IBM Tivoli Endpoint Manager for Security and Compliance

โซลูชันเดียวสำหรับการบริหารจัดการกับความปลอดภัยของ endpoint ทั่วทั้งองค์กร

จุดเด่นของผลิตภัณฑ์

- นำเสนอทัศนวิสัยที่ทันสมัยและการควบคุมจากคอนโซลการจัดการเครื่องเดียว
- ใช้เอเจนต์อัจฉริยะ อเนกประสงค์ “เอเจนต์เดียว” ที่สามารถประเมินและแก้ไขปัญหาเพื่อช่วยให้มั่นใจถึงความปลอดภัยและการปฏิบัติตามข้อบังคับอย่างต่อเนื่อง
- จัดการกับ endpoints จำนวนนับแสนในแบบจริง (Physical) และเสมือน (Virtual) ได้โดยไม่คำนึงถึงที่ตั้ง ชนิดหรือสถานะของการเชื่อมต่อ
- จัดการกับแพตช์โดยอัตโนมัติสำหรับระบบปฏิบัติการและแอพพลิเคชันจำนวนมาก

ในโลกปัจจุบันซึ่งจำนวน endpoints และ threats ได้เพิ่มขึ้นอย่างรวดเร็วและมากขึ้นในอัตราที่ควบคุมได้ยาก IBM Tivoli® Endpoint Manager for Security and Compliance นำเสนอมุมมองในแบบ เรียลไทม์ (Real-Time) และกำหนดเป็นข้อบังคับ (Policy Enforcement) เพื่อป้องกัน ระบบที่ซับซ้อนและมีขนาดใหญ่ของคุณได้อย่างมีประสิทธิภาพ

ออกแบบมาเพื่อให้มั่นใจถึงความปลอดภัยของ endpoint ทั่วทั้งองค์กร Tivoli Endpoint Manager for Security and Compliance สามารถช่วยองค์กรของคุณทั้งในการป้องกัน endpoints และทำให้มั่นใจว่าตัวควบคุมที่คุณมีอยู่ตรงตามมาตรฐานการปฏิบัติตามด้านความปลอดภัย ระบบนี้นับเป็นโซลูชันที่สามารถจัดการได้ง่าย นำไปใช้ได้เร็วและสนับสนุนความปลอดภัยในสภาวะแวดล้อมที่ประกอบด้วย endpoints หลากหลายชนิดและมีจำนวนมาก—จากเซิร์ฟเวอร์ไปยังเดสก์ท็อปพีซี, แล็ปท็อปที่เชื่อมต่ออินเทอร์เน็ตแบบ “roaming” และเครื่องมือพิเศษ เช่น อุปกรณ์ point-of-sale (พีโอเอส), เอทีเอ็มและเครื่องขายสินค้าแบบบริการตนเอง (self service kiosks)

Tivoli Endpoint Manager for Security and Compliance สามารถลดต้นทุนและความซับซ้อนของการจัดการด้านไอที เนื่องจากสามารถเพิ่มความคล่องตัวทางธุรกิจช่วยให้แก้ไขปัญหาได้เร็วขึ้นด้วยความถูกต้อง เนื่องจากระบบนี้ส่งผลกระทบต่อการดำเนินงานของ endpoint น้อยจึงสามารถเพิ่มผลผลิตและทำให้ผู้ใช้ได้รับประสบการณ์ใช้งานที่ดีขึ้น โดยการบังคับการปฏิบัติตามนโยบายอย่างสม่ำเสมอในทุกที่ที่ endpoints roam Tivoli Endpoint Manager for Security and Compliance ช่วยลดความเสี่ยงและเพิ่มทัศนวิสัยการตรวจสอบการปฏิบัติตามข้อบังคับอย่างต่อเนื่อง

การให้ความสำคัญกับความต้องการความปลอดภัยทั่วทั้งองค์กร

Tivoli Endpoint Manager for Security and Compliance ให้ความสำคัญกับปัญหาด้านความปลอดภัยที่เชื่อมโยงกับเดสก์ท็อปและสภาวะแวดล้อมที่แจกจ่าย โดยการนำเสนอการจัดการ endpoint และการรักษาความปลอดภัยในโซลูชันเดียวกัน ช่วยให้มั่นใจได้ถึง การป้องกันและการปฏิบัติตามข้อบังคับอย่างต่อเนื่อง ตัวอย่างเช่น ระบบสามารถลดความเสี่ยงด้านความปลอดภัยลงได้อย่างมากโดยการประยุกต์ใช้ซอฟต์แวร์แพตช์ในเวลาเพียงไม่กี่นาที และยังสามารถช่วยบริดจ์ช่องว่างระหว่างฟังก์ชันต่างๆ เช่น ฟังก์ชันการสร้างและการดำเนินกลยุทธ์และนโยบาย ฟังก์ชันการจัดการอุปกรณ์ในแบบเรียลไทม์ และฟังก์ชันการสร้างรายงานเกี่ยวกับปัญหาด้านความปลอดภัยและการปฏิบัติตามข้อบังคับ

Tivoli Endpoint Manager for Security and Compliance มีความสามารถดังนี้:

- นำเสนอทัศนวิสัยที่ถูกต้อง แม่นยำ ในเวลาที่รวดเร็วและการบังคับใช้คอนฟิกูเรชันด้านความปลอดภัยและแพตช์อย่างต่อเนื่อง
- การจัดการต่อต้านมัลแวร์จากบุคคลที่สามและการป้องกันไฟร์วอลล์จากส่วนกลาง
- นำเสนอวิธีปฏิบัติที่ดีที่สุดแบบไร้ขอบเขตจำกัดที่ตรงกับข้อบังคับ U.S. Federal Desktop Configuration Control (FDCC) และ Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs)
- สนับสนุน Security Content Automation Protocol (SCAP) Tivoli Endpoint Manager ซึ่งนับเป็นผลิตภัณฑ์แรกที่ได้รับการรับรองจาก National Institute of Standards and Technology (NIST) ทั้งในด้านการประเมินและการแก้ไขปัญหา
- ส่งผ่านคำสั่ง endpoint อย่างปลอดภัยดังที่สาธิตผ่านทาง NIAP CCEVS EAL3 และ FIPS 104-2, ใบรับรองระดับ 2
- สนับสนุนมาตรฐาน Open Vulnerability and Assessment Language (OVAL) เพื่อรองรับข้อมูลเนื้อหาเปิดที่มีการรักษาความปลอดภัยแบบพับลิก (public)
- รับและตอบสนองต่อการแจ้งเตือนความเสี่ยงด้านความปลอดภัยตามที่เผยแพร่โดยสถาบัน SANS
- แสดงแนวโน้มและการวิเคราะห์การเปลี่ยนแปลงคอนฟิกูเรชันความปลอดภัยโดยใช้การรายงานขั้นสูง

ความสามารถเพิ่มเติมที่มีอยู่ในผลิตภัณฑ์ทุกรายการในตระกูล Tivoli Endpoint Manager ที่สร้างขึ้นโดยใช้เทคโนโลยี BigFix® มีดังนี้:

- ค้นหา endpoints ที่องค์กรอาจยังไม่ทราบว่ามีอยู่ในสภาวะแวดล้อม—ได้มากกว่า 30 เปอร์เซ็นต์ในบางกรณี
- นำเสนอคอนโซลเดียวสำหรับฟังก์ชันการจัดการ คอนฟิกูเรชันการค้นหาและความปลอดภัย เพื่อให้การดำเนินงานง่ายขึ้น
- การดำเนินการเฉพาะเป้าหมายตามชนิดของคอนฟิกูเรชัน endpoint หรือชนิดผู้ใช้ที่ต้องการ และการใช้คุณสมบัติฮาร์ดแวร์หรือซอฟต์แวร์ในแบบเสมือนเพื่อทำเช่นนั้น
- ใช้โครงสร้างพื้นฐานการจัดการแบบรวมเพื่อประสานงานระหว่างการดำเนินงานด้านไอที ความปลอดภัย เดสก์ท็อป และเซิร์ฟเวอร์
- เข้าถึง endpoints โดยไม่คำนึงถึงที่ตั้ง ชนิดหรือสถานะการเชื่อมต่อด้วยการจัดการแบบครอบคลุมสำหรับระบบปฏิบัติการที่สำคัญทั้งหมดของบุคคลที่สาม และแพตช์ตามนโยบาย Tivoli Endpoint Manager for Security and Compliance

สนับสนุนกระบวนการอัตโนมัติที่มีเป้าหมายจำนวนมากซึ่งนำเสนอตัวควบคุม ทัศนวิสัย และความเร็วซึ่งมีผลต่อการเปลี่ยนแปลงและการรายงานเกี่ยวกับการปฏิบัติตามข้อบังคับ การแก้ไขปัญหา—เกี่ยวกับมัลแวร์และไวรัสใช้เวลาน้อยและรวดเร็วโดยใช้ความสามารถในการจัดการแพตช์ที่รวดเร็ว การนำเสนอฟังก์ชันด้านความปลอดภัยที่มีประสิทธิภาพจำนวนมาก

Tivoli Endpoint Manager for Security and Compliance

มีฟังก์ชันที่สำคัญดังต่อไปนี้และทำให้คุณสามารถเพิ่มฟังก์ชันเป้าหมายอื่นตามต้องการได้ง่าย โดยไม่ต้องเพิ่มโครงสร้างพื้นฐานหรือต้นทุนในการนำไปใช้งาน

การจัดการแพตช์

การจัดการแพตช์รวมถึงความสามารถแบบครอบคลุมสำหรับการจัดส่งแพตช์สำหรับ Microsoft® Windows®, UNIX®, Linux® และ Mac OS และสำหรับผู้จำหน่าย เช่น Adobe®, Mozilla, Apple และ Java™ ที่แจกจ่าย endpoints—โดยไม่คำนึงถึงที่ตั้ง ชนิดหรือสถานะการเชื่อมต่อ เซิร์ฟเวอร์การจัดการเพียงเครื่องเดียวสามารถสนับสนุน endpoints ได้มากถึง 250,000 จุด ส่งผลให้เวลาแพตช์สั้นลงโดยไม่สูญเสียฟังก์ชัน endpoint แม้แต่บนเครือข่ายแบนด์วิธต่ำหรือ

ที่แจกจ่ายไปทั่วโลก การรายงานแบบเรียลไทม์แสดงข้อมูลเกี่ยวกับแพตช์ที่นำไปใช้แล้ว เวลาที่นำไปใช้และบุคคลที่นำไปใช้ ตลอดจนการยืนยันอัตโนมัติว่ามีการประยุกต์ใช้แพตช์สำหรับโซลูชัน closedloop ที่สมบูรณ์ในกระบวนการแพตช์แล้ว

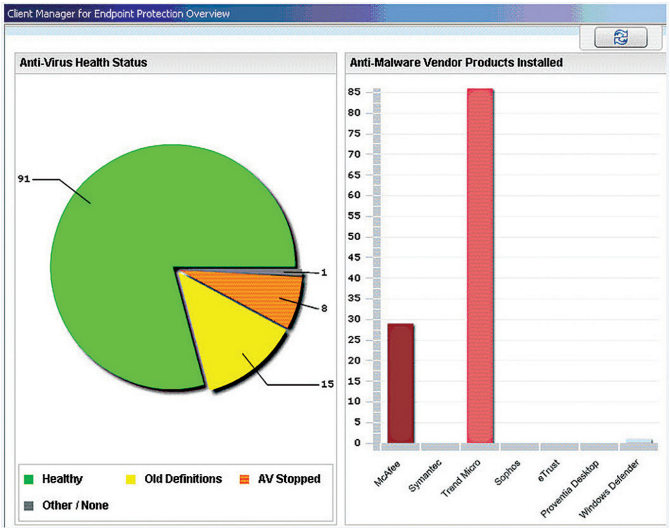
การจัดการคอนฟิกูเรชันด้านความปลอดภัย

ผ่านการตรวจสอบความถูกต้องโดย National Institute of Standards and Technology คุณลักษณะคอนฟิกูเรชันด้านความปลอดภัยของโซลูชันนำเสนอไลบรารีตัวควบคุมด้านเทคนิคแบบครอบคลุมที่สามารถช่วยให้คุณปฏิบัติตามข้อบังคับด้านความปลอดภัยได้สำเร็จโดยการตรวจสอบและบังคับใช้คอนฟิกูเรชันด้านความปลอดภัย ไลบรารีนโยบายสนับสนุนการบังคับใช้พื้นฐานคอนฟิกูเรชันอย่างต่อเนื่อง โดยจะรายงานแก้ไข และยืนยันการแก้ไข endpoints ที่ไม่เป็นไปตามข้อบังคับในแบบเรียลไทม์ และมั่นใจได้กับมุมมองแบบเรียลไทม์ที่ผ่านการตรวจสอบแล้วของ endpoints

ทั้งหมดคุณลักษณะนี้นำเสนอข้อมูลที่มีประโยชน์เกี่ยวกับความสมบูรณ์และความปลอดภัยของ endpoints โดยไม่คำนึงถึงที่ตั้ง ระบบปฏิบัติการ การเชื่อมต่อ (ซึ่งรวมถึงคอมพิวเตอร์ที่เชื่อมต่อหรือแล็ปท็อปเคลื่อนที่ซึ่งเชื่อมต่อเป็นระยะๆ) หรือแอพพลิเคชันที่ติดตั้ง ผลิตภัณฑ์นี้ช่วยรวมวงจรการปฏิบัติตามข้อบังคับ ส่งผลให้เวลาในการคอนฟิกูเรชัน endpoint และการแก้ไขลดลง

การจัดการความเสี่ยง

การจัดการความเสี่ยงช่วยให้คุณค้นพบ ประเมิน และแก้ไขความเสี่ยงได้ก่อนที่ endpoints จะได้รับผลกระทบ คุณลักษณะจะประเมินระบบโดยเปรียบเทียบกับคำนิยามความเสี่ยง open source security language (OVAL) มาตรฐานและรายงานนโยบายการไม่ปฏิบัติตามข้อบังคับในแบบเรียลไทม์ ผลลัพธ์คือทัศนวิสัยที่พัฒนาขึ้นและการรวมเข้ากันโดยสมบูรณ์ในทุกขั้นตอนตลอดทั้งเวิร์กโฟลว์ค้นหา-ประเมิน-แก้ไข-รายงาน



Tivoli Endpoint Manager for Security and Compliance จัดเตรียมรายงานที่ช่วยให้องค์กรมองเห็นภาพของปัญหาที่ส่งผลกระทบต่อประสิทธิภาพความพยายามรักษาความปลอดภัยและการปฏิบัติตามข้อบังคับ

ทีมงานด้านไอทีสามารถระบุและแก้ไขปัญหาความเสี่ยงบน endpoints โดยใช้การดำเนินการแบบอัตโนมัติหรือด้วยตนเอง—โดยการใช้เครื่องมือเพียงชิ้นเดียวทั้งในการค้นหาและแก้ไขปัญหาความเสี่ยง ผู้ดูแลระบบจึงสามารถแก้ไขปัญหาได้รวดเร็วและถูกต้องมากขึ้นสำหรับการนำแพตช์ อัพเดตซอฟต์แวร์และโปรแกรมแก้ไขความเสี่ยงไปใช้ ผู้ดูแลระบบยังสามารถขยายการจัดการ ความปลอดภัยไปยังไคลเอ็นต์แบบเคลื่อนที่ซึ่งเปิดหรือปิดการแจ้งเตือน—ค่าติดตั้งเครือข่ายเพื่อระบุสินทรัพย์ที่หลอกลวงอย่างรวดเร็ว และดำเนินขั้นตอน การค้นหาเพื่อแก้ไขหรือเอาสินทรัพย์นั้นออกไป

การค้นหาสินทรัพย์

ด้วย Tivoli Endpoint Manager for Security and Compliance การค้นหาสินทรัพย์จึงไม่ใช่เรื่อง “การงมเข็มในมหาสมุทร” อีกต่อไประบบจะสร้างการรับรู้ถึงสถานการณ์ที่เปลี่ยนแปลงไปเกี่ยวกับสภาพโครงสร้างพื้นฐานที่เปลี่ยนแปลงไป ความสามารถในการสแกน ทั้งเครือข่ายบ่อยครั้ง ทำให้สามารถนำเสนอทัศนวิสัยทั่วไปและการควบคุม เพื่อให้แน่ใจว่าองค์กรสามารถระบุอุปกรณ์ที่มี IP-address ทั้งหมดได้อย่างรวดเร็ว—รวมถึงเครื่องเสมือน อุปกรณ์เครือข่าย และอุปกรณ์รอบข้าง เช่น เครื่องพิมพ์ เครื่องสแกน เราเตอร์และสวิตช์ต่างๆ เพิ่มเติมจาก endpoints ของคอมพิวเตอร์—โดยสร้างผลกระทบต่อเครือข่ายน้อยที่สุด ฟังก์ชันนี้ช่วยเก็บรักษาทัศนวิสัยไว้ใน endpoints ของเอ็นเตอร์ไพรซ์ทั้งหมด รวมถึง แล็ปท็อปเคลื่อนที่และโน้ตบุ๊กคอมพิวเตอร์ที่ roaming นอกเหนือเครือข่ายเอ็นเตอร์ไพรซ์

บริหารจัดการระบบป้องกัน endpoint จากหลายค่าย

คุณลักษณะนี้ช่วยให้ผู้ดูแลระบบมีจุดควบคุมเพียงจุดเดียวสำหรับการจัดการกับไคลเอ็นต์ความปลอดภัย endpoint ของบุคคลที่สามจากผู้จำหน่ายต่างๆ เช่น Computer Associates, McAfee, Sophos, Symantec และ Trend Micro ด้วยความสามารถในการจัดการจากส่วนกลางนี้ องค์กรจึงสามารถพัฒนาความสามารถในการปรับสเกล ความเร็ว และความน่าเชื่อถือของโซลูชันการป้องกัน คุณลักษณะนี้จะมอนิเตอร์ความสมบูรณ์ของระบบ เพื่อให้แน่ใจว่าไคลเอ็นต์ความปลอดภัย endpoint รันอยู่เสมอและมีการอัพเดตรายชื่อไวรัส นอกจากนี้ ยังนำเสนอมุมมองรวมของเทคโนโลยีที่แตกต่างกันอย่างสิ้นเชิง สนับสนุนการย้าย endpoints จากโซลูชันหนึ่งไปยังโซลูชันอื่นโดย “คลิกเพียงครั้งเดียว” การลบซอฟต์แวร์และการติดตั้งอีกครั้ง การตรวจสอบความถูกต้องของลูปปิดทำให้มั่นใจว่าอัพเดตและการเปลี่ยนแปลงอื่นเสร็จสมบูรณ์แล้วรวมถึงการตรวจสอบความถูกต้องที่ใช้อินเทอร์เน็ตได้ของ endpoints ที่ตัดการเชื่อมต่อจากเครือข่าย

เครือข่ายที่กักกันตัวเอง (Network self-quarantine)

Tivoli Endpoint Manager for Security and Compliance จะประเมิน endpoints โดยอัตโนมัติตามคอนฟิกูเรชันการปฏิบัติตามข้อบังคับที่ต้องการ—และถ้าพบว่า endpoint ไม่เป็นไปตามข้อบังคับโซลูชันสามารถกำหนดคอนฟิก endpoint เพื่อให้มีการวาง endpoint นั้นไว้ในเครือข่ายที่กักกันจนกว่าสามารถปฏิบัติตามข้อบังคับได้สำเร็จ เซิร์ฟเวอร์ Tivoli Endpoint Manager มีสิทธิการจัดการใน endpoint แต่ไม่มีสิทธิอื่นทั้งหมด

เซอร์วิสต่อต้านมัลแวร์และชื่อเสียงเว็บ (optional add-on)

การรวมโดยละเอียดเข้ากับ Core Protection Module (CPM) ของ Trend Micro นำเสนอคุณลักษณะการป้องกัน endpoints จากไวรัส ม้าโทรจัน หนอน สปายแวร์, rootkits, ตัวแปรมัลแวร์ใหม่ และเว็บไซต์ที่ประสงค์ร้ายโดยการเคียวรีอัจริยะกลุ่ม threat ในแบบเรียลไทม์เพื่อตัดความต้องการไฟล์รายชื่อบน endpoint เทคโนโลยี ชื่อเสียงเว็บป้องกันไม่ให้ผู้ใช้เข้าถึงเว็บไซต์ที่ประสงค์ร้ายไม่ว่าโดยการดำเนินการของผู้ใช้เองหรือโดยการดำเนินการแบบอัตโนมัติที่ซ่อนไว้ซึ่งทำโดยมัลแวร์

ตระกูลผลิตภัณฑ์ Tivoli Endpoint Manager

คุณยังสามารถรวมเครื่องมือต่างๆ ลดจำนวนเอเจนต์ endpoint และลดต้นทุนการจัดการของคุณโดยการขยายการลงทุนใน Tivoli Endpoint Manager for Security and Compliance เพื่อรวมคอมโพเนนต์อื่นในตระกูลผลิตภัณฑ์ Tivoli Endpoint Management เนื่องจากฟังก์ชันทั้งหมดดำเนินงานจากคอนโซลเดียวกัน เซิร์ฟเวอร์การจัดการและเอเจนต์ endpoint เพียงเครื่องเดียว การเพิ่มเซอร์วิสจึงสามารถทำได้ง่ายโดยการเปลี่ยนไลเซนส์คีย์

- **Tivoli Endpoint Manager for Power Management**—อ็อพชันนี้จะเปิดทางการบังคับใช้นโยบายการอนุรักษ์พลังงานทั่วทั้งองค์กร ด้วยความละเอียดที่จำเป็นเพื่อให้สามารถประยุกต์ใช้นโยบายบนคอมพิวเตอร์เครื่องเดียว
- **Tivoli Endpoint Manager for Lifecycle Management**—แนวทางแบบครอบคลุมและทรงพลังนี้ให้ความสำคัญกับการรวมฟังก์ชันด้านไอทีเข้าด้วยกันเช่นในปัจจุบัน โดยการนำเสนอทัศนวิสัยสถานะของ endpoints ระบบในแบบเรียลไทม์และจัดเตรียมฟังก์ชันขั้นสูงสำหรับผู้ดูแลระบบในการจัดการกับ endpoints ดังกล่าว

Tivoli Endpoint Manager: สร้างขึ้นโดยใช้เทคโนโลยี BigFix

พลังงานเบื้องหลังฟังก์ชัน Tivoli Endpoint Manager ทั้งหมดคือแนวทางโครงสร้างพื้นฐานเดียวที่ไม่ซ้ำกันซึ่งจะแจกจ่ายการตัดสินใจไปยัง endpoints เพื่อนำเสนอประโยชน์พิเศษบนตระกูลโซลูชันทั้งหมด พร้อมด้วยคุณลักษณะที่รวมถึง:

- **เอเจนต์อัจฉริยะ**—Tivoli Endpoint Manager ใช้ แนวทางชั้นนำของอุตสาหกรรมที่จะวางเอเจนต์อัจฉริยะบน endpoint แต่ละจุด เอเจนต์เดียวนี้จะทำฟังก์ชันหลายอย่าง รวมถึงการประเมินตัวเองและการบังคับใช้นโยบายอย่างต่อเนื่อง—แต่กระทบต่อประสิทธิภาพของระบบน้อยที่สุด ตรงกันข้ามกับสถาปัตยกรรมไคลเอ็นต์-เซิร์ฟเวอร์แบบดั้งเดิมที่รอคำสั่งจากจุดควบคุมส่วนกลางเอเจนต์นี้จะเริ่มต้นการดำเนินการในลักษณะอัจฉริยะโดยส่งข้อความขึ้นไปยังเซิร์ฟเวอร์การจัดการส่วนกลางและดึงแพตช์ คอนฟิกูเรชัน หรือข้อมูลอื่นไปยัง endpoint เมื่อจำเป็นเพื่อให้เป็นไปตามนโยบายที่เกี่ยวข้อง ผลจากความชาญฉลาดและความเร็วของเอเจนต์ทำให้เซิร์ฟเวอร์การจัดการส่วนกลางทราบถึงการปฏิบัติตามข้อบังคับและสถานะที่เปลี่ยนแปลงของ endpoints อยู่เสมอ และสามารถรายงานการปฏิบัติตามข้อบังคับที่ทันสมัยได้อย่างรวดเร็ว
- **การรายงาน**—คอนโซลรวมเครื่องเดียวที่ติดตั้งในตัว TivoliEndpoint Manager ประสานทัศนวิสัยระดับสูงที่รวมการรายงานและการวิเคราะห์ที่ต่อเนื่องแบบเรียลไทม์จากเอเจนต์อัจฉริยะไว้บน endpoint ขององค์กร
- **ความสามารถรีเลย์**—Tivoli Endpoint Manager มีสถาปัตยกรรมน้ำหนักเบาและปรับสเกลได้ที่ช่วยให้สามารถกำหนดคอนฟิกเอเจนต์เป็นรีเลย์ระหว่างเอเจนต์อื่นและคอนโซล ฟังก์ชันรีเลย์นี้ช่วยให้สามารถใช้เซิร์ฟเวอร์หรือเวิร์กสเตชันที่มีอยู่เพื่อโอนย้ายแพ็กเกจบนเครือข่ายและลดความต้องการเซิร์ฟเวอร์
- **ข้อความ IBM Fixlet®** — Fixlet Relevance Language คือภาษาคำสั่งที่เผยแพร่ซึ่งช่วยให้ลูกค้าคู่ค้าทางธุรกิจ และผู้พัฒนาสามารถสร้างนโยบายแบบกำหนดเองและเซอร์วิสสำหรับ endpoints ที่จัดการโดยโซลูชัน Tivoli EndpointManager

การขยายความรับผิดชอบของ Tivoli ในการรักษาความปลอดภัย

Tivoli Endpoint Manager for Security and Compliance เป็นส่วนประกอบหนึ่งของงานด้านความปลอดภัยแบบครอบคลุมของ IBM ที่ช่วยระบุปัญหาความปลอดภัยทั่วทั้งองค์กร ด้วยการสนับสนุนการดำเนินงานด้านไอทีอัจฉริยะที่มีการควบคุมและเชื่อมต่อกันของอุปกรณ์ที่ฉลาดขึ้น โซลูชันการรักษาความปลอดภัยของ IBM ช่วยให้มั่นใจถึงทัศนวิสัยแบบเรียลไทม์การควบคุมจากส่วนกลาง และความปลอดภัยที่พัฒนาขึ้นสำหรับโครงสร้างพื้นฐานด้านไอทีทั้งหมด รวมถึง endpoints ที่แจกจ่ายไปทั่วโลก

ผลิตภัณฑ์ตระกูล Tivoli Endpoint Manager แบบรวดเร็ว

ข้อกำหนดสำหรับเซิร์ฟเวอร์:

- Microsoft SQL Server 2005/2008
- Microsoft Windows Server 2003/2008/2008 R2

ข้อกำหนดคอนโซล:

- Microsoft Windows XP/2003/Vista/2008/2008 R2/7

แพลตฟอร์มที่สนับสนุนสำหรับเอเจนต์:

- Microsoft Windows รวมถึง XP, 2000, 2003, Vista, 2008, 2008 R2, 7, CE, Mobile, XP Embedded และ Embedded Point-of-Sale
- Mac OS X
- Solaris
- IBM AIX®
- Linux บน IBM System z®
- HP-UX
- VMware ESX Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise
- Oracle Enterprise Linux
- CentOS Linux
- Debian Linux
- Ubuntu Linux

สำหรับข้อมูลเพิ่มเติม

หากต้องการศึกษาเพิ่มเติมเกี่ยวกับ IBM Tivoli Endpoint Manager for Security and Compliance โปรดติดต่อตัวแทนฝ่ายขาย IBM ของคุณ หรือ IBM Business Partner หรือเยี่ยมชม: **ibm.com**/tivoli/endpoint

เกี่ยวกับซอฟต์แวร์ Tivoli จาก IBM

ซอฟต์แวร์ Tivoli จาก IBM ช่วยให้องค์กรสามารถจัดการกับรีซอร์สด้านไอที ภารกิจ และกระบวนการต่างๆ ได้อย่างมีประสิทธิภาพและประสิทธิผล เพื่อให้ตรงกับความต้องการทางธุรกิจที่เปลี่ยนแปลงตลอดเวลา และนำเสนอการจัดการเซอร์วิสด้านไอทีที่ยืดหยุ่นที่ตอบสนองอย่างรวดเร็ว อีกทั้งยังช่วยลดต้นทุน ชุดผลิตภัณฑ์ Tivoli ขยายศักยภาพซอฟต์แวร์สำหรับความปลอดภัยการปฏิบัติตามข้อบังคับ การจัดเก็บ ประสิทธิภาพความพร้อมใช้งาน คอนฟิกูเรชันการดำเนินงานและการจัดการวงจรอายุไอที และมีการสนับสนุนโดยเซอร์วิส การสนับสนุน และการวิจัยระดับโลกของ IBM

IBM Corporation Software Group
Route 100
Somers, NY 10589
U.S.A.

ผลิตในประเทศสหรัฐอเมริกา
กุมภาพันธ์ 2011

กรุณารีไซเคิล

Tivoli software

TID14075-USEN-00