MONITORAPP

APPLICATION INSIGHT SVA

Intelligent SSL Visibility Appliance | AiSVA

AISVA – SSL/TLS Visibility Appliance (MONITORAPP)

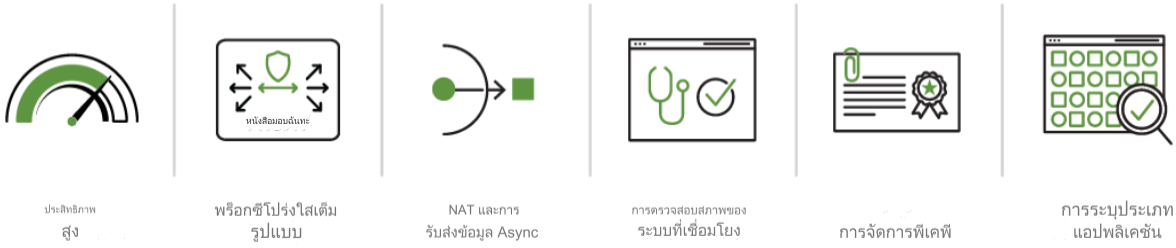
SSL/TLS Visibility Appliance หรือ SVA โซลูชันความปลอดภัยที่ให้การมองเห็นเครือข่ายเพื่อการรักษาความปลอดภัยที่ราบรื่นสมบูรณ์แบบ ไม่สามารถบล็อกการรับส่งข้อมูลที่เข้ารหัสได้เนื่องจากตรวจไม่พบมัลแวร์ ที่ซ่อนอยู่เว้นแต่ว่าการรับส่งข้อมูลจะถูกถอดรหัส อย่างไรก็ตาม มีอุปกรณ์รักษาความปลอดภัยที่มีอยู่เพียงประมาณ 20% เท่านั้นที่สามารถทำการเข้ารหัส SSL ได้ และกระบวนการถอดรหัสอาจทำให้ประสิทธิภาพของอุปกรณ์รักษาความปลอดภัยที่มีอยู่ลดลง ส่งผลให้เกิดความล่าช้าในความเร็วในการตอบสนองของเครือข่าย

นี่คือเหตุผลที่เราต้องการเครื่องมือเข้ารหัสเฉพาะสำหรับการรับส่งข้อมูล SSL/TLS MONITORAPP AISVA (Application Insight SSL Visibility Appliance) จัดทำระบบรักษาความปลอดภัยที่เข้มงวดโดยจัดให้มีการถอดรหัสการเข้ารหัสแบบสองทิศทางสำหรับเซิร์ฟเวอร์และไคลเอนต์ ทำให้มั่นใจถึงประสิทธิภาพชั้นนำของอุตสาหกรรมและการมองเห็นเครือข่ายผ่านการผสมผสานของเทคโนโลยีพร็อกซีที่ปรับให้เหมาะสมสำหรับการเข้ารหัสและการถอดรหัสของ SSL/TLS การรับส่งข้อมูล (HTTPS, SMTPS, POP3S ฯลฯ)

ทำงานได้อย่างสมบูรณ์แบบกับอุปกรณ์รักษาความปลอดภัยใด ๆ

AISVA

- มีการจัดการที่ยืดหยุ่น
- ควบคุมการรับส่งข้อมูล SSL แบบสองทิศทางอย่างสมบูรณ์
- องค์ประกอบที่ง่ายและฟรี
- มั่นใจได้ถึงความเร็วสูงสุด
- จัดการใบรับรองอย่างรวดเร็วและง่ายดาย



MONITORAPP

ทำงานร่วมกับอุปกรณ์รักษาความปลอดภัย ทุกสภาพแวดล้อม

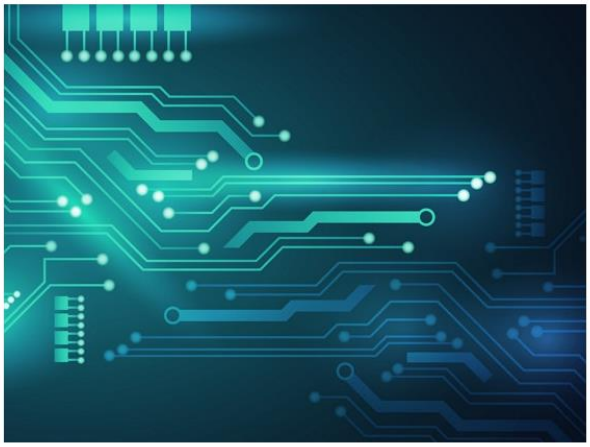
AISVA ของ MONITORAPP ให้การมองเห็น IPS, WAF, APT, DLP ฯลฯ เพื่อทำงานร่วมกับอุปกรณ์รักษาความปลอดภัยที่มีอยู่เพื่อประสิทธิภาพสูงสุดของอุปกรณ์รักษาความปลอดภัยแต่ละชิ้น มีการเข้ารหัสสำหรับโปรโตคอลแอปพลิเคชันทั้งหมดที่ใช้ SSL/TLS มาตรฐาน เช่น POP3, SMTPS และ FTPS รองรับเวอร์ชันโปรโตคอลต่างๆ ตั้งแต่ SSLv3 ถึง TLS1.0, TLS1.1, TLS1.2 และ TLS 1.3 และอัลกอริธึมต่างๆ เช่น RSA, AES, MD5 การมองเห็นเดียวกันสำหรับเครือข่าย IPv4, IPv6

สำหรับการรับส่งข้อมูลที่เข้ารหัสสองทาง

การรับส่งข้อมูลที่เข้ารหัสที่เข้าสู่ศูนย์ข้อมูลภายในจะได้รับการประมวลผลตาม IP: PORT หรือข้อมูลโดเมนที่ระบุสำหรับการถอดรหัส และการรับส่งข้อมูลที่เข้ารหัสที่สื่อสารกับส่วนอินเทอร์เน็ตภายนอกจะเลือกและถอดรหัสการรับส่งข้อมูล SSL/TLS โดยอัตโนมัติโดยไม่ต้องระบุเป้าหมายการถอดรหัสแยกต่างหาก

รับรองความเร็วสูงสุด

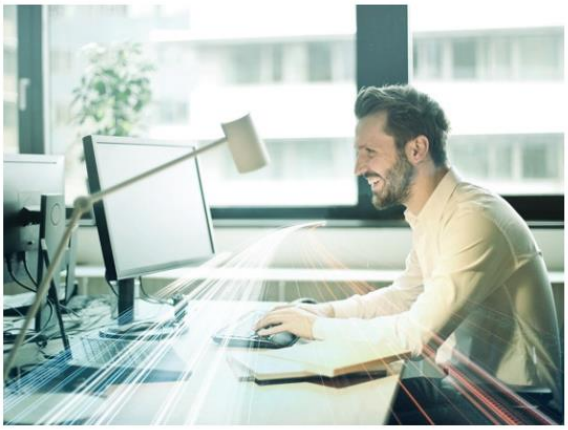
AISVA มอบประสิทธิภาพที่ดีที่สุดในอุตสาหกรรมโดยการรวมเทคโนโลยีการประมวลผลการเข้ารหัส/ถอดรหัสซอฟต์แวร์และเทคโนโลยีการประมวลผลฮาร์ดแวร์ (SSL Accelerator Card) สำหรับการรับส่งข้อมูล SSL/TLS ที่ใช้ Full Transparent Proxy ช่วยลดความล่าช้าของเครือข่ายสำหรับการประมวลผลการรับส่งข้อมูลการเข้ารหัส



MONITORAPP

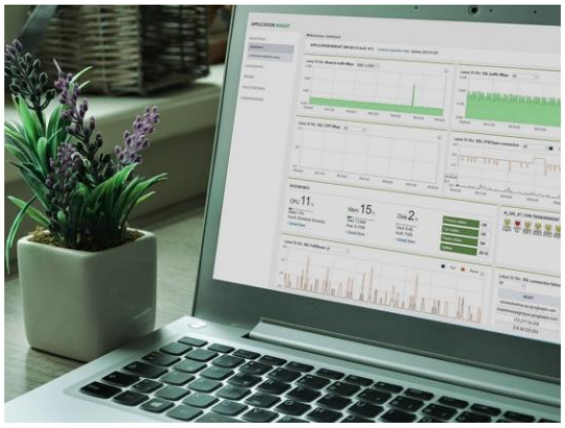
รองรับสภาพแวดล้อมการกำหนดค่าที่หลากหลาย

เทคโนโลยี Transparent Proxy ช่วยให้ปรับใช้ได้ง่ายโดยไม่ต้องเปลี่ยนการกำหนดค่าเครือข่าย โซลูชันการรักษาความปลอดภัยแบบอินไลน์ในส่วนที่ใช้งานและโซลูชันการรักษาความปลอดภัยแบบนอกเส้นทางในส่วนพาสซีฟจะรักษาการกำหนดค่าเครือข่ายที่มีอยู่ของโซลูชันการรักษาความปลอดภัยต่างๆ โดยให้การจัดการการรับส่งข้อมูลเครือข่าย NAT, หลายส่วน และแบบอะซิงโครนัส อำนวยความสะดวกในการปรับใช้งานการกำหนดค่าเครือข่ายใหม่สำหรับโซลูชันความปลอดภัยต่างๆ



จัดการการรับส่งข้อมูลอย่างรวดเร็วโดยไม่มีปัญหาเกี่ยวกับใบรับรอง

การคัดกรองการรับส่งข้อมูล SSL/TLS อัตโนมัติและการเข้ารหัสจะดำเนินการเพื่อให้มองเห็นการรับส่งข้อมูลขาออก เราทำให้สะดวกยิ่งขึ้นด้วยการมอบการแจกจ่ายใบรับรองที่จำเป็นสำหรับการเข้ารหัสและถอดรหัส SSL โดยอัตโนมัติ รายการแอปพลิเคชันที่ไม่สามารถสื่อสารผ่าน SSL ได้เนื่องจากการปักหมุดใบรับรองจะได้รับการอัปเดตเป็นประจำ นอกจากนี้ยังช่วยให้สามารถเรียนรู้ด้วยตนเองและข้ามการตั้งค่าระบบ นอกเหนือจากรายการที่อัปเดตเท่านั้น จึงช่วยขจัดปัญหาที่เกิดจากการตรึงใบรับรอง เพื่อให้มองเห็นการรับส่งข้อมูลขาเข้า จะต้องแทรกใบรับรองและคีย์ส่วนตัวเดียวกันในเซิร์ฟเวอร์ SSL ลงใน AISVA ใบรับรองที่แทรกและคีย์ส่วนตัวจะได้รับการเข้ารหัสและจัดการอย่างปลอดภัยในระบบ



ง่ายต่อการจัดการ

ผู้ดูแลระบบสามารถตรวจสอบการรับส่งข้อมูลเครือข่ายโดยรวมและการรับส่งข้อมูล SSL สำหรับ SSL Full Handshake และการใช้ซ้ำ เหตุการณ์จะถูกบันทึกสำหรับการรับส่งข้อมูลที่เข้ารหัสทั้งหมดที่ได้รับการประมวลผล และเหตุการณ์สำหรับการรับส่งข้อมูลที่เข้ารหัสแบบบายพาสก็จะถูกบันทึกเช่นกัน คุณสามารถกำหนดค่าไคลเอนต์ เซิร์ฟเวอร์ และ URL ได้อย่างยืดหยุ่นเพื่อแยกออกจากการถอดรหัส

MONITORAPP

คุณสมบัติที่สำคัญของ AISVA

1) เพิ่มประสิทธิภาพความเข้ากันได้ของเครือข่าย

> พร็อกซีโปร่งใสทั้งหมด: ไม่จำเป็นต้องเปลี่ยนการกำหนดค่าเครือข่ายที่มีอยู่

> รักษาเซสชัน TCP โดยสมบูรณ์ ข้อมูลเพื่อทำงานร่วมกับโซลูชั่นรักษาความปลอดภัยที่แตกต่างกันได้อย่างราบรื่น

2) โซนที่ใช้งานอยู่

> ให้การมองเห็นโซลูชันการรักษาความปลอดภัยแบบอินไลน์ เช่น NG F/W, DLP, IPS และ WAF

> ใช้งานอยู่: การดำเนินการพร็อกซีในเซสชัน SSL/TLS เพื่อดำเนินการเข้ารหัส/ถอดรหัส

3) โซนพาสซีฟ

> ให้การมองเห็นโซลูชันการรักษาความปลอดภัยนอกเส้นทาง เช่น การกรอง URL, IDS และเซิร์ฟเวอร์รวบรวมบันทึก

> แบบพาสซีฟ: วิธีการคัดลอกการรับส่งข้อมูลที่ถอดรหัสแล้วในโซนที่ใช้งานอยู่และส่งไปยังโซลูชันความปลอดภัย

4) รองรับการรับส่งข้อมูล SSL/TLS มาตรฐาน

> SSL3.0, TLS1.0, TLS1.1, TLS1.2, TLS1.3

5) รองรับอัลกอริธึมการเข้ารหัสที่หลากหลาย

> RSA และ EDH ดอกเคมีเลีย

> AES, DES, เมลิดพีซ, 3DES, RC4

> MD5, SHA-1, SHA-2

6) การระบุเนื้อหาแอปพลิเคชันเครือข่าย

> ระบุประเภทแอปพลิเคชันของการรับส่งข้อมูลที่เข้ารหัส เช่น Office 365, Google APP, Amazon, MSN เป็นต้น

7) การจัดการรายการ PKP

> จัดให้มีการอัปเดตออนไลน์ของแอปพลิเคชันและรายการโดเมนที่ไม่สามารถถอดรหัสได้ การปักหมุดคีย์สาธารณะ

8) ตรวจสุขภาพโซนแอคทีฟ

> การตรวจจับความผิดปกติของโซนที่ใช้งานอยู่และบายพาสผ่านการตรวจสุขภาพ

9) การสนับสนุนสภาพแวดล้อม NAT

> การระบุเซสชันและการเข้ารหัส/ถอดรหัส แม้ว่า NAT (การแปลที่อยู่เครือข่าย) จะเกิดขึ้นในโซนที่ใช้งานอยู่ก็ตาม

10) ความสะดวกในการใช้งานต่างๆ

> แดชบอร์ดรวมแบบเรียลไทม์

> การจัดหาเนื้อหาที่จำเป็นสำหรับการดำเนินงาน

- การบันทึกด้วย Payload สำหรับเซสชันการถอดรหัส
- การบันทึกเซสชันและเหตุผลที่ล้มเหลว
- การบันทึกเซสชันบายพาสและเหตุผล
- สถิติ/การค้นหาไคลเอ็นต์การติดตั้งใบรับรอง

> การตั้งค่านโยบายที่ง่าย

- การระบุการรับส่งข้อมูลที่เข้ารหัสโดยอัตโนมัติ
- การจัดการข้อยกเว้นเพียงคลิกเดียว

การสำรองข้อมูลและการกู้คืนนโยบายอัตโนมัติ

- การซิงโครไนซ์นโยบายแบบเรียลไทม์ระหว่างหลายระบบ

MONITORAPP

ประโยชน์หลักของ AISVA

การมองเห็นแบบบูรณาการ

>มีโหมด Full Transparent Proxy ที่ไม่ส่งผลต่อเครือข่ายที่มีอยู่

- การกำหนดค่าสำหรับการป้องกันเซิร์ฟเวอร์ภายใน
  : การมองเห็นการจราจรขาเข้า
- การกำหนดค่าสำหรับการป้องกันผู้ใช้ภายใน
  : การมองเห็นการจราจรขาออก
- คัดลอกทราฟฟิกที่ถอดรหัสแล้วส่งไปยังโซลูชั่นความปลอดภัย

> รองรับ SSL3.0, TLS 1.0, TLS1.1, TLS1.2, TLS1.3 และอัตโนมัติระบุการรับส่งข้อมูลที่เข้ารหัส

> รองรับอัลกอริธึมการเข้ารหัสที่หลากหลาย เช่น RSA, DH, DHE

> จำแนกประเภทแอปพลิเคชันของการรับส่งข้อมูลที่เข้ารหัส เช่น Office365, IOS, Google APP เป็นต้น

> การตรวจจับใบรับรองที่ไม่ถูกต้องโดยอัตโนมัติ

> รองรับ ALPN (การเจรจาโปรโตคอลชั้นแอปพลิเคชัน)

> รองรับสภาพแวดล้อมเครือข่าย NAT (การแปลที่อยู่เครือข่าย)

> รองรับสภาพแวดล้อมเครือข่ายการรับส่งข้อมูลแบบอะซิงโครนัส

การจัดการและการดำเนินงานที่ง่ายดาย

> แดชบอร์ดที่ผสานรวมที่ใช้งานง่าย เช่น การรับส่งข้อมูล การถอดรหัสสำเร็จ/ล้มเหลว เวอร์ชันโปรโตคอลการเจรจา สถานะสถิติ Cipher-Suite ฯลฯ

> บายพาสอัตโนมัติเมื่อเกิดปัญหาในส่วนการเชื่อมต่อระบบรักษาความปลอดภัย

> การบันทึกเนื้อหาข้อมูลที่ถอดรหัส

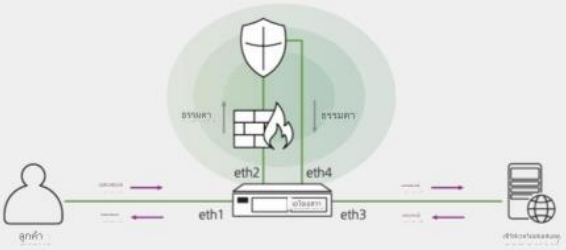
> แสดงสาเหตุของความล้มเหลวในการเจรจาสำหรับเซสชันที่ไม่สามารถถอดรหัสได้

> การจัดจำหน่ายและการจัดการใบรับรองสำหรับขาออก
- ระบุไคลเอ็นต์การติดตั้งใบรับรองและเปลี่ยนเส้นทางหน้าการติดตั้ง
- อัปเดตสถานะการติดตั้งใบรับรองอัตโนมัติผ่าน NAC

> การจัดการใบรับรองสำหรับขาเข้า
- รองรับใบรับรองหลายโดเมนและนามสกุลไฟล์ต่างๆ
- การซิงโครไนซ์รายการ Cipher-Suite โดยอัตโนมัติกับเซิร์ฟเวอร์ที่จะถอดรหัส
- การแจ้งเตือนการหมดอายุของใบรับรองและการตั้งค่าบายพาสอัตโนมัติเมื่อหมดอายุ

> อัปเดตออนไลน์ของรายการ PKP (Public Key Pinning)

การปรับใช้เครือข่าย AISVA



Active - ทำงานร่วมกับระบบรักษาความปลอดภัยแบบอินไลน์

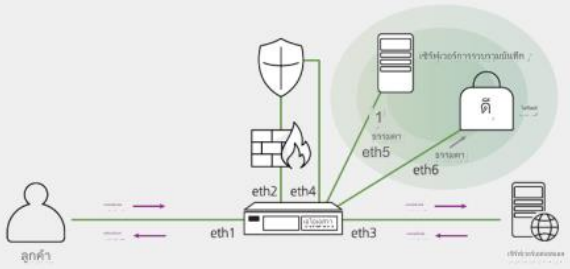
> ปรับใช้แบบอินไลน์และไม่จำเป็นต้องเปลี่ยนแปลงการกำหนดค่าเครือข่าย

> บายพาส S/W และบายพาส H/W ในกรณีที่เกิดความล้มเหลว

> รองรับการประมวลผลการรับส่งข้อมูลแบบหลายส่วนและแบบอะซิงโครนัส

> ถอดรหัสการรับส่งข้อมูลที่เข้ารหัสและส่งการรับส่งข้อมูลต้นทางไปยังลิงก์

> เข้ารหัสการรับส่งข้อมูลการถอดรหัสที่ได้รับอีกครั้งและส่งไปยังปลายทาง



Passive - ทำงานร่วมกับระบบรักษาความปลอดภัยนอกเส้นทาง

> คัดลอกการรับส่งข้อมูลที่ถอดรหัสในโซนที่ใช้งานอยู่ และส่งไปยังระบบที่เชื่อมต่อกัน

> การขยายโซลูชันเป้าหมายการทำงานร่วมกันตามจำนวนพอร์ต NIC ทางกายภาพ