



Защита и контроль доступа к приложениям с помощью **Azure Active Directory**



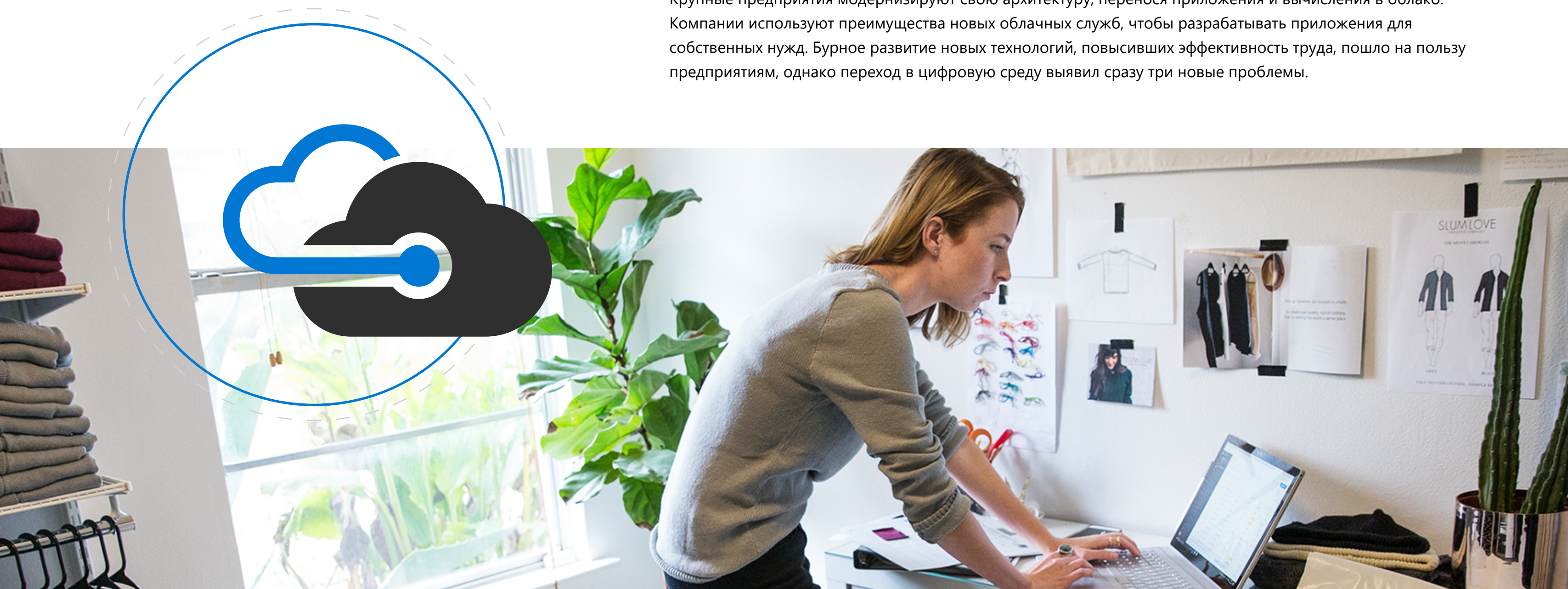
Раздел 1

Что такое система управления
идентификацией и доступом?

Что такое система управления идентификацией и доступом?

Переход на цифровые технологии

Появление облачных вычислений и мобильных устройств привело к преобразованию современной рабочей среды. Благодаря все более интенсивной глобализации трудовых ресурсов нынешние специалисты могут перейти на удаленную работу с помощью бесплатных или недорогих приложений типа программное обеспечение как услуга (SaaS), которые позволяют решить проблемы продуктивности и взаимодействия. Крупные предприятия модернизируют свою архитектуру, перенося приложения и вычисления в облако. Компании используют преимущества новых облачных служб, чтобы разрабатывать приложения для собственных нужд. Бурное развитие новых технологий, повысивших эффективность труда, пошло на пользу предприятиям, однако переход в цифровую среду выявил сразу три новые проблемы.



Что такое система управления идентификацией и доступом?

Новые проблемы

Сложности
перехода на
цифровые
технологии

Угроза безопасности. До появления революционных облачных технологий ИТ-средства использовались в качестве своеобразной охранной службы. Управляемые и защищаемые приложения и платформы находились внутри сетевого периметра. Чтобы получить доступ к корпоративным ресурсам, пользователь сначала должен был пройти проверку брандмауэра. Эти времена остались в прошлом. Теперь работники лучше контролируют службы и приложения, которыми пользуются и для доступа к которым часто требуется Интернет. Киберпреступники научились использовать эти уязвимости. Даже если пользователь указывает верный пароль для учетной записи, не факт, что он тот, за кого себя выдает.

Проблемы администрирования. Число конечных точек стремительно растет. В результате пользователи получают больше возможностей для общения и взаимодействия, а администраторы — новые заботы и тревоги. На многих предприятиях толком не знают, какими средствами пользуются сотрудники, но даже если составить подробный перечень, проблема не исчезнет. Из-за огромного числа облачных приложений приходится контролировать множество систем идентификации, что ведет к увеличению затрат и усугублению уже существующих рисков безопасности.

Неудобная в использовании среда. Пользователи тоже испытывают трудности: им нравятся гибкие возможности нового рабочего места, но раздражает необходимость держать в голове массу учетных данных.



Угроза
безопасности



Проблемы
администрирования



Неудобная
в использовании среда

Что такое система управления идентификацией и доступом?

Управление идентификацией и доступом как ядро системы контроля

Главная причина вышеизложенных проблем заключается в неэффективности систем проверки удостоверений. Удостоверения заменили сетевой периметр и стали основным элементом контроля. Сейчас нужны решения, которые позволили бы объединить различные инструменты, архитектуры, устройства и службы предприятия и при этом надежно защитить корпоративную среду. Это должна быть единая платформа с общей схемой доступа, способная контролировать системы идентификации и доступа (IAM), которыми пользуются сотрудники предприятия и внешние партнеры. Только так можно обеспечить полноценное управление ИТ-средой, удобные средства взаимодействия, не скованные границами одной организации, и надлежащую защиту корпоративных ресурсов. Хорошее IAM-решение позволяет подключаться ко всем рабочим приложениям, облачным и локальным, с помощью одного набора учетных данных. IAM-решения разрабатываются так, чтобы предоставлять пользователям доступ только к тем ресурсам, которые им действительно нужны, и пресекать несанкционированные попытки просмотреть или использовать данные, которые их не касаются. Для управления разрешениями пользователей и их правами на доступ используется централизованный портал, что существенно сокращает объем ручных операций по подготовке и аннулированию учетных записей пользователей. IAM-решения также предоставляют средства для управления политиками безопасности в отношении удостоверений и приложений. Лучшие IAM-решения повышают уровень безопасности удостоверений и эффективность администрирования, а также обеспечивают пользователям больше удобств при работе.

IAM-решения
позволяют
устранить эти
проблемы



Надежная защита
удостоверений



Удобная рабочая
среда



Эффективное
администрирование

Раздел 2

Обзор Azure AD

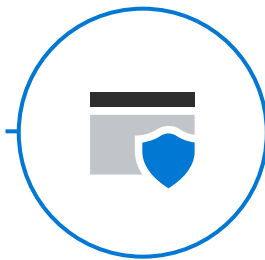
Универсальное решение

Microsoft Azure Active Directory (Azure AD) — это универсальная облачная IAM-система, одна из лучших в сегменте управления каталогами, доступа к приложениям и расширенной защиты удостоверений. Azure AD позволяет организациям успешно контролировать и защищать удостоверения своих сотрудников, партнеров и клиентов, предоставляя доступ только к тем приложениям и службам, которые им действительно требуются. Миллионы организаций используют Azure AD для контроля и защиты более 1 млрд удостоверений.



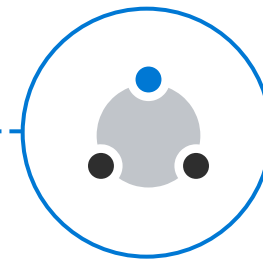
Модернизация средств доступа

Контролируйте и защищайте доступ к облачным и локальным данным и ресурсам организации. Подключите всех ваших пользователей, приложения и устройства к облаку. Таким образом вы обеспечите им гибкий и безопасный доступ, а себе — больше возможностей для слежения и управления. Автоматизируйте рабочие процессы и предоставляйте возможности для самообслуживания, чтобы минимизировать затраты и повысить продуктивность пользователей.



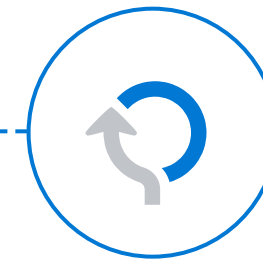
Защита и управление

Ежедневно совершается огромное количество атак на удостоверения. Чтобы предотвратить их компрометацию, необходимо следить за поведением объектов сети, вовремя выявляя отклонения. Для этого используется широчайший набор сигналов, функции искусственного интеллекта и автоматические отклики. Чтобы не жертвовать безопасностью в угоду эффективности, предоставляйте доступ к требуемым ресурсам на определенный срок, регулярно пересматривайте права доступа и принудительно применяйте политики.



Общий доступ и совместная работа

Расширьте свой бизнес с помощью надежной облачной службы, которая способна охватить миллионы пользователей и обладает лучшей в отрасли гибкостью и системой безопасности. Налаживайте связь с внешними пользователями и помогайте им эффективно справляться с задачами благодаря удобным приложениям и службам с функциями самообслуживания и встроенными элементами управления безопасностью.



Разработка и интеграция

Создавайте приложения, которые обеспечат пользователям простую схему входа в личную, учебную или рабочую учетную запись Майкрософт либо в учетные записи социальных сетей. Для начала подключитесь к Microsoft Graph, чтобы открыть доступ к данным и аналитике Microsoft 365, и разрабатывайте функциональные приложения. Задействуйте единый вход, автоматизируйте подготовку пользователей и наладьте связи с крупнейшими мировыми компаниями.

Раздел 3

Azure AD для
приложений

Azure AD для приложений

Универсальная платформа

Azure AD позволяет управлять стандартными удостоверениями всех пользователей гибридной инфраструктуры, чтобы обеспечить им доступ ко всем необходимым приложениям, включая облачные и локальные бизнес-приложения. Управляйте всеми удостоверениями с помощью универсальной платформы, которая повышает эффективность администрирования и обеспечивает больше контроля. Применяйте детальные политики безопасности к каждому приложению, которое используется организацией.



Экономия времени и денег

С Azure AD предварительно интегрированы тысячи приложений, в том числе такие популярные службы, как Workday, ServiceNow, SuccessFactors, Adobe и Concur, поэтому вам не составит труда обеспечить пользователям доступ к ним. Одна-единственная консоль позволяет развернуть согласованные политики и следить за правами доступа. Вы можете автоматизировать процессы подготовки пользователей и управления жизненным циклом, а также сэкономить время и ресурсы, внедрив самостоятельное управление учетными записями. Вы также можете получать информацию о новых пользователях от систем управления персоналом, используя их как источник подлинных данных. Это избавит вас от необходимости писать собственные сценарии или применять ручные процессы для управления атрибутами пользователей.

Приложения, настроенные с помощью Azure AD, поддерживают единый вход, а значит, пользователям не придется запоминать множество учетных данных или рисковать безопасностью информации из-за ненадежных паролей. Учетные записи, подготовка которых осуществляется автоматически, позволяют максимально быстро предоставить пользователям доступ к новым ресурсам. Подготовка новых пользователей в Azure AD поможет вам предоставить новым сотрудникам доступ ко всем требуемым ресурсам с первого дня работы.



**Экономия
времени и денег**



**Встроенные
интеграции SaaS**



Единый вход



**Доступ к нужным
ресурсам с первого
дня работы**

Более безопасный доступ ко всем вашим приложениям

Azure AD обеспечивает всестороннюю защиту удостоверений во всех ваших приложениях: SaaS и локальных бизнес-приложениях. Неважно, к какому приложению пользователь запрашивает доступ — к Microsoft Word или Box, — сначала ему придется пройти проверку Azure AD, которая должна подтвердить его удостоверение. Кроме того, можно установить политики управления доступом, которые будут предоставлять пользователям доступ только к требуемым данным и только на время. Можно сделать так, что пользователи будут запрашивать разрешение на доступ, а также ограничить время использования приложения. Вдобавок можно регулярно проверять процесс предоставления доступа на соответствие требованиям.

Azure AD также использует возможности Microsoft Intelligent Security Graph и машинного обучения, чтобы анализировать миллиарды сигналов, поступающих от наших продуктов и служб, выявлять признаки нетипичного поведения и определять относительный уровень риска для каждого сеанса. Оценивая риски, связанные со входом, Azure AD учитывает устройство, расположение и другую контекстную информацию. В Azure AD можно задать политики условного доступа, которые будут автоматически применять меры безопасности (блокировка запроса доступа, требование смены пароля и др.), если вход оценивается как сопряженный с риском либо в соответствии с условиями конкретной политики.



Меры по обеспечению
безопасности
приложений



Защита
удостоверений



Управление
доступом



Политики
условного доступа

Раздел 4

Контроль и защита приложений с помощью Azure AD

Azure AD позволяет без труда контролировать процессы и сокращать затраты за счет автоматизации, самообслуживания и принудительного применения политик.

Контроль и защита приложений с помощью Azure AD



Интеграция с приложениями Azure AD

Вы можете легко настроить и подключить к вашему клиенту любое из тысяч предварительно интегрированных приложений из коллекции приложений Azure AD. Все они поддерживают единый вход, к тому же для них нетрудно настроить условный доступ Azure AD, который будет предоставляться в зависимости от приложения или которым будут управлять политики, действующие в масштабах всего предприятия. Как только вы добавите приложение и настроите его так, как вам нужно, пользователи с соответствующими правами доступа смогут без труда найти его в разделе "Мои приложения" на портале Azure AD. (На этом централизованном портале конечные пользователи могут находить и запускать требуемые приложения.)

Если вы создали свое приложение или хотите интегрировать существующее приложение в вашу корпоративную систему, вы можете отправить запрос, чтобы его включили в коллекцию приложений Azure AD.

[Узнать больше о тысячах предварительно интегрированных приложений >](#)



Безопасный гибридный доступ

Служба Azure AD Application Proxy обеспечивает безопасный удаленный доступ к локальным и веб-приложениям, основанным на утверждениях, для которого не требуется виртуальная сеть. Для службы App Proxy нужно установить облегченный соединитель. Пользователи и ИТ-специалисты могут работать с ней так же, как с приложениями SaaS, подключенными через коллекцию приложений Azure AD.

Если же вы хотите оправдать вложения в существующую инфраструктуру, затраченные на услуги таких партнеров, как F5 ZScaler, SAP, Oracle, Ping Identity и др., и подключить другие типы приложений (например, использующие протоколы проверки подлинности на основе заголовков или Kerberos), то вы можете это сделать, сохранив все преимущества централизации и безопасности Azure AD.

[Узнайте, как добавить локальное приложение с помощью App Proxy >](#)

[Подключиться к облакам и сетям приложений других партнеров >](#)

Контроль и защита приложений с помощью Azure AD



Автоматизированная подготовка

Azure AD позволяет автоматизировать создание, обслуживание и удаление пользовательских удостоверений в популярных приложениях SaaS. Вы можете автоматически создавать новые учетные записи в требуемых системах для новых сотрудников, присоединившихся к вашей команде или организации. Можно также настроить политики, которые будут автоматически отключать учетные записи уволенных или переведенных в другой отдел сотрудников в соответствующих системах. Автоматизация этих задач позволяет поддерживать актуальное состояние удостоверений в приложениях и системах, которое отражает изменения в каталоге или в вашей системе управления персоналом, что экономит время и сокращает количество ошибок.

[Подробнее о том, как настроить автоматическое предоставление доступа к приложениям SaaS и его отзыв >](#)



Управление группами

Azure AD позволяет обеспечить доступ к корпоративным ресурсам, предоставив соответствующие права одному пользователю или целой группе Azure AD. Используя группы, владелец ресурса может настроить разрешения доступа сразу для всех участников группы, а не предоставлять права каждому поочередно. Это более безопасный метод, так как в этом случае меньше вероятность, что вы случайно предоставите кому-то слишком много прав. К тому же так вы экономите время. Управление группой поддерживает динамическое масштабирование, так что вы можете автоматизировать регистрацию устройств, используя политики на основе атрибутов удостоверений.

[Подробнее о том, как создать группу на портале Azure >](#)

Контроль и защита приложений с помощью Azure AD



Самообслуживание пользователей

Для выполнения некоторых задач не обязательно привлекать ИТ-специалистов, поэтому Azure AD позволяет задействовать других сотрудников организации. Вы можете предоставить пользователям возможность создавать собственные группы безопасности в Azure AD и управлять ими. Владельцы групп могут принимать или отклонять запросы на членство в группе, а также передавать это право другому сотруднику.

[Настройка самоуправляемых групп >](#)

Обычным пользователям тоже доступны функции самообслуживания. Они могут регистрироваться для получения учетной записи через портал самообслуживания, если у них есть проверенный адрес электронной почты. На этот же портал нужно зайти, чтобы сбросить пароли. Эти возможности сэкономят вашей службе поддержки массу времени и средств.

[Настроить самостоятельный сброс пароля](#)



Модернизация проверки подлинности

Если в настоящий момент вы используете локальную службу проверки подлинности, например службы федерации Active Directory (AD FS), вы можете рассмотреть вопрос о переносе ваших приложений в Azure AD. Как пользователь вы сохраните все преимущества, такие как единый вход, и вдобавок сможете пользоваться возможностями облака в отношении масштабирования и безопасности, например, тщательно контролировать доступ к каждому приложению с помощью условного доступа Azure AD или предоставлять партнерам доступ к ресурсам с помощью средств совместной работы Azure AD B2B. Миграцию поддерживают все приложения, использующие стандарты SAML 2.0, WS-Federation, OAuth или OpenID Connect для федеративного входа.

[Создайте политики условного доступа Azure AD для безопасного доступа к вашим приложениям >](#)

[Используйте Azure AD B2B, чтобы наладить гибкую совместную работу с внешними партнерами >](#)

Безопасно подключайте к Azure AD любое приложение из любого облака и с любого сервера.

Уже подключен
1 миллион уникальных
активных приложений.



Начните прямо сегодня.

[Пользуйтесь бесплатной пробной версией Azure AD в течение месяца](#) и узнайте, как легко можно наладить управление доступом пользователей ко всем вашим приложениям и обеспечить безопасность предприятия.

