

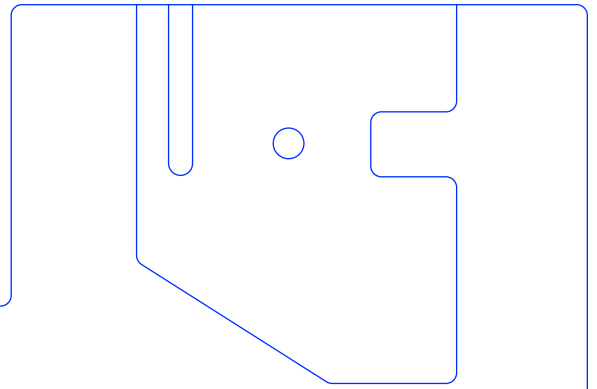


UserGate SIEM+DLP

Контроль
над инцидентами
и утечками данных



UserGate SIEM + DLP: контроль над инцидентами и утечками данных



От точечного обнаружения — к комплексному расследованию и автоматическому реагированию

SIEM (Security Information and Event Management) и DLP (Data Loss Prevention) — две важные технологии обеспечения информационной безопасности. Их взаимодействие в инфраструктуре обладает синергетическим эффектом: позволяет организациям контролировать утечки информации, оперативно реагировать на потенциальные угрозы и расследовать инциденты.

Почему интеграция UserGate SIEM и DLP — это новая ступень защиты

Разрозненные системы безопасности не дают полной картины угроз. DLP фиксирует факт утечки данных, но не всегда отвечает на вопрос «как и почему это произошло?», так как не видит всей цепочки действий злоумышленника или инсайдера в инфраструктуре компании. SIEM, в свою очередь, агрегирует и коррелирует события из разных источников, позволяя установить причины и контекст инцидента.

Совместная работа SIEM и DLP превращает разнородные сигналы в готовые сценарии реагирования. DLP выступает как источник информации о высокоприоритетных инцидентах, связанных с утечками, а SIEM обеспечивает их расследование на основе полного контекста событий со всей ИТ-инфраструктуры. Это позволяет перейти от реагирования к проактивной защите, предотвращая инциденты до того, как данные будут похищены.

Как взаимодействуют DLP и UserGate SIEM



Сбор и анализ данных

- DLP отслеживает потоки данных внутри организации и выявляет попытки передачи конфиденциальной информации: персональных данных, финансовой информации, интеллектуальной собственности и т.д.
- SIEM собирает сведения о событиях безопасности со всей инфраструктуры (от сетевых устройств, серверов, приложений и т.д.), анализирует их и выявляет потенциальные инциденты информационной безопасности.

Интеграция систем

- DLP направляет в SIEM информацию о попытках передачи конфиденциальных данных за пределы организации
- SIEM сопоставляет полученные данные с другими событиями безопасности на основе более 1 000 правил корреляции

Реагирование на инцидент

- DLP детектирует попытку утечки данных
- SIEM отправляет команду NGFW на удаление пользователя из группы VPN и уведомляет об инциденте администратора безопасности
- SIEM проводит глубокое расследование: коррелирует полученный сигнал с событиями из различных источников — от сетевой активности до действий на серверах или ПК. Это позволяет заметить подозрительное действие и вскрыть цепочку комплексной атаки на самой ранней стадии.

Как UserGate SIEM раскрывает масштабные атаки с помощью DLP

DLP может выявлять утечки данных, но не всегда способен определить, связаны ли они с внешними атаками или только с инсайдерскими угрозами. Анализируя данные от DLP в контексте других событий, SIEM выявляет сложные комплексные атаки, такие как APT (Advanced Persistent Threat).

Если DLP обнаруживает утечку данных, это может быть:

- **случайным действием персонала** — сотрудник ошибся или не знает корпоративных политик
- **злонамеренным действием инсайдера** — сотрудник решил продать данные конкурентам или насолить работодателю при увольнении
- **этапом кибератаки** — злоумышленник взломал учетную запись, чтобы похитить данные

UserGate SIEM выявляет, что стоит за инцидентом, используя следующие механизмы:

Корреляция событий

SIEM ищет события, связанные с инцидентом:

- подозрительные входы в систему — с незнакомого IP или в нерабочее время
- аномальная активность на других серверах или в сети
- попытки повышения привилегий или запуска вредоносного ПО

SIEM сопоставляет данные из DLP с другими источниками, чтобы найти признаки многоэтапного взлома:

- утечка данных совпадает по времени с атакой на почтовый сервер
- инцидент DLP произошел после фишинговой атаки

SIEM анализирует поведенческие паттерны и скрытые зависимости между событиями

- несколько сотрудников внезапно начали передавать данные — система определяет это как признак компрометации Active Directory

Расследование и реагирование

SIEM на основании собранных данных:

- обогащает инцидент информацией от сторонних фидов
- определяет, была ли утечка частью APT (Advanced Persistent Threat)
- блокирует затронутые хосты, IP-адреса, удаляет из группы VPN учетные данные пользователей
- оповещает аналитиков и запускает автоматическое реагирование



Как DLP-системы контролируют каналы передачи данных

При попытке передать защищаемую информацию DLP-система не просто фиксирует событие, а блокирует передачу, не позволяя злоумышленнику похитить данные. Таким образом, DLP срабатывает в момент, когда совершается попытка утечки данных.

- **Электронная почта, мессенджеры и веб-трафик:**
DLP анализирует отправляемые сообщения и загружаемые файлы
- **Съемные носители:**
DLP отслеживает копирование информации на USB-накопители и другие внешние устройства
- **Печать документов:**
DLP контролирует печать на локальных и сетевых принтерах

Как UserGate SIEM детектирует масштабные атаки на ранних стадиях

Подключаясь к инциденту, SIEM способен обнаружить признаки атаки до ее завершения и предотвратить нанесение ущерба.

Для этого SIEM сопоставляет косвенные события:

Фаза разведки

- SIEM видит сканирование сети с хоста, на котором сработала DLP
- логи VPN показывают подключения из подозрительных геолокаций или в нерабочее время

Первичный доступ

- антивирус обнаружил вредоносное ПО, но не заблокировал его
- SIEM зафиксировал подозрительные процессы на том же ПК

Горизонтальное перемещение

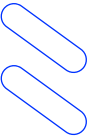
- DLP выявил попытку доступа к файлам на файловом сервере
- SIEM определил, что с того же аккаунта отправляли аномальные запросы к другим системам

Эксfiltrация данных

- DLP блокирует отправку файлов
- SIEM идентифицирует APT-атаку на ранней стадии, оповещает аналитиков и запускает автоматическое реагирование



Ключевые преимущества интеграции DLP и UserGate SIEM



Улучшение видимости событий безопасности

UserGate SIEM агрегирует данные из различных источников (сетевые устройства, серверы, приложения, DLP), предоставляя аналитикам полную картину происходящего в единой панели управления.

Дополнительный контекст

UserGate SIEM обеспечивает аналитиков расширенным контекстом событий, полученных от DLP, а также возможностью ручного и автоматического реагирования непосредственно в интерфейсе SIEM-системы.

Создание отчетов

Готовые шаблоны по требованиям регуляторов или внутренним стандартам позволяют UserGate SIEM формировать отчеты в несколько кликов — с привязкой ко времени, пользователям, объектам инфраструктуры и метрикам эффективности DLP.

Выполнение нормативных требований

Банковский ГОСТ 57580.1-2022 обязывает финансовые организации внедрять как SIEM, так и DLP-системы. Максимальную эффективность защиты обеспечит не их формальное внедрение, а глубокая интеграция.

Объективная оценка инцидентов

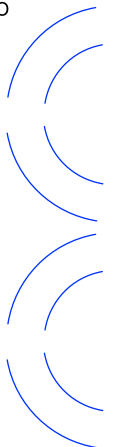
Когда утечка данных рассматривается изолированно, это может привести к недооценке угрозы. UserGate SIEM позволяет определить, был ли инцидент случайностью или одним из звеньев в цепочке масштабной кибератаки.

Повышение эффективности управления рисками

Связка UserGate SIEM и DLP позволяет не только фиксировать события, но и выстраивать целостную систему защиты, где DLP детектирует атаки на данные, а SIEM обеспечивает расследование инцидентов и оперативное реагирование на них.

Сокращение времени реагирования на угрозы

Коррелируя различные события, UserGate SIEM использует для реагирования готовые сценарии или пользовательские правила. Время анализа и ответа на инцидент сокращается до нескольких минут, а автоматизация рутинных процессов позволяет службе ИБ сфокусироваться на действительно важных оповещениях.



Уже используете DLP в своей инфраструктуре и хотите усилить защиту? Протестируйте UserGate SIEM или запросите демонстрацию возможностей интеграции.

Взять на тест



Контактная информация:

Телефон: 8 800 500-40-32
Клиентам: sales@usergate.com
Партнерам: partner@usergate.com
Маркетинг: marketing@usergate.com

Полезные ресурсы UserGate:



© ООО «Юзергейт», 2025.
Все права защищены.

