การเรียนการสอนที่ปลอดภัยสำหรับโรงเรียน K-12 ด้วยโซลูชันด้านการศึกษาของ Lenovo

ความมั่นคงปลอดภัยทางไซเบอร์ที่แข็งแกร่ง AI ขั้นสูง เหมาะสำหรับการเรียนรู้แบบผสมผสาน

อาชญากรไซเบอร์มุ่งเป้าไปที่ระบบที่มีช่องโหว่มากขึ้นเรื่อยๆ และสถาบันการศึกษาเองก็ไม่เว้น โรงเรียน K-12 ต้องเผชิญกับความท้าทายเป็นทวีคูณในการปกป้องข้อมูลสำคัญของนักเรียนและรักษาสภาพแวดล้อมในการเรียนรู้ที่ปลอดภัย

ด้วยเครื่องมือในการเรียนแบบดิจิทัลและห้องเรียนแบบผสมผสานที่เพิ่มขึ้น พื้นที่ในการโจมตีจึงขยายตัวเพิ่มขึ้น ทำให้โรงเรียนกลายเป็นเป้าหมายที่น่าสนใจสำหรับอาชญากรไซเบอร์ การโจมตีด้วยมัลแวร์เรียกค่าไถ่ที่ควบคุมโดยแฮกเกอร์เพิ่มขึ้นมากกว่า 200%[1] และความเสียหายโดยเฉลี่ยจากการรั่วไหลของข้อมูลในปัจจุบันสูงเกินกว่า 5 ล้านเหรียญสหรัฐ[2] มีการคาดการณ์ว่าอาชญากรรมไซเบอร์ทั่วโลกจะมีมูลค่าความเสียหาย 10.5 ล้านล้านดอลลาร์ต่อปีภายในปี 2025[3]

Lenovo ร่วมมือกับผู้นำด้านเทคโนโลยีรายอื่นๆ เช่น Intel® และ Microsoft เพื่อพัฒนาโซลูชันด้านความปลอดภัยที่เป็นนวัตกรรม โดยใช้ AI ขั้นสูงเพื่อปกป้องอุปกรณ์, ข้อมูล และสถาบันการศึกษาต่างๆ การรักษาความปลอดภัยระดับฮาร์ดแวร์ของ Intel® และ Windows 11 ซึ่งเป็น Windows ที่ปลอดภัยที่สุดเท่าที่เคยมีมา ได้ผลักดันให้ฟีเจอร์ด้านความปลอดภัยที่ล้ำสมัยเหล่านี้ขึ้นมาอยู่ในระดับแนวหน้า ช่วยสร้างรากฐานที่แข็งแกร่งเพื่อปกป้องสภาพแวดล้อม K-12 จากรูปแบบภัยคุกคามที่เปลี่ยนแปลงไป เราช่วยท่านดำเนินการเพื่อป้องกันปัญหาในเรื่องอนาคตแห่งยุคดิจิทัลที่ปลอดภัยและยืดหยุ่นยิ่งขึ้นสำหรับโรงเรียน

การโจมตีด้วยมัลแวร์เรียกค่าไถ่ที่ควบคุมโดยแฮกเกอร์เพิ่มขึ้นมากกว่า

200%[1]

ความเสียหายโดยเฉลี่ยจากการรั่วไหลของข้อมูลในปัจจุบันสูงเกินกว่า 5 ล้านเหรียญสหรัฐ[1]

$5M[1]

Lenovo ThinkPad L13 2-in-1

intel CORE ULTRA 7 | intel vPRO

Intel® Core™ Ultra 7 processor powering Intel vPro®

Smarter technology for all

Lenovo

Lenovo ThinkPad T14s Gen 5

รู้หรือไม่ว่าการโจมตีมากกว่า 99% สามารถป้องกันได้?

งานวิจัยระบุว่าการโจมตีทางไซเบอร์ส่วนใหญ่สามารถป้องกันได้ด้วยการนำแนวปฏิบัติพื้นฐานด้านความปลอดภัยมาใช้ เช่น หลักการ Zero Trust, การยืนยันตัวตนโดยใช้หลายปัจจัย, การตรวจจับเหตุการณ์ด้านความมั่นคงปลอดภัยและภัยคุกคามพร้อมทำการตอบสนอง (XDR), การอัปเดตระบบอยู่เสมอ และการปกป้องข้อมูล[1]

Lenovo นำเสนออุปกรณ์ต่างๆ ที่หลากหลายซึ่งขับเคลื่อนด้วยโปรเซสเซอร์ Intel® Core™ Ultra และ Windows 11 Pro ที่มาพร้อมฟีเจอร์ที่ช่วยทำให้พื้นฐานด้านความปลอดภัยสำหรับแผนก IT ของโรงเรียนง่ายขึ้น โดยทำผ่านการรักษาความปลอดภัยระดับฮาร์ดแวร์จาก Intel® และเพิ่มความสามารถขั้นสูง เช่น Copilot* ใน Windows พร้อมการปกป้องข้อมูลเชิงพาณิชย์เพื่อเพิ่มความสามารถในการปรับตัวต่อการเปลี่ยนแปลง นับเป็นรากฐานที่สมบูรณ์แบบสำหรับกลยุทธ์ด้านความปลอดภัยทางไซเบอร์สมัยใหม่ในเรื่องการศึกษา

ก้าวนำภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไปโดยการทำให้แน่ใจว่าระบบของท่านได้รับการสนับสนุนและอัปเดตอย่างต่อเนื่อง วิธีง่ายๆ ในการดำเนินการดังกล่าวคือเปลี่ยนไปใช้ Windows 11 กับ Lenovo ตอนนี้ ก่อนที่ Windows 10 จะสิ้นสุดการให้บริการในเดือน **ตุลาคม 2025** ด้วยอุปกรณ์ที่ล้ำสมัยของเรา เช่น ThinkPad series ที่ทำงานบนอุปกรณ์ที่ใช้โปรเซสเซอร์ Intel® Core™ Ultra ท่านจึงสามารถรับประโยชน์จากข้อได้เปรียบของ Windows 11 ได้ในทันที Windows 11 คือ Windows ที่ปลอดภัยที่สุดเท่าที่เคยมีมา ซึ่งมอบการปกป้องที่ทรงพลังโดยทำงานร่วมกับซอฟต์แวร์ไปจนถึงความปลอดภัยตั้งแต่ระดับซิลิคอนจาก Intel® และ ThinkShield ที่ครอบคลุม เพื่อมอบความได้เปรียบให้กับฝ่าย IT ของโรงเรียน

เพิ่มเติมกับการอัพเกรดที่ง่ายดายและสิทธิประโยชน์มากมายสำหรับโรงเรียน K-12 ด้วยอุปกรณ์ของ Lenovo ที่ทำงานบนโปรเซสเซอร์ Intel® Core™ Ultra และ Windows 11 Pro

- สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ลดลง **58%**[4]
- ความเสี่ยงของการโจมตีที่สำเร็จลดลง **20%**[5]
- การโจมตีเฟิร์มแวร์น้อยลง **3.1 เท่า**[4]

Intel® Core™ Ultra 7 processor powering Intel vPro®

Smarter technology for all

Lenovo

การป้องกันเชิงรุกอัจฉริยะ

Windows 11 ถูกสร้างขึ้นด้วยการป้องกันแบบหลายชั้น หลายอย่างถูกเปิดใช้งานตามค่าเริ่มต้น ดังนั้นเจ้าหน้าที่ของโรงเรียนจึงไม่จำเป็นต้องกังวลเกี่ยวกับการตั้งค่าความปลอดภัย ส่วนประกอบฮาร์ดแวร์และซอฟต์แวร์จาก Lenovo, Intel® และ Microsoft ทำงานร่วมกันเพื่อปกป้องอุปกรณ์และข้อมูลส่วนบุคคลที่มีความอ่อนไหว ซึ่งช่วยเพิ่มประสิทธิภาพการดำเนินงานด้าน IT ตามข้อเท็จจริงแล้ว **โรงเรียน K-12 49% ที่ใช้อุปกรณ์ Microsoft Windows รายงานว่าค่าใช้จ่ายเกี่ยวกับความช่วยเหลือและแก้ปัญหาด้าน IT และค่าบำรุงรักษาลดลง**[6]

เลเยอร์ต่างๆ บนเลเยอร์ด้านความปลอดภัย

คลาวด์
- การปกป้องข้อมูลโรงเรียน
- การปกป้องข้อมูลของนักเรียนและเจ้าหน้าที่

แอปพลิเคชัน
- การควบคุมแอปพลิเคชันและไดรเวอร์
- การแยกแอปพลิเคชัน

ฮาร์ดแวร์ (ชิป)
- รากแห่งความเชื่อถือ (root of trust) ของฮาร์ดแวร์
- ความปลอดภัยที่ถูกสร้างไว้ในระดับซิลิคอน

อัตลักษณ์
- การเข้าสู่ระบบโดยไม่ต้องใช้รหัสผ่าน
- การปกป้องข้อมูลผู้ใช้และรหัสผ่านขั้นสูง
- ความเป็นส่วนตัว

ระบบปฏิบัติการ
- การเข้ารหัสและการปกป้องข้อมูล
- ความปลอดภัยเครือข่าย
- การป้องกันไวรัสและภัยคุกคาม
- ระบบรักษาความปลอดภัย

intel CORE ULTRA 7 | intel vPRO

Intel® Core™ Ultra 7 processor powering Intel vPro®

Smarter technology for all

Lenovo

การรับมือกับภัยคุกคามที่ใหญ่ที่สุด

74% ของช่องโหว่ทั้งหมดเกิดจากความผิดพลาดของมนุษย์, การใช้สิทธิพิเศษในทางที่ผิด, การขโมยข้อมูลผู้ใช้และรหัสผ่าน และการโจมตีด้วยเทคนิคทางจิตวิทยา ซึ่งทำให้นักเรียนและเจ้าหน้าที่กลายเป็นเป้าหมายหลักในการฟิชชิ่ง การขโมยข้อมูลผู้ใช้และรหัสผ่านเป็นช่องทางการโจมตีที่พบได้บ่อยที่สุด คิดเป็น 50%[7]

Lenovo ใช้แนวทางที่ครอบคลุมสำหรับการรักษาความปลอดภัยที่เสนอการเฝ้าระวังแบบใหม่ในปัจจุบันและเตรียมโรงเรียนให้พร้อมสำหรับอนาคตที่ปลอดภัย อุปกรณ์ที่เชื่อถือได้ของเราซึ่งขับเคลื่อนด้วยโปรเซสเซอร์ Intel® Core™ Ultra และ Windows 11 Pro มาพร้อมฟีเจอร์การป้องกันของ ThinkShield, การตรวจจับ และการแจ้งเตือนการโจมตีในระดับ BIOS เพื่อปกป้องเฟิร์มแวร์และฮาร์ดแวร์ โซลูชัน Zero Trust Supply Chain ของ Lenovo ช่วยปกป้องไม่ให้เกิดการปลอมแปลงจากโรงงาน

Windows 11 มี security profile ที่ครอบคลุมและรองรับ Zero Trust ซึ่งประกอบด้วยการป้องกันแอปพลิเคชันที่จำเป็นต่อการอยู่รอดของธุรกิจ, Windows Firewall และ kernel ความปลอดภัยที่ถูกสร้างไว้ในระดับซิลิคอนเพื่อลดภัยคุกคามดังกล่าว และปกป้องอุปกรณ์ทั้งหมดในสถานศึกษา K-12 ของท่าน

เปลี่ยนไปใช้ Windows 11 งายๆ กับ Lenovo

ถึงเวลาแล้วที่จะเปลี่ยนไปอยู่ในสภาพแวดล้อมที่ปลอดภัยและเอื้ออำนวยมากขึ้น ไม่ว่าจะเป็นการย้ายข้อมูลแบบมาตรฐานหรือแบบที่ซับซ้อนกว่า Lenovo ก็มีความเชี่ยวชาญ, ประสบการณ์ และข้อเสนอบริการที่จะทำให้การเปลี่ยนแปลงนี้เป็นไปอย่างราบรื่นและปลอดภัยสำหรับท่าน

เริ่มที่ Lenovo Assessment Service สำหรับ Windows 11
ผู้เชี่ยวชาญของ Microsoft จะกำหนดขนาดและขอบเขตของการย้ายข้อมูลของท่านโดยตรวจสอบให้แน่ใจว่าท่านมีคุณสมบัติตรงตามเงื่อนไขเบื้องต้น, ระบุปัญหาที่อาจเกิดขึ้น และวางแผนเหตุการณ์สำคัญเพื่อให้แน่ใจว่าการย้ายข้อมูลจะราบรื่น ซึ่งช่วยลดความเสี่ยงและระยะเวลาที่อุปกรณ์ขัดข้อง

ได้รับการปกป้องตั้งแต่ซิลิคอนไปจนถึงซอฟต์แวร์

โปรเซสเซอร์ของ Intel® มีความปลอดภัยในระดับคอร์ ซึ่งออกแบบมาให้รับมือกับความท้าทายเฉพาะที่เน้นประเด็นสำคัญ 3 ประการ ได้แก่

- ความปลอดภัยพื้นฐาน: การป้องกันที่สำคัญเพื่อช่วยตรวจสอบความน่าเชื่อถือของอุปกรณ์และข้อมูล
- เวิร์คโหลดและการปกป้องข้อมูล: การดำเนินการที่เชื่อถือได้สำหรับการปกป้องข้อมูลที่แยกด้วยฮาร์ดแวร์
- ความน่าเชื่อถือของซอฟต์แวร์: แพลตฟอร์มที่ช่วยปกป้องจากภัยคุกคามทางไซเบอร์ต่างๆ

การรักษาความปลอดภัยที่ใช้ AI

ปัญญาประดิษฐ์กำลังเปลี่ยนแปลงความมั่นคงปลอดภัยทางไซเบอร์ โดยทำให้การตรวจจับ, การตอบสนอง, การวิเคราะห์ และการคาดการณ์ภัยคุกคามมีความเป็นระบบอัตโนมัติและดียิ่งขึ้น อย่างไรก็ตาม มีความเสี่ยงด้านการปฏิบัติตามกฎหมาย, ความเป็นส่วนตัว และอื่นๆ อีกมากมาย หากการปรับใช้ AI เป็นไปอย่างเร่งรีบ แนวทางที่ผ่านการวิจัยมาอย่างดี ซึ่งอาจรวมไปถึงโปรแกรมการจัดการความน่าเชื่อถือ, ความเสี่ยง และความปลอดภัย (TRiSM) สามารถผสมผสานกับการกำกับดูแลตั้งแต่เริ่มต้นและช่วยให้โรงเรียนประสบความสำเร็จได้

* ช่วงเวลาในการส่งมอบฟีเจอร์และความพร้อมใช้งานอาจแตกต่างกันไปตามตลาดและอุปกรณ์ ใช้ Copilot กับบัญชี Microsoft หรือใช้ Copilot กับการปกป้องข้อมูลเชิงพาณิชย์โดยไม่มีค่าใช้จ่ายเพิ่มเติมโดยการลงชื่อเข้าใช้บัญชีที่ทำงานหรือโรงเรียน (Microsoft Entra ID) ด้วย Microsoft 365 E3, E5, F3, A3 หรือ A5 สำหรับคุณาจารย์, Business Premium และ Business Standard ในอนาคตผู้ใช้ Entra ID จะสามารถใช้งานได้มากขึ้น

** จำเป็นต้องมี Microsoft Intune และ Azure Active Directory (ปัจจุบันเรียกว่า Microsoft Entra ID) ซึ่งจำหน่ายแยกต่างหาก

ที่มา

1 Microsoft, “Digital Defense Report,” ตุลาคม 2023
2 SonicWall, “2024 SonicWall Cyber Threat Report,” 2024
3 Cybercrime, “Cyberwarfare In The C-Suite,” พฤศจิกายน 2020
4 Windows 11 results are in comparison with Windows 10 devices. Techaisle, “Windows 11 Survey Report,” กุมภาพันธ์ 2022
5 จำเป็นต้องมี Microsoft Intune และ Azure Active Directory ซึ่งจำหน่ายแยกต่างหาก
6 Commissioned study delivered by Forrester Consulting, “The Total Economic Impact™ of Microsoft Windows Devices For K-12 Education,” กรกฎาคม 2023
7 Verizon, “2023 Data Breach Investigations Report,” 2023

intel CORE ULTRA 7 | intel vPRO

Intel® Core™ Ultra 7 processor powering Intel vPro®

Smarter technology for all

Lenovo

9 ขั้นตอนสู่ความยืดหยุ่นด้านความปลอดภัยในการศึกษาระดับ K-12

นี่คือแผนปฏิบัติการสำหรับการวางแผนความมั่นคงปลอดภัยทางไซเบอร์เชิงกลยุทธ์ของท่าน

- ☐ **1. เริ่มเปลี่ยนไปใช้ Windows 11 เลย** ตรวจสอบให้แน่ใจว่าโครงสร้างพื้นฐานด้าน IT ของโรงเรียนทานมีความปลอดภัยและทันสมัยโดยเปลี่ยนไปใช้ Windows 11 ก่อนที่การสนับสนุน Windows 10 จะสิ้นสุดลงในวันที่ 14 ตุลาคม 2025 การนำมาใช้ตั้งแต่เนิ่นๆ จะช่วยให้โรงเรียนของทานได้รับประโยชน์จากฟีเจอร์และนวัตกรรมด้านความปลอดภัยล่าสุดได้ทันที
- ☐ **2. ใช้การยืนยันตัวตนแบบไม่ใช้รหัสผ่าน** ให้ครู, เจ้าหน้าที่ และนักเรียนทุกคนเปลี่ยนไปใช้การยืนยันตัวตนแบบไม่ใช้รหัสผ่าน เช่น รหัส PIN, ลายนิ้วมือ หรือการจดจำใบหน้า วิธีนี้จะช่วยลดความเสี่ยงของการโจรกรรมข้อมูลส่วนตัวได้มาก และทำให้การเข้าสู่ระบบง่ายและปลอดภัยยิ่งขึ้นสำหรับผู้ใช้งาน
- ☐ **3. พัฒนาหลักสูตรการศึกษาด้านความมั่นคงปลอดภัยทางไซเบอร์** ให้ความรู้แก่นักเรียน, ครู และเจ้าหน้าที่เกี่ยวกับแนวปฏิบัติพื้นฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ และความสำคัญของการรักษาพฤติกรรมออนไลน์ที่ปลอดภัย การฝึกอบรมเป็นประจำสามารถลดโอกาสเกิดข้อผิดพลาดที่เกิดจากมนุษย์ซึ่งนำไปสู่ช่องโหว่ด้านความปลอดภัยได้
- ☐ **4. จัดลำดับความสำคัญของการอัปเดตเรื่องความปลอดภัยที่จำเป็น** ตรวจสอบให้แน่ใจว่าอุปกรณ์และระบบทั้งหมดของโรงเรียนได้รับการอัปเดตด้วยแพตช์ความปลอดภัยล่าสุดเป็นประจำ ซึ่งจะช่วยปกป้องจากช่องโหว่ที่ถูกรายงานและเผยแพร่ไว้เป็นสาธารณะแล้ว และทำให้สภาพแวดล้อมด้าน IT ของทานมีความยืดหยุ่นต่อภัยคุกคามใหม่ๆ
- ☐ **5. ใช้ประโยชน์จาก AI ในการตรวจจับภัยคุกคาม** ใช้โซลูชันความปลอดภัยที่ขับเคลื่อนด้วย AI ในการตรวจจับ, ตอบสนอง และวิเคราะห์ภัยคุกคามแบบอัตโนมัติให้ดียิ่งขึ้น ซึ่งช่วยให้ฝ่าย IT ของทานจัดการเรื่องความปลอดภัยได้อย่างมีประสิทธิภาพมากขึ้นและโฟกัสที่มาตรการเชิงรุกได้
- ☐ **6. ปฏิบัติตามหลักการ Zero Trust** นำเอาโมเดลด้านความปลอดภัยแบบ Zero Trust มาใช้เพื่อให้มั่นใจว่าผู้ใช้, อุปกรณ์ และแอปพลิเคชันทั้งหมดได้รับการตรวจสอบอย่างต่อเนื่องก่อนที่จะให้สิทธิ์การเข้าถึง ซึ่งจะช่วยปกป้องข้อมูลสำคัญและระบบต่างๆ จากการเข้าถึงโดยไม่ได้รับอนุญาต
- ☐ **7. ร่วมมือกับพันธมิตรที่เชื่อถือได้** ทำงานร่วมกับพันธมิตรด้านเทคโนโลยีที่เชื่อถือได้เพื่อผสานรวมโซลูชันฮาร์ดแวร์และซอฟต์แวร์ที่ได้รับการพิสูจน์แล้วว่าทำงานร่วมกันได้อย่างราบรื่น ซึ่งช่วยให้มั่นใจได้ว่าจะมีกลยุทธ์ด้านความปลอดภัยที่สอดประสานกันและครอบคลุมทุกด้านของโครงสร้างพื้นฐานด้าน IT ของทาน
- ☐ **8. จัดทำแผนการตอบสนองภัยคุกคามกรณีเกิดสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์** พัฒนาและอัปเดตแผนการตอบสนองภัยคุกคามเป็นประจำ เพื่อให้จัดการปัญหาช่องโหว่ด้านความปลอดภัยได้อย่างรวดเร็วและมีประสิทธิภาพ การมีโปรโตคอลที่ชัดเจนช่วยลดความเสียหายและฟื้นตัวจากการโจมตีที่อาจเกิดขึ้นได้อย่างรวดเร็ว
- ☐ **9. ประเมินและจัดการความเสี่ยงในการใช้งาน AI** ก่อนที่จะนำแอปพลิเคชัน AI ไปใช้ในวงกว้าง ควรประเมินความเสี่ยงและประโยชน์ที่เกี่ยวข้อง พิจารณาใช้โปรแกรมการจัดการความน่าเชื่อถือ, ความเสี่ยง และความปลอดภัย (TRiSM) เพื่อให้มั่นใจว่าการใช้งาน AI เชื่อถือได้และปลอดภัย

Lenovo สามารถช่วยให้การเปลี่ยนไปใช้ Windows 11 ทั่วทั้งสถานศึกษา K-12 ของทานเป็นไปอย่างง่ายดายและประสบความสำเร็จ

เรียนรู้เพิ่มเติมได้ที่ **techtoday.lenovo.com/windows-11**

intel CORE ULTRA 7 | intel vPRO

Intel® Core™ Ultra 7 processor powering Intel vPro®

Smarter technology for all

Lenovo