HUAWEI

КОНТАКТ
КОМПЬЮТЕРЫ И КОМПЬЮТЕРНЫЕ СИСТЕМЫ

Безопасность корпоративной сети с решениями Huawei Enterprise

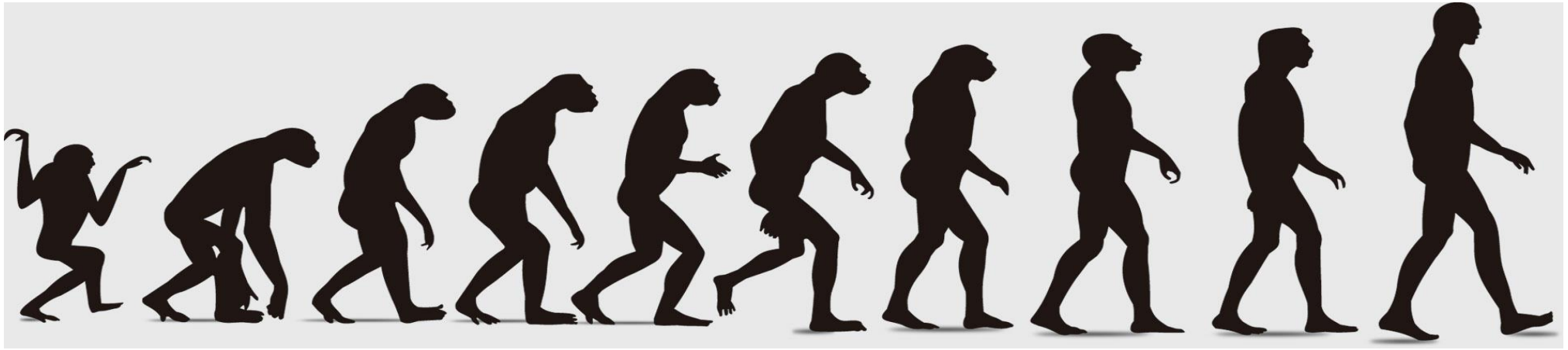
Межсетевые экраны с технологиями искусственного интеллекта

LEADING NEW ICT

История межсетевых экранов

Фильтрация пакетов	Технология SPI (инспекция пакетов)	ASIC-based (интегральные схемы)	Unified Threat Management (UTM)	Multi-core + distributed architecture	NGFW	?
	Check Point/Cisco	NetScreen	Fortinet	Huawei/Juniper	Huawei/Palo Alto	

1989	1994	1998	2004	2008	After 2009	Сегодня
Эпоха ПК	Эпоха сетей	Эпоха Internet	Web 2.0		Эра мобильного Интернета	ИИ (искусственный интеллект)
Базовый контроль доступа	Появление контроля сеансового уровня	Использование специализированных процессоров для повышения эффективности	Многофункциональность	Улучшенная производительность	Контроль приложений, пользователей и контента	



Современные вызовы безопасности корпоративных сетей

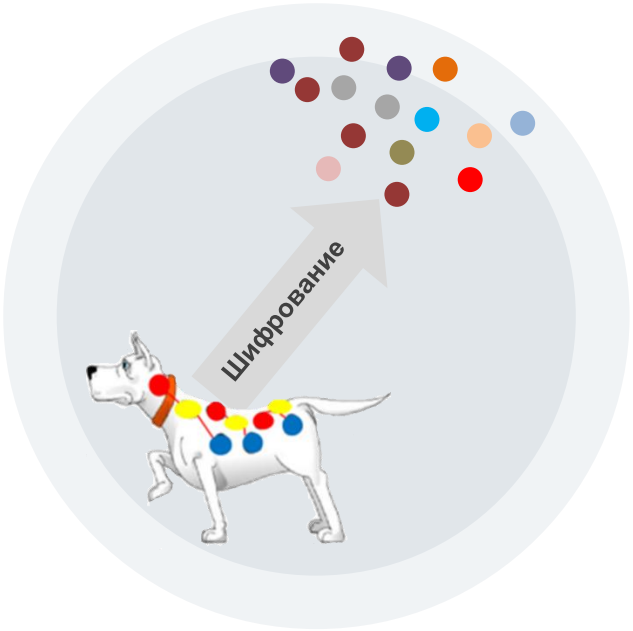
Множественность угроз

Развитая хакерская индустрия;
непрекращающиеся атаки

Скрытые атаки

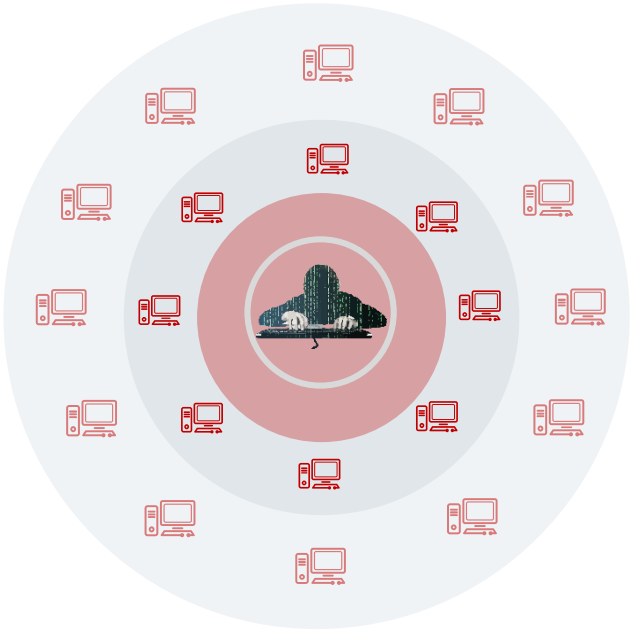
70% атак используют шифрование;

Анализ пакетов неэффективен.



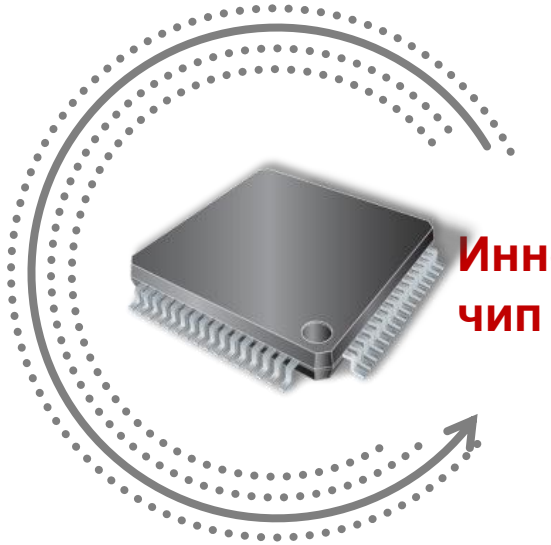
Стремительность

Автоматическое управление атаками и моментальное распространение



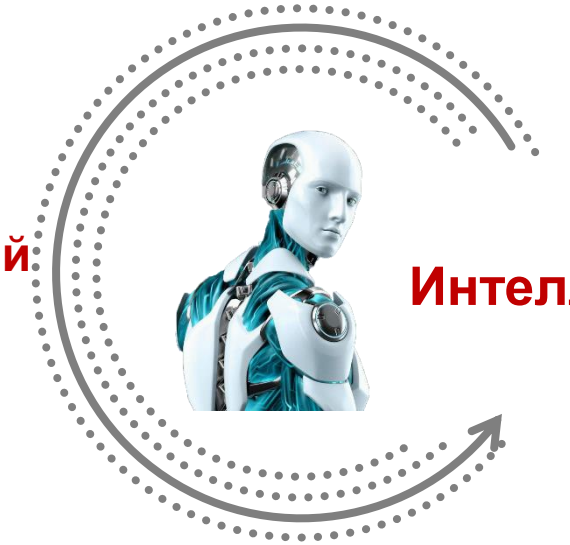
Микросхемы с искусственным интеллектом как ядро интеллектуальной защиты

Межсетевые экраны Huawei с технологиями ИИ, усиленные инновационным чипом.



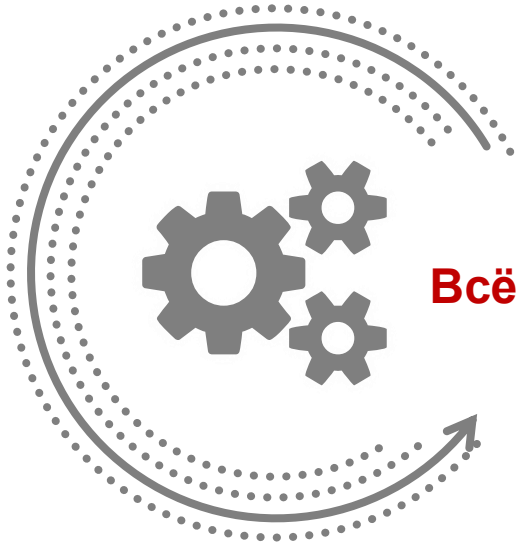
Инновационный чип

- Новейший чип безопасности со встроенным механизмом ускорения, разработанный компанией "Huawei".
- **Производительность в два раза больше, по сравнению со средними показателями в индустрии.**



Интеллект

- Расширенное обнаружение угроз, основанное на ИИ и связи с "облаком".
- Показатель детектирования **> 99%**

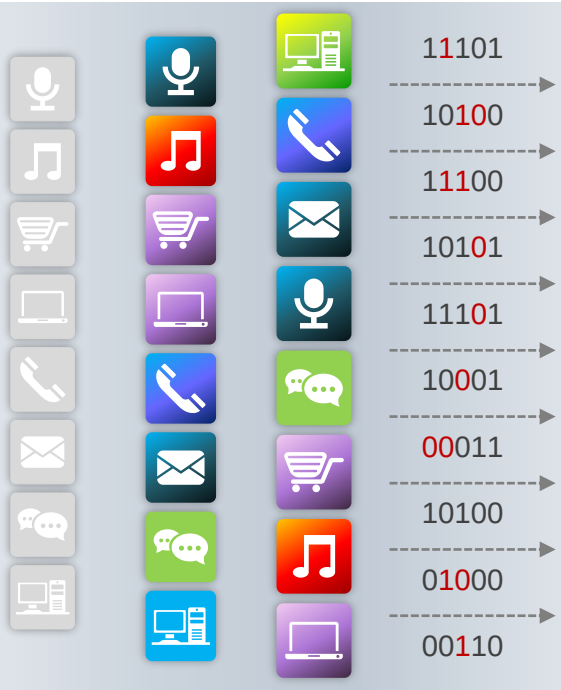


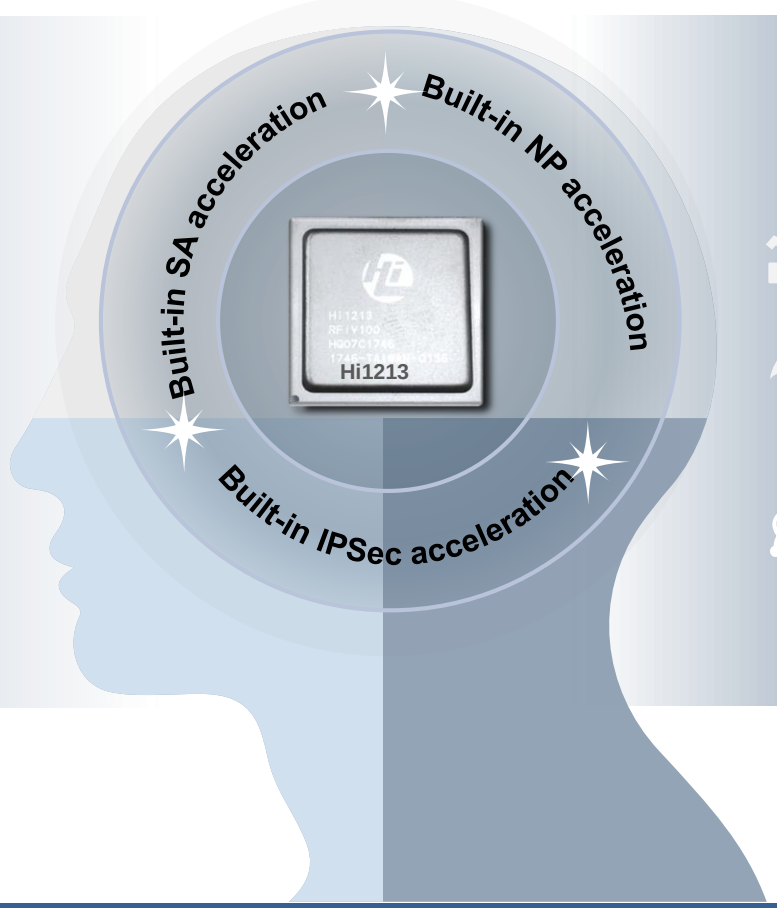
Всё включено

- Архитектура виртуализации, интеграция со множеством сервисов, гибкая интеграция с возможностями сторонних производителей.
- **Капитальные расходы снижаются на 80%**

Инновационный чип: Удвоение производительности

Чип на архитектуре ARM, первый из собственной разработки, оптимизирует и ускоряет ключевые возможности для **удвоения производительности файрвола.**





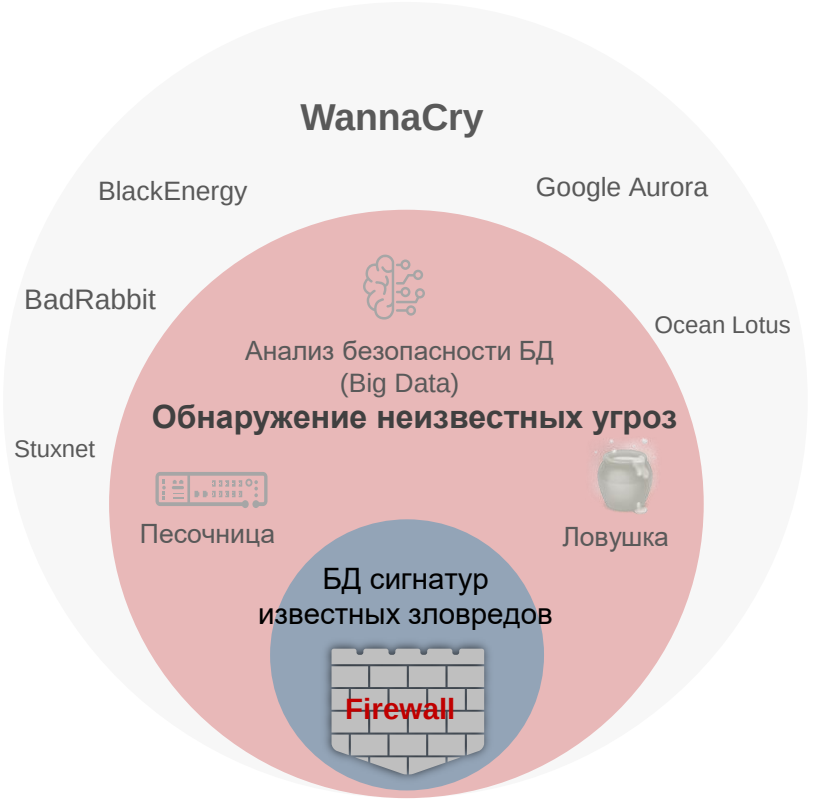
Удвоенная прозводительность при обработке небольших пакетов

Удвоенная производительность IPS (Intrusion Protection System) / Антивирусных сервисов

Удвоенная производительность сервисов IPSec

Интеллектуальный подход: передовой механизм обнаружения угроз, использующий ИИ

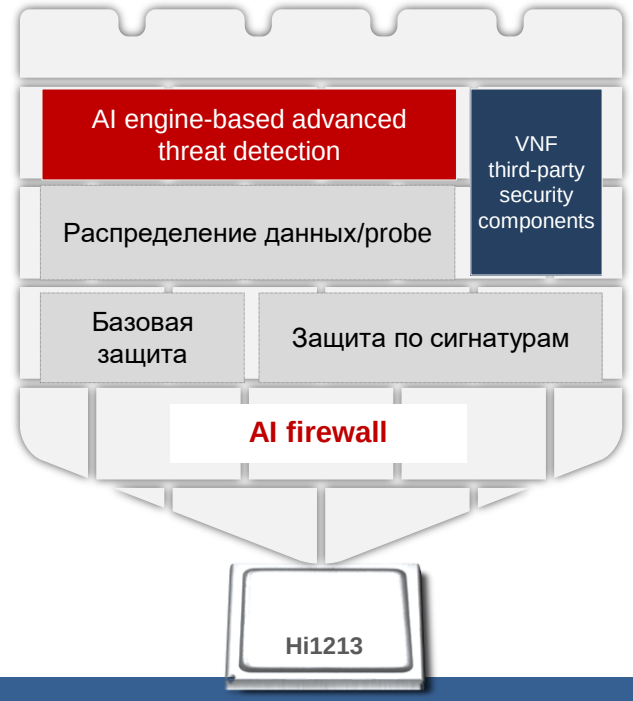
Традиционные средства для предотвращения угроз требуют больших затрат.



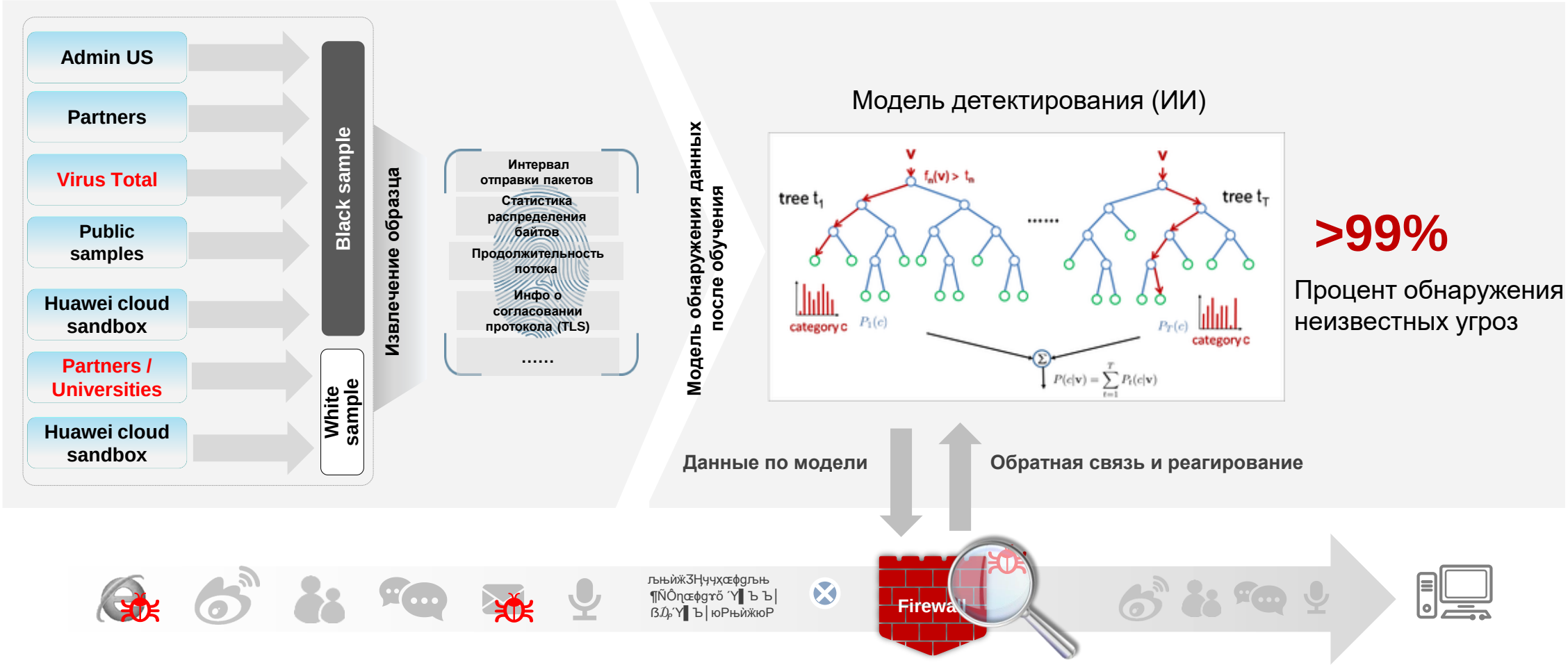
Стоимость оборудования (CapEx) ↓ 80%

Файрвол со встроенными передовыми возможностями по обнаружению - проактивно защищает от неизвестных угроз.

- Встроенный ИИ мгновенно обнаруживает заражение.
- Результат обнаружения передается в облако для оптимизации алгоритмов и моделей ИИ.
- Межсетевой экран обновляет ИИ-модель в режиме реального времени.



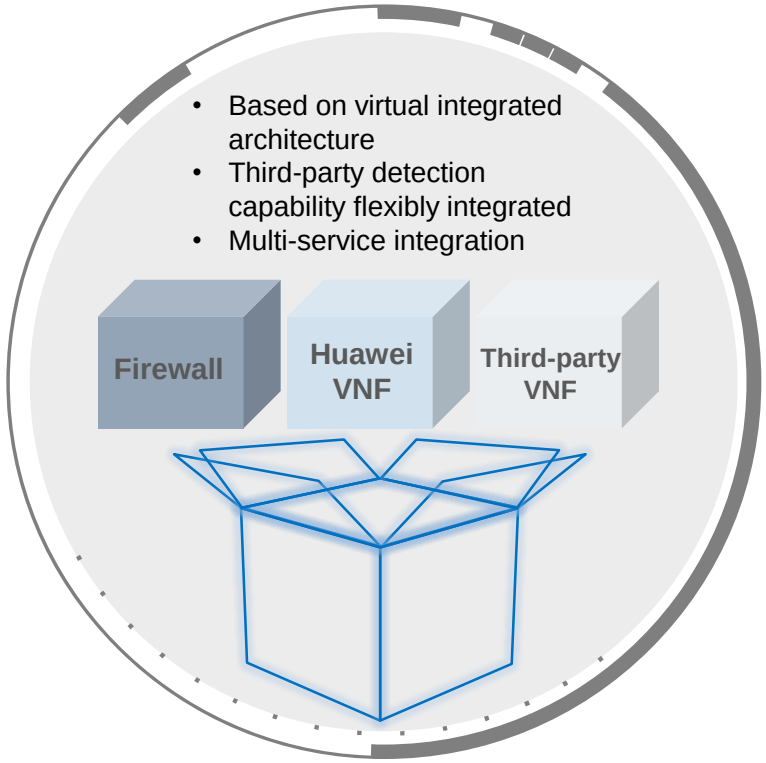
Интеллектуальный подход: обнаружение зашифрованного трафика на основе ИИ без расшифровки/дешифрования



>99%

Процент обнаружения неизвестных угроз

Всё включено: архитектура виртуальной интеграции обеспечивает расширение "по-требованию" сетевых возможностей



Архитектура виртуальной интеграции = 1 + N

- **Быстро**

Удаленная установка новых сетевых возможностей и приложений

- **Экономично**

Не нужно приобретать дополнительное железо.

- **Легко управлять**

Меньше аппаратных устройств;
Проще эксплуатация и обслуживание

- **Легко расширить**

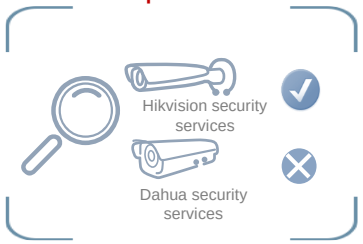
Достаточное количество памяти и места на жестком диске для дальнейшего расширения.

Всё включено: защита доступа, визуализация сетевых угроз

Блокировка неавторизованных устройств

Надежный доступ, безопасность, и легкое развертывание.
Может быть расширено на другие IoT-устройства.

Блокировка неавторизованных сервисов



Вторая линия защиты может быть применена после преодоления аутентификации.
Углубленный анти-спуффинг и предотвращение вторжений

Блокировка вредоносного трафика

★ Постоянно обновляемые возможности безопасности

1 Аутентификация по отпечатку (слепку)

- Динамический сбор слепков устройств.
- Создание факторов аутентификации на основе полученных слепков.
- Получение уникальной аутентификации по слепку.

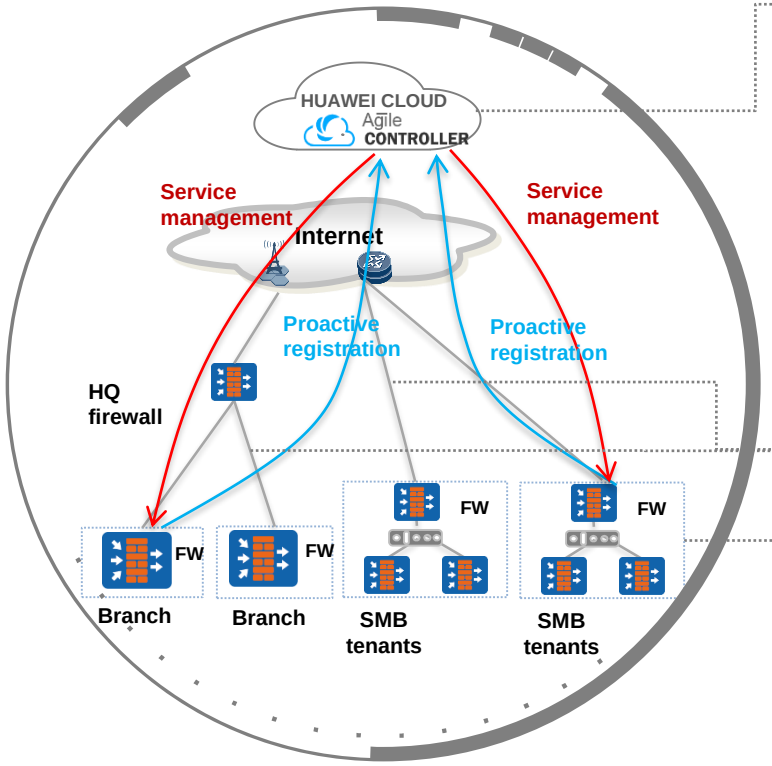
2 Фильтрация слепков на основе трафика

- Dynamically detect security protection service traffic and generate traffic fingerprints
- Access control based on traffic fingerprints

3 Защита на основе уязвимостей протокола

- Continuously focus on camera vulnerabilities to form a vulnerability signature database, and prevent attacks exploiting cameras
- Update the IPS vulnerability database in real time

Все включено: Cloud Management упрощает развертывание устройств и O&M



Доставка политик и unified management

- Удаленное конфигурирование сервисов посредством cloud NMS
- Удаленный мониторинг и траблшутинг устройств
- Cloud-based management и упрощенный O&M для множества устройств
- Автоматическое управление адресацией сайтов филиалов для корректного использования адресного пространства

Шифрование каналов, надежное и безопасное

- Все взаимодействия между cloud NMS и МСЭ надежно зашифрованы
- IPSec туннель между МСЭ филиалов и головным офисом
- Интеллектуальный выбор IPSec соединения между МСЭ филиалов автоматически определяет качество линка и осуществляет переключение туннелей

Plug-and-play и быстрое развертывание

- SMB hosting обеспечивает взаимодействие филиалов крупных корпораций
- Автоматическая регистрация МСЭ и быстрое присоединение его в облачную платформу управления
- Быстрое и непринужденное саморазвертывание устройств

Межсетевые экраны Huawei с искусственным интеллектом

Поднимая безопасность на новые высоты

FW

UTM
IDC Analyze the Future

UTM+
HUAWEI

NGFW
Gartner

NGFW
HUAWEI

AI FW
HUAWEI

NEXT
…

2003	2008	2009	2011	In 2013	2018	2019
Eudemon series firewalls	USG2000/5000 series UTM	USG5500 series UTM+	USG full series application, user, and content control	USG6000 series NGFWs		

Специальное предложение НПК "КОНТАКТ"

Межсетевой экран USG6525E AC Host(2*GE WAN+8*GE Combo+2*10GE SFP+,1 AC power)

~~$ 8000~~

M.2 SSD,SATA 6Gb/s-240GB,Hot-Swappable

Дополнительный БП 60W AC Power Module

399 000руб.

Комплект для установки в стойку

* До 30 октября 2021 года

3 года гарантии, **3-х летние** лицензии:

- SSL VPN Concurrent Users (100 Users)
- IPS Update Service
- URL Filtering Update Service
- Antivirus Update Service

Межсетевой экран USG6525E

Firewall Throughput (1518/512/64-byte, UDP)	2×10GE(SFP+)+8×GE Combo +2GE WAN
Firewall Latency (64-byte, UDP)	18 µs
FW + SA + IPS + Antivirus Throughput	1.5 Gbit/s
Concurrent Sessions (HTTP1.1)	3 000 000
New Sessions/Second (HTTP1.1)	70 000
Maximum IPsec VPN Tunnels (GW to GW)	4 000
IPsec VPN Throughput (AES-256 + SHA256, 1420-byte)	2 Gbit/s
SSL Inspection Throughput	300 Mbit/s
Concurrent SSL VPN Users (Default/Maximum)	100/500
Virtual Firewalls	50
URL Filtering: URLs	A database of over 120 million URLs in the cloud

~~$ 8000~~

399 000руб.

* До 30 октября 2021 года

Спасибо за внимание

Дмитрий Андреев

Ведущий специалист по ПО и безопасности корпоративных сетей

ООО НПК "КОНТАКТ"

a_ada@npk.ru