ซิสโก้ส่งโซลูชั่นรักษาความปลอดภัยชุดใหญ่ เสริมแกร่งความปลอดภัย“ดาต้าเซ็นเตอร์”ที่มีวิวัฒนาการอย่างรวดเร็ว

ซิสโก้ส่งโซลูชั่นรักษาความปลอดภัยชุดใหญ่

เสริมแกร่งความปลอดภัย“ดาต้าเซ็นเตอร์”ที่มีวิวัฒนาการอย่างรวดเร็ว

ด้วยระบบอินทรูชั่น พรีเวนชั่นล่าสุด พร้อม ASA ไฟร์วอลล์ ประสิทธิภาพเยี่ยม

ช่วยปกป้องและจัดการดาต้าเซ็นเตอร์ในรูปแบบเวอช่วลไลซ์และคลาวด์

กรุงเทพ, ประเทศไทย – 18 กันยายน 2012 – ซิสโก้เปิดตัวชุดโซลูชั่นรักษาความปลอดภัยที่ออกแบบมาเพื่อเสริมแกร่งความปลอดภัยให้ดาต้าเซนเตอร์พร้อมต้านภัยคุกคามทุกรูปแบบในยุคสภาพแวดล้อมแบบรวมศูนย์ (Consolidated Environment) และแบบเสมือน (Virtualized Environment) ทั้งช่วยเอื้อให้ธุรกิจได้ประโยชน์จากคลาวด์รูปแบบใหม่อีกด้วย ชุดโซลูชั่นระบบรักษาความปลอดภัยนี้จะช่วยขยายขีดความสามารถระบบรักษาความปลอดภัยของดาต้าเซนเตอร์ที่เปี่ยมประสิทธิภาพอยู่แล้วให้ครอบคลุมไปถึงการปกป้องรักษาความปลอดภัยให้แก่ดาต้าเซ็นเตอร์ขนาดใหญ่และโมบายเวริค์ฟอร์ซแบบครบวงจร (End-to-End) โดยชุดโซลูชันนี้เป็นการผนึกรวมพลังกันของผลิตภัณฑ์ Cisco®Adaptive Security Appliance (ASA) ซึ่งเป็นเวอร์ชวลไลซ์ ASA สำหรับสภาพแวดล้อมที่หลากหลาย และเป็นซอฟต์แวร์ไฟร์วอลล์ที่มีการยอมรับและใช้งานมากที่สุดในโลก: Intrusion Preventive System -IPS ระบบป้องกันการบุกรุกโจมตีสำหรับดาต้าเซ็นเตอร์ และ Cisco AnyConnect®Security® Mobility Client ที่ได้เสริมประสิทธิภาพให้แข็งแกร่งมากขึ้นเพื่อสนองตอบต่อความต้องการทางธุรกิจปัจจุบันที่มุ่งเน้นเรื่องประสิทธิผลและการทำงานที่เน้นแบบโมบายเวริค์ฟอร์ซ ทำงานได้ทุกสถานที่ทุกเวลามากขึ้น

เทรนด์ของเวอร์ชวลไลซ์เซชั่นและคลาวด์ส่งผลให้มีการปรับเปลี่ยนอย่างมากในส่วนของดาต้าเซ็นเตอร์ และยังส่งผลถึงทุก ๆ เรื่อง ตั้งแต่งานบริการด้านไอที โมเดลทางธุรกิจ ตลอดจนสถาปัตยกรรม ซึ่งหากมีการจัดการอย่าง

เหมาะสมจะก่อให้เกิดประโยชน์ในทางธุรกิจอย่างมากมาย เช่น ช่วยลดต้นทุน สร้างรายได้ใหม่ให้แก่องค์กร เพิ่มประสิทธิภาพได้มากขึ้น เพิ่มความคล่องตัวและความยืดหยุ่นซึ่งเป็นเรื่องที่จำเป็นอย่างมากสำหรับยุคโลกาภิวัตน์ การประกาศเปิดตัวโซลูชั่นรักษาความปลอดภัยสำหรับดาต้าเซนเตอร์ของซิสโก้ในครั้งนี้ ถือเป็นการทำให้ระบบรักษาความปลอดภัยหรือระบบซีเคียวริตี้ก้าวไปอีกขั้นและสอดรับความต้องการในสภาพแวดล้อมแบบคลาวด์และเวอร์ช่วลที่เน้นการทำงานด้วยประสิทธิภาพสูงและมีการปลี่ยนแปลงอยู่ตลอดเวลา รวมถึงความต้องการด้านการจัดการกับความซับซ้อนที่มีมากขึ้นที่ต้องเป็นไปตามข้อกำหนดบังคับมาตรฐานสากล (Compliance) และตอบสนองความต้องการของพนักงานที่นิยมนำอุปกรณ์ของตัวเองเข้ามาใช้ในการทำงานมากขึ้น ซึ่งเป็นแนวความนิยมเรื่องหนึ่งในอีกหลายๆเรื่องในปัจจุบัน

ด้วยการบริหารและดำเนินการภายใต้หลักการที่ว่า ระบบการรักษาความปลอดภัยต้องผสานเป็นหนึ่งเดียวทั่วทั้งเน็ตเวิร์คเพื่อให้สามารถปกป้องดาต้าเซ็นเตอร์ที่รวมศูนย์เป็นหนึ่งเดียวได้อย่างมั่นใจ ซิสโก้เชื่อมั่นว่านโยบายด้านเน็ตเวิร์คจะต้องเป็นหนึ่งเดียวทั้งโลกแห่งความจริงและโลกเสมือนจริง การสื่อสารภายในแบบเสมือนจริงนั้นควรต้องมีการปกป้องให้ปลอดภัย และการเข้าถึงการใช้งานแอพพลิเคชั่นทั้งแบบผ่านสาย (wired) และ การใช้งานแอพพลิเคชั่นแบบเคลื่อนที่หรือผ่านโทรศัพท์มือถือก็ต้องได้รับการปกป้องให้ปลอดภัยเช่นกัน การนำเสนอแนวทางการรักษาความปลอดภัยถือเป็นเรื่องสำคัญและจำเป็นอย่างยิ่งด้วยในปัจจุบันลูกค้ากำลังมองหาวิธีที่จะย้ายฐานไปสู่คลาวด์รวมถึงวัฒนธรรมองค์กรที่ยืดหยุ่นมากขึ้นในเรื่องการนำอุปกรณ์มาใช้งานในองค์กร ซึ่งผลิตภัณฑ์ล่าสุดของซิสโก้ก็ได้พัฒนาเพื่อช่วยสนับสนุนแนวทางดังกล่าว

คำกล่าวสนับสนุน:

• มร. คริสโตเฟอร์ ยัง รองประธานอาวุโสและผู้จัดการทั่วไปของกลุ่มรักษาความปลอดภัยและงานภาครัฐของซิสโก้

“เพื่อให้องค์กรมั่นใจว่าจะได้ประโยชน์ทางธุรกิจจากดาต้าเซ็นเตอร์เวอร์ช่วลไลเซชั่นและคลาวด์ ‘การรักษาความปลอดภัย’ จะต้องเป็นศิลปะที่เป็นไปได้ไม่ใช่เป็นอุปสรรค เช่นเดียวกับเน็ตเวิร์คที่ซิสโก้ช่วยให้องค์กรตัดสินใจในการนำระบบรักษาความปลอดภัยไปใช้กับทั้งสภาพแวดล้อมแบบผสม (Hybrid) แบบเสมือนจริง หรือแบบคลาวด์ และช่วยทำให้ดาต้าเซ็นเตอร์สามารถทำ IT as a Service ด้วยความปลอดภัยระดับสูงโดยไม่ก่อกวนประสิทธิภาพของเน็ตเวิร์ค”

• มร. เคน โอเวน ประธานเจ้าหน้าที่ระดับสูงฝ่ายเทคโนโลยี ของ Savvis บริษัทในเครือของ CenturyLink

“ในฐานะที่เป็นผู้ให้บริการระดับโลกด้านคลาวด์ที่เน้นภาคองค์กร Savvisได้ตรวจสอบเทคโนโลยีด้านความปลอดภัยล่าสุดอยู่เสมอ เราประเมินได้ว่า Cisco ASA 1000V Cloud Firewall ไม่เพียงแต่ตอบสนองความต้องการขององค์กรด้านความปลอดภัยของคลาวด์เท่านั้น แต่ยังตอบสนองข้อกำหนดที่เข้มงวดในการใช้งานในองค์กรอีกด้วย”

• มร. นิค ชมิดท์ ผู้จัดการอาวุโสด้านเทคโนโลยีสารสนเทศ ของ CDW

“ความปลอดภัยวัดได้จากระดับของความไว้วางใจ มันเป็นเรื่องของสิทธิในการใช้งานและการเข้าถึงได้ทั่วโลก ในขณะที่มีการเปลี่ยนแปลงอย่างมากที่ส่งผลกระทบในเรื่องของการรักษาความปลอดภัย โซลูชั่นรักษาความปลอดภัยของซิสโก้มีบทบาทสำคัญในการปกป้องบริษัทของเราและช่วยให้เราสามารถใช้วิธีการผสมผสานระหว่างพับบลิคคลาวด์กับไพรเวทคลาวด์ ให้เป็นไปตามที่เราต้องการได้”

• มร. ไมค์ โซซาย่า ผู้จัดการฝ่ายปฏิบัติการ ด้านการรักษาความปลอดภัย/ โมบิลิตี้ /โครงสร้างพื้นฐานของ Nexus IS

“การถือกำเนิดของดาต้าเซ็นเตอร์แบบเวอร์ช่วลไลเซชั่นและโครงสร้างพื้นฐานแบบคลาวด์ได้ยกระดับความปลอดภัยสำหรับลูกค้าของเรา โซลูชั่นรักษาความปลอดภัยแบบบูรณาการที่ซิสโก้ได้นำเสนอล่าสุดนั้นได้ขจัดปัญหาด้านความปลอดภัยของลูกค้าดาต้าเซ็นเตอร์ของเราและช่วยให้ Nexus IS ได้รับนวัตกรรมด้านเทคโนโลยีแบบหนึ่งเดียว (Innovative and Integrated Technology) ช่วยให้ลูกค้าของเราสร้างโซลูชั่นรักษาความปลอดภัยแบบครบวงจร (End-To-End) สำหรับโครงสร้างพื้นฐานเวอร์ช่วลและแบบคลาวด์ที่มีผู้ใช้หลากหลาย (Multitenant Cloud Infrastructure)”

จุดเด่นของผลิตภัณฑ์

- **<u>แพลตฟอร์ม Cisco ASA 9.0</u>:** เป็นการปรับปรุงที่สำคัญให้กับระบบปฏิบัติการ

    - ทำให้สมรรถนะในระดับของดาต้าเซ็นเตอร์รองรับปริมาณงานของไฟร์วอลล์ขนาด 320 Gbps และ IPS ขนาด 60 Gbps ได้ ด้วยการเชื่อมต่อที่ระดับ 1 ล้านหน่วยต่อวินาทีและ การเชื่อมต่อพร้อมกันจำนวน 50 ล้านหน่วย โดยสามารถให้ประสิทธิภาพได้ดีกว่าโซลูชั่นของคู่แข่งถึงแปดเท่า

    - สามารถขยายการเติบโตให้สอดคล้องกับความต้องการของธุรกิจเมื่อปริมาณงานของแอพพลิเคชั่นและ VM มีการขยายตัว ทำให้หมดความจำเป็นกับค่าใช้จ่ายที่ต้องสูญไปกับการลงทุนทางโครงสร้าง สามารถปรับขนาดด้วยการใช้เทคโนโลยีแบบคลัสเตอร์ ซึ่งจะช่วยฝ่ายไอทีในการจัดการกับ ASA จำนวนมากด้วยการแปลงให้เป็นยูนิตเดียวได้

- ใช้ content-awareness เพื่อช่วยสร้างวิสัยทัศน์และการควบคุมสำหรับรุ่นต่อๆไป สร้างสมรรถภาพด้วย TrustSec security group tags และไฟร์วอลล์แบบ Identity-based เพื่อให้มีการแสดงผลที่ชัดเจนขึ้นอันจะทำให้การบังคับใช้นโยบายนั้นสามารถทำได้อย่างถี่ถ้วนยิ่งขึ้น ช่วยรักษาความปลอดภัยในสภาพแวดล้อมที่มีผู้ใช้หลากหลายซึ่งเป็นสภาพการใช้งานคอมพิวเตอร์ในแบบคลาวด์

- ผสมผสานเข้ากับ Cisco Cloud Web security (ซึ่งเดิมเรียกว่า ScanSafe) ช่วยให้สามารถสแกนเนื้อหาได้อย่างละเอียด โดยไม่มีผลกระทบหรือมีผลกระทบเพียงเล็กน้อยกับประสิทธิภาพการทำงานของ ASA

- ช่วยปรับปรุงสมรรถภาพความปลอดภัยในการเข้าถึงจากระยะไกล (remote access) โดยสนับสนุนการเชื่อมต่อแบบ IPv6 โดยที่มีผลกระทบน้อยที่สุดต่อประสิทธิภาพ รวมทั้งขีดความสามารถของ Next Generation Encryption และขั้นตอนวิธีการเข้ารหัสแบบ NSA “Suite B”

- **Cisco ASA 1000V:** เทคโนโลยีของ ASA ที่ได้รับการสร้างให้เหมาะสมกับสภาพแวดล้อมแบบเสมือนจริงและแบบคลาวด์

  - ไฟร์วอลล์ของ ASA ถูกสร้างขึ้นมาโดยเฉพาะสำหรับสภาพแวดล้อมเสมือนจริงและแบบคลาวด์ที่มีผู้ใช้หลากหลาย ซึ่งแตกต่างไปจากผลิตภัณฑ์ของคู่แข่ง เพราะไม่เพียงแต่ให้โครงสร้างทางกายภาพ ที่เป็นแบบ ASA ใน VM เท่านั้น แต่ยังให้ความยืดหยุ่นที่เหนือกว่าและใช้ทรัพยากรอย่างมีประสิทธิภาพมากกว่าอีกด้วย

  - การใช้ ASA 1000V เพียงอินสแตนท์เดียวก็สามารถช่วยป้องกันปริมาณงานได้เป็นอันมากด้วยการใช้นโยบายรักษาความปลอดภัยที่แตกต่างกันไปกับ ESX host หลายๆตัว ซึ่งช่วยลดความซับซ้อนในการใช้งานและสามารถปรับเพิ่มลดขนาดในสภาพแวดล้อมที่ต่างกัน

  - ช่วยปกป้องขอบข่ายของผู้ใช้ระบบคลาวด์และสร้างเซ็กเมนท์ที่มีความปลอดภัยสูงเพื่อให้การรักษาความปลอดภัยเป็นแบบเบ็ดเสร็จและสอดคล้องกันกับสภาพแวดล้อมทั้งที่เป็นแบบกายภาพ แบบเสมือนจริง รวม

ทั้งที่เป็นพับบลิคและไพรเวทคลาวด์ โดยใช้ไฟร์วอลล์ที่เชื่อถือได้

- สืบทอดมาจากสวิตช์รุ่น Nexus ® 1000V ที่สร้างโดยซิสโก้ซึ่งเป็นผู้นำของอุตสาหกรรม Cisco Nexus ® 1000V และเป็นตัวเสริมให้กับ Cisco Virtual Security Gateway (VSG) เพื่อสร้างความปลอดภัยแบบเบ็ดเสร็จให้กับโครงสร้างพื้นฐานเสมือนจริงและของคลาวด์

Cisco IPS 4500 Series: ระบบป้องกันการบุกรุก (Intrusion Prevention System – IPS) ที่สร้างขึ้นใหม่สำหรับดาต้าเซ็นเตอร์:

- มอบประสิทธิภาพที่สูงสุดในอุตสาหกรรม: ที่ 10 กิกะบิตต่อวินาที (Gbps) สำหรับแร็ค แต่ละตัว เพื่อการป้องกันแอพพลิเคชั่นอย่างมีสมรรถภาพสูงสุดให้กับดาต้าเซ็นเตอร์

- สร้างขึ้นมาเป็นการเฉพาะสำหรับดาต้าเซ็นเตอร์ ช่วยปกป้องข้อมูลทรัพยากรที่สำคัญในศูนย์ด้วยรูปแบบ 2RU ที่กะทัดรัด อัดแน่นไปด้วยประสิทธิภาพ IPS ที่เหนือกว่า

- ช่วยให้ง่ายต่อการแทรก IPS เข้าไปในเน็ตเวิร์ครูปแบบต่างๆและสร้างความมั่นใจในการทำงานร่วมกับองค์ประกอบเดิมของเน็ตเวิร์คที่มีอยู่แล้ว

- ช่วยลดการตัดสินใจให้มีประสิทธิภาพด้วยการใช้ context-aware IPS ที่ได้รวมเอาการใช้ network reputation เข้าไว้ด้วย

- สร้างขึ้นจากเทคโนโลยี IPS ที่มีการใช้งานมากที่สุดในธุรกิจ สามารถครอบคลุมการป้องกันการโจมตีทุกรูปแบบ โดยได้รับการพิสูจน์แล้ว (Infonetics[1], Gartner[2])

- **<u>Cisco Security Manager 4.3:</u>** Cisco Security Manager (CSM) มีความสามารถในการปรับขนาดให้เหมาะสม และสามารถจัดการได้จากส่วนกลางโดยที่ผู้บริหารสามารถบริหารจัดการอุปกรณ์รักษาความปลอดภัยที่หลากหลายของซิสโก้ได้อย่างมีประสิทธิภาพ สามารถเห็นการติดตั้งและใช้งานได้ทั่วทั้งเน็ตเวิร์ค และสามารถแบ่งปันข้อมูลกับบริการทางเน็ตเวิร์คที่สำคัญอื่น ๆ เช่นระบบตรวจสอบการปฏิบัติตาม หรือ ระบบการวิเคราะห์การรักษาความปลอดภัยขั้นสูง

  - สามารถบริหารจัดการกับสภาพแวดล้อมการรักษาความปลอดภัยที่มีความหลากหลายของซิสโก้ รวมทั้ง Cisco ASA 5500 และ 5500-X Series Adaptive Security Appliances รวมทั้ง Cisco IPS 4200, 4300 และ 4500 Series Sensor Appliances Cisco AnyConnect Secure Mobility Client และ Cisco Secure Routers

  - แตกต่างจากผลิตภัณฑ์เพื่อการจัดการอื่น ๆ ซึ่งต้องมีการติดตั้งใช้งานหลายครั้งกว่าจะได้ขนาดที่เหมาะสม ระบบนี้ใช้การติดตั้ง CSM อย่างเดียวก็สามารถจัดการกับอุปกรณ์จำนวนมาก และทำให้เกิดการปรับขนาดให้เหมาะสมได้อย่างรวดเร็ว

  - ช่วยให้สภาพและประสิทธิภาพการทำงานของ Cisco ASA และอุปกรณ์ IPS ได้รับการตรวจสอบอย่างต่อเนื่องและส่งการแจ้งเตือนเมื่อถึงเกณฑ์ที่ตั้งไว้

  - ใช้ตัวช่วยเพื่อทำให้ง่ายขึ้นและ ปรับปรุงการอัพเกรดสำหรับ ASA firewall แต่ละตัวหรือกลุ่มของ ASA firewall ให้มีประสิทธิภาพขึ้น

  - ช่วยให้การเข้าถึง API-based สำหรับCisco Security Manager เพื่อช่วยให้องค์กรสามารถแบ่งปันข้อมูลกับเน็ตเวิร์คการให้บริการสำคัญอื่น ๆ เช่นระบบการปฏิบัติตามและระบบการวิเคราะห์การรักษาความปลอดภัยขั้นสูง

- **Cisco AnyConnect 3.1:** ช่วยให้การเข้าถึงระยะไกลไปยังแหล่งอุปกรณ์เน็ตเวิร์คมีความปลอดภัยสูง:

- ช่วยในการเข้าถึงอุปกรณ์ที่แตกต่างกัน เพื่อช่วยเรื่องการติดตั้งใช้งาน BYOD ความสามารถของ IPv6 Capability และ Next Generation Encryption รุ่นล่าสุด และขั้นตอนวิธีการเข้ารหัสแบบ NSA Suite B

• **การบริการด้านความปลอดภัย** บริการและการสนับสนุนแบบมืออาชีพจากซิสโก้และคู่ค้า ช่วยให้ลูกค้าสามารถวางแผนสร้างและจัดการกับดาต้าเซ็นเตอร์และโครงสร้างพื้นฐานคลาวด์ที่มีความซับซ้อนให้มีความปลอดภัยในระดับสูง Cisco Data Center Security Services สามารถช่วยจัดการทั้งเรื่องการป้องกันและการเปิดช่องทางให้ เช่น การปกป้องข้อมูล การอนุญาตให้เข้าถึงข้อมูลที่มีความปลอดภัยสูง ให้เป็นไปตามกฎระเบียบที่ตั้งไว้และสกัดกั้นการบุกรุกไม่ให้เกิดขึ้น

เกี่ยวกับซิสโก้ ซิสเต็มส์

ซิสโก้ (NASDAQ: CSCO) เป็นผู้นำระดับโลกทางด้านเครือข่ายที่เปลี่ยนรูปวิธีการเชื่อมต่อ สื่อสาร และการทำงานร่วมกัน ดูข้อมูลเพิ่มเติมเกี่ยวกับซิสโก้ได้ที่ http://www.cisco.com และข่าวสารเพิ่มเติมที่ http://newsroom.cisco.com