UserGate

UserGate SIEM

СБОР, МОНИТОРИНГ, АНАЛИЗ ДАННЫХ И РЕАГИРОВАНИЕ НА УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

UserGate SIEM
Обнаружение и предотвращение угроз

АНАЛИЗ СОБЫТИЙ И ИНЦИДЕНТОВ ОТ USERGATE

UserGate SIEM

Современный ландшафт угроз настолько разнообразен и динамичен, что использование базовых средств обеспечения безопасности уже не является достаточным для построения защищенной инфраструктуры.

Для обеспечения информационной безопасности предприятий и организаций необходимо анализировать данные, находить среди них значимые события безопасности, выявлять инциденты и расследовать их.

Функции UserGate SIEM

SIEM&IRP

UserGate SIEM сочетает в себе функции SIEM (Security Information and Event Management – управление событиями и инцидентами о безопасности) и IRP (Incident Response Platform – реагирование на инциденты безопасности). Это предоставляет пользователям возможности сбора логов и событий, поиска инцидентов и реагирования на них.

SOAR

Удобная система оркестрирования, автоматизации и реагирования на события безопасности позволяет реализовать концепцию SOAR (Security Orchestration, Automation and Response – оркестрирование, автоматизация и управление системами безопасности) в рамках экосистемы UserGate SUMMA.

TI

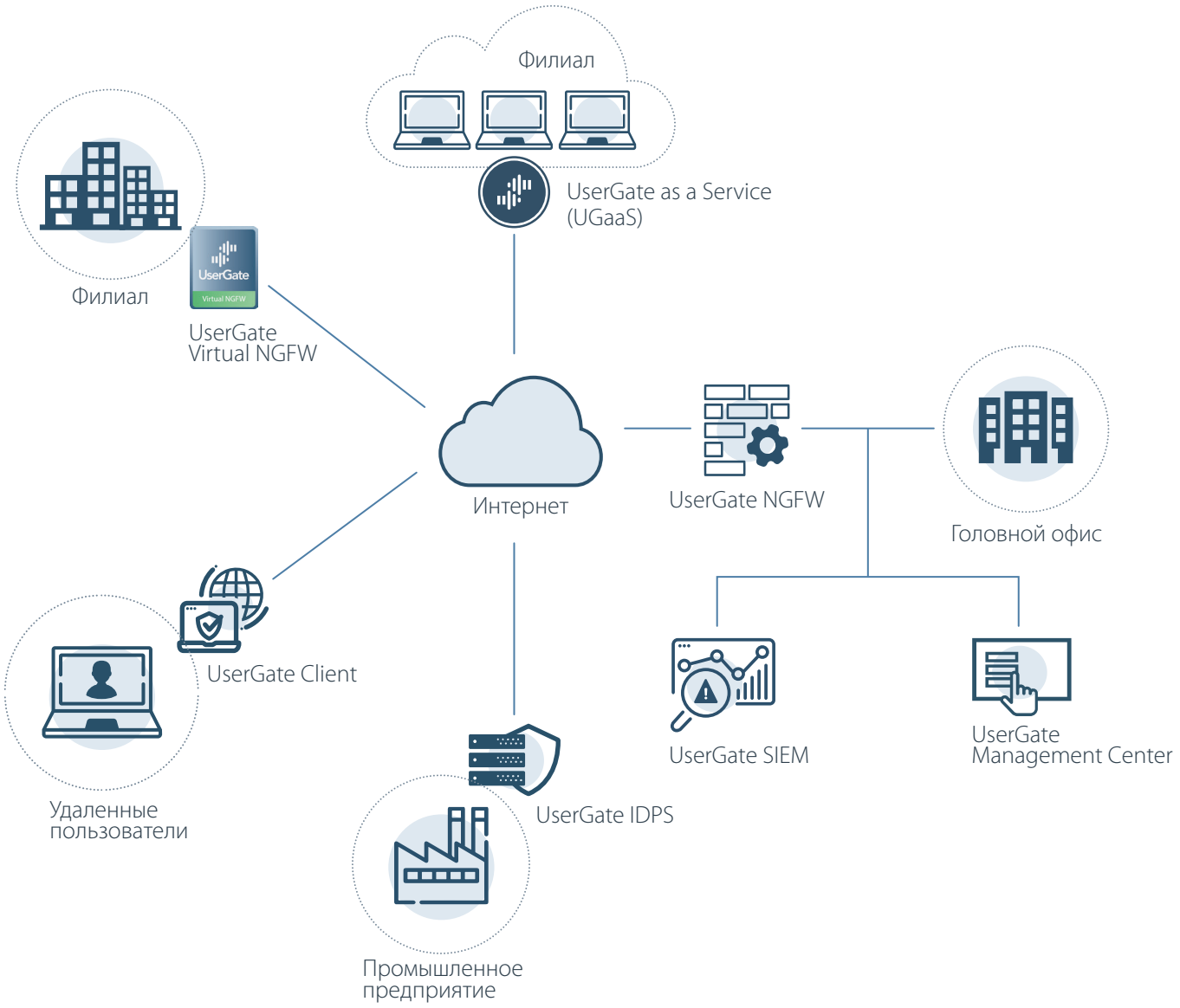
Возможность обогащения инцидентов более, чем десятком фидов с различными индикаторами компрометации, как платными, так и бесплатными.

Возможности и преимущества UserGate SIEM

- оценка состояния информационной безопасности компании;
- 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;
- подключение к личному кабинету ГосСОПКА и отправка информации об инцидентах в ручном или в автоматическом режимах.

Как действует экосистема безопасности UserGate SUMMA

- UserGate SIEM собирает данные со всех продуктов экосистемы безопасности UserGate SUMMA и сторонних устройств.
- UserGate SIEM позволяет обогащать данные для поиска IoC (индикаторов компрометации), а также создавать свои IoC в результате расследования инцидентов. Эти данные (IP-адреса, URL-адреса, hash файла и т. д.) могут быть использованы в экосистеме UserGate SUMMA для блокировки вредоносной активности и предотвращения повторения инцидентов.
- UserGate SIEM отправляет уведомления в UserGate Management Center, который, в свою очередь, посылает управляющие команды в UserGate NGFW и UserGate Client для оперативного реагирования на события безопасности (SOAR).



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. UGMC 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 (СОВ или IDPS). В составе UserGate NGFW присутствует собственный высокопроизводительный модуль СОВ/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 SIEM (SIEM, IRP, SOAR)

Современный ландшафт угроз настолько разнообразен и динамичен, что уже не достаточно использовать только базовые средства защиты и обеспечения безопасности. UserGate SIEM 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
Партнерам: partner@usergate.ru
usergate.ru

UserGate