

# วีเอ็มแวร์เผยกลยุทธ์ระบบซีเคียวริตี้ภายในระดับองค์กร เปิดตัว Service-defined Firewall รายแรกในอุตสาหกรรม



โซลูชันไฟร์วอลล์เพื่อปกป้องจากภายในองค์กรรุ่นใหม่ ที่มีระบบตรวจสอบสถานะพฤติกรรมการทำงาน ทั้งระดับเครือข่ายและโฮสต์ เพื่อลดช่องทางการโจมตีมากขึ้น

กรุงเทพฯ – 18 เมษายน 2562 – บริษัท วีเอ็มแวร์ (NYSE: VMW) เผยกลยุทธ์การช่วยเหลือองค์กรต่างๆ เพื่อสร้างความได้เปรียบเหนือกลุ่มคนร้ายที่มีแผนโจมตีระบบเครือข่ายหรือระบบเน็ตเวิร์กขององค์กร ด้วยแนวทางใหม่ที่มุ่งเน้นแอปพลิเคชันมากกว่าโครงสร้างพื้นฐาน และมุ่งลดช่องทางการโจมตี แทนที่จะวิ่งไล่จับภัยคุกคาม

นอกเหนือจากการนำเสนอโซลูชันซอฟต์แวร์ที่หลากหลาย ครอบคลุมตั้งแต่ระบบคลาวด์ไปจนถึงผู้ใช้แล้ว ล่าสุดวีเอ็มแวร์ได้เปิดตัวไฟร์วอลล์ที่กำหนดด้วยซอฟต์แวร์ (VMware Service-defined Firewall) ซึ่งนับเป็นแนวคิดใหม่สำหรับระบบไฟร์วอลล์ภายในองค์กร โดยจะช่วยลดช่องทางการโจมตีสำหรับระบบที่ติดตั้งในองค์กรและสภาพแวดล้อมคลาวด์ โดยอาศัยระบบรักษาความปลอดภัยที่เป็นส่วนหนึ่งของโครงสร้างพื้นฐาน ด้วยความสามารถที่เหนือชั้นของ VMware NSX และ VMware AppDefense โซลูชัน Service-defined Firewall ของวีเอ็มแวร์จะผสมรวมความสามารถในการตรวจสอบแอปพลิเคชันอย่างทั่วถึง และความเข้าใจเกี่ยวกับลักษณะการทำงานที่เป็นปกติของแอปพลิเคชัน รวมไปถึงความสามารถด้านไฟร์วอลล์อัจฉริยะที่ทำงานแบบอัตโนมัติปรับเปลี่ยนได้อย่างยืดหยุ่น เพื่อช่วยปกป้องแอป ข้อมูล และผู้ใช้ได้ดียิ่งขึ้น

นาย ราจีฟ รามาสวามิ ประธานเจ้าหน้าที่ฝ่ายปฏิบัติการด้านผลิตภัณฑ์และบริการของวีเอ็มแวร์ กล่าวว่า “ระบบซีเคียวริตี้ในปัจจุบันโดยมากแล้วไม่สามารถทำงานได้อย่างมีประสิทธิภาพ เพราะแอปพลิเคชันต่างๆ มีลักษณะกระจัดกระจายมากขึ้น โดยถูกติดตั้งและใช้งานบนระบบคลาวด์ภายในองค์กรและคลาวด์สาธารณะหลายระบบ ซึ่งใช้โครงสร้างพื้นฐานหลายประเภท และมีการเข้าถึงจากอุปกรณ์ที่แตกต่างหลากหลาย ทุกวันนี้ระบบซีเคียวริตี้ประกอบด้วยผลิตภัณฑ์ เอเจนต์ และอินเทอร์เฟซมากมาย ติดตั้งอยู่ตามจุดต่างๆ ทว่าทั้งองค์กร ก่อให้เกิดความยุ่งยากซับซ้อนในการจัดการระบบรักษาความปลอดภัย กลยุทธ์ของวีเอ็มแวร์มุ่งเน้นการขจัดความยุ่งยากซับซ้อนที่เกิดขึ้นกับระบบซีเคียวริตี้ในปัจจุบัน และนำเสนอแนวทางการรักษาความปลอดภัยจากภายในองค์กร ตั้งแต่อุปกรณ์ปลายทางไปจนถึงระบบคลาวด์”

องค์กรต่างๆ ที่กำลังดำเนินการเปลี่ยนผ่านสู่ดิจิทัล (Digital Transformation) ต้องประสบปัญหาสภาพแวดล้อมที่ซับซ้อน ซึ่งเอื้อต่อการถูกโจมตีทางคอมพิวเตอร์ ข้อมูลจาก Ponemon Institute ชี้ว่า “กรณีการรั่วไหลของข้อมูลสร้างความเสียหายเพิ่มขึ้นอย่างต่อเนื่อง และส่งผลให้ข้อมูลของผู้บริโภคสูญหายหรือถูกโจรกรรมในแต่ละปีเพิ่มมากขึ้นเรื่อยๆ” โดยเฉลี่ยแล้วกรณีการรั่วไหลของข้อมูลสร้างความเสียหายโดยรวมประมาณ 2.53 ล้านดอลลาร์ในภูมิภาคอาเซียน(1) ในขณะเดียวกัน ยอดใช้จ่ายสำหรับฮาร์ดแวร์ ซอฟต์แวร์ และบริการที่เกี่ยวข้องกับการรักษาความปลอดภัยในเอเชีย-แปซิฟิกคาดว่าจะแตะระดับ 28.76 พันล้านดอลลาร์ภายในปี 2565 เพิ่มขึ้นกว่า 20 เปอร์เซ็นต์ในช่วงปี 2560-2565 ตามข้อมูลจากไอดีซี (IDC)(2)

วีเอ็มแวร์เชื่อว่าอุตสาหกรรมจำเป็นที่จะต้องเปลี่ยนย้ายจากรูปแบบที่มุ่งเน้นการไล่ล่าลักษณะการทำงานที่ผิดปกติไปสู่การตรวจสอบให้แน่ใจว่าระบบทำงานเป็นปกติ และมุ่งเน้นที่แอปพลิเคชันมากกว่าโครงสร้างพื้นฐาน แนวทางของวีเอ็มแวร์จะช่วยเพิ่มความง่ายให้กับระบบซีเคียวริตี้ซึ่งผสมรวมอยู่ใน ไม่ใช่ติดตั้งแยกต่างหาก และทำให้การรักษาความปลอดภัยมีลักษณะสอดคล้องกับแอปและข้อมูลต่างๆ ซึ่งทั้งหมดนี้จะช่วยให้องค์กรสามารถตรวจสอบแอปพลิเคชันได้อย่างละเอียดและทั่วถึง ครอบคลุมขอบเขตมากกว่าดาต้าเซ็นเตอร์ เพื่อนำเสนอพื้นที่ทำงานดิจิทัลที่ปลอดภัยมากขึ้น ช่วยปกป้องอุปกรณ์ทุกชนิดสำหรับพนักงานทุกคนที่เข้าถึงแอปและข้อมูลจากทุกๆ ที่

นายทอม จิลลิส รองประธานอาวุโสและผู้จัดการทั่วไป ส่วนธุรกิจระบบเครือข่ายและการรักษาความปลอดภัยของวีเอ็มแวร์ กล่าวว่า “ระบบซีเคียวริตี้จากภายในจะใช้ประโยชน์จากคุณลักษณะที่โดดเด่นของแพลตฟอร์มเวอร์ชวลไลเซชัน จึงช่วยให้องค์กรธุรกิจสร้างบริการใหม่ๆ ที่แตกต่างสำหรับการรักษาความปลอดภัย Service-defined Firewall ของวีเอ็มแวร์มุ่งเน้นการสร้างระบบไฟร์วอลล์สำหรับเครือข่ายภายในองค์กร และสิ่งที่แปลกใหม่ก็คือ การตรวจสอบรับรองลักษณะการทำงานที่เป็นปกติของแอปพลิเคชัน แทนการไล่ล่าภัยคุกคาม”

โซลูชัน Service-defined Firewall ของวีเอ็มแวร์ใช้แนวทางที่ต่างออกไปอย่างสิ้นเชิงสำหรับระบบไฟร์วอลล์ โดยโฟกัสไปที่ทรัพยากรที่องค์กรรู้จักเป็นอย่างดี เช่น แอปพลิเคชันที่องค์กรติดตั้ง แทนที่จะมุ่งตรวจสอบแอปพลิเคชันที่ไม่รู้จัก โซลูชันนี้ทำงานบนสภาพแวดล้อม Bare Metal, VM และแอปพลิเคชันที่ใช้คอนเทนเนอร์ และจะรองรับสภาพแวดล้อมไฮบริดคลาวด์ เช่น VMware Cloud on AWS และ AWS Outposts ในอนาคต องค์กรต่างๆ จะสามารถใช้โซลูชันนี้เป็นโซลูชันไฟร์วอลล์เพียงหนึ่งเดียวสำหรับรองรับความต้องการภายในองค์กร โซลูชัน Service-defined Firewall ของวีเอ็มแวร์มีความโดดเด่นในด้านต่างๆ ดังต่อไปนี้:

- Application Verification Cloud: ด้วยการใช้อุปกรณ์จาก VM หลายล้านเครื่องทั่วโลก Application Verification Cloud ในโซลูชันนี้จะสร้างแผนผังที่ถูกต้องแม่นยำเกี่ยวกับสถานะการทำงานที่ “เป็นปกติ” ของแอปพลิเคชัน และหลังจากที่เข้าใจลักษณะการทำงานที่เป็นปกติของแอปพลิเคชันที่รู้จักแล้ว โซลูชันดังกล่าวก็จะสร้างนโยบายการรักษาความปลอดภัยที่ปรับเปลี่ยนอย่างยืดหยุ่นสำหรับโซลูชัน Service-defined Firewall ซึ่งทำงานที่ระดับ Layer 7 และสามารถดำเนินการตรวจสอบแบบ Stateful ได้อย่างสมบูรณ์

- ปกป้องจาก Guest: โซลูชัน Service-defined Firewall ใช้ประโยชน์จากความสามารถภายในของวีเอ็มแวร์ในการตรวจสอบ OS และแอปพลิเคชันของ Guest โดยไม่จำเป็นต้องรวมอยู่ใน Guest นั้นหมายความว่าแม้กระทั่งในกรณีที่ผู้โจมตีสามารถเข้าถึงแบบ Root Access ได้ ก็ไม่สามารถเล็ดลอดผ่านโซลูชัน Service-defined Firewall ไปได้ นอกจากนี้ โซลูชันดังกล่าวยังสามารถตรวจจับและสกัดกั้นทราฟฟิกอันตรายบนเครือข่าย และยิ่งไปกว่านั้นยังสามารถสำรวจตรวจสอบ Guest โดยตรง ระบุและหยุดยั้งพฤติกรรมอันตรายภายใน OS หรือแอปพลิเคชันขณะทำงาน ความสามารถที่โดดเด่นนี้นับเป็นแนวทางใหม่สำหรับไฟร์วอลล์บนเครือข่ายและระบบป้องกันการบุกรุก (IPS) บนโฮสต์

- กระจายตัวอยู่ในซอฟต์แวร์: แนวทางแบบเดิมๆ ของระบบไฟร์วอลล์บนฮาร์ดแวร์ใช้วิธี “คัดแยก” ทราฟฟิกจากสภาพแวดล้อมแบบเวอร์ชวล และส่งไปยังอุปกรณ์ฮาร์ดแวร์เพื่อทำการสแกน ซึ่งนับเป็นวิธีที่ไร้ประสิทธิภาพและยากแก่การปรับเพิ่มขนาด โดยเฉพาะอย่างยิ่งสำหรับแอปพลิเคชันสมัยใหม่ที่ประกอบด้วยคอมโพเนนต์หรือเซอร์วิสมากมายที่รันบนเซิร์ฟเวอร์หลายเครื่อง และมักจะครอบคลุมระบบคลาวด์หลายระบบ โซลูชัน VMware Service-defined Firewall มาพร้อมความสามารถในการกระจายตัว อันหมายถึงระบบสามารถแทรกเข้าไปทำงานในทุกๆ ที่ที่แอปพลิเคชันที่มีการใช้งาน ไปจนถึงการทำงานข้ามระบบคลาวด์ได้ ดังนั้นจึงสามารถบังคับใช้นโยบายในลักษณะที่สอดคล้องกัน โดยไม่ต้องยุ่งยากกับการคัดแยกแพทไฟกบนสภาพแวดล้อมคลาวด์ที่ซับซ้อน

#### ข้อมูลเพิ่มเติม

- อ่านรายละเอียดเกี่ยวกับ VMware Service-defined Firewall ในบล็อกนี้
- อ่านข้อมูลโดยย่อเกี่ยวกับโซลูชัน VMware Service-defined Firewall
- อ่านข้อมูลเพิ่มเติมเกี่ยวกับกลยุทธ์และกลุ่มผลิตภัณฑ์ด้านการรักษาความปลอดภัยของวีเอ็มแวร์ที่นี่
- อ่านข้อมูลเพิ่มเติมเกี่ยวกับนวัตกรรมใหม่ Workspace ONE ของวีเอ็มแวร์ที่นี่

1-2018 Cost of Data Breach Study: Global Overview. กรกฎาคม 2561 การศึกษาวิจัยได้รับการสนับสนุนจาก IBM Security และดำเนินการศึกษาอย่างอิสระโดย Ponemon Institute LLC

2-Worldwide Semiannual Security Spending Guide จาก International Data Corporation (IDC), ตุลาคม 2561

#### เกี่ยวกับวีเอ็มแวร์

วีเอ็มแวร์เป็นผู้นำระดับโลกด้านการพัฒนาซอฟต์แวร์เพื่อช่วยเสริมสร้างประสิทธิภาพโครงสร้างพื้นฐานดิจิทัลที่มีความซับซ้อน ด้วยความร่วมมือกับพาร์ทเนอร์กว่า 75,000 ราย ผนวกกับผลิตภัณฑ์ต่าง ๆ ของวีเอ็มแวร์ อาทิ ระบบประมวลผล ระบบคลาวด์ โมบิลิตี้ เน็ตเวิร์คกิง และระบบรักษาความปลอดภัย วีเอ็มแวร์จึงเป็นผู้ให้บริการระบบดิจิทัลพื้นฐานที่ทำงานได้อย่างมีประสิทธิภาพและคล่องตัว โดยให้บริการแก่ลูกค้ากว่า 500,000 รายทั่วโลก สำนักงานใหญ่วีเอ็มแวร์ตั้งอยู่ที่เมืองพาโล อัลโต รัฐแคลิฟอร์เนีย ในปีนี้ วีเอ็มแวร์ฉลองครบรอบ 20 ปีแห่งความ

ก้าวหน้าในการพัฒนานวัตกรรมที่สร้างผลประโยชน์ต่อทั้งภาคธุรกิจและสังคม สำหรับข้อมูลเพิ่มเติม โปรดดูที่ <https://www.vmware.com/company.html>

VMware, VMware SD-WAN, VeloCloud, vCloud, vCloud NFV, VMware Cloud, VMware Smart Assurance, NSX-T, NSX-T Data Center, VMware Ready, Workspace ONE, Pulse, Pulse IoT Center, Photon, and Photon OS เป็นเครื่องหมายทางการค้าของวีเอ็มแวร์ อิงค์ หรือ บริษัทในเครือในประเทศสหรัฐอเมริกาและเขตอื่นๆ

# # #