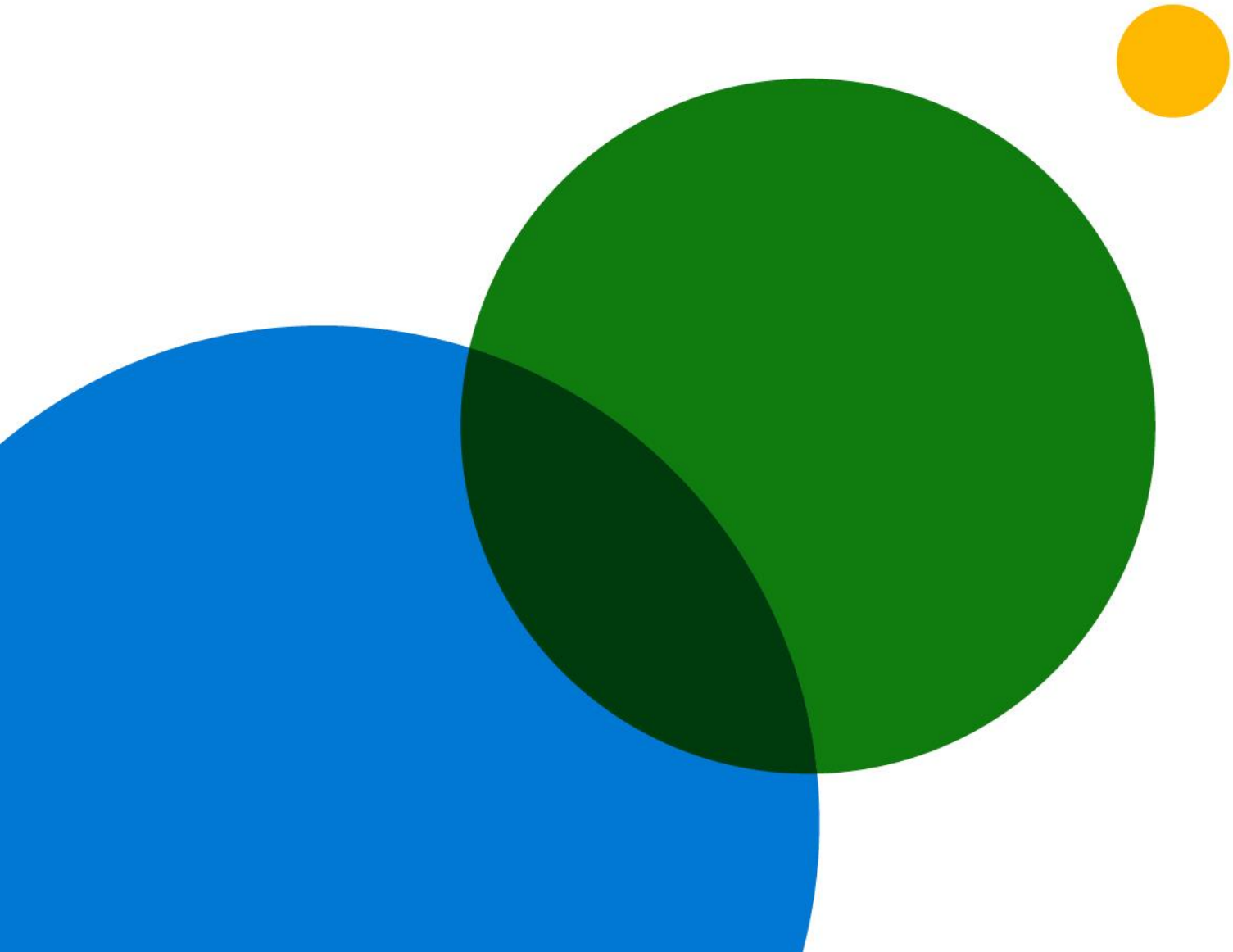
Microsoft Security

hypothesis

Отчет о внедрении модели нулевого доверия



Содержание

Введение

Васу Джаккал (Vasu Jakkal)/Корпоративный вице-президент по безопасности, соответствию требованиям и идентификации

Прошедший год запомнится эволюцией кибербезопасности и развитием модели нулевого доверия в качестве основной стратегии в отраслях и организациях по всему миру.

В начале пандемии рабочее место в одночасье стало почти полностью удаленным. В результате многие организации были вынуждены быстро адаптироваться, чтобы поддержать сотрудников, которые выполняли работу так, как могли — используя личные устройства, взаимодействуя с помощью облачных сервисов и обмениваясь данными за пределами периметра корпоративной сети. По мере того, как организации адаптировались к этой трансформации, они также сталкивались со все более изощренными киберпреступниками, которые постоянно развивали тактику и ресурсы, а также ставили более высокие цели.

Сегодня гибридная работа — это новая реальность. На этом фоне и перед лицом быстрых изменений опрошенные нами организации заявили, что они используют модель нулевого доверия, чтобы усилить безопасность, обеспечить гибкость соблюдения требований, увеличить скорость обнаружения и устранения угроз, а также упростить и повысить доступность средств анализа безопасности.

Комплексная архитектура нулевого доверия основана на принципах явной проверки. Используя доступ с наименьшими привилегиями и предполагая нарушение, она обеспечивает требуемый уровень безопасности для удостоверений, конечных точек, приложений, инфраструктуры, сети и данных, а также улучшает прозрачность, автоматизацию и управление. Мы не только рекомендуем этот подход нашим клиентам и партнерам, но и применяем его для своей системы глобальной безопасности и при разработке программного обеспечения в Microsoft.

В этом отчете рассказывается об опыте внедрения модели нулевого доверия на различных рынках и в различных отраслях. Мы надеемся, что сведения, полученные в результате этого исследования, помогут ускорить внедрение модели нулевого доверия в вашей организации, прольют свет на общий прогресс ваших коллег и дадут представление о будущем этого быстро развивающегося пространства.

Методология

Корпорация Microsoft поручила агентству Hypothesis Group, которое занимается анализом, проектированием и разработкой стратегий, провести исследование и подготовить отчет о внедрении модели нулевого доверия. Исследование в США включало в себя два этапа, чтобы выявить тенденции и текущее состояние внедрения модели нулевого доверия, причем на втором этапе были добавлены дополнительные рынки для выявления глобальных тенденций.

Первоначальное исследование было проведено в августе 2020 года, когда в США был проведен 15-минутный онлайн-опрос с участием 300 лиц, принимающих решения в области безопасности (security decision-maker, SDM) и участвующих в принятии стратегических решений о внедрении модели нулевого доверия в компаниях из ряда отраслей. Помимо онлайн-опроса в сентябре 2020 года было проведено 5 подробных интервью среди SDM из США в ряде отраслей.

В апреле 2021 года глобальные исследования были проведены в США, Германии, Японии, Австралии и Новой Зеландии среди аналогичной группы лиц, принимающих решения в области безопасности. Более 900 участников приняли участие в 15-минутном онлайн-опросе с вопросами о внедрении стратегии нулевого доверия, рекомендациях, преимуществах, проблемах и о планируемых будущих инвестициях.

Полезная информация о внедрении модели нулевого доверия

01 / Организации готовы воспользоваться стратегией нулевого доверия вследствие перехода к гибридным рабочим местам и Covid-19

Лица, принимающие решения в области безопасности, говорят, что разработка стратегии нулевого доверия является их главным приоритетом в области безопасности, причем 96 % заявили, что это имеет решающее значение для успеха их организации. Основными мотивами при внедрении стратегии нулевого доверия являются улучшение общего состояния безопасности и взаимодействие с конечными пользователями. Переход к гибридным рабочим местам, ускоренный пандемией COVID-19, также способствует более широкому внедрению стратегии нулевого доверия: переход к гибридным рабочим местам начали 81 % организаций, причем 31 % полностью его выполнили. Тем не менее, 94 % обеспокоены подобным переходом, главным образом, из-за возможности неправомерного использования, увеличения ИТ-нагрузки и кибератак. Учитывая это, ключевые аспекты стратегии включают в себя усиленное обучение сотрудников и многофакторную аутентификацию для обеспечения удобного взаимодействия и перехода.

02 / Стратегия нулевого доверия обеспечивает гибкость при выборе начальной точки внедрения, таким образом подход может быть адаптирован к их нуждам

Менее 15 % организаций начали внедрять стратегию нулевого доверия в той же области риска. Это в значительной степени связано с тем, что к реализации подходят как к комплексному процессу, объединяющему все элементы и возможности архитектуры системы безопасности, а не как к набору разрозненных, отдельных технологий. Аналогичным образом, порядок, в котором внедряются отдельные компоненты модели нулевого доверия в области риска, сильно варьируется, причем мнения специалистов по безопасности относительно того, какие компоненты внедрять в первую очередь, существенно различаются.

03 / Несмотря на то, что стратегия нулевого доверия получила широкое распространение и помогает организациям справляться с угрозами, многое еще предстоит сделать

76 % организаций по крайней мере начали внедрять стратегию нулевого доверия, а 35 % утверждают, что стратегия полностью реализована. Однако те, кто утверждает, что реализация завершена, также отмечают, что они не закончили внедрение стратегии нулевого доверия во всех областях и компонентах, подвергающихся риску. Стратегия нулевого доверия привлекательна, поскольку она обеспечивает повышенную гибкость, скорость обнаружения угроз и улучшенную способность управлять безопасностью Интернета вещей (IoT) и операционных технологий (OT). Внедрение расширяется в США (с 70 % в августе 2020 года до 79 % в апреле 2021 года). США также продвинулись дальше по сравнению с другими странами, которые начали процесс внедрения позже. Кроме того, организации в США утверждают, что менее ограничены в бюджете. Однако, в то время как 57 % организаций утверждают, что опережают других в процессе внедрения, почти половине все еще предстоит много работы, поскольку они не полностью внедрили модель нулевого доверия во всех областях и компонентах, подвергающихся риску.

04 / Оценивая перспективы, можно сказать, что стратегия нулевого доверия останется главным приоритетом и потребует принятия взвешенных решений относительно сотрудников и поставщиков.

Ожидается, что через 2 года стратегия нулевого доверия останется основным приоритетом безопасности, а организации ожидают увеличения инвестиций. Решение проблем с собственными сотрудниками (включая подбор специалистов по безопасности и поддержку со стороны руководства) станет ключом к удвоению инвестиций в реализацию стратегии нулевого доверия. Когда дело доходит до стратегии поставщика, лица, принимающие решения в области безопасности, отдают предпочтение работе с целостными или консолидированными поставщиками, учитывая, что выбор поставщика часто зависит от наличия опыта и внутренних ресурсов. К преимуществам подхода «лучший в своем классе» относятся расширенный опыт, ресурсы и простота. Однако его реализация может занять больше времени, его сложнее интегрировать в существующую архитектуру системы безопасности, и он увеличивает потенциальную уязвимость.

Участники исследования

По всему миру

Лица, принимающие решения в области безопасности,
которые работают в крупных компаниях *

90 %
знакомы с моделью нулевого доверия
Самостоятельно прошли тест на знания

76 %
реализуют модель нулевого доверия

24 % планируют/рассматривают возможность внедрения модели нулевого доверия

*более 1000 сотрудников в США; более 500 сотрудников в Германии, Японии, Австралии и Новой Зеландии

Общие результаты исследования

Организации готовы применять стратегию нулевого доверия

Стратегия нулевого доверия на сегодняшний день является основным приоритетом безопасности на всех рынках и в отраслях, причем в последние годы ряд организаций внедрял эту стратегию. Стратегия нулевого доверия является приоритетной для большинства (53 %), однако особенно широкое распространение она получила в США (56 %) и Германии (53 %).

Почти все специалисты по безопасности (96 %) считают, что стратегия нулевого доверия имеет решающее значение для успеха их организации. (См. рисунок 1) В дополнение к укреплению общей безопасности и улучшению взаимодействия с конечными пользователями, специалисты по безопасности применяют стратегию нулевого доверия для упрощения процедур системы безопасности для сотрудников. (См. рисунок 2)

Как объясняет один из респондентов, который является лицом, принимающим решения в области безопасности в США в гостиничном бизнесе: *«Цель заключается в том, чтобы улучшить нашу позицию безопасности в целом, но важное значение имеет и уменьшение количества проблем в работе конечных пользователей, что позволит упростить их жизнь».*

Более того, 31 % специалистов по безопасности рассматривают стратегию нулевого доверия как важный инструмент в предстоящем переходе к гибридной работе после пандемии. Этот фактор особенно заметен в Австралии и Новой Зеландии (44 %).

Рисунок 1. Нулевое доверие имеет решающее значение

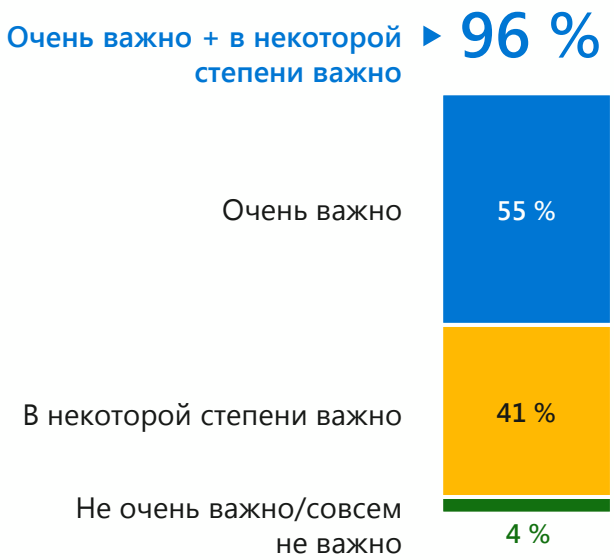


Рисунок 2. Мотивы внедрения модели нулевого доверия

Основные причины	
Повышение общего уровня безопасности	47 %
Улучшение взаимодействия с пользователями и повышение продуктивности	44 %
Преобразование взаимодействия групп безопасности	38 %
Упрощение стека безопасности	35 %
Снижение расходов на безопасность	35 %

Переход к гибридной работе способствует более широкому внедрению стратегии нулевого доверия

81 % организаций начали переход к гибридной работе, а 31 % уже полностью закончили переход. Тем не менее, темп полного внедрения отличается на разных рынках: в то время как Австралия и Новая Зеландия лидируют (37 %), Германия сильно отстает (только 20 % организаций уже перешли на гибридную модель). (См. рисунок 3)

Несмотря на то, что мировые рынки в разном темпе переходят на гибридную работу, подавляющее большинство организаций (91 %), которые еще не завершили переход, планируют завершить его в течение ближайших 5 лет. Важно отметить, что 94 % обеспокоены переходом: их основными опасениями являются неправомерное использование, увеличение ИТ-нагрузки и повышенный риск кибератак. (См. рисунок 4)

Рисунок 3. Гибридное рабочее место

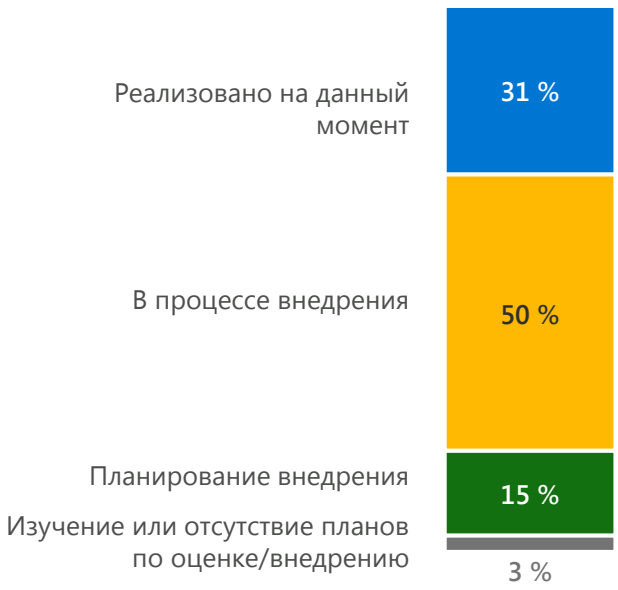
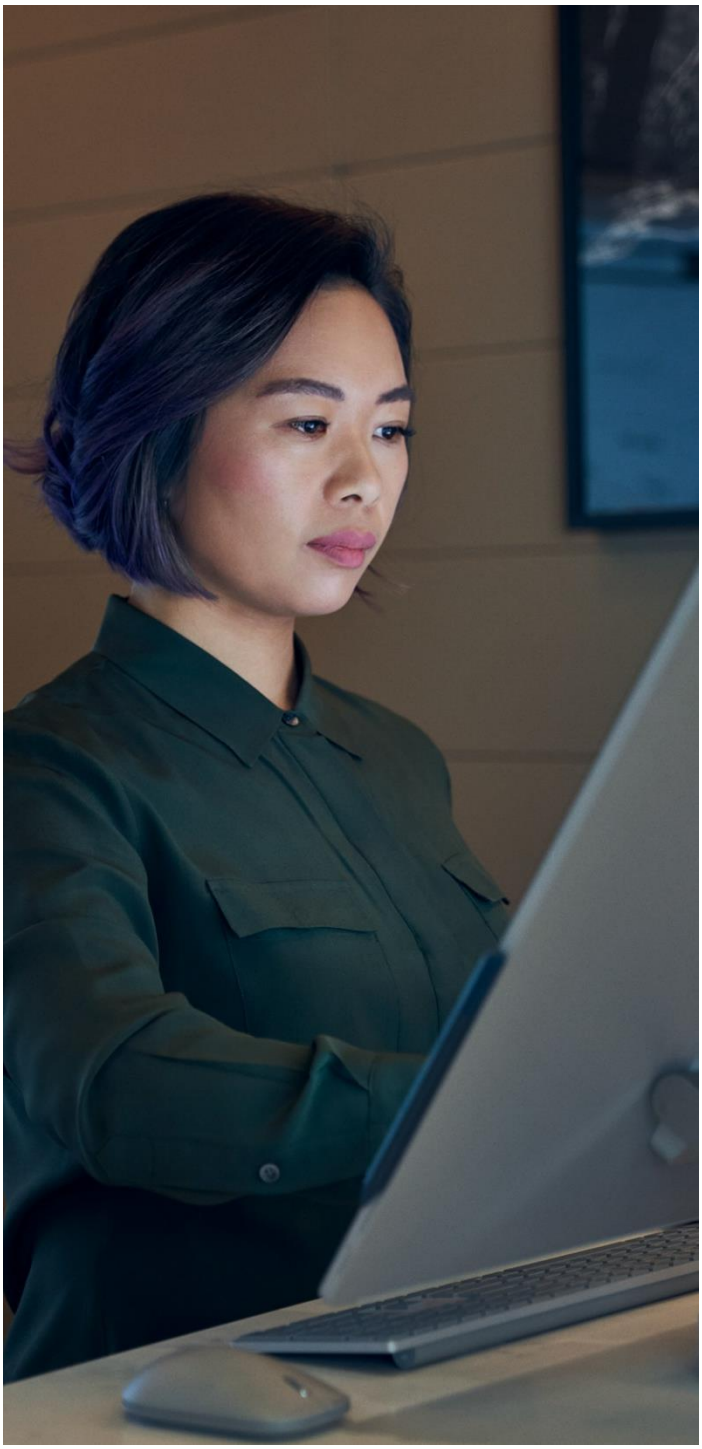


Рисунок 4. Опасения по поводу гибридного рабочего места

Сотрудники загружают небезопасные приложения	37 %
Увеличение рабочей нагрузки на ИТ-отдел	37 %
Программы-вымогатели	36 %
Фишинговые атаки	35 %
Неправильное использование персональных устройств	34 %
Несанкционированный доступ к данным	31 %
Отсутствие возможности управлять всеми устройствами	30 %
Использование личных учетных записей электронной почты	30 %
Несоблюдение правил обработки данных	24 %

Пандемия Covid-19 внесла свои коррективы, которые ускоряют переход к стратегии нулевого доверия



Чтобы свести к минимуму потенциальные проблемы, заинтересованные стороны подчеркивают важность повышения квалификации сотрудников (54 %), особенно в Японии (61 %) и Германии (58 %), и использование многофакторной аутентификации (MFA) (50 %), особенно в Соединенных Штатах (52 %) и Германии (56 %), для обеспечения удобного и простого взаимодействия с пользователями.

Поскольку стратегия нулевого доверия помогает обеспечить безопасность удаленной и гибридной работы, пандемия COVID-19 ускорила внедрение стратегии нулевого доверия для 72 % организаций, несмотря на то, что рынки развиваются асимметрично. Пандемия выступила катализатором внедрения примерно для 7 из 10 организаций в США (76 %), Японии (71 %) и Австралии/Новой Зеландии (69 %). Однако темпы внедрения были заметно ниже в Германии (62 %), возможно, из-за более медленного перехода к гибридному рабочему месту.

Модель нулевого доверия широко реализована по всему миру и все больше распространяется в США

Нулевое доверие — это не просто модное слово, это реальность. 76 % организаций по крайней мере начали реализовывать эту стратегию, а 35 % считают, что стратегия полностью реализована. Тем не менее, эти данные рисуют чрезмерно оптимистичную картину, поскольку многие организации, которые полагают, что закончили внедрение модели, по их собственному признанию, не закончили этот процесс во всех областях риска. Сегодня США опережают другие рынки во внедрении стратегии нулевого доверия и продолжают стремительно расти: по сравнению с августом 2020 года реализация стратегии нулевого доверия в США выросла с 70 % до 79 %, что является значительным скачком всего за восемь месяцев.
(См. рисунок 5)

Стратегия нулевого доверия в настоящее время является самой распространенной в пространстве безопасности, однако это относительно новая тенденция. 82 % компаний внедрили стратегии нулевого доверия в течение последних трех лет, а 21 % — за последние 12 месяцев. 26 % организаций США начали внедрение более 3 лет назад, по сравнению с 19 % японских организаций, 6 % организаций в Австралии и Новой Зеландии и 3 % организаций в Германии. Более раннее внедрение в США — вместе с меньшим количеством бюджетных ограничений — может объяснить, почему организации в США опережают другие рынки во внедрении модели нулевого доверия. Аналогичным образом, относительно новая тенденция внедрения модели нулевого доверия в Германии помогает понять его более низкие темпы внедрения: 97 % немецких организаций начали внедрение только в последние три года.

Рисунок 5. Реализация модели нулевого доверия

	США (2020 г.)	США	Германия	Япония	Австралия/ Н. Зеландия
Реализация модели нулевого доверия	70 %	79 %	75 %	76 %	71 %
• Полностью реализовано	27 %	44 %	19 %	32 %	28 %
• В процессе реализации	43 %	35 %	56 %	44 %	43 %

35 % полностью реализовано

42 % в процессе реализации

Не существует универсального подхода к реализации модели нулевого доверия, позволяющего приступить к реализации где угодно

Ни одна область риска (удостоверения, конечные точки, приложения, сеть, инфраструктура, данные, автоматизация и управление) не выделяется в качестве основной отправной точки для внедрения стратегии нулевого доверия, поскольку менее 15 % организаций начинают с одной и той же области риска. Организации начинают с разного, исходя из своих потребностей и имеющихся внутренних ресурсов. В конечном итоге они стремятся внедрить стратегию нулевого доверия во всех областях риска, чтобы обеспечить еще большую защиту от угроз, поэтому нулевое доверие воспринимается как комплексная стратегия, которая должна быть завершена с течением времени. (См. рисунок 6)

Помимо областей риска стратегии нулевого доверия, организации должны определить отдельные компоненты каждой области риска и расставить приоритеты. Для конечных точек, приложений, сети, данных и автоматизации/управления нет четкой отправной точки. Мнения специалистов по безопасности относительно приоритетных компонентов существенно различаются. Однако строгая проверка подлинности обычно реализуется в первую очередь для удостоверений, а в инфраструктуре явным приоритетом являются средства обнаружения угроз. (См. рисунок 7)

Рисунок 6. Текущая реализация модели нулевого доверия — области риска

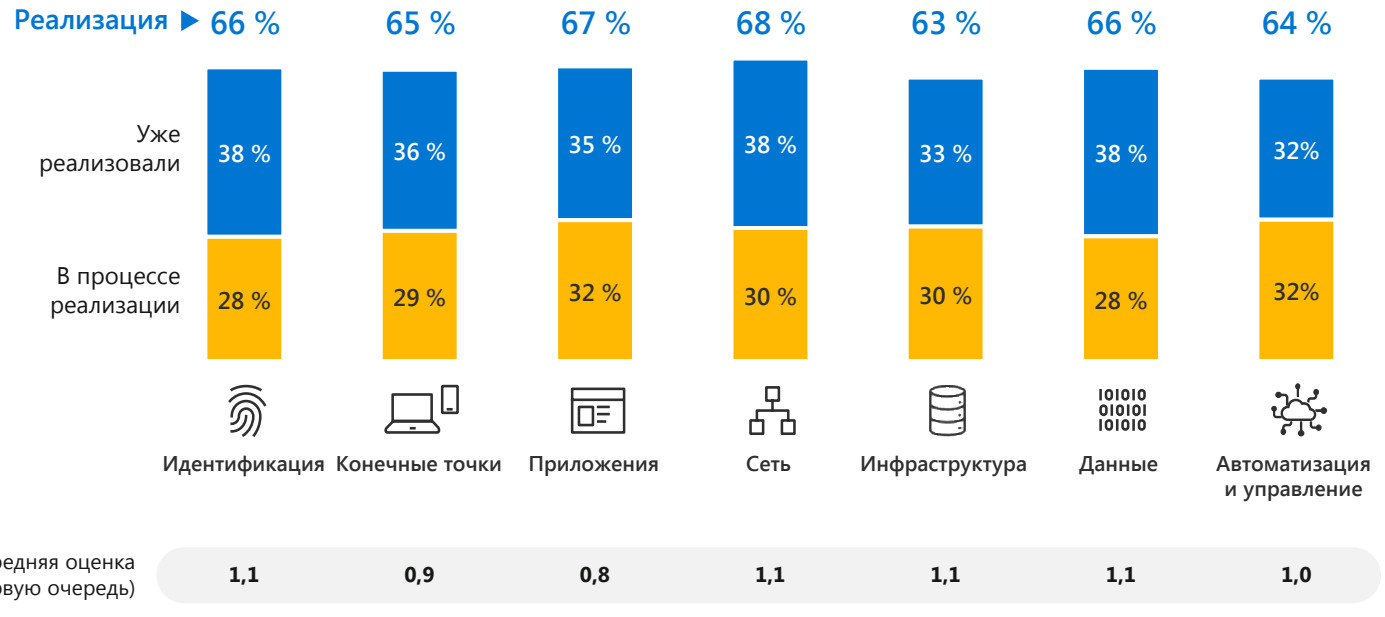


Рисунок 7. Реализация модели нулевого доверия для компонентов (Топ 3) — № 1 по оценкам (реализовано в первую очередь)

Идентификация	
Строгая аутентификация (т. е. многофакторная аутентификация, аутентификация без пароля)	32 %
Автоматическое обнаружение и устранение угроз	27 %
Адаптивные политики доступа для защиты доступа к ресурсам	22 %

Конечные точки	
Политики и элементы предотвращения потери данных для всех неуправляемых и управляемых устройств	27 %
Оценка рисков для устройств в режиме реального времени / обнаружение угроз на конечных точках	26 %
Устройства зарегистрированы у поставщика удостоверений	24 %

Приложения	
Постоянное обнаружение теневых ИТ-ресурсов и оценка рисков	23 %
Детализированное управление доступом к приложениям (например, ограниченная видимость или только чтение)	22 %
Управление доступом к приложениям на основе политик	20 %

Сеть	
Надежный контроль доступа для защиты сетей	25 %
Защита от угроз и фильтрация с помощью контекстных сигналов	24 %
Весь трафик шифруется	20 %

Инфраструктура	
Доступ группы по обеспечению безопасности к средствам обнаружения угроз	25 %
Защита облачных рабочих нагрузок в гибридных и многооблачных средах	19 %
Детальная визуализация и контроль доступа для всех рабочих нагрузок (виртуальные машины, серверы и т. д.)	17 %

Данные	
Разрешения на доступ регулируются механизмом политик безопасности	21 %
Данные классифицируются и маркируются	21 %
Наиболее конфиденциальные файлы постоянно защищены шифрованием	20 %

Автоматизация и управление	
Комплексная визуализация обеспечивается с помощью централизованной платформы для расследования и реагирования	29 %
Данные об угрозах собираются и анализируются в разных доменах (удостоверения, конечные точки, приложения, сеть, инфраструктура)	28 %
Включено автоматизированное расследование и реагирование	22 %

Мы не рассматривали это просто как набор технологий, а как стратегию и подход к рассмотрению каждого пользовательского ресурса, как внутри нашей сети, так и за ее пределами, как ненадежного до тех пор, пока он не будет проверен».

Лица, принимающие решения в области безопасности в США

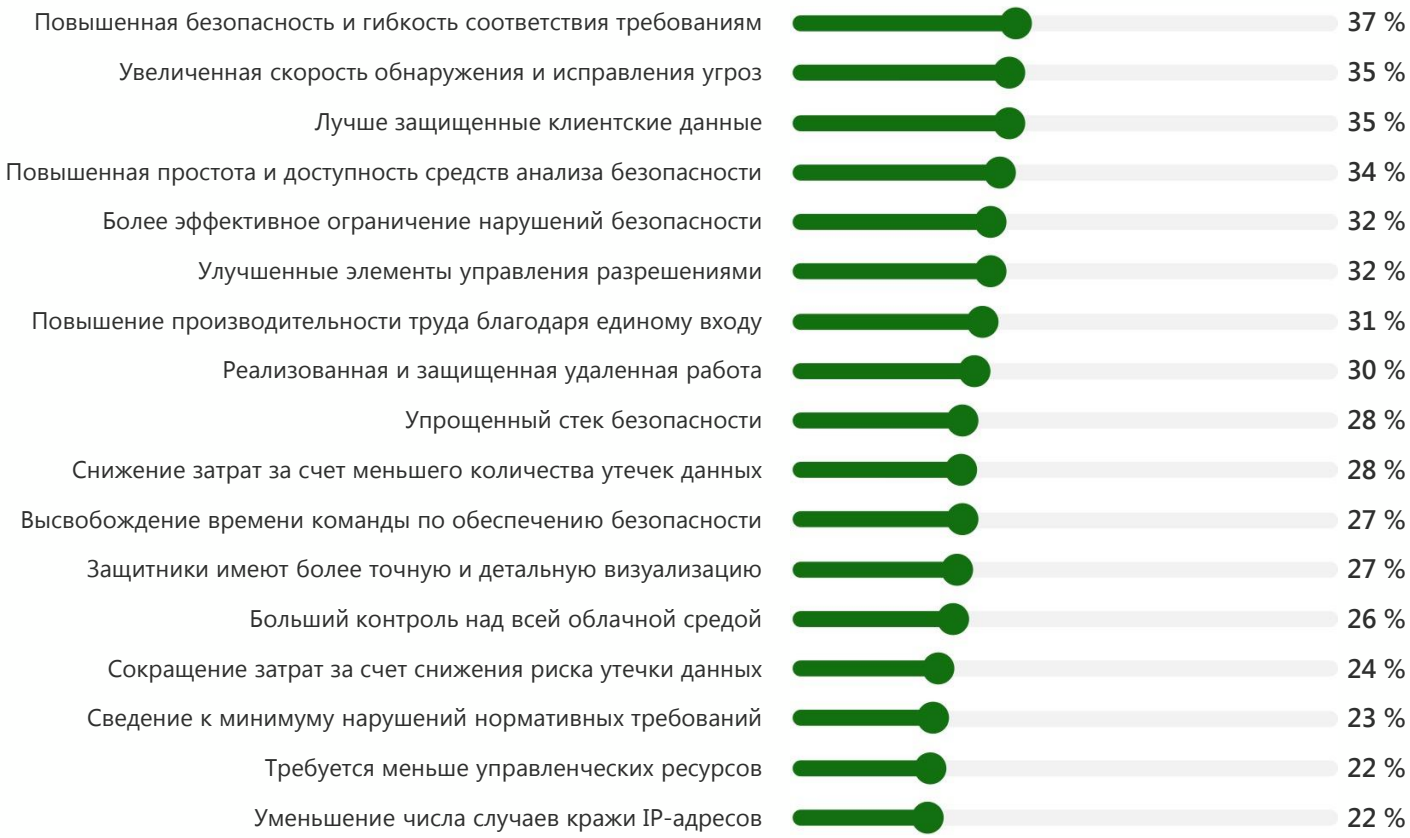
Гостиничный бизнес

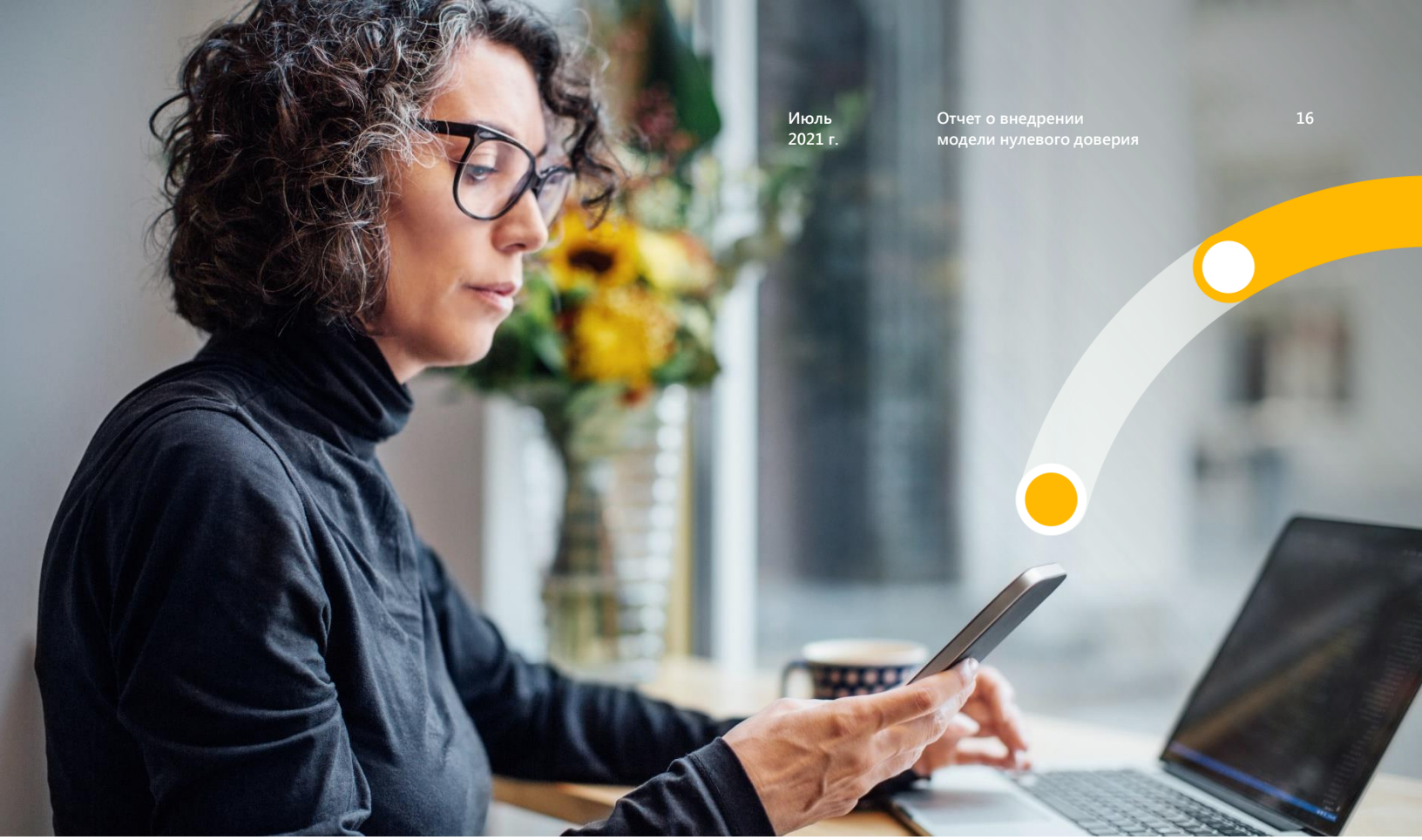
Как только организации начинают внедрять стратегию нулевого доверия, они получают основные преимущества, такие как повышение гибкости, скорости и уровня защиты. Преимущества ресурсов встречаются реже.

После реализации стратегии нулевого доверия организации получают выгоду от повышения гибкости (37 %), скорости (35 %) и защиты данных клиентов (35 %). (См. рисунок 8) Тем не менее, также реализуются прямые выгоды для сотрудников, включая высвобождение времени команды по обеспечению безопасности (27 %) и потребность в меньшем количестве ресурсов для управления инфраструктурой (22 %).

Важно отметить, что организации считают, что их стратегия нулевого доверия поможет им управлять большинством угроз и изменений в среде, особенно в отношении безопасности IoT и OT (47 %).

Рисунок 8. Преимущества внедрения модели нулевого доверия





Организации получают максимальную отдачу от внедрения стратегии нулевого доверия

79 % уверены в своей способности справляться с угрозами безопасности в целом, хотя эта уверенность ослабевает, когда угроза связана с фабрикацией правды: SDM чувствуют себя наименее уверенно в борьбе с угрозами, связанными с синтетическими удостоверениями личности (20 %) и дипфейками (10 %).

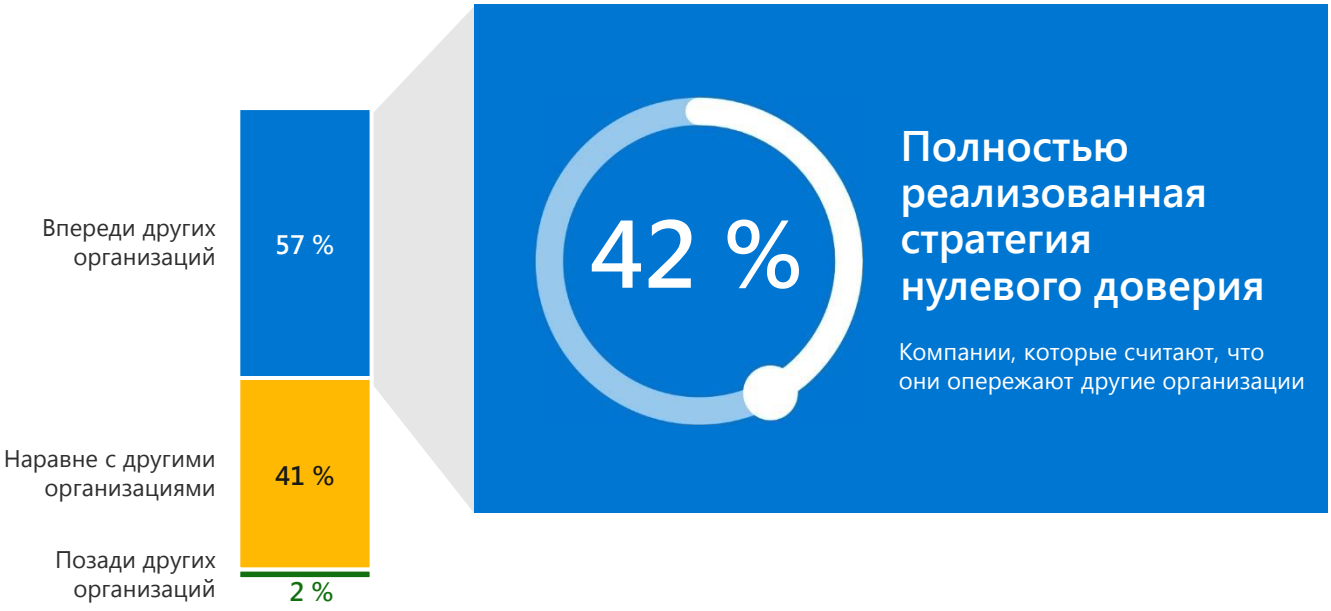
В свете полученных преимуществ модель нулевого доверия обычно вызывает положительные ассоциации. На четырех рынках SDM считают подход своих организаций одновременно практичным и амбициозным, описывая его как уверенный (37 %) и эффективный (31 %), а также мотивированный (25 %), вдохновляющий (25 %) и захватывающий (25 %). В частности, в Японии специалисты по безопасности описывают модель нулевого доверия как требовательную (27 %) и трансформационную (25 %), предполагая, что, несмотря на сложности реализации, она имеет долгосрочные преимущества.

Многие считают, что они опережают другие компании во внедрении модели нулевого доверия, но им еще больше предстоит сделать.

В то время как только 35 % организаций полностью реализовали свою стратегию нулевого доверия, 52 % сообщают, что они опережают свои планы, а 57 % считают, что они опережают другие организации. Организации считают, что они особенно сильно опережают другие, в Японии (66 %) и Австралии/Новой Зеландии (63 %). Несмотря на то, что модель заслуживает доверия на разных рынках, существует пропасть между восприятием и реальностью: среди утверждающих, что они опережают другие организаций, только 42 % сообщают, что полностью реализовали стратегию нулевого доверия. (См. рисунок 9)

Хотя многие организации уверены в стратегии нулевого доверия и чувствуют в себе уверенность справиться с будущими угрозами безопасности, им еще предстоит проделать большую работу для полного внедрения в областях риска. Например, среди организаций, которые считают, что их стратегия нулевого доверия полностью реализована, почти половина в настоящее время не реализовала стратегию в областях риска, причем инфраструктура и удостоверения реализованы с наименьшей вероятностью.

Рисунок 9. Сравнение реализаций модели нулевого доверия



	США	Германия	Япония	Австралия/ Н. Зеландия
Впереди	59 %	46 %	66 %	63 %
Наравне	40 %	52 %	34 %	32 %
Позади	2 %	2 %	0 %	6 %

Оценивая перспективы на ближайшие два года, стратегия нулевого доверия останется главным приоритетом безопасности.

Организации полностью поддерживают стратегию нулевого доверия, и лица, принимающие решения, говорят, что она будет оставаться главным приоритетом безопасности в течение следующих двух лет. Относительная важность стратегии нулевого доверия как инициативы в области безопасности, по прогнозам, возрастет (с 53 % до 58 %) к 2023 году, поскольку SDM ожидают, что стратегия останется критически важной для общего успеха (96 %). (См. рисунок 10)

Ожидаемая важность особенно высока среди японских организаций, причем 70 % сообщают, что стратегия нулевого доверия будет очень важна в ближайшие 2 года по сравнению с общим средним показателем в 56 %. Ожидается, что бюджеты внедрения стратегии нулевого доверия также вырастут: 73 % организаций ожидают увеличения своих бюджетов. Однако эта цифра немного ниже в Германии (67 %), где 31 % ожидают, что их бюджеты останутся прежними. (См. рисунок 11)

Рисунок 10. Ожидаемая важность модели нулевого доверия в ближайшие два года

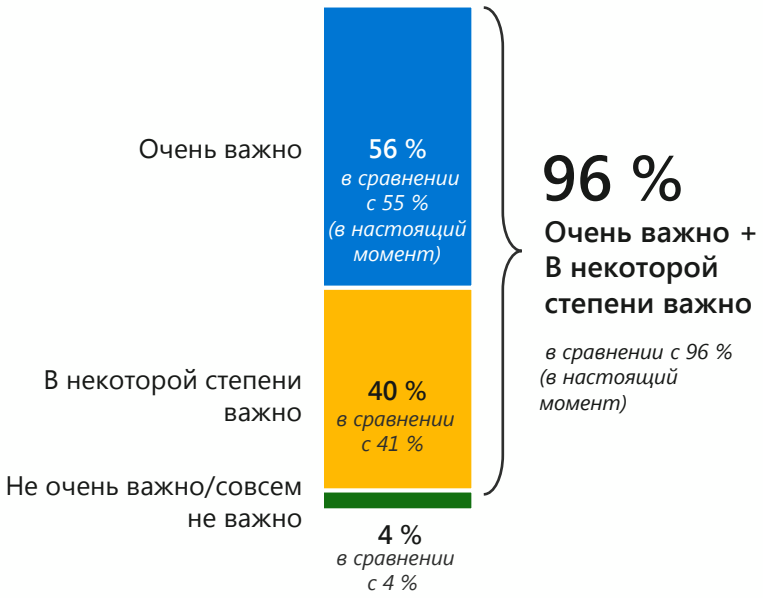
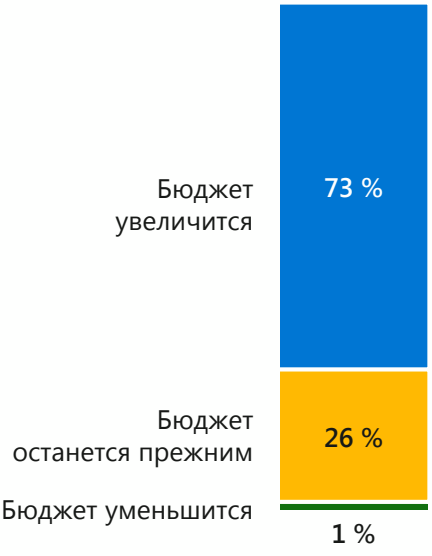
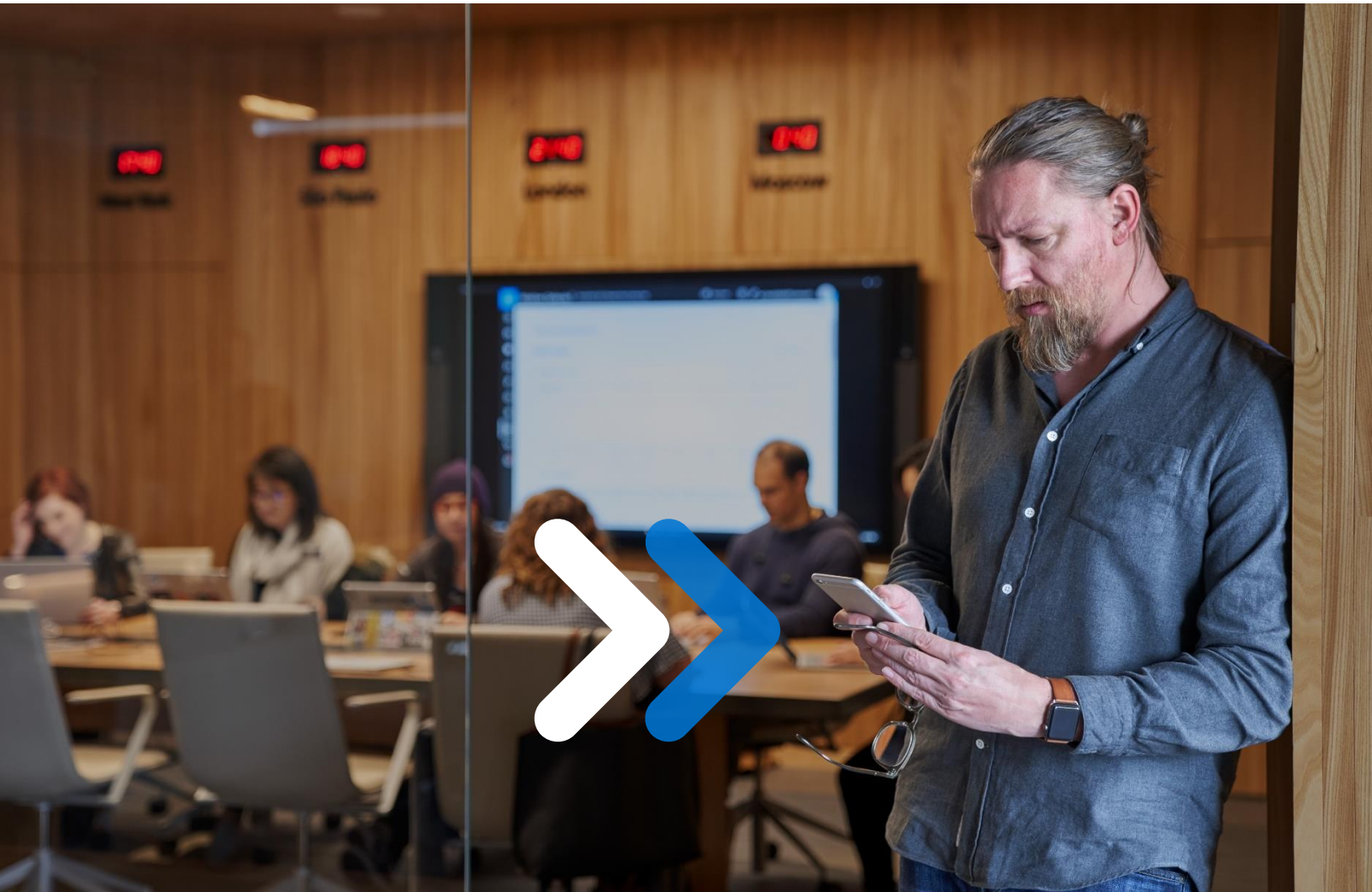


Рисунок 11. Ожидаемый бюджет модели нулевого доверия в следующие два года



Доказательство успеха стратегии нулевого доверия может стимулировать дальнейшие инвестиции

Организации, внедряющие модель нулевого доверия, рассчитывают удвоить свои инвестиции в ближайшие два года, а те, кто еще не начал ее внедрять, рискуют еще больше отстать. Эти организации не только отстают от своих коллег, полностью выполнивших внедрение, когда речь заходит о приоритизации модели нулевого доверия в планах безопасности (42 % в сравнении с 66 %) и ожидаемом увеличении бюджета (66 % в сравнении с 72 %), но также чувствуют себя значительно менее уверенными в управлении безопасностью IoT и OT в будущем (40 % в сравнении с 53 %).



Решение проблем с собственными сотрудниками станет ключом к удвоению инвестиций в реализацию стратегии нулевого доверия

Несмотря на быстрый прогресс во внедрении стратегии нулевого доверия, организации должны преодолеть множество проблем, чтобы продвинуться дальше в реализации. (См. рисунок 12) Проблемы с ресурсами и лидерством наиболее распространены в этих категориях. Время, необходимое для реализации стратегий нулевого доверия, и отсутствие поддержки со стороны высшего руководства возглавляют список препятствий, причем последнее особенно заметно в Австралии и Новой Зеландии (65 %).

Кроме того, бюджетные ограничения, которые 45 % организаций считают препятствием, вероятно также играют роль в проблемах с ресурсами и лидерством.

Например, 21 % SDM ссылаются на трудности с доказательством рентабельности инвестиций в модель нулевого доверия и называют их препятствием для реализации, которое может привести к отсутствию поддержки высшего руководства. Поскольку рынки за пределами США с большей вероятностью имеют бюджетные ограничения (60 % организаций в Японии, 57 % организаций в Германии, 57 % организаций в Австралии и Новой Зеландии), возможно, это имеет волновой эффект, что приводит к снижению и замедлению реализации стратегий нулевого доверия в Японии, Германии и Австралии и Новой Зеландии по сравнению с США.

Рисунок 12. Препятствия при внедрении модели нулевого доверия

Проблемы с ресурсами 60 %	Руководство 53 %	Технологии 46 %	Поставщики 46 %	Ограничения бюджета 45 %
20 % Занимает слишком много времени для реализации	**20 %** Отсутствие поддержки со стороны высшего руководства	**21 %** Сложность интеграции решений безопасности	**21 %** Нуждаются в поддержке внедрения поставщиками	**21 %** Стоимость реализации стратегии нулевого доверия
19 % Отсутствие управления внутренними изменениями	**19 %** Отсутствие поддержки со стороны заинтересованных сторон	**19 %** Несовместимость с устаревшими системами	**21 %** Трудности с определением подходящих поставщиков	**21 %** Сложность подтверждения окупаемости инвестиций
18 % Нуждаются в дополнительных учебных материалах	**19 %** Нужна помощь, чтобы подготовить убедительное бизнес-обоснование	**19 %** Сложность масштабирования в организации	**17 %** Отсутствие возможности найти инновационных партнеров	**14 %** Отсутствие достаточно большого бюджета
17 % Не требуется для организации нашего размера	**18 %** Отсутствие организационной поддержки			
16 % Отсутствие необходимой квалификации для правильной реализации				

«Первоначально поддержка была слабой, но когда мы, как заинтересованные лица, согласились с тем, что будем инвестировать в этот проект, все приступили к работе».

Лица, принимающие решения в области безопасности в США

Финансово-технологическая компания

Лица, принимающие решения в области безопасности, имеют небольшую склонность к выбору комплексных или консолидированных поставщиков

При выборе поставщика модели нулевого доверия организации сталкиваются с выбором лучшего из своего класса или лучшего из своего рода. Первая стратегия включает в себя покупку набора продуктов для всей архитектуры нулевого доверия у комплексного или консолидированного поставщика. Это решение, которое, по мнению SDM, предлагает больше опыта, ресурсов и простоты тем, кто привязан к ресурсам. Однако проблемы, связанные с этим подходом, включают повышенную уязвимость и отсутствие гибкости. (См. рисунок 13)

Последняя стратегия, «лучший в своем роде», предполагает получение отдельных технологических компонентов модели нулевого доверия от специализированных поставщиков. В отличие от подхода «лучший в своем классе», эта стратегия опирается на поставщиков, которые специализируются в разных областях и, таким образом, предлагают большую гибкость и могут более точно соответствовать стратегии организации. Тем не менее, специалисты по безопасности считают, что лучшие в своем роде поставщики стоят дороже, требуют больше ресурсов, препятствуют прозрачности и имеют недостатки, которые в конечном итоге приводят к проблемам с поставщиками и бюджетом. (См. рисунок 14)

В то время как организации в значительной степени разделены, незначительное большинство SDM (55 %) предпочитают работать с комплексными (лучшими в своем классе) поставщиками. (Организации в Австралии и Новой Зеландии, однако, склоняются к противоположному выбору, причем 52 % предпочитают лучших в своем роде.)

Рисунок 13. Преимущества и препятствия подхода «лучший в своем классе» — относится к Топ-2

⊕ Преимущества подхода «лучший в своем классе»	
Поставщик обладает отраслевым опытом в реализации различных решений	24 %
Дополнительные ресурсы помогают планировать внедрение стратегии нулевого доверия	23 %
Упрощенный стек безопасности	22 %

⊖ Недостатки подхода «лучший в своем классе»	
Зависимость от одного поставщика повышает уязвимость	34 %
Требует более сложной интеграции с устаревшей архитектурой	33 %
Меньшая гибкость специальных функций	29 %

Рисунок 14. Преимущества и препятствия подхода «лучший в своем роде» — относится к Топ-2

⊕ Преимущества подхода «лучший в своем роде»	
Гибкость в поиске лучших решений для любого компонента стратегии нулевого доверия	33 %
Можно более тесно согласовать решение с архитектурой или стратегией организации	30 %
Расширение возможностей для инноваций благодаря различным поставщикам	26 %

⊖ Недостатки подхода «лучший в своем роде»	
Повышенные затраты	29 %
Невозможность обмена данными между различными решениями	26 %
Большой объем решений для внедрения и управления внутренними командами	26 %

Заключение

Поскольку риски безопасности становятся не только более частыми, но и более опасными, организации на разных рынках и в отраслях выбирают стратегию нулевого доверия, которая действует по принципу «никогда не доверяй, всегда проверяй». Стратегия нулевого доверия является главным приоритетом безопасности для организаций, которые стремятся улучшить общую безопасность, удобство работы конечных пользователей и производительность, а также упростить процедуры безопасности для сотрудников и сократить расходы. Однако несмотря на то, что преимущества стратегии нулевого доверия хорошо известны, ограниченные ресурсы и скептицизм среди руководства стоят на пути ее повсеместной реализации.

Внедрение стратегии нулевого доверия ускорилось за последние три года отчасти из-за пандемии COVID-19. Важно отметить, что переход к удаленной и гибридной работе способствует более широкому внедрению подходов нулевого доверия, что должно защитить системы и данные, даже когда сотрудники получают к ним доступ за пределами корпоративной сети и иногда на личных устройствах. Ускоренное внедрение из-за пандемии COVID-19 является хорошим показателем готовности к внедрению модели нулевого доверия в целом, причем организации, которые реализовали стратегию во время пандемии, внедрили ее в большем количестве областей риска, чем их коллеги.

Тем не менее, даже у самых продвинутых последователей стратегии нулевого доверия осталась незавершенная работа и неправильное восприятие организациями своей собственной зрелости в вопросе внедрения модели нулевого доверия может создать уязвимость, о которой они могут даже не знать.

Большинство организаций на разных рынках считают, что важность стратегии нулевого доверия будет только расти со временем, и ожидают, что их бюджеты, в свою очередь, увеличатся. Этот ожидаемый сдвиг в расстановке приоритетов особенно важен для рынков за пределами США, где бюджетные проблемы являются заметным препятствием для внедрения. Полное осуществление внедрения может казаться невыполнимым с финансовой и материально-технической точки зрения. Тем не менее, преимущества подхода нулевого доверия неоспоримы, и Microsoft будет направлять и поддерживать организации, когда они приступят к этому процессу.

Чтобы узнать больше о модели нулевого доверия и оценить зрелость организации в вопросах внедрения модели нулевого доверия, посетите

aka.ms/zerotrust

Детализированные цели исследования и характеристики аудитории

Цели исследования:

Понимание текущего состояния подходов к внедрению модели нулевого доверия

Изучение образа мышления, рекомендаций, преимуществ и проблем подходов к внедрению модели нулевого доверия

Оценка перспектив подходов к внедрению модели нулевого доверия

Контекстуализация инноваций и тенденций в подходах к внедрению модели нулевого доверия

Чтобы соответствовать критериям отбора, лица, принимающие решения в области безопасности, должны:

отвечать за безопасность в своей организации, включая кибербезопасность, операции по обеспечению безопасности, защиту от угроз, управление идентификацией, управление рисками, безопасность приложений, цифровую криминалистику и реагирование на инциденты;

работать полный рабочий день в крупной компании (более 1000 сотрудников в США; более 500 сотрудников в Германии/Японии/Австралии/Новой Зеландии);

быть в возрасте 25–75 лет;

быть знакомыми с моделью нулевого доверия;

принимать участие в принятии решений по разработке/реализации стратегии нулевого доверия.

Из 911 лиц, принимающих решения в области безопасности, опрошенных в рамках исследования в апреле 2021 года:

В США опрошено 477 человек

В Германии опрошен 201 человек

В Австралии и Новой Зеландии опрошено 126 человек

В Японии опрошено 107 человек

Примечание. Исследования проводились во время глобальной пандемии COVID-19, которая находилась на различных стадиях эскалации/сдерживания.

Microsoft Security hypothesis