

# UserGate Management Center

Единый центр управления экосистемой  
безопасности UserGate SUMMA



Log Analyzer

NGFW

Client



UserGate SUMMA

СЛАГАЕМЫЕ БЕЗОПАСНОСТИ

Экосистема решений для комплексного подхода к обеспечению информационной безопасности

## UserGate Management Center – централизованная система управления экосистемой безопасности UserGate SUMMA корпоративного уровня.



Удобная система оркестрирования, автоматизации и реагирования на события безопасности, лежащая в основе UserGate Management Center, позволяет применить к вашей IT-инфраструктуре современную концепцию информационной безопасности SOAR (Security Orchestration, Automation and Response) в рамках экосистемы UserGate SUMMA.

UserGate Management Center осуществляет централизованное управление всеми компонентами UserGate SUMMA. Администратор сети из единой точки может устанавливать необходимые настройки и создавать политики доступа, которые применимы к группам пользователей и устройств внутри корпоративной сети.

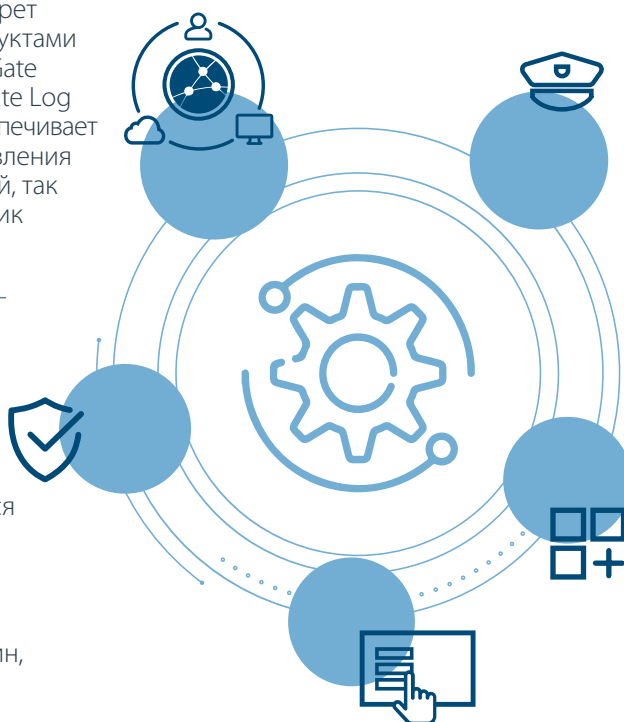
## Основные возможности UserGate Management Center

### Централизованное управление

UserGate Management Center берет на себя управление всеми продуктами экосистемы безопасности UserGate SUMMA: UserGate NGFW, UserGate Log Analyzer, UserGate Client. Это обеспечивает возможность как прямого управления каждой отдельной инсталляцией, так и применения групповых политик и шаблонов.

### Автоматизация процесса безопасности

В сочетании с использованием UserGate Log Analyzer появляется возможность настраивать автоматические реакции на происходящие события безопасности в сети, такие как помещение устройств в карантин, блокирование IP-адресов, блокирование URL-адресов и не только.



### Интеграция в структуру ИБ

Открытый API позволяет UserGate Management Center интегрироваться в общую структуру процессов информационной безопасности в рамках концепции SOAR (Security Orchestration, Automation and Response).

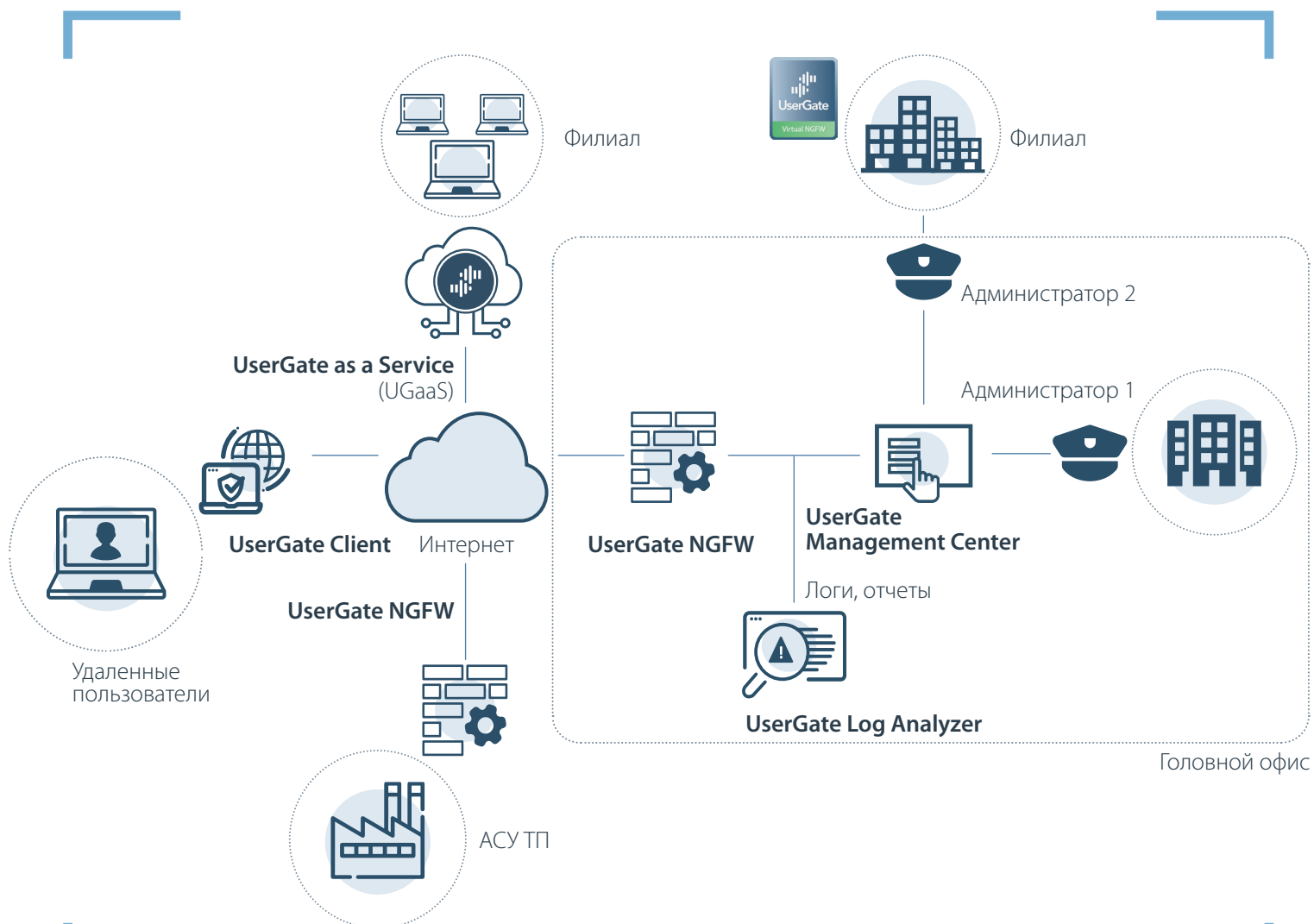
### Ролевой доступ администраторов

Мультиотенантность позволяет UserGate Management Center создавать независимые области управления для разных организаций или подразделений, а также создавать разные профили администраторов с отличающимися матрицами прав и доступа.

### Контроль обновлений

UserGate Management Center может управлять политикой обновлений, устанавливать утвержденные версии, настраивать расписание обновлений. Благодаря этому функционалу появляется возможность планировать проведение работ по обслуживанию продуктов безопасности.

## Механизмы использования UserGate Management Center



## Основные функции UserGate Management Center

- 1 Единый сервер управления
- 2 Управление всеми компонентами экосистемы безопасности UserGate SUMMA
- 3 Применение общих политик и настроек
- 4 Поддержка распределенного парка межсетевых экранов
- 5 Создание управляемых областей
- 6 Управление кластерами

Поставляется в виде:

## Аппаратная платформа



Аппаратная платформа UserGate Management Center обеспечивает управление и поддержку распределенного парка межсетевых экранов нового поколения UserGate для организаций любого масштаба и их филиалов.

## Виртуальная платформа



UserGate Management Center может быть развернут на виртуальной инфраструктуре заказчика.

## Облачная платформа



Облачная платформа UserGate Management Center – универсальный механизм управления безопасностью гибридной инфраструктурой из единой точки. Гибкое ролевое управление может быть распределено между сетевыми администраторами организации или передано на аутсорсинг. Решение позволяет связать воедино аппаратные и виртуальные шлюзы, размещенные на локальных площадках и в облаках, и реализовать концепцию SD-периметра с нулевым доверием.

## SECaaS Безопасность как услуга



UserGate Management Center также поставляется по модели «Безопасность как услуга» (SECaaS).

Линейка решений UserGate сертифицирована ФСТЭК России и находится в едином реестре отечественного ПО.

## Продукты экосистемы UserGate SUMMA

### UserGate NGFW ●

Межсетевой экран нового поколения UserGate предоставляет функции безопасности для сетей любого формата и размера, обеспечивая максимальную видимость событий 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 межсетевой экран нового поколения может дешифровать весь трафик, включая TLS 1.3 и TLS GOST.

### UserGate Management Center ●

Централизованная система управления экосистемой безопасности UserGate SUMMA корпоративного уровня. С помощью UGMC настраиваются все параметры работы межсетевых экранов UserGate: сетевые настройки, правила межсетевого экранирования, контентной фильтрации, системы обнаружения вторжений и другие. UserGate Management Center позволяет систематизировать подход к составлению настроек через применение шаблонов, а также прозрачно применить эти настройки на выбранной части парка межсетевых экранов. Среди основных функций UGMC: централизованное управление, автоматизация безопасности, ролевой доступ администраторов, контроль обновлений.

### Модуль IDPS UserGate ●

Для обнаружения вредоносной активности предприятиям необходимо проводить непрерывный мониторинг трафика. В этом помогают средства обнаружения и предотвращения вторжений (COB или IDPS). В составе UserGate NGFW присутствует собственный высокопроизводительный модуль COB/IDPS. Администратор может создавать различные наборы сигнатур, релевантных для защиты определенных сервисов, и задавать правила, определяющие действия для выбранного типа трафика, который будет проверяться в соответствии с назначенными профилями.

### UserGate Log Analyzer ● (SIEM, IRP, SOAR)

Современный ландшафт угроз настолько разнообразен и динамичен, что уже не достаточно использовать только базовые средства обеспечения безопасности. UserGate Log Analyzer (LogAn) сочетает в себе функции 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 также реализовать концепцию SOAR (Security Orchestration, Automation and Response) в рамках экосистемы UserGate SUMMA.

### UserGate Client ● (EDR, ZTNA, NAC)

Программное обеспечение класса Endpoint Detection & Response (EDR) для конечных устройств. UserGate Client обеспечивает видимость событий безопасности, контроль и сетевой доступ с нулевым доверием (Zero Trust Network Access). 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 VPN-туннелям, обеспечивает запись и хранение информации о сетевой активности и действиях пользователей в конечных точках.

### Модуль WAF UserGate ● (релиз ожидается)

Применение Web Application Firewall считается наиболее эффективным подходом к защите веб-ресурсов. Модуль WAF экосистемы UserGate SUMMA устанавливается на физический или виртуальный сервер и может выявлять разнообразные виды атак. Этот инструмент фильтрации трафика работает на прикладном уровне и защищает веб-приложения методом анализа трафика HTTP/HTTPS и семантики XML/SOAP.





**Контактная информация:**

Телефон: 8 (800) 500 4032

Клиентам: [sales@usergate.ru](mailto:sales@usergate.ru)

Партнерам: [partner@usergate.ru](mailto:partner@usergate.ru)

[usergate.ru](http://usergate.ru)

© 2022 ООО «Юзергейт». Все права защищены.