

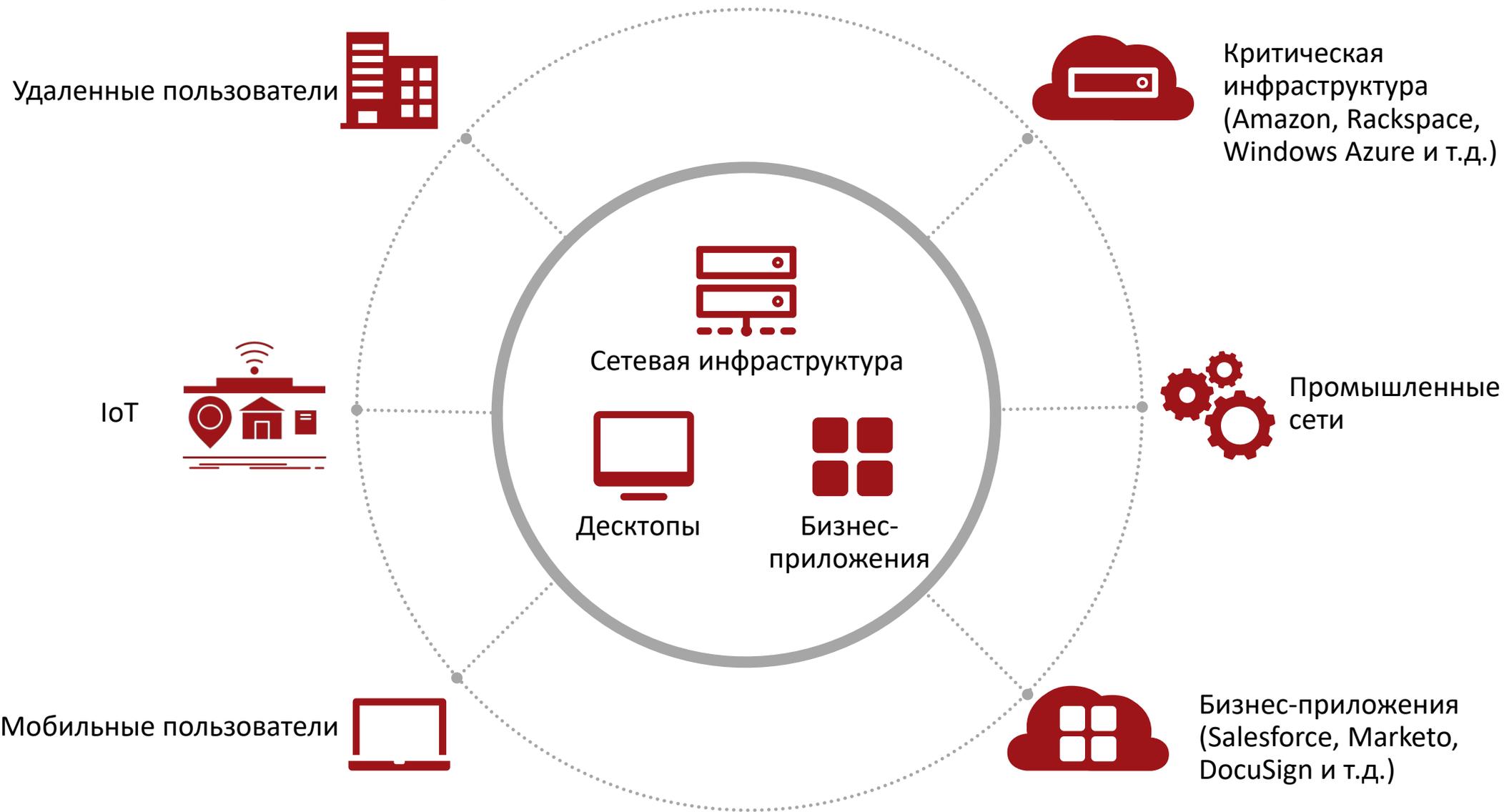
# Вы уверены в безопасности вашей сети?

**Дмитрий Казаков**

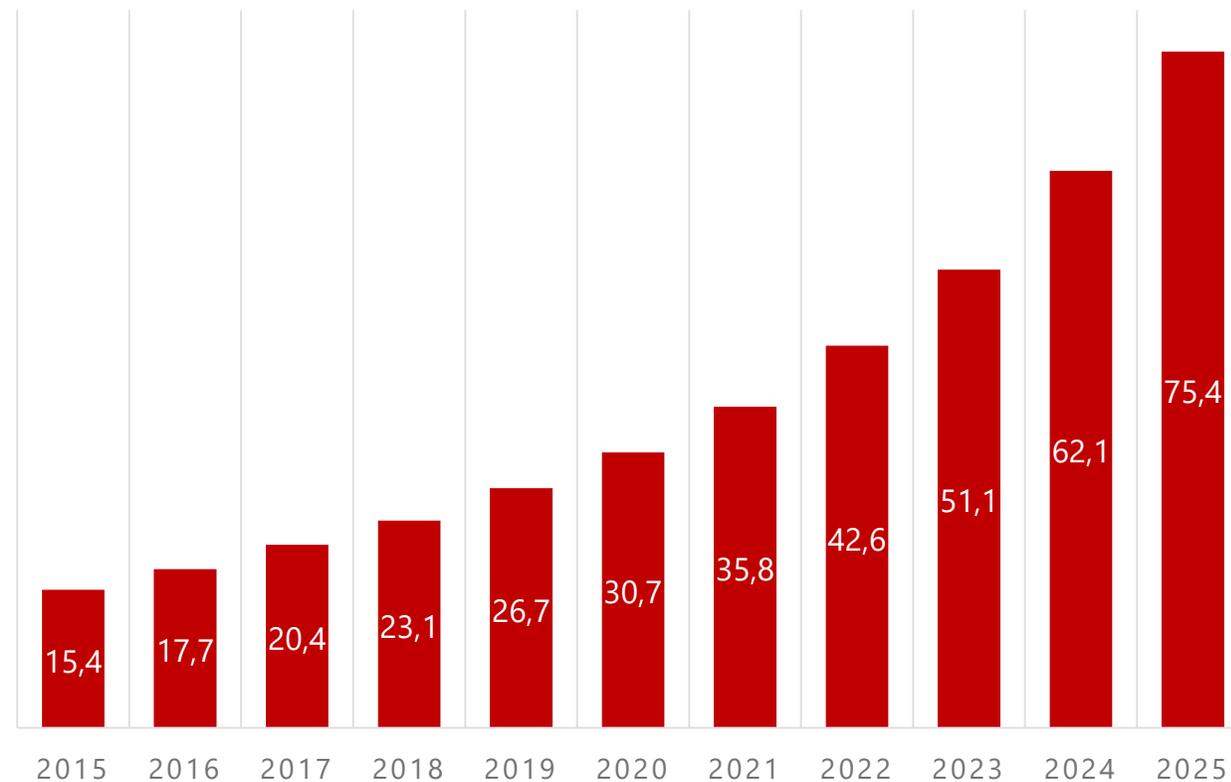
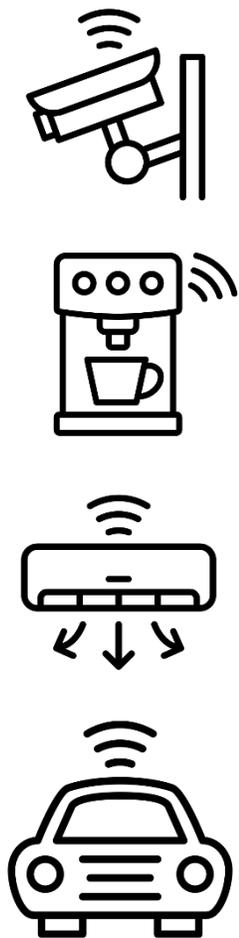
Менеджер по развитию бизнеса Cisco Security  
[D.Kazakov@softline.com](mailto:D.Kazakov@softline.com)



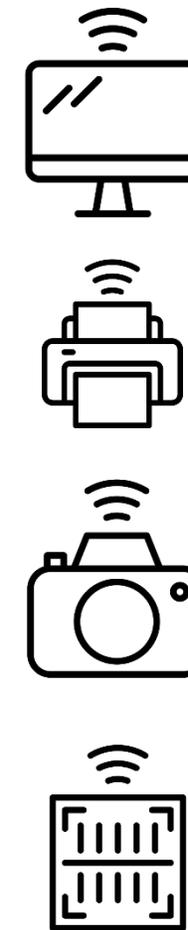
# Что сегодня и завтра?



# Количество IoT устройств



По данным статистического портала Statista



# Рост угроз

На **89%** выросло количество атак

**50 000 000 \$**

Скрытый майнинг

до **18 000 000 \$**

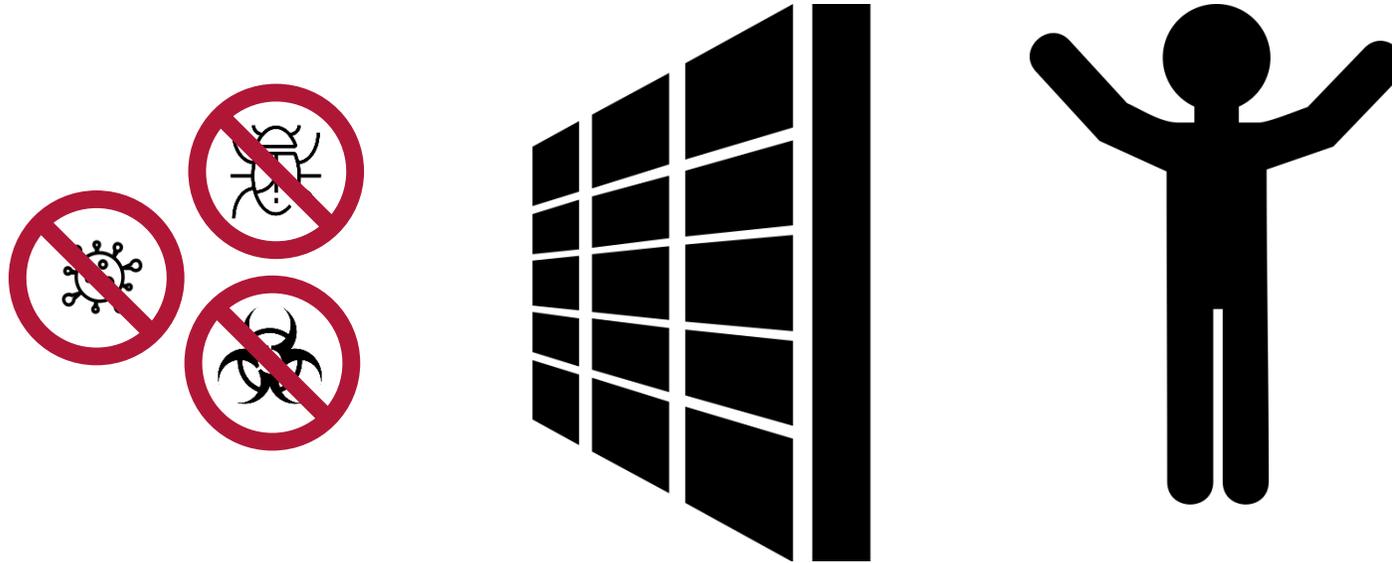
Шифровальщики

**60 000 000 \$**



# Talos

Это почти 3 блокировки на каждого человека



# Самый широкий портфель в индустрии



## Сеть

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



## Оконечные устройства

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



## Облака

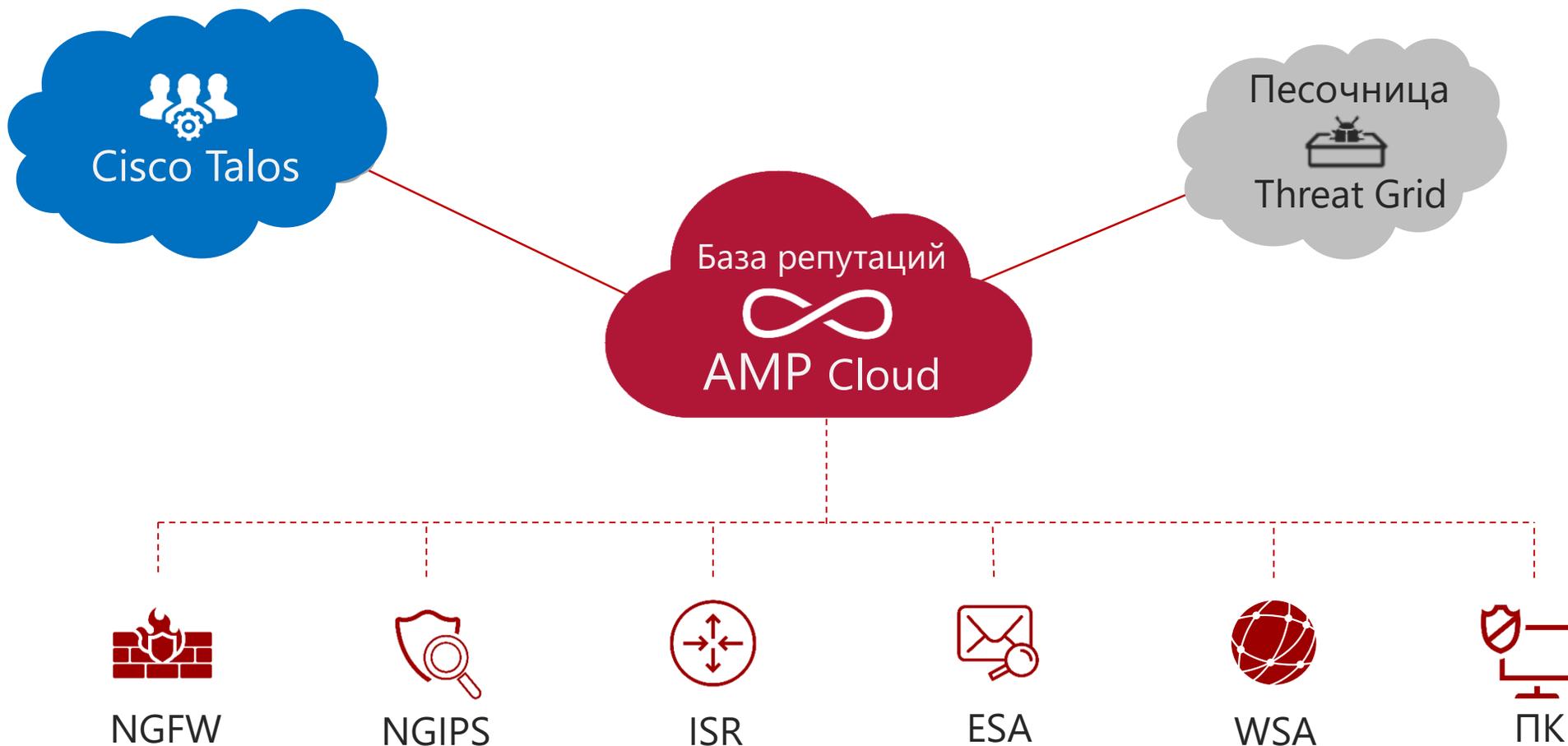
-  Security Internet Gateway
-  Защита публичных облаков
-  Workload Security
-  Защита доступа к облачным сервисам
-  Защита почты

# Advance Malware Protection

DEFENDING

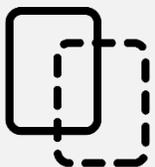
The background features a dark teal grid with glowing blue lines connecting various data visualization icons. These icons include line graphs, bar charts, and document-like screens with text and tables. The overall aesthetic is high-tech and digital.

# AMP уже реализует безопасность будущего



# Алгоритмы обнаружения вредоносной активности

## Фильтрация по репутации



Сравнение  
сигнатур

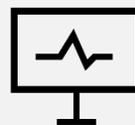


Нечеткие  
идентифицирующие  
метки

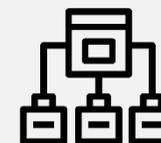


Машинное  
обучение

## Поведенческое обнаружение



Признаки  
компрометации



Сопоставление  
потоков устройств

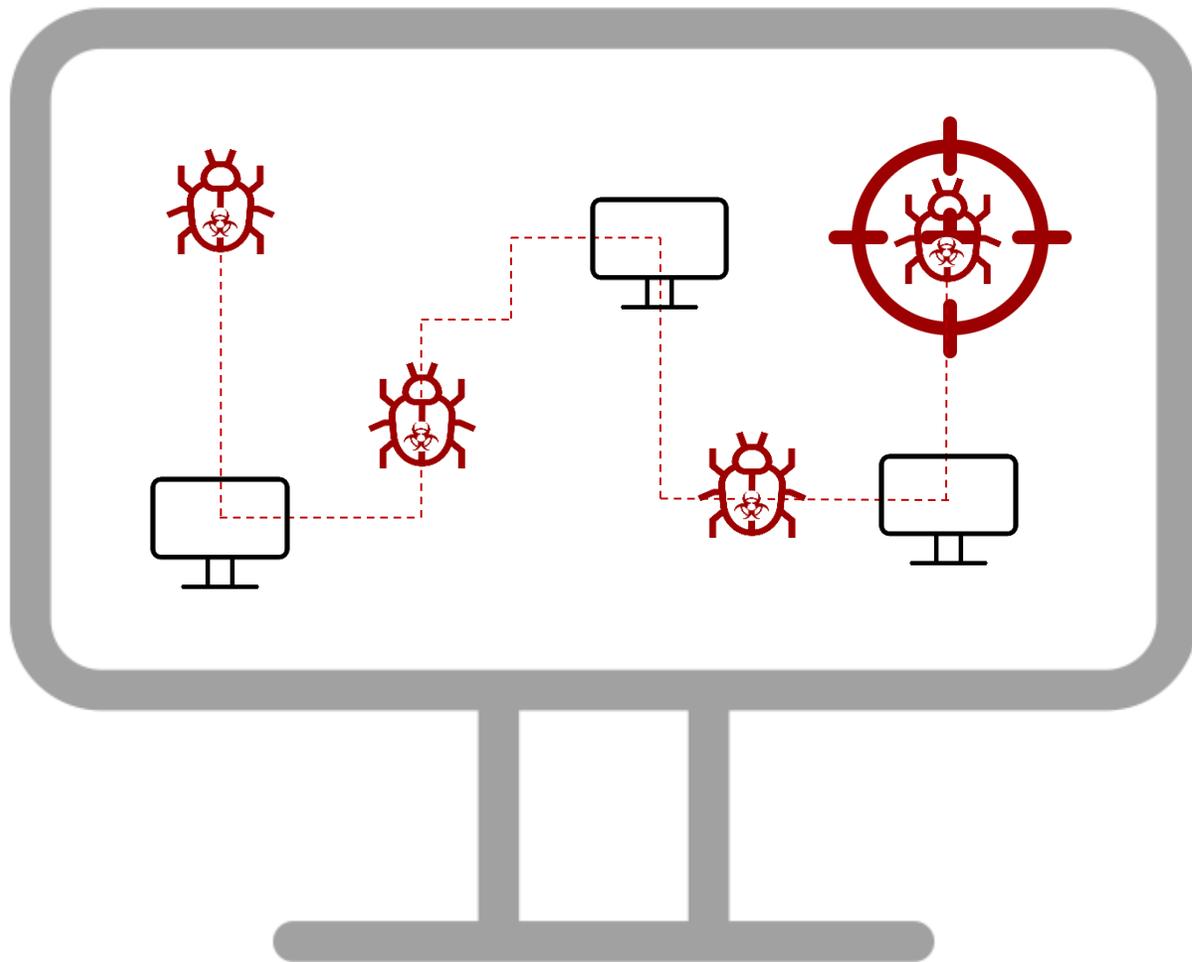


Динамический  
анализ



Расширенная  
аналитика

# Постоянный анализ и ретроспективная безопасность



# Firepower

The background of the slide features a stylized globe of the Earth, rendered in shades of blue and white. Overlaid on the globe is a complex network of glowing blue lines and nodes, resembling a global communication or data network. The lines are thin and curved, connecting various points across the globe. The nodes are small, bright blue spheres. The overall aesthetic is futuristic and technological.

# Cisco Firepower



Высокая  
доступность



Предотвращение  
вторжений NGIPS



Аналитика и  
автоматизация



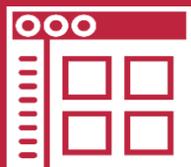
Защита от  
продвинутого  
вредоносного ПО



Фильтрация  
URL-адресов



VPN и  
динамическая  
маршрутизация



Мониторинг и  
контроль  
приложений



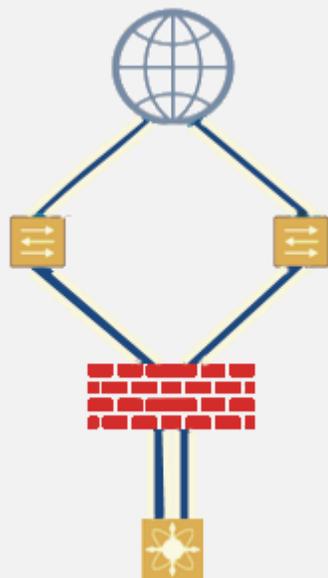
Профилерование  
сетевого трафика



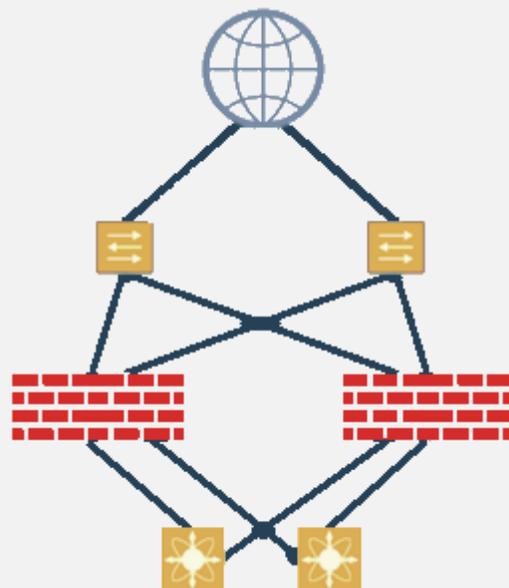
Аутентификация  
пользователей и  
устройств

# Высокая доступность

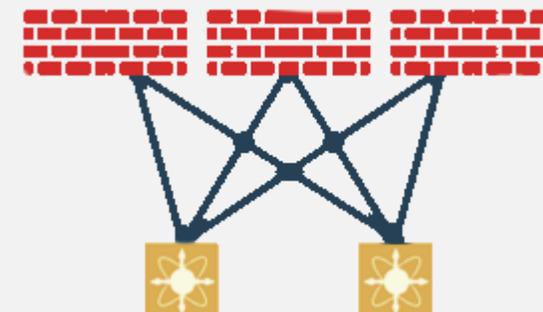
## Резервирование



## 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.

# VPN и динамическая маршрутизация

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



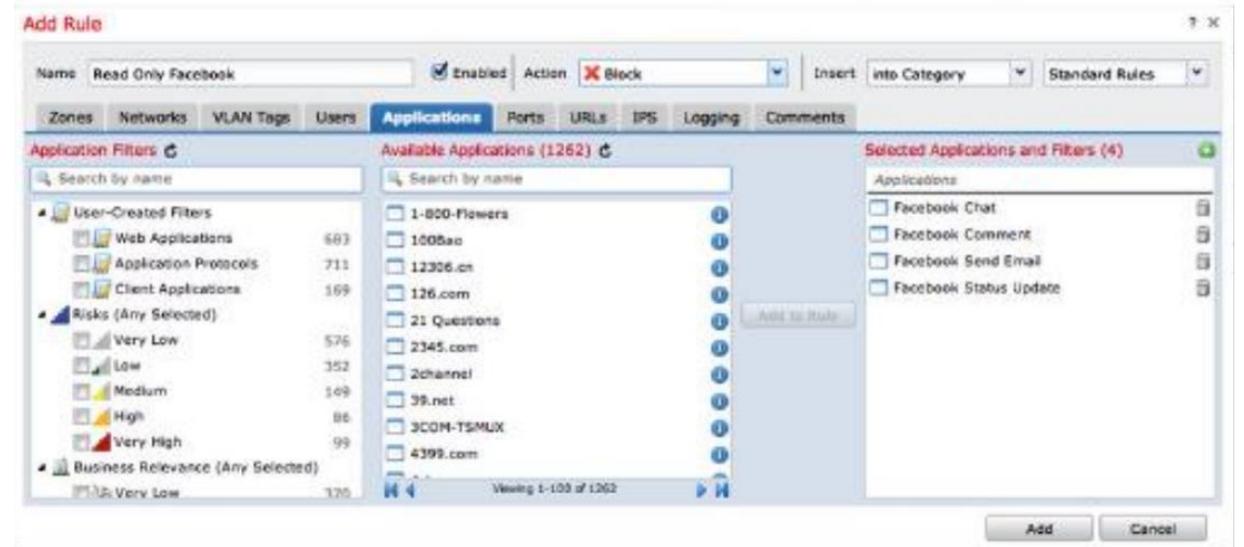
# Мониторинг и контроль приложений

- 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



# Решения для бизнеса любого размера



Virtual



FPR 9300 SeriesSM-40



FPR 4115/25/45



FPR 4110/20/40/50



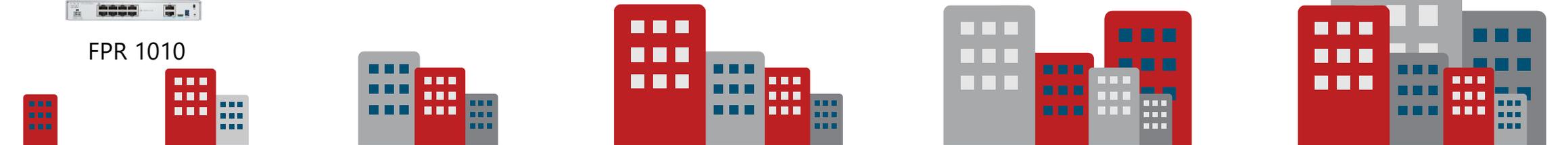
FPR 2110/20/40/50



FPR 1120/40



FPR 1010



SOHO/  
SMB

Branch  
Office

Mid-Size  
Enterprise

Large  
Enterprise

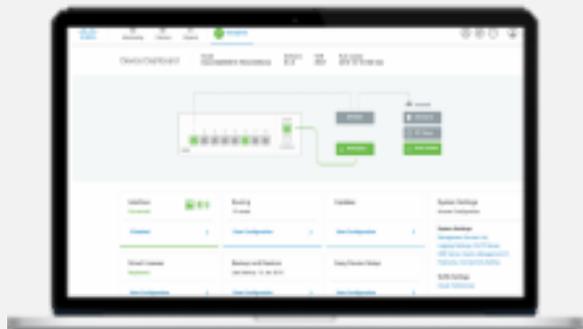
Data  
Center

Service  
Provider

# Варианты управления NGFW

## Firepower Device Manager (FDM)

Автономное



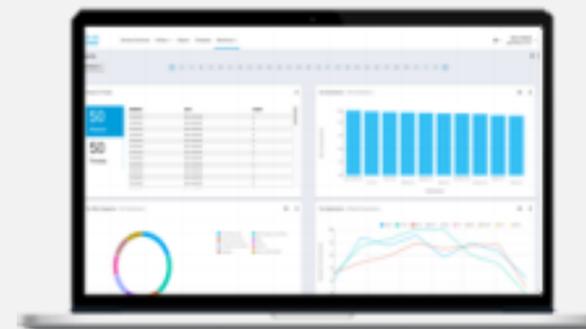
## Firepower Management Center (FMC)

Централизованное



## Cisco Defense Orchestrator (CDO)

Облачное



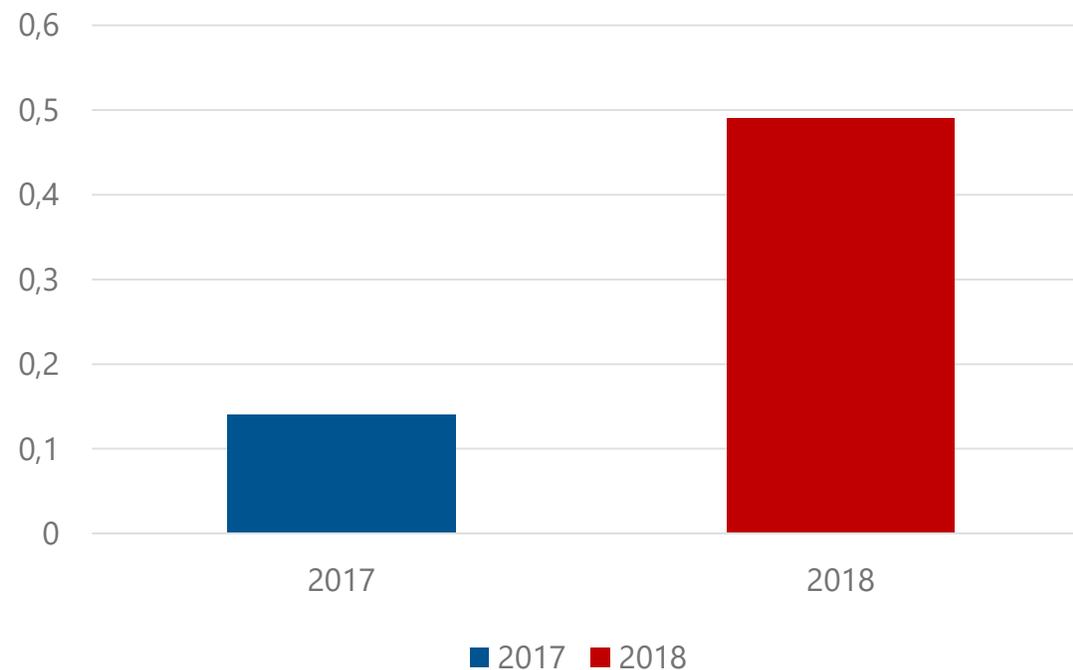
# Email Security



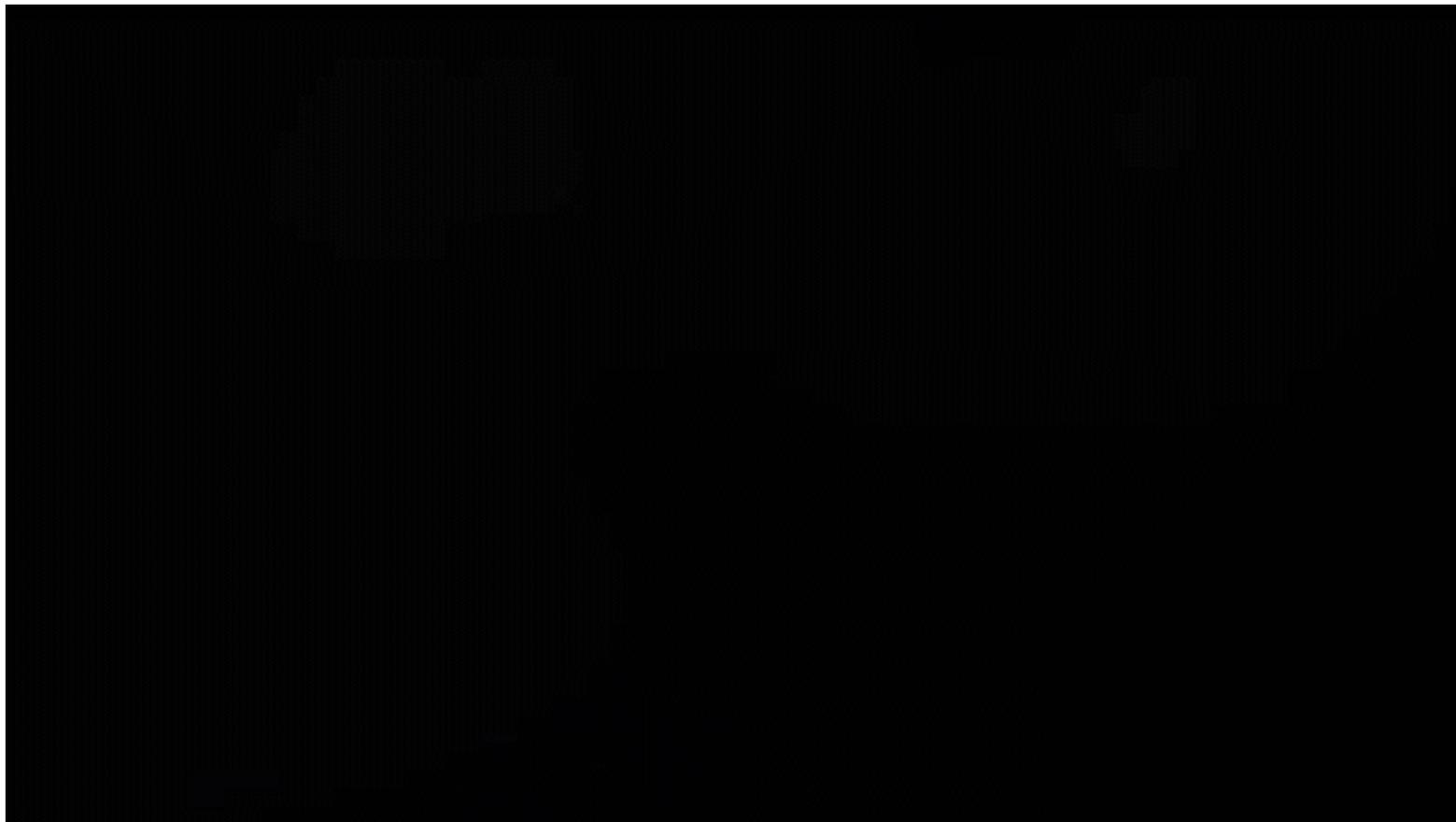
# Угроза фишинга

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

Процент от всего трафика



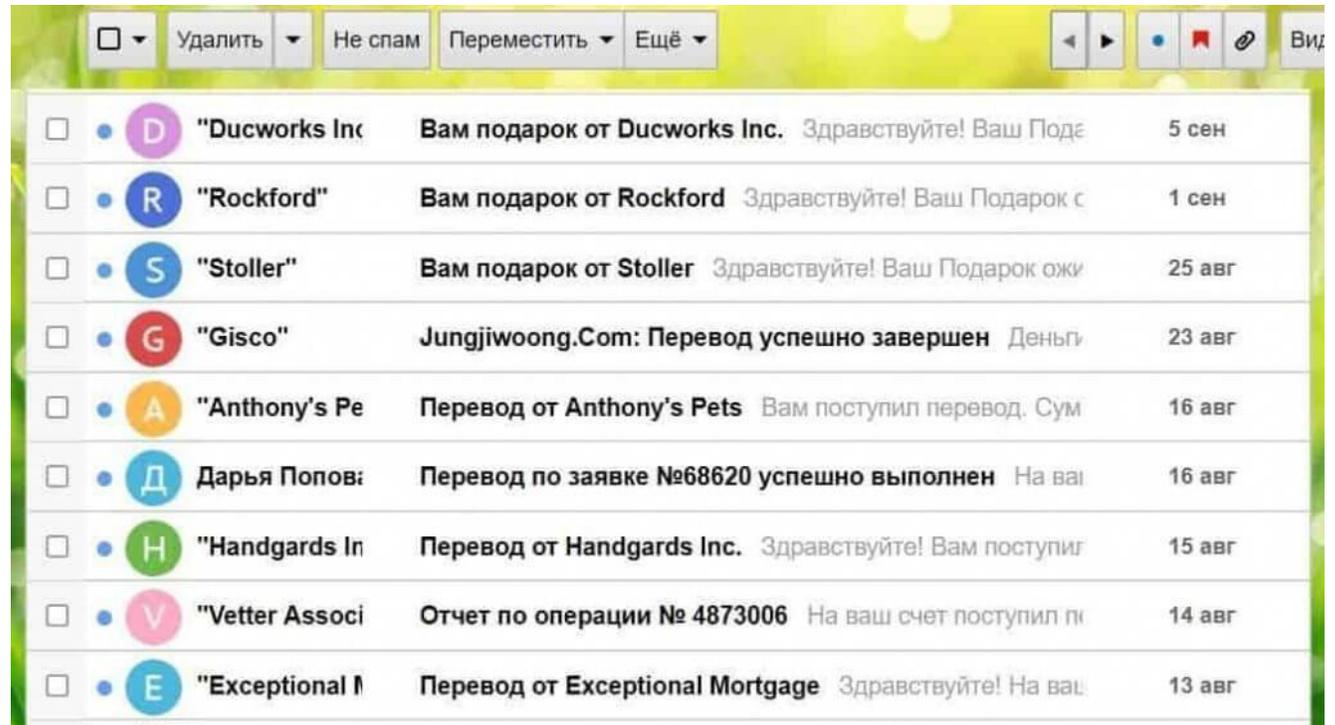
# Как работают хакеры



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

# Количество спама растёт

Спам составляет **86%** от  
всего E-Mail трафика

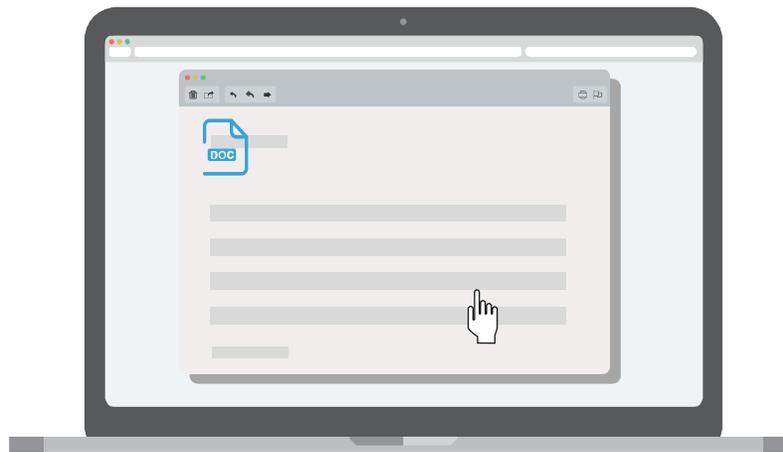
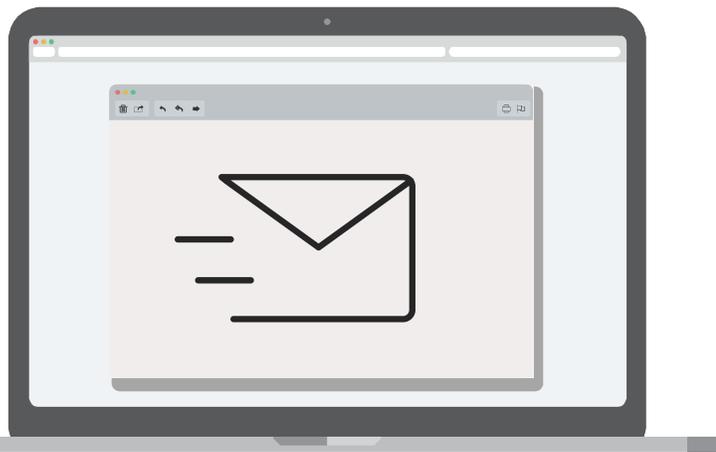
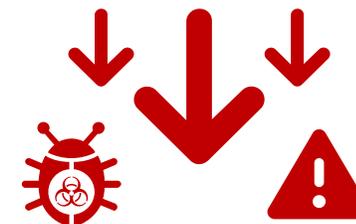


# Как происходит заражение

Алена из HR получает электронное письмо с резюме

Алена открывает вложение

Исполняемый файл загружает вредоносные программы

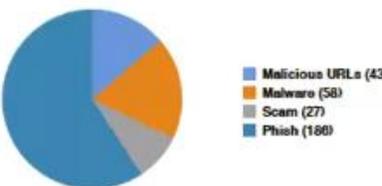


# Полноценная защита почты с ESA



 Deliver  Quarantine  Rewrite  Drop

# Примет отчета

Customer: bce		Email Scan Report		Elapsed Time : 00:32:28	
Mailbox Scan Progress: 100%		Mailboxes Scanned: 14/14		Mailboxes Skipped: 0	
 14 Mailboxes Scanned			 2818 Emails Scanned		
 3 Infected Mailboxes	 198 Spam Found	 43 Malicious URLs	 58 Malware Detected		
<b>Graymail Summary (1164)</b>  <ul style="list-style-type: none"> <li>Bulk (1065)</li> <li>Marketing (99)</li> </ul>			<b>Threat Summary (314)</b>  <ul style="list-style-type: none"> <li>Malicious URLs (43)</li> <li>Malware (58)</li> <li>Scam (27)</li> <li>Phish (186)</li> </ul>		
<b>Top Infected Mailboxes</b> security@bce-demo.com 6 Messages munwar@bce-demo.com 4 Messages emiroyu@bce-demo.com 1 Messages			<b>Top Malware Found</b> W32.9C3390B9AF-100.SBX.TG 1 Messages W32.1C6A8229EC-100.SBX.TG 1 Messages W32.B2F0189C4F-100.SBX.TG 1 Messages W32.3C75596B1D-100.SBX.TG 1 Messages W32.9C70456CF4-100.SBX.TG 1 Messages		

# 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

The image shows a browser window with the URL `https://t-avito.ru/order.php?id=162480fa`. The page is titled "Оплата заказа" (Order Payment) and features the Avito logo. It displays a payment form for a card, with a total amount of 3470 RUB. A modal window titled "Оформление заказа" (Order Form) is overlaid on the right, containing fields for recipient information (Name and Surname, Phone, Email, Delivery Address) and a price breakdown table. The price breakdown shows "Ps vita" for 3000 RUB and "Доставка 1-2 дня" for 470 RUB, totaling 3470 RUB. A blue "Купить" (Buy) button is visible at the bottom right of the modal. The background page includes security logos (MasterCard, Verified by VISA, 3D Secure, AVIS) and a disclaimer about SSL and 3D Secure protection.

Авито доставка - оплата

https://t-avito.ru/order.php?id=162480fa

Avito

### Оплата заказа

Ps vita

Заказ №35271279

Безопасное соединение

ВISA MIR

Товары с доставкой оплачиваются только банковской картой онлайн.

Гарантия возврата денег если:  
— продавец отменил заказ,  
— товар не подошёл или брак,  
— вы не получили товар.

Номер карты  
0000 0000 0000 0000

Срок действия  
00 / 00

CVC

Итого: 3470Р

Оплатить

Для обеспечения безопасности, Ваш счёт к оплате может быть разбит на несколько платежей.

MasterCard SecureCode Verified by VISA 3D Secure AVIS

Интернет-платежи защищены сертификатом SSL и протоколом 3D Secure. АО «Тинькофф Банк» не передает магазинам платёжные данные, в том числе данные карты. Оплачивая заказ вы соглашаетесь с офертой

Сервис предоставлен «Тинькофф Банк»

Тинькофф Оплата

### Оформление заказа

#### Получатель

Имя и фамилия

Телефон

Эл. почта

Адрес доставки

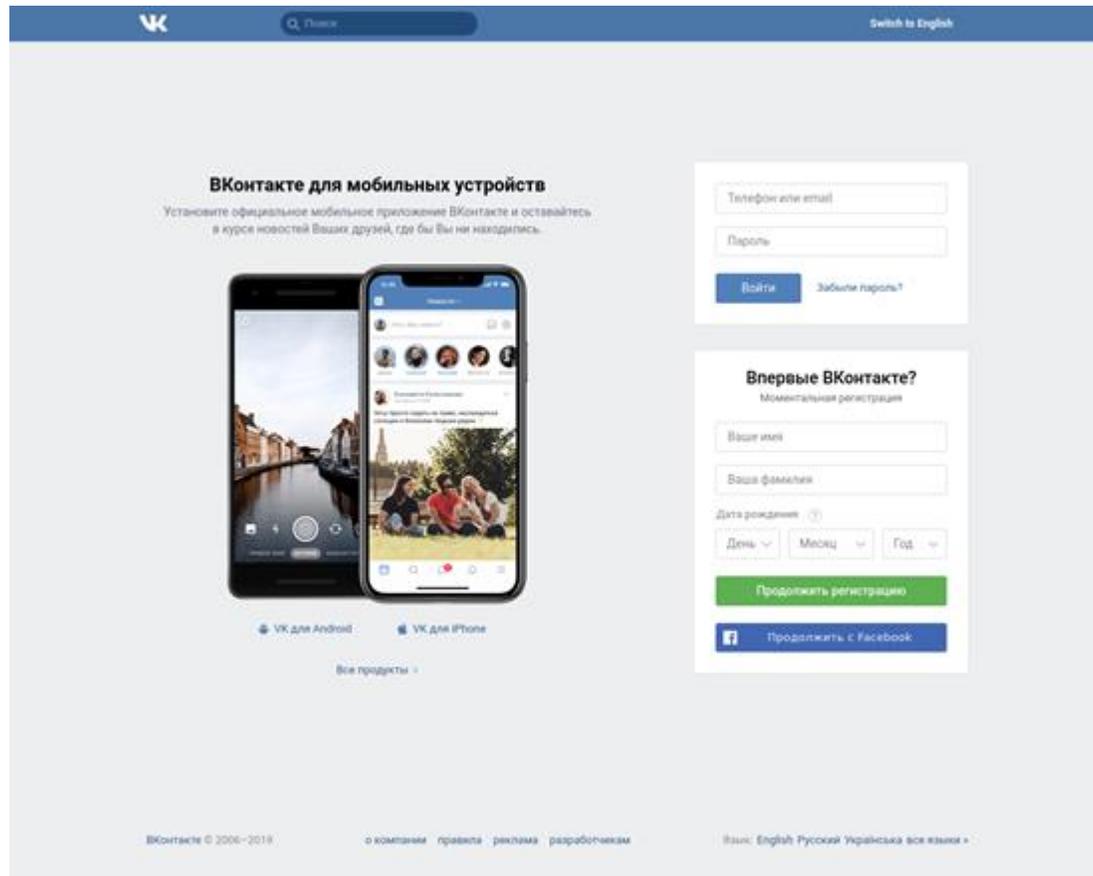
#### Стоимость

Ps vita	3000 Р
Доставка 1-2 дня	470 Р
<b>Итого: 3470 Р</b>	

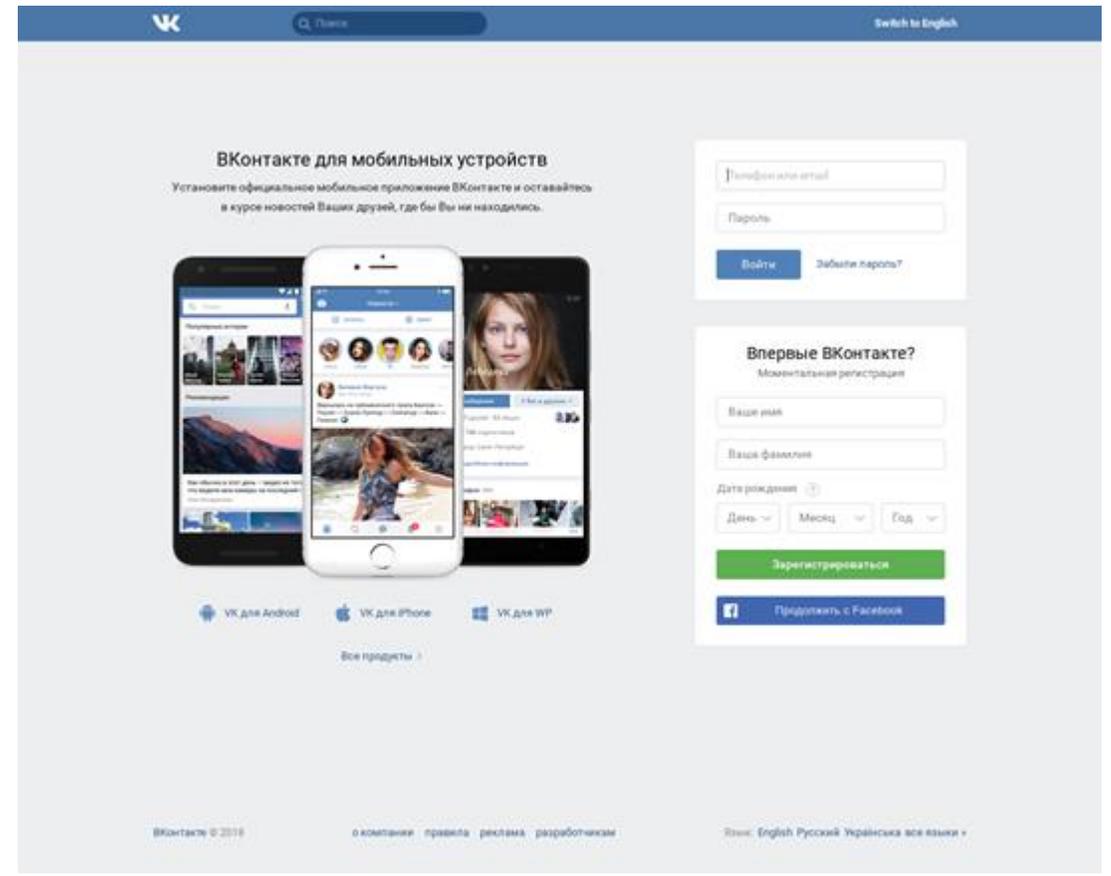
Нажимая «Перейти к оплате», вы принимаете [оферту](#) и подтверждаете достоверность ваших данных.

Купить

# Пример фишинга

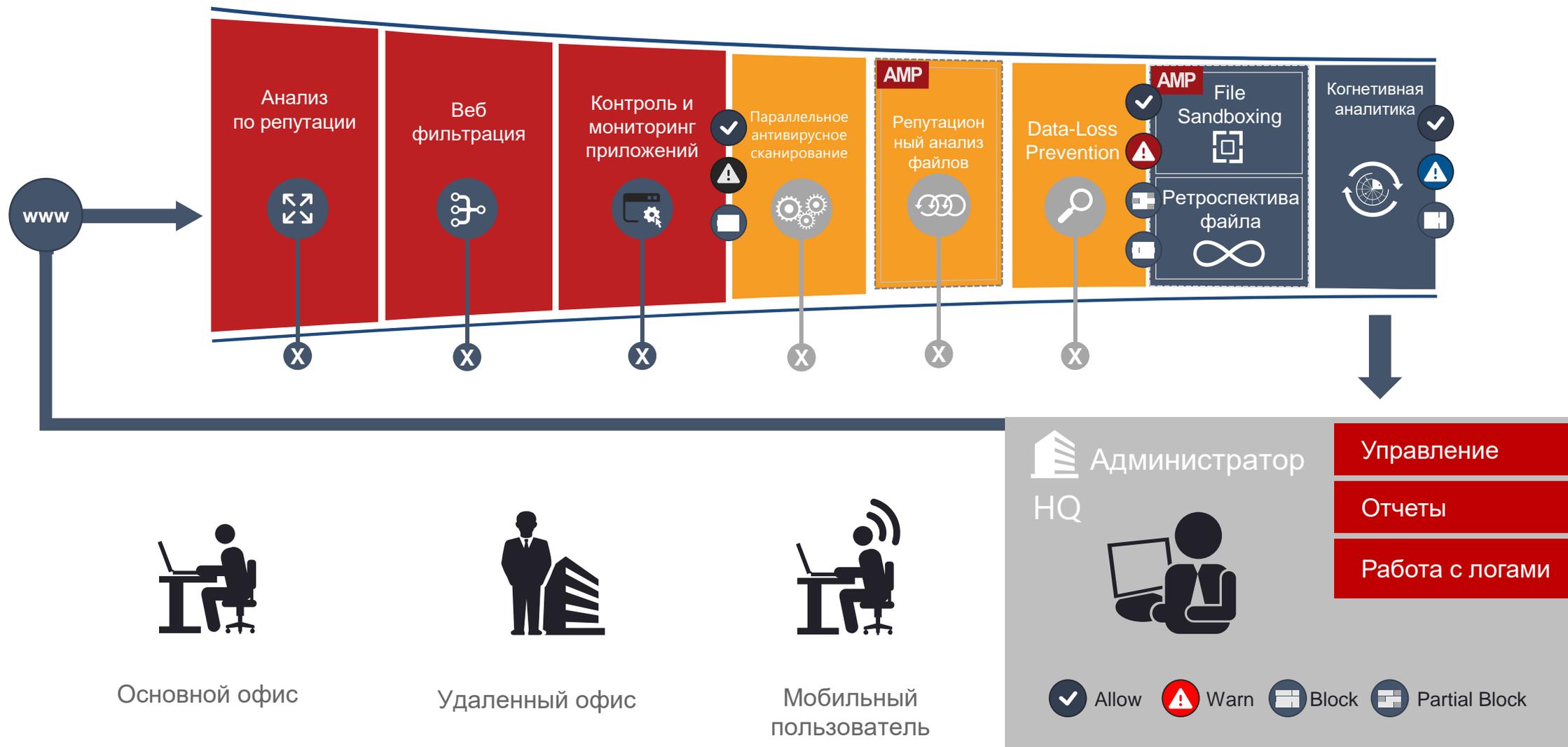


Настоящая страница входа



Фишинговая версия

# Как работает Web Security Appliance



# URL фильтрация

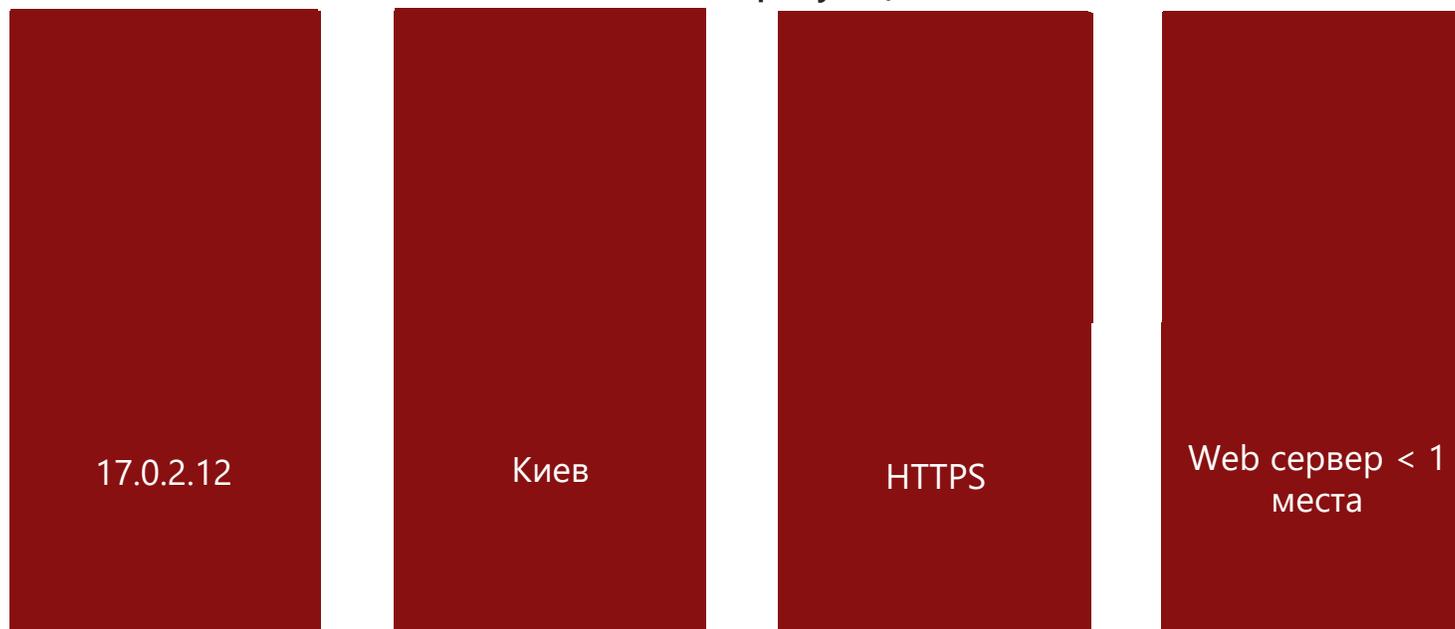


- Финансы
- Развлечения
- Медицина



# Репутационный анализ

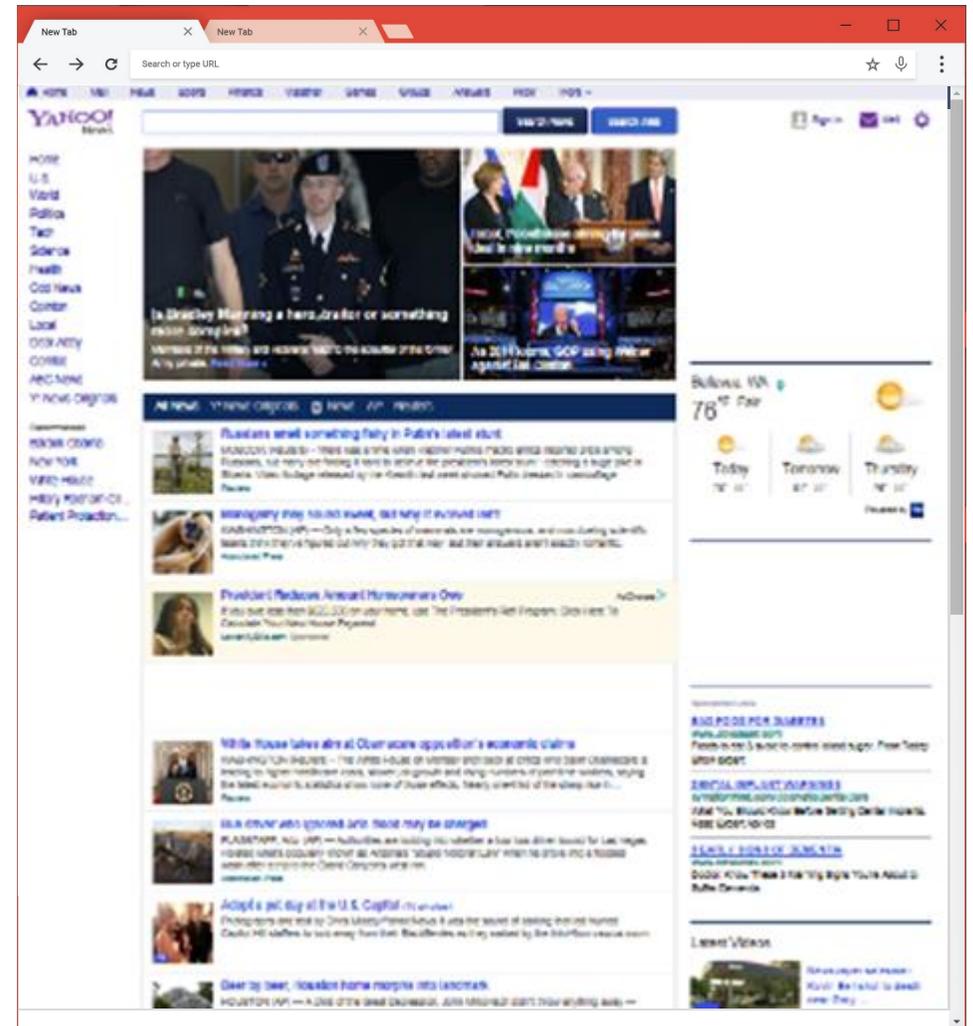
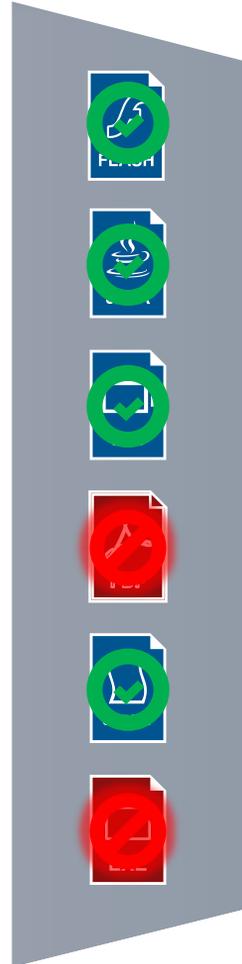
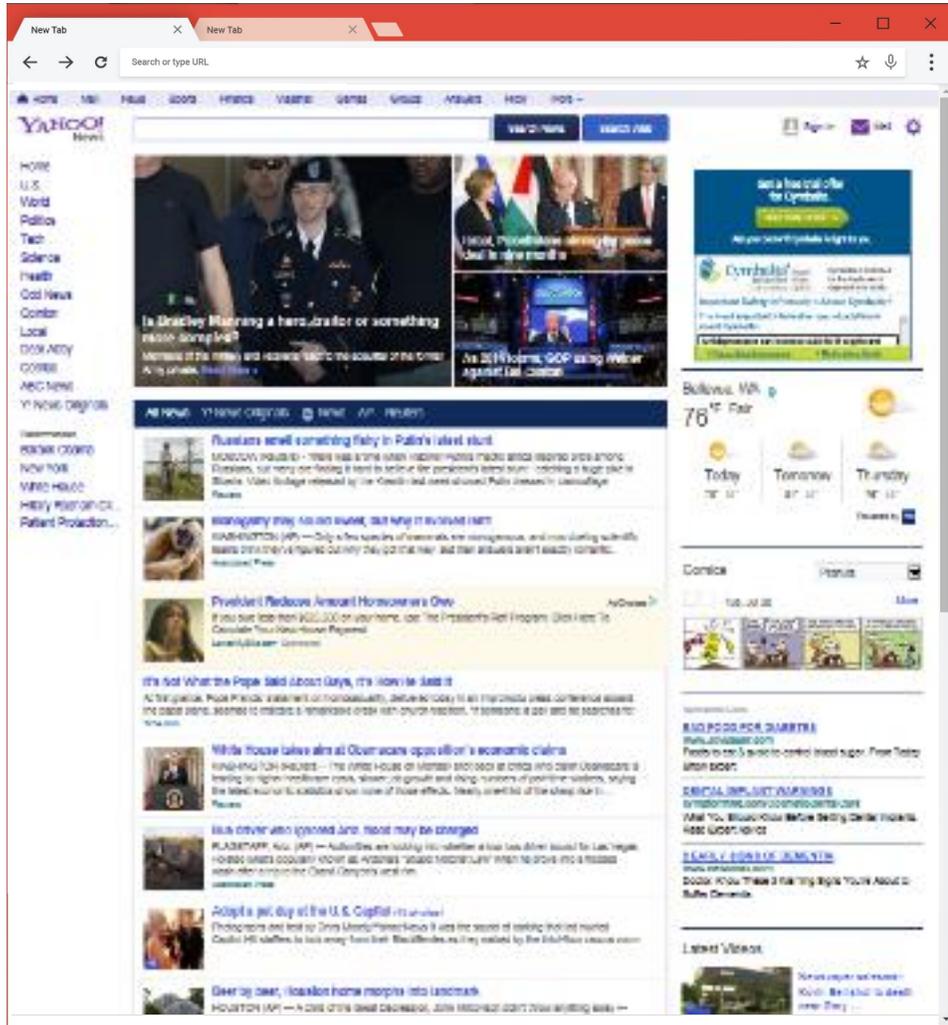
## Сила контекста реального времени



010 10010111001 10 100111 010 000100101 110011 01100111010000110000111000111 100001110001110 1001 1101 1110011 0110011 101000 0110 00 0111000 111010011  
1100110 1100 111010000 110 0001110 00111 010011101 11000 0111 0001110 1001 110011 101000 0110 00 0111000 111010011 101 1100001 11000 111010011101  
0010 010 10010111001 10 100111 010 00010 0101 110011 011 001 110100001100001 10011101 1100001110001110 1001 1101 1110011 0110011 101000 0110 00 0111000 11



# Sandbox реального времени



IDENTITY PROTECTED

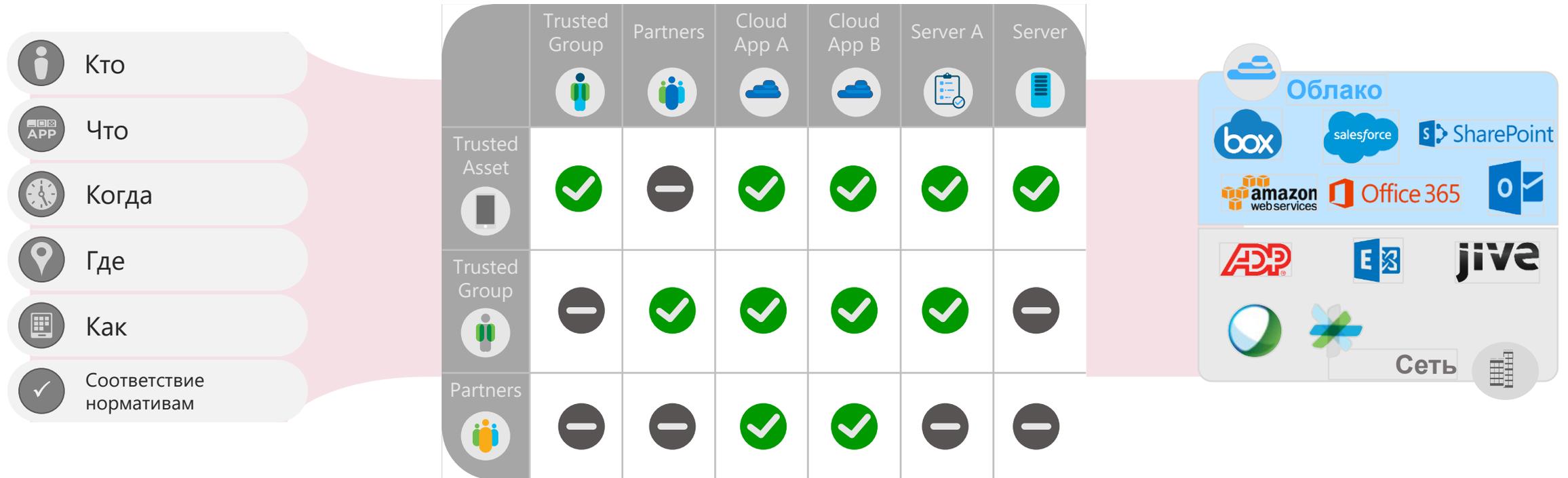
200 841 341 222 100 10 300-2000  
000 254 751 200 200 200-2000  
224 267 254 210 200 200 200-2000  
231 274 222 200 200 200-2000  
224 212 212 200 200 200-2000  
224 217 200 200 200 200-2000

# Identity Service Engine

XXXX XXXX XXXX  
XXX XXX XXX XXX XXX XXX XXX  
XXX XXX XXX XXX XXX XXX XXX



# Как работает ISE



# 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

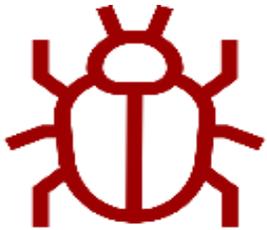
	aruba	MOTOROLA SOLUTIONS	JUNIPER NETWORKS	BROCADE	Hewlett Packard Enterprise	CISCO
Profiling	✓	✓	✓	✓	✓	✓
Posture	✓	✓	✓	✓	✓	✓
Guest	✓	✓	✓	✓	✓	✓
BYOD	✓	✓	✓	✓	✓	✓
MDM	—	—	—	—	—	✓
TrustSec	—	—	—	—	—	✓

[https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/compatibility/b\\_ise\\_sdt\\_26.html](https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/compatibility/b_ise_sdt_26.html)

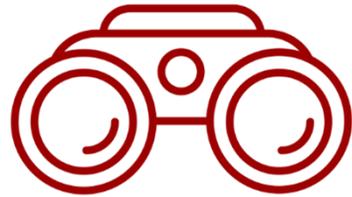
Umbrella



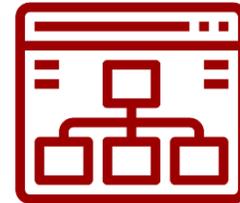
# В чем проблема?



Вредоносный код  
и шифровальщики



Редиректы

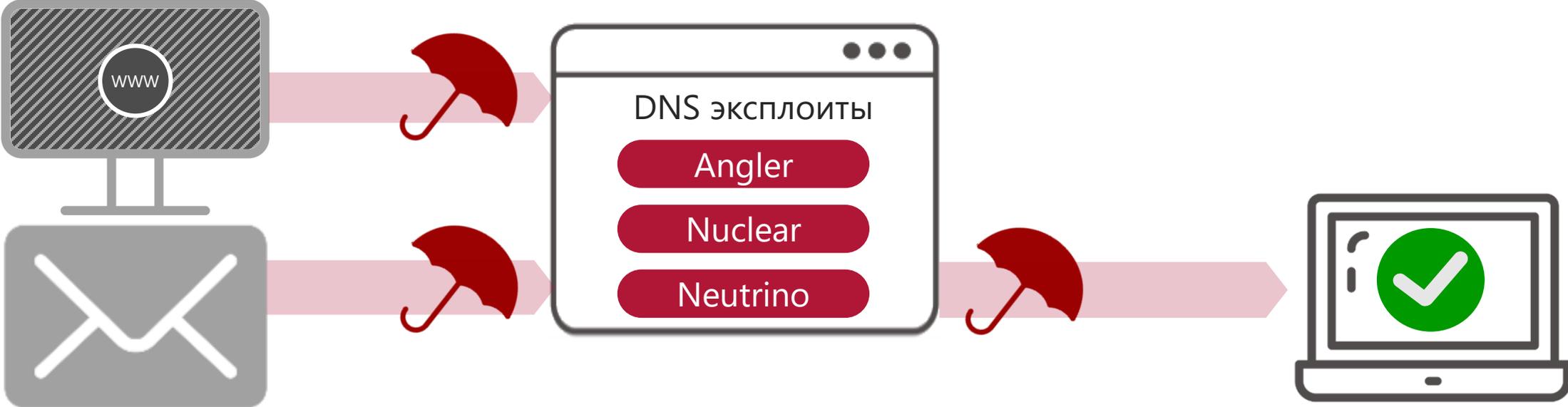


Сайты-клоны

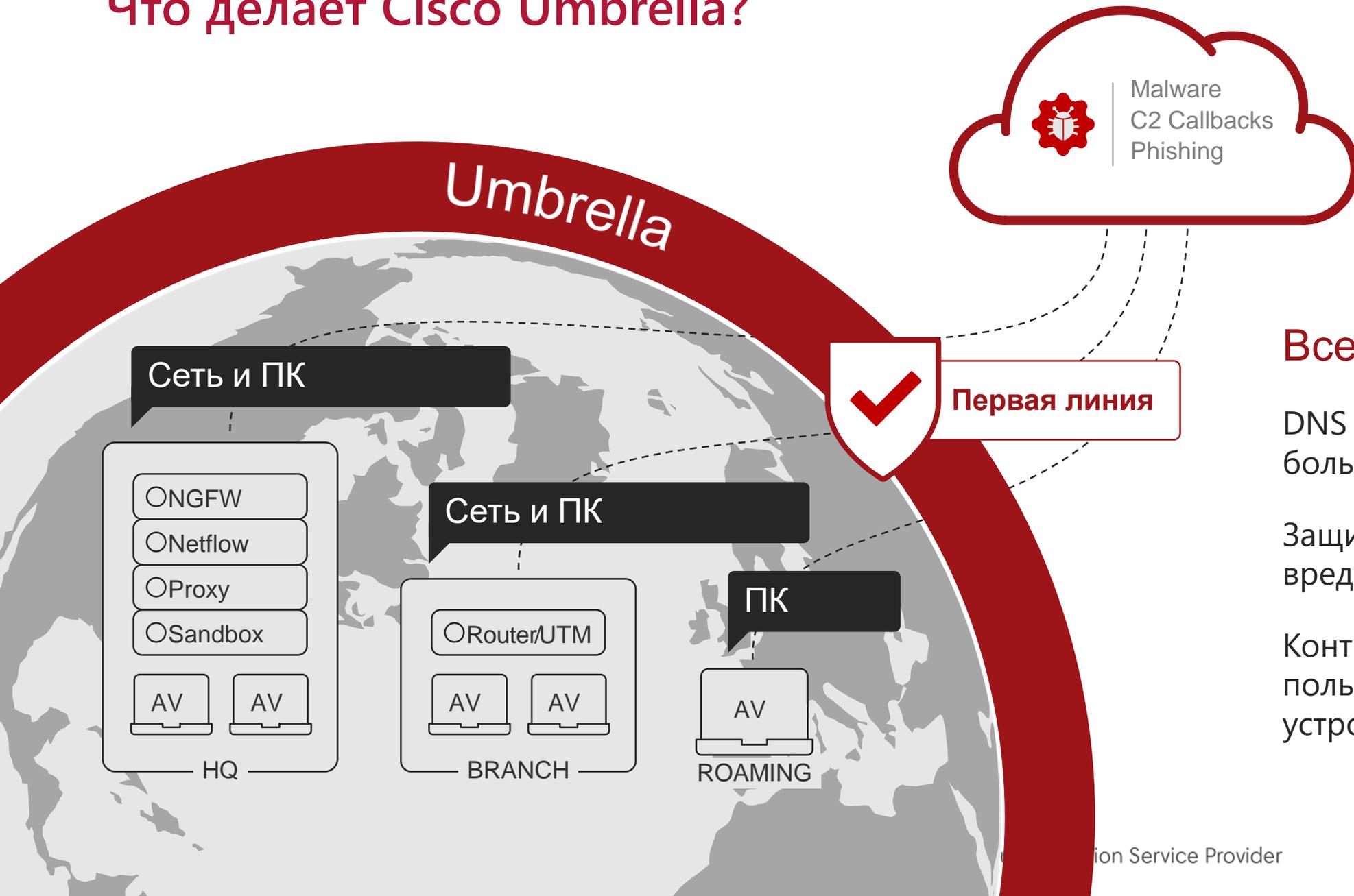


Утечки  
информации

# 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

# Stealthwatch

The image features a stylized world map where the continents are defined by a complex network of glowing blue lines and nodes. The map is set against a dark, starry background. A prominent red rectangular box is overlaid on the left side of the image, containing the word "Stealthwatch" in white, bold, sans-serif font.

# Эффективная безопасность зависит от полной видимости



**ВИДЕТЬ**  
каждый хост



**ЗАПИСАТЬ** каждое  
взаимодействие



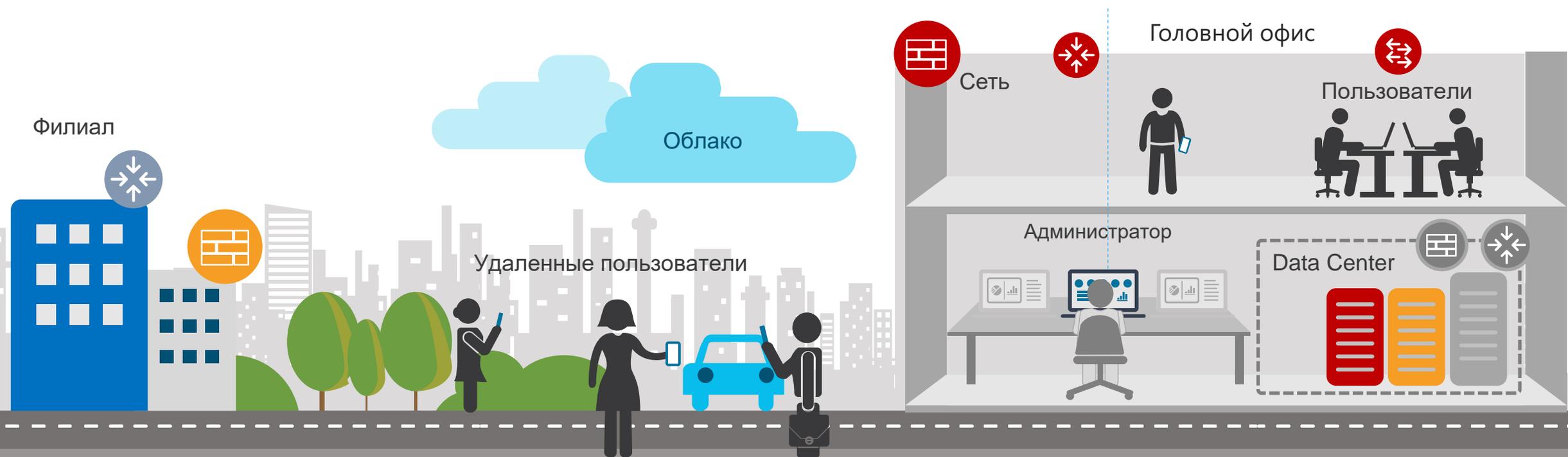
Знать, что поведение  
**НОРМАЛЬНОЕ**



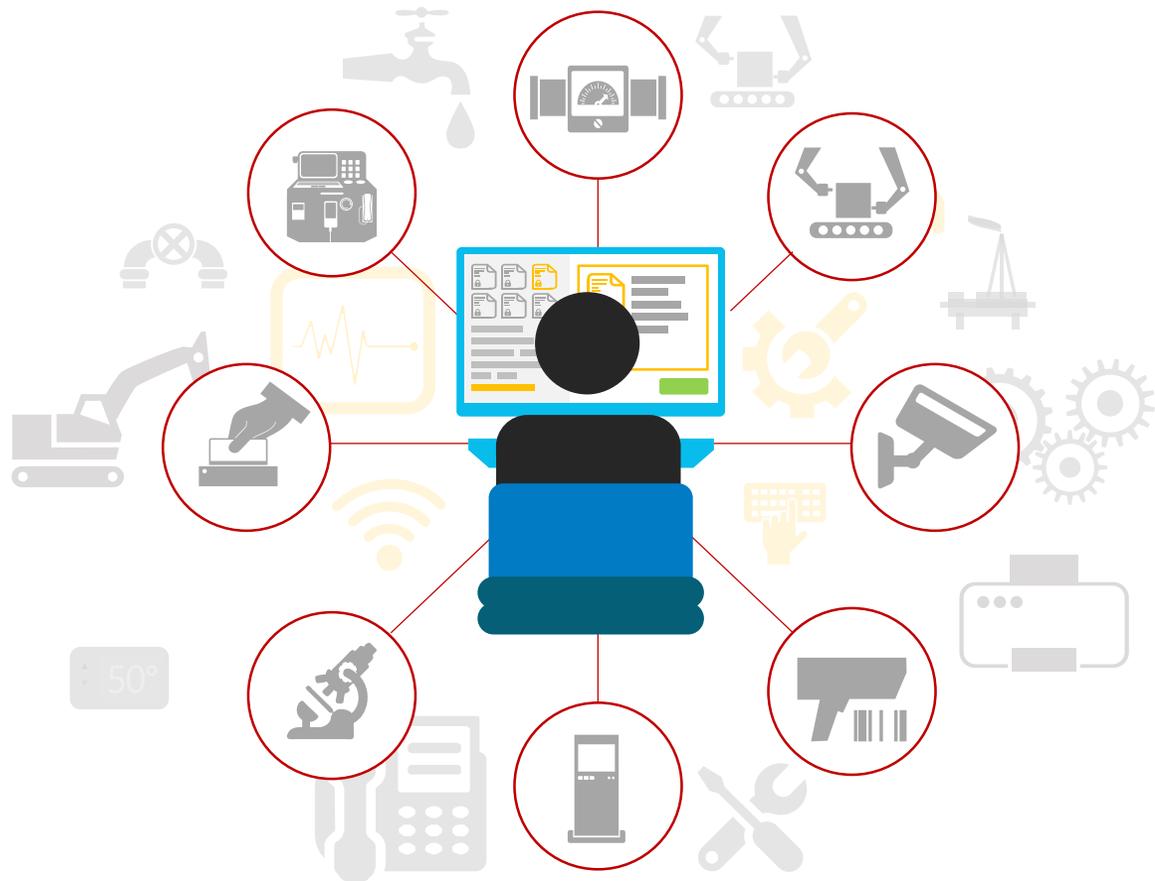
Быть оповещенным  
об **ИЗМЕНЕНИЯХ**



Быстро **РЕАГИРОВАТЬ**  
на угрозы



# Защита устройств Интернета вещей (IoT)



Обнаружение  
вредоносного поведения



Нет агентов конечных  
точек



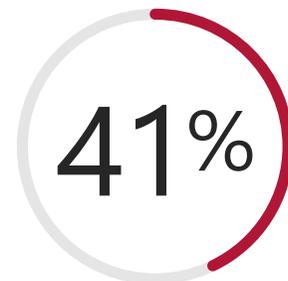
Сегментация



# Encrypted Traffic Analytics

# Шифрованный трафик в сети?

организаций являются жертвами злонамеренной деятельности \*



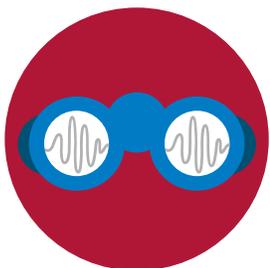
при атаках используется зашифрованный трафик, чтобы избежать обнаружения \*



\*Source: Ponemon Institute – Hidden threats in encrypted traffic

Как обеспечить безопасность при сохранении конфиденциальности?

# Аналитика



Обнаружение угроз  
в зашифрованном  
трафика

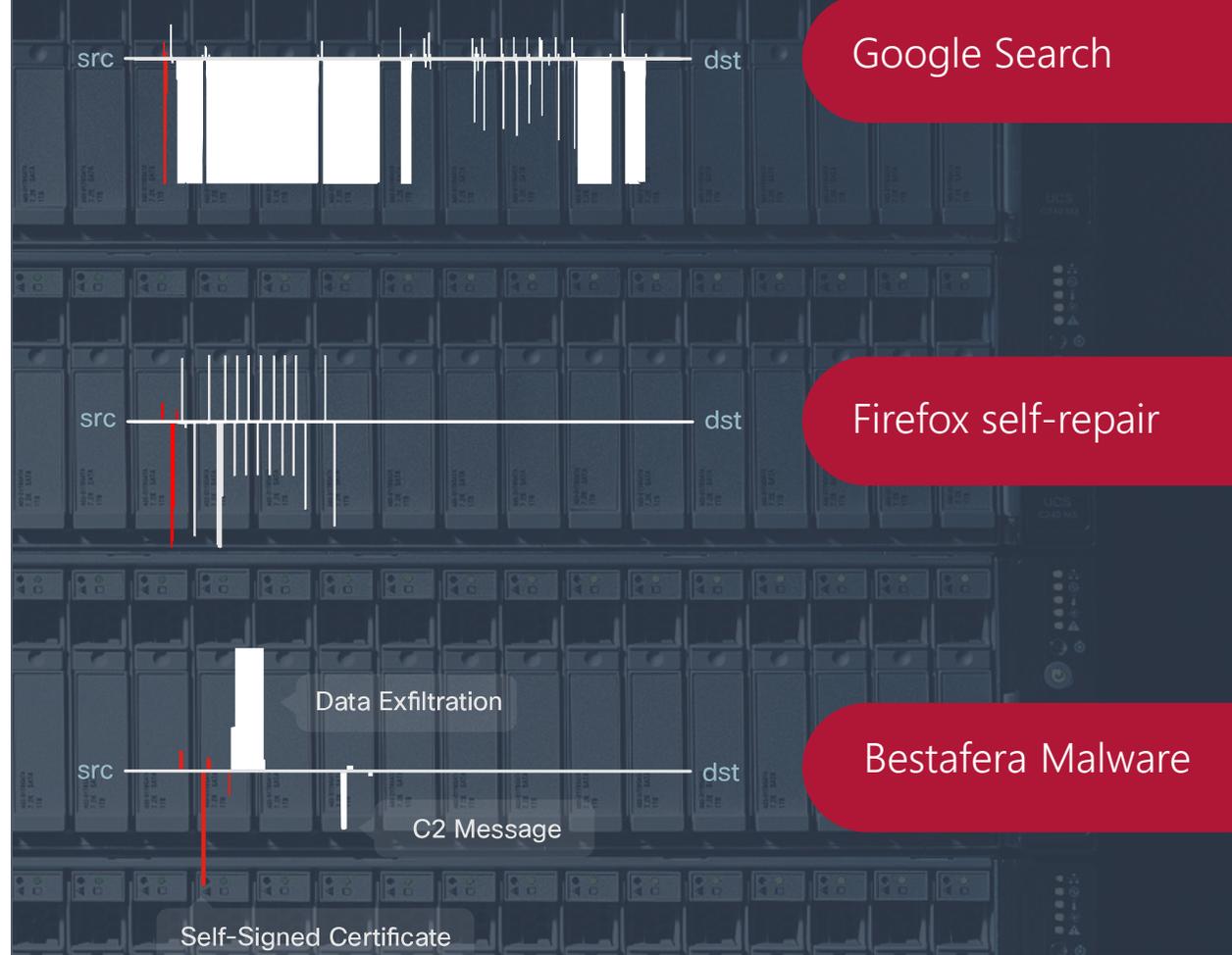


Сохранение  
персональной  
информации

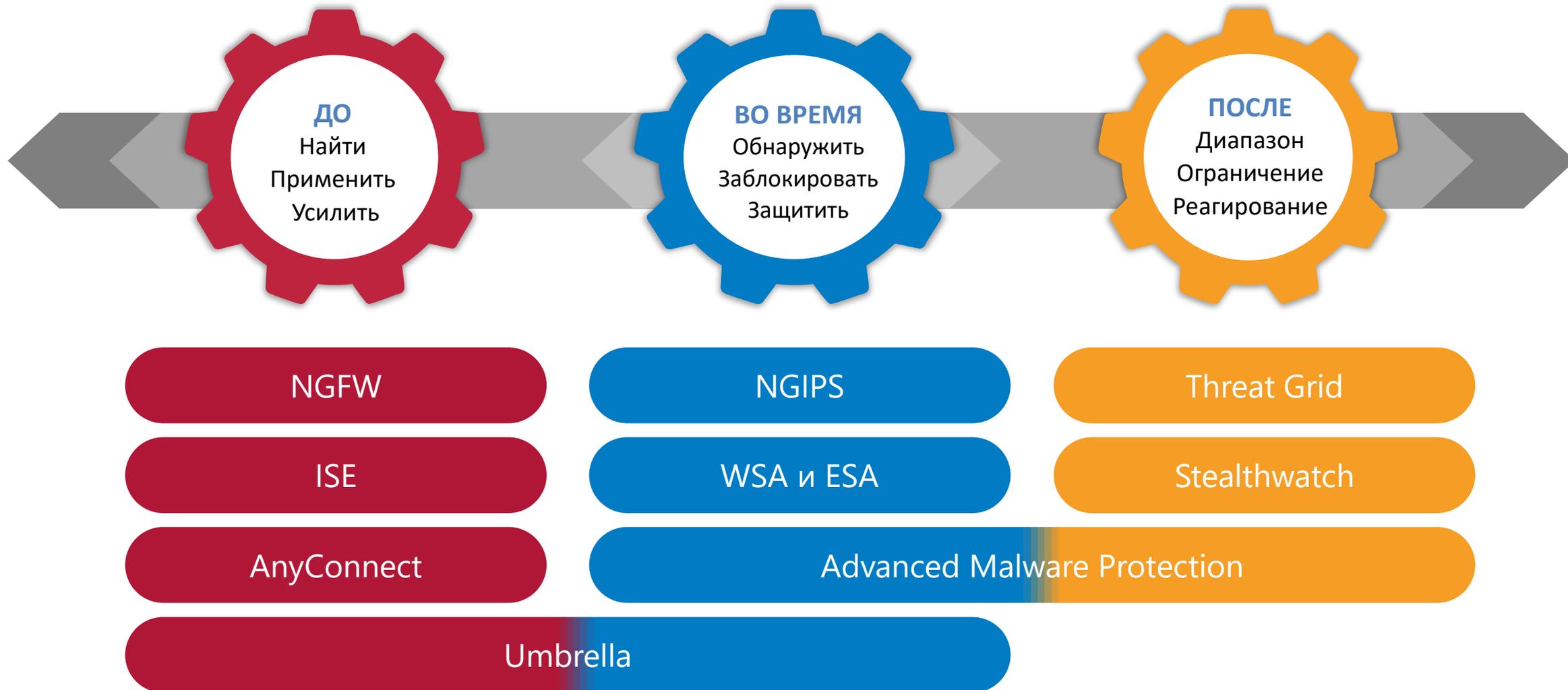


Точность  
обнаружения  
99.99%

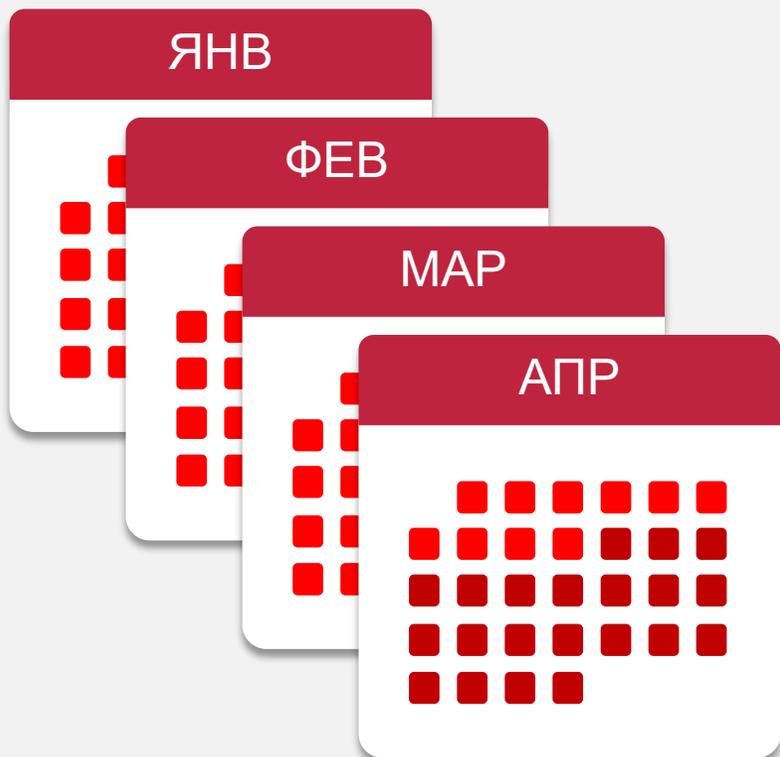
# Представление данных



# Cisco защищает на протяжении всего цикла атаки

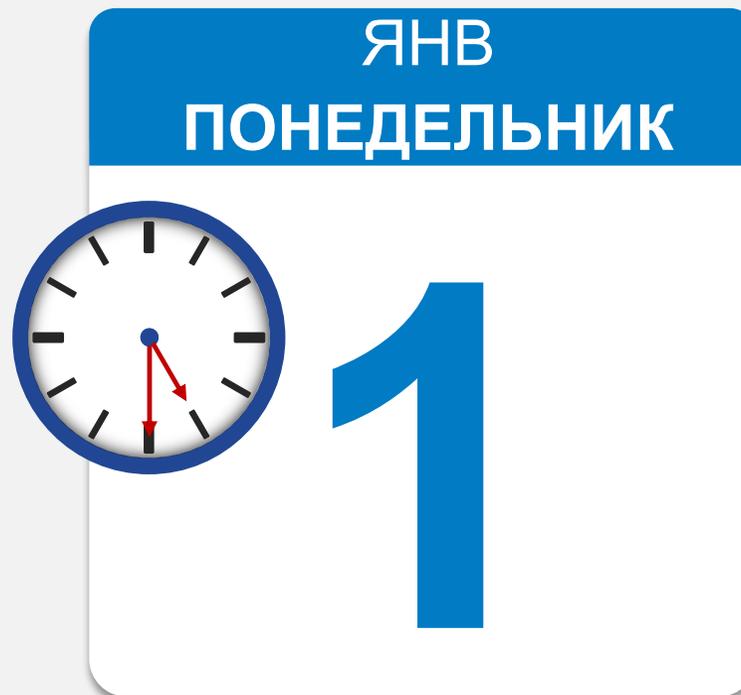


Типичный TTD rate:\* 100 дней



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

Cisco: 17,5 часов



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





GO GLOBAL



GO CLOUD



GO INNOVATIVE

**Дмитрий Казаков**

Менеджер по развитию бизнеса Cisco Security

[D.Kazakov@softline.com](mailto:D.Kazakov@softline.com)