Protect

zcrWAF

ไฟร์วอลล์เว็บแอปพลิเคชัน

zcrWAF ไฟร์วอลล์เว็บแอปพลิเคชันที่พัฒนาโดยทีมไทย คัดกรองทราฟฟิกของเว็บไซต์และ API ก่อนถึงเซิร์ฟเวอร์จริง ป้องกัน OWASP Top 10 บอท และการโจมตีอัตโนมัติ

เหมาะสำหรับ	องค์กรไทย · เว็บไซต์สาธารณะ · ทีมอีคอมเมิร์ซ · เจ้าของ API · ทีม IT และทีมความปลอดภัย
โจทย์ที่ต้องแก้	เว็บไซต์และ API สาธารณะต้องเจอการโจมตีตาม OWASP Top 10 บอท สคริปต์อัตโนมัติ ทราฟฟิกผิดปกติ การยิงคำขอถี่ และการลองรหัสผ่านซ้ำ ๆ ซึ่งแยกจากผู้ใช้งานจริงได้ยาก
ครอบคลุม	เว็บไซต์ · เว็บแอปพลิเคชัน · API · เซิร์ฟเวอร์ต้นทาง · บอท / สคริปต์ · องค์กร
รูปแบบการติดตั้ง	Cloud / SaaS · Virtual Appliance · ICT Hardware Appliance เลือกได้ในขั้นออกแบบโซลูชัน

ความสามารถหลัก

- ป้องกัน OWASP Top 10 และภัยคุกคามเว็บทั่วไป
- จำกัด Traffic สำหรับ Bot, Brute Force, Credential Stuffing, Web Scraping และ Layer 7 DDoS
- ป้องกัน Bot และ Automated Scanner พร้อมควบคุม Traffic ที่ผิดปกติ
- ใช้ CAPTCHA และการยืนยันตัวตนกับผู้ใช้ที่น่าสงสัยและ path ที่มีความเสี่ยงสูง
- สร้างกฎ Allow, Block หรือ Challenge ได้เอง
- Dashboard แบบ Real-Time, Attack Map, Security Log และการมองเห็นสถานะ Backend
- แจ้งเตือนแบบ Real-Time ผ่าน E-Mail, Microsoft Teams, LINE และ Webhook
- แยก Policy และ Dashboard แบบ Multi-Tenant พร้อม RBAC, Least Privilege และ Audit Trail

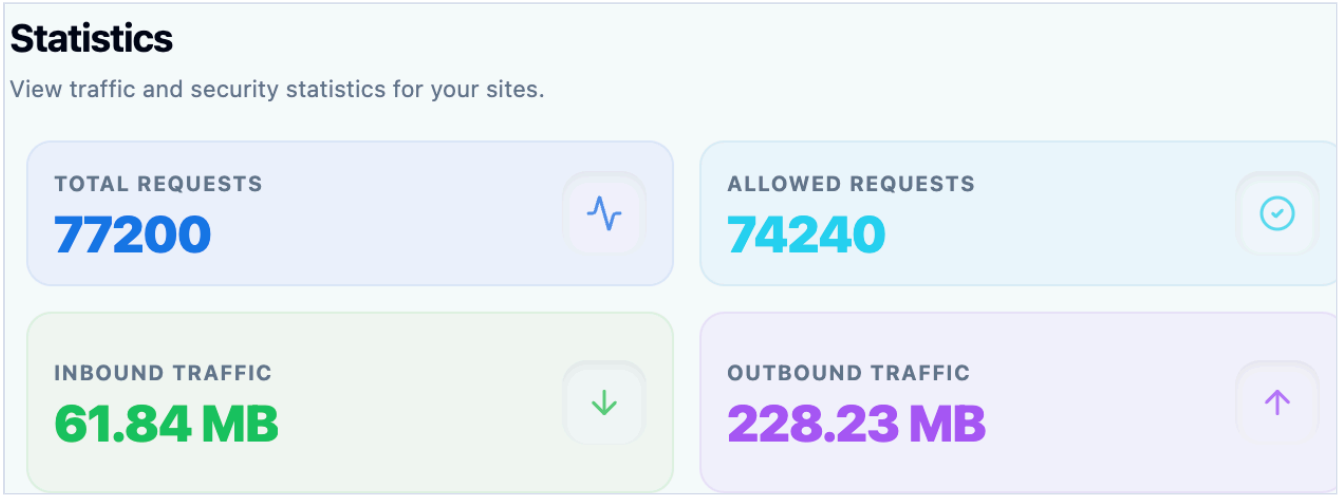
zcrWAF ทำงานอย่างไร

คัดกรองและยืนยันทราฟฟิกก่อนถึงระบบจริง

zcrWAF ตรวจสอบทราฟฟิก จำกัดปริมาณคำขอ เพิ่มแคปช่าหรือการยืนยันตัวตน และมองเห็นเหตุการณ์แบบเรียลไทม์

ผลลัพธ์จาก zcrWAF

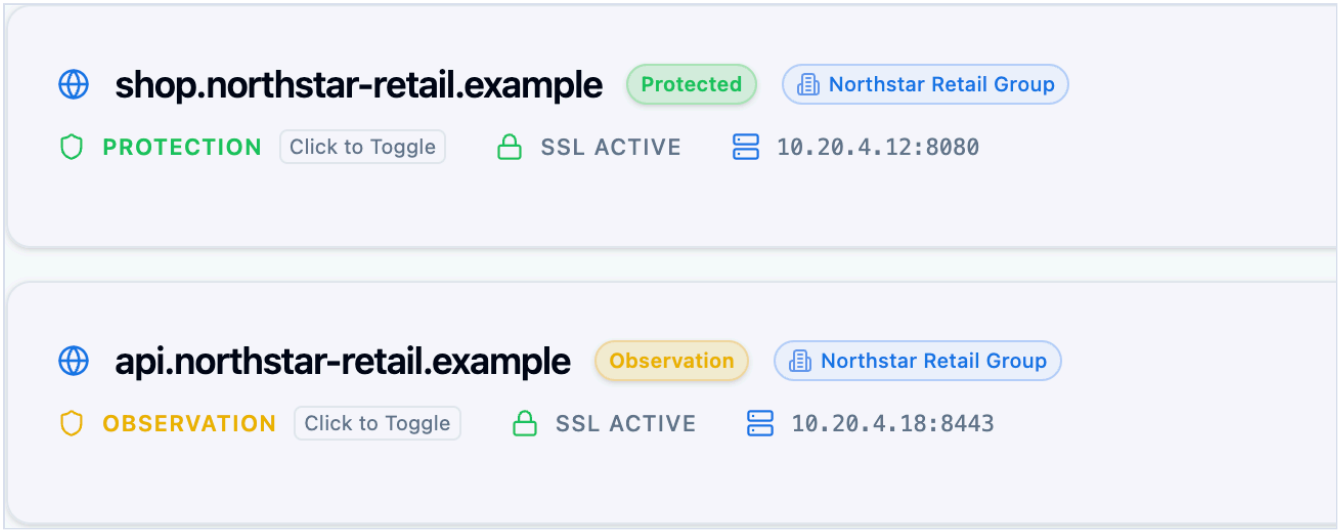
- **ป้องกันระดับเว็บแอปพลิเคชัน** — บล็อกภัยคุกคามเว็บทั่วไปและรูปแบบ OWASP Top 10 ก่อนกระทบระบบจริง
- **ควบคุมทราฟฟิก** — จำกัดทราฟฟิกผิดปกติ การยิงคำขอถี่ และพฤติกรรมลองรหัสผ่าน โดยไม่ตัดผู้ใช้งานจริงแบบเหมารวม
- **ยืนยันผู้ใช้งานเมื่อมีความเสี่ยง** — เพิ่มแคปช่าหรือการยืนยันตัวตนให้หน้าหรือบริการที่มีความเสี่ยงสูง
- **มองเห็นงานปฏิบัติการ** — ดูบันทึกความปลอดภัย การโจมตี แดชบอร์ด และการทำงานของกฎได้แบบเรียลไทม์



ส่วนหนึ่งของ dashboard แสดงยอดคำขอและปริมาณรับส่งในเดโม ไม่ใช่ขีดความสามารถ throughput การรับประกันป้องกันการโจมตี หรือผลลัพธ์ลูกค้า เปิดภาพต้นฉบับ ↗

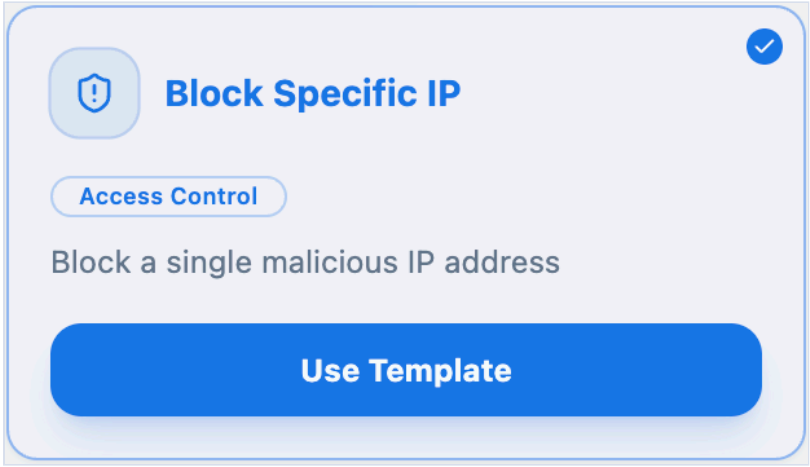
> ข้อมูลเดโมเพื่อประกอบคำอธิบาย ไม่ใช่ผลลัพธ์ลูกค้า ขีดความสามารถ หรือหลักฐานประสิทธิภาพ คง UI ภาษาอังกฤษตามต้นฉบับ

01 · ตรวจสถานะป้องกันจริงของแต่ละไซต์



รายการไซต์ครบสองแถวแสดง Protected เทียบกับ Observation พร้อมสถานะ SSL และ origin โดย Observation ไม่เท่ากับการป้องกันที่เปิดใช้งาน ชื่อไซต์ตัวอย่างไม่ใช่หลักฐานลูกค้า เปิดภาพต้นฉบับ ↗

02 · ตรวจเทมเพลตกฎที่ต้องการใช้



การ์ด Block Specific IP แสดงครบทั้งหมวด Access Control คำอธิบาย และปุ่ม Use Template การเลือกเทมเพลตยังไม่ยืนยันว่าเปิดใช้กฎใน production แล้ว คลังเทมเพลตยังมีการจำกัดหน้า admin และการบล็อกไฟล์สำคัญ ดูรายการอื่นในภาพต้นฉบับแบบเต็ม เปิดภาพต้นฉบับ ↗

> ข้อมูลเดโมเพื่อประกอบคำอธิบาย ไม่ใช่ผลลัพธ์ลูกค้า ขีดความสามารถ หรือหลักฐานประสิทธิภาพ คง UI ภาษาอังกฤษตามต้นฉบับ

คำถามที่พบบ่อย zcrWAF

มีรูปแบบติดตั้งอะไรบ้าง?

zcrWAF มีรูปแบบติดตั้ง 3 แบบ คือ Cloud / SaaS, Virtual Appliance และ ICT Hardware Appliance สำหรับติดตั้งในองค์กร

zcrWAF คิดราคาอย่างไร?

zcrWAF กำหนดราคาตามขนาดระบบ ระยะสัญญา และบริการสนับสนุน — ติดต่อ channel partner ของ zcr.ai เพื่อขอใบเสนอราคา

มีการป้องกันอะไรบ้าง?

ความสามารถหลักประกอบด้วยการป้องกัน OWASP Top 10 การจำกัดปริมาณทราฟฟิก การแยกบอทและสคริปต์อัตโนมัติ แคปช่าหรือการยืนยันตัวตน แดชบอร์ดแบบเรียลไทม์ และบันทึกเหตุการณ์

ขอบเขตการใช้งานและเงื่อนไขเชิงพาณิชย์

Cloud / SaaS	สมัครใช้งาน 1 ปีแบบคลาวด์ ป้องกันได้สูงสุด 3 โดเมน
Virtual Appliance	ติดตั้งเป็นเครื่องเสมือนในองค์กร รองรับโดเมนไม่จำกัด พร้อม ค่าบำรุงรักษา (MA) ปีแรกฟรี
ICT Hardware Appliance	ติดตั้งเป็นอุปกรณ์ในองค์กร รองรับโดเมนไม่จำกัด Throughput 1 Gbps GbE พร้อม ค่าบำรุงรักษา (MA) ปีแรกฟรี

ไฟร์วอลล์เว็บแอปพลิเคชันที่พัฒนาโดยทีมไทย

zcrWAF เหมาะกับองค์กรไทยที่ต้องการรูปแบบติดตั้งยืดหยุ่น บันทึกความปลอดภัยแบบเรียลไทม์ การบำรุงรักษา และการปรับแต่งนโยบายความปลอดภัย

การสนับสนุน: channel partner ของคุณเป็นผู้ให้การสนับสนุนขั้นแรก (first-line) และ zcr ให้การสนับสนุนด้านผลิตภัณฑ์แก่พาร์ทเนอร์

ประเมินระบบผ่านพาร์ทเนอร์ที่ได้รับอนุมัติ

เตรียมโดเมน/API ที่ป้องกัน origin ปลายทาง รูปแบบติดตั้ง ระยะสัญญา และความต้องการสนับสนุน ให้พาร์ทเนอร์ยืนยันขนาดระบบ ขอบเขตบำรุงรักษา และผู้รับผิดชอบปรับนโยบายในข้อเสนอ

พาร์ทเนอร์ที่ได้รับอนุมัติเป็นผู้วางขอบเขตข้อเสนอ เสนอราคา ทำสัญญา และส่งมอบงาน

ติดต่อพาร์ทเนอร์ ↗ แพ็กเกจปัจจุบัน ↗ เอกสารผลิตภัณฑ์ ↗