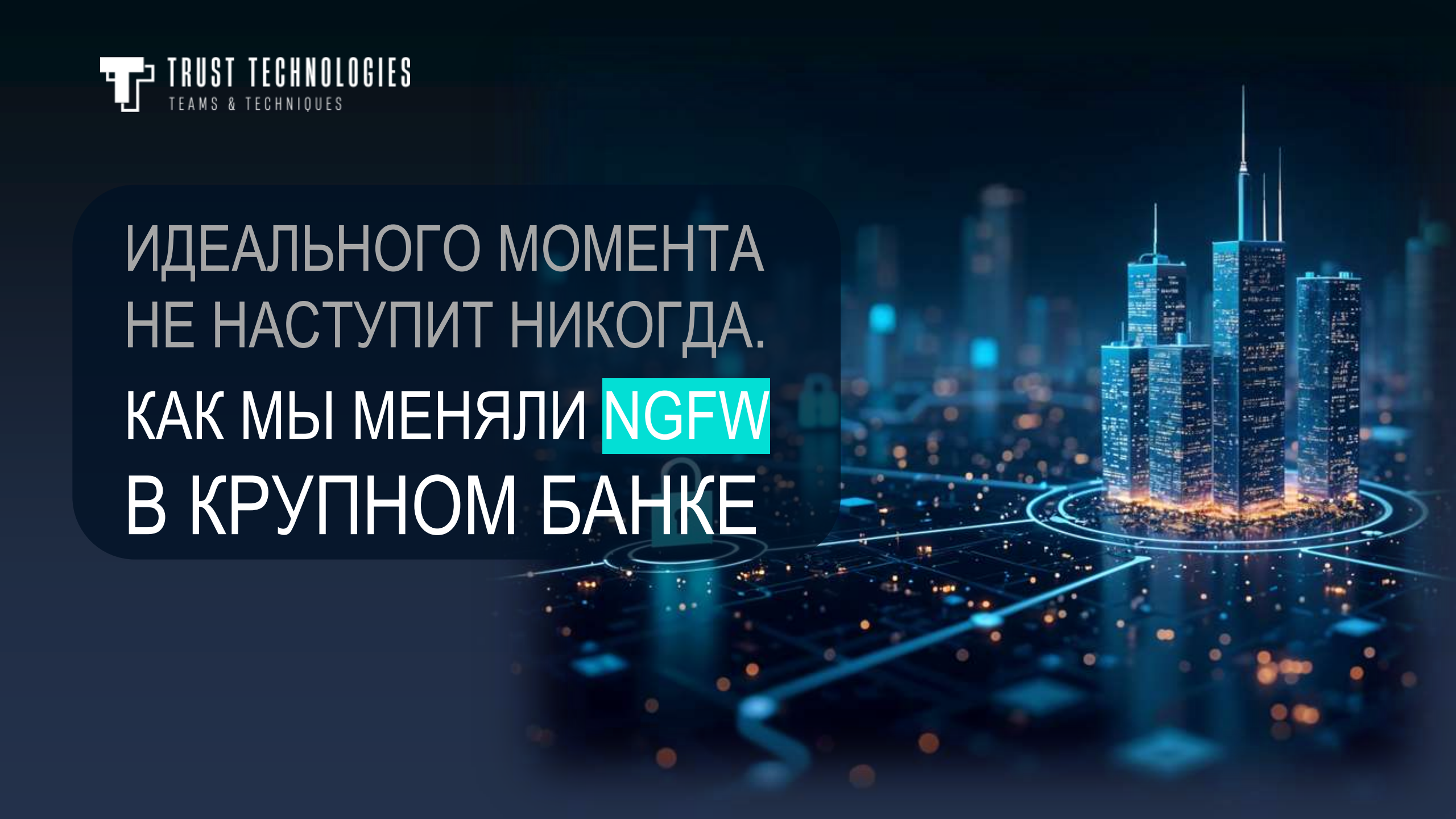
TRUST TECHNOLOGIES
TEAMS & TECHNIQUES

ИДЕАЛЬНОГО МОМЕНТА НЕ НАСТУПИТ НИКОГДА. КАК МЫ МЕНЯЛИ NGFW В КРУПНОМ БАНКЕ



TRUST TECHNOLOGIES
TEAMS & TECHNIQUES

TRUST TECHNOLOGIES – ИНТЕГРАТОР ЦИФРОВОЙ ИНФРАСТРУКТУРЫ

С 2011 года предоставляем комплексные IT-системы и услуги для бизнеса, включая проектирование, разработку, внедрение и сопровождение систем информационной безопасности

IT-компания
аккредитована
Минцифры России

14 лет опыта

350+
клиентов

1000+
реализованных проектов

2000+
защита сетей для банкоматов

TRUST TECHNOLOGIES
TEAMS & TECHNIQUES

ВЫЗОВЫ СОВРЕМЕННОГО БАНКОВСКОГО ПЕРИМЕТРА

- Ужесточение регулирования со стороны ФСТЭК России и ЦБ РФ
- Предотвращение финансовых потерь
- Необходимость соответствия стандарту PCI DSS
- Обеспечение непрерывности бизнес-процессов
- Растущая изощренность кибератак

КЛЮЧЕВЫЕ ЦЕЛИ ПРОЕКТА

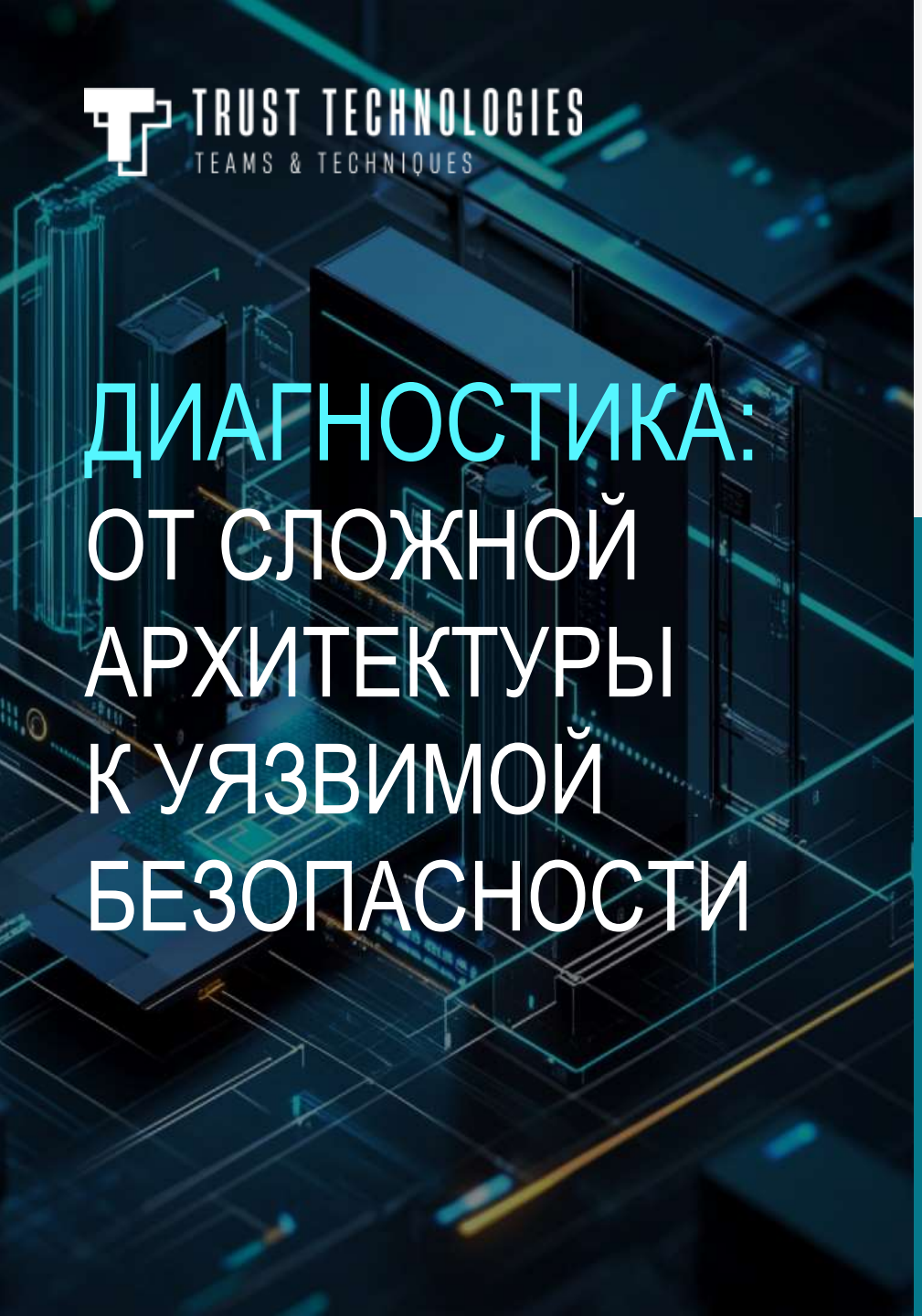
TRUST TECHNOLOGIES
TEAMS & TECHNIQUES

ПОЛНОЕ ИМПОРТОЗАМЕЩЕНИЕ
с соблюдением всех требований ФСТЭК России и PCI DSS

ПЕРЕХОД ОТ L3/L4 к L7:
внедрение глубокого анализа трафика (IPS), контроля приложений и потоковой антивирусной проверки

ГАРАНТИЯ БЕСПЕРЕБОЙНОСТИ И НЕПРЕРЫВНОСТИ БИЗНЕС-ПРОЦЕССОВ во время внедрения в высокодоступную среду

ПОВЫШЕНИЕ ОПЕРАЦИОННОЙ ЭФФЕКТИВНОСТИ за счет централизованного управления и снижения рисков человеческой ошибки



TRUST TECHNOLOGIES
TEAMS & TECHNIQUES

ДИАГНОСТИКА: ОТ СЛОЖНОЙ АРХИТЕКТУРЫ К УЯЗВИМОЙ БЕЗОПАСНОСТИ

ИНФРАСТРУКТУРА

- Три географически распределенных ЦОД
- Решение на базе Open Source
- Spine-Leaf топология
- Два изолированных контура

ПРОБЛЕМЫ

СЛЕПОТА К УГРОЗАМ: отсутствие работающей IPS и контроля на уровне приложений (L7) оставляло сеть уязвимой для современных атак

СЛОЖНОСТЬ УПРАВЛЕНИЯ: поддержка и актуализация разрозненных правил ложились на плечи внутренней IT-команды, отвлекая ресурсы и увеличивая риск ошибок

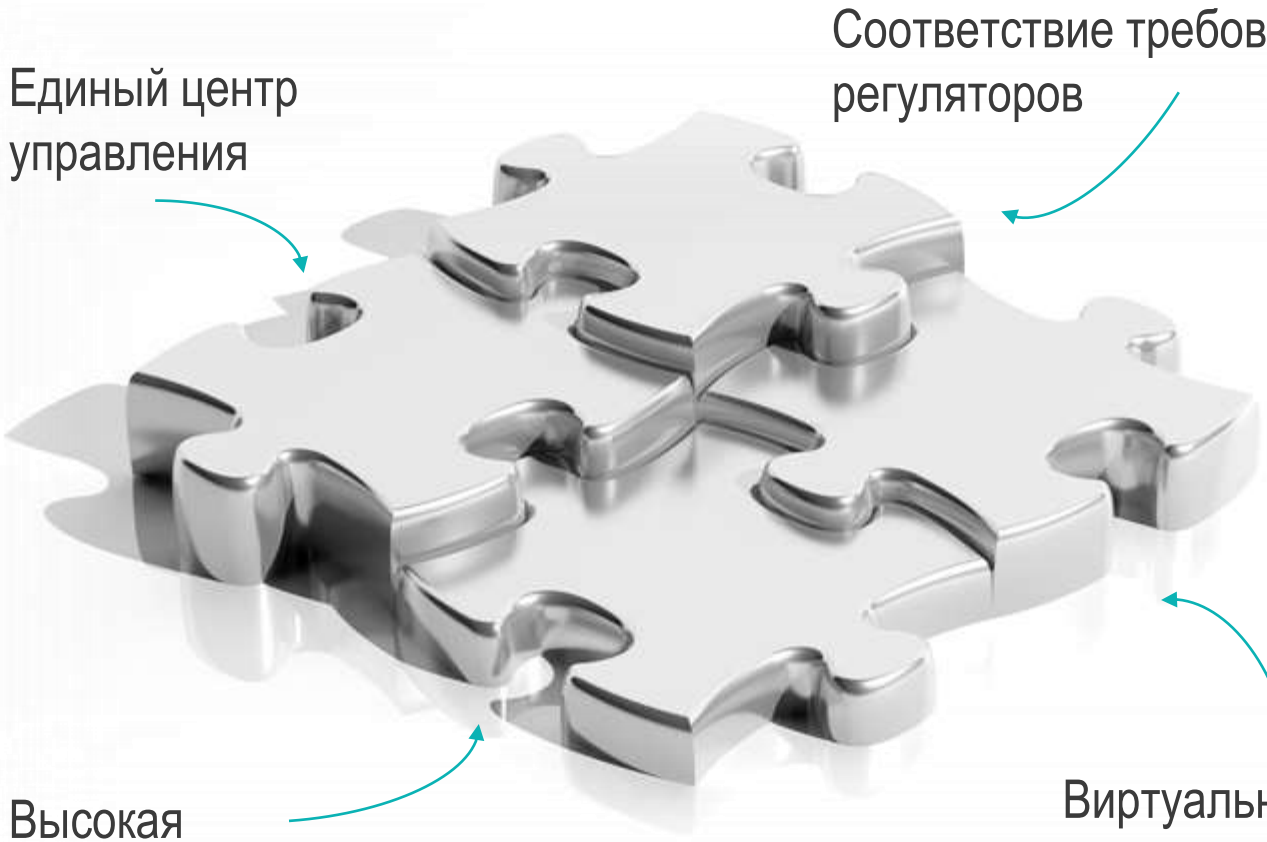
НЕСООТВЕТСТВИЕ ТРЕБОВАНИЯМ РЕГУЛЯТОРОВ: отсутствие сертификатов ФСТЭК России создавало прямые юридические риски

TRUST TECHNOLOGIES
TEAMS & TECHNIQUES

ВЫБОР РЕШЕНИЯ

КАК СОВМЕСТИТЬ БЕЗОПАСНОСТЬ, УНИФИКАЦИЮ И ПРОИЗВОДИТЕЛЬНОСТЬ?

positive technologies



TRUST TECHNOLOGIES
TEAMS & TECHNIQUES

ВИРТУАЛЬНЫЕ КОНТЕКСТЫ

Логическая изоляция вместо физического раздувания

ЗАДАЧА

Изоляция критичных контуров
в соответствии со стандартом PCI DSS

РЕШЕНИЕ

positive technologies

- Контекст для PCI DSS
- Контекст для корпоративной сети

РЕЗУЛЬТАТ

- Унификация требований
- Снижение TCO
- Масштабируемость

TRUST TECHNOLOGIES
TEAMS & TECHNIQUES

ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ

PT MGMT — «мозг» новой системы безопасности

positive technologies

ЗАДАЧА

Сложность администрирования распределённой инфраструктуры:

- три ЦОД;
- кластер в каждом ЦОД;
- в каждом кластере по два виртуальных контекста;

РЕЗУЛЬТАТ

— Единая точка контроля: весь парк межсетевых экранов управляется из одной консоли;

— Групповое управление политиками: изменения вносятся один раз в мастер-политике и автоматически развертываются на все устройства в группе;

— Шаблонизация и безопасность изменений: позволяет обеспечить 100% идентичность правил безопасности на всех площадках;

ИТОГИ ВЫБОРА

TRUST TECHNOLOGIES
TEAMS & TECHNIQUES

ЕДИНАЯ ЭКОСИСТЕМА БЕЗОПАСНОСТИ,

где мощные аппаратные комплексы обеспечивают производительность и изоляцию, а централизованная консоль управления — скорость, контроль и предсказуемость

ВНЕДРЕНИЕ: БЕЗОПАСНОСТЬ, ОТКАЗОУСТОЙЧИВОСТЬ, УПРАВЛЯЕМОСТЬ

ЛОГИЧЕСКАЯ КОНСОЛИДАЦИЯ

- В каждом ЦОД был развернут единый высокопроизводительный кластер PT NGFW
- Созданы два изолированных логических экземпляра — для контура PCI DSS и корпоративного контура
- Соблюдены требования стандартов и снижено TCO

ОТ СЛОВ К СЕГМЕНТАЦИИ

- Отказ от старой модели правил на основе IP- адресов
- Реализация микросегментации на уровне зон: политики безопасности стали прозрачными и безопасными

ВНЕДРЕНИЕ: ИСПЫТАНИЕ НА ПРОЧНОСТЬ

ОТ СЛОВ К СЕГМЕНТАЦИИ

- Перенос динамической маршрутизации;
- Поддержка всех необходимых Route-Map и протокола BFD для мгновенного обнаружения обрывов

ЗАЩИЩЁННЫЙ ХАБ

Для связи между ЦОД была развернута сеть IPsec-туннелей для обеспечения безопасной и отказоустойчивой репликации данных

ЛОГИЧЕСКАЯ КОНСОЛИДАЦИЯ И УПРАВЛЕНИЕ

Развернуто по одному физическому кластеру PT NGFW, внутри которого были созданы изолированные экземпляры для PCI DSS и корпоративного трафика

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ ЧЕРЕЗ PT-MGMT

Мгновенное применение политик для всех трех ЦОД обеспечило их идентичность и значительно ускорило процесс конфигурации

РЕЗУЛЬТАТЫ ПРОЕКТА

РЕГУЛЯТОРНЫЙ ИММУНИТЕТ

Инфраструктура приведена в полное соответствие с требованиями ФСТЭК России и PCI DSS

ЦЕНТР УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ

Централизованное управление политиками для всей распределенной инфраструктуры

ПРОАКТИВНАЯ ЗАЩИТА

Внедрение IPS, контроля приложений и антивируса позволило перейти от пассивной фильтрации к активному предотвращению инцидентов

ОПЕРАЦИОННАЯ ЭФФЕКТИВНОСТЬ

Окупаемость в операционной деятельности и информационной безопасности

TRUST TECHNOLOGIES
TEAMS & TECHNIQUES

Александр Сапрыкин
Главный инженер ИБ
Trust Technologies

Карина Назарова
Руководитель проектов
Trust Technologies

ПОЛУЧИТЬ ДОВЕРЕННУЮ ЭКСПЕРТИЗУ

trusttech.ru

info@trusttech.ru