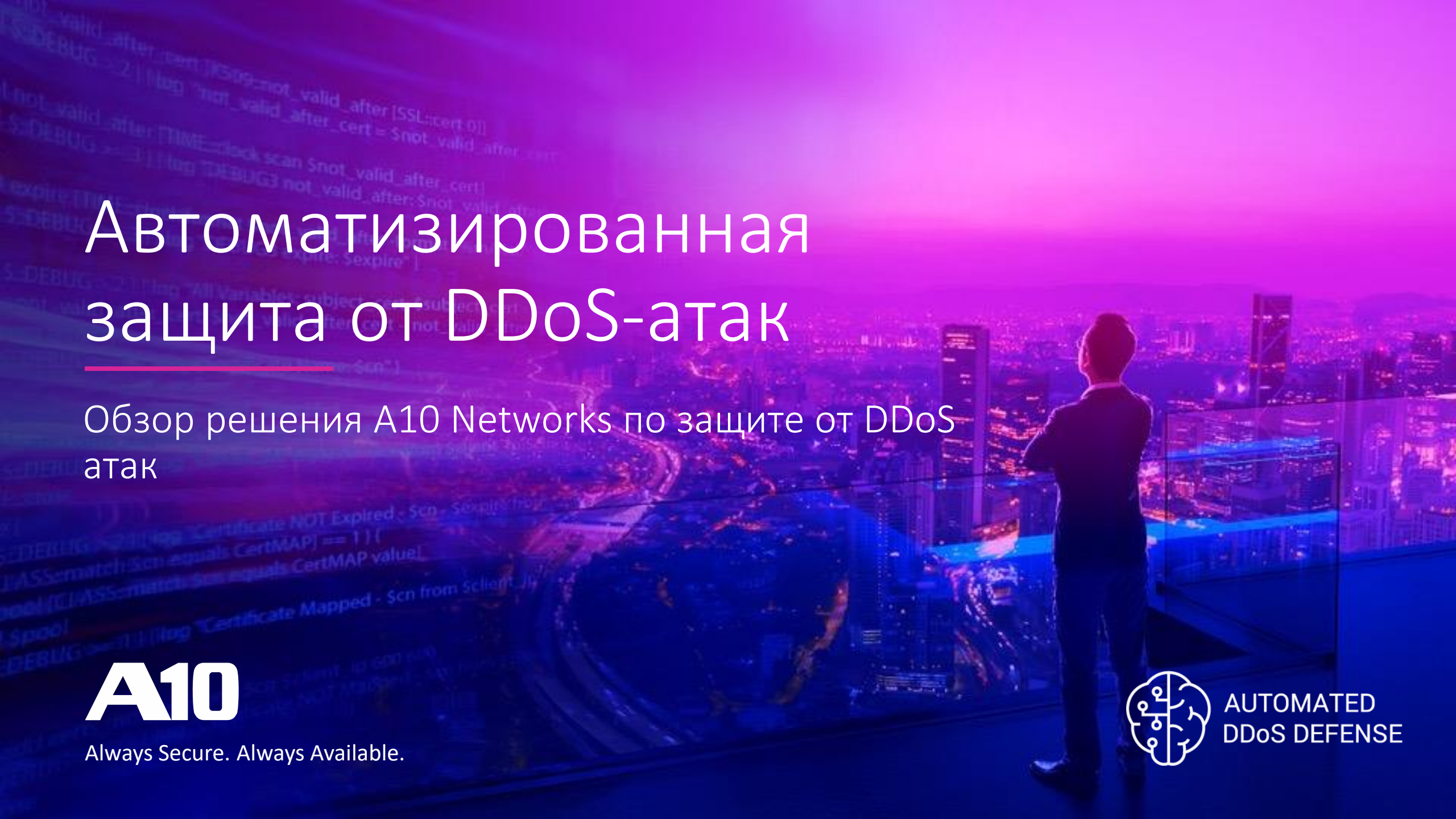


Автоматизированная защита от DDoS-атак

Обзор решения A10 Networks по защите от DDoS атак

A10

Always Secure. Always Available.

AUTOMATED
DDoS DEFENSE

Содержание

Ландшафт угроз DDoS

- Ущерб, причиненный DDoS-атаками
- Мотивация DDoS-атак
- Текущее состояние и будущее DDoS-атак

Современные проблемы

- Проблемы защиты от DDoS-атак для поставщиков услуг
- Недостатки устаревших решений
- Выбор лучшего DDoS-решения

Защита от DDoS атак от A10 Networks

- Преимущество защиты от DDoS-атак A10
- Противодействие
- Определение
- Управление

Кого Мы Защищаем?

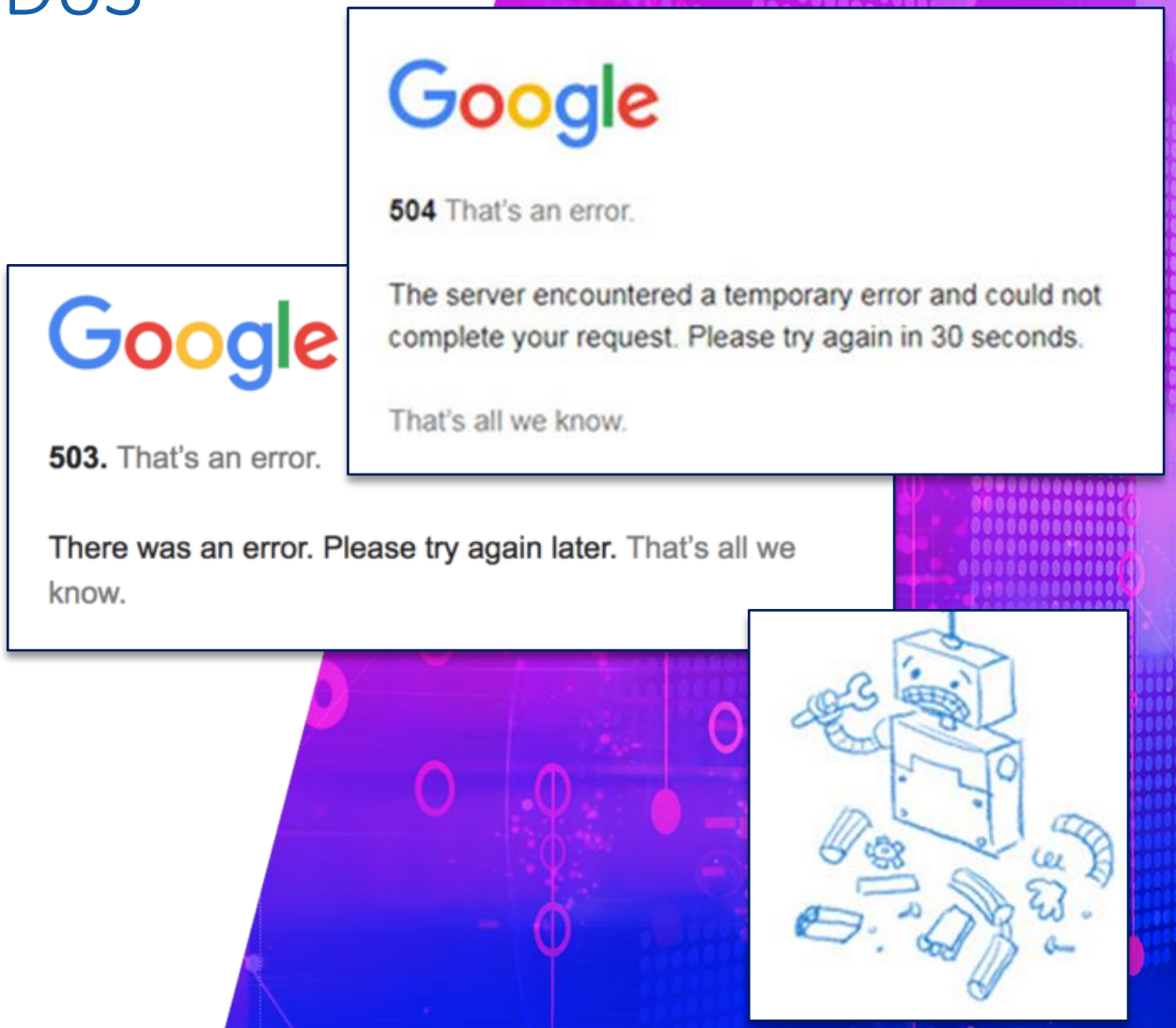
- Отзывы клиентов
- Сертификаты и награды
- Следующие шаги

Ландшафт угроз DDoS

Always Secure. Always Available.

Ущерб, причиненный DDoS-Атаками

- Время простоя и Недоступность услуг
  - Может иметь серьезные последствия в случае критической инфраструктуры и услуг
- Потеря дохода
- Выплаты выкупа
- Потеря репутации и Ущерб бренду
- Прикрытие для инфильтрации и эксфильтрации



Общие Мотивы и Типы атак

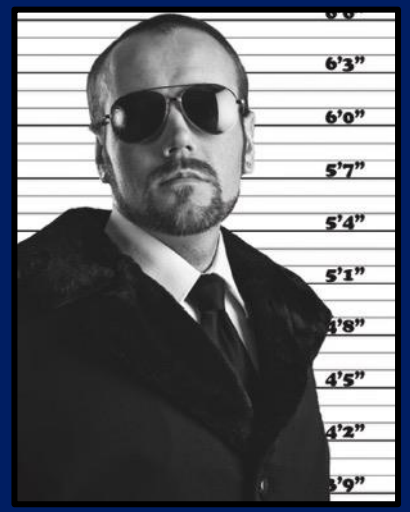
Почему?

- Выкуп и вымогательство
- Атаки для отвлечения внимания
- Кибер-войны и политика
- Хакеры-энтузиасты
- Скука, тщеславие

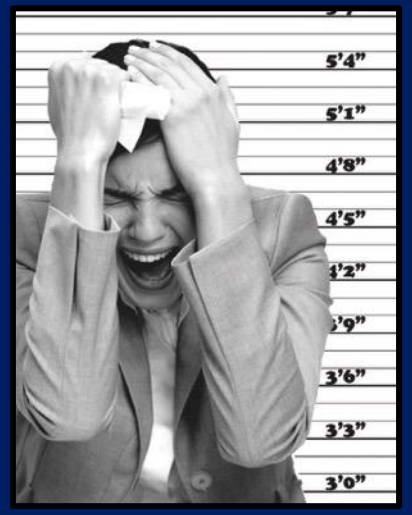
Как?

- DDoS по найму
- Opensource & Freeware
- IoT ботнеты
  - Reflection & amplifications атаки
  - Атаки сетевого уровня
  - Атаки уровня приложений
- Атаки нулевого дня

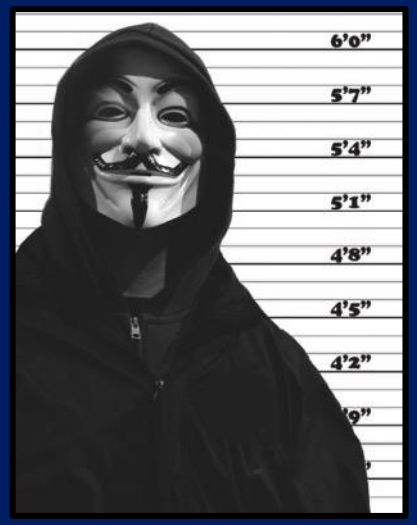
МНОГОЛИКОСТЬ DDOS-АТАКУЮЩИХ



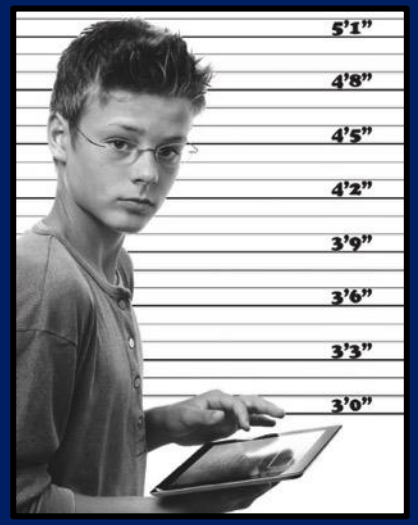
Кибер преступники



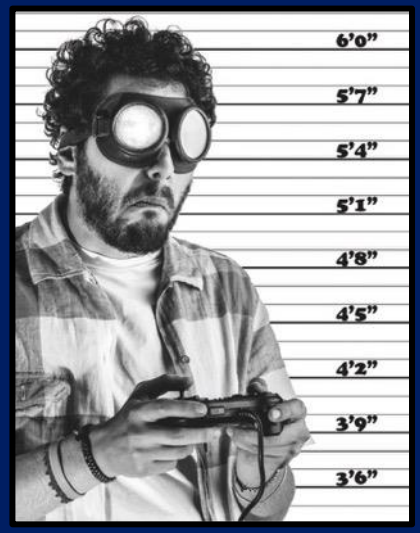
Недовольные сотрудники



Хакеры энтузиасты

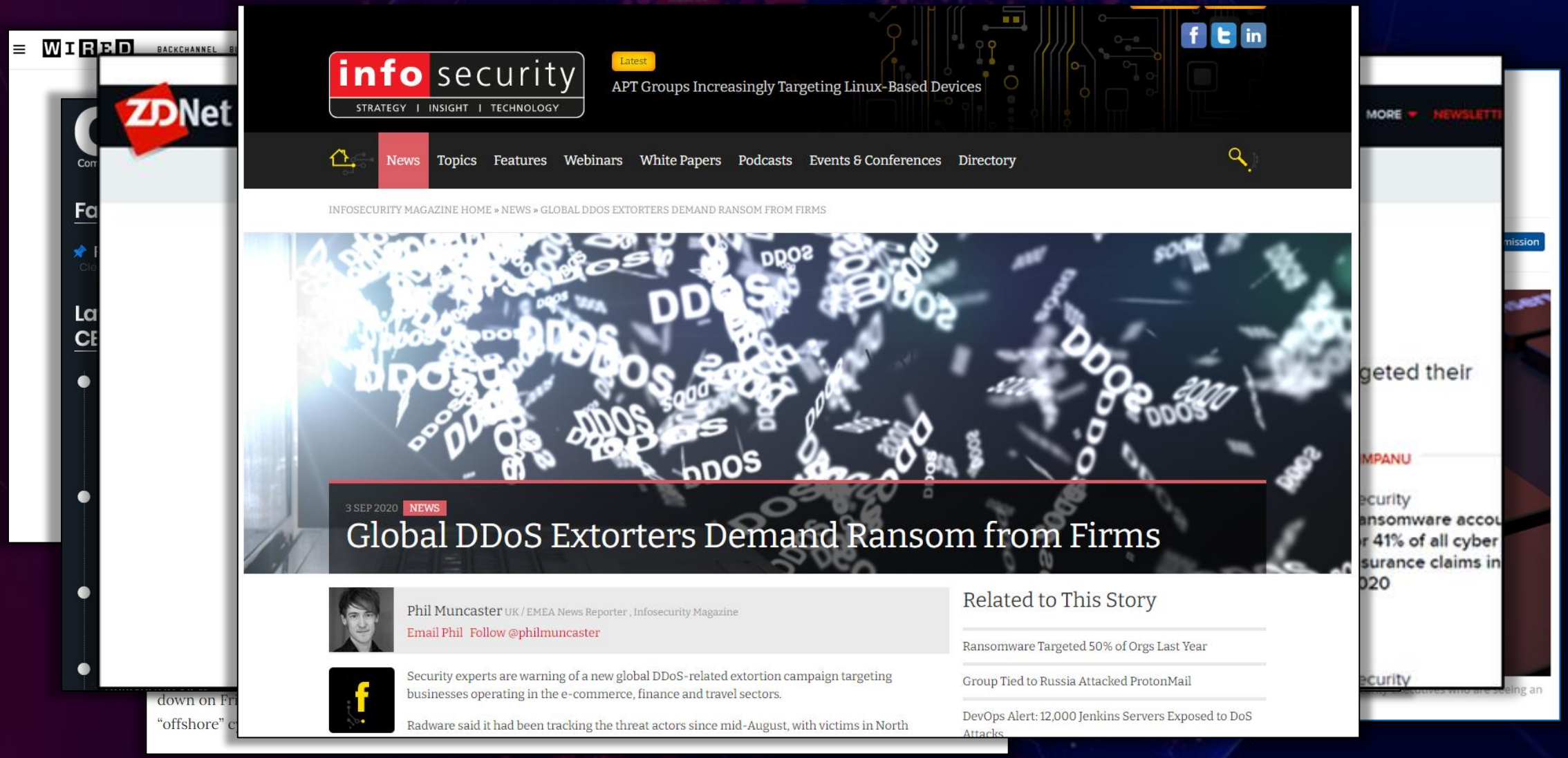


Детские развлечения



Игроки

DDOS-АТАКИ ПРОДОЛЖАЮТ ПОПАДАТЬ В ЗАГОЛОВКИ ГАЗЕТ



Сегодняшние DDoS-Атаки - частые и интенсивные

Малая стоимость

$150 Покупка **1-недельной** DDoS атаки на чёрном рынке

TrendMicro Research

Высокая частота

300% **Рост** количества атак в 2020

Securelist

Высокая интенсивность

4.5x Увеличение **продолжительности** для больших атак

Dark Reading

Ниже радаров

75% Атак < 5Gbps остались незамеченными

Neustar

Цена простоя

Один час простоя стоит больше

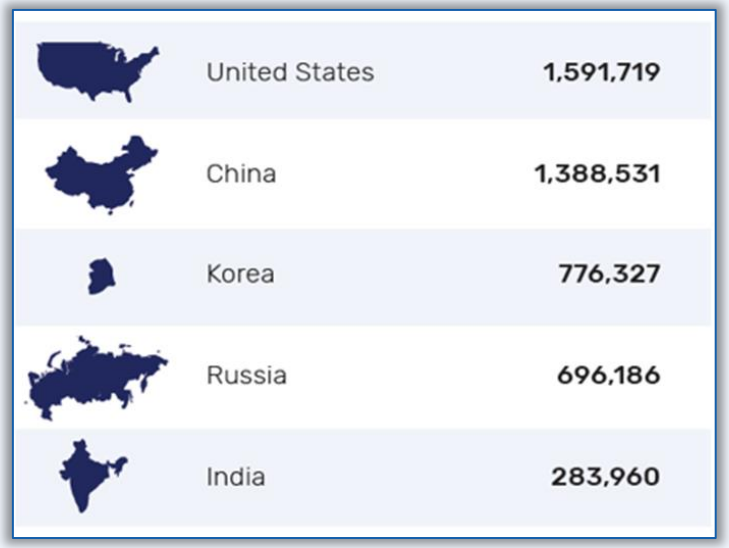
$300K+

ITIC Research

Надвигающаяся Угроза DDoS

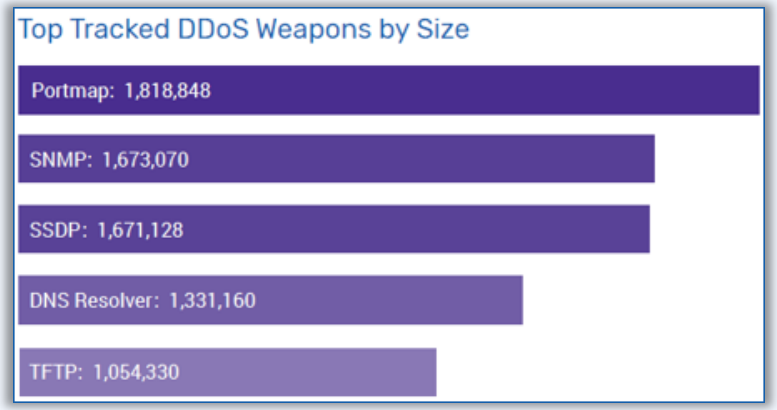
Глобальная проблема

DDoS-оружие доступно по всему миру, причем США, Китай и Корея возглавляют этот список



Массовый Масштаб

Почти 10 миллионов потенциальных DDoS-атак, включая open resolvers, устройства IoT, общедоступные серверы и многое другое



Повышенной Сложности

Работа IoT-устройств в качестве дронов, используемых для сложных многовекторных DDoS-атак

Binary Name	Malware Family
arm7	Gafgyt Family
Cloud.x86	Dark Nexus
mmmmh.x86	Mirai Family
Mozi.m	Gafgyt family
Mozi.a	Gafgyt family

Source: A10 State of DDoS Weapons Report, Q2 2020

DDoS Вещей

Устройства интернета вещей могут быть легко использованы в больших ботнет атаках

- Большие Amplification и распределенные атаки

Mirai – один из ярких примеров

- Сентябрь 2016 – самая большая на тот момент атака (620 Gbps)
- Массированная многовекторная атака (9+ направлений)
- 600,000+ IoT устройств

Количество IoT устройств достигнет 29,3 миллиарда к 2023 году *

UDP Random Flood	Большое количество UDP пакетов в сторону случайных получателей домена-жертвы.
UDP Data Flood	Большое количество UDP пакетов & IP фрагментов в сторону случайных получателей домена-жертвы.
TCP SYN Flood	Большое количество поддельных TCP SYN пакетов в сторону случайных получателей домена-жертвы.
TCP ACK Flood	Большое количество поддельных TCP ACK пакетов в сторону случайных получателей домена-жертвы.
TCP STOMP (Data) Flood	Попытка обхода систем противодействия; соединения в стороны случайных получателей домена-жертвы & пересылка большого количества TCP data.
HTTP Request Flood	Попытка обхода систем противодействия; соединения с случайным HTTP получателем в домене-жертвы & большое количество HTTP запросов.
DNS Water Torture Attack	Большое количество случайных DNS запросов на домен-жертвы к серверам оператора, провоцируя сервер оператора постоянно запрашивать DNS сервер жертвы. В момент перегрузки конечного сервера DNS оператора пересылает на следующий DNS сервер предприятия.
Valve Gaming Server Attack	Большое количество запросов на стриминговые станции сервиса Valve с использованием поддельных запросов.
GRE IP/Ethernet Floods	Большое количество запросов на случайных получателей домена-жертвы с поддельными GRE IP или IP-over-Ethernet-tunneled UDP пакетов.

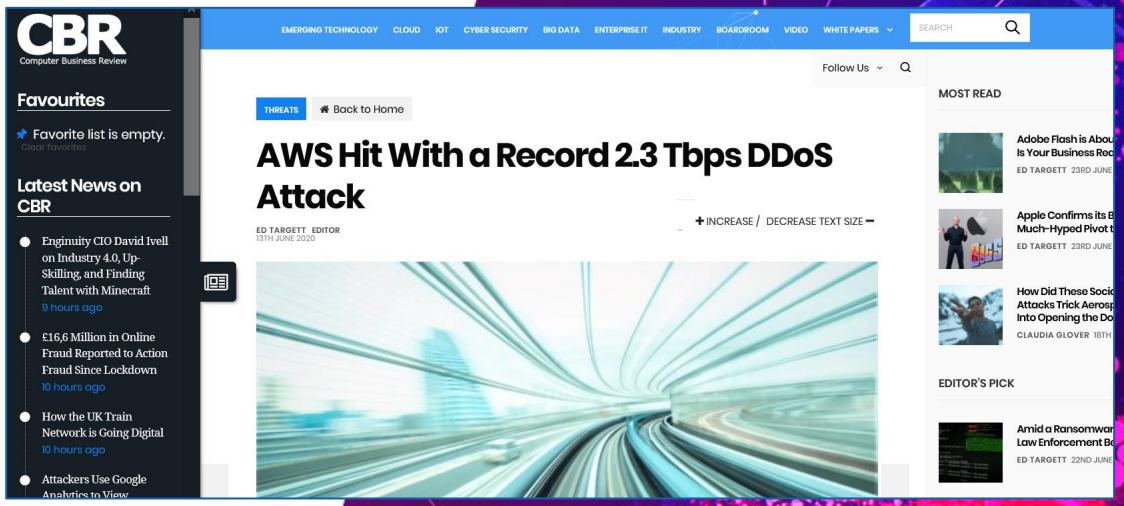
Table Source: Investigating Mirai (A10 Networks White Paper, 2016)
*Cisco Annual Internet Report (2018–2023) White Paper

Каков результат? DDoS-Атаки становятся всё больше

Новая большая атака – AWS: 2.3 Tbps

- Февраль 2020 – длилась 3 дня
- Одновекторная атака – CLDAP
- Очевидная необходимость внедрения защит с правилом «нулевого доверия»

  Атаки на базе усиления и отражения запросов становятся стандартом для больших атак
- Возможность усиления атаки CLDAP, DNS и NTP делает их идеальным оружием
- Даже небольшие разрозненные атаки могут быть использованы в массовых
- Атаки в основном базируются на UDP



DDoS Weapon	Number of Weapons	Weapons Frequency (in comparison to CLDAP)
Portmap	1,818,848	116x
SNMP	1,673,070	107x
SSDP	1,671,128	107x
DNS Resolvers	1,331,160	85x
TFTP	1,054,330	67x
CLDAP	15,651	-

Table Source: https://www.a10networks.com/blog/aws-hit-by-largest-reported-ddos-attack-of-2-3-tbps/

DDoS-Атаки Будут Расти Вместе С 5G

5G предоставляет беспрецедентный охват и масштабируемость

- Мощные устройства IoT в массовом количестве будут основой разрушительных атак

Mobile Broad Band (eMBB)

Высокоскоростной интернет

Fixed Wireless

Сверх малые задержки (URLLC)

Дополненная Реальность

Виртуальная реальность

Дистанционные операции

Управляемые автомобили

Массовый IoT (mMTC)

Умные дома

Умные города

Photo Source: *MWC 2019 - GSMA*

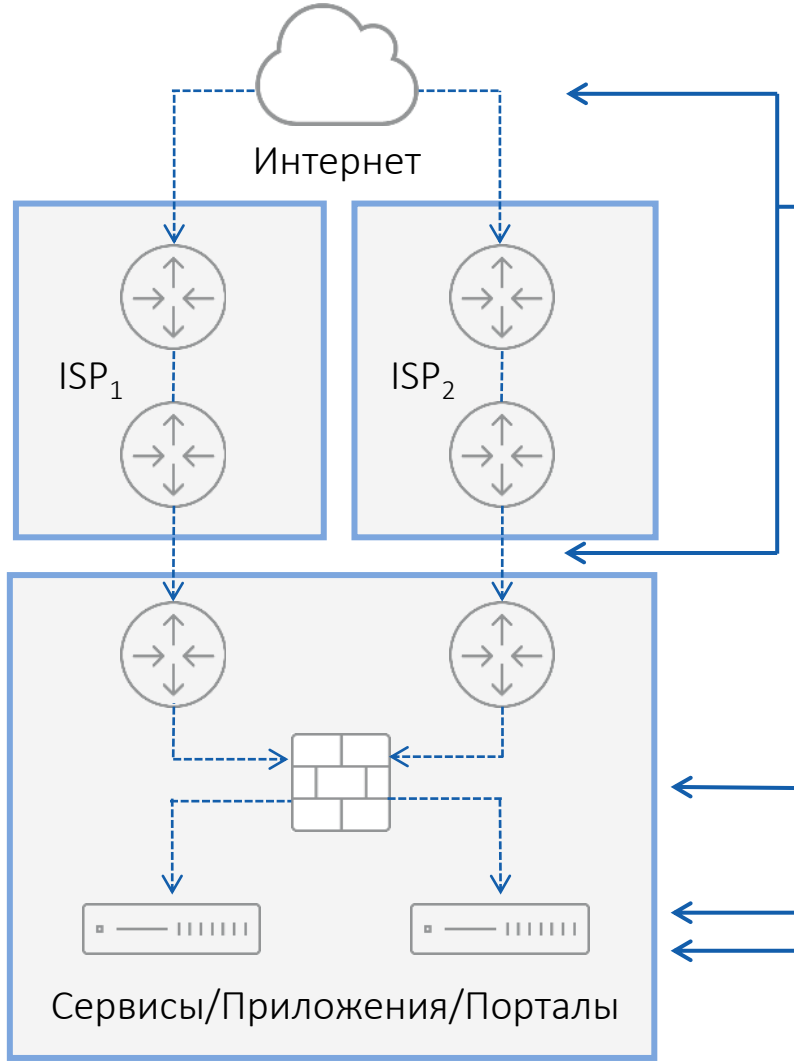
Проблемы защиты от DDoS операторов связи

Always Secure. Always Available.

Проблемы DDoS провайдера услуг

- Большие и сложные сети
- Становятся первой целью для массированных атак
- Основная цель состоит в том, чтобы защитить большое количество нижестоящих клиентов
- Требуются высокопроизводительные и масштабируемые решения защиты от DDoS-атак, соответствующие колоссальным объемам современных атак
  - Обычно развертывается в реактивном режиме

Стратегии и цели многовекторных атак



Инфраструктура оператора связи

Локально на территории бизнес клиентов

Объёмные

- DNS amplification
- NTP amplification
- UDP Flood

Сетевой уровень

- Fragmentation
- SYN floods
- SSL renegotiation

Уровень приложения

- Slowloris
- HTTP floods
- DNS NXDOMAIN attack

Техники защиты

Операторы связи

- Реактивный режим с использованием xFlow телеметрии
- Большое количество объемных атак с высоким PPS

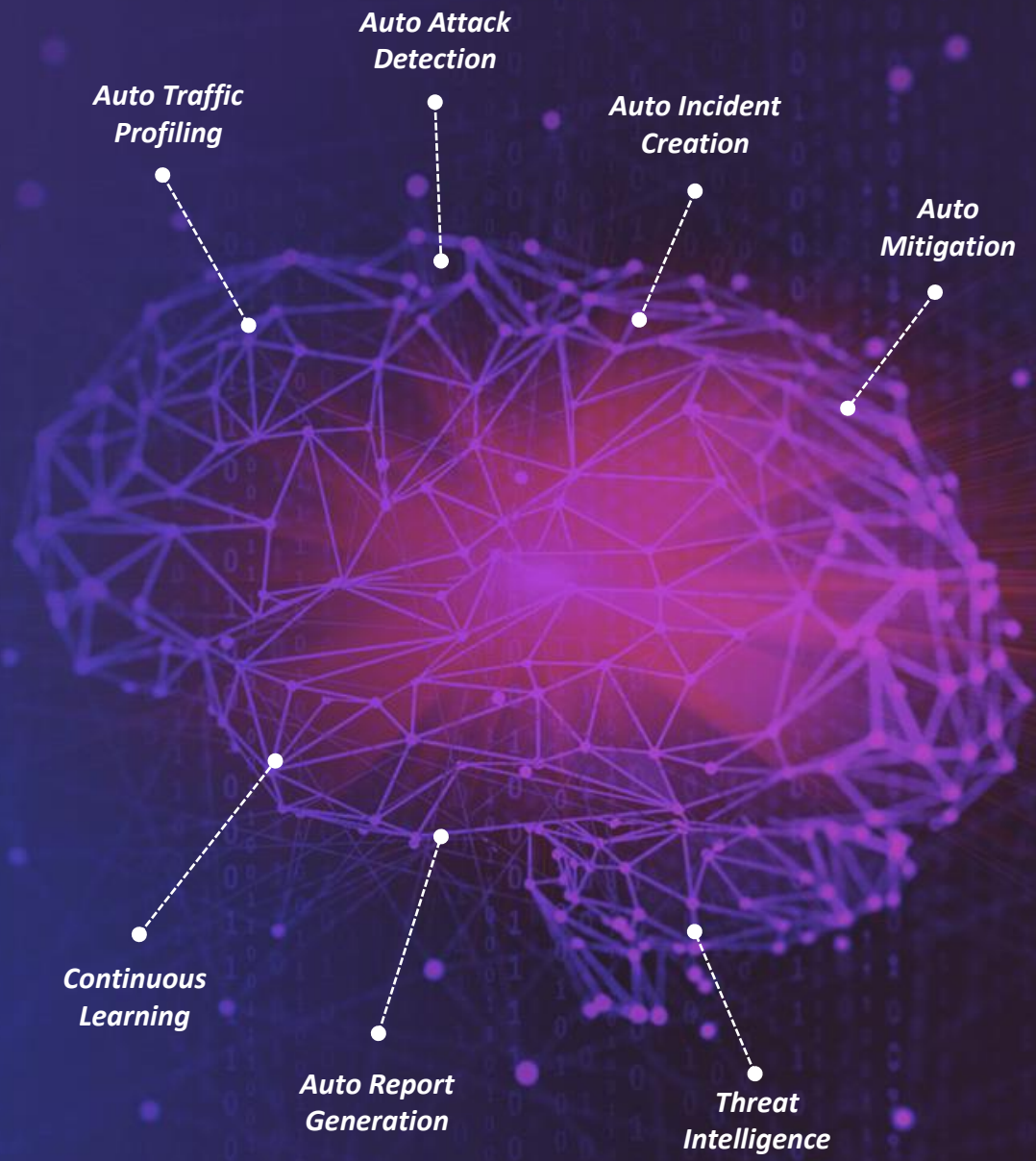
Предприятия

- Инлайн решения с инспекцией всех пакетов
- Объёмные атаки, сетевой уровень & уровень приложения

Проблемы связанные с устаревшими решениями

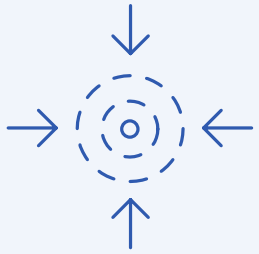
- Атаки остаются невидимы для определения
- Сложные ручные операции
- Медленная реакция на атаки
- Масштабируемость модулей противодействия
- Отсутствие механизмов по защите от атак «нулевого дня»
- Нехватка обученных специалистов
- Стоимость защиты от DDoS

Современная Защита От DDoS
Требует
Интеллектуальная
Автоматизация
& Машинное обучение



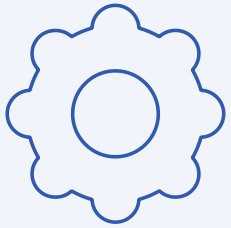
Выбор Лучшей Защиты От DDoS

Что делает решение защиты от DDoS лучше других?



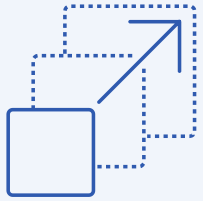
Эффективность

Устранение дорогостоящих ошибок по определению и противодействию



Автоматизация

Уменьшение проблемы специалистов до минимума



Масштабируемость

Оптимизация краткосрочных и защита долгосрочных инвестиций

Доступность цены

Производительность заложенная в дизайне позволяет снизить стоимость

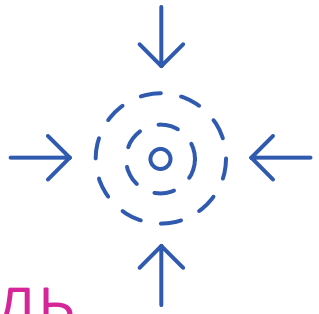
Защита от DDoS атак
A10 Networks

AUTOMATED
DDoS DEFENSE

Always Secure. Always Available.

Преимущества защиты от DDoS A10

Эффективность



Исключение ложных срабатываний

Негативная модель

Более 30+ отслеживаемых индикаторов трафика для снижения дорогостоящих ошибок

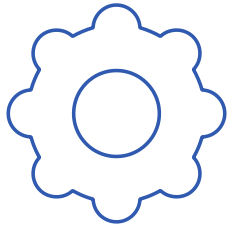
Исключение ложных срабатываний

Позитивная модель

Единственная в отрасли прогрессивная 5-уровневная эскалация снижающая риск и последствия для пользователей

A10 AUTOMATED DDoS DEFENSE

Автоматизация



Единственные в индустрии

5 уровней эскалации

Автоматизация рутинных операций

Снижение ручных операция для уменьшения времени реакции

Атаки нулевого дня

Предотвращение атак

Динамические шаблоны атак, распознавание в реальном времени

Единственные в индустрии

Действенная

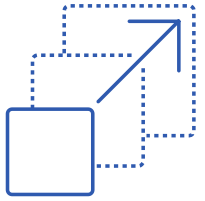
Платформа защиты от DDoS

96 миллионов записей в чёрном списке

Блокирование многократно используемых ресурсов (открытые сервера, ботнеты)

Преимущество защиты от DDoS-атак A10

Масштабируемость



22X Определение атак на базе Flow-телеметрии

Самое производительное решение по определению - **6 миллионов fps** в одном устройстве

12X Отслеживаемых политик

Обучение и отслеживание до **128K** индивидуальных профилей

15X Одновременных Активных политик защиты

До **3K** защищаемых зон

A10 AUTOMATED DDoS DEFENSE

Ценовая доступность

Самое быстрое

Производительность

1.2 Tbps скорость аппаратного блокирования,
380 Gbps пропускной полосы & **500 MPPS**,
в 1RU устройстве – Thunder 7655 TPS

Простота

Интеграция

BGP, ISIS, OSPF поддержка маршрутизации

23X Эффективные вложения

Наращивание до тысяч **независимых контекстов** с изоляцией сервисов для клиентов

Обзор защиты от DDoS-атак A10

AUTOMATED DDoS DEFENSE

- **Интеллектуальная автоматизация** для быстрого реагирования (управление, определение и очистка)
- **Гибкое масштабирование** с возможностью модели подписки и работы в режиме кластера
- **Гибкость развёртывания** – варианты виртуальных и аппаратных платформ
- **Полнофункциональный, открытый API** для интеграции

Очистка

- Самое быстрая и точная очистка в отрасли
- Интеллектуальная автоматизация и работа с политиками очистки
- Фильтрация шаблонов атак на базе ML и защита от атак нулевого дня

Определение

- Адаптивное профилирование трафика для автоматического обнаружения атак и анализа аномалий
- Лучшая в отрасли точность и производительность обнаружения на базе flow телеметрии

Управление & интеграция

- Централизованная консоль работы с инцидентами и отчётами
- Автоматическое определение и автоматизация очистки
- Интеграция с Детекторами других производителей

Высокопроизводительная очистка

Первая в индустрии очистка на базе ML

- Точная очистка с защитой от атак нулевого дня A10 (ZAP)

Самая высокопроизводительная в отрасли автоматизированная защита от DDoS-атак

- Самая производительная аппаратная платформа в индустрии (до 3x раз по сравнению с конкурентами)
- Самая производительная виртуальная платформа в индустрии (до 5x раз по сравнению с конкурентами)

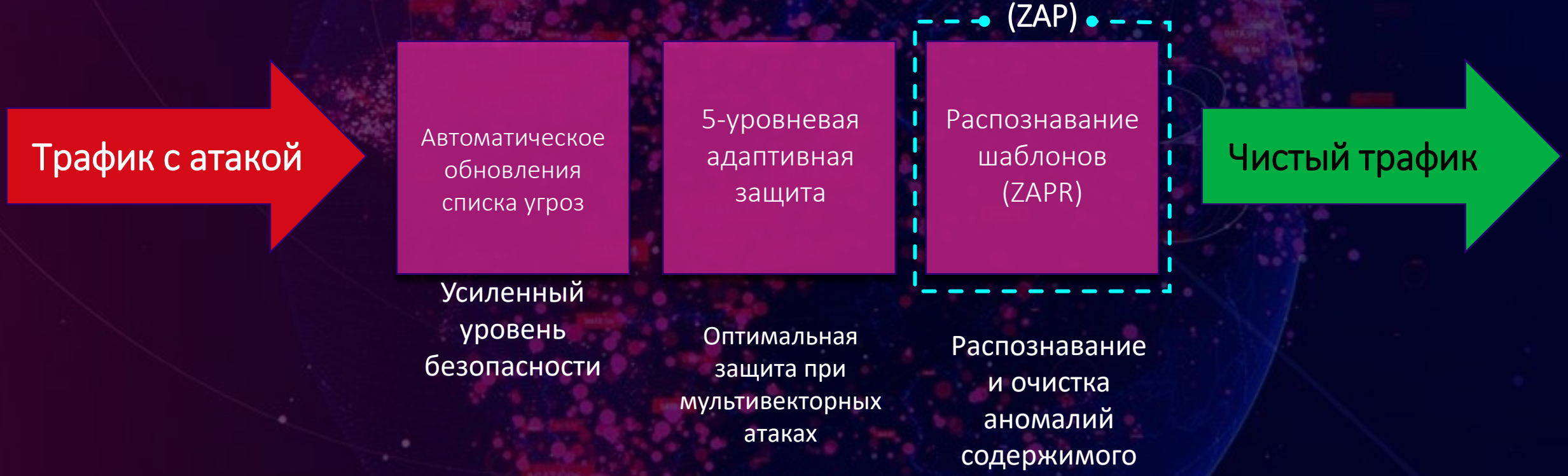
Масштабирование и развёртывание

- До 1.2 Tbps на базе виртуальных или аппаратных решений от A10
- Проактивные и реактивные схемы развёртывания

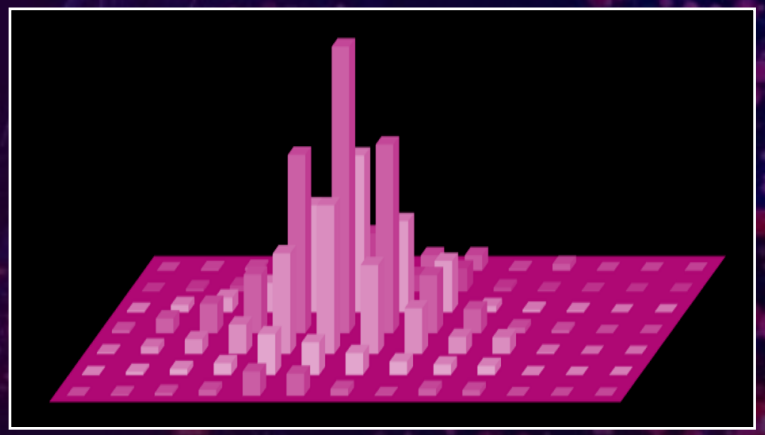
Очистка

ЗАЩИТА С МУЛЬТИ МОДУЛЬНОЙ ОЧИСТКОЙ

Автоматизированная защита от атак нулевого дня



Распознавание шаблонов атак нулевого дня A10 (ZAPR)



Модуль определения на базе машинного обучения

Пакетная фильтрация

Вредоносный запрос

Шаблон содержимого

Рефлектор

Шаблон содержимого

DDoS Бот

Легитимный пользователь

Защищаемый сервис

Обычный трафик

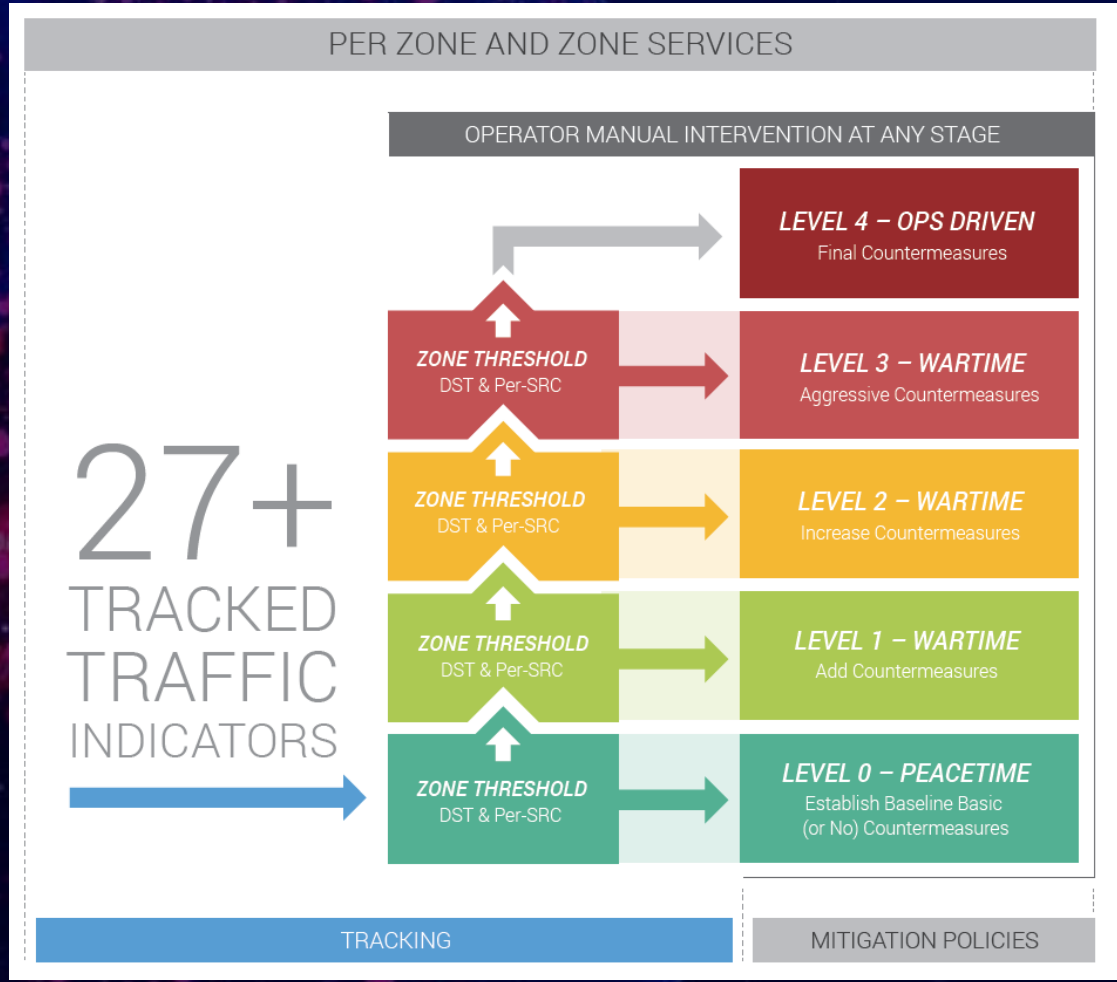
Thunder TPS

Модуль машинного обучения

Противодействие в реальном времени

АВТОМАТИЗАЦИЯ ДЛЯ ОТРАЖЕНИЯ АТАК

- Полностью автоматизированный и рабочий на протяжении всего жизненного цикла атаки
- Автоматическое и всестороннее профилирование трафика
- Автоматическое обнаружение атак
- Автоматическое создание инцидентов и отражение атак
- Автоматическая эскалация/деэскалация политик защиты в каждой зоне безопасности
- Автоматическое прекращение инцидентов и генерация отчетов



Policy based automatic mitigation escalation per Zone

ВЗАИМОДЕЙСТВИЕ С DDOS THREAT INTELLIGENCE

Сервис A10 Threat Intelligence Service проактивно блокирует DDoS атаки используя список угроз

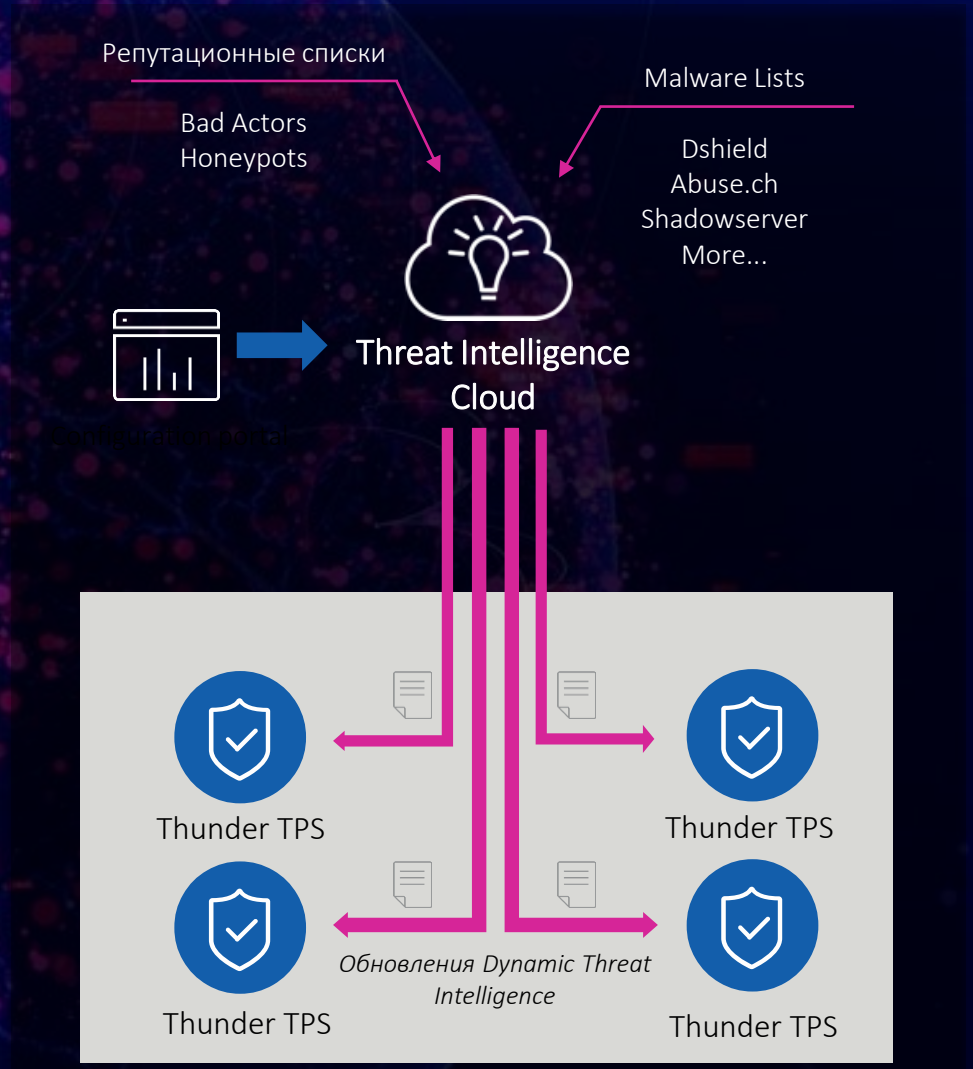
- Списки известных IP-адресов злоумышленников

Расширяет защиту против ботнетов,, **C&C соединений, атак на отражение, и т.д.**

- Повышение эффективности и результативности
- DDoS threat intelligence без зависимости от масштаба
- Блокирование трафика помимо DDoS (например SPAM)

Включено в **A10's DSIRT**
(DDoS Security Incident Response Team)
поддержку

Powered by
A10 Security
Research
+
Threat
STOP



ЛИДИРУЮЩЕЕ РЕШЕНИЕ ПО ЗАЩИТЕ ОТ DDoS

По сравнению с альтернативными решениями

3x Больше производительности

3x Плотность

3x Пропускной полосы

1.2 Tbps
Противодействие

500 MPPS
Пакетная производительность

256 Million
Одновременных сессий

Thunder 7655 TPS
1.5 RU

Высокоточное определение DDoS

- Быстрое обнаружение на базе поведенческой модели
  - Более 30+ отслеживаемых индикаторов позволяют с высокой достоверностью определять атаки
- Возможность установки границ для каждого защищаемого сервиса
  - Автоматическое построение поведенческого профиля трафика
  - Установка границ срабатывания, анализ и определение аномалий
- Мониторинг пороговых значений для протоколов в дополнение к индикаторам пакетов или бит

Детектирование

Универсальный инструмент для обнаружения DDoS

Мониторинг двунаправленного трафика в реактивном и проактивном режиме

- Проактивный режим:
  - Развёртывание в режиме инлайн для защиты DNS/SIP/Website/Gaming
- Реактивный режим:
  - Развёртывание для защиты инфраструктуры; получает телеметрию xFlow с пограничных маршрутизаторов

Высокая скорость, высокая точность, обнаружение на базе flow телеметрии

- Время обнаружения 3 секунды
- Использование sFlow и NetFlow

Варианты использования

- Независимый программный или аппаратный детектор
- Детектор на базе виртуального aGalaxy
- Встроенный детектор в систему очистки

Интеграция с сторонними производителями

FlowTraq

kentik

genieNetworks

Flowmon Networks

Беспроблемная интеграция с Thunder TPS Mitigator

- Для использования в реактивном режиме
- Дополнительные функции, не только определение DDoS

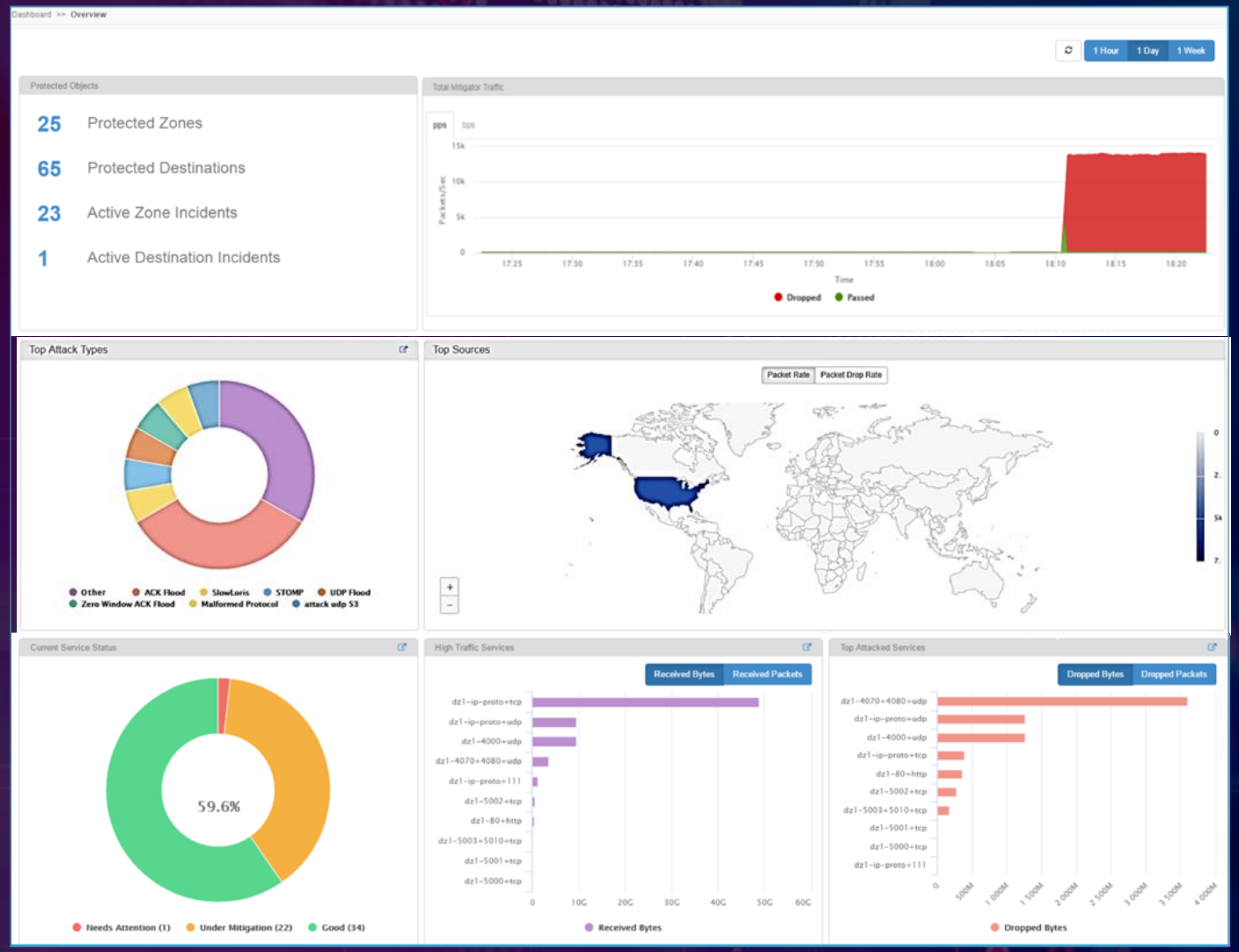
Комплексное Управление

- Централизованный инструмент для управления и отчётности
  - Управление защищенными объектами и инцидентами в одном пользовательском интерфейсе системы
  - Полная поддержка RESTful API для интеграции SecOps
- Интуитивно понятный интерфейс настройки со встроенными шаблонами политик
  - Автоматическая конфигурация на основе инцидентов для противодействия и детекторов
- Автоматизированная генерация отчетов освобождает от ручных процессов
  - Комплексные отчеты с защищенными объектами и сервисами, а также подробности инцидентов DDoS

Управление & Взаимодействие

АВТОМАТИЗАЦИЯ ОРИЕНТИРОВАННАЯ НА ЗАЩИТУ

- Современный дизайн пользовательского интерфейса с панелью управления
- Интеллектуальное взаимодействие всех компонент решения
- Оптимизированные рабочие процессы для ускорения выполнения задач операторов
- Автоматическое применение мер по противодействию, вызванное предупреждениями об обнаружении



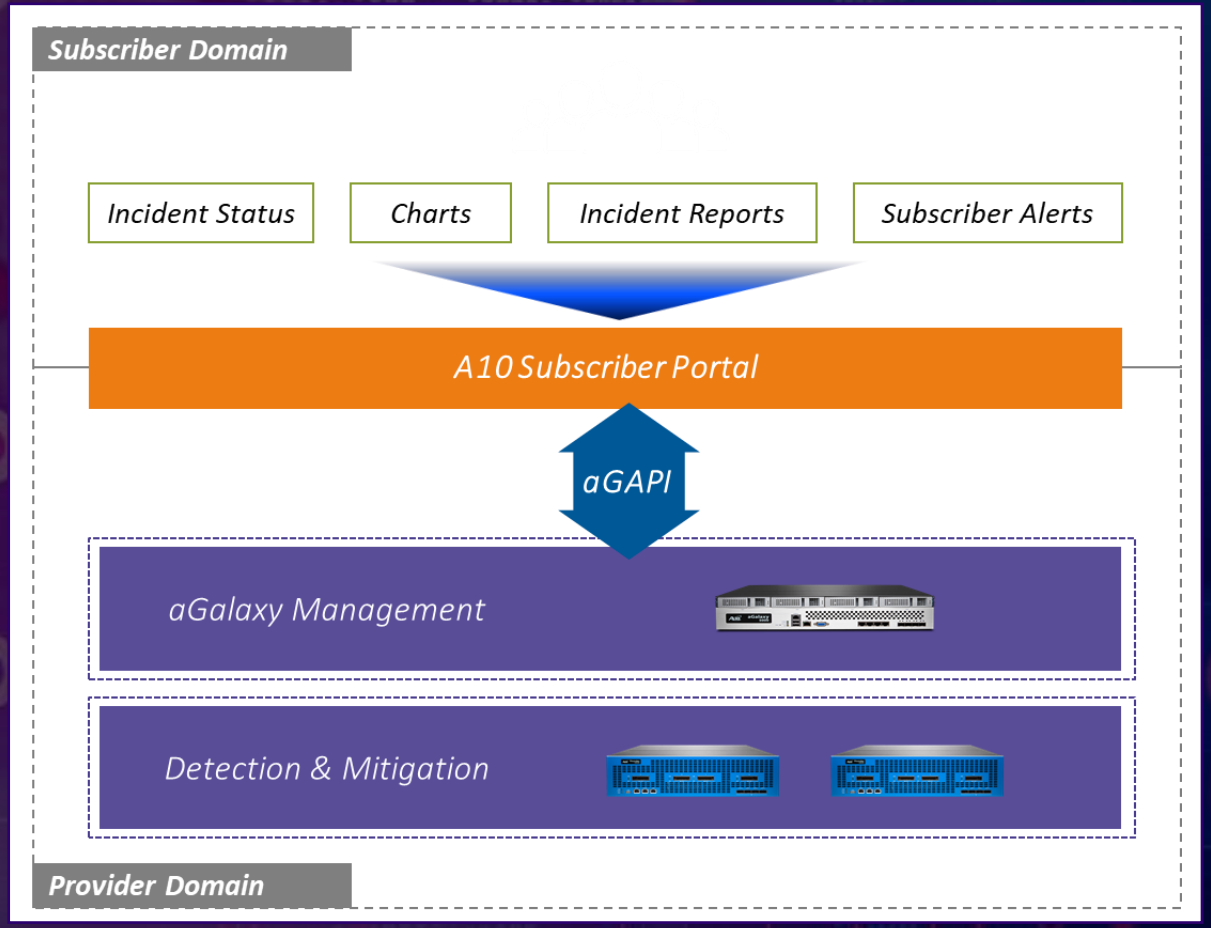
MSSP развёртывание и портал пользователя

Готовый пользовательский портал для защиты от DDoS-атак-MSSP (как услуга)

Обеспечивает упрощенный пользовательский интерфейс и дополнительную безопасность

- Административный портал для интеграции aGalaxy
- Поддерживает несколько подключений aGalaxy, обеспечивая консолидированную отчётность для подписчиков
- Просмотр инцидентов для каждого из арендаторов подсистемы

Индивидуальные отчёты и формы для операторов и клиентов



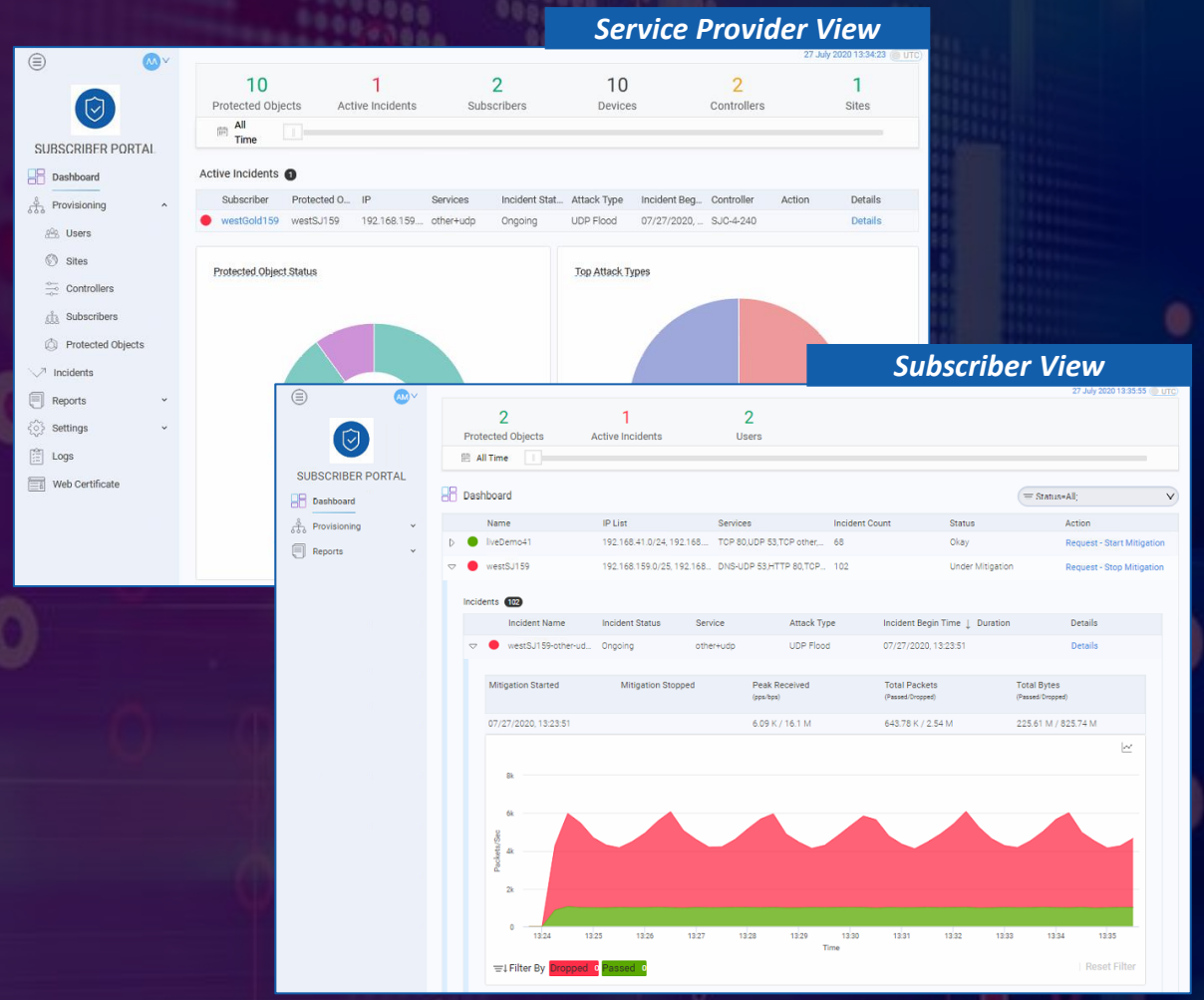
MSSP развёртывание и портал пользователя

Готовый пользовательский портал для защиты от DDoS-атак-MSSP (как услуга)

Обеспечивает упрощенный пользовательский интерфейс и дополнительную безопасность

- Административный портал для интеграции aGalaxy
- Поддерживает несколько подключений aGalaxy, обеспечивая консолидированную отчётность для подписчиков
- Просмотр инцидентов для каждого из арендаторов подсистемы

Индивидуальные отчёты и формы для операторов и клиентов



Программные и аппаратные платформы A10

Thunder TPS: от 1 Gbps до 1.2 Tbps

Малый сегмент / CPE

Thunder 3040
10 Gbps очистки

Thunder 1040
5 Gbps очистки
HW bypass option

vThunder TPS
От 1 до 5 Gbps очистки

Средний сегмент

Thunder 5845
250 Gbps блокирования, 100 Gbps очистки
100 GbE порты

Thunder 4435
38 Gbps очистки

vThunder TPS
10-100 Gbps KVM SR-IOV

Высший сегмент

Thunder 7655
1.2 Tbps блокирования, 380 Gbps очистки
100 GbE порты

Thunder 14045
500 Gbps блокирования, 300 Gbps очистки
100 GbE порты

Thunder 7445
500 Gbps блокирования, 220 Gbps очистки
100 GbE порты

Определение*

vThunder TPS
Detector

Управление

aGalaxy 5000

aGalaxy-VM

Subscriber Portal
(VM)

Высокопроизводительный процессор
Security & Policy Engine (SPE)
с Flexible Traffic Accelerator (FTA)

**aGalaxy также имеет функции программного детектора, плюс - каждый модуль очистки может быть сконфигурирован в качестве детектора*

Поддержка A10’s мирового уровня

DDoS SIRT (DSIRT) & Threat Intel

- Круглосуточная помощь : 24x7x365

Помощь во время атаки:

- DDoS Security Incident Response Team

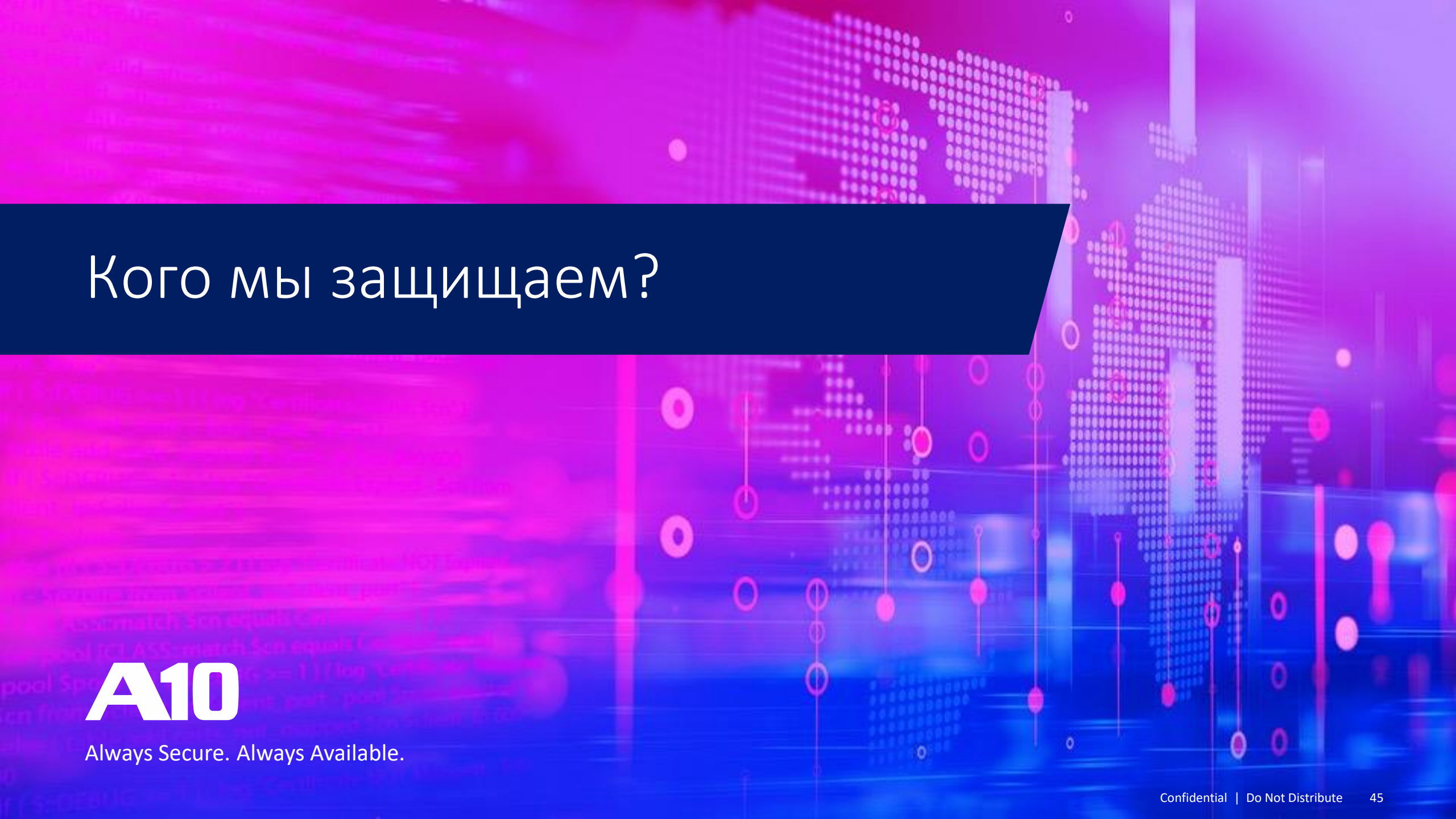
Профилактика:

- Включает в себя Threat Intelligence Service

Ежеквартальная DDoS-отчётность

- Ежеквартальный отчет A10 Networks Security Research
  - Доступно по адресу https://www.a10networks.com/marketing-comms/reports/state-ddos-weapons/
- Изучение методов DDoS атак для разработки методов противодействия
- Изучение роли эксплойтов для борьбы с ботнетами IoT

Кого мы защищаем?



A10

Always Secure. Always Available.

A10 защищает высоконагруженные сети по всему миру

... И много других

A10 защищаетсамые большие игровые порталы

BLIZZARD ENTERTAINMENT

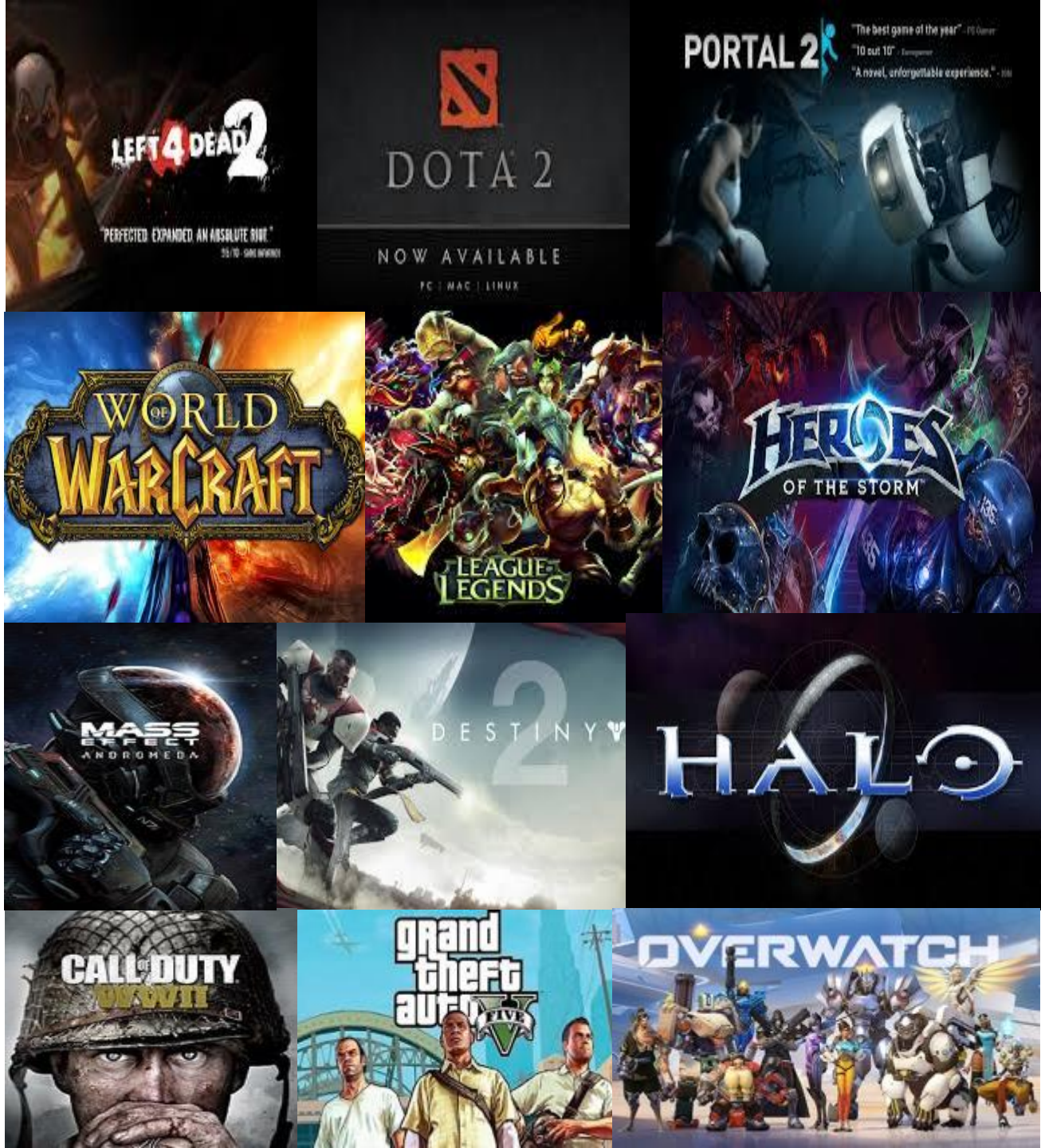
T2 TAKE-TWO INTERACTIVE

RIOT GAMES

SEGA

XBOX

BUNGIE



Что говорят клиенты о решениях A10

IT Central Station
Unbiased reviews from the tech community

Производительность против устаревших решений

"Based on previous equipment that we had, it's amazing that this device can do what it can do in a 1U form factor. The devices that we have right now have never gone over capacity and we've actually mitigated some pretty large attacks with these devices."

Security Operations Manager at a Large Media Company

ROI против облачных решений

"If we had a bad month of attacks, or even one bad day where somebody attacked us for 20 or 24 hours straight, we could be looking at spending $30,000 or $40,000 with that cloud provider. Today, it's nothing. There's no expense."

Director of IT at a Large Service Provider

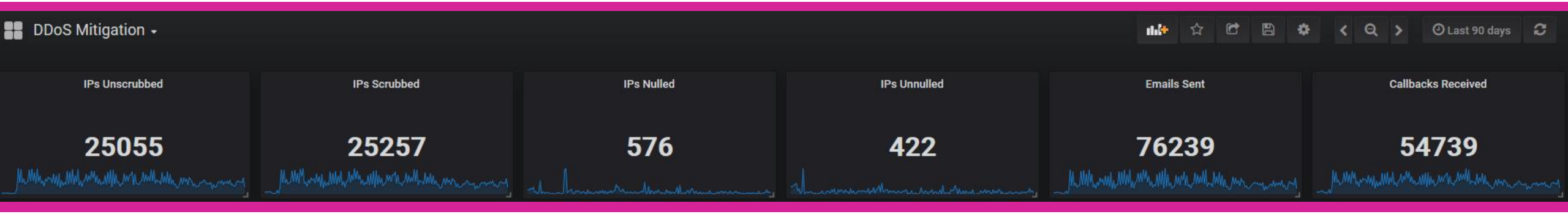
Надежность против устаревших решений

"The solution has been rock solid for us. We haven't had any issues. We've had numerous attacks and it's worked perfectly."

Network Engineer at Large Service Provider

Сервис очистки облачного веб провайдера

Результаты (90 после развёртывания)



- 97,77% всех атак были отражены платформами очистки
- Увеличение NPS (Net Promoter Score)
- Снижение нагрузки на сервисный центр ~11%

“Возможность автоматизации и масштабирования решения для предоставления услуг может оказать существенное влияние на качество и экономику услуг по очистке от DDoS-атак. Инновации A10-это значительные преимущество”

Bart van der Sloot, Managing Director of Leaseweb Network

“A10 Networks предлагает передовые автоматизированные решения по обнаружению и противодействию DDoS-атакам, с возможностью масштабирования.”

Christopher Rodriguez, Research Manager, Cybersecurity Products
New Approaches to DDoS Protection Offer Better Security and Economic Scale, June 2019

IDC
Analyze the Future

Защита от DDoS от A10 – тесты и оценки

CERTIFIED EFFECTIVE
All attacks detected and mitigated with no manual intervention

CERTIFIED PERFORMANCE
Passed all mitigation tests under high load

EAL2+ Certified
Meets International security standards

Награды

Итоги

A10

Always Secure. Always Available.

AUTOMATED
DDoS DEFENSE

Модернизируйте свою защиту с помощью A10

Улучшенная безопасность

Доступная, интеллектуальная защита от нулевого дня

Умная защита

Современная автоматизация и машинное обучение

Масштабируемость

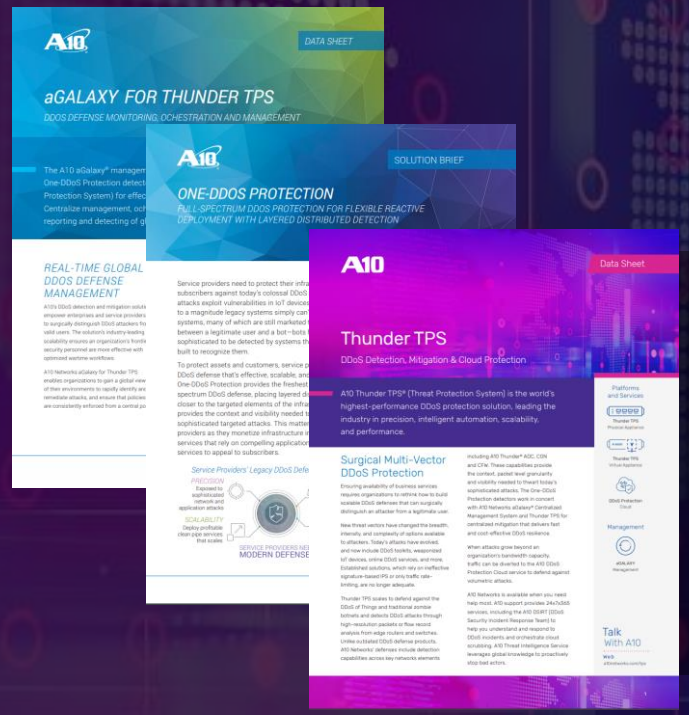
Противодействие ботнетам и многовекторным DDoS атакам

Следующие шаги на пути к защите от DDoS

AUTOMATED DDoS DEFENSE

- Расчёт необходимой производительности
- Мониторинг и построение границ трафика
- Развёртывание подсистемы защиты от DDoS
- Подготовка внутренних и внешних процедур

Прочитайте отчёт о DDoS атаках для того, чтобы знать больше о современном окружении и угрозах



Запросите образ для тестирования

Изучите материалы и обзоры решений TPS


Thank You
A10
Always Secure. Always Available.