Securing Internet of Things (IoT) with AWS

Secure Cloud Adoption

April 2019

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Purpose

This whitepaper is a detailed look at the security-enabling Internet of Things (IoT) services that customers can harness in the AWS Cloud. This paper is intended for senior-level program owners, decision makers, and security practitioners considering secure enterprise adoption of IoT solutions.

Background

IoT technology enables organizations to optimize processes, enhance product offerings, and transform customer experiences in a variety of ways. While business leaders are excited about the way in which their businesses can benefit from this technology, security, risk, and privacy concerns remain. This is, in part, due to a struggle with disparate, incompatible, and sometimes immature security offerings that fail to properly secure deployments, leading to an increased risk for customer or business owner data.

Organizations are eager to deliver smart services that can drastically improve the quality of life for populations, business operations and intelligence, quality of care from service providers, smart city resilience, environmental sustainability, and a host of scenarios yet to be imagined. Most recently, AWS has seen an increase in IoT adoption from the healthcare sector and municipalities, with other industries expected to follow in the near term. Many municipalities are early adopters and are taking the lead when it comes to integrating modern technologies, like IoT. For example:

- **Kansas City, Missouri:** Kansas City created a unified smart city platform to manage new systems operating along its KC streetcar corridor. Video sensors, pavement sensors, connected street lights, a public WiFi network, and parking and traffic management have supported a 40% reduction in energy costs, $1.7 billion in new downtown development, and 3,247 new residential units.
- **City of Chicago, Illinois:** Chicago is installing sensors and cameras in intersections to detect pollen count and air quality for its citizens.
- **City of Catania, Italy:** Catania developed an application to let commuters know where the closest open parking spot is on the way to their destination.
- **City of Recife, Brazil:** Recife uses tracking devices placed on each waste collection truck and cleaning trolley. The city was able to reduce cleaning costs by $250,000 per month, while improving service reliability and operational efficiency.
- **City of Newport in Wales, UK:** Newport deployed smart city IoT solutions to improve air quality, flood control, and waste management in just a few months.
- **Jakarta, Indonesia:** As a city of 28 million residents that often deals with flooding, Jakarta is harnessing IoT to detect water levels in canals and lowlands, and is using social media to track citizen sentiment. Jakarta is also able to provide early warning and evacuation to targeted neighborhoods so that the government and first responders know which areas are most in need and can coordinate the evacuation process.

According to Machina Research, the global IoT market will reach $4.3 trillion by 2024.[1] Per the UK's Department for Business Innovation and Skills report, the global market for smart city solutions and the additional services required to deploy them is estimated to be $408 billion by 2020.[2] In addition, Forbes[3] estimates that "Predictive maintenance, self-optimizing production, and automated inventory management are the three top uses cases driving IoT market growth through 2020." Forbes asserts that companies want to leverage established and mature IT vendors with reliable infrastructure when building or deploying IoT solutions due to the magnitude of customer impact.

While customers are eager to leverage business opportunities available through IoT, historically, secure IoT adoption has been unclear. Features and services which enable solutions were not always secure by default, leaving potential security gaps in the architectural foundations. Furthermore, updates and maintenance were not automatic on key practices such as encrypted communications and over-the-air (OTA) updates. Lastly, few providers supported the ability for devices and gateways to be remotely patched after deployment, leaving these devices susceptible to emerging security risks.

In contrast, AWS takes security very seriously, supporting millions of active customers from a wide range of industries and geographies with various data sensitivity and confidentiality requirements. AWS invests significant resources into ensuring that security is incorporated into every layer of its services, extending that security out to devices with IoT. Helping to protect the confidentiality, integrity and availability of customer systems and data while providing a safe, scalable, and secure platform for IoT solutions is a priority for AWS.

Security Challenges

Security risks and vulnerabilities have the potential to compromise the security and privacy of customer data in an IoT application. Coupled with the growing number of devices, and the data generated, the potential of harm raises questions about how to address security risks posed by IoT devices and device communication to and from the cloud.

Common customer concerns regarding risks center on the security and encryption of data while in transit to and from the cloud, or in transit from edge services to and from the device, along with patching of devices, device and user authentication, and access control. Securing IoT devices is essential, not only to maintain data integrity, but to also protect against attacks that can impact the reliability of devices. As devices can send large amounts of sensitive data through the Internet and end users are empowered to directly control a device, the security of "things" must permeate every layer of the solution.

News of data compromise brings IoT security under additional scrutiny by customers, offering lessons learned and encouraging better practices. The foundation of an IoT solution should start and end with security, along

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

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

[3] See https://www.forbes.com/sites/louiscolumbus/2017/01/29/internet-of-things-market-to-reach-267b-by-2020/#74c8f8c7609b.

with using services capable of continuously auditing IoT configurations[4] to ensure that they do not deviate from security best practices. Once a deviation is detected, alerts should be raised so appropriate corrective action can be implemented — ideally, automatically.

To keep up with the entry of devices into the marketplace as well as the threats coming online, it is best to implement services that address each part of the IoT ecosystem and overlap in their capability to secure and protect, audit and remediate, and manage fleet deployments of IoT devices (with or without connection to the cloud).

How Are Governments Addressing IoT Security?

While private sector organizations are actively deploying IoT in use cases such as healthcare, industrial construction, and low-power consumer goods, governments at the national and local levels are beginning to address IoT adoption and security (see Appendix 2). In addition to assessing the future policy landscape of IoT, AWS continues to add services to various compliance frameworks to help customers meet their compliance obligations (see Appendix 3).

AWS IoT Services and Security Capabilities

AWS offers a suite of IoT services to help customers secure their devices, connectivity, and data. These services enable customers to leverage end-to-end security from device protection to data in transit and at rest. They also provide security features that enable the application and execution of security policies required to meet their security watermark.

AWS IoT provides broad and deep functionality; customers can build IoT solutions for virtually any use case across a wide range of devices. AWS IoT integrates with artificial intelligence (AI) services so customers can make devices smarter — even without Internet connectivity. Built on the AWS Cloud and used by millions of customers in 190 countries, AWS IoT can easily scale as customers' device fleets grow and their business requirements evolve. AWS IoT also offers comprehensive security features so customers can create preventative security policies and respond immediately to potential security issues.

AWS IoT provides cloud services and edge software, enabling customers to securely connect devices, gather data, and take intelligent actions locally, even when Internet connectivity is down. Cloud services allow customers to quickly onboard and securely connect large and diverse fleets, maintain fleet health, keep fleets secure, and detect and respond to events across IoT sensors and applications. To accelerate IoT application development, customers can easily connect devices and web services using a drag-and-drop interface. AWS IoT can also be used to analyze data and build sophisticated machine learning (ML) models. These models can be deployed in the cloud or down to customer devices to make devices smarter.

[4] A configuration is a set of technical controls customers set to help keep information secure when devices are communicating with each other and the cloud.

While current AWS IoT services[5] range widely to allow for innovative and comprehensive IoT solutions, this whitepaper focuses on the following five services, which are foundational for IoT security. Service descriptions and security features are further discussed below.

- **Amazon FreeRTOS** is an open source operating system for microcontrollers that makes small, low-power edge devices easy to program, deploy, secure, connect, and manage.
- **AWS IoT Greengrass** is software that lets customers run local compute, messaging, data caching, sync, and ML inference capabilities on connected devices.
- **AWS IoT Core** is a managed cloud service that lets connected devices easily and securely interact with cloud applications and other devices.
- **AWS IoT Device Management** is a cloud-based device management service that makes it easy to securely onboard, organize, monitor, and remotely manage IoT devices at scale.
- **AWS IoT Device Defender** is an IoT security service that continuously monitors and audits customers' IoT configurations to ensure that they do not deviate from security best practices.

Amazon FreeRTOS – Device Software

Service Overview: Amazon FreeRTOS (a:FreeRTOS) is an open source operating system for microcontrollers[6] that makes small, low-power edge devices easy to program, deploy, secure, connect, and manage. Amazon FreeRTOS is based on the FreeRTOS kernel, a popular open source operating system for microcontrollers, and extends it with software libraries that make it easy to securely connect customers' small, low-power devices directly to AWS Cloud services, like AWS IoT Core, or to more powerful edge devices running AWS IoT Greengrass.

Security Capabilities: Amazon FreeRTOS comes with libraries to help secure device data and connections, including support for data encryption and key management. Amazon FreeRTOS includes support for Transport Layer Security (TLS v1.2) to help devices connect securely to the cloud. Amazon FreeRTOS also has a code signing feature to ensure customer device code is not compromised during deployment as well as capabilities for OTA updates to remotely update devices with feature enhancements or security patches.

[5] AWS IoT services include Amazon FreeRTOS, AWS IoT Greengrass, AWS IoT Core, AWS IoT Device Management, AWS IoT Device Defender, AWS IoT Things Graph, AWS IoT Analytics, AWS IoT SiteWise, and AWS IoT Events. For more information, visit https://aws.amazon.com/iot.

[6] A microcontroller is a single chip containing a simple processor that can be found in many devices, including appliances, fitness trackers, industrial automation sensors, and automobiles. Many of these small devices could benefit from connecting to the cloud or locally to other devices. For example, smart electricity meters need to connect to the cloud to report on usage, and building security systems need to communicate locally so that a door will unlock when someone badges in.

AWS IoT Greengrass – Software for Edge Computing

Service Overview: AWS IoT Greengrass is software that lets customers run local compute, messaging, data caching, sync, and ML inference capabilities for connected devices,[7] allowing connected devices to operate even with intermittent connectivity to the cloud. Once the device reconnects, AWS IoT Greengrass synchronizes the data on the device with AWS IoT Core, providing constant functionality regardless of connectivity. AWS IoT Greengrass seamlessly extends AWS to devices so they can act locally on the data they generate, while still using the cloud for management, analytics, and durable storage.

Security Capabilities: AWS IoT Greengrass authenticates and encrypts device data for both local and cloud communications, and data is never exchanged between devices and the cloud without proven identity. The service uses security and access management similar to what customers are familiar with in AWS IoT Core, with mutual device authentication and authorization, and secure connectivity to the cloud.

More specifically, AWS IoT Greengrass uses X.509[8] certificates, managed subscriptions, AWS IoT policies, and AWS Identity and Access Management (IAM) policies and roles to ensure that AWS IoT Greengrass applications are secure. AWS IoT devices require an AWS IoT thing, a device certificate, and an AWS IoT policy to connect to the AWS IoT Greengrass service. This allows AWS IoT Greengrass core devices to securely connect to the AWS IoT cloud service. It also allows the AWS IoT Greengrass cloud service to deploy configuration information, AWS Lambda functions, and managed subscriptions to AWS IoT Greengrass core devices. In addition, AWS IoT Greengrass provides hardware root of trust private key storage for edge devices.

Other important security capabilities of AWS IoT Greengrass are monitoring and logging. For example, core software in the service can write logs to Amazon CloudWatch[9] (which also functions for AWS IoT Core) and to the local file system of customers' core devices. Logging is configured at the group level and all AWS IoT Greengrass log entries include a time stamp, log level, and information about the event. AWS IoT Greengrass is integrated with AWS CloudTrail[10] — a service that provides a record of actions taken by a user, role, or an AWS service in AWS IoT Greengrass — and if activated by the customer, it captures all application programming interface (API) calls for AWS IoT Greengrass as events. This includes calls from the AWS IoT Greengrass console and code calls to the AWS IoT Greengrass API operations. For example, customers can create a trail and calls can enable continuous delivery of AWS CloudTrail events to an Amazon Simple Storage Service (Amazon S3) bucket,

[7] In order to get started with AWS IoT Greengrass, customers will need a device capable of running the AWS IoT Greengrass core. There is a full list of qualified devices and technical dependencies here. Click here for a hands-on getting started guide. Customers can find the detailed developer reference here.

[8] X.509 certificates are digital certificates that use the X.509 public key infrastructure standard to associate a public key with an identity contained in a certificate. X.509 certificates are issued by a trusted entity called a certification authority (CA). The CA maintains one or more special certificates called CA certificates that it uses to issue X.509 certificates. Only the certification authority has access to CA certificates. See https://docs.aws.amazon.com/iot/latest/developerguide/x509-certs.html for more information.

[9] See https://aws.amazon.com/cloudwatch.

[10] See https://aws.amazon.com/cloudtrail.

including events for AWS IoT Greengrass. If customers don't want to create a trail, they can view the most recent events in the AWS CloudTrail console in event history (if enabled). This information can be used to do a number of things, like determining when a request was made to AWS IoT Greengrass and the IP address from which the request was made.

Best practice options are available to secure customers' data on the device and should be utilized whenever possible. For AWS IoT Greengrass, all IoT devices should enable full disk encryption and follow key management best practices. Customers can utilize full disk encryption, using AES 256-bit keys based on NIST FIPS 140-2 validated algorithms[11] and follow key management best practices. For low-power devices such as those using Amazon FreeRTOS, customers can follow NIST 8114 lightweight cryptography[12] recommendations.

The above sections covered microcontrollers and edge use cases. Below, the paper will focus on IoT services that operate in the cloud.

AWS IoT Core – Cloud-Based IoT Gateway

Service Overview: AWS IoT Core is a managed cloud service that lets connected devices easily and securely interact with cloud applications and other devices. AWS IoT Core provides secure communication and data processing across different kinds of connected devices and locations so customers can easily build IoT applications. Examples of customer use cases include industrial solutions and connected home solutions, with the ability to support billions of devices and trillions of messages that can be processed and routed to AWS endpoints and other devices reliably and securely.

Security Capabilities: AWS IoT Core offers a number of solutions to customers that help enable and maintain security. AWS Cloud security mechanisms protect data as it moves between AWS IoT and other devices or AWS services. Devices can connect using a variety of identity options (X.509 certificates, IAM users and groups, Amazon Cognito identities, or custom authentication tokens) over a secure connection. While customers perform the client-side validations (i.e., chain of trust validation, hostname verification, secure storage, and distribution of their private keys), AWS IoT Core provides secure transportation channels using TLS. The AWS IoT rules engine also forwards device data to other devices and AWS services according to customer-defined rules. AWS access management systems are used to securely transfer data to its final destination. Another AWS IoT authorization feature worth noting is AWS IoT policy variables, which helps avoid the provisioning of over-privileged credentials to a device. These features, used in conjunction with general cybersecurity best practices, work to protect customer data.

[11] NIST FIPS 140-2 Approved Cryptographic Algorithms: https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402annexa.pdf.

[12] NIST 8114 – Lightweight Cryptography: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf.

AWS IoT Device Management – Cloud-Based IoT Device Management Service

Service Overview: AWS IoT Device Management helps customers onboard, organize, monitor, and remotely manage IoT devices at scale. AWS IoT Device Management integrates with AWS IoT Core to easily connect devices to the cloud and other devices so customers can remotely manage their fleets of devices. AWS IoT Device Management helps customers onboard new devices by using AWS IoT within the AWS Management Console or an API to upload templates that they populate with information like device manufacturer and serial number, X.509 identity certificates, or security policies. Following this, customers can then configure the entire fleet of devices with this information with a few clicks in AWS IoT within the AWS Management Console.

Security Capabilities: With AWS IoT Device Management, customers can group their device fleet into a hierarchical structure based on function, security requirements, or similar categories. They can group a single device in a room, multiple devices on the same floor, or all the devices that operate within a building. These groups can then be used to manage access policies, view operational metrics, or perform actions across the entire group. Additionally, a feature known as "Dynamic Things" can automatically add devices that meet the customer-defined criteria and remove devices that no longer match the requirements. This securely streamlines the process while maintaining operational integrity. Dynamic Things also makes it easy to find device records based on any combination of device attributes and allows customers to perform bulk updates.

With AWS IoT Device Management, customers can also push software and firmware to devices in the field to patch security vulnerabilities and improve device functionality; execute bulk updates; control deployment velocity; set failure thresholds; and define continuous jobs to update device software automatically so that they are always running the latest version of software. Customers can remotely send actions, like device reboots or factory resets, to fix software issues in the device or restore the device to its original settings. Customers can also digitally sign files that are sent to their devices, helping to ensure the devices are not compromised.

The ability to push software updates isn’t limited to cloud services. In fact, OTA update jobs in Amazon FreeRTOS allow customers to use AWS IoT Device Management to schedule software updates. Similarly, customers can also create an AWS IoT Greengrass core update job for one or more AWS IoT Greengrass core devices using AWS IoT Device Management in order to deploy security updates, bug fixes, and new AWS IoT Greengrass features to connected devices.

AWS IoT Device Defender – Cloud-Based IoT Device Security Service

Service Overview: AWS IoT Device Defender is a fully managed service that helps customers audit security features established for their fleet of IoT devices. The service continuously audits IoT configurations to ensure that configurations aren’t deviating from security best practices to maintain and enforce IoT configurations — such as ensuring device identity, authenticating and authorizing devices, and encrypting device data. The service can send an alert if there are any gaps in a customer's IoT configuration that might create a security risk, such as identity certificates being shared across multiple devices or a device with a revoked identity certificate trying to connect to AWS IoT Core.

Security Capabilities: In addition to the service's monitoring and auditing capabilities, customers can set alerts that take action to remediate any deviations found in devices. For example, spikes in outbound traffic might indicate that a device is participating in a distributed denial of service (DDoS) attack. AWS IoT Greengrass and Amazon FreeRTOS also automatically integrate with AWS IoT Device Defender to provide security metrics from the devices for evaluation.

AWS IoT Device Defender can send alerts to AWS IoT, Amazon CloudWatch, and Amazon Simple Notification Service (Amazon SNS), with alerts publishing to Amazon CloudWatch metrics. If a customer decides to address an alert, AWS IoT Device Management can be used to take mitigating actions such as pushing security fixes.

AWS IoT Device Defender audits IoT configurations associated with customer devices against a set of defined IoT security best practices so customers can see where the security gaps exist and run audits on a continuous or ad-hoc basis. There are also security practices within AWS IoT Device Defender that can be selected and run as part of the audit. This service also integrates with other AWS services — such as Amazon CloudWatch and Amazon SNS — to send security alerts to AWS IoT when an audit fails or when behavior anomalies are detected so customers can investigate and determine the root cause. For example, AWS IoT Device Defender can alert customers when device identities are accessing sensitive APIs. AWS IoT Device Defender can also recommend actions that minimize the impact of security issues such as revoking permissions, rebooting a device, resetting factory defaults, or pushing security fixes to any of the customers' connected devices.

Customers may also be concerned about bad actors; human or systemic errors and authorized users with malicious intentions can introduce configurations with negative security impacts. AWS IoT Core provides the security building blocks for customers to securely connect devices to the cloud and to other devices. The building blocks allow enforcing security controls such as authentication, authorization, audit logging, and end-to-end encryption. Then, AWS IoT Device Defender steps in and helps to continuously audit security configurations for compliance with security best practices and customers' own organizational security policies.

Leveraging Provable Security to Enhance IoT – an Industry Differentiator

New security services and technologies are being built at AWS to help enterprises secure their IoT and edge devices. In particular, AWS has recently launched checks within AWS IoT Device Defender, powered by an AI technology known as automated reasoning, which leverages mathematical proofs to verify software is written correctly and determine if there is unintended access to the devices. The AWS IoT Device Defender is an example of a way customers can directly use automated reasoning to secure their own devices. Internally, AWS has used automated reasoning to verify the memory integrity of code running on Amazon FreeRTOS and to protect against malware. Investment in automated reasoning to provide scalable assurance of secure software, referred to as "provable security," allows customers to operate sensitive workloads on AWS.

AWS Zelkova[13] uses automated reasoning to prove that customer data access controls are operating as intended. The access control checks in AWS IoT Device Defender are powered by Zelkova, allowing customers to ensure their data is appropriately protected. An AWS IoT policy is overly permissive if it grants access to resources outside of a customer's intended security configuration. The Zelkova-powered controls baked into AWS IoT Device Defender verify that policies don't allow actions restricted by the customer's security configuration and that intended resources have permissions to perform certain actions.

Other automated reasoning tools have been used to help secure the AWS IoT infrastructure. The open source formal verification tool CBMC has been used to strengthen the foundations of the AWS IoT infrastructure by proving the memory safety of critical components of the Amazon FreeRTOS operating system. A proof of memory safety minimizes the potential of certain security issues, allowing customers and developers to focus on securing other areas in their environment. The memory safety proofs are automatically checked every time a code change is made to Amazon FreeRTOS, providing both customers and AWS developers ongoing confidence in the security of these critical components.

Automated reasoning continues to be implemented across a variety of AWS services and features, providing heightened levels of security assurance for critical components of the AWS Cloud. AWS continues to deploy automated reasoning to develop tools for customers as well as internal infrastructure verification technology for the AWS IoT stack.

What Are Key IoT Security Best Practices?

Despite the number of best practices available, there is no one-size-fits-all approach to mitigating the risks to IoT solutions. Depending on the device, system, service, and environment in which the devices are deployed, different threats, vulnerabilities, and risk tolerances exist for customers to consider. Here are recommended practices when incorporating end-to-end security across data, devices, and cloud services:

1. **Incorporate Security at the Design Phase**
   The foundation of an IoT solution starts and ends with security. As devices may send large amounts of sensitive data, and end users of IoT applications may also have the ability to directly control a device, the security of "things" must be a pervasive design requirement. Security is not a static formula; IoT applications must be able to continuously model, monitor, and iterate on security best practices.
   A challenge for IoT security is the lifecycle of a physical device and the constrained hardware for sensors, microcontrollers, actuators, and embedded libraries. These constrained factors may limit the security capabilities each device can perform. With these additional dynamics, IoT solutions must continuously adapt their architecture, firmware, and software to stay ahead of the changing security landscape. Although the constrained factors of devices can present increased risks, hurdles, and

[13] To learn more about Zelkova, visit https://aws.amazon.com/blogs/security/protect-sensitive-data-in-the-cloud-with-automated-reasoning-zelkova.

potential tradeoffs between security and cost, building a secure IoT solution must be the primary objective for any organization.

2. **Build on Recognized IT Security and Cybersecurity Frameworks**
AWS supports an open, standards-based approach to promote secure IoT adoption. When considering the billions of devices and connection points necessary to support a robust IoT ecosystem for consumer, industrial, and public sector use, interoperability is vital. Thus, AWS IoT services adhere to industry standard protocols and best practices. Additionally, AWS IoT Core supports other industry-standard and custom protocols, allowing devices to communicate with each other even if they are using different protocols. AWS is a strong proponent of interoperability so that developers can build on top of existing platforms to support evolving customer needs. AWS also supports a thriving partner ecosystem to expand the menu of choices and stretch the limits of what is possible for customers. Applying globally-recognized best practices carries a number of benefits across all IoT stakeholders including:
    - Repeatability and reuse, instead of re-starting and re-doing
    - Consistency and consensus to promote the compatibility of technology and interoperability across geographical boundaries
    - Maximizing efficiencies to accelerate IT modernization and transformation

3. **Focus on Impact to Prioritize Security Measures**
Attacks or abnormalities are not identical and may not have the same impact on people, business operations, and data. Understanding customer IoT ecosystems and where devices will operate within this ecosystem informs decisions on where the greatest risks are — within the device, as part of the network, or physical component or security. Focusing on the risk impact assessment and consequences is critical for determining where security efforts should be directed along with whom is responsible for those efforts in the IoT ecosystem.

Conclusion

Along with an exponential growth in connected devices, each "thing" in IoT communicates packets of data that require reliable connectivity, storage, and security. With IoT, an organization is challenged with managing, monitoring, and securing immense volumes of data and connections from dispersed devices. But this challenge doesn't have to be a roadblock in a cloud-based environment. In addition to scaling and growing a solution in one location, cloud computing enables IoT solutions to scale globally and across different physical locations while lowering communication latency and allowing for better responsiveness from devices in the field. AWS offers a suite of IoT services with end-to-end security, including services to operate and secure endpoints, gateways, platforms, and applications as well as the traffic traversing across these layers. This integration simplifies secure use and management of devices and data that continually interact with each other, allowing organizations to benefit from the innovation and efficiencies IoT can offer while maintaining security as a priority.

Appendix 1 – AWS IoT Service Integration

AWS IoT integrates directly with the following AWS services:

- **Amazon Simple Storage Service (Amazon S3)** provides scalable storage in the AWS Cloud. For more information, see Amazon S3.
- **Amazon DynamoDB** provides managed NoSQL databases. For more information, see Amazon DynamoDB.
- **Amazon Kinesis** enables real-time processing of streaming data at a massive scale. For more information, see Amazon Kinesis.
- **AWS Lambda** runs customers' code on virtual servers from Amazon Elastic Compute Cloud (Amazon EC2) in response to events. For more information, see AWS Lambda.
- **Amazon Simple Notification Service (Amazon SNS)** sends or receives notifications. For more information, see Amazon SNS.
- **Amazon Simple Queue Service (Amazon SQS)** stores data in a queue to be retrieved by applications. For more information, see Amazon SQS.

Appendix 2 – Governments Addressing IoT

United States

The National Institute of Standards and Technology (NIST) – Department of Commerce

The United States Department of Commerce is spearheading multiple efforts to address IoT security. The National Institute of Standards and Technology (NIST) published a whitepaper[14] that brings to light topics that customers and government agencies alike consider when assessing the security of data and devices. In the whitepaper, readers are invited to assess these concerns and are provided recommendations on how to mitigate the problems. NIST also released NIST Internal Report (NISTIR) 8228,[15] which identifies risks that may negatively impact IoT adoption. The document also offers recommendations for mitigating or reducing the effects of these concerns. NIST is also convening public and private partnerships, soliciting comments, and hosting workshops related to smart cities and international standardization of IoT, among a host of other initiatives.[16] Though in its infancy, early indicators point to potential cybersecurity and privacy risks as serious challenges to the gains that governments and consumers can harness through IoT.

Department of Defense

Another example within the government is found in the defense community. In 2016, the Chief Information Officer of the US Department of Defense (DoD) issued policy recommendations to address the vulnerabilities and risks to IoT.[17] According to the policy recommendation, DoD already provisions millions of IoT devices and sensors across DoD facilities, vehicles, and medical devices and is considering incorporating them into weapons and intelligence systems. The complexity of securing IoT stems from the limited processing power of the devices to run firewalls and anti-malware as well as the vast number of devices, which compound vulnerability exposure to a different level than traditional mobile devices.

DoD's recommended approach and policy action to address IoT security risks include: 1) a security and privacy risk analysis supporting each IoT implementation and associated data streams, 2) encryption at every point, where costs are commensurate with risk and value, and 3) monitoring IoT networks to identify anomalous traffic and emergent threat.

Federal Trade Commission (FTC)

The FTC has been an important participant in IoT security conversations, pursuing action against device manufacturers who have misrepresented or demonstrated negligence in their security commitments. The FTC

[14] Jeffrey Voas (NIST), Richard Kuhn (NIST), Phillip Laplante (Penn State University), and Sophia Applebaum (MITRE), "Internet of Things (IoT) Trust Concerns" (October 16, 2018, https://csrc.nist.gov/publications/detail/white-paper/2018/10/17/iot-trust-concerns/draft.)

[15] NISTIR 8228, "Considerations for Managing IoT Cybersecurity and Privacy Risks Out for Public Comment" (September 26, 2018, https://www.nist.gov/news-events/news/2018/09/draft-nistir-8228-considerations-managing-iot-cybersecurity-and-privacy.)

[16] See https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot.

[17] See 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.

has set its bar to "reasonable data security." The FTC identified the following repeated security deficiencies in device manufacturers:

- Security not built into devices
- Developers are not training their employees on good security practices
- Not ensuring downstream security and compliance (via contracts)
- Lack of defense in depth strategies
- Lack of reasonable access controls (customers can bypass or guess default passwords)
- Lack of a data security program

State of California

California is amongst the first states within the United States to pass legislation on IoT. The current bills address issues such as security of device design and data protection, but do not have specific requirements of IoT manufacturers. Instead, lawmakers have focused on security at the design phase, writing that protection of data must be "appropriate to the nature and function of the device" and "appropriate to the information it may collect, contain, or transmit."

United Kingdom

The UK's Department for Digital, Culture, Media and Sport ("DCMS") published the final version of its Code of Practice for Consumer IoT Security in October 2018.[18] This Code of Practice was jointly drafted with the National Cyber Security Centre and included input from consumer associations, industry, and academia. The document provides 13 guidelines on how to achieve a "secure by design" approach for all organizations involved in developing, manufacturing, and retailing consumer IoT products.

The Code of Practice emphasizes three leading practices for enabling users to achieve the greatest and most immediate security benefits, and urges IoT stakeholders to prioritize them: 1) No default passwords: Many users do not change the default password, which has been the source of many IoT security issues. 2) Implement a vulnerability disclosure policy: IoT device, service, and app developers should have a vulnerability disclosure policy and public point of contact to allow for the reporting (and remediation) of vulnerabilities in a timely manner. 3) Keep software updated: Software updates need to be timely, easy to implement, and not disruptive to the functioning of the device.

Based on the concerns and approaches outlined by both the US and UK, the security of IoT will continue to be top of mind for governments. Efforts are also underway by national and international standards bodies to

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

develop standards, guidelines, and best practices for securing IoT,[19] including the International Organization for Standardization (ISO) IoT Reference Architecture and the International Telecommunication Union (ITU) study group on IoT and smart cities.[20]

In the context of IoT, customers should have the flexibility of using existing, time-tested practices already in use in what's considered more "traditional network cybersecurity." For example, when trying to identify vulnerabilities, detect irregularities, respond to potential incidents, and recover from damage or disruption to IoT devices, customers can use the cybersecurity controls mapped against the NIST Cybersecurity Framework (CSF).[21] This foundational set of cybersecurity disciplines is recognized globally and has been supported by governments and industries as a recommended baseline for use by any organization, regardless of its sector or size. The advantage of utilizing the NIST CSF is not just in its reputation, but also in the flexibility it allows for applying cybersecurity while keeping in mind its effect on physical, cyber, and people dimensions. Along with the human aspect, the framework applies to organizations relying on technology, whether the focus is primarily on information technology, industrial control systems, cyber-physical systems, or IoT.

[19] For a compendium of current standards and initiatives on IoT security, refer to the US Department of Commerce, National Telecommunications and Information Administration (NTIA) catalog: https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog_draft_17.pdf.

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

[21] For additional details on how to align with the NIST CSF using AWS services, refer to this whitepaper and customer workbook: https://d0.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.pdf.

Appendix 3 – AWS IoT Services and Compliance

As a global, hyperscale cloud service provider, AWS takes a rigorous, risk-based approach to the security of its IoT services and the safeguarding of customer data. AWS enforces internal security processes on all of its cloud services to evaluate the effectiveness of the managerial, technical, and operational controls necessary for protecting against current and emerging security threats impacting security and resiliency. This mandatory security assurance process results in not only attestation to various compliance frameworks, but also doubles down on AWS's commitment to embed security throughout all phases of the development and operational processes of its services lifecycle. AWS offers hyperscale commercial cloud services that have been accredited against leading, internationally-recognized standards, such as International Standards Organization 27001 (ISO),[22] Payment Card Industry Data Security Standard (PCI),[23] and the Service Organization Control Reports (SOC),[24] among other international, national, and sectoral accreditations. AWS also meets the rigorous security requirements around supporting the classified environments of certain intelligence agencies. Taken together, customers in any sector and of any size using AWS Cloud services achieve security benefits by proxy because AWS applies the "high watermark" across its services.

AWS is sensitive to the fact that customers may have specific compliance requirements that must be demonstrated and complied with. Keeping this in mind, AWS continually adds services that align with compliance programs based on customer demand. The IoT services in scope are listed by compliance program on the AWS website.[25]

[22] ISO 27001/27002 is a widely-adopted global security standard that sets out requirements and best practices for a systematic approach to managing company and customer information that's based on periodic risk assessments appropriate to ever-changing threat scenarios. ISO 27018 is a code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls applicable to public cloud Personally Identifiable Information (PII). It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO 27002 control set.

[23] The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard administered by the PCI Security Standards Council (https://www.pcisecuritystandards.org), which was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. PCI DSS applies to all entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) including merchants, processors, acquirers, issuers, and service providers.

[24] Service Organization Controls reports (SOC 1, 2, 3) are intended to meet a broad range of financial auditing requirements for US and international auditing bodies. The audit for this report is conducted in accordance with the International Standards for Assurance Engagements No. 3402 (ISAE 3402) and the American Institute of Certified Public Accountants (AICPA): AT 801 (formerly SSAE 16).

[25] See https://aws.amazon.com/compliance/services-in-scope.