คู่มือปฏิบัติการเตรียมองค์กรให้พร้อมรับมือจากภัยคุกคามและการโจมตีจาก Ransomware ขั้นสูงสุด ด้วย NetBackup Isolated Recovery Environment (IRE)

สารบัญ

บทนำ

ปัจจุบันเป็นเรื่องปกติที่การโจมตีของมัลแวร์จะเข้าสู่อุปกรณ์หลักของคุณและรวมถึงอุปกรณ์สำรองข้อมูลของคุณด้วย ทำให้ลูกค้าเริ่มมีความกังวลเกี่ยวกับความน่าเชื่อถือและความเร็วในการกู้คืนจากการโจมตีของแรนซัมแวร์ หลังจากทำสถิติสูงสุดตลอดปี 2021 โดย SonicWall ถูกโจมตีด้วยแรนซัมแวร์ มากถึง 78.4 ล้านครั้งในเดือนมิถุนายน 2021 เพียงอย่างเดียว (มากกว่า 30 ครั้งต่อวินาที) SonicWall ยังรายงานว่ามีการโจมตีมากกว่า 623.3 ล้านทั่วโลก ยอดรวมนี้เพิ่มขึ้น 105% ในปี 2020 และมากกว่าสามเท่าของตัวเลขที่เห็นในปี 2019

Isolated Recovery Environment คืออะไร?

เพื่อเพิ่มความแข็งแรงของการปกป้องภัยแรนซัมแวร์ที่ได้รับการปรับปรุงให้ดีมากขึ้นจากเดิม สิ่งสำคัญคือต้องรักษาความปลอดภัยข้อมูลสำรองของคุณบนพื้นที่จัดเก็บที่ไม่สามารถแก้ไขได้ และรักษาสำเนาข้อมูลสำรองของคุณแบบแยกเดี่ยว ซึ่งเรียกอีกอย่างว่าสำเนาข้อมูลแบบแยกจากกัน (Air Gapped Copy) ซึ่งสภาพแวดล้อมการกู้คืนแบบแยกเดี่ยว (IRE) คือการปิดใช้งานของสำเนาสำรองข้อมูลแบบแยกจากกันโดยปิดการเชื่อมต่อเครือข่าย เพื่อเก็บสำเนาข้อมูลสำคัญของคุณอย่างปลอดภัย โดยมอบให้ผู้ดูแลระบบเป็นผู้จัดการและดึงสำเนาข้อมูลชุดใหม่มาเก็บรักษาทั้งหมดเองตามความต้องการ เพื่อกำจัดผลกระทบจากการโจมตีของแรนซัมแวร์

โซลูชั่นปกป้องภัยจากแรนซัมแวร์ขั้นสูงสุดด้วย NetBackup Isolated Recovery Environment

โซลูชั่นการแยกเครือข่ายแบบดั้งเดิมจะใช้วิธีการที่ทั่วไปเรียกว่า “การพุช” หรือการส่งสำเนาสำรองข้อมูลจากต้นทางไปยังเป้าหมายแบบอิสระ ทำให้ข้อมูลมีความปลอดภัยน้อยลงและยังมีความเสี่ยงที่จะรับภัยคุกคามจากแรนซัมแวร์ได้ ในทางตรงกันข้าม โมเดล "การดึง " จะดึงสำเนาสำรองข้อมูลจากแหล่งที่มาผ่านหน้าต่างเฉพาะตามที่กำหนดไว้ใน IRE และตั้งแต่ NBU เวอร์ชัน 10.1 เป็นต้นไป โซลูชั่น IRE ของ NetBackup จะเพิ่มประสิทธิภาพการเคลื่อนย้ายข้อมูลโดยนำเสนอโมเดลจำลองแบบดึง ซึ่งคำขอเพื่อส่งข้อมูลจะมาจากฝั่ง IRE เท่านั้น และเป็นการเชื่อมต่อแบบย้อนกลับของ MSDP เพื่อควบคุมการไหลของข้อมูลได้ดีขึ้นและรักษาความปลอดภัยให้กับทั้งสภาพแวดล้อมแบบลอจิคอลและฟิกสิคอล

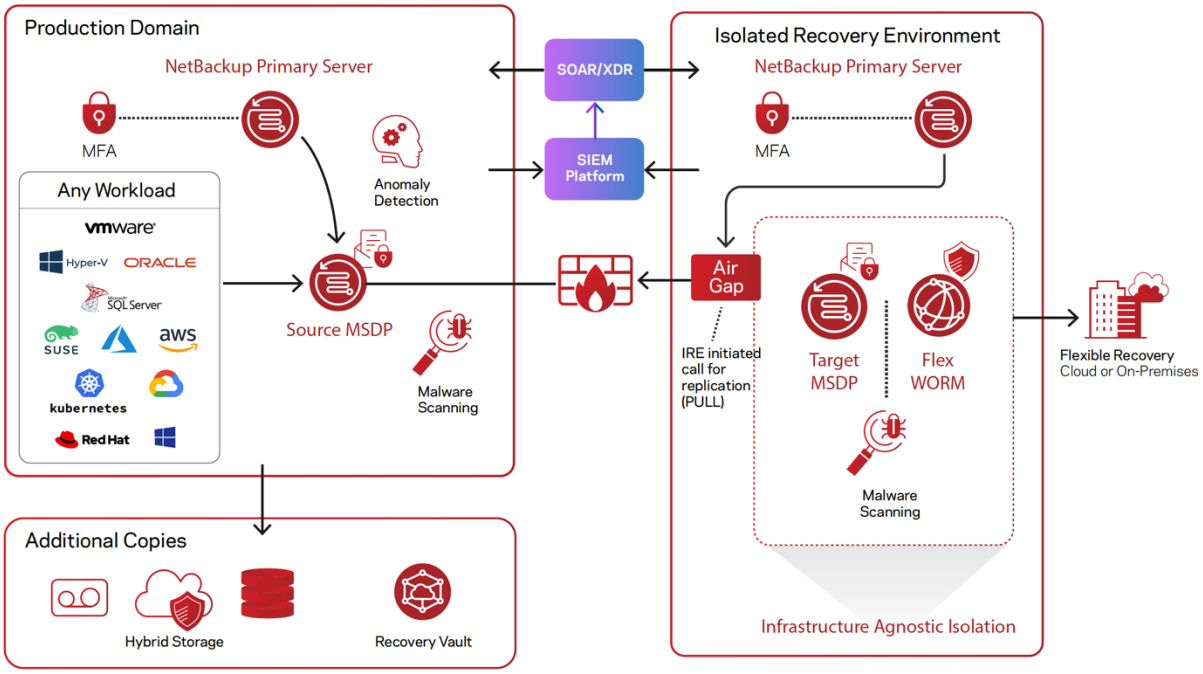
NetBackup Isolated Recovery Environment ช่วยลดภัยคุกคามจากแรนซัมแวร์ อย่างไร?

- จัดเก็บสำเนาข้อมูลที่ไม่สามารถแก้ไขหรือลบได้ ให้แยกออกจากกัน

- ตรวจจับแรนซัมแวร์ภายในข้อมูลที่ได้รับการป้องกันแล้ว เพื่อป้องกันการติดเชื้อซ้ำกรณีต้องการกู้คืนข้อมูล

-สามารถกู้คืนข้อมูลได้สำหรับทุกขนาดของข้อมูล ทำให้ธุรกิจดำเนินงานได้ตามที่กำหนดระดับบริการไว้ (SLA)

-มีกระบวนการกู้คืนข้อมูลที่คาดการณ์ได้ และสามารถทดสอบได้ทั้งบน on-premises หรือระบบคลาวด์ได้



ส่วนประกอบเพิ่มเติมที่ต้องพิจารณาด้วยสำหรับ IRE

โซลูชั่นการจัดเก็บข้อมูลระดับตติยภูมิ (สำเนาที่สาม) เป็นส่วนเสริมที่ยอดเยี่ยมสำหรับ IRE ซึ่งสอดคล้องกับอุดมคติของการสำรองข้อมูลหลายชุดที่จัดเก็บไว้ในหลายตำแหน่งแบบมาตรฐาน 3-2-1-1

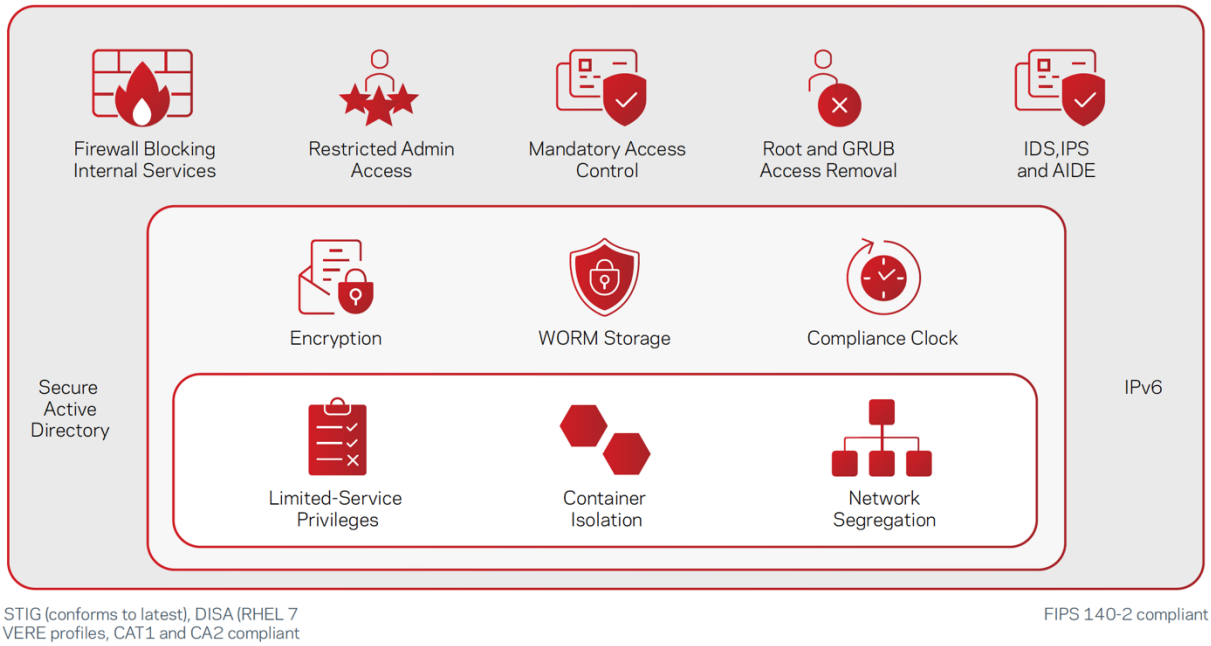
สำหรับความปลอดภัยของข้อมูลและการกู้คืนข้อมูลและความปลอดภัยของข้อมูล ให้พิจารณา NetBackup Recovery Vault เป็นการทำสำรองข้อมูลในระดับที่สาม ทำให้ลดความซ้ำซ้อนของข้อมูลและสร้างความปลอดภัยของข้อมูลได้เป็นอย่างดีในระบบคลาวด์

การเพิ่มระดับความปลอดภัยด้วย NetBackup Flex Appliance

NetBackup Flex Appliance ได้รับการออกแบบให้มีความปลอดภัยระดับแนวหน้าและมอบโซลูชั่นการจัดเก็บข้อมูลที่ไม่สามารถแก้ไขและลบได้อย่างสมบูรณ์เพื่อให้แน่ใจว่าระบบและข้อมูลของคุณสามารถกู้คืนได้

สถาปัตยกรรมของ Flex Appliance Zero Trust

สถาปัตยกรรมแบบ Zero-Trust ได้รับการออกแบบให้ใช้สิทธิ์ขั้นต่ำที่จำเป็นในการทำงานเฉพาะให้สำเร็จตามบทบาทและการอนุญาต รวมกับการให้สิทธิ์ผู้ใช้ที่แข็งแกร่งและการปกป้องข้อมูลตามนโยบาย สถาปัตยกรรม Zero-Trust ของ NetBackup Flex Appliances มอบแนวทางแพลตฟอร์มแบบง่ายๆหลายเลเยอร์แบบครบวงจรเพื่อผสานรวมการป้องกันอัจฉริยะ การตรวจจับที่ครอบคลุม และการสำรองและกู้คืนระดับแนวหน้าของอุตสาหกรรมได้อย่างราบรื่น สำหรับสถาปัตยกรรมแบบคอนเทนเนอร์ Flex นำเสนอการแยกหลายโดเมน การแยกเครือข่าย และสิทธิ์บริการแบบจำกัด นอกจากนี้ ด้วยพื้นที่เก็บข้อมูลแบบ WORM, การปิด-เปิด service บน OS ที่เป็นไปตามมาตรฐาน STIG, การเข้ารหัสข้อมูลตามมาตรฐาน FIPS 140-2 และการควบคุมการเข้าถึงความปลอดภัยที่ครอบคลุม NetBackup Flex Appliances มอบโซลูชันพื้นที่เก็บข้อมูลที่ไม่สามารถเปลี่ยนแปลงและไม่สามารถลบออกได้ เพื่อให้แน่ใจว่าระบบและข้อมูลของคุณปลอดภัยและสามารถกู้คืนได้ในยามจำเป็น



Vertias Appliance เป็นอุปกรณ์ปกป้องข้อมูลจากแรนซัมแวร์ และสามารถกู้คืนสำคัญทางธุรกิจได้ในทุกขนาดของข้อมูล โดยมี RPO และ RTO เกือบเป็นศูนย์ ประโยชน์ที่สำคัญบางประการรวมถึง :

-การบริหารจัดการด้านไอทีอย่างง่ายขึ้นด้วยที่จัดเก็บข้อมูลที่ไม่สามารถแก้ไขหรือลบได้

-สถาปัตยกรรมที่ปลอดภัยโดยค่าเริ่มต้น

-การกำหนดค่าระบบที่พร้อมใช้งานสูงแบบบูรณาการ

NetBackup และ Flex Appliance เป็นโซลูชั่นจัดเก็บข้อมูลแบบไม่สามารถแก้ไขหรือลบได้ เป็นไปตามข้อกำหนดการประเมินการไม่เปลี่ยนรูปของ Cohasset (ในโหมดการปฏิบัติตามข้อกำหนด):

-สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (SEC) ใน 17 CFR § 240.17a-4(f)

-หน่วยงานกำกับดูแลอุตสาหกรรมการเงิน (FINRA) กฎ 4511(c)

-Commodity Futures Trading Commission (CFTC) ตามข้อบังคับ 17 CFR § 1.31(c)-(d)

สามารถดูข้อมูลเพิ่มเติมได้ที่ **https://www.veritas.com/form/whitepaper/cohasset-associates-immutability-assessment-for-netbackup.**

NetBackup Flex IRE Architecture

โซลูชัน Veritas IRE มุ่งเน้นไปที่ 3 เสาหลัก ได้แก่ ปกป้อง ตรวจจับ และกู้คืน

การปกป้อง (Protect)

หลักการสำรองข้อมูลชุดที่หนึ่งจะถูกจัดเก็บไว้ในไซต์หลัก และสำเนาชุดที่สองจะถูกโอนย้ายนำไปเก็บไว้ที่สตรอเรจจัดเก็บแบบ WORM บนอุปกรณ์ Flex Appliance. ส่วน IRE จะเป็นการป้องกันอีกชั้นหนึ่งจากมัลแวร์โดยการแยกสำเนาชุดที่สองโอนย้ายไปเก็บยังสตรอเรจที่แก้ไขไม่ได้ (immutable storage) ในเครือข่ายอื่นที่แตกต่างกัน อาจจะเก็บไว้บน Flex Appliance อีกชุดที่แยกจากกัน และที่สำคัญ IRE ที่ใช้อุปกรณ์ Flex Appliance ชุดนี้จะมีการทำงานโดยปิดการเข้าถึงข้อมูลที่เก็บอยู่ในสตรอเรจที่แก้ไขไม่ได้นี้ และยังรวมถึงการรักษาความปลอดภัยหลายชั้นในตัวรวมถึง OS ที่แข็งแกร่ง (Hardened OS), สถาปัตยกรรมแบบ Zero trust คือป้องกันทุกอย่างเนื่องจากมีสมมุติฐานว่าไม่มีอะไรปลอดภัยร้อยเปอร์เซ็นต์

การตรวจจับ (Detect)

โซลูชั่น Veritas IRE ประกอบด้วยการตรวจจับสิ่งผิดปกติและการสแกนมัลแวร์ การตรวจจับความผิดปกติที่ขับเคลื่อนด้วย AI สามารถระบุได้ พฤติกรรมการสำรองข้อมูลผิดปกติและสามารถเริ่มต้นการสแกนมัลแวร์ได้โดยอัตโนมัติ การสแกนมัลแวร์สามารถตรวจจับได้ ไฟล์ที่ติดไวรัสภายในอิมเมจสำรอง

การกู้คืน (Recover)

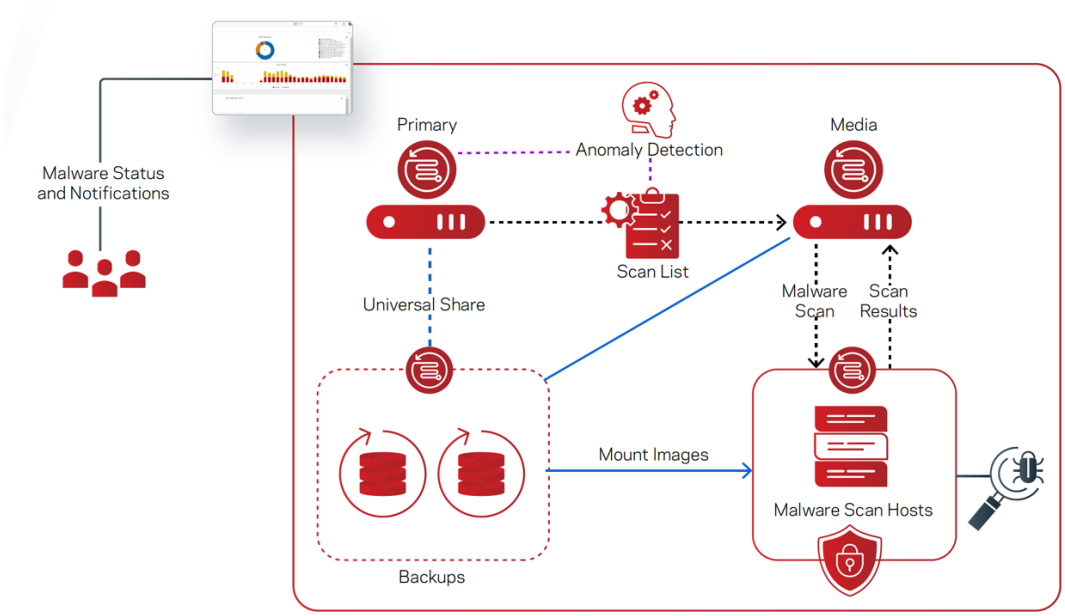
IRE ให้สำเนาที่ปลอดภัยของข้อมูลสำรองที่สำคัญ มอบชุดไฟล์ที่สะอาดตามความต้องการสำหรับผู้ดูแลระบบการกู้คืน. NetBackup ตรวจพบภาพที่ได้รับผลกระทบ แจ้งเตือนผู้ดูแลการสำรองข้อมูล และให้ความสามารถในการดู รายการไฟล์ที่ได้รับผลกระทบ สำเนาทั้งหมดจะหมดอายุ รูปภาพที่ใช้งานได้ล่าสุดจะมองเห็นได้ชัดเจนในเวิร์กโฟลว์การกู้คืนและ การเลือกรูปภาพที่ได้รับผลกระทบจะแสดงคำเตือนหลายอย่างแก่ผู้ใช้

NetBackup Malware Scanning and Anomaly Detection

การตรวจจับมัลแวร์ของ NetBackup ให้การควบคุมเพิ่มเติมในส่วนการตรวจจับและการกู้คืนของเวิร์กโฟลว์. NetBackup นำเสนอวิธีการสแกนมัลแวร์สองวิธีเพื่อปกป้องความสมบูรณ์ของข้อมูลและอิมเมจของข้อมูลสำรอง การสแกนตามต้องการและการสแกนโดยอัตโนมัติตามคะแนนความผิดปกติสูง

NetBackup เวอร์ชั่น 10.0 ได้เพิ่มระบบการตรวจสอบมัลแวร์เพื่อเป็นตัวช่วยให้คุณทำการสแกนอิมเมจสำรองตามต้องการสำหรับภัยคุกคามที่แอบแฝง นอกจากนี้ ยังสามารถทำงานร่วมกับตัวสแกนมัลแวร์ชั้นนำ เช่น Microsoft Defender และ Symantec Protection Engine

การจัดเก็บสถานะของการสแกนในแคตตาล็อก NetBackup ช่วยให้คุณกู้คืนได้อย่างมั่นใจด้วยการมองเห็นสถานะการสแกนมัลแวร์ เพิ่มกลไกการสแกนมัลแวร์ของคุณใน NetBackup เพื่อเพิ่มความต้านทานต่อภัยคุกคามจากการก่อการร้ายทางไซเบอร์ที่เพิ่มขึ้น



วิธีติดตั้งง่ายๆ สำหรับ IRE

คุณสามารถกำหนดค่าต่างๆของสภาพแวดล้อมการกู้คืนแบบแยก (IRE) บนเซิร์ฟเวอร์แบบ BYO หรือ Flex Appliance WORM Storage เพื่อสร้างสำเนาข้อมูลแบบแยกจากกัน ระหว่างสภาพแวดล้อมการใช้งานจริงกับสำเนาของข้อมูลที่ได้รับการป้องกัน การสร้างสำเนาข้อมูลแบบแยกจากกัน จะจำกัดการเข้าถึงเครือข่ายไปยังข้อมูล ยกเว้นในช่วงเวลาที่เกิดการส่งข้อมูล ซึ่งเป็นการป้องกันเพิ่มเติมจากแรนซัมแวร์และมัลแวร์

ในการกำหนดค่า IRE คุณต้องมีสภาพแวดล้อม NetBackup ที่ใช้งานจริงและสภาพแวดล้อม NetBackup IRE ที่แตกต่างกันโดยกำหนดค่าเซิร์ฟเวอร์ MSDP สภาพแวดล้อมที่ใช้งานจริงไม่ต้องการขั้นตอนอะไรเพิ่มเติมจากปกติ การเปิดใช้งานฟังก์ชัน IRE นั้นดำเนินการภายใน IRE เอง โดยแยกแหล่งที่มาที่เชื่อถือได้และ ตารางเวลาเท่านั้น.

สรุป

Veritas ยังคงเสริมความแข็งแกร่งให้กับการควบคุม Isolated Recovery Environment ของ NetBackup เพื่อให้ปลอดภัยจากการโจมตีจากแรนซัมแวร์และมัลแวร์ ด้วยการควบคุมแบบละเอียดของ NetBackup สำหรับการดำเนินการ IRE และ SLP ทำให้คุณมั่นใจมากยิ่งขึ้นสำหรับการรักษาความปลอดภัยของข้อมูลองค์กร

ข้อมูลอ้างอิง

Flex Appliance Product:
https://sort.veritas.com/documents/doc_details/FAPP/2.1/Veritas%205350/Documentation/

NetBackup Product:
https://sort.veritas.com/documents/doc_details/NetBackup/10.0/Windows%20and%20UNIX/Documentation/