



WEBTOTEM

Платформа для защиты веб-приложений,
предназначенная для бизнеса и целых стран, на основе
машинного обучения



Проблема

90% веб-сайтов уязвимы к атакам

Среднестатистический
веб-сайт подвергается
кибератаке 44 раза/день.

В настоящее время средний
ущерб от кибератак для
компаний составляет около
\$200 000.

10%

87%

77%

организаций озабочены
вопросами ИБ

пентестов заканчивается
проникновением во
внутреннюю сеть компании

атак были совершены при
использовании уязвимостей
веб-приложений



Ежедневный мониторинг Казахстанского сегмента сети Интернет

156 449 Веб-ресурсов доменной зоны .kz

Количество веб-ресурсов, использующих действующий сертификат SSL, увеличилось вдвое по сравнению с 2019 годом. Количество сайтов, использующих валидный SSL-сертификат за 2019 год составило 24 756, а на текущий момент в Казнете 46 732 таких веб-ресурсов.

Количество зараженных веб-ресурсов увеличилось с 1780 до 1366. Общее количество зафиксированных зараженных веб-ресурсов за период март-декабрь 2020 года составляет 1788.

Благодаря совместной работе с Министерством цифрового развития, инноваций и аэрокосмической промышленности РК количество дефейсов (замена главной страницы веб-ресурса) снизилось с 20 до 3

150k

3000

1 ТБ

зловредных запросов обнаружил за 2020 год

зараженных файлов за 2020 год

Данных собирается и обрабатывается за месяц



Почему WebTotem?

WebTotem проактивная защита веб-ресурсов

Охватывает два важнейших уровня архитектуры веб-приложений:
Веб-сервер и Сервер приложений.

Обладает простым в использовании API и легко интегрируется с другими данными и системами менеджмента ИБ

Обеспечивает полный цикл безопасности приложения: мониторинг активов, защита от вредоносных программ, сканирование уязвимостей и управление ими.

Имеет профессиональный центр реагирования на инциденты

Эффективно справляется с нагрузкой по защите 159 000 сайтов одновременно, используя при этом 1 аккаунт.





Мониторинг



Модуль Сканер дефейсов

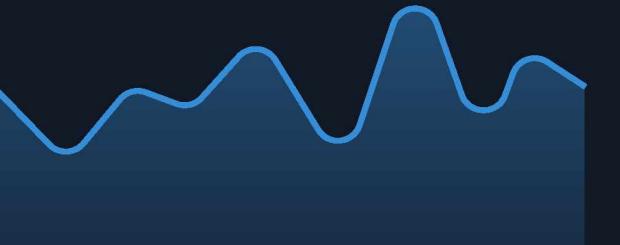
Обеспечивает подлинность страниц веб-сайта.
Показывает сайты, где хакеры подменили страницу.



Модуль SSL

Гарантирует, что веб-сайт имеет безопасное соединение и шифрование данных. Показывает дату истечения срока действия SSL-сертификата веб-сайта.

Total downs
2.442



Модуль Доступности

Отслеживает доступность веб-сайта и время отклика страницы. Помогает оптимизировать работу сайта.



Модуль Репутации

Ensures the website is available in search results.
Shows blacklist entries and has a de-blacklisting tool.



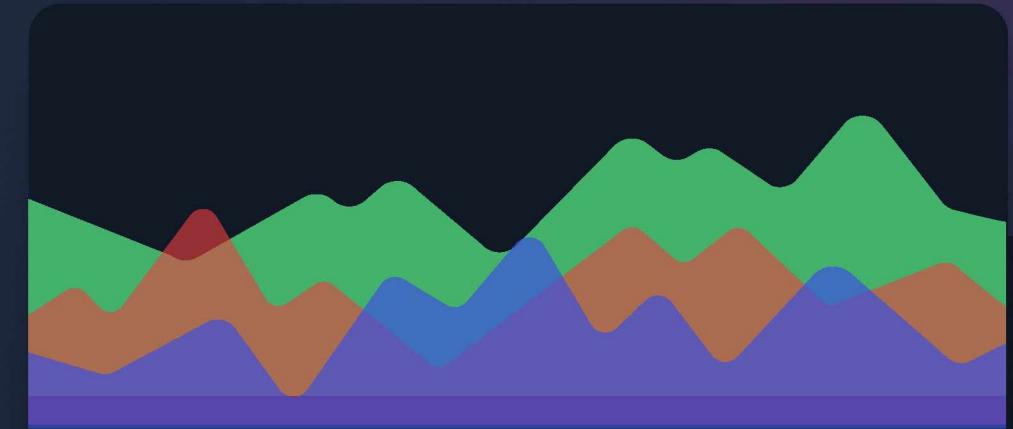
Модуль Ресурсы сервера

Показывает данные о загрузке оперативной памяти/процессора и использовании диска сервера.
Помогает оптимизировать работу сайта.



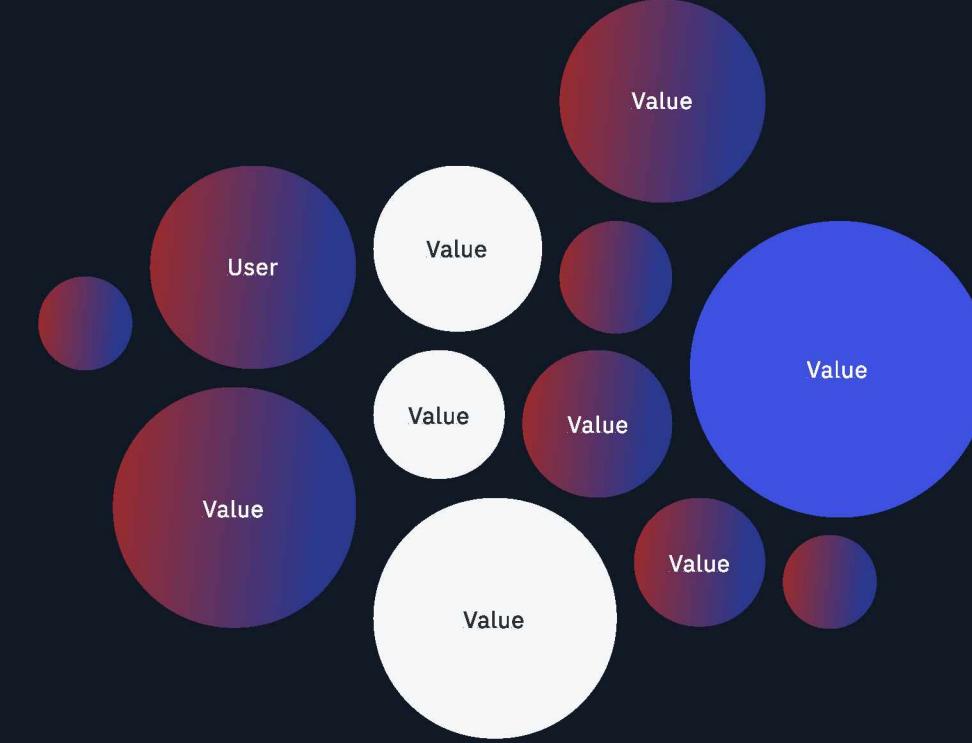
Защита от вредоносного ПО

Firewall



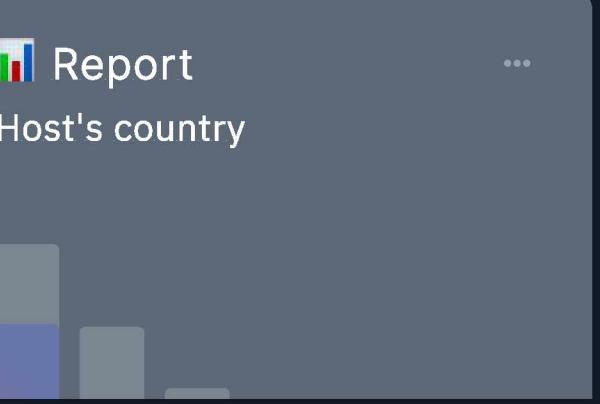
Уровни

Работает на уровне веб-сервера
и уровне веб-приложений.
Защищает базу данных от
SQL-инъекций.



AI and herd immunity

Основанный на ИИ брандмауэр WebTotem
отслеживает и фильтрует трафик веб-сайтов и не
позволяет злоумышленникам получить доступ к
конфиденциальным данным. Firewall становится
умнее с каждой атакой.



Глобальная сеть обороны

Уменьшает количество ложных
срабатываний за счет
расширения и обмена базой
знаний об атаках между сайтами
в сети.



Область

Защищает от вредоносных
ботов, брутфорс атак,
SQL-инъекций, DOS - атак и
многих других известных и
распространенных типов
атак.



Защита от вредоносного ПО

Antivirus



Удаление вредоносных ПО

Удаляет зараженные файлы и сохраняет их резервные копии.



Механизм машинного обучения

Работает на движке машинного обучения
WebTotem Antivirus сканирует файлы и удаляет вредоносные программы.



Контроль файлов и проверка разрешений

Обнаруживает изменения файлов, в том числе изменения в их правах или разрешениях



Автоматическое сканирование и сканирование по требованию/запросу

Сканирование выполняется автоматически каждые 12 часов, но также есть возможность выполнить его в любое время, когда вам это потребуется .



Управление уязвимостями

70% всех нарушений безопасности сегодня происходят из-за уязвимостей, связанных с неправильной конфигурацией приложений и серверов.

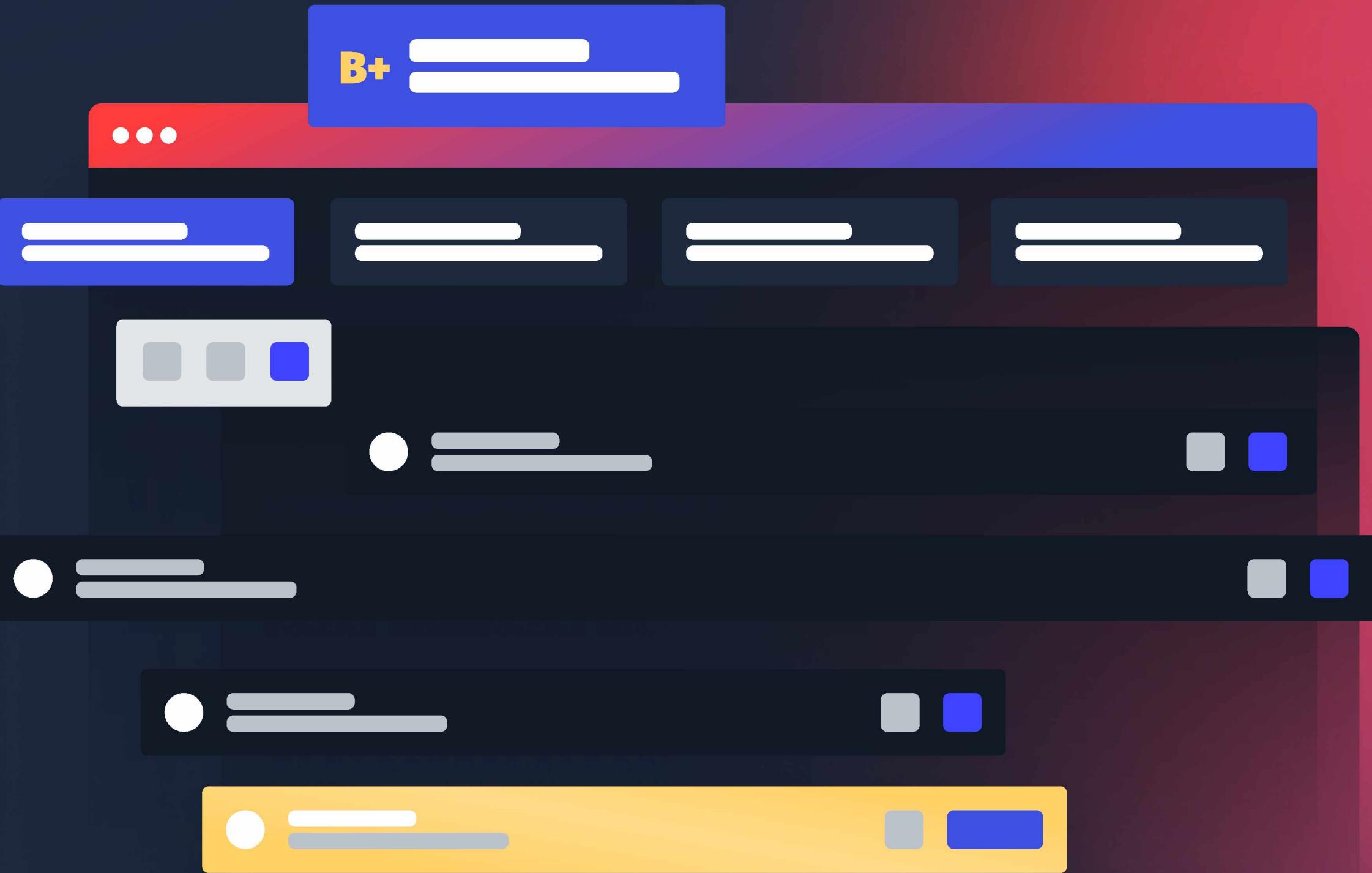


Открытые порты

Обнаружение открытых портов на веб-сервере, которые могут быть использованы злоумышленниками.

Scoring

Оценка степени безопасности веб-сайта и обнаружение неправильных конфигураций компонентов веб-сайта. Дает рекомендации по их предотвращению.





КОНТАКТЫ

info@wtotem.com