

ข้อกำหนดคุณลักษณะของโปรแกรมป้องกันไวรัส

โปรแกรมป้องกันไวรัสจะต้องประกอบด้วย

1. โปรแกรมบริหารจัดการระบบป้องกันไวรัสจากส่วนกลาง (Antivirus Network Server)
2. โปรแกรมป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่มีระบบปฏิบัติการ Microsoft Windows
3. โปรแกรมป้องกันไวรัสบนเครื่องคอมพิวเตอร์ลูกข่าย (Clients)

1. โปรแกรมบริหารจัดการระบบป้องกันไวรัสจากส่วนกลาง (Antivirus Network Server)

มีคุณสมบัติอย่างน้อย ดังนี้

- 1.1 สามารถติดตั้งโปรแกรมบริหารจัดการได้บนเครื่อง Windows Server 2003 SP2, Windows Server 2008 R2, Windows Server 2012 Windows XP SP3, Windows 7, Windows 8, Windows 8.1
- 1.2 รองรับการใช้งานกับ Database Microsoft SQLServer 2008, 2005 หรือดีกว่า MySQL 5.0 หรือดีกว่า
- 1.3 สามารถบริหารจัดการความปลอดภัยบนเครื่องคอมพิวเตอร์สำหรับองค์กรที่ประกอบไปด้วยเทคโนโลยีทางด้าน Anti-Malware, Personal Firewall, Intrusion Detection และ Device, Web and Application Control เป็นอย่างน้อย อยู่ใน Agent เดียว
- 1.4 สามารถทำการ update virus/spyware pattern แบบ incremental update เพื่อลดภาระในระบบเครือข่ายได้
- 1.5 สามารถทำการ Update โดยกำหนดให้เครื่องลูกข่ายอื่น ๆ เป็นแหล่งของการเข้ามา update ได้ (Update Agent)
- 1.6 สามารถแสดงรายงานของไฟล์ที่ถูกสำรองข้อมูลไว้หากถูกลบไป (backup) หรือ โดนกักกัน (quarantine) ไว้ได้จากส่วนกลางและสามารถส่งคืนค่าไฟล์ดังกล่าวได้จากส่วนกลาง
- 1.7 สามารถตรวจสอบโปรแกรมต่างๆ ที่ติดตั้งอยู่บนเครื่องลูกข่ายในระบบได้ และสามารถออกรายงานของโปรแกรมต่างๆ เพื่อให้ผู้ดูแลระบบสามารถตรวจสอบถึงโปรแกรมที่ไม่เป็นที่ต้องการขององค์กรได้ (Inventory)
- 1.8 สามารถทำการกู้คืนและสำรองฐานข้อมูลของเครื่องแม่ข่ายเพื่อป้องกันในกรณีระบบเกิดการเสียหาย (Backup)
- 1.9 สามารถดึง (import) เอรายละเอียดกลุ่มที่ได้สร้างเอาไว้จาก Active Directory เพื่อนำมาแบ่งกลุ่มการใช้งานตัวโปรแกรมบริหารจากส่วนกลางได้
- 1.10 สามารถสร้างรายงาน ในรูปแบบ PDF, XML และ HTML ได้
- 1.11 สามารถควบคุมและบริหารจัดการจากโปรแกรมบริหารจัดการเดิมที่ ศทส. ใช้งานอยู่เดิมได้
- 1.12 สามารถตั้งรหัสในการป้องกันการใช้งานโปรแกรมจัดการป้องกันไวรัสที่ติดตั้งบนเครื่องควบคุมส่วนกลางได้
- 1.13 สามารถจัดตั้งเครื่องควบคุมส่วนกลางได้หลายเครื่องเพื่อส่งข้อมูลและสั่งงานกันได้ระหว่างเครื่องจัดการและบริหารโปรแกรมป้องกันไวรัสจากศูนย์กลางกันเองและเครื่องลูกข่ายได้

รณ พจน *ธน* *อภิเดช*

2. ข้อกำหนดคุณสมบัติของโปรแกรมป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่มีระบบปฏิบัติการ Microsoft Windows มีคุณสมบัติอย่างน้อย ดังนี้

- 2.1 สามารถติดตั้งบนระบบปฏิบัติการ Windows รุ่นต่าง ๆ เช่น Windows Server 2003, Windows Server 2008, Windows server 2008 R2 และ Windows server 2012 ทั้งแบบ 32 และ 64 bits ได้
- 2.2 สามารถป้องกันจาก Malware (Virus, Spyware, Bots, Backdoors, Key loggers, Root kits, Dialers, Adware, Trojans, Phishing และ Worm) แบบ Real time protection ได้
- 2.3 มีเทคโนโลยีในการตรวจจับ Malware แบบ Signature base, Proactive, Cloud Technology
- 2.4 สามารถทำงานแบบ Personal firewall และสามารถทำการตรวจจับการโจมตีผ่านทางระบบเครือข่าย พร้อมทั้งแสดงถึงแหล่งที่มาของการโจมตีเหล่านั้นได้ (Intrusion Detection System)
- 2.5 สแกนไฟล์ในรูปแบบ Compressed, Installation packages และ OLE objects ได้
- 2.6 สามารถป้องกันตนเอง (self-Defense) การปิด Service ของโปรแกรม Antivirus ได้ ถึงแม้ว่าจะมีสิทธิ์เป็น Administrator ของระบบก็ตาม
- 2.7 สามารถกำหนด Password จาก Server ในการป้องกันการตั้งค่าตัวโปรแกรม เพื่อไม่ให้ User สามารถแก้ไข หรือ Uninstall โปรแกรมได้
- 2.8 สามารถทำการ scan โดยไม่ไป scan หรือตรวจสอบไฟล์เดิมซ้ำ เป็นการลดเวลาในการตรวจสอบไฟล์
- 2.9 สามารถกำหนดการยกเว้นการ Scan โดยระบุเป็นนามสกุลไฟล์ได้ สามารถทำการสั่ง Scan โดย On-Demand ได้ (Trust Zone)
- 2.10 สามารถส่งอีเมล หรือ Alert Message ไปยังผู้ดูแลระบบได้ เมื่อเครื่อง Server ตรวจพบไวรัส สามารถนำ Alert Message ออกรายงานในรูปแบบ HTML หรือ Text ได้
- 2.11 มีโมดูล Application Privilege Control เพื่อป้องกันไวรัสติดไฟล์เอกสาร Microsoft Office

รณ พิศน ภาณุ ภิธาน

๒๒ ก.ย. ๒๕๕๙

3. ข้อกำหนดคุณสมบัติของโปรแกรมป้องกันไวรัสบนเครื่องคอมพิวเตอร์ลูกข่าย (Clients)

มีคุณสมบัติอย่างน้อย ดังนี้

- 3.1 สามารถติดตั้งบนระบบปฏิบัติการ Windows รุ่นต่าง ๆ เช่น Windows XP, Windows Vista , Windows 7, Windows 8, Windows 8.1 , Windows 10 ทั้งแบบ 32 และ 64 bits ได้
- 3.2 สามารถป้องกันจาก Malware (Virus, Spyware, Bots, Backdoors, Key loggers, Root kits, Dialers, Adware, Trojans, Phishing และ Worm) แบบ Real time protection ได้
- 3.3 มีเทคโนโลยีในการตรวจจับ Malware แบบ Signature base, Proactive, Cloud Technology
- 3.4 สามารถทำงานแบบ Personal firewall และสามารถทำการตรวจจับการโจมตีผ่านทางระบบเครือข่าย พร้อมทั้งแสดงถึงแหล่งที่มาของการโจมตีเหล่านั้นได้ (Intrusion Detection System)
- 3.5 สามารถป้องกันตนเอง (self-Defense) การปิด Service ของโปรแกรม Antivirus ได้ ถึงแม้ว่าจะมีสิทธิ์ Administrator ของระบบก็ตาม
- 3.6 สามารถกำหนด Password จาก Server ในการป้องกันการตั้งค่าตัวโปรแกรม เพื่อไม่ให้ User สามารถแก้ไข หรือ Uninstall โปรแกรมได้
- 3.7 สามารถทำการตรวจสอบเฉพาะไฟล์สร้างใหม่หรือมีการเปลี่ยนแปลง เพื่อลดเวลาในการตรวจสอบไฟล์
- 3.8 สามารถกำหนดการยกเว้นการ Scan โดยระบุเป็นนามสกุลไฟล์ได้ สามารถทำการสั่ง Scan โดย On-Demand ได้ (TrustZone)
- 3.9 สามารถส่งอีเมล หรือ Alert Message ไปยังผู้ดูแลระบบได้ เมื่อเครื่อง Server ตรวจพบไวรัส สามารถนำ Alert Message ออกรายงานในรูปแบบ HTML หรือ Text ได้
- 3.10 สามารถกู้คืนความเสียหายที่เกิดขึ้นจากพฤติกรรมของไวรัสได้ (Roll back Malicious Activity)
- 3.11 สามารถกำหนด อนุญาต/ไม่อนุญาต/แจ้งเตือน การเข้าใช้งาน website ของ user แต่ละคนได้
- 3.12 สามารถอนุญาต/ไม่อนุญาต/ตรวจสอบ การใช้งานโปรแกรมที่ใช้อยู่ในเครื่องได้
- 3.13 สามารถอนุญาต/ไม่อนุญาต การใช้งานอุปกรณ์พกพาจำพวก Flash drive memory, cd-dvd drive, Bluetooth ของแต่ละ User ได้
- 3.14 สามารถตรวจสอบถึงพฤติกรรมอันตรายของไฟล์เพื่อเป็นการยับยั้งการแพร่ระบาดของโปรแกรมที่มีความร้ายแรงได้ (System Watcher) รวมไปถึงวิเคราะห์พฤติกรรมของไฟล์นั้นๆ ว่าอันตรายหรือไม่ หากเป็นอันตรายต้องสามารถห้ามไม่ให้ใช้งานไฟล์ดังกล่าวได้
- 3.15 มีโมดูล Application Privilege Control เพื่อป้องกันไวรัสติดไฟล์เอกสาร Microsoft Office
- 3.16 สามารถควบคุมบริหารจัดการสิทธิ์ในการใช้งานโปรแกรมต่างๆ บนเครื่องลูกข่ายได้
- 3.17 สามารถกำหนดสิทธิ์ในการ อ่าน เขียน ลบ และสร้างไฟล์ในการใช้งานโปรแกรมต่างๆ ได้

Signature *Man* *Amir*

๒๕๕๙