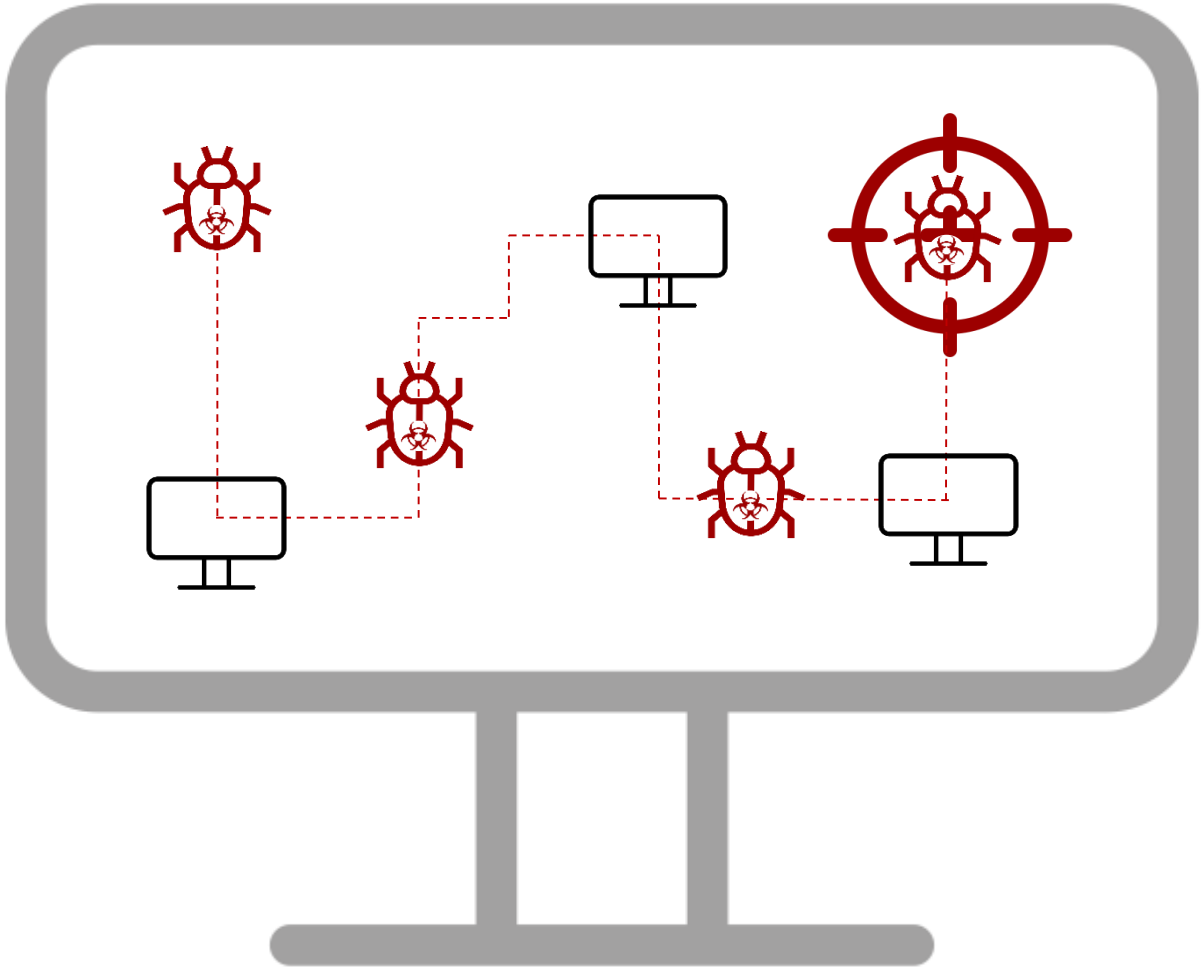
Признаки компрометации

Сопоставление потоков устройств

Динамический анализ

Расширенная аналитика

Постоянный анализ и ретроспективная безопасность



Определение точки входа

Увидеть, где был этот файл

Что файл делает

Следить за распространением

Гибко отслеживать и отправлять в карантин

Firepower

Cisco Firepower

Высокая доступность

Предотвращение вторжений NGIPS

Аналитика и автоматизация

Защита от продвинутого вредоносного ПО

Фильтрация URL-адресов

VPN и динамическая маршрутизация

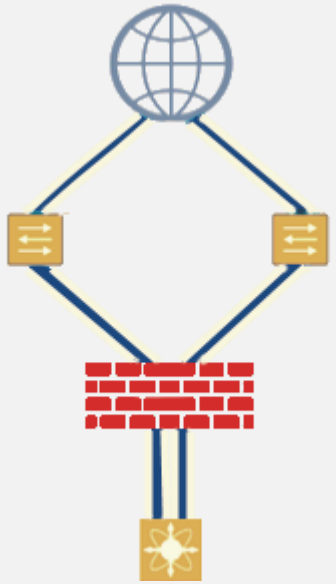
Мониторинг и контроль приложений

Профилирование сетевого трафика

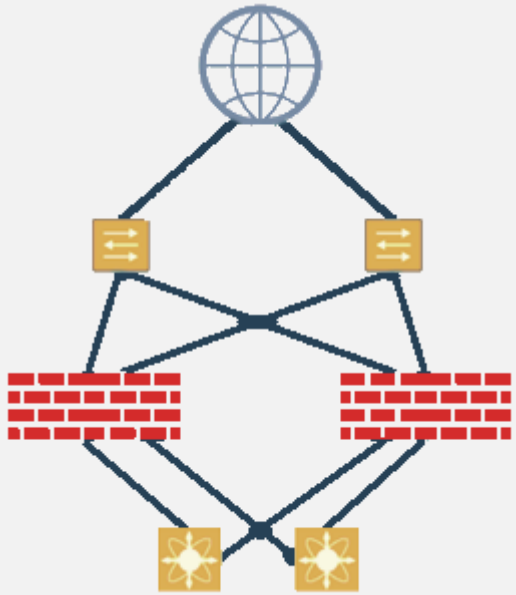
Аутентификация пользователей и устройств

Высокая доступность

Резервирование



Active / Standby



Кластеризация

Предотвращение вторжений NGIPS

- Алгоритм IPS следующего поколения
- Увеличена скорость
- Снижено количество ложных срабатываний

Cisco Firepower 4120

Using the recommended policy, the Firepower 4120 Security Appliance blocked 95.70% of attacks.

NSS Labs

VPN и динамическая маршрутизация

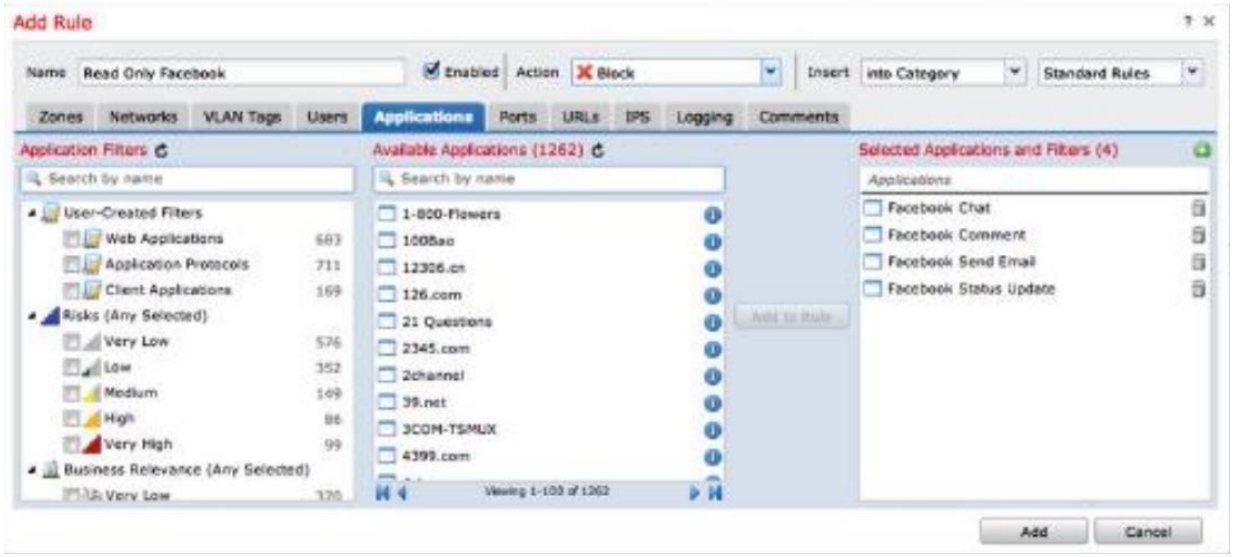
- AnyConnect
- Новое поколение процессоров Intel для шифрования
- Поддержка всех протоколов маршрутизации

Мониторинг и контроль приложений

- Поддержка всех типовых приложений
- Применение политик
- Приложения классифицированы по уровню риска и релевантности для бизнеса

Фильтрация URL-адресов

- 84 категории
- Всегда актуальные базы из Talos
- 280 миллиардов URL-адресов
- Автоматизированная система оценки репутации



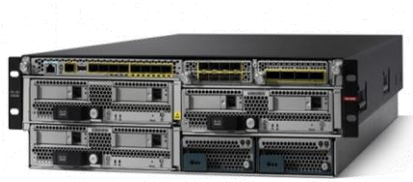
TALOS

Решения для бизнеса любого размера

Virtual

FPR 4115/25/45

FPR 4110/20/40/50



FPR 9300 SeriesSM-40

FPR 2110/20/40/50

FPR 1120/40

FPR 1010

SOHO/ SMB

Branch Office

Mid-Size Enterprise

Large Enterprise

Data Center

Service Provider

Варианты управления NGFW

Firepower Device Manager (FDM)

Автономное

Firepower Management Center (FMC)

Централизованное

Cisco Defense Orchestrator (CDO)

Облачное

Email Security

Угроза фишинга

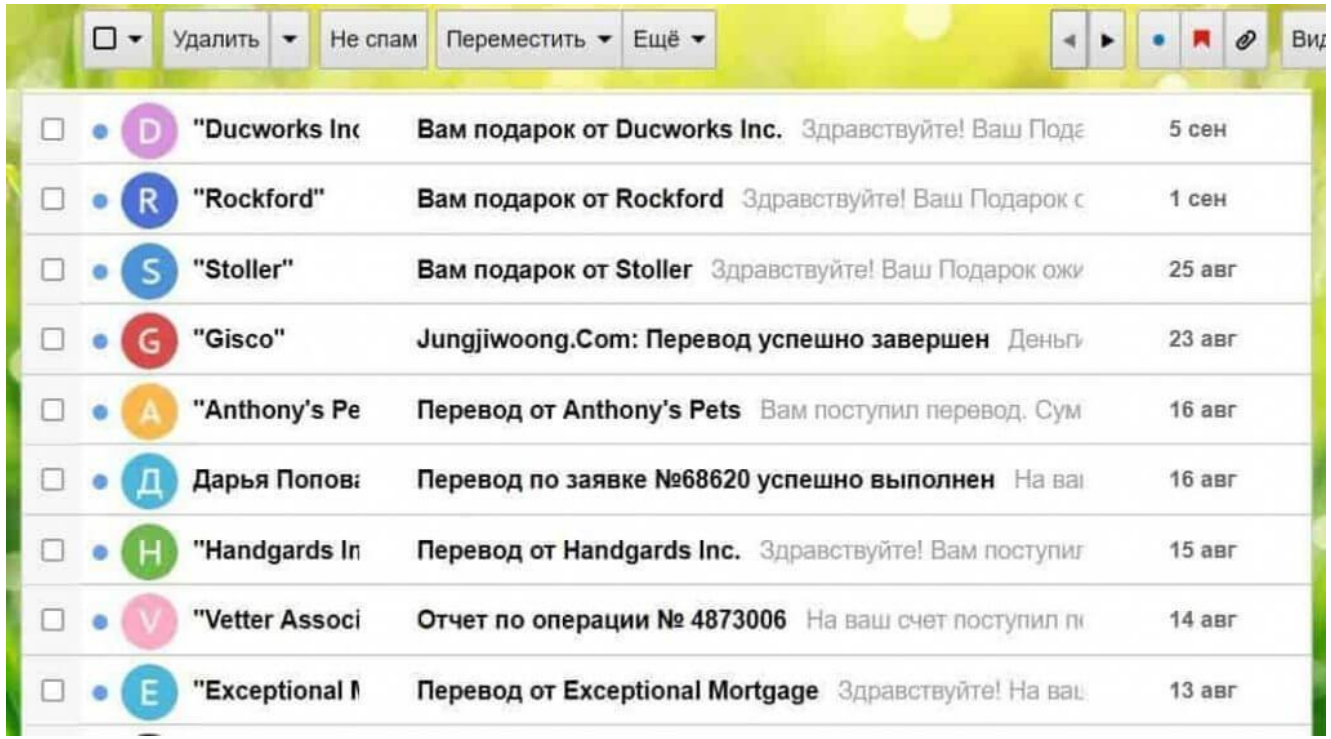
- Общий ущерб более 1,5 млрд. $
- Более 1 000 000 банковских карт
- Ущерб более 663 000 000 $

Как работают хакеры

Ссылка на YouTube: https://youtu.be/4gR562GW7TI

Количество спама растёт

Спам составляет 86% от всего E-Mail трафика



Как происходит заражение

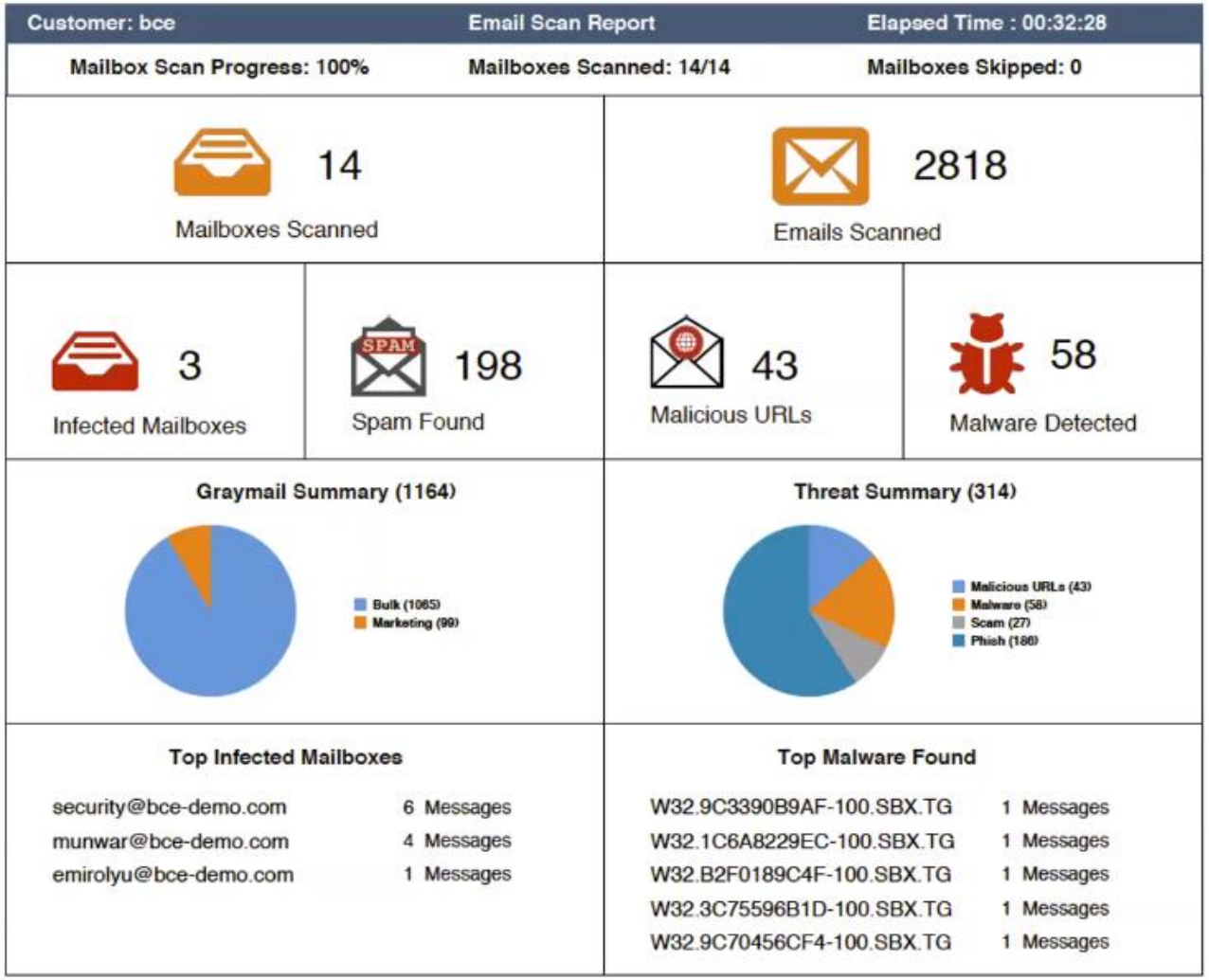
Алена из HR получает электронное письмо с резюме

Алена открывает вложение

Исполняемый файл загружает вредоносные программы

Полноценная защита почты с ESA

Примет отчета



Web Security

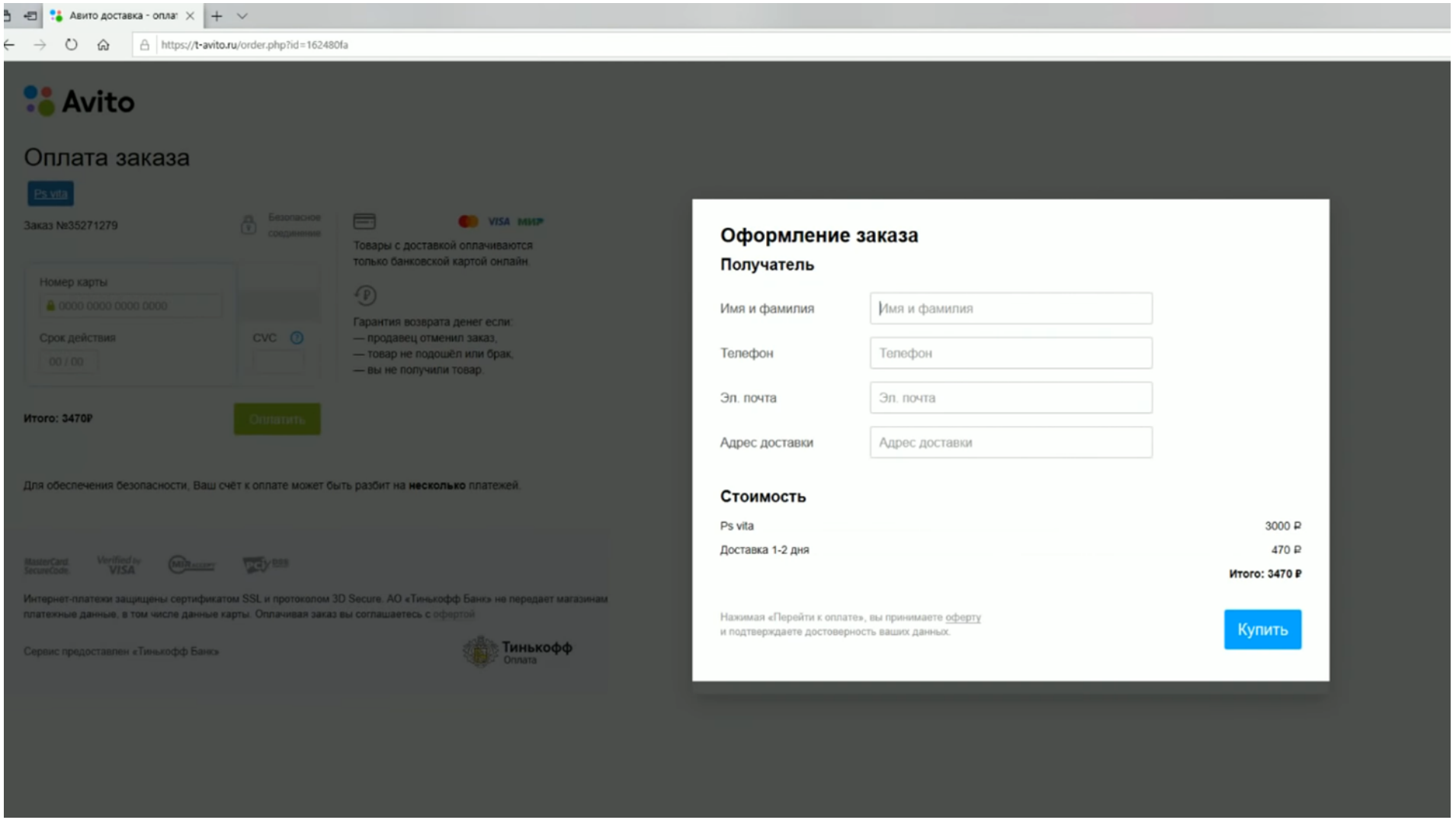
Количество атак

- Количество ежедневных успешных фишинговых атак 1274
- Число хакерских групп на 95%

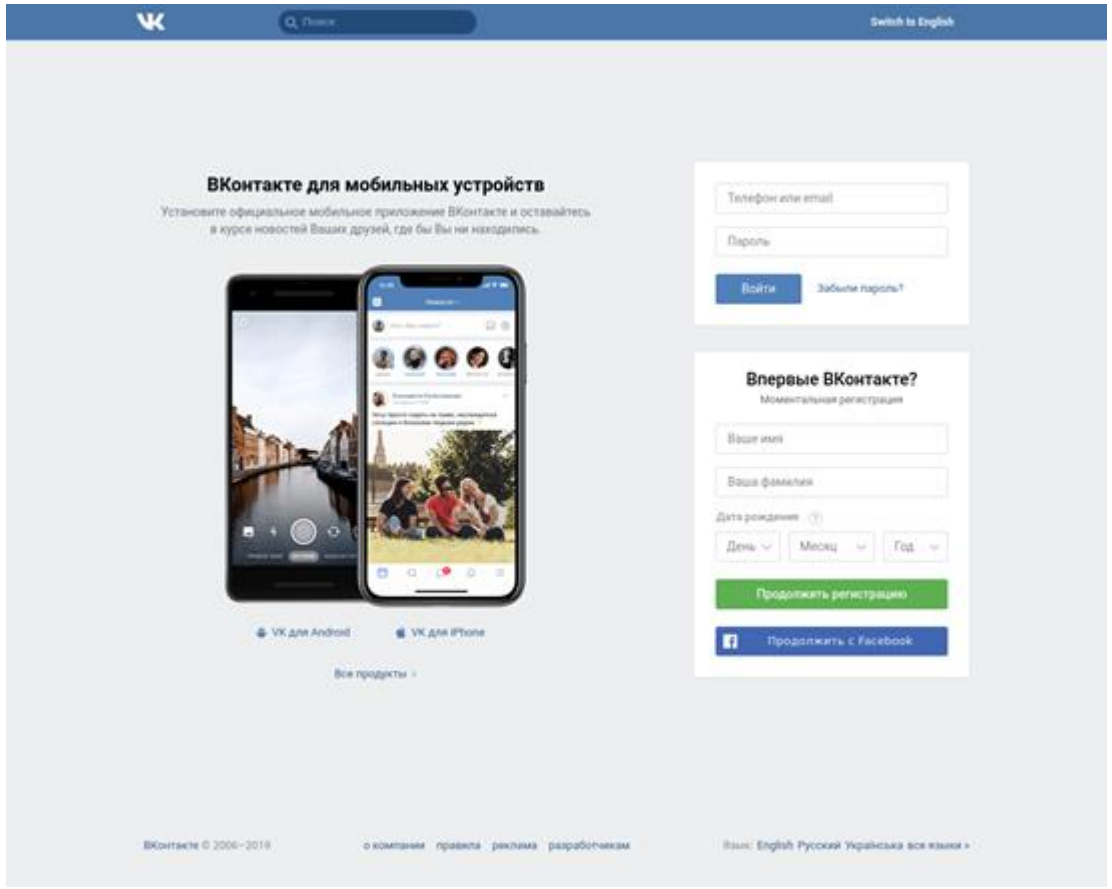
Ущерб от атак

- 251 000 000 рублей за 2018 год
- Увеличилось на 6%

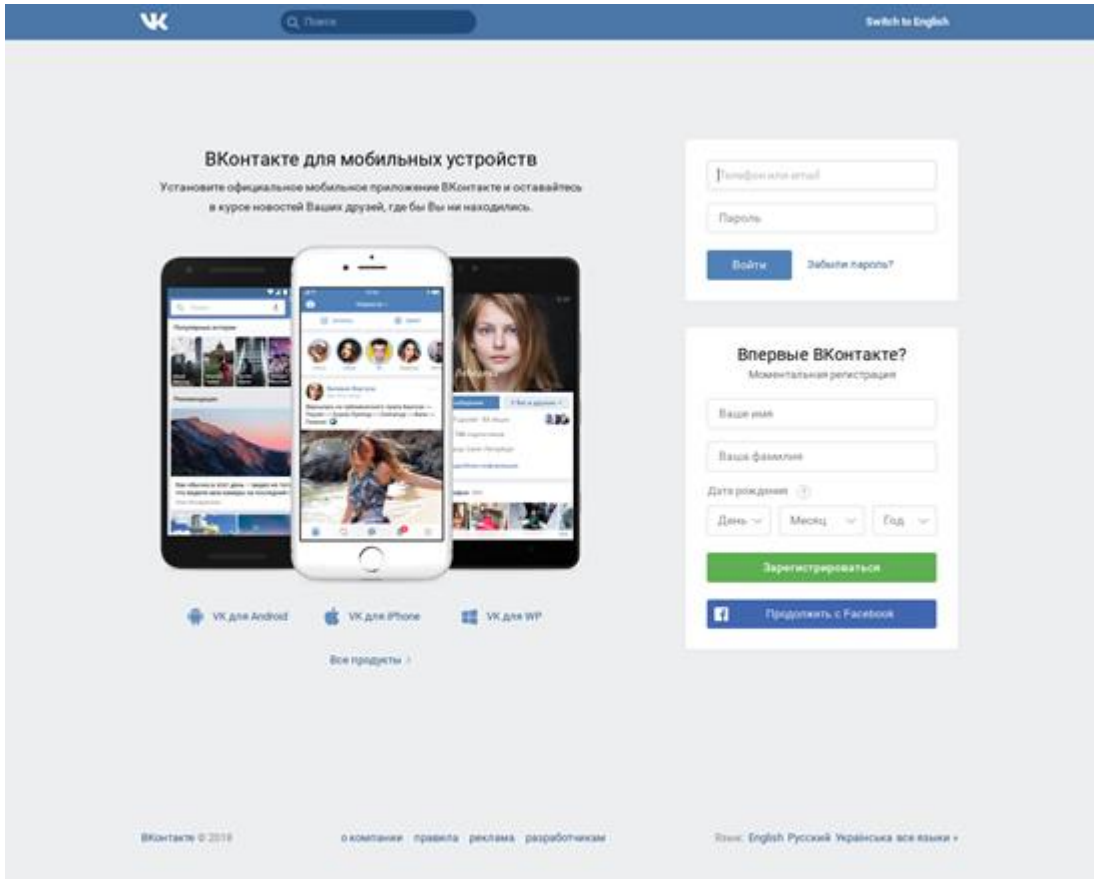
Пример фишинга



Пример фишинга



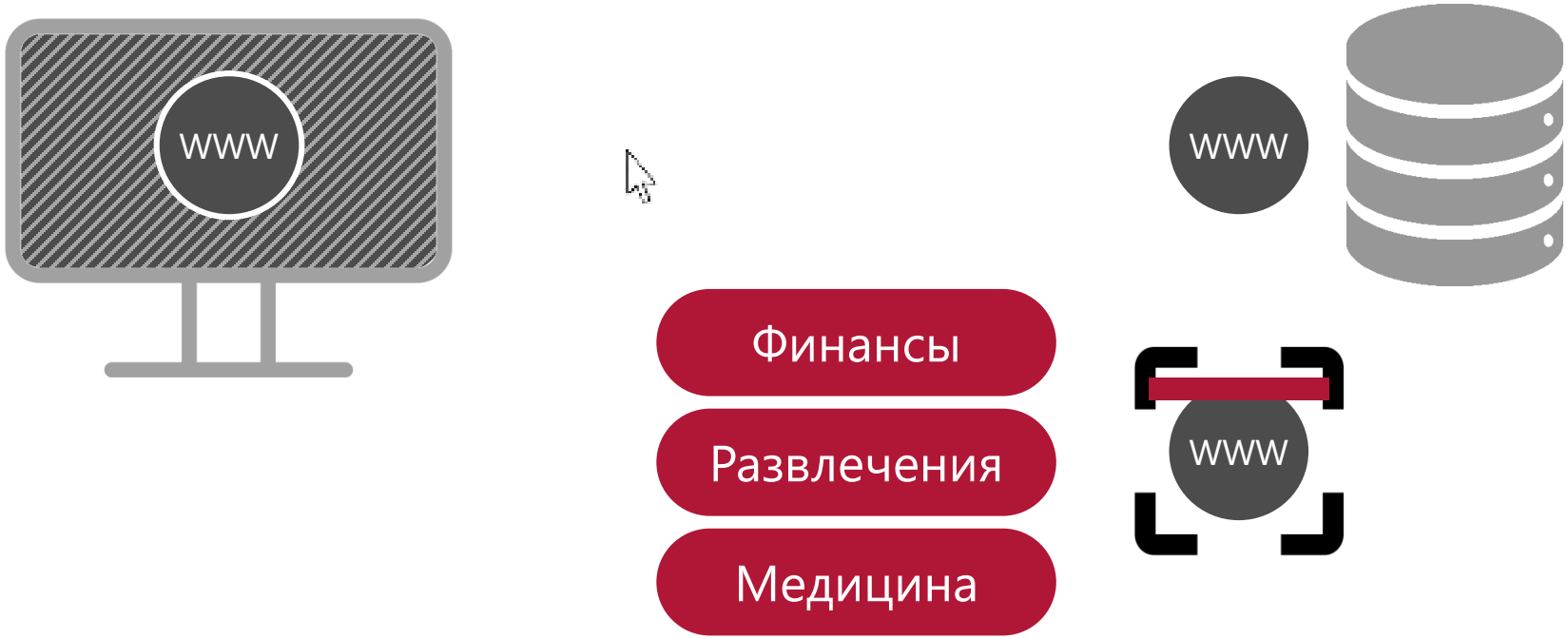
Настоящая страница входа



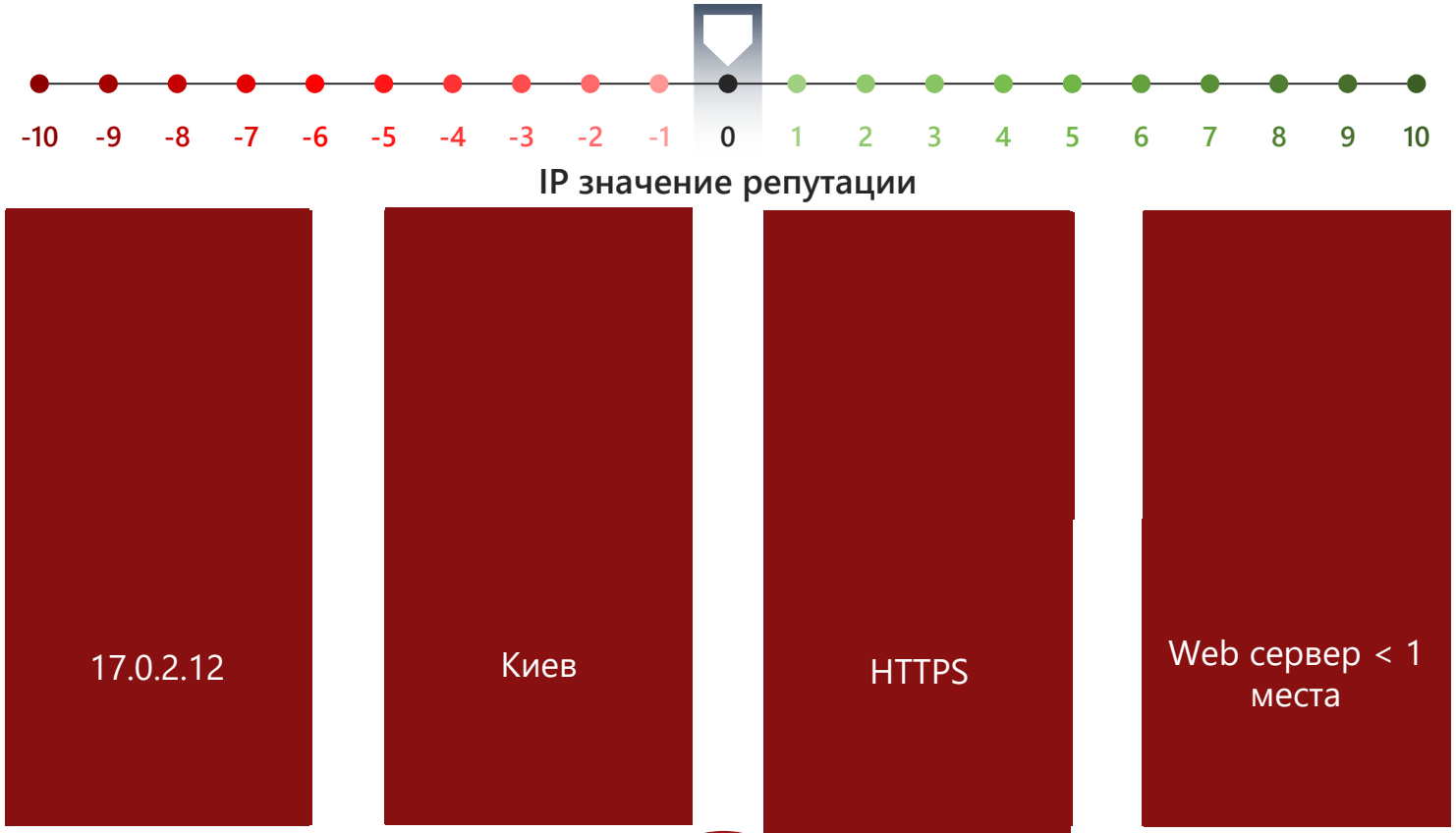
Фишинговая версия

Как работает Web Security Appliance

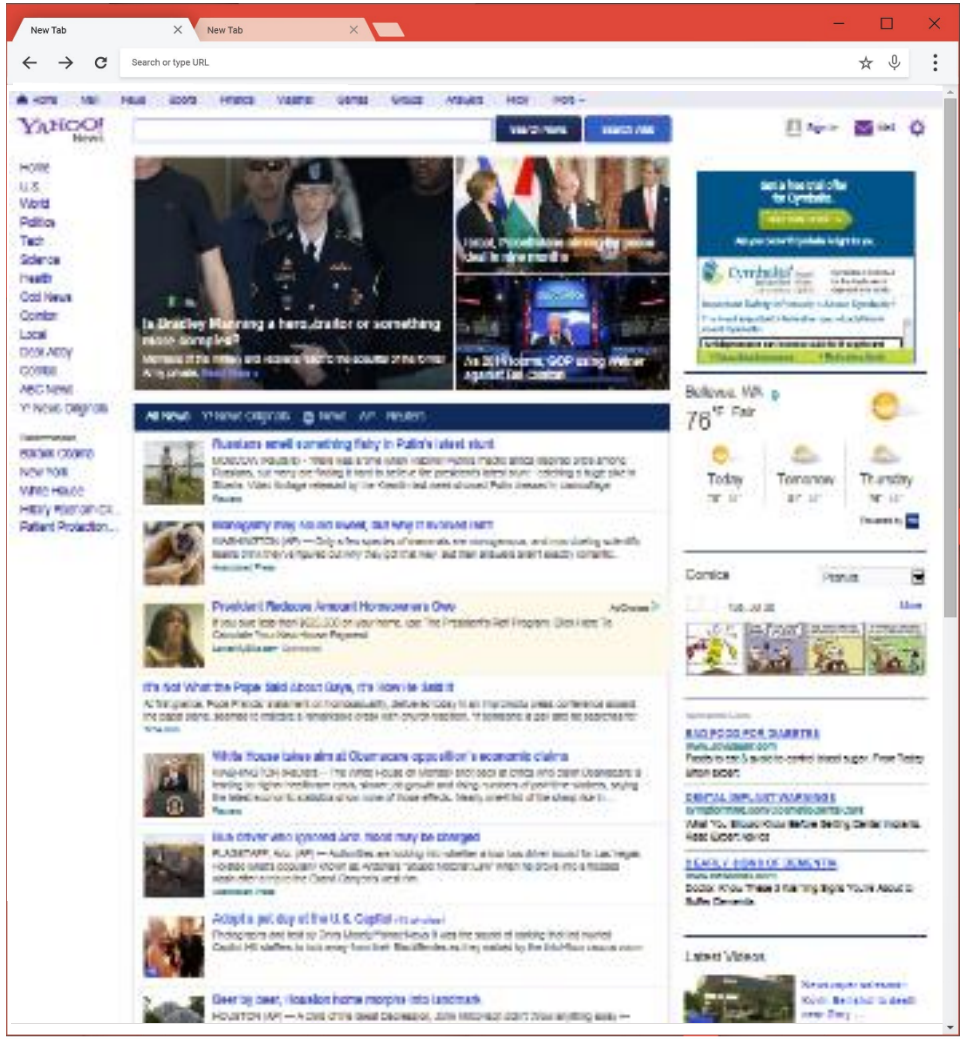
URL фильтрация

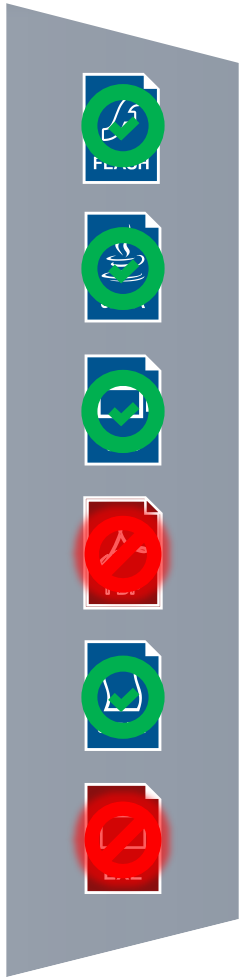


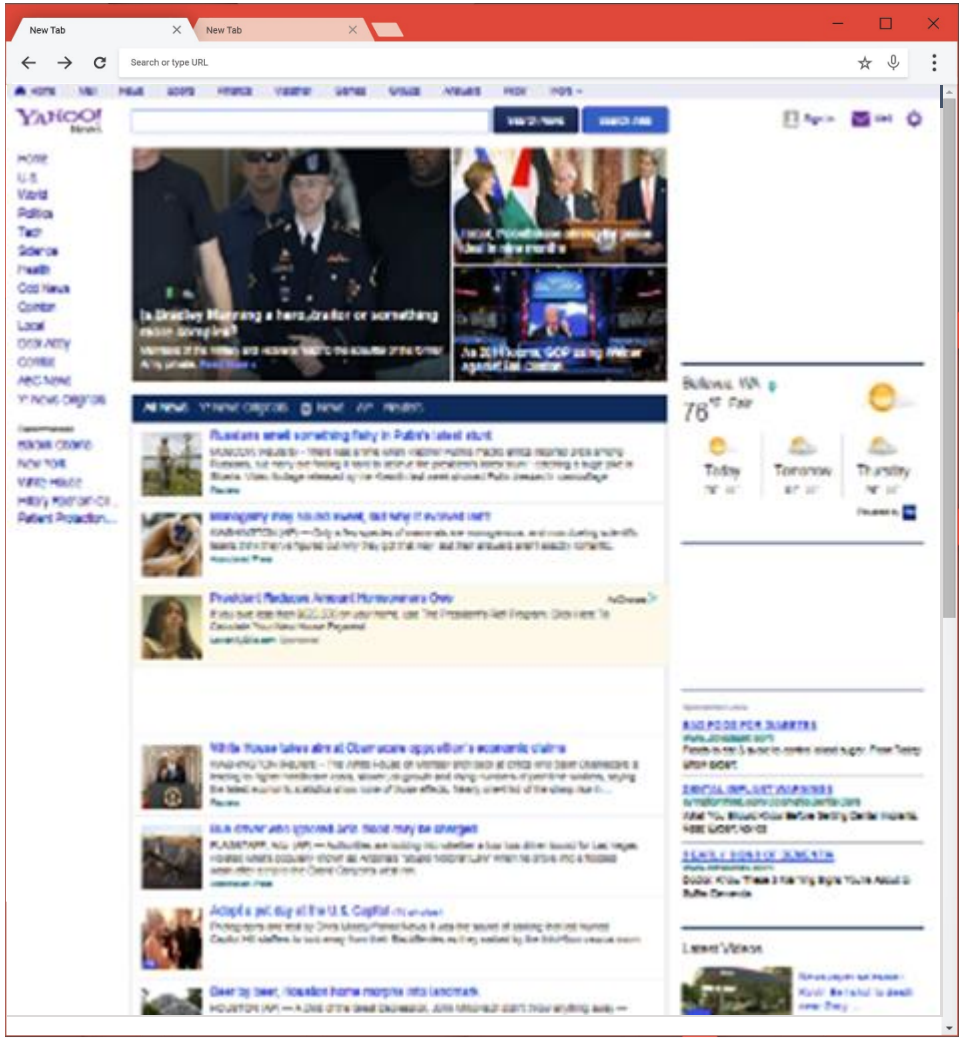
Репутационный анализ
Сила контекста реального времени



Sandbox реального времени



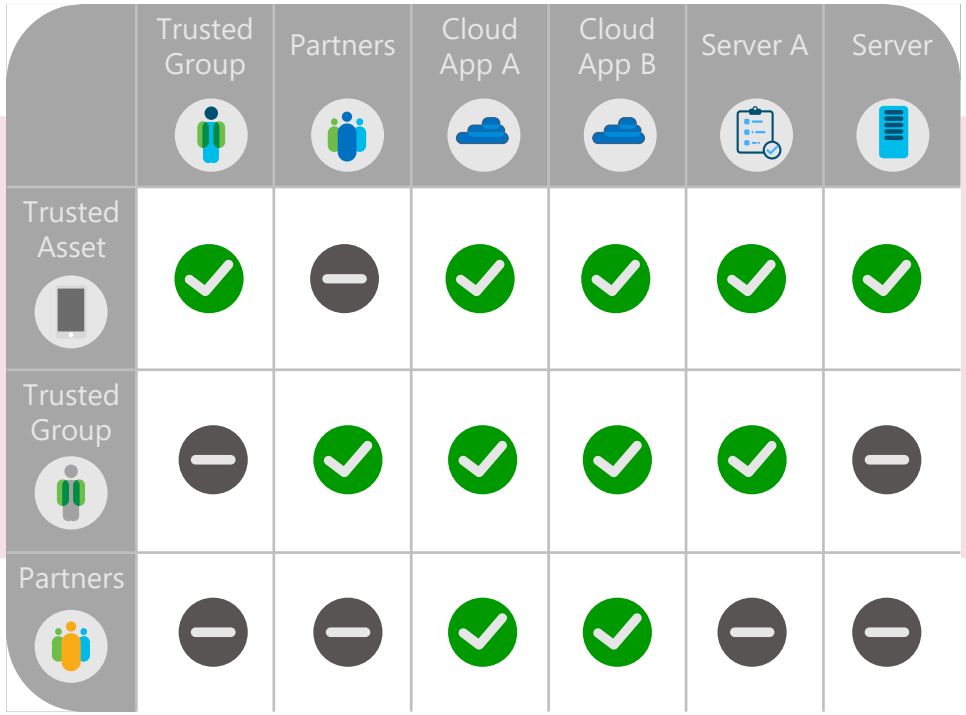


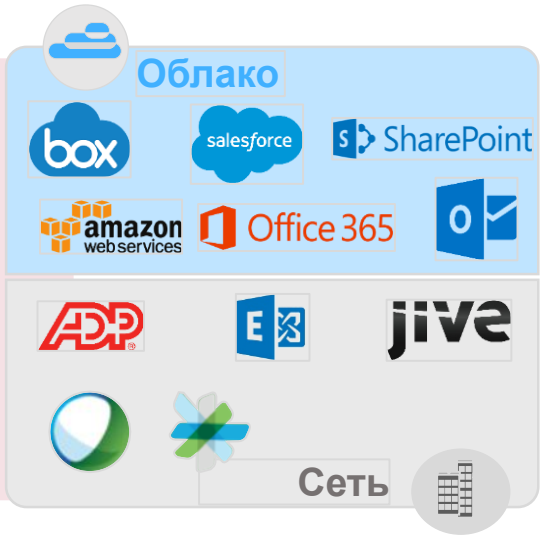


Identity Service Engine

Как работает ISE

- Кто
- Что
- Когда
- Где
- Как
- Соответствие нормативам





Автоматическая изоляция угроз с Firepower & ISE

Работник скачивает файл

FMC собирает и сопоставляет данные

FMC посылает предупреждение в ISE

Firepower автоматически ограничивает доступ

Приложение или устройство помещено в карантин

ISE работает с другими вендорами

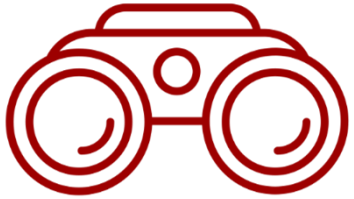
	aruba	MOTOROLA SOLUTIONS	JUNIPER NETWORKS	BROCADE	Hewlett Packard Enterprise	CISCO
Profiling	✓	✓	✓	✓	✓	✓
Posture	✓	✓	✓	✓	✓	✓
Guest	✓	✓	✓	✓	✓	✓
BYOD	✓	✓	✓	✓	✓	✓
MDM	–	–	–	–	–	✓
TrustSec	–	–	–	–	–	✓

https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/compatibility/b_ise_sdt_26.html

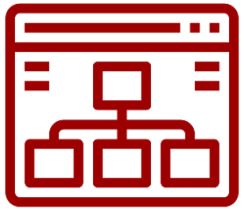
Umbrella

В чем проблема?

Вредоносный код
и шифровальщики



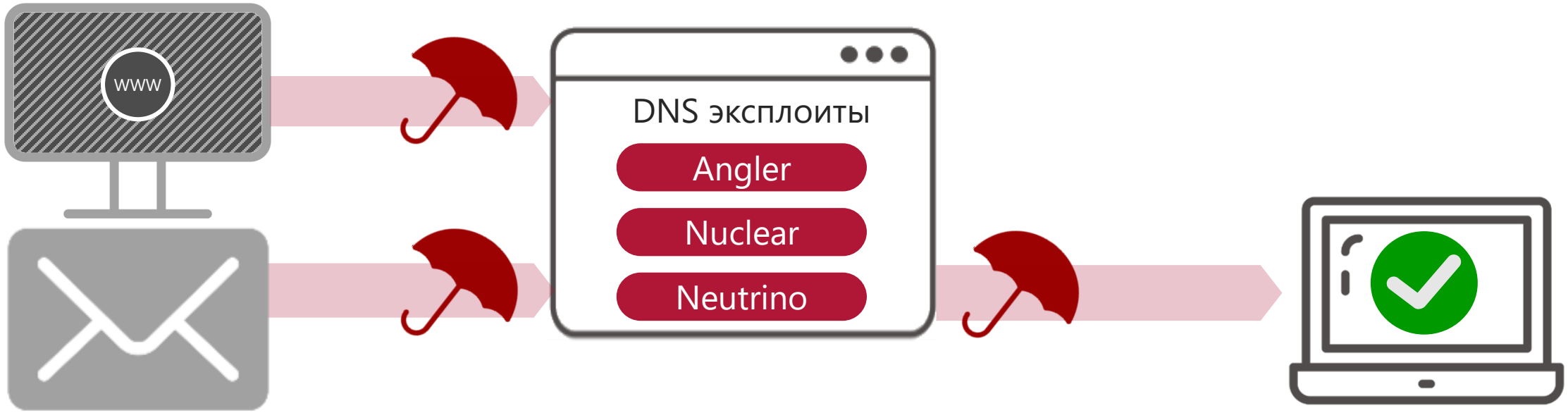
Редиректы



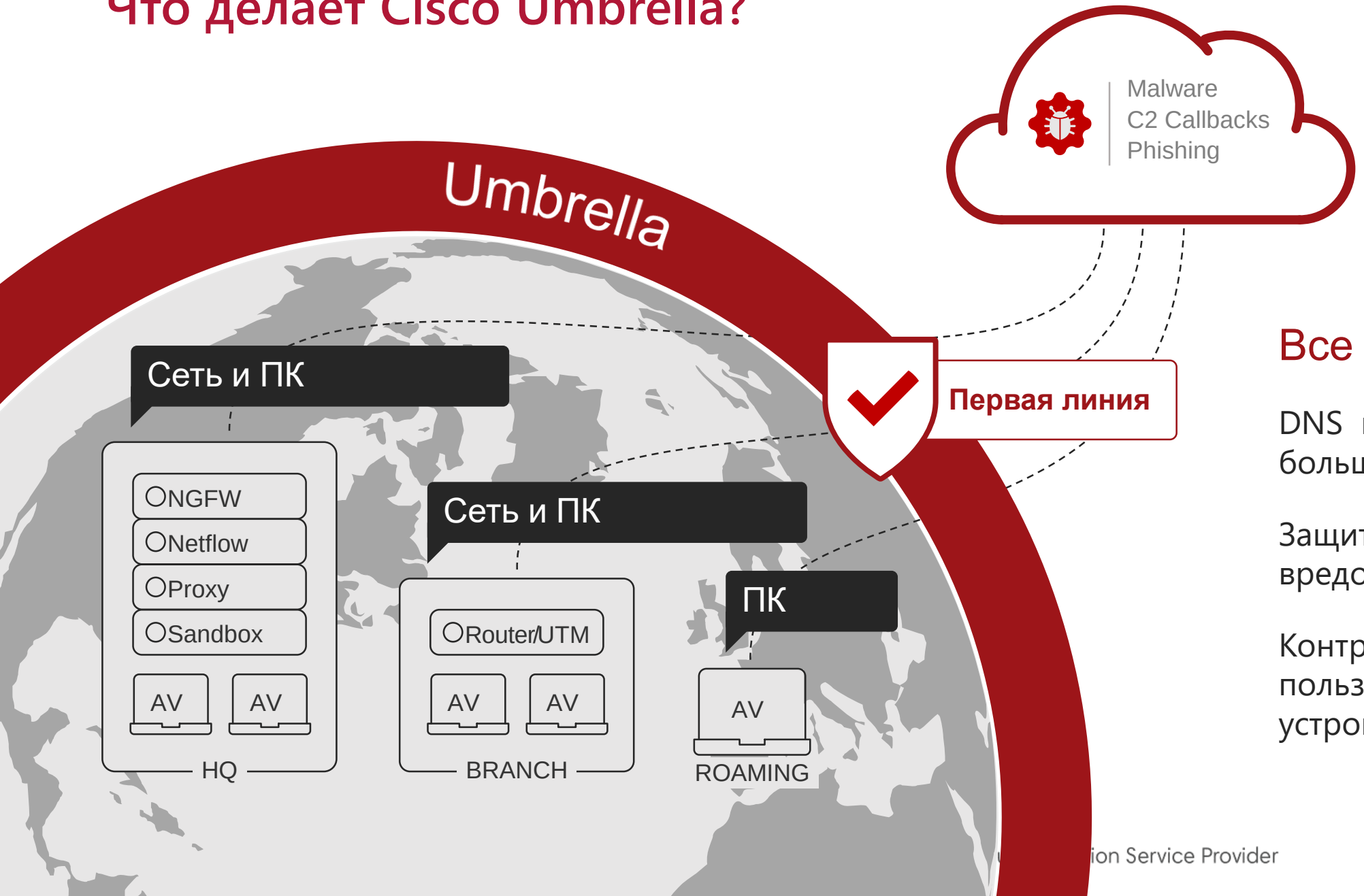
Сайты-клоны

Утечки
информации

Cisco Ransomware Defense



Что делает Cisco Umbrella?



Все начинается с DNS

DNS используется большинством устройств

Защита от фишинга и вредоносного ПО

Контроль над всеми пользователями и устройствами

softline®


Stealthwatch

Эффективная безопасность зависит от полной видимости

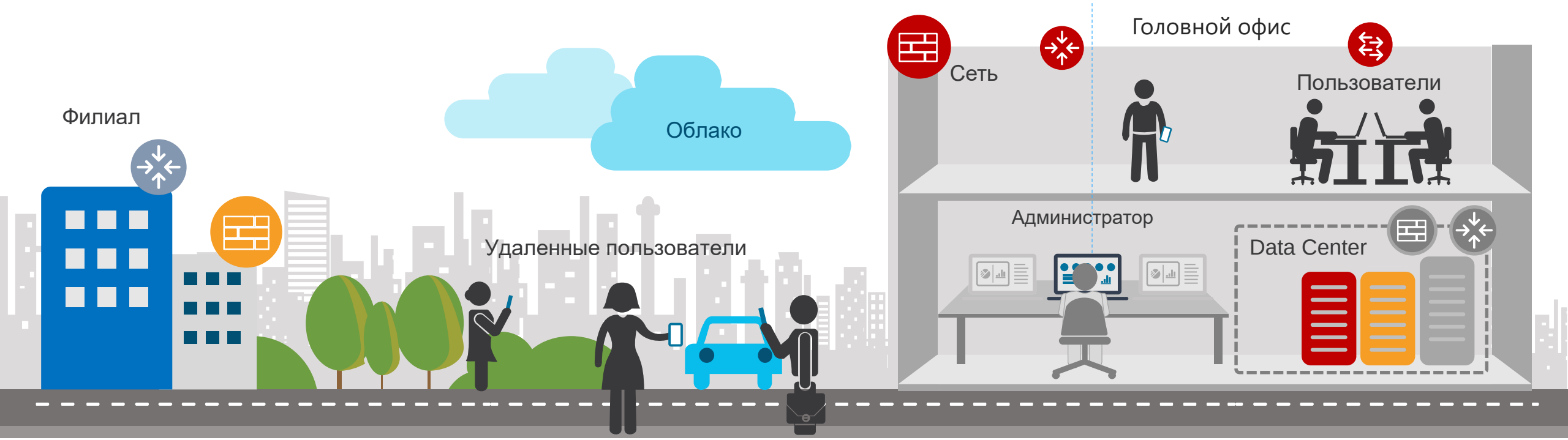
ВИДЕТЬ каждый хост

ЗАПИСАТЬ каждое взаимодействие

Знать, что поведение **НОРМАЛЬНОЕ**

Быть оповещенным об **ИЗМЕНЕНИЯХ**

Быстро **РЕАГИРОВАТЬ** на угрозы



Защита устройств Интернета вещей (IoT)

- Обнаружение вредоносного поведения
- Нет агентов конечных точек
- Сегментация

Encrypted Traffic Analytics

Шифрованный трафик в сети?

организаций являются жертвами злонамеренной деятельности *

80%

41%

при атаках используется зашифрованный трафик, чтобы избежать обнаружения *

*Source: Ponemon Institute – Hidden threats in encrypted traffic

Как обеспечить безопасность при сохранении конфиденциальности?

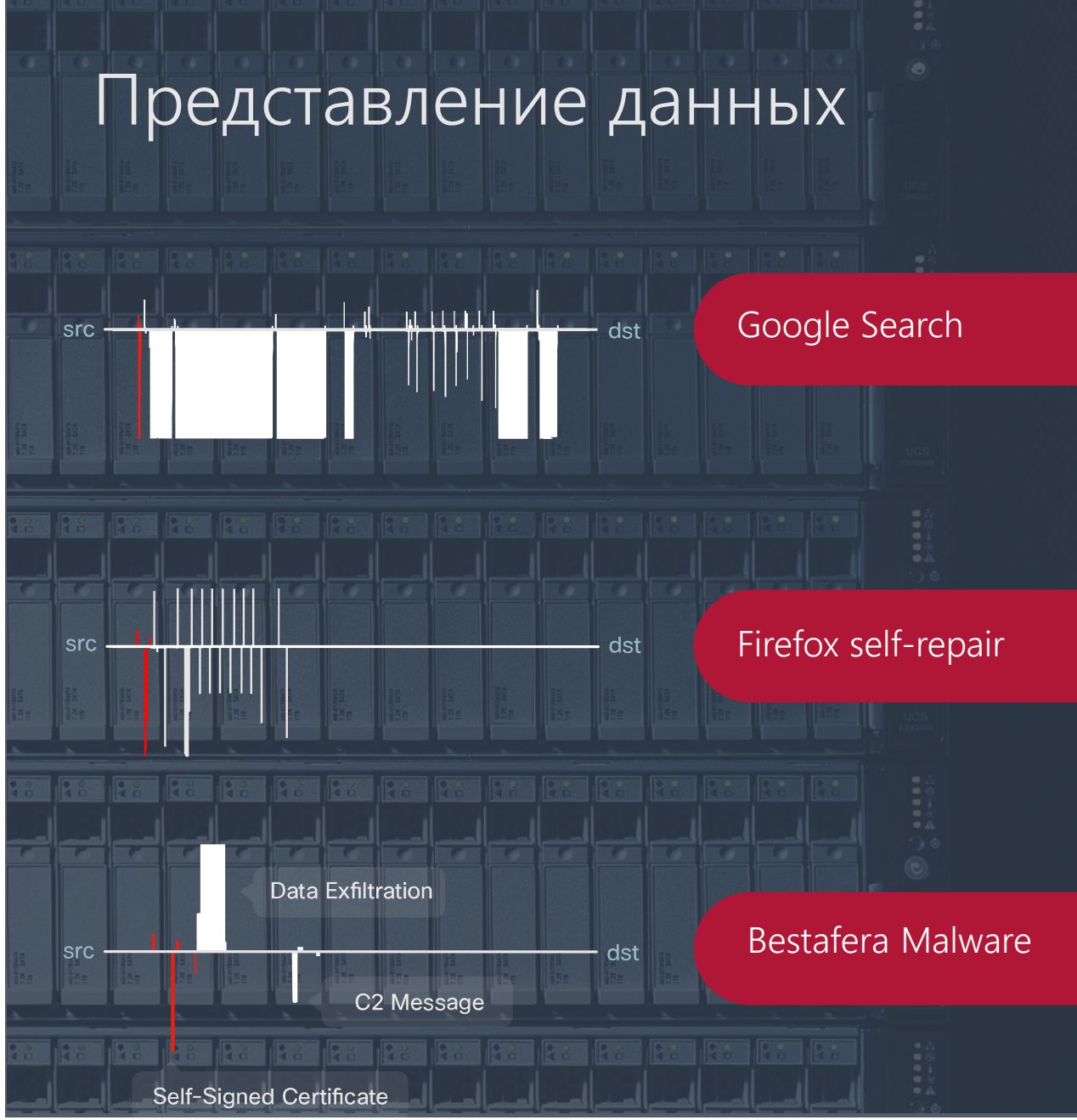
Аналитика

Обнаружение угроз в зашифрованном трафика

Сохранение персональной информации

Точность обнаружения 99.99%

Представление данных



Cisco защищает на протяжении всего цикла атаки

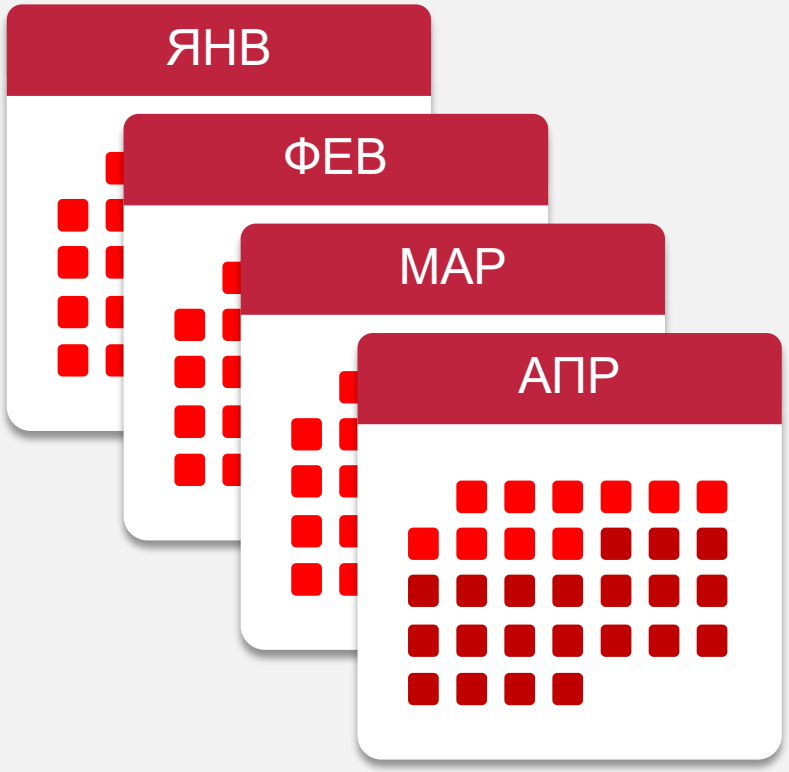
NGFW | NGIPS | Threat Grid

ISE | WSA и ESA | Stealthwatch

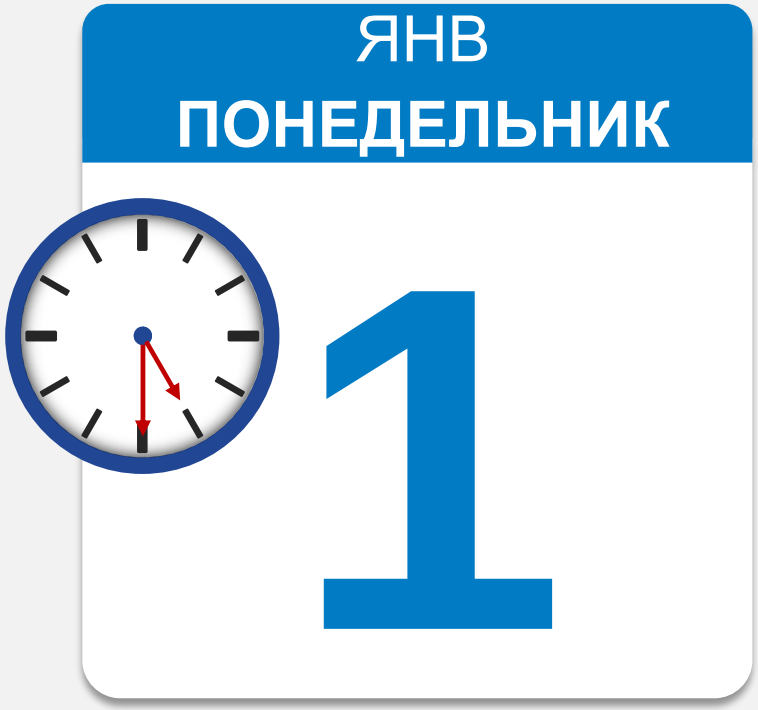
AnyConnect | Advanced Malware Protection

Umbrella

Типичный TTD rate:* 100 дней



Cisco: 17,5 часов



Source: Cisco® 2018 Annual Security Report
*Median time to detection (TTD)

Оборудование

Поддержка

Аудит

Лицензии

Обучение специалистов по ИБ

Сертификация

Партнерство с Cisco

Специализации

- **Advanced Enterprise Networks Architecture Specialization**
- **Advanced Collaboration Architecture Specialization**
- **Advanced Data Center Architecture Specialization**
- **Advanced Security Architecture Specialization**
- Advanced Unified Computing Technology Specialization
- Advanced Unified Fabric Technology Specialization

Облачные и управляемые услуги

Cloud and Managed Services Master
Cisco Powered Infrastructure as a Service
Cisco Powered Disaster Recovery as a Service
Cisco Powered Managed Security

Другие авторизации

Learning Partner - Associate
Academy Network Partner
Multinational Certified Partner

Дмитрий Казаков

Менеджер по развитию бизнеса Cisco Security

D.Kazakov@softline.com