Trust Technologies

Безопасность и доверие

СИСТЕМНЫЙ ИНТЕГРАТОР РЕШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ООО «ТРАСТ ТЕХНОЛОДЖИЗ»

О КОМПАНИИ

Trust Technologies
Безопасность и доверие

ООО «Траст Технолоджиз» системный интегратор в области информационной безопасности, реализующий программные продукты, программно-аппаратные комплексы и осуществляющий их сопровождение с 2011 г.

10+
лет на рынке

100+
клиентов

1 000+
реализованных проектов

СИЛЬНАЯ ЭКСПЕРТИЗА ИНЖЕНЕРОВ

КЛЮЧЕВЫЕ КОМПЕТЕНЦИИ

Trust Technologies
Безопасность и доверие

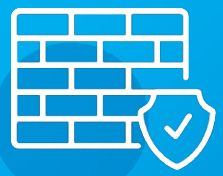
Подключение к ЕБС

Обеспечение сетевой безопасности

Защита виртуальных сред

Безопасность мобильных устройств

Двухфакторная идентификация



Межсетевые экраны

Выявление вредоносные программ

Проведение Аудитов по ИБ

НАШИ ПРОДУКТЫ

Trust Technologies
Безопасность и доверие

Межсетевые экраны нового поколения (NGFW)

NGFW - это комплексное решение сетевой безопасности, обеспечивающее контроль трафика, управление доступом пользователей и приложений, антивирусную защиту и предотвращение атак.

01

Web Application Firewall

Web Application Firewall (WAF) – это эффективное средство для защиты веб ресурсов. WAF вобрали в себя средства защиты от большинства информационных атак, что позволяет разработчикам сосредоточиться на реализации бизнес-логики приложения без ограничений.

02

Защита от таргетированных атак и угроз нулевого дня / Anti APT

Защита от таргетированных атак в комплексной системе безопасности компания – такая же необходимость как использование межсетевого экрана или антивируса на рабочей станции.

03

SD-WAN

SD-WAN предоставляют организациям дополнительные преимущества за счет использования корпоративной глобальной сети (WAN) совместно с несколькими облачными инфраструктурами.

04

Контроль привилегированных пользователей

Контроль подрядчиков и привилегированных пользователей, подключающихся удаленно к корпоративным ресурсам, одна из важнейших функций системы информационной безопасности.

05

Двухфакторная аутентификация

Двухфакторная аутентификация — это метод идентификации пользователя в каком-либо сервисе при помощи запроса аутентификационных данных двух разных типов.

06

Обучение сотрудников информационной безопасности

Повышение осведомленности сотрудников компании в вопросах информационной безопасности является такой же важной составляющей в комплексе мер по обеспечению информационной безопасности, как использование антивирусного ПО.

07

Защита виртуальных сред

Специальные решения защиты виртуальных сред обеспечивают большую надежность и функциональность, чем традиционные программно-аппаратные решения, при этом они повышают удобство пользования сетевыми сервисами и упрощают администрирование.

08

Мониторинг и корреляция событий

Современные информационные системы и системы информационной безопасности генерируют гигабайты событий в сутки. Основная задача SIEM систем — выявить атаки на информационные активы компании и отреагировать на них до наступления существенного ущерба.

09

Защита конечных точек

Невозможно обеспечить должную защиту ресурсов компании без защиты конечных устройств - рабочих станций, ноутбуков, серверов. И все они — потенциальные лазейки, ведущие прямо к вашим корпоративным секретам, которые необходимо защищать.

10

Безопасность мобильных устройств

Все современные компании пользуются мобильными технологиями. Для защиты данных, доступ к которым могут получить посторонние, можно их зашифровать на устройстве, изолировать от корпоративных материалов, но поддерживать при этом процедуры контроля доступа.

11

Защита от DDoS

DDoS атака - распределенная атака типа «отказ в обслуживании», целью которой является вывести из строя сайт путем постоянного потока запросов, поступающих на него с десятков и сотен тысяч зараженных компьютеров, разбросанных по всему миру.

12

Защита от утечек конфиденциальной информации

Система контроля утечек конфиденциальной информации предназначена для защиты корпоративных данный от случайных и преднамеренных утечек по различным каналам связи.

13

УСЛУГИ

Trust Technologies
Безопасность и доверие

Надежные решения в сфере информационной безопасности

01

Тестирование на проникновение (Penetration test)

Услуга по проверке инфраструктуры заказчика на возможность проникновения в ходе, которой проводится:

- анализ общедоступной информации о Компании;
- сбор информации о доступных из сетей общего доступа информационных ресурсах Компании;
- выявление уязвимостей ресурсов, способных привести к возможности осуществления несанкционированных воздействий на них;
- разработку векторов и методов проникновения с учетом анализа полученных данных;
- попытки получения доступа к информационным ресурсам с использованием инструментальных средств и выявленных уязвимостей.

02

Аудит информационных систем и информационной безопасности

Аудит информационной безопасности (ИБ)— системный процесс получения объективных качественных и количественных оценок о текущем состоянии ИБ автоматизированной системы в соответствии с определёнными критериями и показателями безопасности. Аудит информационной безопасности необходим информационной системе, даже если она работает без нареканий. Устаревшие версии, не пропатченные программы могут стать причиной проникновения в систему, и только внешний аудит выявит ее слабые места.

03

Техническая поддержка и центр мониторинга 24X7

Компания Траст Технолоджиз имеет свой собственный центр мониторинга и технической поддержки, работающий в режиме 24x7. Аутсорсинг – отдельный вид технической поддержки, когда помимо работы над инцидентами наши инженеры осуществляют управление и настройку средств защиты информации Заказчика.

04

Подключение к единой биометрической системе

Сервис позволяет получать услуги удалённо — с помощью биометрии (лица и голоса). Как следует из Информационного письма Банка России, в рамках выполнения Закона № 482-ФЗ в отделениях банков требуется предоставить возможность сбора биометрических данных граждан для передачи их в Единую биометрическую систему. Инициатором создания Единой Биометрической Системы выступили Банк России и Министерство цифрового развития, связи и массовых коммуникаций РФ.

05

Защита каналов связи с помощью криптографического модуля «КРИПТОSDK»

«КриптоSDK» — криптографический модуль, разработанный компанией ПАО «Ростелеком», предназначенный для построения защищенного канала связи от приложения пользователя до Единой биометрической системы (ЕБС) или другой информационной системы.

06

Проектирование и внедрение систем информационной безопасности

Целью проектирования системы обеспечения информационной безопасности (СОИБ) является выработка рекомендаций, организационных и технических решений по обеспечению безопасности инфоресурсов хранимых и передаваемых по каналам связи в информационных системах.

ПАРТНЕРЫ

Trust Technologies
Безопасность и доверие

Компания «Траст Технолоджиз» предлагает своим клиентам набор эффективных решений для комплексного обеспечения информационной безопасности организации.

Цель «Траст Технолоджиз» – помочь улучшить прибыльность вашего бизнеса и качество вашей жизни за счет наиболее эффективного использования технологий, предложив лучшие решения для всех ваших пожеланий. Компания работает с ведущими производителями в области информационной безопасности, среди которых:

КОД безопасности
positive technologies
Check Point SOFTWARE TECHNOLOGIES LTD
Центр Биометрических Технологий
BI.ZONE Cybersecurity
ЦФТ ЦЕНТР ФИНАНСОВЫХ ТЕХНОЛОГИЙ
Ростелеком
BIOSMART
КРИПТОПРО
UserGate
phishman
КОМПАНИЯ ИНДИД
AVSOFT
АСТРА
DEPO [computers]
MULTIFACTOR
Антифишинг
NGRSOFTLAB
Новые Платформы
ФАКЕЛ
Dr.WEB
Вебмониторэкс защита веб-приложений
ИнфраМенеджер
EVERYTAG
VolgaBlob
с•терра
Т-КОМ РОСАТОМ
F.A.C.C.T.
Эшелон комплексная безопасность
kaspersky
CROSSTECH SOLUTIONS GROUP
CYBER MEDIA
Vkorpe
ГАРДА ТЕХНОЛОГИИ
НАУЧНО-ИСПЫТАТЕЛЬНЫЙ ИНСТИТУТ СИСТЕМ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ
QRATOR LABS
SEARCHINFORM INFORMATION SECURITY
INFOWATCH
ideco
NGENIX
AERODISK faster, higher, safer
rrc
WorksPad
MONT
FORTIS
AXOFT
OCS DISTRIBUTION
ЦИАМ
R-Vision
QTECH МИР ДОСТУПНЕЕ
RTT

КЕЙСЫ

Trust Technologies
Безопасность и доверие

ВТБ АРЕНА

Защита биометрических данных

Клиент: «ВТБ Арена»

Задача
Обеспечить безопасность персональных данных (в том числе биометрических) посетителей стадиона с использованием средств криптографической защиты информации.

Результат
В рамках проекта мы развернули на объектах заказчика инфраструктуру защищенной криптографической сети передачи данных. По ней будут передаваться сведения, содержащие персональные данные посетителей стадиона. Развертывание подсистемы криптографической защиты состояло из двух этапов:

1. Защита внутренних сетей заказчика: арена, ЦОД.
2. Защита каналов взаимодействия с ЕБС.

Для построения инфраструктуры надежной криптографической защиты было использовано решение на базе криптошлюзов «Континент».

ОСК

Аудит сети защищенных каналов связи

Клиент: АО «ОСК»
Задача
1. Оценить уровень конфиденциальности, целостности и доступности информации, передаваемой по открытым каналам связи;
2. Обеспечить своевременное предупреждение и противодействие угрозам устойчивости и безопасности функционирования контура ИТ-инфраструктуры предприятий, входящих в АО «ОСК».
3. Полностью соответствовать нормам закона. Иметь все действующие сертификаты соответствия требованиям безопасности для средств криптографической защиты информации.

Этапы работы
- Оценка и проверка сети защищенных каналов связи между предприятиями группы компаний;
- Разработка плана обновления и рекомендаций по обновлению для дочерних организаций;
- Обновление платформ в головной компании;
- Разработка плана модернизации сети.

HOME CREDIT BANK

Услуги по подключению к системе единой биометрии. Облачное типовое решение по информационной безопасности (ОТИБ)

Клиент: Хоум Кредит Банк

Задача
Подключение информационной системы к промышленному контуру ЕБС.

Результат
- Возможность дистанционно открывать счета новым клиентам, что обеспечит рост доходов и переход в digital.
- Снижение финансовых рисков: биометрия на сегодня лучшая технология, позволяющая с высокой степенью надежности подтвердить личность человека при удаленной идентификации.
- Сокращение расходов на развитие и поддержание сети филиалов банка.
- Дополнительное продвижение в регионы.
- Возможность допродажи новых услуг, требующих повышенного уровня защищенности при удаленной идентификации пользователя.

MOEX МОСКОВСКАЯ БИРЖА

Внедрение средства защиты информации vGate R2

Клиент: MOEX «Московская биржа»

Задача
Заказчик хотел защитить свои виртуальные инфраструктуры в соответствии с требованиями регулятора по защите финансовых организаций ГОСТ Р 57580.1-2017.

Результат
В рамках проекта выполнены работы по установке и настройке средства защиты информации vGte r2. Защитные компоненты установлены на 24 ESXi сервера и на 2 сервера управления VCSA, также установлены агенты аутентификации всем администраторам виртуализации и администраторам информационной безопасности. Настройки произведены в соответствии с требованиями регулятора по защите информации финансовых организаций ГОСТ Р 57580.1-2017. Инженерами Тарст Технолоджиз был разработан и применен шаблон политики безопасности, обеспечивающий контроль целостности виртуальных машин, разграничение доступа к виртуальным машинам. Созданы правила запрещающего доступа до среды виртуализации без агента аутентификации vGate.

КЛИЕНТЫ

Trust Technologies
Безопасность и доверие

Клиенты «Траст Технолоджиз» - компании среднего и крупного бизнеса, которые заинтересованы в повышении информационной безопасности организации и защите компьютерных сетей.

ГОСУДАРСТВЕННЫЕ СТРУКТУРЫ

- Департамент информационных технологий города Москвы
- Единый портал Электронной подписи

РИТЕЙЛ

- BUSINESS CAR
- Globus
- РИГЛА

ПРОМЫШЛЕННОСТЬ

- ТМК Трубная металлургическая компания
- Центр Внедрения ПРОТЕК
- enel
- Группа СИНАРА
- ИНТЕР РАО Нижневартовская ГРЭС
- МашКомплектСервис

ТЕЛЕКОМ

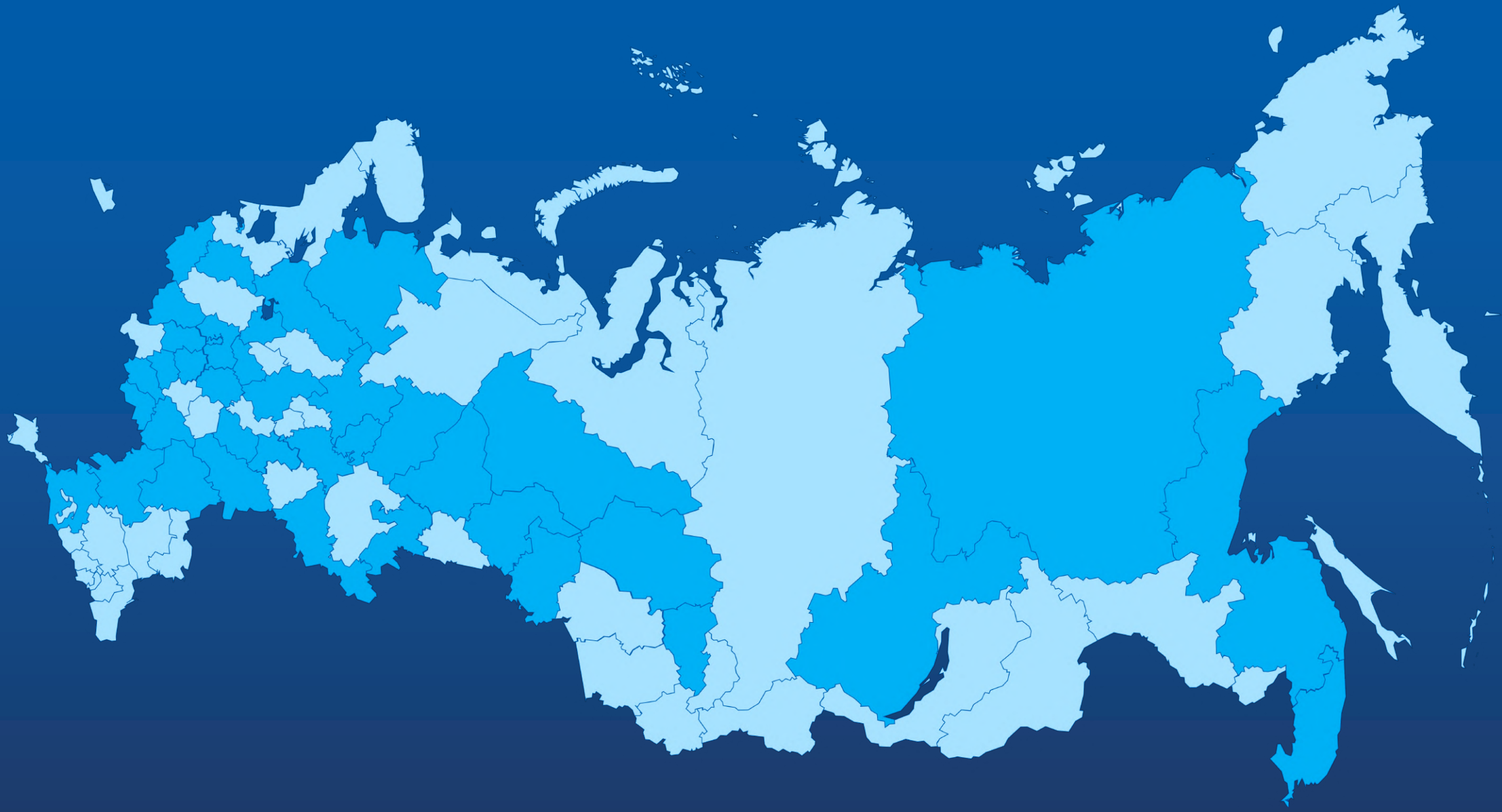
- МТС
- TAX COM
- Новые Платформы
- 3data Premium Data Centers
- АТЛАС научно-технический центр
- 1С Фирма "1С"

ФИНАНСЫ

- ВТБ
- Открытие Банк
- Хоум Банк
- ОТП Банк
- ББР Банк
- Ингосстрах Банк
- fin Банк Финсервис
- Челиндбанк
- Севергазбанк
- Держава Банк
- ТХБ тольяттихимбанк
- Банк Оренбург
- Банк Пойдём!
- Углеметбанк
- Банк РостФинанс
- Стройлесбанк Мой надежный банк
- Уралпромбанк
- Тендер Банк
- Великие Луки Банк
- Развитие консалтинг
- Акционерная финансовая корпорация Система

ГЕОГРАФИЯ

Trust Technologies
Безопасность и доверие



Trust Technologies

Безопасность и доверие

Телефон:
+7 (495) 120-85-95
(многоканальный)

Сайт:
www.trusttech.ru

Email:
info@trusttech.ru

vk.com/
trust_technologies

t.me/
trusttechnologies

youtube.com/
@trusttechru

Адрес офиса:
115533 г. Москва, проспект Андропова,
д. 22, офис 0901