CYBER SECURITY
และแนวทางป้องกัน

Information Technology

CYBER SECURITY คืออะไร ทำไมทุกองค์กรถึงให้ความสำคัญ

Cyber Security คือเทคโนโลยี, กระบวนการและวิธีปฏิบัติที่ถูกออกแบบมาเพื่อปกป้องเครือข่าย, อุปกรณ์, โปรแกรมและข้อมูลจากการโจมตี, ความเสียหายหรือการเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต สรุปสั้น ๆ **Cyber Security** อาจเรียกว่าความมั่นคงปลอดภัยทางไซเบอร์

ความสำคัญของ Cyber Security

การรักษาความมั่นคงปลอดภัยไซเบอร์ ความสำคัญอย่างยิ่ง เนื่องจากองค์กร ไม่ว่าจะเป็นภาครัฐหรือเอกชนต่างรวบรวม, ประมวลผลและจัดเก็บข้อมูลจำนวนมากบนคอมพิวเตอร์และอุปกรณ์อื่น ๆ ซึ่งข้อมูลเหล่านั้นอาจเป็นข้อมูลที่ค่อนข้างละเอียดอ่อนไม่ว่าจะเป็นทรัพย์สินทางปัญญา, ข้อมูลทางการเงินข้อมูลส่วนบุคคลหรือข้อมูลประเทศอื่น ๆ ที่บุคคลอื่นสามารถเข้าถึงหรือเปิดเผยได้โดยไม่ได้รับอนุญาตอาจส่งผลกระทบด้านลบกับองค์กรได้ เพราะองค์กรมักส่งข้อมูลที่มีความสำคัญข้ามเครือข่ายและอุปกรณ์ในการทำธุรกิจ ข้อมูลเหล่านั้นจึงควรได้รับการปกป้องโดยเฉพาะในยุคที่การโจมตีทางไซเบอร์นั้นมีความซับซ้อนมากขึ้น การโจมตีทางไซเบอร์และการสอดแนมทางดิจิทัลเป็นภัยคุกคามที่สำคัญที่สุดต่อการทำธุรกิจ

ดังนั้นเพื่อความปลอดภัยบนโลกไซเบอร์ที่มีประสิทธิภาพองค์กรจำเป็นต้องมี **Cyber Security** เพราะมันเป็นสิ่งที่ครอบคลุมสิ่งต่อไปนี้

- **Network security :** เป็นกระบวนการปกป้องเครือข่าย หรือเน็ตเวิร์คจากผู้ใช้ที่ต้องการการโจมตีและการบุกรุก
- **Application security :** แอปพลิเคชั่นต้องการการอัพเดทและการทดสอบอย่างต่อเนื่องเพื่อให้แน่ใจว่าโปรแกรมเหล่านี้ปลอดภัยจากการโจมตีของบุคคลที่สาม
- **Data security :** สิ่งที่อยู่ภายในเครือข่ายและแอปพลิเคชันคือข้อมูล การปกป้องข้อมูล บริษัท และลูกค้าเป็นความปลอดภัยอีกขั้นหนึ่ง
- **Cloud security :** ในปัจจุบันไฟล์จำนวนมากอยู่ในสภาพแวดล้อมแบบดิจิทัลหรือ“ คลาวด์” การปกป้องข้อมูลในสภาพแวดล้อมที่เป็นออนไลน์ถือเป็นความท้าทายอย่างหนึ่ง ที่องค์กรควรให้ความสำคัญ

ทำความรู้จักกับมัลแวร์ (MALWARE) และวิธีการป้องกันง่าย ๆ ด้วยตัวคุณเอง

MALWARE

Malicious Software หรือที่เรารู้จักกันว่ามัลแวร์ (Malware) เป็นชื่อเรียกโดยรวมของเหล่าโปรแกรมคอมพิวเตอร์ทุกชนิดที่ถูกออกแบบมาเพื่อมุ่งร้ายต่อคอมพิวเตอร์และเครือข่าย ไม่ว่าจะเป็น ไวรัส (Virus), วอร์ม (Worm), โทรจัน (Trojan), สปายแวร์ (Spyware) เป็นต้น ดังนั้น ผู้ใช้งานคอมพิวเตอร์ทุกคนควรรู้ลักษณะและพฤติกรรมการทำงานของมัลแวร์ในทุกรูปแบบ รวมถึงการป้องกันตัวเองจากมัลแวร์ง่าย ๆ ที่ใคร ๆ ก็สามารถทำได้

ลักษณะและพฤติกรรมการทำงานของมัลแวร์ในแต่ละประเภท

- **Virus:** มักจะแฝงตัวมากับโปรแกรมคอมพิวเตอร์หรือไฟล์และสามารถแพร่กระจายไปยังเครื่องอื่น ๆ ได้โดยแนบตัวเองไปกับโปรแกรมหรือไฟล์ดังกล่าว แต่ไวรัสจะทำงานก็ต่อเมื่อมีการรันโปรแกรมหรือเปิดไฟล์เท่านั้น
- **Worm:** สามารถแพร่กระจายตัวเองไปยังคอมพิวเตอร์และอุปกรณ์เครื่องอื่น ๆ ผ่านทางระบบเครือข่าย เช่น อีเมล หรือระบบแชร์ไฟล์
- **Trojan:** หลอกล่อผู้ใช้ว่าเป็นโปรแกรมที่ปลอดภัย แต่จริง ๆ แล้วจะทำให้เกิดความเสียหายเมื่อผู้ใช้หลงเชื่อนำไปติดตั้ง โดยที่ผู้ใช้ไม่รู้ตัวว่ามีโปรแกรมอื่นที่อันตรายแฝงตัวมาด้วย
- **Backdoor:** เปิดช่องทางให้ผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์ของเราโดยไม่รู้ตัว
- **Rootkit:** เปิดช่องทางให้ผู้อื่นเข้ามาติดตั้งโปรแกรมเพิ่มเติมเพื่อควบคุมเครื่อง พร้อมได้สิทธิ์ของผู้ดูแลระบบ (Root)
- **Spyware:** แอบดูพฤติกรรมและบันทึกการใช้งานของผู้ใช้ และอาจขโมยข้อมูลส่วนตัว เช่น บัญชีชื่อผู้ใช้งาน, รหัสผ่าน หรือข้อมูลทางการเงิน เป็นต้น พร้อมทั้งส่งข้อมูลดังกล่าวไปในเครื่องปลายทางที่ได้ระบุเอาไว้อีกด้วย
- **Ransomware:** ทำการเข้ารหัสหรือล็อกไฟล์ ผู้ใช้จะไม่สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้ จากนั้นก็จะส่งข้อความ “เรียกค่าไถ่” เพื่อแลกกับการถอดรหัสเพื่อกู้ข้อมูลคืนมา

ข้อแนะนำในการป้องกันการติดมัลแวร์

1. อัพเดทคอมพิวเตอร์และซอฟต์แวร์ในเครื่องสม่ำเสมอ

2. ติดตั้งโปรแกรมป้องกันมัลแวร์ (Anti-malware) บนคอมพิวเตอร์

3. ระมัดระวังการใช้งานอุปกรณ์เชื่อมต่อทั้งหลาย เช่น แฟลชไดร์ฟ (USB) เป็นต้น ควรทำการสแกนไวรัสทุกครั้งก่อนใช้งาน

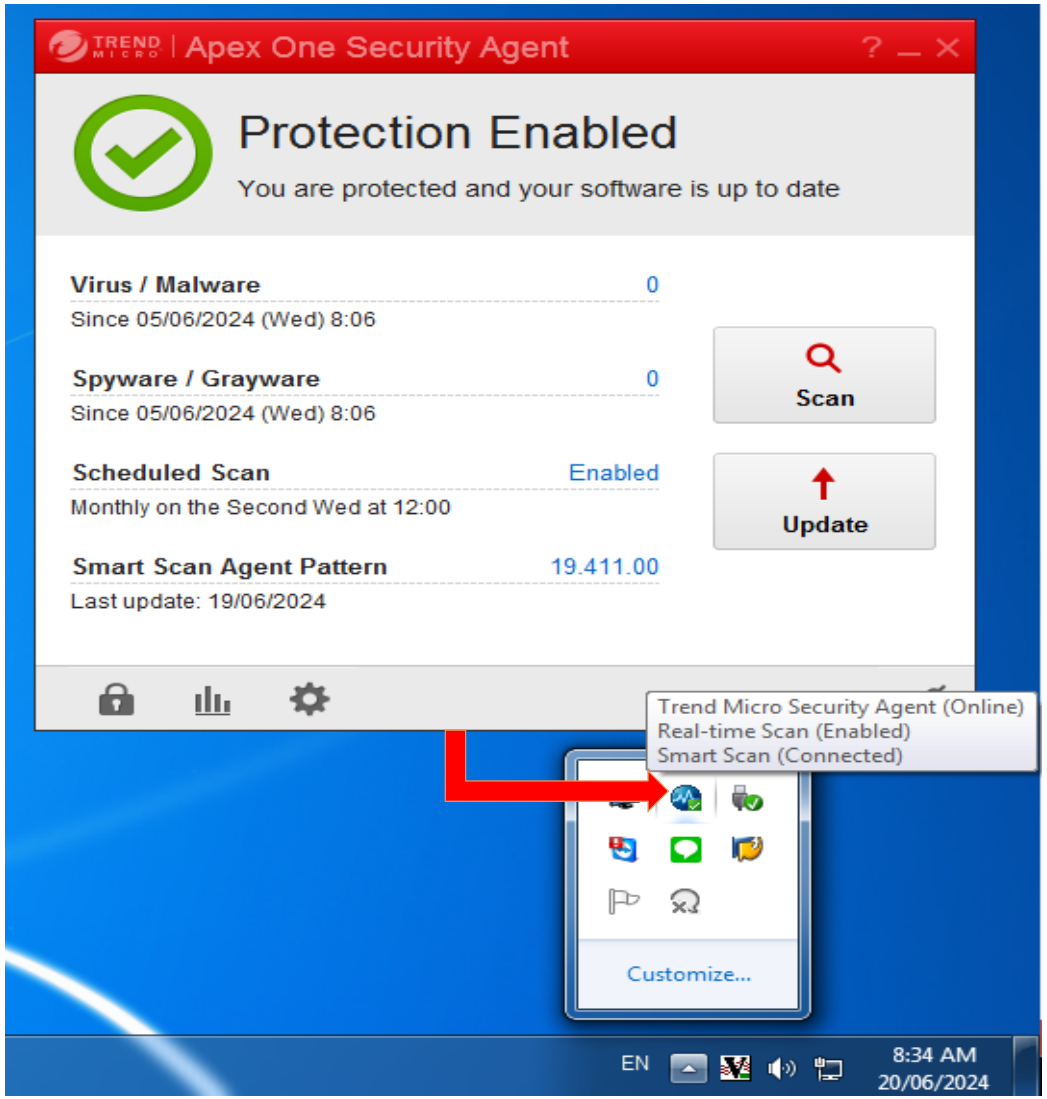
4. ไม่คลิกข้อความที่แสดงโฆษณาหรือหน้าต่าง pop-up ปลอม (Adware) บนเว็บไซต์ที่เยี่ยมชม เพราะจะเป็นการเริ่มดาวน์โหลดมัลแวร์ จะต้องเช็คและตรวจสอบก่อนคลิกเสมอ

5. ไม่ดาวน์โหลดโปรแกรมจากแหล่งที่ไม่น่าเชื่อถือ เสี่ยงต่อการมีมัลแวร์แฝงอยู่

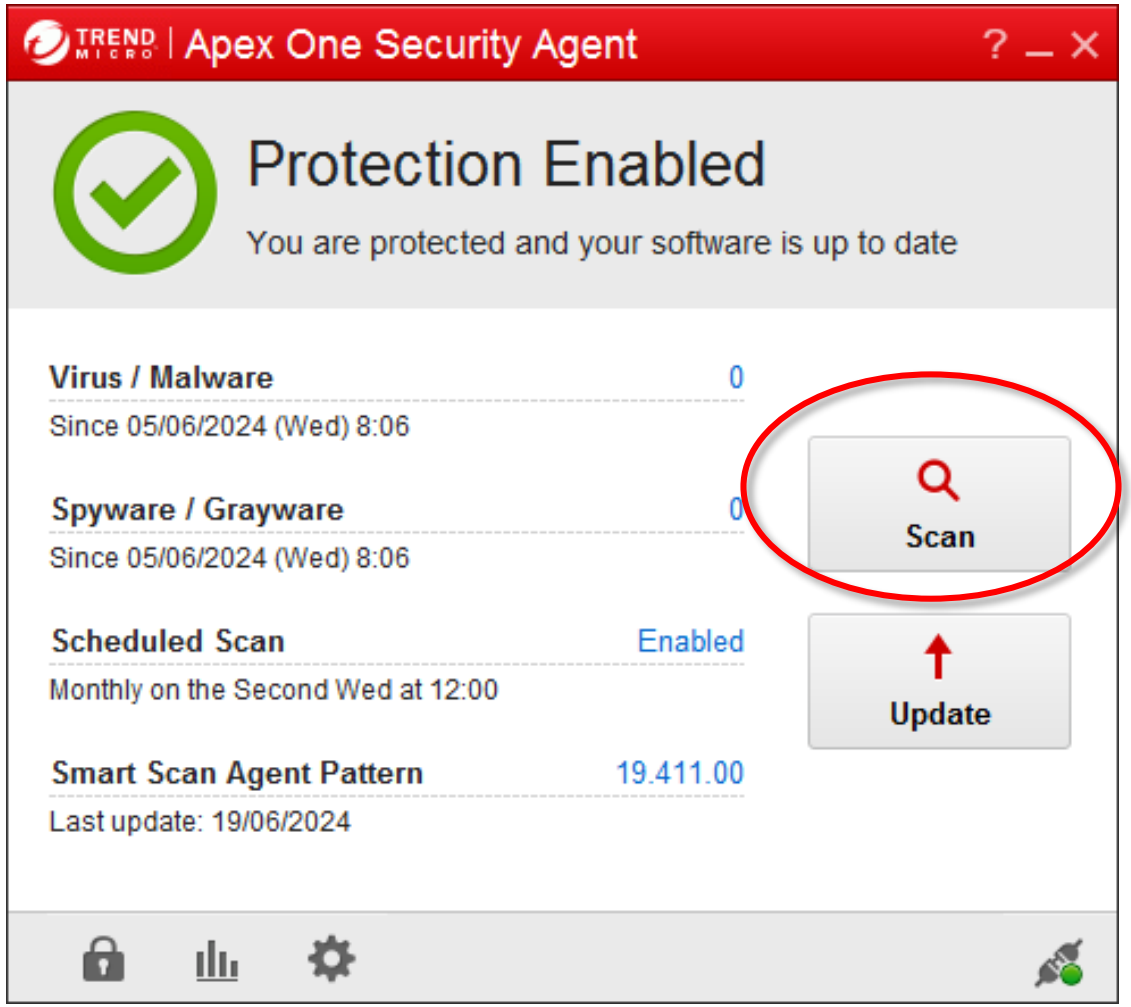
6. หลีกเลี่ยงการเปิดอีเมล รวมไปถึงไฟล์แนบที่ต้องสงสัยใด ๆ ที่ส่งมาจากอีเมลที่เราไม่รู้จัก และต้องตรวจสอบทุกครั้งก่อนดาวน์โหลดหรือเปิดไฟล์ขึ้นมา

การใช้งานโปรแกรม

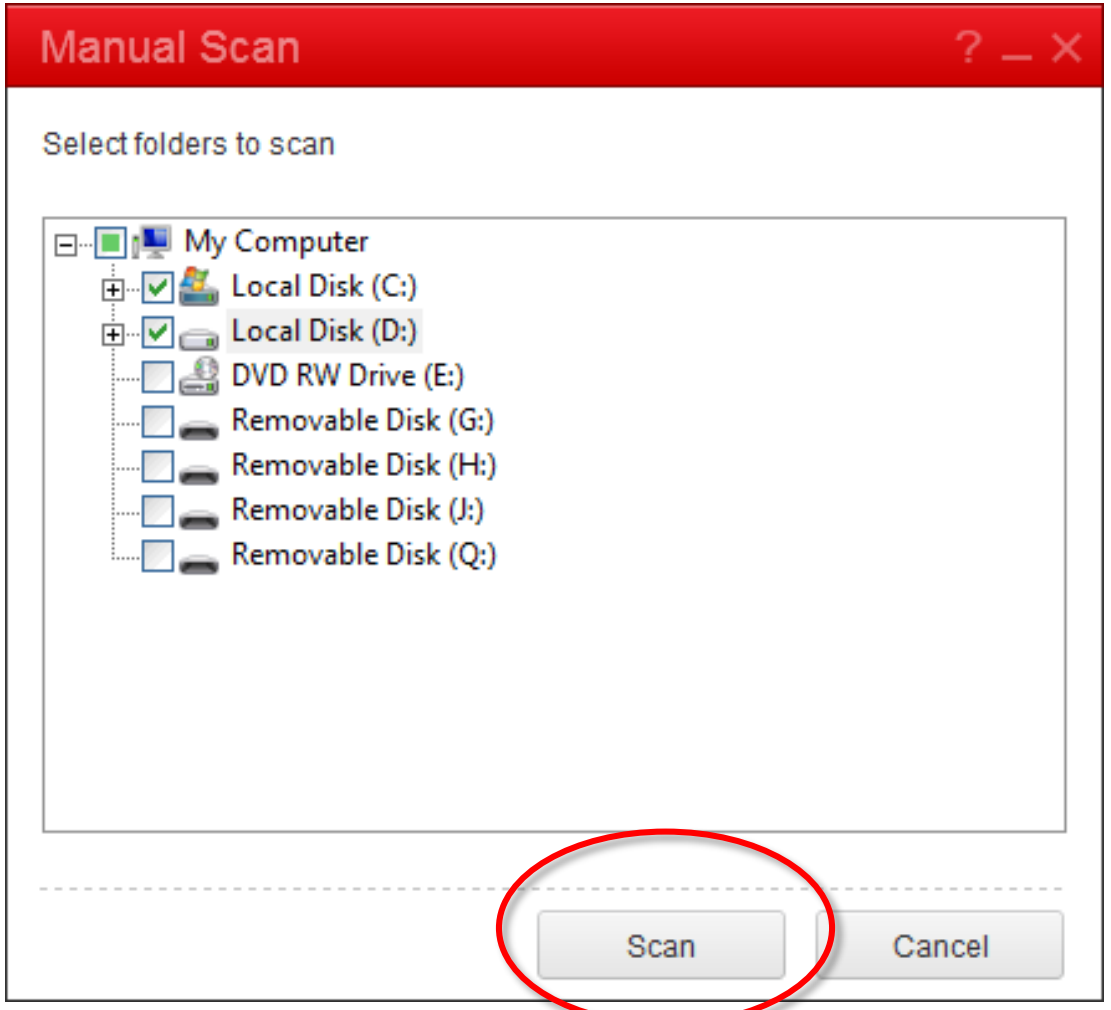
Antivirus Apex One



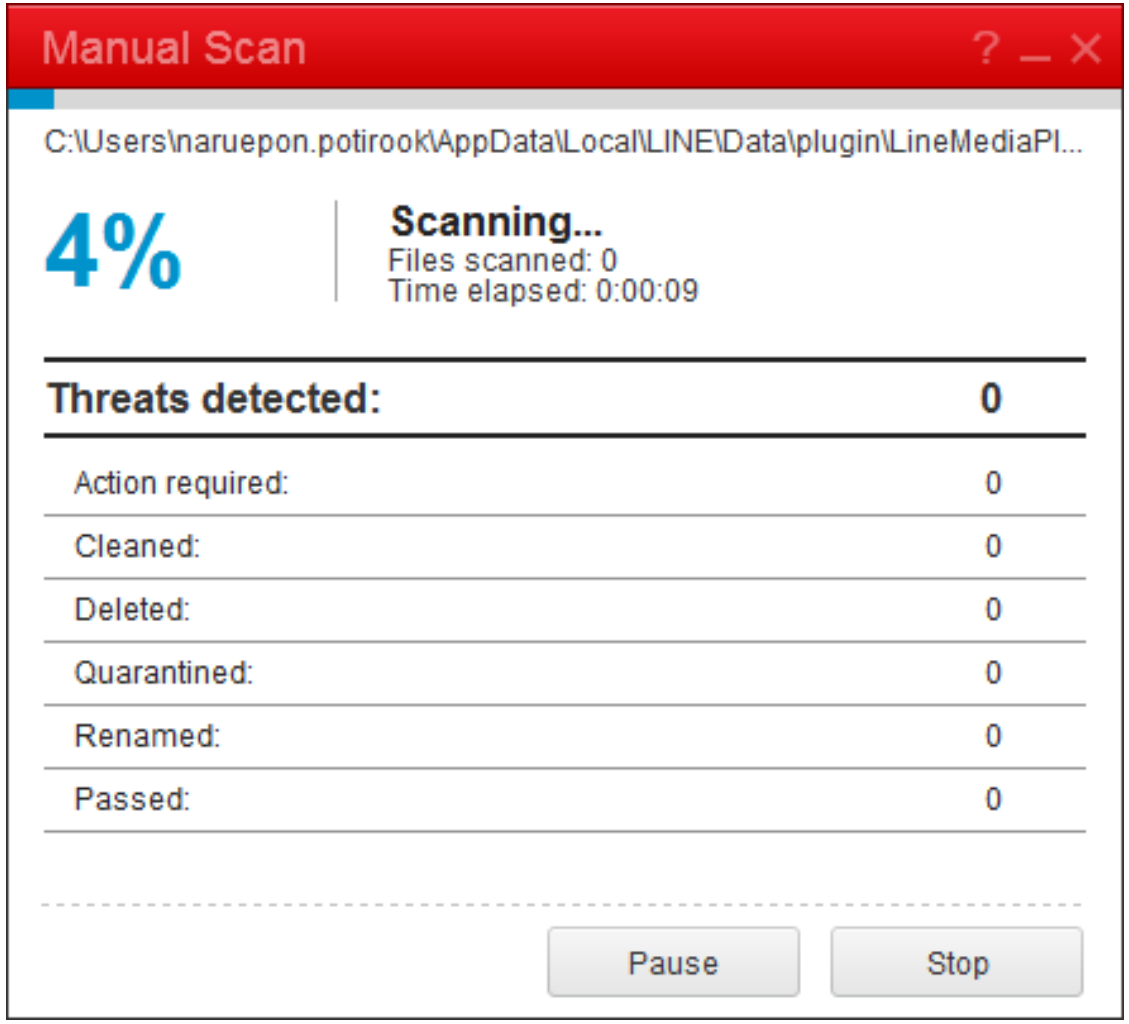
- Click Scan



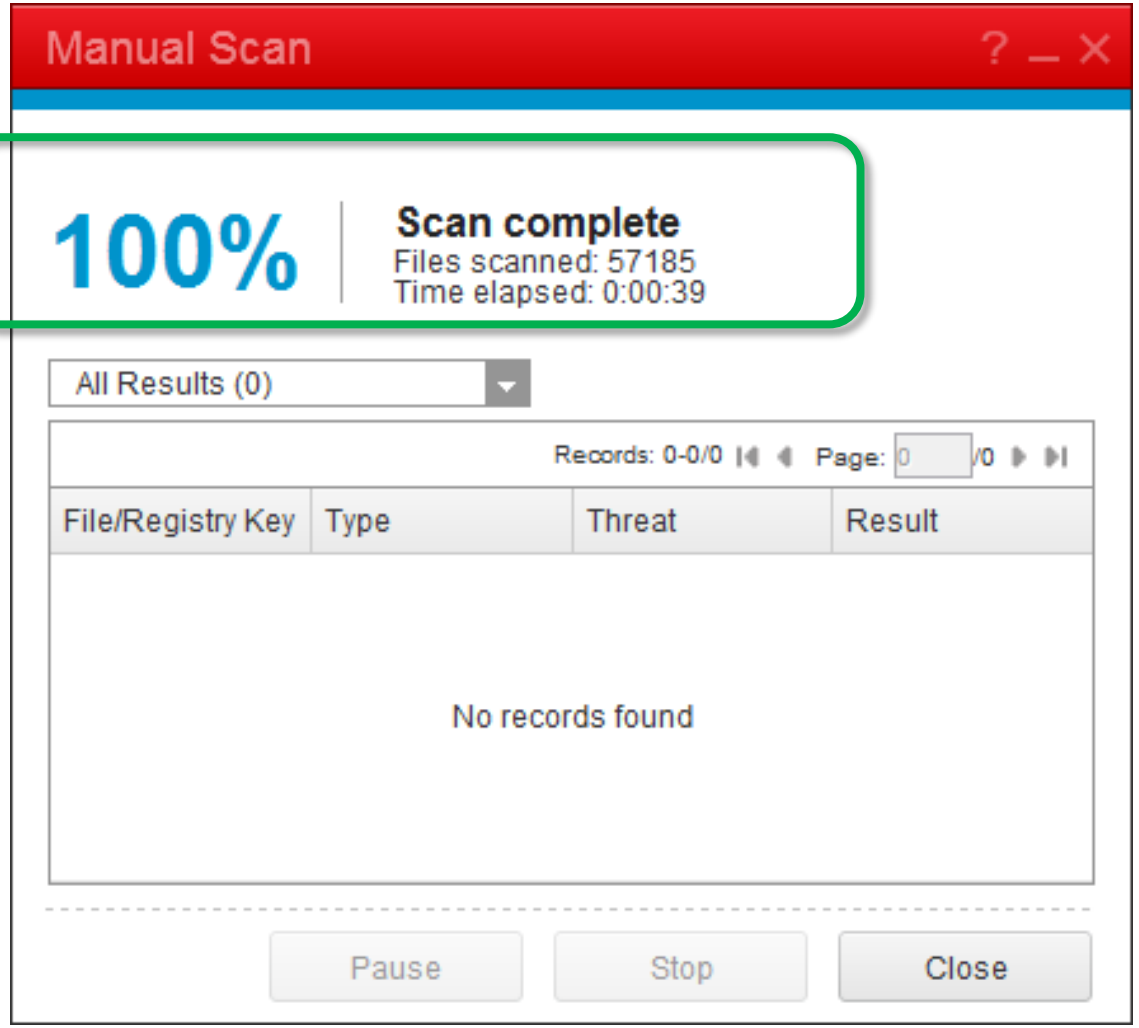
- เลือก Drive ที่ต้องการ Scan Virus กดปุ่ม Scan



- เครื่องจะเริ่ม **Scan Virus** และ **Show %** การทำงาน



- หลังจาก **Scan** ครบ 100% จะโชว์ **Report** การตรวจ **Virus**




THANK YOU