

APPLICATION **i**NSIGHT SWG

Intelligent Secure Web Gateway | *ai*swg



AISWG – Secure Web Gateway (MONITORAPP)

Secure Web Gateway หรือ SWG เป็นโซลูชันป้องกันภัยคุกคามทางไซเบอร์ ปกป้องผู้ใช้จากภัยคุกคามบนเว็บ นอกเหนือจากการใช้และบังคับใช้นโยบายการใช้งานที่ได้รับการยอมรับขององค์กร ผู้ใช้จะเข้าถึง SWG ซึ่งมีหน้าที่ในการเชื่อมต่อผู้ใช้กับเว็บไซต์ที่ต้องการและใช้งานฟังก์ชันต่าง ๆ เช่น การกรอง URL การเปิดเผยเว็บ การตรวจสอบเนื้อหาที่เป็นอันตราย การควบคุมการเข้าถึงเว็บ และมาตรการรักษาความปลอดภัยอื่น ๆ

- บล็อกการเข้าถึงเว็บไซต์ หรือเนื้อหาที่ไม่เหมาะสมตามนโยบายขององค์กร
- บังคับใช้นโยบายความปลอดภัย เพื่อให้การเข้าถึงอินเทอร์เน็ตปลอดภัยยิ่งขึ้น
- ช่วยปกป้องข้อมูลจากการถ่ายโอนโดยไม่ได้รับอนุญาต

URL Filtering

การกรอง URL เป็นโซลูชันการรักษาความปลอดภัยเว็บที่ควบคุมการเข้าถึงเว็บไซต์ตาม URL เพื่อป้องกันไม่ให้พนักงานเข้าถึงเนื้อหาที่เป็นอันตรายหรือไม่เหมาะสม การรับส่งข้อมูลทางอินเทอร์เน็ตนั้นถูกป้องกันหรืออนุญาตตามหมวดหมู่ URL ผู้ใช้ กลุ่ม หรือเครื่อง ด้วยการกรอง URL ผู้ดูแลระบบสามารถรับข้อมูลว่าพนักงานคนใดกำลังเข้าถึงเว็บไซต์ใด

Application Control

การควบคุมแอปพลิเคชันช่วยให้ผู้ดูแลระบบสามารถสร้างนโยบายความปลอดภัยเว็บแบบละเอียดตามผู้ใช้เพื่อระบุ บล็อก หรือจำกัดการใช้งานเว็บแอปพลิเคชันและวิดเจ็ต สิ่งนี้ทำให้มั่นใจได้ว่าข้อมูลที่ใช้และแบ่งปันระหว่างแอปพลิเคชันนั้นเป็นส่วนตัวและปลอดภัยภายในองค์กร

Data Loss Prevention

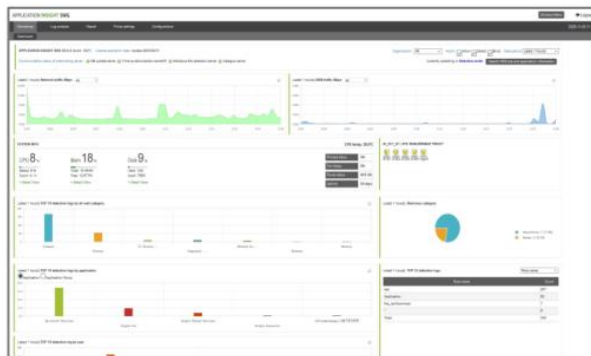
การป้องกันข้อมูลสูญหาย (DLP) ช่วยให้เห็นใจได้ว่าข้อมูลสำคัญและละเอียดอ่อนจะไม่ถูกส่งออกไปนอกเครือข่ายขององค์กร การป้องกันการสูญหายของข้อมูลช่วยปกป้องธุรกิจของคุณจากการสูญเสียข้อมูลที่มีค่าและละเอียดอ่อนโดยไม่ตั้งใจ โดยการติดตามความเคลื่อนไหวของข้อมูลและปฏิบัติตามกฎระเบียบและมาตรฐานการปฏิบัติตามข้อกำหนด



ประโยชน์หลักของ AISWG

การควบคุมเว็บและการมองเห็นที่ปลอดภัย	การจัดการและการทำงานของอุปกรณ์ที่สะดวก
> วิเคราะห์การรับส่งข้อมูลค่าขอเพื่อล็อกการเข้าถึง URL ที่เป็นอันตรายและไม่เกี่ยวข้องกับการทำงาน - มีหมวดหมู่การกรอง URL มากกว่า 60 หมวดหมู่เพื่อจัดการนโยบายที่ง่ายด้วย > วิเคราะห์การรับส่งข้อมูลการตอบสนองเพื่อป้องกันการกรุกของมัลแวร์ > บล็อกคุกกี้ C&C และการรับส่งข้อมูลมัลแวร์ > ควบคุมบริการเว็บเนลยอดนิยตามฟังก์ชัน > ให้ความสำคัญความปลอดภัยระดับเดียวกันสำหรับ HTTP และ HTTPS > บล็อกโปรแกรมพร็อกซีและ VPN ที่พยายามเสี่ยงผ่าน SWG > จัดเตรียมการกรองแอปพลิเคชัน เช่น แอปโซเชียลมีเดียและแอป Messenger > WEB DLP พร้อมการควบคุมไฟล์แนบด้วยคำหลักและนิพจน์ทั่วไป > Youtube กรองตามเนื้อหา > เว็บแคชและ QoS เพื่อปรับปรุงคุณภาพบริการเว็บ	> โหมดความโปร่งใสไม่ส่งผลกระทบต่อเครือข่ายที่มีอยู่ > โหมดการกำหนดค่า HA (ความพร้อมใช้งานสูง): ใช้งาน-สแตนด์บาย, ใช้งาน-ใช้งานอยู่ > รองรับสภาพแวดล้อม NAT/DHCP ผ่านการตรวจสอบผู้ใช้ > จัดการผู้ใช้หลายคนได้อย่างง่ายดายด้วยการสร้างกลุ่มผู้ใช้ > การถอดรหัสด้วยตนเอง/การเข้ารหัสการรับส่งข้อมูล SSL - หน้าการแจกจ่ายใบรับรอง SSL เพื่อการปรับใช้ที่ง่ายดาย - ส่งกราฟฟิค HTTPS ที่ถอดรหัสแล้วไปยังโซลูชันความปลอดภัยบุคคลที่สาม > แดชบอร์ดที่ครอบคลุมพร้อมการอัปเดตแบบเรียลไทม์ > จัดทำรายงานและบันทึกต่างๆ เช่น การตรวจจับ/การเชื่อมต่อ SSL/บันทึกการตรวจสอบ > รายการ PKP ที่อัปเดตเป็นประจำสำหรับการเลือกนายพาสา

GUI การดูแลระบบ AISWG



1) การตรวจสอบระบบ

- > สถานะระบบเรียลไทม์และข้อมูลการรับส่งข้อมูล

2) การวิเคราะห์บันทึก

- > การวิเคราะห์บันทึกโดยละเอียดพร้อมตัวเลือกการค้นหาที่หลากหลาย
- > การบันทึกประวัติการเข้าถึงเว็บโดยไคลเอนต์

3) การกำหนดนโยบาย

- > การตั้งค่านโยบายโดยละเอียดโดยผู้ใช้หรือตามกลุ่ม

4) สถิติและการรายงาน

- > รายงานโดยละเอียดเกี่ยวกับสถานะการรับส่งข้อมูลและข้อมูลการตรวจจับการโจมตีต่างๆ เช่น IP, URL, ผู้ใช้ และหมวดหมู่

คุณสมบัติที่สำคัญของ AISWG

1) โหมดการกำหนดค่าเครือข่ายต่างๆ

- > อินเทอร์เน็ต: พร็อกซีแบบโปร่งใสเต็มรูปแบบ
- > ไม่อยู่ในเส้นทาง: ส่งต่อพร็อกซี, มิเรอร์

2) แพลตฟอร์มข่าวกรองภัยคุกคาม

- > อัปเดตข้อมูลภัยคุกคามแบบเรียลไทม์โดย AICC
- > URL ตามการเรียนรู้ของเครื่องและการวิเคราะห์ไฟล์ และหลักฐานโดยละเอียดที่ให้ไว้

3) การรับรองความถูกต้องของผู้ใช้

- > การตั้งค่านโยบายแบบเต็มโดยผู้ใช้ในสภาพแวดล้อม NAT/DHCP พร้อมการตรวจสอบสิทธิ์ผู้ใช้

4) การจัดการกลุ่มและผู้ใช้

- > การจัดการผู้ใช้ที่ง่ายผ่านการสร้างองค์กรและนโยบายอิสระตามองค์กร

5) การบันทึกการเข้าถึงแบบเต็ม

- > การบันทึกประวัติการเข้าถึงเว็บของไคลเอนต์ทั้งหมด

6) รองรับ HTTP/2 เต็มรูปแบบ

- > รองรับการเชื่อมต่อและการแยกวิเคราะห์ HTTP/2
- > มีฟังก์ชันความปลอดภัยเช่นเดียวกับ HTTP/1.1

7) การเข้ารหัส/ถอดรหัสการรับส่งข้อมูล SSL ด้วยตนเอง

- > จัดการกับความปลอดภัยที่ซ่อนอยู่ในการรับส่งข้อมูล SSL ด้วยการเข้ารหัส/ถอดรหัสด้วยตนเอง
- > ส่งพร็อกซี HTTPS ที่ถอดรหัสแล้วไปยังโฮสต์ความปลอดภัยของบุคคลที่สาม

8) เว็บ DLP

- > ป้องกันข้อมูลรั่วไหลผ่านการตรวจสอบแพ็คเกจเชิงลึก
- > สร้างกฎที่มีเงื่อนไขต่างๆ เช่น คำสำคัญ นิพจน์ทั่วไป นามสกุลไฟล์ และขนาด

9) ตัวกรองหมวดหมู่

- > การตั้งค่าการควบคุมเว็บไซต์ที่ง่ายด้วยหมวดหมู่หมวดหมู่มากกว่า 60 รายการ (หุ้น ซอปปิง เกม โซเชียลมีเดีย ฯลฯ)

10) การเร่งความเร็วของเว็บ

- > ลดการรับส่งข้อมูลและเวลาตอบสนองผ่านการแคชเว็บ

11) การกรองแอปพลิเคชันเครือข่าย

- > แยกแยะจากการเข้าชมเว็บแล้ว SWG ยังมีการกรองแอปพลิเคชันและสามารถตรวจจับแอปพลิเคชันได้มากกว่า 1,000 รายการ

12) การบล็อกการโจมตี ATP

- > การกรองการเข้าถึง URL ที่เป็นอันตราย
- > การกรองเซิร์ฟเวอร์ C&C และการรับส่งข้อมูลมัลแวร์
- > วิเคราะห์ไฟล์แบบและตรวจจับ/บล็อก URL ที่เป็นอันตรายอยู่ในไฟล์แนบหรือไม่
- > ตรวจจับ/บล็อกโค้ดที่เป็นอันตรายในเพจโฮสต์การตอบสนอง
- > (ทางเลือก) การแยกไฟล์แบบเรียลไทม์และการวิเคราะห์แบบคงที่/ไดนามิกจากการเข้าชมเว็บ

13) การจัดการรายการ PKP

- > รักษาความปลอดภัยของบริการผ่านรายการ PKP ที่อัปเดตเป็นประจำ

AICC สำหรับข่าวกรองภัยคุกคาม



การปรับใช้เครือข่าย AISWG

