# Kona Site Defender

**ปกป้องเว็บไซต์ เว็บแอปพลิเคชัน และ API ของคุณจากการหยุดชะงักของระบบและการโจรกรรมข้อมูล**

**รักษาความปลอดภัย API ที่สามารถปรับให้เหมาะสมกับธุรกิจ สถานะความปลอดภัย และพื้นที่การโจมตีระบบของคุณ**

## ภาพรวมโซลูชัน

ความไว้วางใจของผู้ใช้บริการที่มีต่อความมั่นคงปลอดภัย ความพร้อมใช้งาน และแบรนด์ของคุณ เป็นเรื่องละเอียดอ่อนกว่าเดิมมาก ความไว้วางใจต่อการดำเนินงาน เครือข่ายห่วงโซ่อุปทาน และความคงสภาพของข้อมูลอาจสูญหายได้เมื่อข้อมูลถูกโจรกรรม เพื่อสร้างและรักษาความไว้วางใจ องค์กรต้องลดความเสี่ยงทั้งทางธุรกิจและการดำเนินงานที่เกิดจากภัยคุกคามทางไซเบอร์ เพื่อให้ได้ผลลัพธ์ด้านความปลอดภัยระดับสูงสุด

Kona Site Defender คือ ไฟร์วอลล์เว็บแอปพลิเคชันชั้นนำที่ใช้งานในระบบคลาวด์ ทำหน้าที่ควบคุมการมองเห็นโดยทำงานผ่านแพลตฟอร์ม Akamai Intelligent Edge ในการป้องกันการโจมตีโดยปฏิเสธการให้บริการ (DDoS) การโจมตีเว็บแอปพลิเคชัน และการโจมตีบน API ที่ซับซ้อนสูงสุด เพื่อรักษาสิ่งที่สำคัญมากที่สุด ซึ่งก็คือ ความไว้วางใจ

## Firewall ขั้นสูง และระบบข้อมูลภัยคุกคาม

Kona Site Defender ประกอบด้วยชุดข้อกำหนดไฟร์วอลล์เลเยอร์แอปพลิเคชันแบบกำหนดค่าไว้ล่วงหน้าที่มีการอัปเดตอย่างต่อเนื่องผ่านการศึกษาวิจัยด้านภัยคุกคามทางไซเบอร์ของ Akamai เครื่องมืออันชาญฉลาดนี้ถูกสร้าง ขึ้นมาจากส่วนการเรียนรู้ของเครื่อง (Machine Learning) และการวิเคราะห์โดยมนุษย์ (Human Analysis) ที่มีระบบตรวจจับขั้นสูงและมีความแม่นยำ สูงสุด ข้อกำหนดที่ตั้งค่าเองได้และโปรไฟล์ป้องกันภัยคุกคามอัตโนมัติถูกออกแบบมาให้มีความยืดหยุ่นและสามารถรองรับการขยายตัวจากปริมาณการใช้งานให้ครอบคลุมพื้นที่เว็บไซต์และ API ทั้งหมด โดยมีการปรับปรุงประสิทธิภาพการดำเนินงานและสามารถร่นระยะเวลาส่งมอบบริการตามความต้องการให้เร็วขึ้น

## การป้องกัน DDoS ภายในเครือข่ายและเลเยอร์แอปพลิเคชัน

แพลตฟอร์ม Edge อัจฉริยะที่กระจายในหลายประเทศทั่วโลกของ Akamai ได้รับการออกแบบให้เป็น Reverse Proxy ที่สามารถรับส่งข้อมูลผ่านพอร์ต 80 และ 443 การโจมตี DDoS ในเลเยอร์เครือข่ายทั้งหมดจะลดน้อยลงบริเวณขอบทันทีด้วย Zero-Second SLA การโจมตี DDoS ในเลเยอร์แอปพลิเคชันและการโจมตีผ่าน API จะถูกตรวจจับด้วย Kona Site Defender ในขณะเดียวกันก็ให้สิทธิ์การเข้าถึงสำหรับผู้ใช้ที่ลงทะเบียนแล้วอย่างถูกต้อง นอกจากนี้ การโจมตี DDoS ที่เกิดขึ้นกับโครงข่ายเซิร์ฟเวอร์ DNS ของคุณยังลดลงได้ด้วยโซลูชัน Edge DNS ของ Akamai

## ประโยชน์ที่ธุรกิจของคุณจะได้รับ

- ปกป้องข้อมูลรายได้ความเชื่อมั่นของลูกค้าและคุณค่าของแบรนด์
- รักษาประสิทธิภาพการทำงานของแอปพลิเคชัน แม้ในภาวะที่กำลังถูกโจมตี
- ลดต้นทุนการจัดการอันเกิดจากการเพิ่มขึ้นอย่างรวดเร็วของทราฟฟิกที่ถูกโจมตี
- การรักษาความปลอดภัยให้กับแอปพลิเคชันโดยอัตโนมัติ ด้วยกระบวนการ CI/CD
- ตัดสินใจใช้ระบบป้องกันความปลอดภัยโดยใช้ข้อมูล ด้วย Cloud Security Intelligence
- ลดภาระในการดูแลผู้ปฏิบัติงานที่มีทักษะด้วยระบบ SOCC ของ Akamai

# Kona Site Defender

**ปกป้องเว็บไซต์ เว็บแอปพลิเคชัน และ API ของคุณจากการหยุดชะงักของระบบ และการโจรกรรมข้อมูล**

## การตรวจสอบและการรักษาความปลอดภัยสำหรับ API โดยอัตโนมัติ

Kona Site Defender จะตรวจสอบทราฟฟิก API ที่ข้ามผ่านแพลตฟอร์ม Akamai โดยอัตโนมัติเพื่อแสดงรายการ API ที่ไม่ได้ระบุไว้ก่อนหน้าซึ่งรวมถึง API ปลายทาง คุณลักษณะ และข้อกำหนด API การตรวจสอบนี้จะช่วยให้ทีมป้องกันความปลอดภัยสามารถเท่าทันภัยคุกคามที่เปลี่ยนแปลงไปและสามารถลงทะเบียนรายการ API เพื่อป้องกันได้อย่างสะดวก Kona Site Defender ช่วยให้โมเดลการป้องกันความปลอดภัยทั้งในเชิงบวกและเชิงลบสามารถปกป้อง API จากการเข้าถึงที่เป็นอันตรายได้ รูปแบบการป้องกันความปลอดภัยเชิงลบจะวิเคราะห์และตรวจสอบทราฟฟิกข้อมูล XML และ JSON โดยอัตโนมัติเมื่อมีการโจมตีแอปพลิเคชัน ในขณะที่รูปแบบเชิงบวกจะอนุญาตเฉพาะทราฟฟิกข้อมูล API ที่กำหนดไว้ล่วงหน้า นอกจากนี้ การแจ้งเตือนรายงานและการวิเคราะห์แบบเรียลไทม์ยังสามารถสร้างได้ที่ระดับข้อมูล API

## การนำมาใช้ร่วมกับกระบวนการ CI/CD

Kona Site Defender ช่วยให้องค์กรสามารถนำ WAF ที่ใช้ในการป้องกันมาทำงานร่วมกับกระบวนการพัฒนาโดยการจัดการด้านโปรแกรมและเชื่อมโยงระบบควบคุมความมั่นคงปลอดภัยในช่วงเริ่มต้นของวงจรการพัฒนา โดยนักพัฒนา ระบบป้องกันความปลอดภัย และทีมปฏิบัติการสามารถใช้ API การจัดการที่หลากหลายและอินเตอร์เฟสคำสั่ง (CLI) เพื่อบูรณาการค่าความปลอดภัยเข้ากับกระบวนการ CI/CD เพื่อให้เกิดแนวทางปฏิบัติด้านความปลอดภัยที่ดีที่สุดและกระบวนทัศน์รูปแบบ "shift left"

> “เราใช้โซลูชัน Akamai WAF มาตลอดห้าปีที่ผ่านมาและโซลูชันนี้ได้ส่งมอบผลลัพธ์ที่เราในฐานะองค์กรต้องการเพื่อปกป้องข้อมูลของเราบริเวณขอบเครือข่าย”
>
> — วิศวกรอาวุโสด้านความมั่นคงปลอดภัยทางไซเบอร์ จากภาคอุตสาหกรรมบริการ

> “Kona WAF SaaS ทำงานให้เราได้อย่างไร้ที่ติมานานกว่าสี่ปี.... ระบบของเราไม่เคยหยุดทำงานเลยเมื่อถูกโจมตีทางไซเบอร์ ซึ่งแตกต่างจากประสบการณ์เดิมที่เราเคยได้รับโดยสิ้นเชิง เว็บไซต์จำนวนมากของเราเป็นเหมือนแม่เหล็กดึงดูดการโจมตีและอยู่ภายใต้การโจมตีตลอด 24 ชั่วโมง... ตามรายงานบันทึก”
>
> — หัวหน้าฝ่ายโครงข่าย MCIT จากภาคอุตสาหกรรมการเงิน

ที่มา: Gartner Peer Insights

# Kona Site Defender

**ปกป้องเว็บไซต์ เว็บแอปพลิเคชัน และ API ของคุณจากการหยุดชะงักของระบบ และการโจรกรรมข้อมูล**

## Features

**แอปพลิเคชันไฟร์วอลล์** - โหมดการทำงานสองโหมดทั้งในรูปแบบการจัดการด้วยตนเองและการจัดการโดย Akamai ทำให้ระบบมีความยืดหยุ่นสูงสุดและครอบคลุมการทำงานทั้งหมดของระบบ โหมดการจัดการด้วยตนเอง (Kona Rule Set) จะควบคุมขอบเขตความปลอดภัยที่สามารถกำหนดค่าได้เอง ในขณะที่โหมดการจัดการโดย Akamai (กลุ่มป้องกันการโจมตีอัตโนมัติ) จะช่วยขจัดความจำเป็นในการกำหนดค่าและการอัปเดตข้อกำหนดทั้งหมด ไม่เพียงเท่านี้ ข้อกำหนดที่จัดการโดย Akamai ยังมีโลจิกตรวจจับขั้นสูงที่ปรับเปลี่ยนแบบไดนามิกตามลักษณะคำขอที่ส่งเข้ามา ตัวเลือกโหมดการจัดการทั้งสองนี้ช่วยให้องค์กรสามารถปกป้องแอปพลิเคชันและ API ได้มากขึ้นถึง 50% และใช้ความพยายามในการจัดการน้อยลง 50%

**การป้องกันการโจมตี DoS (การควบคุมอัตราคำขอ)** - ป้องกันอัตราคำขอและการโจมตีโดยปฏิเสธการให้บริการ (DoS) ที่มากเกินไปผ่านการตรวจสอบและการควบคุมอัตราคำขอ ผู้บุกรุกจะถูกปิดกั้นโดยอัตโนมัติเพื่อป้องกันการเข้าถึงข้อมูลบริเวณต้นกำเนิดของเว็บไซต์

**การวิเคราะห์ข้อมูลการป้องกันความมั่นคงปลอดภัยทางเว็บไซต์ขั้นสูง** - เข้าถึงข้อมูลการโจมตีจากระยะไกลโดยละเอียดและการวิเคราะห์เหตุการณ์ด้านความปลอดภัยเพื่อประเมินว่าต้องมีการเปลี่ยนแปลงใดบ้างเพื่อปรับปรุงระบบป้องกันความปลอดภัยและเพิ่มประสิทธิภาพการกำหนดค่าที่เหมาะสมกับความต้องการทางธุรกิจของคุณ

**Network (IP/Geo) Edge Firewall** - การควบคุม IP/Geo ช่วยให้คุณสามารถปิดกั้นหรืออนุญาตทราฟฟิกที่มาจาก IP ซับเน็ต หรือพื้นที่ทางภูมิศาสตร์จำเพาะ วิธีนี้ช่วยให้คุณสามารถปิดกั้นคำขอที่เป็นอันตรายจากที่อยู่ IP หรือทราฟฟิกเฉพาะจาก The Onion Router (Tor) ที่แฮกเกอร์ใช้ซ่อนตัวตน

**Open APIs และ CLI** - สามารถเข้าถึง แก้ไข และตรวจสอบการกำหนดค่าความปลอดภัยได้โดยสมบูรณ์ Open API และ CLI ทำให้คุณสามารถบูรณาการการทำงานและปรับตั้งค่าตามข้อกำหนดของคุณเองได้อย่างอิสระ

**ข้อกำหนดที่ตั้งค่าเองได้** - Kona Site Defender นำเสนอโปรแกรมสร้างข้อกำหนดที่สามารถตั้งค่าได้เองอย่างรวดเร็วและง่ายดาย โดยนำมาใช้เพื่อจัดการสถานการณ์เฉพาะหน้าที่ไม่ได้เป็นไปตามข้อกำหนดมาตรฐานหรืออุดช่องโหว่เว็บไซต์ใหม่ได้ทันที

**การโต้ตอบ** - สร้างและส่งข้อความโต้ตอบได้หลากหลายวิธี รวมถึงการโต้ตอบที่กำหนดขึ้นเองทั้งหมด คุณสามารถส่งข้อความแจ้งข้อผิดพลาด ส่งแบรนด์เพจที่มีโลโก้ของคุณเอง หรือกำหนดและส่งข้อความตอบกลับแบบ HTML, XML หรือ JSON ตามความต้องการของคุณ

**โหมดการประเมิน** - ประเมินข้อกำหนด WAF ใหม่หรืออัปเดตข้อกำหนดได้อย่างง่ายดายเกี่ยวกับทราฟฟิกในขณะนั้น ควบคู่ไปกับการป้องกันที่ใช้งานอยู่เพื่ออัปเกรดระบบป้องกันล่าสุด แม้ว่า Akamai จะอัปเดตข้อกำหนด WAF อย่างโปร่งใสและต่อเนื่อง แต่คุณก็ยังเป็นผู้ควบคุมการประเมินและเป็นผู้เปิดการใช้งานระบบโดยสมบูรณ์

**ประสิทธิภาพและการส่งมอบข้อมูล** – สามารถรองรับการขยายตัวได้อย่างราบรื่นเพื่อให้เป็นไปตามปริมาณทราฟฟิก เนื่องจากปริมาณทราฟฟิกนั้นจะแตกต่างกันไปตามช่วงเวลา สามารถกระจายเนื้อหาไปยัง CPU และหน่วยความจำได้ตามความ ขต้องการ สามารถส่งเนื้อหาแคชจากขอบเครือข่าย และสามารถดำเนินการป้องกันได้อย่างต่อเนื่องโดยที่ระบบไม่หยุดชะงักเพื่อประสิทธิภาพสูงสุดในการส่งมอบข้อมูล

# Kona Site Defender

## ปกป้องเว็บไซต์ เว็บแอปพลิเคชัน และ API ของคุณจากการหยุดชะงักของระบบ และการโจรกรรมข้อมูล

**การรายงาน**-เครื่องมือรายงานความปลอดภัยของเว็บไซต์จะคอยตรวจสอบและประเมินประสิทธิภาพระบบป้องกันของคุณอย่างต่อเนื่อง คุณสามารถสร้างรายงานแบบเรียลไทม์เพื่อตรวจสอบกิจกรรมประจำวัน โดยสามารถตรวจสอบการโจมตีตามประเภทและนโยบายด้านความปลอดภัย และสามารถดูรายงานเกี่ยวกับ API เป้าหมาย ทราฟฟิก DoS และข้อมูลต่าง ๆ

**การแจ้งเตือนแบบเรียลไทม์**-สร้างการแจ้งเตือนทางอีเมลแบบเรียลไทม์โดยใช้ตัวกรองแบบคงที่และข้อจำกัดที่สามารถกำหนดค่าได้อย่างง่ายดายเพื่อแจ้งไปยังผู้รับที่กำหนดไว้

**Site Shield** - เลเยอร์ป้องกันเพิ่มเติมช่วยป้องกันไม่ให้ผู้โจมตีข้ามผ่านระบบป้องกันบนคลาวด์หรือวางเป้าหมายการโจมตีไปที่โครงข่ายต้นทางของคุณ

**SIEM Integration** - ตัวเชื่อมต่อที่สร้างไว้ล่วงหน้าช่วยให้คุณสามารถใช้แอปพลิเคชัน SIEM ได้ทั้งในสถานที่ติดตั้งระบบและผ่านระบบคลาวด์ เช่น Splunk, QRadar, ArcSight เป็นต้น

## โซลูชันอื่น ๆ เพื่อเพิ่มประสิทธิภาพการป้องกัน

**ชื่อเสียงของลูกค้า** - ระบบการให้คะแนนชื่อเสียงอัจฉริยะจะขึ้นอยู่กับการพิจารณาของ Akamai เกี่ยวกับพฤติกรรม (Behavior) ก่อนหน้าของที่อยู่ IP ส่วนบุคคลและที่อยู่ IP ที่ใช้ร่วมกัน

**ระบบจัดการบอต** - ตรวจจับ ระบุ จัดหมวดหมู่ และจัดการบอตที่เข้าถึงเว็บไซต์ของคุณ อัลกอริธึมการเรียนรู้ของระบบใช้การส่งข้อมูลพฤติกรรมระยะไกลทั้งของบอตและของมนุษย์เพื่อให้บอตดีผ่านไปได้ ในขณะเดียวกันก็หยุดบอตที่เป็นอันตรายและอาจโจมตีคุณได้ เช่น การละเมิดข้อมูลส่วนบุคคลและการโจรกรรมข้อมูลบัญชีส่วนบุคคล เป็นต้น

**บริการด้านความมั่นคงปลอดภัยที่ต้องบริหารจัดการ** - ออฟโหลดหรือเสริมระบบจัดการความปลอดภัย การตรวจสอบและลดภัยคุกคาม ผ่านการดำเนินงานโดยผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยของ Akamai

**ระบบตรวจสอบความสมบูรณ์ของหน้าเว็บไซต์** - ปกป้องเว็บไซต์จากการคุกคาม JavaScript เช่น การสกิมมิงเว็บไซต์ การโจมตีในรูปแบบ Formjacking และการโจมตีจากกลุ่ม Magecart โดยการอุดแหล่งที่มาที่มีช่องโหว่ คอยตรวจจับพฤติกรรมที่น่าสงสัย และปิดกั้นกิจกรรมที่เป็นอันตราย

Akamai

Akamai เพิ่มความปลอดภัยและมอบประสบการณ์ดิจิทัลแก่บริษัทขนาดใหญ่หลายแห่งทั่วโลก แพลตฟอร์มอัจฉริยะของ Akamai สามารถใช้งานได้รอบด้าน ไม่ว่าจะภายในองค์กรหรือในระบบคลาวด์ทำให้ลูกค้าและธุรกิจของคุณสามารถดำเนินกิจการได้ด้วยความรวดเร็ว ฉลาด และปลอดภัย Akamai สนับสนุนแบรนด์ชั้นนำทั่วโลกเพื่อช่วยให้แบรนด์เหล่านั้นเห็นข้อได้เปรียบในการแข่งขันผ่านโซลูชันที่รวดเร็วที่สามารถเพิ่มพลังโครงข่ายมัลติคลาวด์ของตนได้ นอกจากนี้ Akamai ยังช่วยให้ผู้ใช้งานสามารถควบคุมการตัดสินใจ การใช้แอปพลิเคชัน และประสบการณ์ของลูกค้าได้มากกว่าสิ่งใด และช่วยขจัดการโจมตีและภัยคุกคามทางไซเบอร์ ทั้งนี้กลุ่มผลิตภัณฑ์ Edge Security ระบบเพิ่มประสิทธิภาพการใช้งานผ่านเว็บและอุปกรณ์เคลื่อนที่ ระบบองค์กร และโซลูชันการส่งมอบสื่อวิดีโอของ Akamai จะไม่สามารถดำเนินงานได้หากไร้ระบบบริการลูกค้า ระบบวิเคราะห์ และการตรวจสอบตลอด 24 ชั่วโมง หากต้องการทราบว่าทำไมแบรนด์ชั้นนำทั่วโลกจึงไว้วางใจ Akamai

World Information Technology Co.,Ltd.
อาคารสกุลไทย สุรวงศ์ ทาวเวอร์ ชั้น 19 บี 141/24 ถนนสุรวงศ์ แขวงสุริยวงศ์ เขตบางรัก กรุงเทพฯ 10500
02 237 3555 @witofficial www.wit.co.th