การป้องกัน **DDoS** ด้วยระบบป้องกันของ **A10:**

โซลูชัน DDoS ที่ครอบคลุมสำหรับองค์กร

DDoS ยังคงเป็นเหตุการณ์ภัยคุกคามอันดับหนึ่ง ดังนั้นจึงจำเป็นต้องมีแผนการป้องกันแบบเลเยอร์ที่มีหลายรูปแบบ การป้องกัน DDoS ของ A10 เป็นโซลูชันแบบรวมที่ประกอบด้วยการตรวจจับ การบรรเทาผลกระทบ การประสานงาน และข่าวกรองเฉพาะ DDoS ซึ่งให้การป้องกันในเชิงรุกที่แม่นยำ ปรับขนาดได้ ชาญฉลาด และจำเป็นในการต่อสู้กับการโจมตีที่ซับซ้อนในปัจจุบัน ระบบป้องกันของ A10 ที่ออกแบบมาเพื่อการบูรณาการอย่างไร้รอยต่อ ช่วยให้มั่นใจถึงการป้องกันระดับสูงสุดในขณะที่ยังคงประสิทธิภาพการทำงานเอาไว้ ซึ่งจะปกป้องโครงสร้างพื้นฐานจากภัยคุกคามของ DDoS ที่เพิ่มขึ้นอย่างต่อเนื่อง

การป้องกันภัยคุกคาม

กรณีการใช้งาน 1: การป้องกันภัยคุกคาม

การป้องกันภัยคุกคามแบบคลาวด์เนทีฟของ A10 ซึ่งให้บริการในรูปแบบโซลูชัน SaaS จะช่วยปกป้องธุรกิจของคุณให้มีการหยุดชะงักน้อยที่สุด โดยจะช่วยยกระดับการป้องกัน DDoS ด้วยข้อมูลและการวิเคราะห์เชิงลึกที่ไม่มีการสูญเสียประสิทธิภาพ โดยไม่จำเป็นต้องมีอุปกรณ์ด้าน DDoS โดยเฉพาะ แพลตฟอร์มข่าวกรองเฉพาะ DDoS ของ A10 ยังสามารถสร้างรายการบล็อกที่ชาญฉลาดซึ่งจะยับยั้งภัยคุกคามในเชิงรุกก่อนที่ภัยคุกคามจะส่งผลกระทบต่อการดำเนินงานของคุณ รายการเหล่านี้สามารถผสานรวมเข้ากับโครงสร้างพื้นฐานด้านความปลอดภัยที่มีอยู่แล้วได้อย่างง่ายดาย ซึ่งจะให้การป้องกันแบบครบวงจรจากภัยคุกคามที่ซับซ้อนและมีจำนวนมากขึ้นเรื่อย ๆ ได้อย่างมีประสิทธิภาพ

การตรวจจับภัยคุกคาม

กรณีการใช้งาน 2: การตรวจจับภัยคุกคาม

โซลูชันการตรวจจับเฉพาะ DDoS ของ A10 สามารถทำการตรวจจับได้อย่างรวดเร็วและมีความแม่นยำสูงด้วยการใช้ข้อมูลตัวชี้วัดของทราฟฟิค (Flow-based approach) ซึ่งจะระบุภัยคุกคามที่อาจเกิดขึ้นได้ภายในเวลาเพียงสามวินาที ความสามารถในการตรวจจับที่รวดเร็วนี้ช่วยให้ลูกค้าลดเวลาขัดข้องของระบบและทำให้บริการพร้อมใช้งานอยู่เสมอแม้ในขณะที่ถูกโจมตี ความยืดหยุ่นของโซลูชันนี้จะสนับสนุนการตรวจจับ DDoS โดยไม่รบกวนการดำเนินงานในปัจจุบัน

การบรรเทาภัยคุกคาม

กรณีการใช้งาน 3: การบรรเทาภัยคุกคาม

โซลูชันการบรรเทาผลกระทบจาก DDoS ของ A10 มอบการป้องกันแบบเรียลไทม์ที่แข็งแกร่งต่อการโจมตีแบบ DDoS ทั้งในระดับปริมาณและระดับแอปพลิเคชัน จึงทำให้มั่นใจได้ว่าธุรกิจของคุณจะยังคงออนไลน์อยู่ท่ามกลางภัยคุกคามที่ร้ายแรงที่สุด ความสามารถในการยกระดับแบบอัตโนมัติทำให้ A10 สามารถจัดการกับความเสียหายได้อย่างชาญฉลาด โดยไม่จำเป็นต้องมีการแทรกแซงด้วยมนุษย์ โซลูชันนี้สามารถใช้งานได้แบบอินไลน์หรือแบบผสานรวมผ่านการกำหนดเส้นทาง BGP หรือการกำหนดเส้นทาง DNS สำหรับธุรกิจที่มีปริมาณการรับส่งข้อมูลพุ่งสูงขึ้นอย่างไม่คาดคิด ปัจจุบัน A10 จะมีการกรองข้อมูลบนคลาวด์เป็นโซลูชันแบบไฮบริด ซึ่งจะเปลี่ยนเส้นทางการรับส่งข้อมูลเมื่อจำเป็นเพื่อรับประกันความปลอดภัยอย่างต่อเนื่องและรักษาเวลาที่พร้อมให้บริการ

ข้อได้เปรียบในการป้องกัน DDoS ด้วยระบบป้องกันของ A10

- **รับรู้ภัยคุกคามอยู่เสมอ:** ใช้ประโยชน์จากข่าวกรองเชิงลึกที่แม่นยำและไม่มีการสูญเสียประสิทธิภาพ เพื่อตรวจจับและบล็อกการโจมตีก่อนที่จะทำให้ธุรกิจของคุณหยุดชะงัก
- **พร้อมให้บริการอย่างต่อเนื่อง:** การบรรเทาผลกระทบแบบอัตโนมัติที่ชาญฉลาดและปรับขนาดได้ช่วยรับประกันเวลาที่พร้อมให้บริการแม้ในระหว่างการโจมตีขนาดใหญ่
- **การป้องกันที่ใช้งานง่าย:** การประสานงานแบบเฉพาะจะลดความซับซ้อนและเวลาในการตอบสนอง และเพิ่มความแม่นยำเพื่อการกู้คืนที่รวดเร็วยิ่งขึ้น

> *การโจมตีด้วยการปฏิเสธการให้บริการ **(Denial of service)** ยังคงมีอยู่ทั่วไปและเป็นรูปแบบของเหตุการณ์ที่เกิดขึ้นเป็นอันดับต้น ๆ*
>
> — รายงานการสืบสวนการละเมิดข้อมูลของ **Verizon ในปี 2024**

แหล่งที่มา: verizon.com/business/resources/Tfd3/reports/2024-dbir-data-breach-investigations-report.pdf

ติดต่อเราเพื่อเข้าร่วมการประชุมวางแผนโซลูชัน

apac@a10networks.com
A10Networks.com