

MATICHON INFORMATION CENTER		Subject Heading :	
Source :	สยามธุรกิจ	54172125	
Date :	31 ส.ค. 2554	Page :	๑๔
		No :	

ชีวิตยุค 3G

ระบบป้องกันข้อมูล รั่วไหล (ตอนที่ 1)

ไซแมนเทค คอร์ป ประกาศเปิดตัว ระบบป้องกันข้อมูลรั่วไหล เวอร์ชัน 11 (Symantec Data Loss Prevention 11) มุ่งเน้นในการตรวจจับความผิดปกติพร้อมทั้งปกป้องข้อมูลมีค่า อันเป็นทรัพย์สินทางปัญญาขององค์กรธุรกิจได้ง่ายขึ้น ทั้งนี้ชุดโซลูชันชั้นนำในตลาดเพื่อการรักษาความปลอดภัยของข้อมูล เวอร์ชันใหม่จากไซแมนเทค พร้อมนำเสนอคุณสมบัติของเทคโนโลยี เวกเตอร์ แมชชีน เลิร์นนิง (Vector Machine Learning) ซึ่งเป็นเทคโนโลยีแรกและเทคโนโลยีเดียวที่เรียนรู้ข้อมูลสำคัญด้วยตัวเอง ออกแบบมาเพื่อช่วยให้การตรวจจับสินทรัพย์ทางปัญญาซึ่งเป็นสิ่งที่ทำได้ยาก กลายเป็นเรื่องง่ายขึ้น นอกจากนี้ Symantec Data Loss Prevention 11 ยังช่วยให้กระบวนการแก้ไขความผิดปกติ มีประสิทธิภาพมากยิ่งขึ้น และยังเพิ่มศักยภาพในเรื่องของการนำเสนอข้อมูลเชิงลึกพร้อมการตรวจวัดความปลอดภัยเพิ่มขึ้นส่วนอื่นด้วย

ข้อมูลมากขึ้น ความเสี่ยงเพิ่มขึ้น

ในแต่ละปีข้อมูลที่ถูกรวบรวมไม่เพียงแต่มีอัตราเติบโตมากขึ้นถึงกว่า 60 เปอร์เซ็นต์ และกำลังกลายเป็นปัญหายุ่งยากในการบริหารจัดการและดูแลป้องกันไม่ให้สูญหาย ข้อมูลที่มีค่าที่สุดสำหรับองค์กรธุรกิจ ก็คือ ทรัพย์สินทางปัญญา ที่มีค่าจะถูกฝังรวมอยู่ในเอกสารที่จัดเก็บไม่เป็นระบบซึ่งมีจำนวนเพิ่มมากขึ้นทุกที และเอกสารบางอย่างก็ไม่ค่อยสำคัญเท่าไรนัก ซึ่งข้อมูลที่จัดเก็บไม่เป็นระบบเหล่านี้ มักไม่ค่อยปลอดภัยเท่ากับข้อมูลอื่นๆ ที่อยู่ในคลังข้อมูล ทำให้เกิดความเสียหายที่ข้อมูลอาจสูญหายได้มาจากภัยคุกคามทั้งภายในและนอกองค์กร และจากการที่เราได้เห็นการโจมตีแบบมีเป้าหมาย เช่น Hydraq รวมถึงการรั่วไหลของเอกสารสำคัญอื่นๆ จึงยิ่งทำให้ทรัพย์สินทางปัญญาตกอยู่ในความเสี่ยงมากกว่าที่เคยเป็นมา

เทคโนโลยี Vector Machine Learning ช่วยระบุถึงความปลอดภัยได้ง่ายขึ้น

องค์กรธุรกิจจำเป็นต้องระบุว่าเอกสารใดมีความสำคัญ และต้องดำเนินการเพื่อปกป้องเอกสารเหล่านั้น การป้องกันข้อมูลสูญหายที่ผ่านมามักจะใช้เทคโนโลยีการตรวจจับความผิดปกติ 2 ประเภทด้วยกัน ได้แก่ เทคโนโลยีตรวจสอบรูปแบบข้อมูลแบบ Fingerprint และการระบุลักษณะเนื้อหาของข้อมูล ทั้งนี้เทคโนโลยีตรวจสอบรูปแบบข้อมูลแบบ Fingerprint จะต้องทำการเก็บรวบรวมเอกสารทั้งหมดเพื่อกำหนด Fingerprint เฉพาะของแต่ละไฟล์ อีกทางเลือกหนึ่งคือ การระบุลักษณะเฉพาะเนื้อหาของข้อมูล ซึ่งจะเกี่ยวเนื่องกับการสร้างลิสต์คีย์เวิร์ด และสัญลักษณ์เครื่องหมายต่างๆ เพื่อระบุว่าเอกสารนั้นเป็นเอกสารสำคัญ การจัดทำเรื่องของรูปแบบของข้อมูลแบบ Fingerprint อาจเป็นเรื่องท้าทายสำหรับองค์กรที่มีข้อมูลอยู่กระจัดกระจาย และการกำหนดนโยบายต่างๆ ในการอธิบายรายละเอียดของข้อมูล อาจทำให้เสียเวลาในการดำเนินการขณะที่การระบุลักษณะเนื้อหาที่มีความแม่นยำน้อยกว่าการตรวจสอบจากรูปแบบข้อมูลแบบ Fingerprint

เทคโนโลยี Vector Machine Learning คือนวัตกรรมใหม่ที่ไซแมนเทค ออกแบบมาเพื่อก้าวข้ามข้อจำกัดของเทคโนโลยีการตรวจจับที่มีอยู่ในปัจจุบัน การทำงานของ Vector Machine Learning สามารถเรียนรู้ด้วยตัวเองจากเอกสารตัวอย่างที่มีอยู่เพื่อเรียนรู้คุณลักษณะของข้อมูล พร้อมทั้งความแตกต่างระหว่างข้อมูลที่สำคัญและไม่สำคัญ เทคนิคนี้ช่วยลดความจำเป็นในการกำหนดนโยบายในการสร้างคีย์เวิร์ดหรือพยายามใช้วิธีการจดจำข้อมูลแบบ Fingerprint สำหรับทุกเอกสารที่มีการสร้างขึ้นใหม่ ด้วยเทคโนโลยี Vector Machine Learning แคตัวอย่างของเอกสารแบบก็เพียงพอสำหรับการสร้างนโยบายที่ให้ความถูกต้องแม่นยำที่จะเพิ่มมากขึ้นเรื่อยๆ เมื่อมีเอกสารอ้างอิงเพิ่มเข้ามาในระบบ (อ่านต่อฉบับหน้า)

ข้อมูลจาก ไซแมนเทค คอร์ป