Aruba 360 Secure Fabric โซลูชั่นระบบความปลอดภัยบนเครือข่ายช่วยลดความเสี่ยงในยุคแห่งอุปกรณ์พกพา คลาวด์ และ อินเตอร์เน็ตของสรรพสิ่ง

Aruba 360 Secure Fabric มาพร้อมกับความสามารถในการขับเคลื่อนด้วยการวิเคราะห์ (analytics-driven) ใหม่ ๆ มีการป้องกันภัยไซเบอร์ที่ล้ำสมัยเพียบพร้อมด้วยนวัตรกรรมเกี่ยวกับ UEBA ที่พัฒนามาอย่างต่อเนื่อง และช่วยให้การดูแลความปลอดภัยบนระบบเครือข่ายขององค์กรทำได้ง่ายขึ้น

กรุงเทพมหานคร,วันที่ 16 มกราคม พ.ศ. 2561- อรูบ้าบริษัทหนึ่งในเครือฮิวเลตต์ แพคการ์ด เอ็นเตอร์ไพรส์ (NYSE:HPE) ได้ประกาศเปิดตัว Aruba 360 Secure Fabric ชุดผลิตภัณฑ์ซอฟต์แวร์ที่เป็นเฟรมเวิร์กให้องค์กรต่าง ๆ สามารถทำการขับเคลื่อนการวิเคราะห์ตรวจจับการโจมตีภัยออนไลน์แบบ 360 องศาและตอบโต้ได้ในทันควัน เพื่อช่วยลดความเสี่ยงขององค์กรจากการโจมตีที่มีการเปลี่ยนแปลงรูปแบบอยู่ตลอดเวลาในทุกวันนี้ อรูบ้ายังเป็นผู้สรรค์สร้างนวัตกรรมหลายประการใน User and Entity Behavioral Analytics (UEBA) โดยการเพิ่มผลิตภัณฑ์ในกลุ่ม Aruba IntroSpect ทำให้องค์กรต่าง ๆ มีการตรวจจับพฤติกรรมผิดปกติในระบบเครือข่ายโดยใช้ machine-learning ที่ขยายได้อย่างง่ายดายและรวดเร็วโดยเริ่มจากโครงการเล็ก ๆ และขยายให้ครอบคลุมทั่วทั้งองค์กรขนาดใหญ่ได้ในอนาคต

Gartner ทำการวิจัยเกี่ยวกับภัยคุกคามภายในองค์กร (insider threats) พบว่าองค์กรต่าง ๆ ไม่ค่อยสนใจเกี่ยวกับความเสี่ยงภายในองค์กรที่เกิดจากผู้ใช้ภายใน (trusted users) ของตนอย่างเพียงพอ ถึงแม้ว่ามีตัวอย่างมากมายขององค์กรที่เคยประสบภัยนี้มาแล้ว ในข้อเสนอสรุปในรายงานฉบับนี้ของ Gartner ได้แทรกคำแนะนำให้องค์กรลูกค้าของตนตระหนักถึงภัยคุกคามจากภายในที่เพิ่มขึ้นถึง 100 % และ UEBA เป็นหนึ่งในเทคโนโลยีหลักที่ควรจะนำมาใช้ป้องกันภัยนี้

เพื่อช่วยให้องค์กรสามารถระบุภัยคุกคามใหม่ ๆ และไม่รู้ตัวมาก่อนนี้ได้ Aruba 360 Secure Fabric เสนอเพิ่มความสามารถใหม่ให้แก่ระบบความปลอดภัย (security) และทีมงาน IT ด้วยวิธีการที่ครบวงจรในการตรวจจับอย่างรวดเร็วและตอบโต้อย่างทันควันต่อการโจมตีทางไซเบอร์ จากขั้นตอน pre-authorization จนถึง post-authorization อย่างครอบคลุมแม้จะอยู่บนโครงสร้างพื้นฐานระบบเครือข่ายไอทีที่อุปกรณ์มาจากผู้ผลิตที่หลาก

หลายและสามารถรองรับองค์กรได้ทุกขนาด
องค์ประกอบของ Aruba 360 Secure Fabric มีดังต่อไปนี้ :
• Aruba IntroSpect UEBA solution: เป็นผลิตภัณฑ์ในกลุ่ม network-agnostic ตัวใหม่ที่ใช้ในการตรวจสอบ (monitoring) อย่างต่อเนื่องและเป็นซอฟต์แวร์ในการตรวจจับการโจมตีที่ก้าวหน้า ประกอบด้วยผลิตภัณฑ์ในระดับเริ่มต้นตัวใหม่ และใช้ machine-learning ตรวจจับการเปลี่ยนแปลงในพฤติกรรมของผู้ใช้และอุปกรณ์ต่าง ๆ เพื่อบ่งชี้ถึงแนวโน้มการโจมตีซึ่งต่างไปจากการป้องกันความปลอดภัยในระบบดั้งเดิมอย่างสิ้นเชิง Machine-learning algorithms จะช่วยระบุคะแนนความเสี่ยง (risk score) ที่ขึ้นอยู่กับระดับของการโจมตีและทำการแจ้งเตือนทีมงานดูแลระบบความปลอดภัยได้ทันท่วงที
• Aruba ClearPass: เป็นโซลูชั่นในการควบคุมการเข้าถึงระบบเครือข่าย (NAC) และบริหารจัดการนโยบายความปลอดภัยที่ได้รับการยอมรับอย่างสูง สามารถสร้างโปรไฟล์ให้แก่ BYOD และ IoT ทั้งผู้ใช้และอุปกรณ์ มีความสามารถทำการโต้ตอบการโจมตีโดยอัตโนมัติ ปัจจุบันถูกรวมเข้าไปอยู่ในกลุ่มผลิตภัณฑ์ Aruba IntroSpect ซอฟต์แวร์ ClearPass สามารถนำมาใช้ได้กับอุปกรณ์ของทุกผู้ผลิตที่อยู่ในระบบเครือข่าย
• Aruba Secure Core: ความสามารถในการป้องกันการโจมตีที่จำเป็นถูกฝังอยู่ในตัวอุปกรณ์ของ Aruba ทั้งหมด อันได้แก่ Wi-Fi access point , wireless controller และ switches รวมทั้งในอุปกรณ์ campus core switch และ aggregation switch รุ่น Aruba 8400 ที่พึ่งเปิดตัวไปเมื่อเร็ว ๆ นี้

ผลิตภัณฑ์ซอฟต์แวร์ในระดับเริ่มต้นตัวใหม่ในกลุ่มผลิตภัณฑ์ Aruba IntroSpect UEBA
Aruba IntroSpect Standard อยู่ในกลุ่มผลิตภัณฑ์ IntroSpect UEBA โดยมีคุณลักษณะใหม่ ๆ ถูกเพิ่มเข้าไปเช่นเดียวกับ Aruba IntroSpect Advanced ซึ่งเป็นผลิตภัณฑ์หลักของบริษัท การเพิ่มผลิตภัณฑ์ในกลุ่มผลิตภัณฑ์ IntroSpect UEBA ช่วยทำให้ทีม security มีทางเลือกเพิ่มขึ้นและมีวิธีการทำ implement UEBA ที่เร็วขึ้น Aruba IntroSpect Standard เป็นแนวทางง่าย ๆ ที่องค์กรจะสามารถเริ่มนำระบบรักษาความปลอดภัยที่ใช้ UEBA machine learning มาใช้กับแหล่งข้อมูล (data sources) ขั้นพื้นฐานเพียงไม่กี่แหล่ง ช่วยเร่งความเร็วขององค์กรในการทำ time-to-protection ให้แก่ข้อมูลองค์กรและข้อมูลลูกค้า โดยถูกออกแบบมาสำหรับทำการตรวจสอบ และตรวจจับอย่างง่าย ๆ ต่อ ความผิดปกติที่เกิดขึ้นบ่อย จุดเปราะบาง พฤติกรรมต่าง ๆ ในระบบเครือข่ายไปจนถึงอุปกรณ์พกพา คลาวด์ อุปกรณ์ IoT และแอพพลิเคชั่นทั้งหมด เพื่อระบุสัญญาณการเกิดของภัยคุกคามได้ก่อนที่จะขยายตัวออกไปและทำสัญญาณเตือน รวมทั้งทำการป้องกันการรั่วไหลของข้อมูล
ระบบสามารถเรียนรู้จาก common data source จากแหล่งต่าง ๆ อันได้แก่ Microsoft Active Directory หรือ LDAP authentication records อื่น ๆ และ identity information , firewall logs จาก sources อื่นอย่างเช่น Checkpoint , Palo Alto networks หรือ Aruba monitoring (AMON) logs จากโครงสร้างพื้นฐานของ Aruba เอง การโต้ตอบการคุกคามทำได้อย่างรวดเร็วโดยใช้ ClearPass ทำการ กัก (quarantine) , จำกัดขอบเขต (restrict) หรือนำออกจากระบบ (remove) ต่อภัยคุกคามที่ระบุได้
ทีม security สามารถเริ่มจากนำ IntroSpect Standard มาใช้ก่อนแล้วอัพเกรดได้อย่างง่ายดายขึ้นไปเป็น

IntroSpect Advanced เมื่อมีความต้องการขยายตัวมากขึ้น

ยกระดับความสามารถในการตรวจจับภัยคุกคามได้ตั้งแต่เริ่มต้นเกิดโดยใช้ Aruba IntroSpect Advanced Edition

Aruba IntroSpect Advanced มีความสามารถในเรื่อง security ที่กว้างมากกว่า IntroSpect Standard ในกา ตรวจจับการโจมตีโดยการหาความสัมพันธ์ของข้อมูลจาก data sources ที่กว้างขวางและครอบคลุมมากกว่า ช่วย ในการตรวจสอบเหตุการณ์ผิดปกติได้อย่างรวดเร็วขึ้น และปรับปรุงการตามล่าภัยคุกคาม การค้นหา และทำการ วิเคราะห์ตรวจสอบร่องรอยเชิงลึก (deep forensics) ได้ดีขึ้น โดยประกอบด้วย machine learning model มาก กว่า 100 models ทั้งแบบที่ต้องกำกับดูแลและไม่ต้องกำกับดูแล ทำให้สามารถทำ unmatched analytics และ ตรวจสอบร่องรอยจากข้อมูลที่เป็น packet , flow , logs ,alerts , endpoint และรวมถึง traffic ของอุปกรณ์พกพา คลาวด์ และอุปกรณ์ IoT ทั้งหมด เพิ่มความสามารถขององค์กรในการระบุความเสี่ยงได้อย่างมีประสิทธิผลชัดเจน คุณลักษณะใหม่ ๆ ของ IntroSpect Advanced ประกอบด้วย:

• ระบบรักษาความปลอดภัยอัจริยะ (Smart Security) ด้วย Dynamic Machine Learning, ทำให้ทีม security สามารถทำการปรับแต่ง analytical model ของ IntroSpect ได้ง่ายโดยดูที่สภาพแวดล้อมของการโจมตีล่าสุดและ จัดลำดับความสำคัญของการป้องกัน ประกอบด้วย “chaining” ที่มี 100+ out-of-the box machine learning models ซึ่งสามารถนำมาเชื่อมต่อเข้าด้วยกันเพื่อสร้าง detection scenarios และ จัดทำความสัมพันธ์ของคะแนน ความเสี่ยงใหม่ ๆ ได้

• จัดกลุ่ม อุปกรณ์พกพา คลาวด์ และ IoT โดยใช้ Device Peer Group: ใช้ความสามารถในการทำโปรไฟล์ของ ClearPass จัดกลุ่มอุปกรณ์เข้าเป็นกลุ่ม ๆ ที่เหมือนกันแม้จะรู้เพียง IP address ของมัน อย่างเช่น ClearPass จะ แยกประเภทว่าเป็นกล้องวงจรปิดหรือเซ็นเซอร์ในโรงงาน แล้ว IntroSpect จะเทียบพฤติกรรมของมันกับเพื่อนที่ อยู่ในกลุ่มเดียวกันตัวอื่น ๆ IntroSpect จะตรวจหาพฤติกรรมที่ผิดปกติของอุปกรณ์โดยเทียบกับตัวอื่น ๆ ในกลุ่ม เดียวกัน เป็นความสามารถที่สำคัญมากในการทำให้ UEBA สามารถทำงานได้ครอบคลุมทุกประเภทของอุปกรณ์ IoT ที่เพิ่มขึ้นอย่างรวดเร็วขณะนี้

• เข้าแก้ไขการโจมตีได้เร็วขึ้นด้วย Integrated Attached Response: ช่วยให้สามารถวิเคราะห์ระบบความ ปลอดภัยเพื่อตอบโต้การโจมตี โดยกระตุ้นให้เกิดการตอบโต้ที่ ClearPass ในทันทีโดยตรงจาก IntroSpect console.

สร้างรากฐานของระบบเครือข่ายให้น่าเชื่อถือและปลอดภัยด้วย Aruba Secure Core

อุปกรณ์ในโครงสร้างพื้นฐานของระบบเครือข่ายทุกผลิตภัณฑ์ล้วนฝัง Aruba Secure Core ไว้ซึ่งมีความจำเป็น อย่างสูงในการป้องกันระบบเครือข่ายทุกระบบ ประกอบด้วย secure boot , embedded firewall , centralized encryption , deep packet inspection และ intrusion prevention การออกแบบโครงสร้างพื้นฐานที่เป็น เอกลักษณ์นี้ช่วยลดอันตรายจาก physical tempering ขณะเดียวกันก็ทำการป้องกันและตรวจสอบการจราจรบน ระบบเครือข่าย

การนำ Aruba IntroSpect UEBA และ Araba ClearPass เชื่อมเข้ากับ Aruba Secure Core ทำให้สามารถสร้าง

การป้องกันที่ต่อเนื่องตั้งแต่การค้นหาอุปกรณ์และการตรวจจับการเข้าถึงเพื่อโจมตีและทำการตอบโต้ ช่วยให้ลูกค้าของอรูบ้ามีความสามารถที่โดดเด่นในการตรวจจับการโจมตีและทำการตอบโต้โดยอัตโนมัติหรือวิเคราะห์หาแนวทางในการป้องกันทรัพย์สินที่มีคุณค่าขององค์กร ตั้งแต่การทำ network reauthentication ไปจนถึงการกักหรือทำการขึ้นบัญชีดำผู้ใช้และอุปกรณ์ที่เป็นภัยคุกตาม
โครงการ Araba Security Exchange : การป้องกันระบบอย่างครบวงจรครอบคลุมอุปกรณ์ของทุกผู้ผลิตที่อยู่ในระบบเครือข่าย
Aruba 360 Security Exchange เป็นโครงการที่ประกอบด้วยพาร์ทเนอร์และแหล่งเทคโนโลยีต่าง ๆ จาก IntroSpect Technology Partner program และ Aruba ClearPass Partner program มีโซลูชั่นด้าน security และโครงสร้างพื้นฐานชั้นนำมากกว่า 100 ผลิตภัณฑ์เข้าร่วมโครงการ ทำให้ลูกค้าและ channel partners ทำการตรวจสอบความสามารถในการทำงานร่วมกันได้ง่าย จึงสามารถสร้างระบบให้ใช้งาน (deploy) ได้เร็วและมั่นใจได้ ลูกค้าของอรูบ้ายังสามารถใช้ประโยชน์จากการลงทุนในระบบ security เดิมด้วยการเชื่อมต่อเข้ากับโซลูชั่นของ อรูบ้าได้อย่างราบรื่น เป็นผลดีอันเนื่องมาจากโซลูชั่นของอรูบ้ามีความเป็นอันหนึ่งอันเดียวกัน และมีความยืดหยุ่นจากการออกแบบมาให้เป็นระบบเปิด (open architecture)

เกี่ยวกับอรูบ้าบริษัทหนึ่งในเครือบริษัทฮิวเลตต์ แพคการ์ด เอ็นเตอร์ไพรส์

อรูบ้าหนึ่งในเครือบริษัทฮิวเลตต์ แพคการ์ด เอ็นเตอร์ไพรส์และเป็นผู้นำในการจัดหาโซลูชั่นระบบเครือข่ายที่ล้ำสมัยสำหรับองค์กรทุกขนาดทั่วโลก บริษัทเป็นผู้ผลิตโซลูชั่นด้านไอทีที่ช่วยเพิ่มพลังให้องค์กรในการให้บริการแก่ผู้ใช้รุ่นใหม่ที่ต้องพึ่งพาอุปกรณ์พกพาผู้ซึ่งใช้ apps ต่าง ๆ ทางธุรกิจที่วางอยู่บนคลาวด์ในทุก ๆ ขั้นตอนของการดำเนินชีวิตทั้งในที่ทำงานและเรื่องส่วนตัว
เรียนรู้เพิ่มขึ้น เกี่ยวกับอรูบ้าได้ที่ http://www.arubanetworks.com ถ้าต้องการข้อมูลที่ล่าสุดตลอดเวลาสามารถติดตามโดยการ follow onTwitter และ Facebook สำหรับการพูดคุยทางเรื่องเทคโนโลยีล่าสุดเกี่ยวกับ mobility และผลิตภัณฑ์ของอรูบ้า เยี่ยมชม Airheads Social ที่ http://community.arubanetworks.com.