

Защитите каждое AI-взаимодействие сотрудника

Генеративный AI трансформирует работу, но стремительное внедрение порождает «слепые зоны», риски утечки данных и проблемы соответствия требованиям. Решение Check Point Workforce AI Security обеспечивает единую видимость, оценку рисков и применение политик во всех AI-взаимодействиях сотрудников — не замедляя инновации.

Использование AI превращается в стратегические задачи безопасности для CISO

- Какие AI-приложения — санкционированные или теневые — используются в организации?
- Как управлять использованием AI сотрудниками?
- Какие конфиденциальные данные передаются в промптах?
- Безопасны ли они и соответствуют ли требованиям?
- Кто использует GenAI и для чего?
- Как защитить автономные AI-агенты и действия MCP?

Использование AI превращается в стратегические задачи безопасности для CISO

Workforce AI Security охватывает веб-приложения, SaaS-интеграции, расширения браузеров, настольные агенты и инструменты разработчиков.

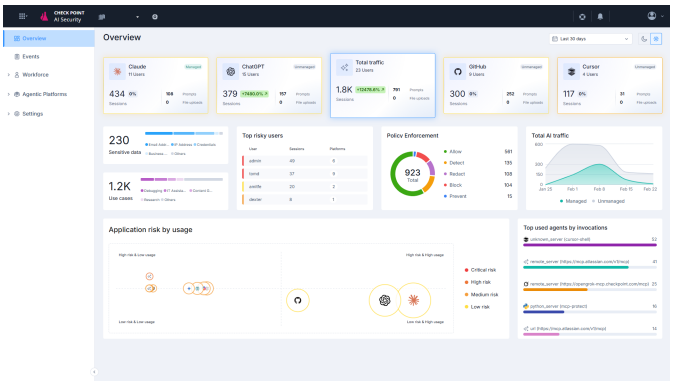
© 2026 Check Point Software Technologies Ltd. Все права защищены.

Обнаружение

Получите видимость всего использования AI — от агентов для написания кода до теневого AI

Оценка

Поймите AI-риски относительно ваших требований к безопасности и соответствию



Управление

Задавайте гибкие политики для контроля рискованных AI-приложений и действий сотрудников

Защита

Блокируйте небезопасные действия в реальном времени с помощью AI-ограничителей и DLP

Точно определяйте контекст и чувствительность данных в диалоговых промптах

› Мы готовимся приобрести Best.ai за 470, чтобы усилить наши рекламные сервисы. **Предложите письмо для внутренней коммуникации.**

ОТПРАВИТЬ

› Я собираюсь приобрести пару беговых кроссовок за $300. **Составьте персональный план тренировок на ближайшие три месяца.**

ОТПРАВИТЬ

© 2026 Check Point Software Technologies Ltd. Все права защищены.

Генеративные AI-приложения ускоряют ваш бизнес, но подвергают риску ваши данные и соответствие требованиям

Теневой AI
Несанкционированное использование AI-инструментов создаёт «слепые зоны» и риски безопасности.

Устаревшие средства контроля
Устаревшие DLP-решения не понимают диалоговые промпты, оставляя незамеченными рискованные намерения и конфиденциальные данные.

Раскрытие данных
Промпты могут раскрывать конфиденциальные данные, например финансовую информацию, рискуя утечками в AI.

Пробелы в управлении
Команды безопасности не могут управлять индивидуальным использованием AI-инструментов.

Workforce AI Security обеспечивает безопасное внедрение AI-инструментов сотрудниками.

Полное покрытие
Везде, где сотрудники взаимодействуют с AI.

Защита в реальном времени
Обнаруживайте и редактируйте конфиденциальные данные до того, как они покинут вашу среду.

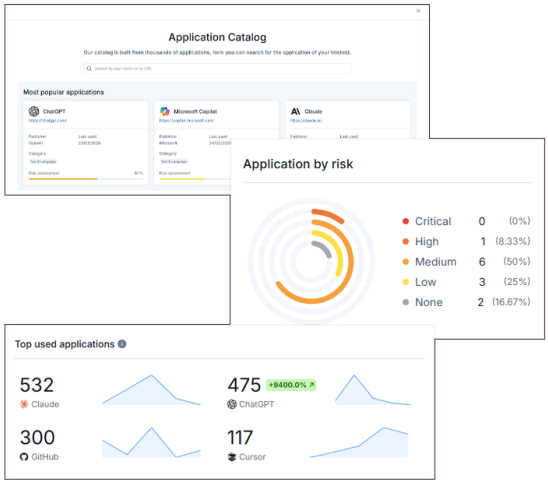
Детализированное применение политик
Определяйте средства контроля для каждого приложения и сценария, включая ограничения промптов, правила копирования/вставки и политики для файлов.

Обеспечьте соответствие и формируйте отчёты
Журналы аудита и настраиваемые отчёты для GDPR, HIPAA и EU AI Act.

© 2026 Check Point Software Technologies Ltd. Все права защищены.

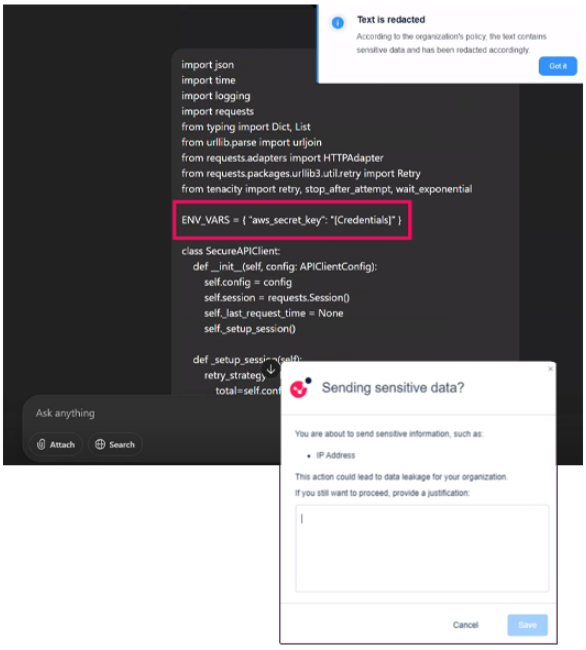
Обнаружьте каждое используемое AI-приложение и инструмент

- Обнаруживайте и отслеживайте санкционированные и теневые AI-инструменты, а также MCP, используемые сотрудниками; классифицируйте содержимое промптов, включая файлы.
- Понимайте намерения пользователей для оценки риска и применения политик с разбивкой AI-взаимодействий на уровнях приложения, сессии и пользователя — включая описание, действие пользователя, источник данных и многое другое.
- Выявляйте использование AI в подключённых SaaS-платформах, обеспечивая единообразное управление приложениями и интеграциями в едином дашборде.
- Выявляйте тренды внедрения — какие приложения стимулируют внедрение AI — по областям риска
- Просматривайте каталог AI-приложений и ищите любое приложение, даже ещё не используемое в вашей организации.





Редактирование конфиденциальных данных



Мастер проверки действий

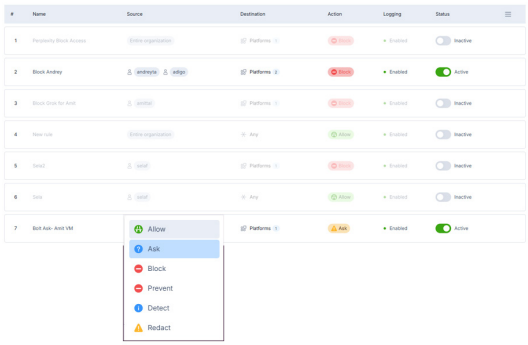
Управляйте с детализированным доступом и средствами контроля безопасности

- Понимайте, для чего используется GenAI, с помощью AI-анализа, который точно классифицирует диалоговые данные в промптах по десяткам категорий сценариев: маркетинг, отладка, юридические вопросы, электронная почта и коммуникации и многое другое.
- Определяйте детализированные политики для каждого приложения, включая ограничения копирования/вставки и конфиденциальных данных внутри промптов.
- Редактируйте конфиденциальные данные в реальном времени, заменяя их помеченными заполнителями для учётных данных, PII и другого.
- Интерактивный пользовательский опыт с мастером проверки действий, минимизирующий риск потери данных и сохраняющий продуктивность.

© 2026 Check Point Software Technologies Ltd. Все права защищены.

Защищайте с помощью AI-DLP для контекстной защиты

- Блокируйте доступ сотрудников к неавторизованным AI-приложениям
- Применяйте разные политики для управляемых и неуправляемых приложений
- Задавайте правила для предотвращения рискованных соединений между AI-инструментами и корпоративными ресурсами
- Управляйте сторонними интеграциями с SaaS-платформами
- Задавайте детализированные политики времени выполнения по приложению, пользователю и типу данных



Разверните за минуты, защищайте с первого дня

- Развёртывайте мгновенно на всех браузерах и устройствах.
- Без сложной настройки и простоев.
- Получите полную видимость всех AI-взаимодействий сотрудников, включая теневые приложения, и сразу применяйте политики.

Начните сегодня

QR-код для запроса демо

Всемирная штаб-квартира
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Тел.: +972-3-753-4599

Представительство в России
Россия, 109240, Москва, бульвар Энтузиастов, д. 2 | Тел.: +7 495 967-7444

www.checkpoint.com