الفصل المنطقي

تقييم لمتطلبات أمن السحابة لوزارة الدفاع الأمريكية
لأعباء العمل الحساسة

مايو ٢٠١٨

[سلسلة كتيبات AWS الحكومية]

إشعارات

هذا المستند مقدم لأغراض معلوماتية فقط. يحتوي على عروض منتجات AWS وممارساتها الحالية في تاريخ إصدار هذا المستند، والتي تخضع للتغيير دون إشعار مسبق. إن العملاء مسؤولون عن تقييمهم المستقل للمعلومات الموجودة في هذا المستند وعن أي استخدام لمنتجات AWS أو خدماتها، والتي تتاح كل منها "كما هي" بدون ضمان من أي نوع، سواء صريح أو ضمني. ولا يمثل هذا المستند أي ضمانات أو تمثيلاً أو التزامات تعاقدية أو شروطًا أو تأكيدات من AWS أو أي من الشركات التابعة لها أو مورديها أو الحاصلين على تراخيصها. وتتحكم اتفاقية AWS في مسؤوليات AWS والتزاماتها نحو عملائها، وهذا المستند ليس جزءًا من أي اتفاقية مبرمة بين AWS وعملائها كما لا يمثل تعديلاً لها.

جدول المحتويات

الهدف

يبحث هذا المستند تكافؤ أمان الفصل المنطقي للعملاء الذين يستخدمون البنية التحتية كخدمة (IaaS) لخدمات Amazon Web Services (AWS) لتلبية متطلبات الفصل المنصوص عليها في دليل متطلبات أمن الحوسبة السحابية (SRG) التابع لوزارة الدفاع (DOD). يناقش هذ المستند نهجًا ثلاثي الأبعاد — الاستفادة من المحاكاة الافتراضية، والتشفير، ونشر الحوسبة على الأجهزة المخصصة — التي يمكن للحكومات في جميع أنحاء العالم أن تستخدمها لترحيل أحمال العمل الحساسة غير المصنفة (مثل، عالية التأثير) بثقة إلى السحابة دون الحاجة إلى بنية تحتية مخصصة فعليًا.

المقدمة

تستفيد التكنولوجيا السحابية من التقنيات التحويلية في تكنولوجيا المعلومات (IT). ويستفيد العملاء الذين يستخدمون السحابة من البنية الهندسية لمركز البيانات والشبكة المصممة لتلبية متطلبات معظم المؤسسات الحساسة من ناحية الأمان في العالم. تساهم النماذج التشغيلية الجديدة والأفكار التجريدية الحديثة التي توفرها التقنيات السحابية في خلق بيئة أكثر أمنًا لتكنولوجيا المعلومات. يستخدم مقدمو الخدمات السحابية (CSP) مثل AWS السحابة للابتكار وتزويد العملاء بميزات أمان جديدة ومحسّنة. توفر AWS الخدمات المتاحة بسهولة وتدعم إمكانات "الدفاع في العمق" و"الدفاع في اتساع" مع آليات الأمن المتأصلة في تصميمات الخدمات السحابية وعملياتها.

تمنح AWS للعملاء ملكية المحتوى الخاص بهم والتحكم فيه عن طريق التصميم من خلال الأدوات التي تسمح للعملاء بتحديد مكان تخزين محتوياتهم. توفر ميزات AWS للعملاء القدرة على تأمين المحتوى الخاص بهم خلال مرحلة الانتقال وأثناء الاستراحة، وإدارة الوصول إلى خدمات AWS ومواردها لمستخدميها. يحافظ عملاء AWS على التحكم الكامل في الوصول إلى المحتوى الخاص بهم مما يمنع المستخدمين والعملاء غير المصرح لهم من الوصول إلى حسابات العملاء الآخرين. توفر AWS خدمات متعددة المستأجرين مع أفضل أمان فصل في هذا القطاع للمستأجر. يوفر هذا الفصل المنطقي بين بيئات العملاء التي توفرها AWS أمانًا أكثر فعالية وموثوقية أكثر من البنية الأساسية المادية المخصصة.

الخلفية

في ديسمبر ٢٠١١ وضع كبير مسؤولي المعلومات الفيدرالي في الولايات المتحدة سياسة على مستوى الحكومة تقضي بتكليف الوكالات الفيدرالية باستخدام برنامج المخاطر الفيدرالية وإدارة التخويل (FedRAMP) - وهو برنامج موحد ويتم استخدامه على نطاق فيدرالي واسع للحصول على الترخيص الأمني للخدمات السحابية. تم تصميم نهج "التنفيذ مرة واحدة، والاستخدام عدة مرات" في برنامج المخاطر الفيدرالية وإدارة التخويل "FedRAMP" لتقديم فوائد كبيرة، مثل زيادة الاتساق والموثوقية في تقييم عناصر التحكم الأمنية، وخفض التكاليف لمقدمي الخدمات وعملاء الوكالة، وتبسيط عمليات تقييم الترخيص المكرر عبر الوكالات التي تحصل على نفس الخدمة. الهيئة الرئيسية للحوكمة وصنع القرار في برنامج المخاطر الفيدرالية وإدارة التخويل "FedRAMP" هي مجلس التفويض المشترك (JAB)، والذي يتألف من كبار موظفي المعلومات (CIO) لإدارة الخدمات العامة، وزارة الأمن القومي، ووزارة الدفاع "DoD".

لدى FedRAMP حاليًا ثلاثة خطوط أساسية قياسية للأمان — ذات تأثير منخفض ومتوسط ومرتفع — بناءً على تصنيفات منشور معايير معالجة المعلومات الفيدرالية 199 (FIPS) . تم تطوير خطوط الأساس هذه من خلال التعاون مع خبراء الأمان على الإنترنت عبر الصناعة الخاصة والحكومة الأمريكية (بما في ذلك وزارة الدفاع DoD). في حين أن وزارة الدفاع "DoD" استخدمت مبدأ المعاملة بالمثل مع خط الأساس المعتدل لـ FedRAMP، إلا أنها لم تستخدم مبدأ المعاملة بالمثل مع خط الأساس العالي لـ FedRAMP. وبدلاً من ذلك، قامت وزارة الدفاع بتطوير وتنفيذ ما يُعد فعليًا مجموعة "FedRAMP plus" من عناصر التحكم في الأمان والمتطلبات عبر دليل متطلبات أمن الحوسبة السحابية لوزارة الدفاع (SRG).

على وجه الخصوص، تتطلب وزارة الدفاع من خلال دليل متطلبات أمن الحوسبة السحابية "SRG" الفصل بين وزارة الدفاع والمستأجرين/المهام الحكومية الفيدرالية إما عبر الوسائل المادية أو المنطقية. وبشكل أكثر تحديدًا، فإن دليل متطلبات أمن الحوسبة السحابية "SRG" ينص على أنه "يجب على مقدمي الخدمة السحابية تقديم دليلاً على الضوابط والمراقبة القوية على الفصل الافتراضي، والقدرة على تلبية متطلبات "التفتيش والضبط" دون الإفراج عن معلومات وبيانات وزارة الدفاع". والأكثر من ذلك، بالنسبة إلى أنظمة Impact Level 5 (IL5)،[1] تطلب وزارة الدفاع DoD "الفصل المادي (مثل البنية الأساسية المخصصة) من المستأجرين من خارج وزارة الدفاع/الحكومة الفيدرالية". تركز متطلبات وزارة الدفاع هذه على مخاوف وزارة الدفاع فيما يتعلق باختلاط بيانات وزارة الدفاع مع بيانات المستأجرين الآخرين من خلال تسرب البيانات أو نشرها والوصول غير المصرح به أو العبث ببيانات وزارة الدفاع من قِبل مستأجر من خارج وزارة الدفاع.

لتنفيذ أفضل الممارسات التي تركز على النتائج، أقر دليل متطلبات أمن الحوسبة السحابية "SRG" باستخدام الفصل المنطقي كنهج قابل للاستمرار لتلبية متطلبات فصل DoD IL5:

"قد يوفر مقدم الخدمة السحابية حلولاً بديلة توفر أمانًا مكافئًا للمتطلبات المذكورة. سيتم تقييم الموافقة على أساس كل حالة على حدة أثناء عملية تقييم PA [الترخيص المؤقت]".

---

١ موقع 5.2.2.2 Impact Level ومتطلبات الفصل

لا يمكن معالجة المعلومات التي يجب معالجتها وتخزينها في Impact Level 5 إلا في بنية أساسية مخصصة أو داخليًا أو خارجيًا في أي نموذج نشر سحابي يقيد الموقع الفعلي للمعلومات كما هو موضح في القسم ٥-٢-١، "متطلبات الاختصاص القضائي / الموقع". وهذا يستثني عروض الخدمة العامة.

يتم تطبيق ما يلي:

- وحدها الأنظمة السحابية الخاصة لوزارة الدفاع أو مجتمع وزارة الدفاع أو مجتمع الحكومة الفيدرالية مؤهلة لـ Impact Level 5.
- قد يدعم كل نموذج نشر العديد من المهام أو مستأجرين / مهام من كل مؤسسة تابعة للعميل.
- يُسمح بالفصل الافتراضي / المنطقي بين وزارة الدفاع ومستأجري / مهام الحكومة الفيدرالية.
- هناك حاجة إلى الحد الأدنى من الفصل الظاهري / المنطقي بين أنظمة المستأجرين / المهام.
- وأيضًا الفصل المادي (مثل البنية الأساسية المخصصة) من المستأجرين من خارج وزارة الدفاع/الحكومة الفيدرالية" مطلوب.

ملحوظة: قد يوفر مقدم الخدمة السحابية حلولاً بديلة توفر أمانًا مكافئًا للمتطلبات المذكورة. سيتم تقييم الموافقة على أساس كل حالة على حدة أثناء عملية تقييم الترخيص المؤقت.

https://iasecontent.disa.mil/cloud/Downloads/Cloud_Computing_SRG_v1r3.pdf

ما أوجه القصور في متطلبات الفصل المادي؟

متطلبات العروض السحابية المخصصة ماديًا هي المحرك الأساسي للمخاوف المتعلقة بالوصول إلى جهات خارجية أو غير ذلك من الوصول غير المصرح به إلى التطبيقات أو المحتوى أو البيانات، بما في ذلك الوصول الممنوح في إطار إنفاذ القانون والوصول غير المصرح به من طرف ثالث. ومع ذلك، بالنسبة للأنظمة التي يمكن الوصول إليها عبر شبكة أو عبر الإنترنت، فإن الفصل المادي لتلك الأنظمة، مثل وضعها في قفص مغلق أو مركز منفصل للبيانات، لا يوفر أمانًا أو مزيدًا من التحكم في إمكانية الوصول. ببساطة، يتم التحكم في جميع عناصر التحكم في الوصول للأنظمة المتصلة عبر عناصر التحكم المنطقية في الوصول وإدارة الأذونات وتوجيه حركة مرور الشبكة والتشفير. تعالج AWS أية مخاوف تتعلق بالفصل المادي من خلال قدرات الأمن المنطقي التي نقدمها لجميع عملائنا وضوابط الأمان التي نطبقها لحماية بيانات العملاء، والموصوفة بشكل أكبر في نهج الفصل المنطقي ثلاثي الأبعاد الموجود أدناه.

إن البيئات الصغيرة والمنفصلة ماديًا لا تكافئ البيئات السحابية المتوفرة بشكل عام؛ وبالتالي يمكن لأيّ من متطلبات الفصل المادي قصر أو الحد من قدرة العميل على الاستفادة من الاستثمارات المبتكرة (بما في ذلك الابتكارات في ميزات الأمان) التي يتم إجراؤها نيابةً عن جميع العملاء الذين يستخدمون خدمات AWS. تشمل العيوب أيضًا هيكل تكلفة أعلى وقلة استخدام ناتجة عن الاستخدام الأقل كفاءة للمساحة فضلاً عن خيارات وخصائص التكرار المحدودة مقارنة بالتنوع الجغرافي لمناطق مراكز البيانات التجارية.

كيف يكون الفصل المنطقي أكثر فعالية من الفصل المادي؟

يمكن للعملاء الاستفادة من النهج ثلاثي المحاور أدناه لتحقيق النتائج الأمنية المكافئة للفصل المادي بنجاح، كما هو مطلوب في DoD IL5.

١. السحابة الخاصة الافتراضية (VPC) - عرض توضيحي كافٍ أن VPC تنشئ ما يعادل نطاقات شبكة منفصلة بالكامل لكل مستأجر؛

٢. تشفير البيانات أثناء الراحة وخلال مرحلة الانتقال - الاستفادة من إمكانيات تشفير البيانات المقدمة من المستخدم أو الجوهرية لخدمات AWS السحابية مثل EBS وS3 وDynamoDB، مع مفاتيح التشفير التي يتم إنشاؤها وتخزينها بواسطة AWS Key Management Service (KMS) و/أو AWS Cloud Hardware Security Module (CloudHSM)؛ و

٣. يمكن للمضيفات المخصصة والمثيلات المخصصة ومالكي مهام Bare Metal — التابعة لوزارة الدفاع تقديم مضيفات فعلية لـ AWS من أجل معالجة كل من مثيلات الأجهزة المرئية وغير المرئية التي تقوم بتعيينها وأعباء العمل المرتبطة بها.

١. سحابة خاصة افتراضية (VPC)

تعمل السحابة الخاصة الافتراضية لـ AWS على تمكين إنشاء منطقة معزولة على إحدى الشبكات المنفصلة بشكل منطقي ضمن شبكة سحابة AWS للحوسبة المرنة (Amazon EC2) التي يمكنها توفير موارد الحوسبة والتخزين. يمكن توصيل هذه البيئة بالبنية الأساسية الحالية للعميل من خلال اتصال شبكة خاصة افتراضية (VPN) عبر الإنترنت، أو من خلال AWS Direct Connect، وهي خدمة توفر اتصالاً خاصًا بسحابة AWS. يوفر استخدام سحابة خاصة افتراضية "VPC" لأصحاب المهام المرونة والأمان والتحكم الكامل في تواجد شبكاتهم في السحابة. ويتيح ذلك إمكانية الانتقال بشكل منظّم إلى السحابة باستخدام نموذج مركز البيانات الحالي ومخطط الإدارة الخاص بالعميل. يتحكم العميل في البيئة الخاصة بما في ذلك عناوين IP والشبكات الفرعية وقوائم التحكم بالوصول إلى الشبكة ومجموعات الأمان وجُدر الحماية الخاصة بنظام التشغيل وجداول التوجيه و/أو الشبكات الظاهرية الخاصة و/أو بوابات الإنترنت. توفر Amazon VPC عزلاً منطقيًا قويًا لكافة موارد العملاء. على سبيل المثال، يتم تفويض كل حزمة تتدفق على الشبكة بشكل فردي للتحقق من صحة المصدر والوجهة الصحيحة قبل إرسالها وتسليمها. لا يمكن نقل المعلومات بين العديد من المستأجرين دون تصريح خاص من قِبل كل من العملاء المرسلين والمستلمين. إذا تم توجيه حزمة إلى وجهة بدون قاعدة تطابقها، يتم إسقاط الحزمة. وعلاوة على ذلك، بينما تقوم حزم "بروتوكول تحليل العنوان" (ARP) بتشغيل بحث قاعدة بيانات مصادق، لا تقوم حزم ARP بالضغط على الشبكة نظرًا لعدم الحاجة إليها لاكتشاف مخطط الشبكة الافتراضية، لذلك من المستحيل استخدام انتحال ARP. وكذلك، لا يكشف الوضع المختلط عن أي عملية نقل غير تلك المرتبطة من وإلى نظام تشغيل العميل. هذه المجموعات الدقيقة من القواعد الخاصة بالدخول والخروج والتي تم وضعها بواسطة العميل لا تسمح فقط بزيادة المرونة في الاتصال، بل تتيح أيضًا تحكم المزيد من العملاء في تجزئة الحركة وتوجيهها.

على سبيل المثال، تشمل خيارات اتصال VPC[٢] قدرة العميل على:

- الاتصال بالإنترنت باستخدام ترجمة عنوان الشبكة (الشبكات الفرعية الخاصة) - يمكن استخدام الشبكات الفرعية الخاصة للمثيلات التي لا ينبغي أن يكون لها وصول مباشر إلى أو من الإنترنت. يمكن للمثيلات الموجودة في شبكة فرعية خاصة الوصول إلى الإنترنت دون الكشف عن عنوان IP الخاص بها عن طريق توجيه حركة المرور الخاصة بها من خلال بوابة ترجمة عنوان الشبكة (NAT) في شبكة فرعية عامة.
- الاتصال بمركز بيانات شركتك بأمان - يمكن توجيه جميع عمليات النقل من وإلى مثيلاتها في VPC إلى مركز البيانات الخاص بشركتك عبر اتصال VPN خاص بأجهزة IPSec ومعايير الصناعة.
- الاتصال بشكل خاص مع السحابات الخاصة الافتراضية "VPC" الأخرى - اتصال السحابات الخاصة الافتراضية "VPC" للنظراء معًا لمشاركة الموارد عبر العديد من الشبكات الظاهرية التي تملكها حسابات AWS.
- ربط خدماتك الداخلية بشكل خاص عبر حسابات مختلفة وسحابات خاصة افتراضية "VPC" داخل المؤسسات الخاصة بك، مما يؤدي إلى تبسيط البنية الأساسية للشبكة الداخلية بشكل كبير.

---

٢ ملحوظة: يُعد استخدام VPC مع بوابة خاصة إلى نقطة وصول سحابة معتمدة (CAP) أو حل البنية الأساسية للحوسبة السحابية الآمنة (SCCA) التابع لوزارة الدفاع، إلزاميًا لجميع العملاء الذين يستخدمون أحمال عمل SRG IL5 في منطقة GovCloud الأمريكية التابعة لـ AWS ما لم يتم التنازل عن ظروف خاصة بواسطة DoD CIO.

٢. تشفير البيانات أثناء الراحة وخلال مرحلة الانتقال

بالنسبة للبيانات التي يخزنها أصحاب المهام على خدمات تخزين AWS أو عبر شبكاتنا، فإننا نوصي بشدة بتشفير البيانات أثناء الراحة وخلال مرحلة الانتقال. من أجل جعلها سهلة وآمنة لعملائنا، فإننا نقدم عددًا من الأدوات والميزات التي تسمح لهم بتشفير البيانات بالإضافة إلى العديد من خيارات البنية الأساسية لإدارة مفاتيح التشفير. تم دمج ميزات التحكم في الوصول إلى التشفير والبيانات هذه بالفعل في عروض الخدمات الأساسية مثل Amazon Simple Storage Service (Amazon S3)، وهي خدمة تخزين كائن قابلة للتطوير بشكل كبير، وAmazon Elastic Block Store (Amazon EBS)، والتي توفر تخزينًا مرفقًا بالشبكة لمثيلات EC2، وAmazon Relationa Database Service (Amazon RDS)، والتي توفر محركات قاعدة البيانات المُدارة. هذه الميزات جاهزة للاستخدام وتوفر مجموعة كبيرة من المستندات لمساعدة العملاء على فهم كيفية حماية بياناتهم وخيارات التكوين التي يمكنهم التحكم بها لتخصيص من يمكنه الوصول إلى الأنظمة. تتمتع الخدمات الأصلية لـ AWS بقدرات أمان متطورة لا يمكن تحقيقها في البيئات القديمة إلا من خلال تجميع موردي الجهات الخارجية. الآن أصبحت هذه الإمكانيات متاحة بشكل متزايد، مما يتيح للعملاء التركيز على الابتكار في الخدمات.

إن الجمع بين خدمة AWS Key Management Service (KMS) وAWS CloudHSM هما محور أحد حلول التشفير الصارم. AWS KMS هي خدمة إقليمية مدارة بشكل كامل ومتوفرة على مستوى عالٍ باستخدام المستوى ٣ من FIPS 140-2 لوحدات تأمين الأجهزة (HSM) (الأمان المادي) التي تم التحقق منها[٣] في قاعدتها، مع برمجيات متطورة للتوزيع يمكنها التعامل مع مئات الآلاف من طلبات API في الثانية. حيث تمنح العملاء القدرة على أداء وظائف الإدارة الرئيسية بطريقة تتكامل بدرجة كبيرة مع خدمات AWS الأخرى. يوفر AWS CloudHSM وحدات تأمين أجهزة (HSM) مخصصة، المستوى ٣ من FIPS 140-2 (بشكل عام)، ضمن سيطرتك الحصرية، مباشرة في Amazon Virtual Private Cloud (VPC) الخاصة بك.[٤] توفر خدمة CloudHSM توافرًا آليًا ونسخًا متماثلاً ونسخًا احتياطيًا لأجهزة HSM المخصصة لعميل واحد عبر مناطق توافر الخدمات. وتتكامل مع التطبيقات المملوكة للعملاء باستخدام واجهات برمجة تطبيقات التشفير القياسية في هذا المجال. على الرغم من إمكانية تطبيقها في سياقات مختلفة، تعمل كلتا الخدمتين على ضمان أن تكون خوارزمية التشفير قوية بما يكفي لجعل البيانات غير مفهومة وحماية المفاتيح بشكل كاف بحيث يكون النص المشفر غير قابل للقراءة من قِبل أشخاص غير مخولين. وبعبارة أخرى، يمكن أن يوفر تخزين البيانات المشفرة بشكل مناسب مع مفاتيح آمنة ومدارة بشكل صحيح ضمانًا للبيانات المحمية بالكامل. هذا النهج له نفس القدر من الأهمية وقابلية التطبيق والفعالية بغض النظر عما إذا كان قد تم نشره في بيئة سحابة تجارية معزولة ماديًا أو معزولة منطقيًا.

مع التشفير، تعتبر سرية مفاتيح التشفير الخاصة بمالك المهمة أمراً بالغ الأهمية. يعتمد الأمان على مكان تشفير البيانات ومن يمكنه الوصول إلى المفاتيح ويحميها. إذا تم تشفير البيانات من قِبل مالك المهمة قبل أن يتم استيعابها في السحابة، فلا يوجد سبب لكي يتمكن مقدم الخدمة السحابية من الوصول إلى المفاتيح — يتمتع مالك المهمة بالتحكم الكامل والمسؤولية. من ناحية أخرى، إذا تم تشفير البيانات باستخدام خدمات مدمجة لدى مقدم الخدمة السحابية، فسيكون كل من مقدم الخدمة السحابية ومالك البيانات في سلسلة الاحتفاظ بالمفاتيح. تم تصميم AWS KMS بحيث لا يمكن لأحد، بما في ذلك موظفي AWS، استرداد مفاتيح النص غير المشفر من الخدمة. تستخدم الخدمة FIPS 140-2 وحدات تأمين الأجهزة HSM التي تم التحقق من صحتها لحماية سرية المفاتيح الخاصة بك وسلامتها بغض النظر عما إذا كنت تطلب KMS لإنشاء مفاتيح نيابة عنك أو قمت باستيرادها إلى الخدمة.

---

٣ https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3139

٤ https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3108

لا تتم كتابة مفاتيح النص غير المشفر مطلقًا على القرص وتستخدم فقط في ذاكرة الوصول العشوائي لوحدات تأمين الأجهزة "HSM" للوقت اللازم لتنفيذ عملية التشفير المطلوبة. لا يتم أبدًا نقل مفاتيح KMS خارج مناطق AWS التي تم إنشاؤها فيها. يتم التحكم في وصول التحديثات إلى البرامج الثابتة KMS HSM عن طريق التحكم في الوصول القائم على النصاب القانوني الذي يتم مراجعته وتدقيقه من قِبل مجموعة مستقلة داخل Amazon. هذه السياسات والعمليات والإجراءات تم تدقيقها واعتمادها بشكل مستقل بموجب FedRAMP ووزارة الدفاع (DoD). يلخص القسم أدناه قدرات AWS KMS وAWS CloudHSM. يمكن للعملاء الرجوع إلى الروابط المضمنة للحصول على موارد إضافية حول AWS KMS وAWS CloudHSM.

(KMS) AWS Key Management Service

توفر خدمة AWS Key Management Service (KMS) للعملاء التحكم بشكل مركزي في مفاتيح التشفير المستخدمة لحماية بياناتهم. باستخدام AWS KMS، يمكن للعملاء إنشاء سياسات الاستخدام ومراجعة استخدام مفاتيح التشفير المستخدمة لتشفير بيانات العملاء وتدويرها وتعطيلها وحذفها وتحديدها. تم دمج AWS KMS مع خدمات AWS، مما يجعل من السهل تشفير البيانات المخزنة في هذه الخدمات مع مفاتيح التشفير التي يديرها العميل (أو عبر مفاتيح التشفير الافتراضية التي تديرها خدمة AWS نيابة عن العميل). تم تضمين هذه الخدمة مع خمس خدمات أساسية معتمدة لتلبية متطلبات DoD IL5 لتمكين تشفير البيانات أثناء الراحة وخلال مرحلة الانتقال، وتوفر فصلًا منطقيًا كافيًا لبيانات وزارة الدفاع (DoD) التي تمر عبر البنية الأساسية لـ AWS وتشترك في موقعها على الأجهزة مع بيانات العملاء غير التابعة لوزارة الدفاع. على سبيل المثال، في حالة وجود بيانات أثناء الراحة، يكون استخدام خوارزميات التشفير القوية للفصل المنطقي لبيانات العميل هو الأساس لإنشاء معادلة للفصل الفعلي للبيانات أثناء الراحة - وهو أحد متطلبات IL5.

الحدود الأمنية الداخلية لـ AWS KMS هي وحدة الأمان المشددة (HSM). تحتوي وحدة الأمان المشددة (HSM) على واجهة برمجة التطبيقات المستندة إلى الويب الداخلية المحدودة ولا توجد واجهات فعلية نشطة أخرى في حالتها التشغيلية. يتم تكوين وحدة الأمان المشددة (HSM) التشغيلية وتحميلها مع مفاتيح التشفير المناسبة أثناء التهيئة. يتم تخزين مواد التشفير الحساسة لـ HSM فقط في ذاكرة الوصول العشوائي، ويتم محوها عند نقل HSM خارج الحالة التشغيلية، بما في ذلك عمليات الإغلاق أو إعادة التشغيل المقصودة أو غير المقصودة. عندما تكون في حالة التشغيل، لا يمكن لأي مشغل بشري الوصول إلى HSM. يمكن فقط لمستضيفي الخدمة الذين يتعاملون مع طلبات العملاء إجراء اتصالات عبر واجهة برمجة التطبيقات المحدودة. تتوافر واجهات برمجة التطبيقات الخاصة بـ HSM عبر جلسة سرية موثقة بشكل متبادل يحددها مشغلون بشريون (عندما يكونون خارج أوقات العمل) أو مضيفين للخدمة (عندما يكونون أثناء أوقات العمل).

تم تصميم النظام بحيث يتطلب الأمر وجود عدة مشغلين بشريين يستخدمون المصادقة الثنائية من خلال عملية تستند إلى النصاب القانوني لتحديث البرامج الثابتة أو تكوين البرامج على أيّ من وحدات KMS HSM ولكن حتى بعد ذلك فقط يتم وضعه في حالة غير تشغيلية ولا يحتوي على مفتاح مواد.

ملحوظة: تستخدم خدمة AWS Key Management Service (KMS) الآن FIPS 140-2 لوحدات تأمين الأجهزة التي تم التحقق منها (HSM) وتدعم FIPS 140-2 لنقاط النهاية التي تم التحقق منها، والتي توفر تأكيدات مستقلة حول سرية المفاتيح الخاصة بك وسلامتها.

AWS Cloud HSM

توفر AWS CloudHSM إدارة فعالة لمفاتيح الأجهزة على مستوى السحابة لأعباء العمل الحساسة والمنظمة. يتيح CloudHSM لأصحاب المهام توفير مفاتيح التشفير والاستفادة منها لتشفير بياناتهم ضمن خدمات AWS وتطبيقاتهم المقيمة. مع CloudHSM، يقوم العملاء بإدارة مفاتيح التشفير الخاصة بهم باستخدام FIPS 140-2 المستوى ٣ من وحدة HSM التي تم التحقق من صحتها، كما يتيح مرونة التكامل مع تطبيقاتهم باستخدام واجهات برمجة التطبيقات القياسية الصناعية، مثل PKCS # 11 وJava Cryptography Extensions (JCE) ومكتبات Microsoft CryptoNG (CNG). كما أنها متوافقة مع المعايير وتمكن أصحاب المهام من تصدير جميع المفاتيح لمعظم أجهزة HSM الأخرى المتاحة تجاريًا. CloudHSM هي خدمة مدارة تقوم بأتمتة المهام الإدارية التي تستغرق وقتًا طويلاً، مثل توفير الأجهزة وتصحيح البرامج والتوافر العالي والنسخ الاحتياطي. لحماية خدمة CloudHSM الخاصة بك وعزلها عن عملاء Amazon الآخرين، يجب توفير CloudHSM داخل VPC.

الفصل بين الواجبات والتحكم في الوصول المستند إلى الأدوار مدمج في تصميم CloudHSM. لدى AWS وصول محدود إلى HSM مما يسمح لنا بمراقبة HSM والحفاظ على سلامتها وتوافرها، والحصول على نسخ احتياطية مشفرة، واستخراج سجلات التدقيق إلى سجلات CloudWatch الخاصة بك ونشرها. لا تستطيع AWS معرفة المفاتيح الخاصة بك أو الوصول إليها أو استخدامها، أو تتسبب في قيام HSM لديك بتنفيذ أي عملية تشفير باستخدام المفاتيح الخاصة بك.

٣. مضيفون مخصصون ومثيلات مخصصة ومعادن عادية

بالإضافة إلى توفير خدمات حوسبة عالية الأمان ومعزولة منطقيًا ومتعددة المستأجرين، توفر AWS أيضًا ثلاث وسائل لنشر الحوسبة على أجهزة مخصصة باستخدام مثيلات مخصصة ومضيفين مخصصين ومعادن عادية. يمكن استخدام خيارات النشر هذه لتشغيل مثيلات Amazon EC2 على الخوادم الفعلية المخصصة لاستخدامك. والمثيلات المخصصة هي مثيلات Amazon EC2 مرئية ويتم تشغيلها في سحابة خاصة افتراضية (VPC) على أجهزة مخصصة لعميل واحد. المثيلات المخصصة معزولة بشكل مادي على مستوى الجهاز المضيف من المثيلات التي تنتمي إلى حسابات AWS الأخرى. المثيلات المخصصة ربما تشارك الأجهزة مع مثيلات أخرى من حساب AWS نفسه غير المثيلات المخصصة. يُعد المضيف المخصص خادمًا فعليًا مخصصًا لاستخدامك. مع المضيف المخصص، تتمتع برؤية وتحكم في كيفية وضع المثيلات المرئية على الخادم. المثيلات المعدنية هي أجهزة تستخدمها الأجهزة المضيفة غير المرئية. باستخدام تقنية AWS Nitro لإلغاء تحميل الشبكة والتخزين، فضلاً عن رقاقة أمان Nitro للتخلص من المخاطر المرتبطة بالإيجار المنفرد التسلسلي على المعدن، يمكن للعملاء الوصول المباشر إلى أجهزة Amazon EC2. هذه المثيلات المعدنية هي أعضاء شاملة في خدمة Amazon EC2 ولديهم إمكانية الوصول إلى خدمات مثل Amazon VPC وAmazon Elastic Block Store (EBS).[٥]

[٥] في الوقت الحالي، يمكن تجربة Amazon EC2 Bare Metal على سلسلة مثيل I3 على شكل نوع المثيل i3.metal.

لا يوجد أي اختلافات في الأداء أو الأمان بشكل فعلي بين المثيلات المخصصة والمثيلات المنشورة على "المضيفين المخصصين". ومع ذلك، يمنح المضيفون المخصصون لمالكي المهام تحكمًا إضافيًا على كيفية وضع المثيلات على خادم فعلي وكيفية استخدام هذا الخادم. عند استخدام المضيفون المخصصون، يمكنك التحكم في موضع المثيل على المضيف باستخدام Host Affinity وإعدادات تحديد موقع المثيل بشكل تلقائي. إذا كانت مؤسستك ترغب في استخدام AWS، ولديها ترخيص برنامج حالي يتطلب تشغيل البرنامج على قطعة معينة من الأجهزة لحد أدنى من الوقت. يسمح المضيفون المخصصون برؤية أجهزة المضيف، مما يتيح لك تلبية متطلبات الترخيص هذه.

كيف تدعم سحابة المستأجرين المتعددين طلبات إنفاذ القانون للبيانات دون إصدار بيانات DoD؟

تمتثل AWS لطلبات إنفاذ القانون القانونية للبيانات. في حين أن الأنظمة الداخلية عادةً ما تسمح للسلطات بالتحكم في الأجهزة المادية من مالك البيانات أو الوصول إليها بشكل مباشر، تقدم الحوسبة السحابية نموذجًا مختلفًا منذ استضافة البيانات في بيئة متعددة المستأجرين. لا يمكن التحكم فعليًا في الأجهزة المادية أو الوصول إليها في AWS نظرًا لأنه يتم نشر البيانات الخاصة بعميل واحد عبر الأجهزة المادية المختلفة، مما يجبر جميع طلبات البيانات على المرور بعملية استرجاع منطقية معتمدة ومصرح بها. من خلال اعتماد FedRAMP، تمتثل AWS لعناصر تحكم NIST 800-53 التي تضم خط أساس FedRAMP المعتدل، بما في ذلك عناصر التحكم في الأمان "التعامل مع المعلومات والاحتفاظ بها" و"النظام وسلامة المعلومات". وهذا يعني، من بين أمور أخرى، أن خدمات AWS توضح الحدود الفاصلة بين حسابات العملاء المختلفة، وتمنع أي اختلاط بين حسابات العملاء، وتؤدي إلى تحكم العملاء في محتويات وعمليات حسابات AWS الفردية بشكل كامل. يمكن لعملاء وزارة "DoD"، مثل جميع العملاء، التأكد من أن أي طلب لإنفاذ القانون بشكل قانوني لن ينطبق إلا على البيانات الموجودة في حساب العميل الخاضع للطلب. كما أننا نلتزم أيضًا بضوابط "سلامة النظام والمعلومات"، التي تتطلب أن يوفر مقدمو الخدمات السحابية المتوافقين للعملاء إمكانية الوصول إلى بياناتهم وتكليف الوكالات المتوافقة بالاحتفاظ بالبيانات الخاصة بهم بما يتفق مع القوانين المعمول بها. بالإضافة إلى ذلك، تتطلب ضوابط "التدقيق والمساءلة" أن تحتفظ المؤسسات بسجلات تدقيق لتوفير الدعم للتحقيقات بعد وقوع الحوادث الأمنية ولتلبية متطلبات الاحتفاظ بالمعلومات التنظيمية والمؤسسية. يمكن للعملاء استرداد سجلات التدقيق السحابية والتقارير من خلال الاستفادة من CloudTrail وCloudWatch Logs، والتي يمكنهم بعد ذلك تقديمها إلى السلطات المختصة. تمكّن هذه الحلول وزارة الدفاع "DoD" من الاستجابة مباشرةً لطلبات المفتش العام أو إنفاذ القانون للحصول على المعلومات، مما يمكّن المسؤولين الحكوميين من الوصول المباشر إلى المعلومات التي قد يحتاجونها دون الاستيلاء على الأجهزة.

كما تطبق AWS سياسات وضوابط قوية فيما يتعلق بالإزالة والتدمير. على سبيل المثال، تقوم AWS بتتبع إجراءات إزالة الوسائط والتخلص منها وتوثيقها والتحقق منها. يتمتع العميل في أي وقت من الأوقات بالوصول الفعلي إلى الوسائط التي تم تعيينها إلى وحدة التخزين المنطقية أو كائنها المنطقي. يتم تنفيذ جميع عمليات إزالة الوسائط والتخلص منها بواسطة موظفي AWS المعينين. يتم التعامل مع المحتوى الموجود على محركات الأقراص على أعلى مستوى من التصنيف وفقًا لسياسة تصنيف البيانات الخاصة بـ AWS. يتم جعل جميع الوسائط غير قابلة للقراءة وتدميرها في نهاية دورة حياة الوسائط قبل مغادرة غرفة بيانات مركز AWS وفقًا للمعايير الأمنية لـ AWS كجزء من عملية إنهاء الخدمة.

كيف تتم حماية السحابة متعددة المستأجرين من الوصول غير المصرح به من طرف ثالث، بما في ذلك وصول موظف مقدم الخدمة السحابية "CSP"، إلى بيانات وزارة الدفاع "DoD"؟

وهناك شاغل ذي صلة بما سبق يتعلق باتساع قدرة إنفاذ القانون على طلب بيانات العميل بطريقة شرعية، وهو إمكانية وصول طرف ثالث غير مصرح به إلى محتوى العميل ومدى كفاءة إجراءات التحكم في الوصول لمنع الوصول غير المصرح به من جانب موظفي مقدم الخدمة السحابية "CSP". لا نقوم بالوصول إلى المحتوى الخاص بالعملاء أو استخدامه لأي غرض آخر سوى المطلوب قانونًا وكذلك للحفاظ على خدمات AWS وتوفيرها للعملاء وللمستخدمين النهائيين لديهم.

يتم تخصيص وصول الموظف إلى أنظمة AWS على أساس امتياز أقل، معتمد من قِبل شخص معتمد قبل توفير إمكانية الوصول، ويشرف عليه موظف في AWS. يجب الفصل بين الواجبات ومجالات المسؤولية (على سبيل المثال، طلب الوصول والموافقة وطلب إدارة التغيير والموافقة، وغير ذلك) عبر الأفراد المختلفين لتقليل فرص التعديل غير المصرح به أو غير المقصود أو إساءة استخدام أنظمة AWS. يجب على موظفي AWS الذين لديهم أعمال بحاجة للوصول إلى مستوى الإدارة أن يستخدموا أولاً مصادقة متعددة العوامل، تختلف عن أوراق اعتماد Amazon العادية للشركات، للوصول إلى المضيفين الإداريين المصممين لغرض محدد. هذه المضيفات الإدارية عبارة عن أنظمة مصممة خصيصًا وتم تصميمها وتكوينها وتقويتها لحماية مستوى الإدارة. يتم تسجيل كل عمليات الوصول وتدقيقها. في حالة عدم احتياج أحد الموظفين إلى عمل يحتاج إلى الوصول إلى مستوى الإدارة، يتم إلغاء الامتيازات والدخول إلى هذه المضيفات والأنظمة ذات الصلة. نفذت AWS سياسة تأمين جلسة عمل يتم إنفاذها بشكل منهجي. يتم الاحتفاظ بتأمين جلسة العمل حتى يتم تنفيذ إجراءات تحديد الهوية والتوثيق.

يقوم العملاء بإدارة الوصول إلى محتوى العملاء الخاص بهم وخدمات AWS ومواردها. نقدم مجموعة متقدمة من ميزات الوصول والتشفير والتسجيل لمساعدتك في القيام بذلك بفاعلية (مثل AWS CloudTrail وCloudWatch وCloudHSM وAWS KMS كما هو موضح أعلاه).

ما هي توصيات AWS إلى الحكومات التي تفكر في متطلبات الفصل المادي؟

من خلال عملية ترخيص SRG للحوسبة السحابية في وزارة الدفاع، أثبتت AWS كفاية الفصل المنطقي لتحقيق الهدف من طلب بنية أساسية معزولة ماديًا وبشكل مخصص لأحمال عمل وزارة الدفاع الأكثر حساسية وغير المصنفة. يؤكد منهجنا على أن البيئات المنفصلة بشكل منطقي متعددة المستأجرين والتي تلبي ضوابط الأمان القوية يمكن أن توفر مستوى من الأمان يتفوق على عمليات نشر السحابة الخاصة، مع توفير مزايا كبيرة فيما يتعلق بالتوافر وقابلية التطوير وانخفاض التكلفة. توفر التكنولوجيا السحابية الحديثة من مقدمي الخدمات المحددين حلولاً جديدة يمكنها تلبية هدف أمان التقنية التقليدية طالما أن أساليب الاعتماد مرنة بما يكفي لاستضافة التطبيقات البديلة.

في حين أن مراجعة ضوابط الأمان قد تكون ذات قيمة لإثبات الامتثال، فقد أظهرت تجربتنا أن المؤسسات التي تركز في المقام الأول (وفي بعض الحالات بشكل حصري) على تنفيذ الضوابط التقليدية يمكن أن تحد من وصولها إلى الحلول الأمنية الأفضل في فئتها دون قصد. بينما تقوم الحكومات بتقييم ما إذا كان مقدمو الخدمات السحابية يستوفون متطلبات تستند إلى مفاهيم قديمة، يجب عليهم بوضوح توضيح النتيجة الأمنية المنشودة والسماح لمقدمي الخدمات السحابية "CSP" بتطوير التقنيات المثلى لتحقيق (إذا لم تتجاوز) تلك النتائج. إن التركيز على الهدف الأمني المطلوب وراء متطلبات محددة يمكن أن يساعد الوكالات الفيدرالية في التركيز على النتائج التي تريد تحقيقها وليس تفاصيل التنفيذ.

مع تنامي برامج ضمان الأمان وتوسيع نطاقها لمواكبة الوتيرة المتسارعة للميزة السحابية والابتكار في مجال الأمن، سيصبح التحكم في تفاصيل التنفيذ غير ذي أهمية بشكل متزايد بالنسبة إلى القدرات التي يمتلكها مقدمو الخدمة السحابية "CSP". لن تتحقق الحالة النهائية المرغوبة - الأمان السحابي القوي، والمستندة إلى إطار محدد من خلال نتائج أمان العملاء وتقنيات الأمان المحددة لمقدمي الخدمة السحابية "CSP" من أجل تلبية هذه النتائج - إلا نتيجة للحوار المستمر عبر مجتمع أصحاب المصلحة في ضمان أمان السحابة. ونعتقد أن هذا النهج سيوفر تحسينات مهمة في الحفاظ على ضمان وضع الأمان لدى مقدم الخدمة السحابية "CSP".

بالإضافة إلى تقديم حل بديل مكافئ منطقيًا، استخدمت AWS منهجًا متكاملاً وشاركت في جلسات طويلة للتعامل مع مخاوف الأمان الرئيسية لدى وزارة الدفاع. وبدءًا باحتياجات العميل التي تم إظهارها في "دليل متطلبات الأمان" (SRG) للحوسبة السحابية الخاص بـ "وزارة الدفاع" (DoD)، عقدت AWS عدة جلسات تعريف لتثقيف وزارة الدفاع حول كيفية تلبية نهجنا ذي الثلاث محاور لتلبية متطلبات الفصل المادي. كما شارك خبير الجهة الخارجية التي صادقت على خدماتنا في هذه الجلسات ليشهد على دقة تأكيداتنا ويقدم تقييمه المستند إلى المخاطر. لقد كانت هذه الجلسات التعاونية بمثابة وسيلة قيّمة وفعالة تكفل تحقيق ضمان الأمان وتسريع الاعتماد وفي النهاية تحقيق أهداف تحديث تكنولوجيا المعلومات في وزارة الدفاع "DoD".

يشجعنا تطور وزارة الدفاع على قبول حلول مبتكرة ومتوافقة مع السحابة لتحقيق الهدف من متطلبات الفصل المادي في السحابة. نحن ملتزمون بالتعاون المستمر مع الحكومات في جميع أنحاء العالم التي تقوم بتقييم المزايا وأفضل الممارسات من نهج معادلة الفصل المنطقي في وزارة الدفاع "DoD".