การป้องกันภัยคุกคามแบบครบวงจรโดย Morphisec

การปกป้องภัยคุกคามที่ไม่เคยพบเห็นมาก่อนด้วยวิธีการป้องกันในรูปแบบเปลี่ยนกลุ่มเป้าหมายเป็นแบบเคลื่อนที่

Morphisec ปกป้องธุรกิจของคุณจากช่องโหว่ของ application, zero day attack และภัยคุกคามตัวฉกาจที่สามารถหลบหลีกได้ด้วยการป้องกันในรูปแบบเปลี่ยนกลุ่มเป้าหมายเป็นแบบเคลื่อนที่ Morphisec ทำงานอยู่เบื้องหลังเพื่อปกป้อง application และ web browser ของคุณรวมถึงป้องกันการพยายามเข้าถึงต่างๆ คุณจะได้รับการปกป้องที่ทรงพลังซึ่งใช้งานง่าย, และเฉียบขาด

การปิดช่องโหว่ความปลอดภัย

ภัยคุกคามที่ผู้โจมตีได้ปล่อย malware ออกมาหลายล้านตัวในแต่ละปี ล้วนมีความเฉลียวฉลาดมากกว่าที่เคย มีวิธีการโจมตีหลากหลายรูปแบบและสามารถทนทานการโจมตีต่อ Anti virus ได้เป็นอย่างดี โดยรูปแบบการโจมตีที่เกิดขึ้น มีการเปลี่ยนแปลงไปอย่างรวดเร็วเกินกว่าที่วิธีการป้องกันในรูปแบบที่ขึ้นอยู่กับ signature หรือการใช้พฤติกรรมบ่งชี้ หรือแม้แต่รูปแบบการดักจับภัยคุกคามโดยใช้เทคโนโลยี AI, ML ที่สามารถจับได้เร็วกว่า จะสามารถตามทันการโจมตีในรูปแบบใหม่ได้ ในด้านการทำลายล้างของ malware ผู้โจมตีได้ใช้ความรู้ในเชิงลึกเกี่ยวกับสภาพแวดล้อมเป้าหมายเพื่อพัฒนาการโจมตี การกำหนดเป้าหมายขั้นสูง ใช้ความหลากหลายรูปแบบในการทำงาน การทำให้เกิดความสับสน เข้ารหัสและเทคนิคขั้นสูงอื่น ๆ เพื่อหลีกเลี่ยงกลไกความไม่ปลอดภัย แต่ Morphisec สามารถก้าวข้ามผ่านวิธีการโจมตีในรูปแบบที่ได้กล่าวมาขั้นต้นได้ด้วยวิธีการอย่างชาญฉลาดในรูปแบบของ Morphisec เสมอ

การลดความเสี่ยงและค่าใช้จ่าย

Morphisec สามารถป้องกันได้อย่างแท้จริงก่อนที่ malware พยายามจะเข้ามาในระบบด้วยวิธีการป้องกันกลุ่มเป้าหมายแบบเคลื่อนที่ หากลองเปรียบเทียบกับวิธีการแก้ไขอื่นๆ จะเห็นว่ามีการใช้เทคโนโลยีในการดักจับที่หลากหลาย แต่วิธีการดังกล่าว จะต้องมีการระบุตัวตนก่อน จากนั้นจึงระงับการโจมตี แต่ Morphisec จะหยุดการโจมตีในขั้นตอนแรกก่อน จากนั้นจึงค่อยระบุประเภทการโจมตีในลำดับต่อมา โดยไม่ต้องเดาแบบสุ่มเสี่ยง Morphisec สามารถโจมตีแบบไม่พลาดเป้าหมาย ไม่ทำให้เกิดความเสียหาย Morphisec สามารถควบคุมการรุกราน การตรวจจับ Malware และการโจมตีแบบไม่มีการจัดการล่วงหน้า โดยไม่ต้องพึ่งพา IOCs ก่อนที่ความเสียหายจะเกิดขึ้น โดยวิธีการของ Morphisec สามารถปรับใช้ไปยังโครงสร้างพื้นฐานความปลอดภัยที่มีอยู่อย่างง่ายดาย และไม่มีการแจ้งเตือนที่ผิดพลาด

Morphisec ถูกสร้างขึ้นเพื่อระงับการโจมตีแบบ Fileless

Morphisec ถูกสร้างขึ้นเพื่อระงับการโจมตีแบบ Fileless (การโจมตีในหน่วยความจำที่พยายามหลีกเลี่ยงการตรวจจับจากทรัพยากรของเครื่องคอมพิวเตอร์โดยชอบด้วยกฎหมาย) โดย malware ชนิดนี้ มีแนวโน้มถึง 10 เท่าที่จะโจมตีองค์กรมากกว่า malware ชนิดอื่น แต่ Morphisec สามารถป้องกันการโจมตีดังกล่าวล่วงหน้า ด้วยการทำให้ภัยร้ายเหล่านี้ไม่สามารถเข้าถึงได้

ป้องกันการโจมตีได้ตั้งแต่ระยะขั้นต้น

การป้องกันภัยคุกคามเชิงรุกของ Morphisec สามารถช่วยป้องกันภัยคุกคามทั้งที่เป็นที่รู้จัก (known attack) และไม่รู้จัก (unknown attack) ได้ตั้งแต่ระยะต้นของวัฏจักรการโจมตี

- ป้องกันภัยคุกคามขั้นสูงและช่องโหว่ทันทีและครบถ้วน ไม่มีการตรวจจับแบบเดาสุ่มหรือตามล่าหาการโจมตีที่ไม่ใช่เป้าหมาย
- ตั้งค่าและลืมไปได้เลย เป็นระบบที่ทำงานแบบไม่รบกวนผู้ใช้งาน ไม่ลดประสิทธิภาพการทำงาน และไม่จำเป็นต้องอัพเดต signature ใดๆ เพราะ Morphisec ไม่ใช่ solution ในการสแกน
- ลดความผิดพลาดในการแจ้งเตือน (False Positive) ไม่มีการแจ้งเตือนเสียเปล่าหรือสิ้นเปลืองทรัพยากรในการโจมตีที่ไม่มีทางไม่เกิดขึ้น

ความปลอดภัยที่ทำให้ IT บริหารงานง่ายขึ้น

ลดความเสี่ยงด้านความปลอดภัยในการบริหารงานหรือเป็นการเพิ่มประสิทธิภาพธุรกิจให้ดียิ่งขึ้น Morphisec ถูกสร้างและออกแบบจากพื้นฐานความต้องการของผู้ใช้งาน เพื่อให้สอดคล้องกับความต้องการทางธุรกิจและตอบโจทย์ด้านความปลอดภัย

- ป้องกันภัยคุกคาม โดยไม่ต้องตรวจสอบตลอดเวลา หรือผลิตข้อมูลเอกสารออกมาจำนวนมาก
- ลดความซับซ้อนด้าน IT และปกป้องการทำธุรกิจให้ดำเนินไปได้อย่างต่อเนื่อง
- สามารถทำ Virtual Patching ให้ Windows 7 ได้ แทนระบบของความปลอดภัยของ Microsoft เนื่องจาก Window 7 ได้ End of Life ไปแล้ว
- สามารถมองเห็นวิถีการโจมตีอุปกรณ์ endpoint ทั้งหมด รวมถึงข้อมูลการดักจับ Malware โดย Window Defender AV
- ดู Timeline การโจมตีแบบครบถ้วน รวมถึงเหตุการณ์ที่เชื่อมโยงความสัมพันธ์กันเพื่อทำให้การทำงานทรงประสิทธิภาพมากขึ้นและสามารถตัดสินใจได้รวดเร็วขึ้น
- ปรับใช้ได้งานได้บนสิ่งแวดล้อมแบบ virtual, physical หรือ hybrid

MORPHISEC
Moving Target Defense

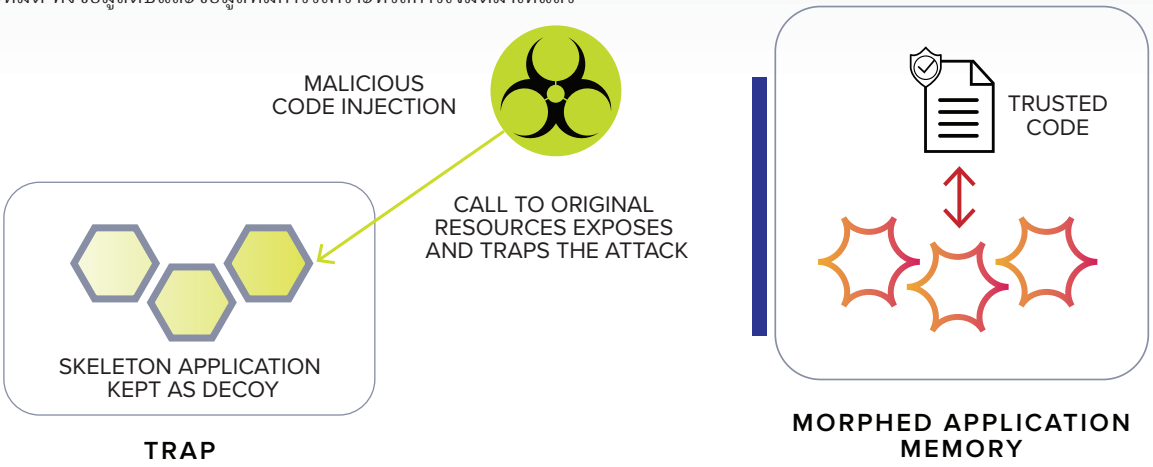
การป้องกันกลุ่มเป้าหมายแบบเคลื่อนที่

การป้องกันกลุ่มเป้าหมายแบบเคลื่อนที่ เป็นกลยุทธ์การป้องกันการโจมตีตั้งแต่ระยะเริ่มต้น โดยใช้วิธีการโจมตีแบบเดียวกันกับผู้โจมตี เช่น การหลอกล่อ ทำให้สับสน การปรับเปลี่ยนรูปแบบและความหลากหลายของรูปแบบ การป้องกันภัยคุกคามแบบครบวงจรของ Morphisec เป็นเพียงแพลตฟอร์มการป้องกันอุปกรณ์ปลายทางเดียวเท่านั้น ที่ใช้เทคโนโลยีขั้นสูงที่มีความสลับซับซ้อน โดยวิธีการของ Morphisec จะใช้วิธีการเคลื่อนที่แบบสุ่มและเปลี่ยนแปลงรูปแบบทรัพยากรหน่วยความจำซึ่งเป็นเป้าหมายหลักของการถูกโจมตีขั้นสูงอย่างต่อเนื่อง วิธีนี้จะทำลายกลไกระบบการโจมตีและขั้นตอนการเจาะระบบเพื่อโจมตีเป้าหมาย เพื่อป้องกันการคุกคามได้ทันทีและอย่างไม่มีเงื่อนไข

Morphisec สามารถปกป้องอุปกรณ์ปลายทาง (endpoint) ได้จากการโจมตีผ่านช่องโหว่ ทั้งที่รู้จักและไม่รู้จัก รวมถึงการโจมตีผ่านทางหน่วยความจำใน application ต่างๆ เช่น browserนอกจากนี้ Morphisec ยังสามารถป้องกันการโจมตีที่มีความชำนาญด้านการหลบเลี่ยง (evasive attacks), การโจมตีแบบใหม่ที่ยังไม่มีการป้องกัน (zero -days attacks) และการโจมตีไปที่เป้าหมายที่มีช่องโหว่แต่ยังไม่มีการอัพเดท Security Patch ซึ่ง Morphisec สามารถทำงานได้อย่างแม่นยำ โดยไม่มีความจำเป็นต้องวิเคราะห์ alert ที่เกิดขึ้น เพียงทำงานผ่าน agent ที่มีขนาด 2 MB ซึ่งมีขนาดเล็กและไม่จำเป็นต้องมีการดูแลระบบใดๆ

วิธีการทำงาน

1. **ปรับเปลี่ยนและปกปิด: เปลี่ยนเป้าหมายเดิมให้เป็นเป้าหมายที่ไม่สามารถคาดเดาได้**
   เมื่อ applicationโหลดไปยังพื้นที่หน่วยความจำ Morphisec จะปรับโครงสร้างกระบวนการย้าย และเปลี่ยนไลบรารีฟังก์ชันตัวแปรและส่วนข้อมูลอื่น ๆ ในลักษณะที่ควบคุมได้ การดำเนินการแต่ละครั้งไม่ซ้ำกันตามแต่ละกระบวนการทำให้หน่วยความจำไม่สามารถคาดการณ์ได้จากการโจมตี
2. **ปกป้องและสร้างกับดัก: การเข้าถึงโครงสร้างที่มีการปรับเปลี่ยน**
   DLL ของ Application ที่ชอบด้วยกฎหมาย จะได้รับการอัพเดทตลอดเวลา โดยที่ Application ยังคงสามารถโหลดและรันได้ตามปกติ และชิ้นส่วนโครงสร้างหน่วยความจำของจริงจะถูกทิ้งไว้ให้เป็นกับดัก
3. **ป้องกันและเผยโฉมภัยคุกคาม : รักษาสถานภาพของอุปกรณ์ endpoint และเปิดเผยการโจมตี**
   การโจมตีหน่วยความจำของจริงจะไม่มีทางเกิดขึ้น เพราะไม่สามารถเข้าถึงสิ่งที่ตัวคุกคามคาดหวังและต้องการเพื่อดำเนินการต่อได้ การโจมตีจะได้รับการป้องกันในทันที และตามด้วยการดักจับตัวคุกคาม และบันทึกรายละเอียดวิถีการโจมตีทั้งหมด ทั้งข้อมูลดิบและข้อมูลที่มีการวิเคราะห์วิถีการโจมตีมาให้แล้ว



ประโยชน์ที่ได้รับ

ระงับการโจมตีที่มีความสลับซับซ้อน (unknown threats)
ป้องกันการโจมตีหน่วยความจำ เช่น zero-days attack, fileless memory, เอกสารที่เป็นอันตรายและภัยคุกคามบน browserในระยะเสี้ยววินาที

กลไกจัดการป้องกันความเสียหายอย่างเด็ดขาด
ช่วยให้ธุรกิจของคุณได้รับการปกป้องจากช่องโหว่แม้ขณะที่ Security Patch ของระบบยังไม่พร้อมใช้งานี

ลดค่าใช้จ่ายในการดำเนินงานด้านความปลอดภัย
ไม่จำเป็นต้องตรวจสอบหรือวิเคราะห์ไม่มีการแจ้งเตือนผลลัพธ์ที่ผิดพลาด ซึ่งทำให้มีค่าใช้จ่ายเพิ่มขึ้น

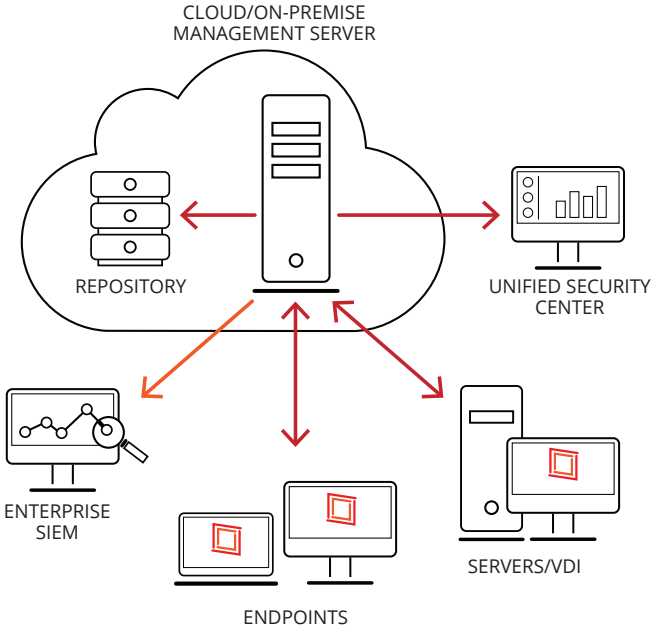
สามารถเห็นเหตุการณ์ตั้งแต่เริ่มมีการโจมตีจนสิ้นสุดการโจมตี
ตรวจสอบวิถีการโจมตีได้ทุกอุปกรณ์ endpoint ตั้งแต่ต้นจนจบ

การควบคุมการทดแทนระบบ
การควบคุมการทดแทนในระบบ Windows 7 เพื่อชดเชยการควบคุมตามวัตถุประสงค์

ง่ายต่อการบริหาร
สามารถปกป้องได้ในขณะที่มีการ offline และติดตั้งได้อย่างรวดเร็ว โดยไม่ต้องมีการจัดการ ดังนั้นจึงไม่ได้ส่งผลต่อการทำงานในการใช้ CPUในการประมวลผล

โครงสร้างพื้นฐานในส่วนของวิธีการทำงาน

Morphisec Endpoint Threat Prevention เป็น Windows Service Application ที่สร้างขึ้นบนสถาปัตยกรรมระดับสูง สามารถรองรับการใช้งานได้กับองค์กรทุกขนาด ไม่ว่าจะเป็นองค์กรเดียวหรือองค์กรที่มีหลายสาขา วิถีการโจมตีแบบเต็มรูปแบบจะถูกส่งไปยังหน่วยควบคุมการจัดการหรือ SIEM ขององค์กรเพื่อการวิเคราะห์วิถีการโจมตีแบบเต็มรูปแบบ โดยการสื่อสารในระบบทั้งหมดจะได้รับการเข้ารหัสและการเชื่อมต่อระหว่าง agent และ server ที่มีการยืนยันการเชื่อมต่อซึ่งกันและกันเป็นที่เรียบร้อยแล้ว



ส่วนประกอบสำคัญ

Server การจัดการ

Morphisec สามารถจัดการและติดตาม agent ของอุปกรณ์ endpoint ได้อย่างมีประสิทธิภาพ สามารถผสมผสานกับการทำงานกับ SIEM ขององค์กร และสามารถแสดงข้อมูลวิถีการโจมตีอย่างเต็มรูปแบบใน dashboard ได้

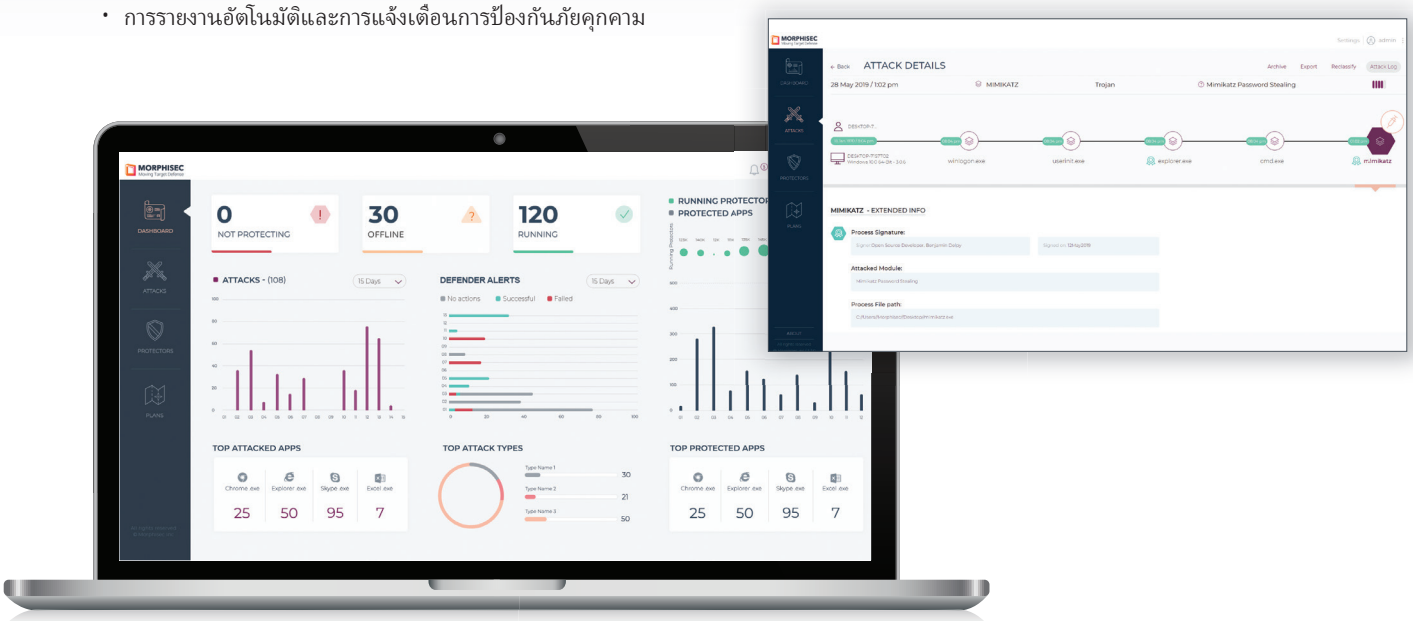
Unified Security Center

สามารถนำเสนอการควบคุมระบบได้อย่างสมบูรณ์และการมองเห็นวิถีการโจมตีแบบครบวงจรจนเสร็จสิ้นภารกิจการโจมตีผ่าน dashboard อย่างชัดเจน มีประสิทธิภาพและปรับแต่งได้อย่างเหมาะสม โดยรายละเอียดที่สามารถเห็นได้จาก dashboard ได้แก่

- จำนวนการถูกโจมตีและการป้องกันการโจมตีผ่านทางช่องโหว่ของ application และ KPIs ที่ผู้ใช้งานสามารถปรับแต่งได้
- มุมมองภาพรวมของการโจมตีทั้งหมดของอุปกรณ์ endpoint รวมถึงการดักจับของ Defender AV
- การจดจำลักษณะเฉพาะและการวิเคราะห์อย่างชาญฉลาดและเห็นภาพได้ในมุมมองเชิงลึก
- การรายงานอัตโนมัติและการแจ้งเตือนการป้องกันภัยคุกคาม

Agent

- ฟังค์ชั่นการป้ องกันทั้งหมดจะถูกดำเนินการอย่างอัตโนมัติโดย Agent ที่มี DLL ขนาด 2 MB
- ป้องกันการโจมตีโดยไม่รู้ล่วงหน้า – ไม่จำเป็นต้องอัพเดทลักษณะเฉพาะหรือฐานข้อมูล และไม่ต้องเรียนรู้อัลกอริทึมเพิ่มเติม
- ปกป้อง application ทั้งหมดของผู้ใช้งาน โดยไม่ต้องมีการกำหนดค่าที่น่าเบื่อ
- ไม่ส่งผลต่อการ runtime ส่วนประกอบใดๆและมีการสื่อสารที่ปลอดภัยกับ Unified Security Center เพื่อเป็นไปตามวัตถุประสงค์การรายงานและการติดตามเท่านั้น



เหมาะสำหรับองค์กรผู้ประกอบการและธุรกิจทุกขนาด

Morphisec สามารถปรับให้เข้ากับความต้องการทางธุรกิจขององค์กรทุกขนาด มีระบบปกป้องทรัพย์สินทางปัญญาและการออกแบบ โดยที่ไม่ขัดขวางการดำเนินงานของธุรกิจ คุณลักษณะที่สำคัญสำหรับองค์กร ได้แก่ การมองเห็นภัยคุกคามตลอดทั้งการโจมตี ความสามารถในการตรวจสอบ การรวม Active Directory และการทำงานร่วมกันกับระบบที่องค์กรใช้งาน เช่น SIEM เป็นต้น

ความสามารถในการป้องกันที่ไม่เหมือนใครของ Morphisec ไม่ได้ขึ้นอยู่กับข้อมูลลักษณะเฉพาะที่บันทึกไว้ ดังนั้นในบางธุรกิจที่มีทรัพยากรอย่างจำกัด จะได้รับการปกป้องในระดับเช่นเดียวกันกับองค์กรขนาดใหญ่ Morphisec ไม่ต้องการการบำรุงรักษารายวันหรือการตั้งค่าต่างๆ อีกทั้ง Morphisecไม่มีผลกระทบต่อประสิทธิภาพในเวลาทำงาน จึงสามารถกำจัดภัยคุกคามตามเป้าหมายที่ต้องการด้วยประสิทธิภาพระดับสูง ทำให้ภัยคุกคามไม่สามารถหลุดรอดไปได้ ด้วยวิธีการทำงานของ Morphisec อย่างรวดเร็ว

Morphisec สำหรับ VDI

Morphisec ไม่ได้ส่งผลต่อการประมวลผลของCPU และไม่ต้องการการอัพเดทเพื่อป้องกันภัยคุกคามใหม่ๆ ดังนั้นจึงไม่ลดประสิทธิภาพการทำงานของ VDI หรือส่งผลกระทบต่อเวลาการโหลด instance การป้องกันภัยคุกคาม Morphisec Unified Threat Prevention สามารถปกป้องได้ทั้งสภาพแวดล้อมที่เป็น virtual, physical และ hybrid อย่างไร้รอยต่อในส่วนประกอบที่สำคัญของ VDI นอกจากนี้ยังรองรับแพลตฟอร์ม application virtualization เช่น Citrix XenApp

ความร่วมมือและระบบการทำงานร่วมกันกับพันธมิตร

- **MISA partner:** Member of the Microsoft Intelligent Security Association, integration with Microsoft Defender ATP
- **CitrixReady partner:** Certified for the latest versions of Citrix XenApp and Citrix XenDesktop, and Citrix Azure
- **VMWare technology alliance partner:** VMWare Horizon
- **Opswat bronze partner:** Tested by Opswat for quality, false positives, and compatibility with over 1,000 devices from 40+ leading access control vendors
- **RSA Netwitness partner:** Certified interoperability with RSA Netwitness Integrations
- **SIEM Integrations:** McAfee Enterprise Security Manager, Splunk Enterprise Security, IBM QRadar, HP Arcsite, Rapid7 InsightIDR

ข้อมูลจำเพาะทางเทคนิคและข้อกำหนด

ENDPOINT PROTECTOR	
Hardware	Hardware recommended by Microsoft to run the software
Software	A physical or virtual image running the following: Microsoft Windows 7 (32-bit and 64-bit) with a Windows update that supports SHA-2; Microsoft Windows 7, Service Pack 1 (32-bit and 64-bit); Microsoft Windows 8, 8.1; Microsoft Windows 10; Microsoft Windows Server 2008 R2, 2012/2012 R2, 2016 In addition, the image must include Microsoft .net 4.0 or later.

MANAGEMENT SERVER	
Hardware	Intel 64-bit Pentium 2 CPU 4 core or 8 core hyper threading, Recommended RAM 16G **Disk size:** Recommended 1T, minimum 250G **Disk:** Recommended: Raid 5 with backup. Minimum: Raid 1
Software	A physical or virtual image running Microsoft Windows Server 2012 R2 or later.

ABOUT MORPHISEC

Morphisec has revolutionized endpoint protection with its Moving Target Defense technology, which instantly and deterministically stops the most dangerous and evasive attacks while allowing companies to cut operational costs. With a true prevention-first approach to stopping zero-days, with no false positives, Morphisec eliminates the complexity and burden for organizations struggling to respond to cyberattacks.

MORPHISEC
Moving Target Defense

www.morphisec.com