Глобальные сетевые тенденции

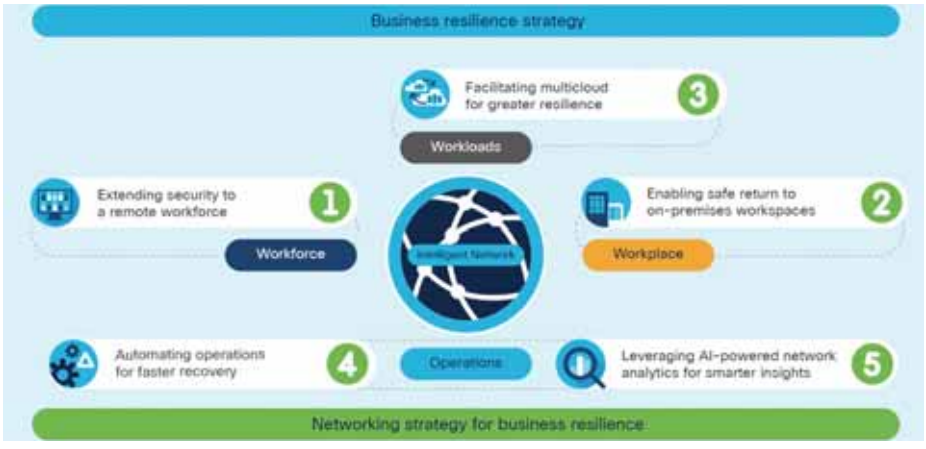
Чтобы встретить следующий кризис во всеоружии, Cisco предлагает руководителям ИТ-служб и ИТ-специалистам по вопросам стратегии развития ознакомиться с «Отчетом о глобальных сетевых тенденциях» (Global Networking Trends Report), в котором не только изложены последние сетевые тренды, но и предлагаются рекомендации, как действовать в тех или иных условиях, и приводится статус внедрения ряда технологий, которые могут в этом помочь.

COVID-19

Очевидно, что предприятия по всему миру, как и частные лица, оказались не готовыми к глобальному, долгосрочному кризису, который обрушил на них COVID-19. Так, многие компании и организации оказались в ситуации, когда им буквально за одну ночь необходимо было перевести весь коллектив на удаленную работу. Кто-то пытался скорее перевести все свои товары и услуги в онлайн, кто-то менял цепочки поставок, отыскивая новых поставщиков. Конечно, это было серьезное испытание, но давайте не забывать о том, что кризисы случались с компаниями и ранее. По данным PwC: Global Crisis Survey 2019, семь из десяти организаций пережили как минимум один серьезный кризис за последние пять лет, при этом 95% опрошенных были абсолютно уверены, что этот кризис на их веку не последний.

Сегодня уже не надо никого убеждать в том, что все критически важные бизнес-процессы компаний и организаций (даже целых государств) зависят от все более сложной системы цифровых технологий и платформ, которые обеспечивают фундамент для достижения организационной жизнестойкости. Всем понятно, что пережить последствия пандемии COVID-19 без опоры на современные ИТ было бы невозможно. За прошедший год ИТ-службы по всему миру приложили огромные усилия, обеспечивая работу сетей, без которых большинству организаций пришлось бы, скажем мягко, намного хуже.

«За период пандемии мир изменился очень сильно. Инструменты и решения, ускоряющие цифровую трансформацию, стали играть еще более важную роль, – комментирует Андрей Кузьмич, директор по технологиям Cisco в России. – Компания Cisco, являясь лидером рынка цифровой трансформации и во многом формируя направления его развития, традиционно публикует сетевую аналитику, которая помогает тысячам компаний по всему миру развивать свои корпоративные сети. Уверен, что данное исследование поможет нашим заказчикам сфокусироваться на наиболее важных технологических тенденциях и наилучшим способом адаптировать свои бизнесы к «новой нормальности».



Пять сетевых трендов укрепления жизнестойкости бизнеса с учетом растущей вероятности кризисов

Новые времена — новое ИТ-мышление

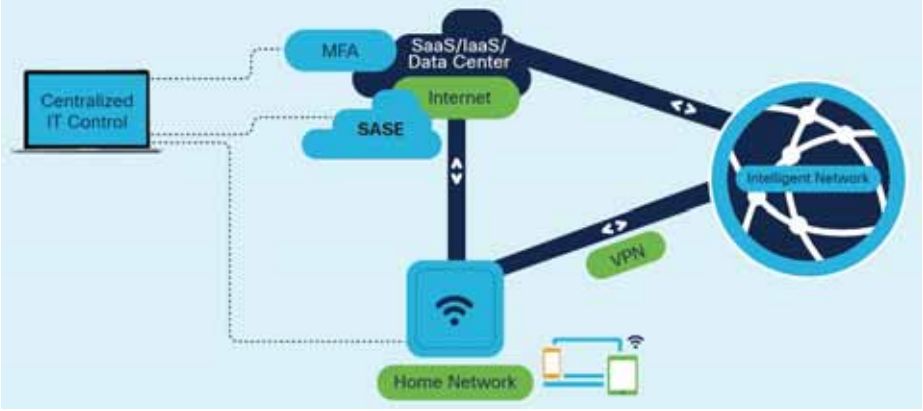
Для успешного преодоления кризиса ИТ-руководителям придется принять новый образ мышления: сделать основной акцент на гибкости ИТ, которая необходима для достижения жизнестойкости бизнеса; пора уходить от реактивного (предполагающего действия по последствиям) к проактивному (прогнозирование событий) подходу. Традиционное планирование «непрерывности бизнеса» в наше время не срабатывает. Для устойчивого ведения бизнеса организация или компания должна быть готова к любым неожиданностям и воспринимать их как данность, а не как снежный ком, случайно упавший на голову.

Здесь решаются сразу две фундаментальные задачи. Непрерывность бизнеса: способность организации продолжать предоставление

продуктов или услуг на приемлемых, заранее определенных уровнях, даже после серьезного сбоя в работе. Жизнестойкость бизнеса: способность организации адаптироваться к моментально меняющейся среде и достигать поставленных целей, причем не просто выживать, а процветать. При этом планирование бизнеса, основываясь на принципах непрерывности, обязано сегодня выходить за традиционные рамки непрерывности и ориентироваться на жизнестойкость. Организациям необходимо умение адаптироваться как к вполне предсказуемым, так и к неожиданным дестабилизирующим факторам. Жизнестойкость бизнеса помогает укрепить «иммунную систему» организации, чтобы бизнес мог легко справляться с проблемами.

Традиционной (классической) устойчивости сети, которая только поддерживает сетевое подключение и время безотказной работы, уже недостаточно. Компаниям сегодня нужна качественно иная устойчивость, обеспечиваемая передовой сетевой платформой, которая может быстро реагировать на любые новые обстоятельства, задействовать новые операционные модели и услуги, интегрироваться с ИТ-процессами и защищать своих сотрудников, основные виды деятельности компании, клиентов и бренд. Фактически мы в нескольких фразах описали ту самую передовую модель сети новой эпохи, которая необходима для поддержки инициатив цифровой трансформации.

Парой абзацев выше мы сопоставили два ключевых понятия: непрерывность бизнеса и жизнестойкость бизнеса (Business continuity и Business resilience). Теперь же копнем немного глубже и перейдем к следующей паре: устойчивость сети и сетевая стратегия для жизнестойкости бизнеса (Network resilience и Business resilience networking). Мы специально поставили в скобках английские варианты понятий, чтобы бросилось в глаза следующее обстоятельство: в этих четырех терминах три раза повторяются слова



Разверните границу служб безопасного доступа Cisco SASE, чтобы обеспечить защиту доступа в многооблачной среде

Business (бизнес) и resilience (жизнестойкость, устойчивость, упругость, эластичность), так что сразу понятно, в каком направлении идет рассуждение.

Итак, устойчивость сети (в классическом понимании) подразумевает ее способность обеспечивать и поддерживать приемлемый уровень обслуживания, несмотря на сбои и проблемы в нормальной работе конкретной сети связи, благодаря подготовленным средствам. А новая сетевая стратегия для жизнестойкости бизнеса подразумевает наличие такой сети, которая обязана обеспечить для организации возможность быстро, безопасно, а главное – эффективно реагировать как на ожидаемые, так и неожиданные трудности.

Чтобы помочь бизнесу оценить и развить свои стратегические планы, Cisco подготовила «Отчет о глобальных сетевых тенденциях 2021: Специальное издание «Жизнестойкость бизнеса» (2021 Global Networking Trends Report: Business Resilience Special Edition). Его основная тема почти дословно совпадает с последним из представленных терминов – сетевая стратегия как фундамент стратегии обеспечения жизнестойкости бизнеса. Компания Cisco выделила пять сетевых трендов.

- Тренд 1. Безопасный удаленный доступ.
- Тренд 2. Интеллектуально-доверенные рабочие места.
- Тренд 3. Многооблачные сети.
- Тренд 4. Автоматизация сети.
- Тренд 5. Обеспечение работоспособности сервисов с применением AI.

Безопасный удаленный доступ

Все большее число организаций по всему миру постепенно приходят к пониманию того, что новые, более гибкие подходы к работе – это не какой-то временный авральный режим «ковидной действительности», а наше будущее, наша «новая нормальность» или «новая реальность» – называйте ее как вам удобнее – для собственных сотрудников.

При использовании своих личных устройств для удаленного доступа к корпоративным приложениям и данным сотрудники на дому становятся особенно уязвимыми для атак кибермошенников. Многие сегодня легко обходят VPN и подключаются напрямую к сервисам и корпоративным приложениям в общедоступном облаке, которое остается самой сложной средой для защиты.

Для реализации масштабных моделей безопасной работы из дома ИТ-командам следует придерживаться определенной тактики:

- масштабируйте виртуальные частные сети для защиты своих удаленных сотрудников – корпоративные VPN по-прежнему являются одними из самых эффективных и быстрых способов обеспечить контроль и защиту на уровне предприятия для удаленных клиентов;

используйте MFA – многофакторную аутентификацию (Multi-Factor Authentication) для защиты приложений. MFA проверяет личность пользователя, прежде чем разрешить ему доступ в корпоративную сеть или к конфиденциальным приложениям и данным, критически важным для защиты организации;
- разверните границу служб безопасного доступа (Cisco SASE – Secure Access Service Edge), чтобы обеспечить защиту доступа в многооблачной среде. Этот инструмент от компании Cisco помогает защищаться от интернет-угроз независимо от соединения, пользовательского устройства или облачной среды.

Интеллектуально-доверенные рабочие места

Хотя с будущим мировой экономики остается много неясного, очевидно, что рабочие места после окончания пандемии будут возвращаться на офисную территорию. Многие компании сейчас внедряют новые услуги и меры безопасности, такие как мониторинг физического расстояния, отчеты о близости, повышенная автоматизация рабочего места. А в некоторых компаниях уже всерьез задумываются о замене людей роботами.

Современная гибкая сеть – это критически важный механизм, обеспечивающий безопасную и бесперебойную работу, возвращение людей в офисные помещения. Избежать проблем с «обратной волной офисного планктона» помогут следующие мероприятия:
- нагрузочное тестирование сети – помните, что во многих случаях сеть компании не работала в течение нескольких недель, месяцев. Не считайте само собой разумеющимся, что сеть по-прежнему может предоставлять необходимые проводные и беспроводные услуги;
- автоматизация безопасного доступа в корпоративную сеть на основе идентификационных данных – организациям необходимо четко сегментировать подключение пользователей и устройств и их доступ к службам независимо от того, подключаются они из офисного помещения, из дома или из общедоступных сетей;
- повысьте безопасность сотрудников и клиентов с помощью анализа местоположения – включите рабочее место в систему мониторинга, соберите данные, которые помогут защитить здоровье и безопасность сотрудников, партнеров, гостей и клиентов, используя существующие сети Wi-Fi.

Многооблачные сети

ИТ-руководители сегодня все чаще используют облачные сервисы в качестве средства повышения устойчивости бизнеса в свете глобальных событий, связанных с пандемией. Сюда входит и гораздо более широкое внедрение модели мультиоблака – распределение приложений, рабочих нагрузок и данных по локальным центрам обработки данных и по общедоступным и частным облакам для снижения затрат, повышения гибкости и защиты от риска катастрофических сбоев.

Для обеспечения единообразного взаимодействия с пользователями, командами DevOps и организациями необходима проактивная стратегия мультиоблачной сети, которая объединяет сеть с облаком, безопасностью, приоритетами ИТ-операций. Для формирования успешной стратегии создания сетей с несколькими облаками имеет смысл основываться на трех ключевых принципах:
- рабочая нагрузка – внедрение облачной операционной модели для упрощения политик, безопасности и управления рабочими нагрузками и сервисами в локальных центрах обработки данных, нескольких разрозненных облаках или в других вычислительных средах;
- доступ – использование подходов Cisco SD-WAN и SASE в целях обеспечения стабильной безопасности мультиоблака (включая модель SaaS). Доступ для пользователей и устройств в корпоративных и общедоступных сетях из кампуса, филиала, дома или в дороге;
- безопасность сети – снижение риска, связанного с пользователями, устройствами и приложениями, распределенными в нескольких разрозненных облаках и других вычислительных средах.

Автоматизация сети

Резкое увеличение количества разрозненных удаленных сотрудников – это отнюдь не единственное, что создает чрезвычайное напряжение на ИТ-инфраструктуру. Пандемия COVID-19 также вызвала беспрецедентные колебания количества клиентов, моделей трафика приложений и новых вариантов их использования, таких как электронное обучение, видеоконференции, виртуальные мероприятия, удаленное обслуживание, автоматизация процессов и другие сетевые сервисы.

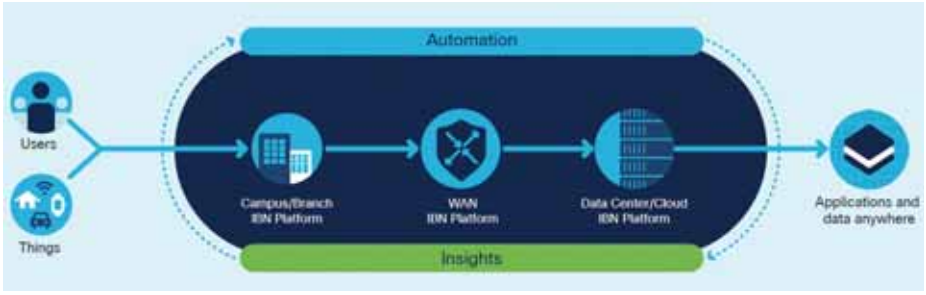
Проактивная стратегия мультиоблачности объединяет сеть с облаком, безопасностью и приоритетами ИТ-операций

Команды сетевиков могут добиться перманентного улучшения работы и способности реагировать на растущие угрозы, применяя пошаговый подход:

- автоматизируйте повторяющиеся административные задачи, такие как инициализация сети, настройка и управление, чтобы снизить административную нагрузку и улучшить соответствие требованиям в каждом домене;
- автоматизируйте доступ к своей сети, адаптацию и сегментацию для защиты групп распределенных пользователей и для предотвращения распространения атак;
- автоматизируйте сетевую политику в корпоративном центре обработки данных с помощью сегментации, ориентированной на приложения, которая защищает приложения и данные и отслеживает рабочую нагрузку;
- автоматизируйте политику за пределами центра обработки данных – в облаке, с помощью облачной операционной модели, которая обеспечивает согласованную политику приложений для локальных и гибридных облачных сред;
- автоматизируйте сквозную сегментацию на основе политик для нескольких доменов, чтобы установить согласованную, сквозную модель доступа с нулевым доверием от пользователей к рабочим нагрузкам.

Обеспечение работоспособности сервисов с применением ИИ

Очевидно, что сетевым командам необходима помощь расширенной аналитики для принятия разумных и своевременных решений по исправлению ситуации. Используя сетевую аналитику и методы машинного обучения на базе ИИ, администраторы достигают гораздо более управляемого набора задач. Сокращение числа задач позволяет командам сосредоточивать все свои усилия на вещах, которые действительно важны, и проблемах, способных оказать негативное воздействие на бизнес.



50% организаций отдают приоритет автоматизации сети, а 35% планируют, что их сети будут основаны на намерениях

И этот вопрос больше не ограничивается корпоративной сетью. Теперь, когда большинство сетевых транзакций либо исходит из традиционной корпоративной сети, либо завершается за ее пределами, сетевым администраторам необходимы видимость и аналитика для общедоступных сетей, к которым они подключены. Это особенно важно в периоды необычного сетевого стресса, как при недавней пандемии COVID-19. Чтобы разобраться в ситуации с этой цунами событий, сетевым командам следует внедрять системы сетевой аналитики и обеспечения безопасности на базе ИИ. На практике это гарантирует следующее:

- точное обнаружение – повышение точности автоматического обнаружения проблем и аномалий внутри и между доменами сети;
- более быстрое исправление – коррелируйте события для обнаружения и четкого описания наиболее вероятной основной причины проблем и аномалий;
- автоматизированное управление политиками – выявляйте устройства, приложения и тенденции, после чего предлагайте рекомендуемые обновления политик;
- снижение общей деградации сети – выявляйте закономерности и тенденции и предоставляйте контекстную аналитическую информацию, которая ускоряет проактивные, корректирующие и предупреждающие воздействия;
- аналитические данные о том, что происходит у соседей, – предоставляйте сведения и аналитику, которые помогают администраторам сети сравнивать производительность своей сети с глобальными, отраслевыми и региональными эталонными показателями.

Итоги

Разумеется, преобразование сетей – процесс бесконечный и его влияние постоянно растет. И как бы нам ни хотелось поскорее справиться с пандемией, сейчас необходимо заранее подготавливать сети к любым неприятным сюрпризам.

Пришло время переосмыслить, как ваша сетевая стратегия обеспечивает стратегию жизнестойкости бизнеса компании, и расставить приоритеты для использования новых сетевых возможностей, чтобы опережать проблемы, а не следовать за ними по пятам. Автоматизация и аналитика с использованием ИИ, предлагаемые Intent-Based Networking (IBN) – сетями на основе намерений, обеспечивают мощную платформу, которая поможет адаптироваться к любым новым обстоятельствам. Сети на основе намерений обеспечивают гибкость, безопасность, интеллект и скорость, необходимые для поддержки жизнестойкости бизнеса.

Чтобы встретить следующий кризис во всеоружии, мы предлагаем руководителям ИТ-служб и специалистам по вопросам стратегии проанализировать последние сетевые тренды, подумать над рекомендациями Cisco и решить, как действовать в тех или иных условиях, какие из новых цифровых технологий взять на вооружение.

Бизнесу, обладающему мощной, эластичной, интеллектуальной сетевой инфраструктурой, никакой COVID не страшен. ■

www.connect-wit.ru