# تأمين إنترنت الأشياء (IoT) باستخدام AWS

## الاستخدام الآمن للسحابة

*أبريل 2019*

## الإشعارات

يتوفر هذا المستند لأغراض معلوماتية فقط. فهو يمثل العروض والممارسات الخاصة بمنتجات AWS الحالية اعتبارًا من تاريخ إصدار هذا المستند، والتي تخضع للتغيير دون إشعار مسبق. يتحمل العملاء مسؤولية إجراء تقييمهم المستقل للمعلومات الواردة في هذا المستند وأي استخدام لمنتجات أو خدمات AWS، والتي يتم توفير كل منها «كما هي» دون أي ضمان من أي نوع، سواء أكان صريحًا أم ضمنيًا. لا يوفر هذا المستند أي ضمانات أو إقرارات أو التزامات تعاقدية أو شروط أو تأكيدات من AWS أو الشركات التابعة لها أو الموردين أو المرخصين. يتم التحكم في مسؤوليات والتزامات AWS لعملائها من خلال اتفاقيات AWS، ولا يعد هذا المستند جزءًا من أية اتفاقية بين AWS وعملائها، وكذلك لا يعدلها.

# المحتويات

**الغرض.....1**
**المعلومات الأساسية ..... 1**
**كيف تتعامل الحكومات مع قضية أمان إنترنت الأشياء؟ ..... 3**
**خدمات AWS IoT وإمكانات الأمان الخاصة بها..... 3**
Amazon FreeRTOS - برنامج الجهاز.....4
AWS IoT Greengrass - برنامج لحوسبة التخزين المؤقت.....5
AWS IoT Core - بوابة إنترنت الأشياء المستندة إلى السحابة.....6
AWS IoT Device Management - خدمة إدارة أجهزة إنترنت الأشياء المستندة إلى السحابة.....7
AWS IoT Device Defender - خدمة أمان أجهزة إنترنت الأشياء المستندة إلى السحابة.....7
**الاستفادة من الأمان المبرهن لتعزيز إنترنت الأشياء - أداة تمييز في الصناعة ..... 8**
**ما أفضل الممارسات الرئيسية لأمان إنترنت الأشياء؟ ..... 9**
**الخاتمة ..... 10**
**الملحق 1 - تكامل خدمات AWS IoT..... 11**
**الملحق 2 - كيفية تعامل الحكومات مع إنترنت الأشياء..... 12**
الولايات المتحدة.....12
المملكة المتحدة.....13
**الملحق 3 - الامتثال والخدمات الخاصة بـ AWS IoT..... ..... 15**

# الغرض

تمثل وثيقة المعلومات هذه نظرة تفصيلية على خدمات إنترنت الأشياء (IoT) التي تدعم الأمان، والتي يمكن للعملاء الاستفادة منها في سحابة AWS. وهذه الوثيقة مخصصة لمالكي البرامج رفيعة المستوى وصانعي القرار وممارسي الأمان الذين يفكرون في تبني حلول إنترنت الأشياء الآمنة للمؤسسات.

# المعلومات الأساسية

تمكن تقنية إنترنت الأشياء المؤسسات من تحسين العمليات وتعزيز عروض المنتجات وتحويل تجارب العملاء بطرق متنوعة. وعلى الرغم من تحمس قادة الأعمال للطريقة التي يمكن أن تستفيد بها أعمالهم من هذه التقنية، تظل المخاوف المتعلقة بالأمان والمخاطر والخصوصية قائمة. ويرجع ذلك جزئيًا إلى الصراع مع عروض الأمان المتباينة والمتضاربة وغير الناضجة أحيانًا، والتي تعجز عن تأمين عمليات التوزيع بشكل مناسب، مما يؤدي إلى زيادة المخاطر على بيانات العملاء أو مالك الشركة.

تتطلع المؤسسات إلى تقديم الخدمات الذكية التي يمكنها إحداث تحسين كبير في جودة حياة السكان والعمليات التجارية والذكاء، وجودة الرعاية المقدمة من موفري الخدمات، ومرونة المدن الذكية، والاستدامة البيئية، ومجموعة من السيناريوهات التي لم يتم تصورها بعد. وفي الآونة الأخيرة، شهدت AWS زيادة في استخدام إنترنت الأشياء من جانب قطاع الرعاية الصحية والبلديات، ومن خلال صناعات أخرى من المتوقع لها أن تسير على النهج نفسه في القريب العاجل. وهناك العديد من البلديات التي تعد من أوائل المستخدمين لإنترنت الأشياء، كما أنها تأخذ زمام المبادرة عندما يتعلق الأمر بدمج التقنيات الحديثة، مثل إنترنت الأشياء. على سبيل المثال:

- **كانساس سيتي، ميسوري:** أنشأت كانساس سيتي منصة مدينة ذكية موحدة لإدارة الأنظمة الجديدة التي تعمل على طول ممر عربة الترام في كانساس سيتي. وقد ساهم كل من مستشعرات الفيديو ومستشعرات الأرصفة وأنوار الشوارع المتصلة وشبكة WiFi عامة وإدارة حركة المرور وساحات انتظار السيارات في دعم انخفاض تكاليف الطاقة بنسبة 40%، و1.7 مليار دولار في تطوير مشاريع جديدة في وسط المدينة، و3247 وحدة سكنية جديدة.
- **مدينة شيكاغو، إلينوي:** تقوم شيكاغو بتركيب أجهزة استشعار وكاميرات في التقاطعات للكشف عن عدد حبوب اللقاح وجودة الهواء لمواطنيها.
- **مدينة كاتانيا، إيطاليا:** طورت كاتانيا تطبيقًا للسماح للركاب بمعرفة أقرب مكانمفتوح لوقوف السيارات في الطريق إلى وجهتهم.
- **مدينة ريسيفي، البرازيل:** تستعين مدينة ريسيفي بأجهزة تتبع تم وضعها على كل شاحنة لجمع النفايات وعربات التنظيف. وتمكنت المدينة من تخفيض تكاليف التنظيف بمقدار 250000 دولار شهريًا، مع تحسين موثوقية الخدمات والكفاءة التشغيلية.
- **مدينة نيوبورت في ويلز، المملكة المتحدة:** نشرت نيوبورت حلول إنترنت الأشياء للمدينة الذكية لتحسين جودة الهواء، والسيطرة على الفيضانات، وإدارة النفايات في غضون بضعة أشهر فقط.
- **جاكرتا، إندونيسيا:** وباعتبار جاكرتا مدينة تضم 28 مليون نسمة وتتعامل في أغلب الأحيان مع الفيضانات، فإنها تسخر إنترنت الأشياء للكشف عن مستويات المياه في القنوات والأراضي المنخفضة، وتستخدم وسائل التواصل الاجتماعي لمعرفة مشاعر المواطنين. كما تتمكن جاكرتا أيضًا من توفير الإنذار المبكر وسبل الإخلاء للأحياء المستهدفة بحيث تتعرف الحكومة والمستجيبون الأوائل على المناطق الأكثر احتياجًا، وتتمكن من تنسيق عملية الإخلاء.

وفقًا لشركة ماشينا للأبحاث، فإن السوق العالمية لإنترنت الأشياء ستصل إلى 4.3 تريليون دولار بحلول عام 2024.[1] وحسب تقرير وزارة الأعمال والابتكار والمهارات بالمملكة المتحدة، يُقدر حجم السوق العالمية لحلول المدن الذكية والخدمات الإضافية اللازمة لنشرها بمبلغ 408 مليارات دولار بحلول عام 2020.[2] علاوةً على ما سبق، تُقدر شركة فوربس[3] أن «الصيانة التنبؤية والإنتاج الذاتي الأمثل وإدارة المخزون المؤتمتة هي أفضل ثلاث حالات للاستخدام من شأنها تشجيع سوق إنترنت الأشياء على النمو حتى عام 2020.» وتؤكد شركة فوربس أن الشركات ترغب في الاستفادة من موردي تقنية المعلومات سواء الراسخين والناضجين من ذوي البنية التحتية الموثوقة عند إعداد حلول إنترنت الأشياء أو توزيعها بسبب حجم تأثير العملاء.

على الرغم من تطلع العملاء إلى الاستفادة من فرص الأعمال المتوفرة خلال إنترنت الأشياء، فإن استخدام إنترنت الأشياء بشكل آمن لم يكن واضحًا من الناحية التاريخية. لم تكن الميزات والخدمات التي تمكن الحلول آمنة على الدوام بشكل افتراضي، مما أدى إلى ترك فجوات أمنية محتملة في أسس التصميم. وعلاوةً على ذلك، لم تكن عمليات التحديث والصيانة تلقائية فيما يتعلق بالممارسات الرئيسية، مثل الاتصالات المشفرة والتحديثات عبر الهواء. وأخيرًا، قدم عدد قليل للغاية من موفري الخدمات القدرة على تصحيح الأجهزة والبوابات عن بُعد بعد التوزيع، مما جعل هذه الأجهزة عرضة للمخاطر الأمنية الناشئة.

على النقيض من ذلك، تتناول AWS قضية الأمان بصورة جادة للغاية، وتدعم الملايين من العملاء النشطاء من مجموعة واسعة من الصناعات والمناطق الجغرافية ذات متطلبات متباينة من السرية وحساسية البيانات. تستثمر AWS موارد كبيرة في ضمان دمج الأمان في كل طبقة من خدماتها، وتوسيع نطاق هذا الأمان ليشمل الأجهزة التي تحتوي على إنترنت الأشياء. تتمثل أولوية AWS في تقديم المساعدة في حماية سرية البيانات وأنظمة العملاء وسلامتها وتوافرها وكذلك توفير منصة آمنة وقابلة للتطوير ومؤَمنة لحلول إنترنت الأشياء.

## التحديات الأمنية

تنطوي المخاطر الأمنية ونقاط الضعف على إمكانية المساس بأمان بيانات العملاء وخصوصيتها في تطبيق إنترنت الأشياء. بالإضافة إلى العدد المتزايد من الأجهزة والبيانات التي تم إنشاؤها، تثير احتمالات الضرر الأسئلة حول كيفية معالجة المخاطر الأمنية التي تفرضها أجهزة إنترنت الأشياء واتصالات الأجهزة من السحابة وإليها.

وتتمركز مخاوف العملاء الشائعة فيما يتعلق بالمخاطر حول أمان البيانات وتشفيرها أثناء نقلها إلى السحابة ومنها، أو أثناء النقل من الخدمات المتطورة إلى الجهاز ومنه، بالإضافة إلى تصحيح الأجهزة، ومصادقة الجهاز والمستخدم، والتحكم في الوصول. يعد تأمين أجهزة إنترنت الأشياء أمرًا ضروريًا، ليس فقط للحفاظ على سلامة البيانات، ولكن أيضًا للحماية من الهجمات التي يمكن أن تؤثر على موثوقية الأجهزة. ونظرًا لأن الأجهزة يمكن أن ترسل كميات كبيرة من البيانات الحساسة عبر الإنترنت، ويتم تمكين المستخدمين النهائيين من التحكم مباشرةً في جهاز ما، فإن أمان «الأشياء» يجب أن يتخلل كل طبقة من الحل.

إن أخبار تسوية البيانات تضع أمان إنترنت الأشياء تحت المزيد من الفحص الدقيق من قِبل العملاء، وتقدم الدروس المستفادة، وتشجع الممارسات الأفضل. يجب أن يكون الأمان هو محور بداية أساس حل إنترنت الأشياء ونهايته، إلى جانب

---

1 حسب https://machinaresearch.com/news/the-global-iot-market-opportunity-will-reach-usd43-trillion-by-2024.

2 راجع https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/249423/bis-13-1217-smart-city-market-opportunties-uk.pdf.

3 راجع https://www.forbes.com/sites/louiscolumbus/2017/01/29/internet-of-things-market-to-reach-267b-by-2020/#c8f8c7609b74.

من خلال استخدام خدمات قادرة على مراجعة تكوينات إنترنت الأشياء باستمرار[4] لضمان عدم انحرافها عن أفضل الممارسات الأمنية. وبمجرد اكتشاف الانحراف، يجب إثارة التنبيهات بحيث يمكن تنفيذ الإجراءات التصحيحية المناسبة - تلقائيًا، بشكل مثالي.

من أجل مواكبة دخول الأجهزة إلى السوق إلى جانب التهديدات القادمة عبر الإنترنت، من الأفضل تطبيق الخدمات التي تعالج كل جزء من المنظومة المتكاملة لإنترنت الأشياء والتداخل في قدرتها على تأمين عمليات توزيع أسطول أجهزة إنترنت الأشياء وحمايتها وتدقيقها ومعالجتها وإدارتها (سواء مع الاتصال بالسحابة أو بدونه).

## كيف تتعامل الحكومات مع قضية أمان إنترنت الأشياء؟

وبينما تعمل مؤسسات القطاع الخاص بنشاط على نشر إنترنت الأشياء في حالات الاستخدام، مثل الرعاية الصحية والإنشاء الصناعي والسلع الاستهلاكية منخفضة الطاقة، تشرع الحكومات على الصعيدين الوطني والمحلي في معالجة قضية استخدام إنترنت الأشياء وأمانه (راجع الملحق 2). بالإضافة إلى تقييم المشهد السياسي المستقبلي لإنترنت الأشياء، تستمر AWS في إضافة الخدمات إلى مختلف أطر العمل الخاصة بالامتثال لمساعدة العملاء في الوفاء بالتزامات الامتثال لديهم (راجع الملحق 3).

## خدمات AWS IoT وإمكانات الأمان الخاصة بها

تقدم AWS مجموعة من خدمات إنترنت الأشياء لمساعدة العملاء في تأمين أجهزتهم واتصالهم وبياناتهم. وتتيح هذه الخدمات للعملاء الفرصة للاستفادة من الأمان الشامل بدءًا من حماية الجهاز إلى حماية البيانات سواء أثناء النقل وأثناء فترة عدم النشاط. كما أنها توفر أيضًا ميزات أمنية من شأنها تمكين تطبيق وتنفيذ سياسات الأمان اللازمة للوفاء بعلامتها المائية الخاصة بالأمان.

توفر AWS IoT وظائف شاملة وعميقة؛ بحيث يتسنى للعملاء تأسيس حلول إنترنت الأشياء لأي حالة استخدام افتراضيًا عبر مجموعة واسعة من الأجهزة. تتكامل AWS IoT مع خدمات الذكاء الاصطناعي (AI) بحيث يتمكن العملاء من جعل الأجهزة أكثر ذكاءً - حتى دون أي اتصال بالإنترنت. تأسست منصة AWS IoT على سحابة AWS، ويستخدمها الملايين من العملاء في 190 دولة، ويمكنها التوسع بسهولة مع زيادة أساطيل أجهزة العملاء وتطور متطلبات أعمالهم. كما توفر AWS IoT ميزات أمان شاملة، بحيث يمكن للعملاء إنشاء سياسات أمنية وقائية والاستجابة الفورية لمشكلات الأمان المحتملة.

توفر AWS IoT خدمات سحابية وبرامج متطورة، مما يمكّن العملاء من توصيل الأجهزة بشكل آمن وجمع البيانات واتخاذ إجراءات ذكية محليًا، حتى عندما يكون الاتصال بالإنترنت معطلاً. وتتيح الخدمات السحابية للعملاء إمكانية الاتصال السريع بالأساطيل الكبيرة والمتنوعة وربطها بأمان، والحفاظ على سلامة الأسطول، والحفاظ على تأمين الأساطيل، واكتشاف الأحداث والاستجابة لها عبر المستشعرات والتطبيقات الخاصة بإنترنت الأشياء. لتسريع تطوير تطبيق إنترنت الأشياء، يمكن للعملاء توصيل الأجهزة وخدمات الويب بسهولة باستخدام واجهة السحب والإفلات. كما يمكن استخدام AWS IoT أيضًا لتحليل البيانات وإنشاء نماذج متطورة لتعلم الآلة (ML). ويمكن توزيع هذه النماذج في السحابة أو وصولاً إلى أجهزة العملاء لجعل الأجهزة أكثر ذكاءً.

4 يمثل التكوين مجموعة من عناصر التحكم التقنية يعدها العملاء للمساعدة في الحفاظ على أمان المعلومات عند اتصال الأجهزة مع بعضها البعض ومع السحابة.

على الرغم من أن خدمات AWS IoT الحالية[5] تتراوح على نطاق واسع للسماح بإيجاد حلول مبتكرة وشاملة لإنترنت الأشياء، تركز وثيقة المعلومات هذه على الخدمات الخمس التالية، والتي تعد خدمات أساسية لأمان إنترنت الأشياء. وترد أدناه مواصفات الخدمة وميزات الأمان بمزيد من التفصيل.

- **Amazon FreeRTOS** هو نظام تشغيل مفتوح المصدر لوحدات التحكم الدقيقة التي تجعل أجهزة التوصيل الطرفية الصغيرة ذات الطاقة المنخفضة سهلة البرمجة والتوزيع والتأمين والاتصال والإدارة.
- **AWS IoT Greengrass** هو برنامج يتيح للعملاء تشغيل الحوسبة المحلية، والمراسلة، والتخزين المؤقت للبيانات، والمزامنة، وإمكانات واجهة التعلم الآلي على الأجهزة المتصلة.
- **AWS IoT Core** عبارة عن خدمة سحابية مُدارة تتيح للأجهزة المتصلة التفاعل بسهولة وأمان مع التطبيقات السحابية والأجهزة الأخرى.
- **AWS IoT Device Management** عبارة عن خدمة إدارة الأجهزة المستندة إلى السحابة التي تجعل من السهل ربط أجهزة إنترنت الأشياء وتنظيمها ومراقبتها وإدارتها عن بُعد على نطاق واسع.
- **AWS IoT Device Defender** عبارة عن خدمة أمان إنترنت الأشياء التي تراقب تكوينات إنترنت الأشياء للعملاء وتدققها بصفة مستمرة للتأكد من أنها لا تحيد عن أفضل الممارسات الأمنية.

## Amazon FreeRTOS – برنامج الجهاز

**نظرة عامة على الخدمة:** Amazon FreeRTOS (a:FreeRTOS) هو نظام تشغيل مفتوح المصدر لوحدات التحكم الدقيقة[6] يجعل أجهزة التوصيل الطرفية ذات الطاقة المنخفضة سهلة البرمجة والتوزيع والتأمين والاتصال والإدارة. يعتمد Amazon FreeRTOS على نواة FreeRTOS، وهو نظام تشغيل شائع مفتوح المصدر لوحدات التحكم الدقيقة، ويمكن توسعته من خلال مكتبات البرامج التي تجعل من السهل توصيل أجهزة العملاء الصغيرة ومنخفضة الطاقة بأمان وبصورة مباشرة بخدمات سحابة AWS، مثل AWS IoT Core ، أو توصيلها بأجهزة توصيل طرفية أكثر قوة تقوم بتشغيل AWS IoT Greengrass.

**إمكانات الأمان:** يأتي Amazon FreeRTOS مزودًا بمكتبات للمساعدة في تأمين بيانات الجهاز واتصالاته، بما في ذلك دعم تشفير البيانات وإدارة المفاتيح. يشتمل Amazon FreeRTOS على دعم بروتوكول أمان طبقة النقل (1.2TLS v) لمساعدة الأجهزة في الاتصال بالسحابة بشكل آمن. يحتوي Amazon FreeRTOS أيضًا على ميزة توقيع التعليمات البرمجية لضمان عدم تعرض التعليمة البرمجية لجهاز العميل للخطر أثناء التوزيع، بالإضافة إلى إمكانات تحديثات OTA لتحديث الأجهزة عن بُعد باستخدام تحسينات الميزات أو تصحيحات الأمان.

---

5 تشتمل خدمات AWS IoT على Amazon FreeRTOS و AWS IoT Greengrass و AWS IoT Core و AWS IoT Device Management و AWS IoT Device Defender و AWS IoT Things Graph و AWS IoT Analytics و AWS IoT SiteWise و AWS IoT Events. لمزيد من المعلومات، يرجى زيارة https://aws.amazon.com/iot.

6 وحدة التحكم الدقيقة عبارة عن رقاقة واحدة تحتوي على معالج بسيط يمكن العثور عليها في العديد من الأجهزة، بما في ذلك الأجهزة المنزلية وأجهزة تتبع اللياقة البدنية ومستشعرات الأتمتة الصناعية والسيارات. ويمكن أن تستفيد العديد من هذه الأجهزة الصغيرة من الاتصال بالسحابة أو الاتصال محليًا بأجهزة أخرى. فعلى سبيل المثال، تحتاج عدادات الكهرباء الذكية إلى الاتصال بالسحابة للإبلاغ عن الاستخدام، وتحتاج أنظمة أمان المباني إلى الاتصال محليًا بحيث يتم فتح الباب عند دخول شخص ما.

# AWS IoT Greengrass – برنامج لحوسبة التخزين المؤقت

**نظرة عامة على الخدمة:** AWS IoT Greengrass عبارة عن برنامج يتيح للعملاء تشغيل الحوسبة المحلية والمراسلة والتخزين المؤقت للبيانات والمزامنة وإمكانات واجهة تعلم الآلة للأجهزة المتصلة،[7] مما يسمح للأجهزة المتصلة بالعمل حتى مع الاتصال المتقطع بالسحابة. وبمجرد إعادة توصيل الجهاز، يقوم AWS IoT Greengrass بمزامنة البيانات الموجودة على الجهاز مع AWS IoT Core، مما يوفر وظائف ثابتة بغض النظر عن الاتصال. ويعمل برنامج AWS IoT Greengrass على توسيع AWS بسلاسة لتصل إلى الأجهزة بحيث تتمكن من العمل محليًا على البيانات التي أنشأتها، مع الاستمرار في استخدام السحابة للإدارة والتحليلات والتخزين الدائم.

**إمكانات الأمان:** يقوم برنامج AWS IoT Greengrass بمصادقة بيانات الجهاز وتشفيرها لكل من الاتصالات المحلية والسحابية على السواء، ولا يتم تبادل البيانات أبدًا بين الأجهزة والسحابة دون هوية مثبتة. وتستخدم الخدمة إدارة الأمان والوصول على غرار ما اعتاد عليه العملاء في AWS IoT Core، مع مصادقة الجهاز المتبادل وترخيصه، والاتصال الآمن بالسحابة.

وبشكل أكثر تحديدًا، يستخدم AWS IoT Greengrass شهادات X.509[8] والاشتراكات المُدارة وسياسات AWS IoT وسياسات AWS Identity and Access Management (IAM) والأدوار لضمان تأمين تطبيقات AWS IoT Greengrass. تتطلب أجهزة AWS IoT وجود AWS IoT Thing وشهادة الجهاز وسياسة AWS IoT للاتصال بخدمة AWS IoT Greengrass. ويؤدي ذلك إلى السماح لأجهزة AWS IoT Greengrass الأساسية بالاتصال بشكل آمن بخدمة سحابة AWS IoT. كما تسمح أيضًا لخدمة سحابة AWS IoT Greengrass بنشر معلومات التكوين ووظائف AWS Lambda والاشتراكات المُدارة لأجهزة AWS IoT Greengrass الأساسية. وبالإضافة إلى ذلك، يوفر AWS IoT Greengrass تخزين المفاتيح الخاصة لجذر الثقة لأجهزة التوصيل الطرفية.

تتمثل إمكانات الأمان المهمة الأخرى لبرنامج AWS IoT Greengrass في الرصد والتسجيل. فعلى سبيل المثال، يمكن للبرامج الأساسية في الخدمة كتابة سجلات إلى Amazon CloudWatch[9] (الذي يعمل أيضًا من أجل AWS IoT Core) وإلى نظام الملفات المحلي للأجهزة الأساسية للعملاء. ويتم تكوين التسجيل على مستوى المجموعة، وتشتمل جميع إدخالات سجلات AWS IoT Greengrass على طابع زمني ومستوى سجل ومعلومات حول الحدث. تم دمج AWS IoT Greengrass مع AWS CloudTrail[10] - وهي خدمة توفر سجلاً للإجراءات التي اتخذها مستخدم أو دور أو خدمة AWS في AWS IoT Greengrass - وإذا تم تنشيطها من قبل العميل، فإنها تلتقط جميع استدعاءات واجهة برمجة التطبيقات (API) لبرنامج AWS IoT Greengrass كأحداث. ويتضمن ذلك الاستدعاءات من وحدة تحكم AWS IoT Greengrass واستدعاءات التعليمات البرمجية إلى عمليات واجهة برمجة التطبيقات لبرنامج AWS IoT Greengrass. فعلى سبيل المثال، يمكن للعملاء إنشاء سجل متابعة، ويمكن للاستدعاءات تمكين التوصيل المستمر لأحداث AWS CloudTrail إلى حاوية Amazon Simple Storage Service (Amazon S3) ، بما في ذلك أحداث AWS IoT Greengrass. إذا لم يرغب العملاء في إنشاء سجل متابعة، يمكنهم عرض آخر الأحداث في وحدة تحكم AWS CloudTrail في سجل الأحداث (في حالة التمكين). يمكن استخدام هذه المعلومات للقيام بعدد من الأمور، مثل تحديد وقت تقديم طلب إلى AWS IoT Greengrass وعنوان IP الذي تم تقديم الطلب منه.

---

7 من أجل البدء في استخدام AWS IoT Greengrass، سيحتاج العملاء إلى جهاز قادر على تشغيل البرنامج الأساسي لـ AWS IoT Greengrass. هناك قائمة كاملة من الأجهزة المؤهلة والتبعيات التقنية هنا. انقر هنا للحصول على دليل بدء الاستخدام العملي. يمكن للعملاء العثور على مرجع مطور مفصل هنا.

8 شهادات X.509 هي شهادات رقمية تستخدم معيار البنية التحتية للمفتاح العام X.509 لربط مفتاح عام بهوية واردة في الشهادة. ويتم إصدار شهادات X.509 من قبل كيان موثوق به يسمى المرجع المصدق (CA). ويحتفظ المرجع المصدق بشهادة خاصة واحدة أو أكثر تسمى شهادات المرجع المصدق والتي يستخدمها لإصدار شهادات X.509. يتمتع المرجع المصدق وحده بحق الوصول إلى شهادات المرجع المصدق. راجع https://docs.aws.amazon.com/iot/latest/developerguide/x509-certs.html لمزيد من المعلومات.

9 راجع https://aws.amazon.com/cloudwatch.

10 راجع https://aws.amazon.com/cloudtrail.

تتوفر خيارات أفضل الممارسات لتأمين بيانات العملاء على الجهاز، ويجب استخدامها كلما أمكن ذلك. بالنسبة لبرنامج AWS IoT Greengrass، يجب على جميع أجهزة إنترنت الأشياء تمكين التشفير الكامل للقرص واتباع أفضل الممارسات لإدارة المفاتيح. يمكن للعملاء الاستفادة من التشفير الكامل للقرص، وذلك باستخدام مفاتيح AES 256 بت استنادًا إلى خوارزميات NIST FIPS 140-2 التي تم التحقق منها[11] واتباع أفضل الممارسات لإدارة المفاتيح. بالنسبة للأجهزة منخفضة الطاقة مثل تلك التي تستخدم Amazon FreeRTOS، يمكن للعملاء اتباع توصيات التشفير خفيف الوزن NIST 8114[12].

تناولت الأقسام المذكورة أعلاه وحدات التحكم الدقيقة وحالات الاستخدام الطرفية. سيركز هذا المستند أدناه على خدمات إنترنت الأشياء التي تعمل في السحابة.

## AWS IoT Core – بوابة إنترنت الأشياء المستندة إلى السحابة

**نظرة عامة على الخدمة:** AWS IoT Core هي خدمة سحابية مُدارة تتيح للأجهزة المتصلة التفاعل بسهولة وأمان مع تطبيقات السحابة والأجهزة الأخرى. وتوفر AWS IoT Core الاتصالات والمعالجة الآمنة للبيانات عبر أنواع مختلفة من الأجهزة والمواقع المتصلة بحيث يمكن للعملاء إنشاء تطبيقات إنترنت الأشياء بسهولة. وتتضمن أمثلة حالات استخدام العملاء الحلول الصناعية والحلول المنزلية المتصلة، مع القدرة على دعم مليارات الأجهزة وتريليونات الرسائل التي يمكن معالجتها وتوجيهها إلى نقاط نهاية AWS والأجهزة الأخرى بشكل موثوق وآمن.

**إمكانات الأمان:** تقدم AWS IoT Core عددًا من الحلول للعملاء والتي تساعد في تمكين الأمان والحفاظ عليه. تحمي آليات أمان سحابة AWS البيانات أثناء انتقالها بين AWS IoT والأجهزة الأخرى أو خدمات AWS. ويمكن للأجهزة الاتصال باستخدام مجموعة متنوعة من خيارات الهوية (شهادات X.509 أو مستخدمو IAM ومجموعاته أو هويات Amazon Cognito أو الرموز المميزة للمصادقة المخصصة) عبر اتصال آمن. على الرغم من إجراء العملاء لعمليات التحقق من جانب العميل (أي سلسلة التحقق من صحة الثقة، والتحقق من اسم المضيف، والتخزين الآمن، وتوزيع مفاتيحهم الخاصة)، فإن خدمة AWS IoT Core توفر قنوات نقل آمنة باستخدام TLS. كما يقوم محرك قواعد AWS IoT بإعادة توجيه بيانات الجهاز إلى الأجهزة الأخرى وخدمات AWS وفقًا للقواعد المحددة من قِبل العميل. ويتم استخدام أنظمة إدارة الوصول من AWS لنقل البيانات بشكل آمن إلى وجهتها النهائية. ثمة ميزة تصريح AWS IoT أخرى جديرة بالملاحظة تتمثل في متغيرات سياسة AWS IoT، والتي تساعد في تجنب توفير بيانات الاعتماد المتميزة بشكل مفرط إلى جهاز ما. تعمل هذه الميزات، المستخدمة جنبًا إلى جنب مع أفضل الممارسات العامة للأمن السيبراني، على حماية بيانات العملاء.

11 خوارزميات التشفير المعتمدة لـ NIST FIPS 140-2: https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402annexa.pdf.

12 NIST 8114 - التشفير خفيف الوزن: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf.

# AWS IoT Device Management – خدمة إدارة أجهزة إنترنت الأشياء المستندة إلى السحابة

**نظرة عامة على الخدمة:** تساعد AWS IoT Device Management العملاء في ربط أجهزة إنترنت الأشياء وتنظيمها ومراقبتها وإدارتها عن بُعد على نطاق واسع. وتتكامل AWS IoT Device Management مع AWS IoT Core لتوصيل الأجهزة بسهولة إلى السحابة والأجهزة الأخرى بحيث يمكن للعملاء إدارة أساطيل أجهزتهم عن بُعد. تساعد AWS IoT Device Management العملاء في ربط الأجهزة الجديدة باستخدام AWS IoT داخل وحدة الإدارة في AWS أو واجهة برمجة التطبيقات لتحميل القوالب التي يزودونها بمعلومات، مثل الشركة المصنعة للجهاز أو الرقم التسلسلي أو شهادات الهوية X.509 أو سياسات الأمان. بعد ذلك، يمكن للعملاء تكوين أسطول كامل من الأجهزة باستخدام هذه المعلومات من خلال بضع نقرات في AWS IoT داخل وحدة الإدارة في AWS.

**إمكانات الأمان:** من خلال AWS IoT Device Management، يمكن للعملاء تجميع أسطول أجهزتهم في بنية هرمية تستند إلى الوظيفة أو متطلبات الأمان أو الفئات المشابهة. يمكنهم تجميع جهاز واحد في غرفة، أو أجهزة متعددة في نفس الطابق، أو جميع الأجهزة التي تعمل داخل المبنى. يمكن بعد ذلك استخدام هذه المجموعات لإدارة سياسات الوصول أو عرض المقاييس التشغيلية أو تنفيذ الإجراءات عبر المجموعة بأكملها. بالإضافة إلى ذلك، يمكن لميزة تعرف باسم «الأشياء الديناميكية» إضافة الأجهزة التي تلبي المعايير المحددة من قبل العميل وإزالة الأجهزة التي لم تعد تناسب المتطلبات بشكل تلقائي. ويعمل ذلك على تبسيط العملية بشكل آمن مع الحفاظ على سلامة التشغيل. كما تسهل ميزة «الأشياء الديناميكية» العثور على سجلات الأجهزة المستندة إلى أي مجموعة من سمات الأجهزة، وتسمح للعملاء بإجراء تحديثات مجمعة.

باستخدام AWS IoT Device Management، يتسنى للعملاء أيضًا دفع البرامج والبرامج الثابتة إلى الأجهزة في هذا المجال لتصحيح الثغرات الأمنية وتحسين وظائف الجهاز؛ وتطبيق التحديثات المجمعة؛ والتحكم في سرعة التوزيع؛ وتعيين حدود الفشل؛ وتحديد المهام المستمرة لتحديث برامج الجهاز تلقائيًا بحيث يتم دائمًا تشغيل أحدث إصدار من البرامج. ويمكن للعملاء إرسال الإجراءات عن بُعد، مثل إعادة تشغيل الجهاز أو إعادة تعيين إعدادات المصنع، لإصلاح مشكلات البرامج في الجهاز أو استعادة الجهاز إلى إعداداته الأصلية. ويمكن للعملاء أيضًا التوقيع رقميًا على الملفات التي يتم إرسالها إلى أجهزتهم، مما يساعد في ضمان عدم تعرض الأجهزة للخطر.

لا تقتصر القدرة على دفع تحديثات البرامج على الخدمات السحابية فقط. ففي الواقع، تتيح مهام تحديث OTA في FreeRTOS Amazon للعملاء استخدام AWS IoT Device Management لجدولة تحديثات البرامج. وبالمثل، يمكن للعملاء أيضًا إنشاء مهمة التحديث الأساسية لبرنامج IoT Greengrass AWS لجهاز واحد أو أكثر من الأجهزة الأساسية التي تقوم بتشغيل AWS IoT Greengrass باستخدام AWS IoT Device Management من أجل نشر التحديثات الأمنية وإصلاح الأخطاء والميزات الجديدة لبرنامج AWS IoT Greengrass للأجهزة المتصلة.

# AWS IoT Device Defender – خدمة أمان أجهزة إنترنت الأشياء المستندة إلى السحابة

**نظرة عامة على الخدمة:** AWS IoT Device Defender عبارة عن خدمة مُدارة بالكامل من شأنها مساعدة العملاء في تدقيق ميزات الأمان المعدة لأسطول أجهزة إنترنت الأشياء لديهم. وتقوم الخدمة باستمرار بمراجعة تكوينات إنترنت الأشياء لضمان عدم انحراف التكوينات عن أفضل ممارسات الأمان للحفاظ على تكوينات إنترنت الأشياء وتطبيقها - مثل ضمان هوية الجهاز ومصادقة الأجهزة وترخيصها وتشفير بيانات الجهاز. يمكن أن ترسل الخدمة تنبيهًا إذا كانت هناك أي ثغرات في تكوين إنترنت الأشياء لدى العميل مما قد يؤدي إلى حدوث خطر أمني، مثل شهادات الهوية التي تتم مشاركتها عبر أجهزة متعددة أو جهاز ذي شهادة هوية تم إبطالها يحاول الاتصال بـ AWS IoT Core.

**إمكانات الأمان:** بالإضافة إلى إمكانات مراقبة الخدمة وتدقيقها، يمكن للعملاء تعيين التنبيهات التي تتخذ إجراءات لتصحيح أي انحرافات موجودة في الأجهزة. فعلى سبيل المثال، قد تشير الزيادة في حركة المرور الصادرة إلى مشاركة جهاز في هجمة رفض الخدمة الموزعة (DDoS). ويندمج برنامج AWS IoT Greengrass وبرنامج Amazon FreeRTOS أيضًا تلقائيًا مع AWS IoT Device Defender لتوفير مقاييس الأمان من الأجهزة للتقييم.

يمكن لخدمة AWS IoT Device Defender إرسال تنبيهات إلى AWS IoT وAmazon CloudWatch و Amazon Simple Notification (Service Amazon SNS) مع نشر التنبيهات إلى مقاييس Amazon CloudWatch. وإذا قرر أحد العملاء معالجة تنبيه ما، يمكن استخدام خدمة AWS IoT Device Management لاتخاذ إجراءات تخفيفية، مثل دفع إصلاحات الأمان.

تقوم خدمة AWS IoT Device Defender بتدقيق تكوينات إنترنت الأشياء المقترنة بأجهزة العملاء في ضوء مجموعة من أفضل الممارسات لأمان إنترنت الأشياء المحددة بحيث يتمكن العملاء من معرفة الثغرات الأمنية وتشغيل عمليات التدقيق على بصفة مستمرة أو مخصصة. وهناك أيضًا ممارسات أمنية داخل AWS IoT Device Defender يمكن اختيارها وتشغيلها كجزء من عملية التدقيق. وتتكامل هذه الخدمة أيضًا مع خدمات AWS الأخرى - مثل Amazon CloudWatch وAmazon SNS - لإرسال تنبيهات أمان إلى AWS IoT عند فشل التدقيق أو عند اكتشاف حالات شاذة للسلوك بحيث يتمكن العملاء من التحقيق وتحديد السبب الجذري. فعلى سبيل المثال، يمكن لخدمة AWS IoT Device Defender تنبيه العملاء عند وصول هويات الأجهزة إلى واجهات برمجة التطبيقات الحساسة. ويمكن لخدمة AWS IoT Device Defender أيضًا التوصية بالإجراءات التي تقلل من تأثير مشكلات الأمان، مثل إبطال الأذونات أو إعادة تشغيل الجهاز أو إعادة ضبط إعدادات المصنع الافتراضية أو دفع إصلاحات الأمان إلى أي من الأجهزة المتصلة للعملاء.

قد يشعر العملاء بالقلق أيضًا إزاء الجهات الفاعلة السيئة؛ حيث يمكن للأخطاء البشرية أو المتعلقة بالنظام والمستخدمين المصرح لهم الذين لديهم نوايا ضارة إدخال تكوينات ذات تأثيرات أمنية سلبية. يوفر AWS IoT Core عناصر الأمان الأساسية للعملاء لتوصيل الأجهزة بالسحابة والأجهزة الأخرى بأمان. تسمح العناصر الأساسية بفرض الضوابط الأمنية، مثل المصادقة والتخويل وتسجيل التدقيق والتشفير الشامل. بعد ذلك، تتدخل خدمة AWS IoT Device Defender وتساعد في تدقيق تكوينات الأمان بشكل مستمر للامتثال إلى أفضل الممارسات الأمنية وسياسات الأمان المؤسسية الخاصة بالعملاء.

## الاستفادة من الأمان المبرهن لتعزيز إنترنت الأشياء - أداة تمييز في الصناعة

يجري تأسيس خدمات وتقنيات الأمان الجديدة في AWS لمساعدة الشركات في تأمين أجهزة التوصيل الطرفية وأجهزة إنترنت الأشياء لديها. وعلى وجه الخصوص، قامت AWS مؤخرًا بتشغيل عمليات الفحص داخل AWS IoT Device Defender، المدعومة بتقنية الذكاء الاصطناعي المعروفة باسم «المنطق الآلي»، والتي تستفيد من البراهين الرياضية للتحقق من كتابة البرنامج بشكل صحيح وتحديد ما إذا كان هناك وصول غير مقصود إلى الأجهزة. وتعد خدمة AWS IoT Device Defender مثالاً على طريقة استخدام العملاء للمنطق الآلي مباشرةً لتأمين أجهزتهم الخاصة. وعلى المستوى الداخلي، استخدمت AWS المنطق الآلي للتحقق من سلامة الذاكرة من التعليمات البرمجية التي تعمل على Amazon FreeRTOS والحماية من البرامج الضارة. ويتمكن العملاء من تشغيل أعباء العمل الحساسة على AWS من خلال الاستثمار في المنطق الآلي لتوفير ضمان قابل للتطوير للبرامج الآمنة، والذي يُشار إليه باسم «الأمان المبرهن».

يستخدم AWS Zelkova[13] المنطق الآلي لإثبات أن ضوابط الوصول إلى بيانات العملاء تعمل على النحو المنشود. ويتم تشغيل فحوصات التحكم في الوصول في AWS IoT Device Defender بواسطة Zelkova، مما يسمح للعملاء بضمان حماية بياناتهم بشكل مناسب. تعتبر سياسة AWS IoT متساهلة بشكل مفرط إذا كانت تمنح الوصول إلى الموارد خارج تكوين الأمان المنشود للعميل. إن الضوابط التي تعمل بواسطة Zelkova، والتي تم تخزينها في AWS IoT Device Defender، تتحقق من أن السياسات لا تسمح بالإجراءات المقيدة بتكوين أمان العميل وأن الموارد المخصصة تتمتع بأذونات لتنفيذ إجراءات معينة.

ساعدت الأدوات الأخرى المستندة إلى المنطق الآلي في تأمين أسس البنية التحتية لـ AWS IoT. ثمة أداة مفتوحة المصدر تسمى CBMC تم استخدامها لإثبات صحة Amazon FreeRTOS، مما يوفر ثقة أكبر للعملاء لتشغيل أعباء العمل على أجهزة Amazon IoT. ويضمن ذلك عدم تمكن أي مهاجم من استغلال الوصول غير المصرح به إلى Amazon FreeRTOS أو الحصول عليه. ويتم دمج آليات التحكم في المنطق الآلي في Amazon FreeRTOS بشكل مستمر كعمليات فحص للتحقق من التحديثات التي تم إجراؤها على نظام التشغيل. ويضمن ذلك أنه في كل مرة يتم إجراء تغيير التعليمة البرمجية، يتم وضع التدابير بحيث يمكن لمطوري AWS التحقق تلقائيًا من أن برنامج Amazon FreeRTOS بذاكرة آمنة.

يستمر تطبيق المنطق الآلي عبر مجموعة متنوعة من خدمات وميزات AWS، مما يوفر مستويات عالية من ضمان الأمان للعناصر الحيوية في سحابة AWS. وتواصل AWS نشر المنطق الآلي لتطوير أدوات للعملاء إلى جانب تقنية التحقق من البنية التحتية الداخلية لمكدس AWS IoT.

## ما أفضل الممارسات الرئيسية لأمان إنترنت الأشياء؟

على الرغم من عدد أفضل الممارسات المتوفرة، فإنه لا يوجد نهج واحد يناسب الجميع للتخفيف من حدة المخاطر على حلول إنترنت الأشياء. ووفقًا للجهاز والنظام والخدمة والبيئة التي يتم فيها نشر الأجهزة، توجد تهديدات ونقاط ضعف وتجاوزات مختلفة للمخاطر يجب على العملاء وضعها في الاعتبار. وفيما يلي الممارسات الموصى بها عند دمج الأمان الشامل عبر البيانات والأجهزة والخدمات السحابية:

1. **دمج الأمان في مرحلة التصميم**

يعد الأمان محور بداية ونهاية أساس حل إنترنت الأشياء. ونظرًا لأن الأجهزة قد ترسل كميات كبيرة من البيانات الحساسة، وقد يتمتع المستخدمون النهائيون لتطبيقات إنترنت الأشياء أيضًا بالقدرة على التحكم المباشر في الجهاز، فيجب أن يكون أمان «الأشياء» مطلبًا منتشرًا للتصميم. لا يشكل الأمان صيغة ثابتة؛ ويجب أن تتحلى تطبيقات إنترنت الأشياء بالقدرة على نمذجة أفضل الممارسات الأمنية ورصدها وتكرارها باستمرار. يتمثل أحد التحديات التي تواجه أمان إنترنت الأشياء في دورة حياة جهاز فعلي والأجهزة المقيدة لأجهزة الاستشعار ووحدات التحكم الدقيقة ووحدات التشغيل والمكتبات المضمنة. قد تحد هذه العوامل المقيدة من إمكانات الأمان التي يمكن أن يؤديها كل جهاز. باستخدام هذه الديناميات الإضافية، يجب على حلول إنترنت الأشياء تكييف تصميمها وبرامجها الثابتة وبرمجياتها باستمرار بحيث تظل في طليعة المشهد الأمني المتغير. على الرغم من أن العوامل المقيدة للأجهزة يمكن أن تشكل مخاطر متزايدة وعقبات و وحلول تسوية محتملة بين الأمان والتكلفة، فإن إعداد حل آمن لإنترنت الأشياء يجب أن يكون الهدف الرئيسي لأي مؤسسة.

---

13 لمعرفة المزيد عن Zelkova، يرجى زيارة https://aws.amazon.com/blogs/security/protect-sensitive-data-in-the-cloud-with-automated-reasoning-zelkova/.

2. **تعمل هذه الميزات، المستخدمة جنبًا إلى جنب مع أطر الأمن السيبراني وأمن تقنية المعلومات، لتمكن**

AWS من تدعيم نهجًا منفتحًا يستند إلى المعايير لتعزيز الاستخدام الآمن لإنترنت الأشياء. وعند النظر في مليارات الأجهزة ونقاط الاتصال اللازمة لدعم منظومة قوية متكاملة لإنترنت الأشياء للاستخدام على مستوى قطاع المستهلك والقطاع الصناعي والقطاع العام، تعتبر قابلية التشغيل البيني أمرًا حيويًا. ولذلك، تلتزم خدمات AWS IoT ببروتوكولات معايير الصناعة وأفضل الممارسات. وبالإضافة إلى ذلك، يدعم AWS IoT Core البروتوكولات الأخرى ذات المعايير الصناعية والمخصصة، مما يسمح للأجهزة بالاتصال مع بعضها البعض حتى لو كانت تستخدم بروتوكولات مختلفة. تعد AWS مؤيدًا قويًا لقابلية التشغيل البيني بحيث يمكن للمطورين الاستفادة من أفضل المنصات الحالية لدعم احتياجات العملاء المتطورة. كما تدعم AWS أيضًا منظومة متكاملة شريكة مزدهرة لتوسيع قائمة الخيارات وبسط حدود ما هو ممكن للعملاء. ينطوي تطبيق أفضل الممارسات المعترف بها عالميًا على عدد من الفوائد عبر جميع الجهات المعنية في إنترنت الأشياء، بما في ذلك:

- التكرار وإعادة الاستخدام، بدلاً من إعادة التشغيل وإعادة الإجراءات
- الاتساق وتوافق الآراء لتعزيز التوافق بين التقنية وقابلية التشغيل البيني عبر الحدود الجغرافية
- تحقيق أقصى قدر من الكفاءة لتسريع تحديث تقنية المعلومات وتحولها

3. **التركيز على الأثر من أجل منح الأولوية للتدابير الأمنية**

لا تتطابق الهجمات أو حالات الشذوذ، وقد لا يكون لها نفس التأثير على الأشخاص والعمليات التجارية والبيانات. يؤدي فهم النظم المتكاملة لإنترنت الأشياء للعملاء وموضع تشغيل الأجهزة داخل هذه المنظومة المتكاملة إلى توجيه القرارات بشأن مواضع أكبر المخاطر — سواء داخل الجهاز، باعتباره جزءًا من الشبكة، أو المكون المادي أو الأمان. إن التركيز على تقييم أثر المخاطر وعواقبها أمر بالغ الأهمية لتحديد المجالات التي ينبغي فيها توجيه الجهود الأمنية إلى جانب الجهة المسؤولة عن تلك الجهود في المنظومة المتكاملة لإنترنت الأشياء.

# الخاتمة

جنبًا إلى جنب مع النمو الهائل في الأجهزة المتصلة، فإن كل «شيء» في إنترنت الأشياء ينقل حزمًا من البيانات التي تتطلب إمكانية اتصال وتخزين وأمان موثوق بها. في ظل وجود إنترنت الأشياء، تواجه المؤسسة تحديات في إدارة كميات هائلة من البيانات والاتصالات من الأجهزة المنتشرة ورصدها وتأمينها. ولكن هذا التحدي لا يجب أن يكون حجر عثرة في بيئة تستند إلى السحابة. بالإضافة إلى توسيع نطاق الحل ونموه في موقع واحد، تعمل الحوسبة السحابية على تمكين حلول إنترنت الأشياء من التوسع عالميًا وعبر مواقع فعلية مختلفة مع تقليل زمن انتقال الاتصالات والسماح باستجابة أفضل من الأجهزة في هذا المجال. تقدم AWS مجموعة من خدمات إنترنت الأشياء المزودة بأمان شامل، بما في ذلك خدمات التشغيل وتأمين نقاط النهاية والبوابات والمنصات والتطبيقات، بالإضافة إلى عبور حركة المرور عبر هذه الطبقات. يعمل هذا التكامل على تبسيط الاستخدام الآمن وإدارة الأجهزة والبيانات التي تتفاعل باستمرار مع بعضها البعض، مما يسمح للمؤسسات بالاستفادة من الابتكار والكفاءات التي يمكن أن تقدمها إنترنت الأشياء مع الحفاظ على الأمان باعتباره أولوية.

# الملحق 1 - تكامل خدمات AWS IoT

تندمج AWS IoT مباشرةً مع خدمات AWS التالية:

- **Amazon Simple Storage Service (Amazon S3)** توفر إمكانية تخزين قابلة للتطوير في سحابة AWS. للمزيد من المعلومات، راجع Amazon S3.
- **Amazon DynamoDB** يوفر قواعد بيانات NoSQL مُدارة. لمزيد من المعلومات، راجع Amazon DynamoDB.
- **Amazon Kinesis** يتيح معالجة البيانات المتدفقة في الوقت الحقيقي على نطاق واسع. للمزيد من المعلومات، راجع Amazon Kinesis.
- **AWS Lambda** تقوم بتشغيل التعليمة البرمجية للعملاء على الخوادم الافتراضية من Amazon Elastic Compute Cloud (Amazon EC2) كاستجابة للأحداث. لمزيد من المعلومات، راجع AWS Lambda.
- **Amazon Simple Notification Service (Amazon SNS)** ترسل الإشعارات أو تتلقاها. للمزيد من المعلومات، راجع Amazon SNS.
- **Amazon Simple Queue Service (Amazon SQS)** تقوم بتخزين البيانات في قائمة انتظار ليتم استردادها بواسطة التطبيقات. للمزيد من المعلومات، راجع Amazon SQS.

# الملحق 2 - كيفية تعامل الحكومات مع إنترنت الأشياء

## الولايات المتحدة

### المعهد الوطني للمعايير والتقنية (NIST) — وزارة التجارة

تقود وزارة التجارة في الولايات المتحدة جهودًا متعددة لمعالجة أمان إنترنت الأشياء. ونشر المعهد الوطني للمعايير والتقنية (NIST) وثيقة معلومات[14] تسلط الضوء على الموضوعات التي يأخذها كل من العملاء والوكالات الحكومية بعين الاعتبار عند تقييم أمان البيانات والأجهزة. وتتم دعوة القراء في هذه الوثيقة إلى تقييم هذه المخاوف، فضلاً عن تقديم توصيات لهم بشأن كيفية التخفيف من حدة المشكلات. وأصدر المعهد تقريرًا داخليًا NISTIR 8228[15]، الذي يحدد المخاطر التي قد تؤثر سلبًا على استخدام إنترنت الأشياء. وتقدم الوثيقة أيضًا توصيات لتخفيف آثار هذه المخاوف أو الحد منها. كما يعقد المعهد شراكات بين القطاعين العام والخاص، ويلتمس التعليقات، ويستضيف ورش عمل تتعلق بالمدن الذكية والتوحيد القياسي الدولي لإنترنت الأشياء، من بين مجموعة من المبادرات الأخرى. [16] وعلى الرغم من أن حداثة المجال، فإن المؤشرات المبكرة تشير إلى المخاطر المحتملة للأمن السيبراني والخصوصية باعتبارها تحديات خطيرة للمكاسب التي يمكن للحكومات والمستهلكين الاستفادة منها من خلال إنترنت الأشياء.

### وزارة الدفاع

ثمة مثال آخر داخل الحكومة يتجسد في وزارة الدفاع. في عام 2016، أصدر كبير مسؤولي المعلومات بوزارة الدفاع الأمريكية توصيات السياسة لمعالجة نقاط الضعف والمخاطر الخاصة بإنترنت الأشياء.[17] و وفقًا لتوصية السياسة، توفر وزارة الدفاع بالفعل الملايين من أجهزة الاستشعار والأجهزة الخاصة بإنترنت الأشياء عبر مرافق وزارة الدفاع ومركباتها وأجهزتها الطبية، كما تفكر حاليًا في دمجها في نظم الأسلحة والاستخبارات. وينبع تعقيد تأمين إنترنت الأشياء من قوة المعالجة المحدودة للأجهزة لتشغيل جدران الحماية وبرامج مكافحة البرامج الضارة، فضلاً عن العدد الهائل من الأجهزة، مما يضاعف مخاطر التعرض إلى مستوى مختلف عن الأجهزة المحمولة التقليدية.

يشتمل النهج الذي أوصت به وزارة الدفاع وإجراءات السياسة المعنية بمعالجة المخاطر الأمنية لإنترنت الأشياء على ما يلي: 1) تحليل مخاطر الأمان والخصوصية الذي يدعم كل تنفيذ لإنترنت الأشياء وتدفقات البيانات المرتبطة بها، و2) التشفير في كل نقطة، حيث تتناسب التكاليف مع المخاطر والقيمة، و3) مراقبة شبكات إنترنت الأشياء لتحديد حركة المرور غير العادية والتهديدات الناشئة.

### لجنة التجارة الفيدرالية (FTC)

لقد كانت لجنة التجارة الفيدرالية مشاركًا مهمًا في المناقشات التي تعلقت بأمان إنترنت الأشياء، ومتابعة اتخاذ إجراءات ضد مصنعي الأجهزة الذين أظهروا إهمالاً في الوفاء بالتزامات الأمان لديهم أو كانوا مثالاً سيئًا على ذلك.

---

14 جيفري فواس (المعهد الوطني للمعايير والتقنية)، وريتشارد كون (المعهد الوطني للمعايير والتقنية)، وفيليب لابلانت (جامعة ولاية بنسلفانيا)، وصوفيا أبلباوم (شركة MITRE)، «مخاوف الثقة المتعلقة بإنترنت الأشياء» (16 أكتوبر 2018، https://csrc.nist.gov/publications/detail/white-paper/2018/10/17/iot-trust-concerns/draft.)

15 NISTIR 8228، «اعتبارات إدارة مخاطر الخصوصية والأمن السيبراني لإنترنت الأشياء للتعليق العام» (26 سبتمبر 2018، https://www.nist.gov/news-events/news/2018/09/draft-nistir-8228-considerations-managing-iot-cybersecurity-and-privacy.)

16 راجع https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot.

17 راجع https://dodcio.defense.gov/Portals/0/Documents/Announcement/DoD%20Policy%20Recommendations%20for%20Internet%20of%20Things%20-%20White%20Paper.pdf?ver=2017-01-26-152811-440.

وضعت لجنة التجارة الفيدرالية معاييرها الخاصة بـ «أمان البيانات المعقول». وحددت اللجنة أوجه القصور الأمنية المتكررة التالية في الشركات المصنعة للأجهزة:

- الأمان غير مضمّن في الأجهزة
- عدم تدريب المطورين لموظفيهم على الممارسات الأمنية الجيدة
- عدم ضمان الأمان والامتثال في مرحلة ما بعد الإنتاج (عبر العقود)
- الافتقار إلى الدفاع في الإستراتيجيات المتعمقة
- عدم وجود ضوابط وصول معقولة (يمكن للعملاء تجاوز كلمات المرور الافتراضية أو تخمينها)
- عدم وجود برنامج لأمان البيانات

### ولاية كاليفورنيا

تعد كاليفورنيا من بين أولى الولايات داخل الولايات المتحدة التي سنت تشريعات بشأن إنترنت الأشياء. تعالج الفواتير الحالية مشكلات، مثل أمان تصميم الجهاز وحماية البيانات، ولكنها لا تحتوي على متطلبات محددة لمصنعي إنترنت الأشياء. وبدلاً من ذلك، ركز واضعو القوانين على الأمان في مرحلة التصميم، وذكروا أن حماية البيانات يجب أن تكون «ملائمة لطبيعة الجهاز ووظيفته» و«ملائمة للمعلومات التي قد يجمعها أو يحتويها أو ينقلها».

## المملكة المتحدة

نشرت وزارة الشؤون الرقمية والثقافة والإعلام والرياضة (DCMS) في المملكة المتحدة الإصدار النهائي من قواعد ممارسات أمان إنترنت الأشياء للمستهلك في أكتوبر 2018. [18] وقد تم إعداد مسودة مدونة الممارسات هذه بالاشتراك مع المركز الوطني للأمن السيبراني، وتضمنت معلومات من اتحادات المستهلكين والصناعة والأوساط الأكاديمية. تقدم الوثيقة 13 مبدأً توجيهيًا حول كيفية تحقيق نهج «آمن من خلال التصميم» لجميع المؤسسات المشاركة في تطوير منتجات إنترنت الأشياء الاستهلاكية وتصنيعها وتجارة التجزئة الخاصة بها.

تؤكد مدونة الممارسات على ثلاث ممارسات رائدة لتمكين المستخدمين من تحقيق أكبر الفوائد الأمنية وأكثرها إلحاحًا، وتحث الجهات المعنية لإنترنت الأشياء على منحها الأولوية: 1) عدم وجود كلمات مرور افتراضية: لا يقوم العديد من المستخدمين بتغيير كلمة المرور الافتراضية، والتي تعد مصدر العديد من مشكلات أمان إنترنت الأشياء. 2) تطبيق سياسة الكشف عن نقاط الضعف الأمنية: يجب أن تتوفر لدى مطوري الأجهزة والخدمات والتطبيقات الخاصة بإنترنت الأشياء سياسة الكشف عن نقاط الضعف الأمنية إلى جانب توفر نقطة اتصال عامة للسماح بالإبلاغ عن نقاط الضعف الأمنية (ومعالجتها) في الوقت المناسب. 3) الحفاظ على تحديث البرنامج: يجب أن يتم إجراء تحديثات البرامج في الوقت المناسب، وأن تكون سهلة التطبيق، ولا تؤدي إلى تعطيل عمل الجهاز.

18 راجع https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security.

بالاستناد إلى المخاوف والنهج التي حددتها كل من الولايات المتحدة والمملكة المتحدة، سيظل أمان إنترنت الأشياء يحتل قمة اهتمامات الحكومات. كما يتم أيضًا بذل الجهود من قِبل الهيئات الوطنية والدولية المعنية بالمعايير من أجل وضع المعايير والمبادئ التوجيهية وأفضل الممارسات لتأمين إنترنت الأشياء،[19] بما في ذلك الهيكل المرجعي لإنترنت الأشياء التابع للمنظمة الدولية للمعايير وفريق الدراسة التابع للاتحاد الدولي للاتصالات بشأن إنترنت الأشياء والمدن الذكية.[20]

في سياق إنترنت الأشياء، يجب أن يتمتع العملاء بالمرونة في استخدام الممارسات الحالية التي تم اختبارها وفقًا للوقت والمستخدمة بالفعل في ما يعتبر بـ «الأمن السيبراني الشبكي الأكثر تقليديًا.» على سبيل المثال، عند محاولة تحديد نقاط الضعف واكتشاف حالات الشذوذ والاستجابة للحوادث المحتملة والتعافي من الأضرار أو الأعطال التي لحقت بأجهزة إنترنت الأشياء، يمكن للعملاء استخدام ضوابط الأمن السيبراني التي تم تعيينها في ضوء إطار عمل الأمن السيبراني (CSF) التابع للمعهد الوطني للمعايير والتقنية.[21] وهذه المجموعة التأسيسية من ضوابط الأمن السيبراني معترف بها عالميًا، وتدعمها الحكومات والصناعات باعتبارها قاعدة موصى باستخدامها من قِبل أي مؤسسة بغض النظر عن قطاعها أو حجمها. ولا تقتصر ميزة الاستفادة من إطار عمل الأمن السيبراني على ذيوع الصيت فحسب، ولكنها تتضح أيضًا في المرونة التي تتيحها لتطبيق الأمن السيبراني مع مراعاة تأثيره على الأبعاد المادية والسيبرانية والشخصية. وبالإضافة إلى الجانب الإنساني، ينطبق إطار العمل على المؤسسات التي تعتمد على التقنية، سواء أكان التركيز في المقام الأول على تقنية المعلومات أم أنظمة التحكم الصناعية أم الأنظمة الفعلية السيبرانية أم إنترنت الأشياء.

---

19 للحصول على خلاصة وافية للمعايير والمبادرات الحالية بشأن أمان إنترنت الأشياء، يرجى الرجوع إلى كتالوج إدارة الاتصالات والمعلومات الوطنية (NTIA) التابعة لوزارة التجارة الأمريكية: https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog_17.pdf.

20 راجع https://www.itu.int/en/ITU-T/about/groups/Pages/sg20.aspx.

21 لمزيد من التفاصيل حول كيفية المواءمة مع إطار عمل الأمن السيبراني التابع للمعهد الوطني للمعايير والتقنية باستخدام خدمات AWS، راجع وثيقة المعلومات هذه ودليل العملاء: https://d0.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.pdf.

# الملحق 3 — الامتثال والخدمات الخاصة بـ AWS IoT

نظرًا لاعتبار AWS موفرًا عالميًا للخدمات السحابية الفائقة، فهي تتبع نهجًا صارمًا يستند إلى المخاطر الكامنة في أمان خدمات إنترنت الأشياء وحماية بيانات العملاء. وتفرض AWS عمليات الأمان الداخلية على جميع خدماتها السحابية لتقييم فعالية الضوابط الإدارية والتقنية والتشغيلية اللازمة للحماية من التهديدات الأمنية الحالية والناشئة التي تؤثر على الأمان والمرونة. لا تسفر هذه العملية الإلزامية لضمان الأمان عن التصديق على مختلف أطر الامتثال فحسب، ولكن تؤدي أيضًا إلى مضاعفة التزام AWS بتضمين الأمان في جميع مراحل التطوير والعمليات التشغيلية لدورة حياة خدماتها. تقدم AWS خدمات سحابية تجارية فائقة الجودة تم اعتمادها وفقًا للمعايير الرائدة المعترف بها عالميًا، مثل منظمة المعايير الدولية 27001 (ISO)،[22] ومعيار الأمان الخاص ببيانات صناعة بطاقات الدفع (PCI)،[23] وتقارير مراقبة تنظيم الخدمة (SOC)،[24] من بين الاعتمادات الدولية والوطنية والقطاعية الأخرى. كما تفي AWS بالمتطلبات الأمنية الصارمة حول دعم البيئات السرية لبعض وكالات الاستخبارات. يتمكن العملاء، مجتمعين، في أي قطاع وبأي حجم من تحقيق الفوائد الأمنية عند استخدام خدمات AWS السحابية عن طريق الوكيل لأن AWS تطبق «العلامة المائية رفيعة المستوى» عبر خدماتها.

تعد AWS حساسة لحقيقة أن العملاء قد يكون لديهم متطلبات امتثال محددة والتي يجب إظهارها والامتثال لها. ويجب الأخذ في الاعتبار استمرار AWS في إضافة الخدمات التي تتماشى مع برامج الامتثال تبعًا لطلب العملاء. ويتم سرد خدمات إنترنت الأشياء في النطاق عن طريق برنامج الامتثال على موقع AWS.[25]

---

22 ISO 27002/27001 هو معيار أمان عالمي قائم على نطاق واسع يحدد المتطلبات وأفضل الممارسات لنهج منهجي لإدارة معلومات الشركة والعملاء التي تستند إلى تقييمات المخاطر الدورية المناسبة لسيناريوهات التهديدات المتغيرة باستمرار. ISO 27018 هو معيار يعبر عن قواعد الممارسات التي تركز على حماية البيانات الشخصية في السحابة. ويستند إلى معيار أمان المعلومات ISO 27002، ويوفر إرشادات التنفيذ على ضوابط ISO 27002 المطبقة على السحابة العامة «معلومات التعريف الشخصية» (PII). كما يوفر مجموعة من الضوابط الإضافية والتوجيهات المرتبطة بها التي تهدف إلى معالجة متطلبات حماية معلومات التعريف الشخصية المتوفرة على السحابة العامة التي لا تتناولها مجموعة الضوابط الحالية ISO 27002.

23 معيار الأمان الخاص ببيانات صناعة بطاقات الدفع (PCI DSS) عبارة عن معيار خاص بأمان معلومات الممتلكات يديره مجلس معايير الأمان لصناعة بطاقات الدفع (PCI) (https://www.pcisecuritystandards.org)، الذي أسسته شركات American Express وDiscover Financial Services وJCB International وMasterCard Worldwide وVisa Inc. ينطبق معيار PCI DSS على جميع الكيانات التي تقوم بتخزين أو معالجة أو نقل بيانات حامل البطاقة أو بيانات المصادقة الحساسة (SAD) أو كلتيهما، بما في ذلك التجار والمعالجون والمشترون والمصدرون وموفرو الخدمات.

24 تهدف تقارير مراقبة تنظيم الخدمة (1، 2، 3) إلى تلبية مجموعة واسعة من متطلبات التدقيق المالي لهيئات التدقيق الأمريكية والدولية. ويتم إجراء تدقيق هذا التقرير وفقًا للمعايير الدولية لارتباطات التأكيد معيار رقم 3402 (ISAE 3402) والمعهد الأمريكي للمحاسبين المعتمدين (AICPA): في 801 (المعروف سابقًا باسم SSAE 16).

25 راجع https://aws.amazon.com/compliance/services-in-scope.