

UserGate SUMMA

СЛАГАЕМЫЕ БЕЗОПАСНОСТИ

Экосистема решений для комплексного подхода к обеспечению информационной безопасности

ICS

Client

MC

SIEM

WAF

NGFW

DCFW

Новый подход к безопасности

Современные сети сильно преобразились за последнее время. Приложения и сервисы уходят в облака, пользователи перемещаются из офисов на удаленную работу. Периметр сети в классическом понимании уже отсутствует.

Новый подход к безопасности получил название Cybersecurity Mesh Architecture (CSMA), что можно

буквально перевести как «ячеистая архитектура кибербезопасности».

Данная концепция говорит о важности взаимосвязей между продуктами кибербезопасности, обмена информацией и координированной работы по обнаружению инцидентов и ликвидации последствий.

Для решения этих задач в UserGate разработали экосистему продуктов безопасности UserGate SUMMA



Комплексная информационная безопасность на единой платформе

UserGate SUMMA включает в себя все необходимые инструменты для комплексной защиты современной IT-инфраструктуры: виртуальные платформы и программно-аппаратные комплексы на базе собственной операционной системы UGOS, а также комплементарные продукты компании, обеспечивающие гибкое и целостное управление безопасностью сетей.



Ядром безопасности UserGate SUMMA является собственная операционная система UGOS.

Такой подход позволяет обеспечивать независимость от заимствованного программного кода, обрабатывать и анализировать сетевой трафик на высоконагруженных каналах связи, развивать и адаптировать решения UserGate для разных условий и уровней сложности.

Ключевые аспекты работы UserGate SUMMA

100% видимость сети

Основная проблема в расследовании инцидентов – это недостаток информации, который формируется из-за слабого покрытия источников и невозможности их интерпретации. Технологии UserGate SUMMA позволяют идентифицировать абсолютно всех пользователей сети, определить все приложения и расшифровать до 98% всего неизвестного трафика. Таким образом, UserGate SUMMA обеспечивает практически 100% видимость сети.

Широкая область контроля

Продукты UserGate SUMMA контролируют сетевой трафик на всех рубежах сетевого взаимодействия. Пользовательские рабочие места, локальная сеть, интернет, облачные сервисы и приложения, территориальные филиалы и удаленные сотрудники – везде можно установить продукты экосистемы UserGate SUMMA для комплексного сбора данных и защиты инфраструктуры.

Автоматизация

Продукты экосистемы безопасности UserGate SUMMA интегрированы друг с другом, а набор механизмов автоматизации позволяет настраивать сценарий мгновенного реагирования на события безопасности и увеличивать скорость реакции на инцидент.

Соответствие законам РФ

UserGate соответствует требованиям ФСТЭК России к профилям защиты, межсетевых экранов типа А и Б 4 класса защиты, системам обнаружения вторжений 4 класса защиты и по 4 уровню доверия. UserGate внесен в реестр российского ПО (регистрационный номер 1194).

Агрегация

Единые дашборды, сводные отчеты, централизованная консоль управления – все это позволяет элементам UserGate SUMMA функционировать сплоченно и слаженно.

Экспертиза Центра мониторинга и реагирования UserGate (MRC UserGate) дополнит технологический стек экосистемы UserGate SUMMA и в совокупности обеспечит максимальный уровень безопасности.

Реагирование

С UserGate SUMMA в распоряжении специалиста по безопасности находится полный набор инструментов для мониторинга сети, выявления инцидентов, а также расследования и реагирования на произошедшие события.

Совокупность решений и технологий экосистемы UserGate SUMMA, а также экспертиза MRC UserGate дают синергетический эффект и позволяют решать ключевые задачи для бизнеса – сокращать скорость реакции на нежелательные события, уменьшать последствия киберинцидентов и минимизировать время остановки бизнес-процессов.

Вариативность поставки

Продукты UserGate в разных сочетаниях и моделях использования и дополнительные формы поставки, такие как виртуальные машины, аппаратные комплексы и сервисная модель безопасности (Безопасность как услуга или Security as a Service) дают безграничные возможности имплементации решений как в существующую инфраструктуру организации, так и в проектируемую.

Продукты UserGate SUMMA



Межсетевой экран нового поколения UserGate предоставляет функции безопасности для сетей любого формата и размера, обеспечивая максимальную видимость событий безопасности и высокий уровень защиты от угроз. Огромную роль в построении защищенной инфраструктуры играет возможность увидеть, проанализировать и интерпретировать все события безопасности, к которым относятся действия пользователей, приложений и устройств. Для этого необходимо обеспечивать качественную и производительную инспекцию SSL-трафика. Благодаря передовым технологиям UserGate NGFW может дешифровать весь трафик, включая TLS 1.3 и TLS GOST.

Возможности и преимущества UserGate Next Generation Firewall:

- максимальная видимость событий безопасности – решение позволяет обнаружить скрытые атаки на инфраструктуру и вовремя отреагировать на них;

UG NGFW

- использование функций безопасности – вы можете расширить защиту своей сети за счет встроенных и дополнительных функций безопасности;
- вариативность форматов поставки – программно-аппаратный комплекс, виртуальный межсетевой экран, безопасность как сервис (SECaaS) увеличивают количество сценариев и гибкость имплементации UserGate NGFW;
- режимы работы – возможность выбирать, в каком режиме работы и с каким набором функций безопасности вы будете использовать свое устройство UserGate NGFW;
- различные способы интеграции – L2 bridge, L3 bridge, transparent proxy, proxy, default gateway и другие – позволят оптимально подобрать подходящий формат для вашей IT-инфраструктуры.

ЭКОСИСТЕМА UserGate SUMMA

UserGate NGFW является частью экосистемы продуктов безопасности UserGate SUMMA, которая расширяет его функциональные возможности.



UserGate MC – централизованная система управления экосистемой безопасности UserGate SUMMA корпоративного уровня. С его помощью настраиваются все параметры работы межсетевых экранов UserGate: сетевые настройки, правила межсетевого экранирования, контентной фильтрации, системы обнаружения вторжений и другие настройки. UserGate Management Center позволяет систематизировать подход к составлению настроек через применение шаблонов, а также прозрачно применять эти настройки на выбранной части парка межсетевых экранов.

UG MC

Возможности и преимущества UserGate Management Center:

- повышение эффективности работы службы информационной безопасности;
- управление динамичной средой информационной безопасности из единого окна;
- быстрое применение новых политик безопасности;
- среди основных функций: централизованное управление, автоматизация безопасности, ролевой доступ администраторов, контроль обновлений.

ЭКОСИСТЕМА UserGate SUMMA

UserGate Management Center управляет всеми продуктами экосистемы UserGate SUMMA. Совместно с UserGate Log Analyzer реализует концепцию SOAR (Security Orchestration, Automation and Response) в рамках экосистемы UserGate SUMMA.



UserGate Log Analyzer (SIEM, IRP, SOAR)

Современный ландшафт угроз настолько разнообразен и динамичен, что использование только базовых средств обеспечения безопасности уже не является достаточным для построения защищенной инфраструктуры. Необходимо анализировать данные, находить среди них значимые события безопасности, выявлять инциденты и расследовать их. UserGate Log Analyzer (LogAn) сочетает в себе функционал SIEM (Security Information and Event Management) и IRP (Incident Response Platform), что предоставляет возможности для сбора логов и событий, поиска инцидентов и реагирования на них. Удобная система оркестрирования, автоматизации и реагирования на события безопасности позволяет реализовать концепцию SOAR (Security Orchestration, Automation and Response) в рамках экосистемы UserGate SUMMA.

UG LogAn

Возможности и преимущества UserGate Log Analyzer:

- мониторинг событий безопасности в реальном времени и расследование инцидентов;
- ретроспективный анализ событий безопасности, хранение и резервирование данных;
- сокращение времени реакции на инцидент;
- обеспечение непрерывности бизнес-процессов;
- видимость событий безопасности;
- доступность данных корпоративного уровня;
- автоматизация процессов безопасности;
- ролевой доступ для администраторов системы.

ЭКОСИСТЕМА UserGate SUMMA

UserGate LogAn собирает данные со всех продуктов экосистемы безопасности UserGate SUMMA и сторонних устройств, позволяя выявлять IoC (индикаторы компрометации), которые могут быть задействованы в продуктах SUMMA для блокирования нежелательного трафика. UserGate LogAn отправляет управляющие команды на UserGate Management Center для оперативного реагирования на события безопасности (SOAR).



UserGate Client (EDR, ZTNA, NAC)

UserGate Client – программное обеспечение класса Endpoint Detection & Response (EDR) для конечных устройств. Данный агент UserGate SUMMA обеспечивает видимость событий безопасности, контроль и сетевой доступ с нулевым доверием (Zero Trust Network Access). UserGate Client предоставляет дополнительную информацию о конечной точке и возможность контролировать устройство внутри и за пределами периметра. Программный продукт централизованно развертывается на тысячах устройств, осуществляет сбор логов, журналов и отчетов для SIEM-системы UserGate Log Analyzer, позволяет быстро и безопасно подключаться к корпоративным сетям по IPSec-туннелям. Решение обеспечивает запись и хранение

информации о сетевой активности и действиях пользователей в конечных точках.

Возможности и преимущества UserGate Client:

- управление политиками используемых на устройстве приложений;
- защита уровня персонального межсетевое экрана;
- контроль доступа в сеть на основе политик соответствия требованиям (Network Access Control);
- безопасное удаленное соединение (VPN);
- реализация концепции сетевого доступа с нулевым доверием (ZTNA).

ЭКОСИСТЕМА UserGate SUMMA

UserGate Client сообщает экосистеме UserGate SUMMA о состоянии конечных устройств, включая информацию о запущенных приложениях и версиях ПО.

UserGate SUMMA – решение задач безопасности и бизнеса



Организация удаленного доступа в концепции ZTNA

Компоненты UserGate SUMMA обеспечивают простой и защищенный доступ к корпоративным сетям для удаленной работы по модели «нулевого доверия». С помощью UserGate NGFW проводится микросегментация сети, в том числе на L7-уровне. Обязательное шифрование реализуется с помощью встроенных инструментов по построению VPN-туннелей, а также публикациями reverse-proxy и созданием SSL VPN порталов для доступа к веб-приложениям. UserGate Client обеспечивает безопасность конечных устройств. UserGate LogAn и UserGate Management Center позволяют специалистам контролировать все события в сети в режиме real-time, выявлять и оперативно реагировать на угрозы и инциденты, осуществлять проактивную защиту от будущих атак.



Защита государственных и корпоративных ЦОД

Дата-центры являются объектами таргетированных атак злоумышленников, а также подвержены проблемам, связанным с распространением вредоносных программ и уязвимостями используемого ПО. Экосистема UserGate SUMMA защитит ЦОД от внешних вторжений, вирусов и другого вредоносного программного обеспечения.

Решение обеспечивает автоматизированную реакцию на инциденты в соответствии с актуальной концепцией SOAR (Security Orchestration, Automation and Response), а также способно оповещать администраторов о подозрительных событиях. UserGate отвечает требованиям меняющейся архитектуры ЦОД, в том числе при переходе к облачным средам.



Комплексная безопасность корпоративных сетей

Современная инфраструктура предприятия может быть представлена большим количеством территориально распределенных офисов, филиалов, точек продаж и производственных площадок. IT-ландшафт продолжает динамично меняться с развитием облачных сервисов и внедрением практики удаленной работы. UserGate SUMMA включает в себя решения для защиты всех сегментов корпоративной IT-инфраструктуры и обеспечивает гибкое централизованное управление безопасностью.



Комплексная защита объектов КИИ

UserGate SUMMA – комплексное сертифицированное решение, обеспечивающее безопасность

информационных систем, информационно-телекоммуникационных сетей, а также автоматизированных систем управления (АСУ) субъектов КИИ. UserGate обеспечивает сбор и хранение информации о произошедших на объекте инцидентах безопасности для последующей передачи данных в SIEM и систему ГосСОПКА. Решение UserGate широко используется на объектах КИИ в сферах здравоохранения, связи, финансов, ТЭК, транспорта, оборонной и гражданской промышленности.



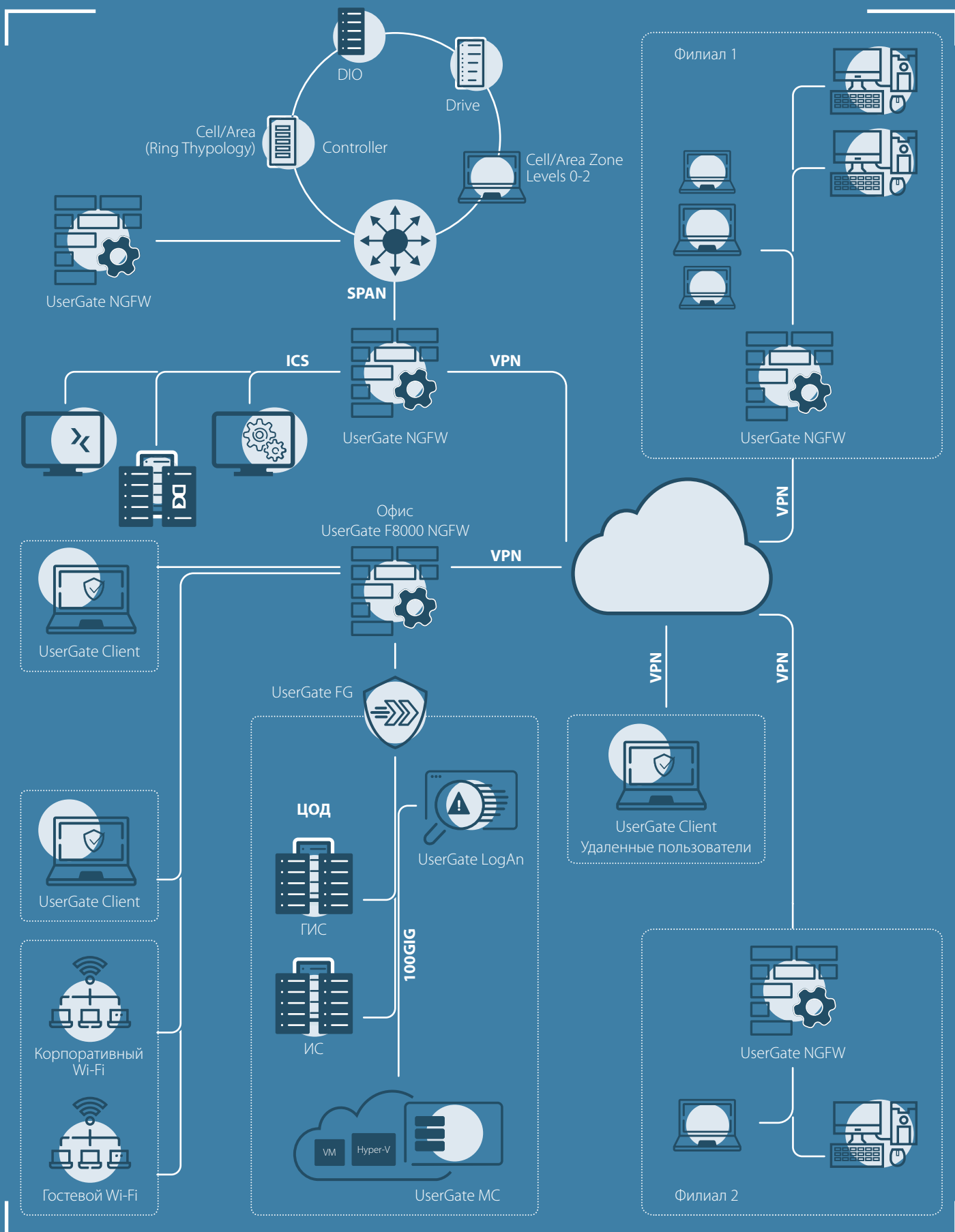
Безопасность малого и среднего бизнеса

Для малых и средних предприятий оптимальным является применение комплексного решения по безопасности, удобного в управлении и настройке.

UserGate SUMMA позволит сосредоточиться на развитии вашего бизнеса, а не на решении проблем с программным и аппаратным обеспечением. С помощью разных форм поставки, таких как ПАК, виртуальный образ и Security as a Service, открывается бесконечное количество сценариев встраивания функций безопасности в IT-архитектуру.

UserGate SUMMA

100% ВИДИМОСТЬ СОБЫТИЙ БЕЗОПАСНОСТИ





Контактная информация:

info@global-it.ru
+7(495)108-48-17