
aws
The ultimate IoT security best practices guide

Introduction

Today's Internet of Things (IoT) solutions are accelerating business results through a wide variety of use cases across just about every market, including industrial, commercial, and consumer applications. The IoT space is growing fast: IDC estimates that by 2025, the world will have 41.6 billion connected devices generating a total of 79.4 zettabytes of data.[1] And Statista predicts there will be over 75 billion connected endpoints online in 2025.[2]

To protect your customers, your devices, and your organization, the foundation of your ***IoT ecosystem*** should be built around security. The best IoT security solution offers multi-layered protection from the edge to the cloud, providing safeguards for your IoT devices, their connections, and their data. It should also include both preventative measures and active monitoring/alerts—so you can ensure your devices are secure and functioning as expected in the field, while reacting to and managing new security issues as they arise.

IoT fleets present a number of unique security challenges that can't be solved solely by traditional means, such as firewalls and antivirus software. In fact, relying exclusively on these traditional solutions has proven to be insufficient for securing any system, IoT or non-IoT. In the case of IoT devices, sometimes using traditional means is not even feasible. For instance, antivirus software often cannot be run on constrained devices.

IoT devices typically have low compute, memory, and storage capabilities, limiting opportunities for implementing security directly on their hardware.

Also, the software and hardware components of connected devices are often built by different manufacturers, which can lead to ambiguity around ownership of security elements.

New attack vectors are constantly emerging, requiring continuous auditing of device settings and health and the remediation of identified security issues (i.e., updating firmware and patching). That means your IoT security strategy will need to look to the future, providing regular firmware updates and enforcement of configuration policies to account for new devices, expanding data, and evolving threats.

This guide will arm you with the practical advice you need to successfully protect your IoT ecosystem—and, more importantly, ensure it stays protected as the IoT security landscape changes and grows.

[1] https://www.idc.com/getdoc.jsp?containerId=prUS45213219
[2] https://www.statista.com/statistics/471264/iot-number-of-connected devices-worldwide

Key term definition

IoT ecosystem–All elements of your IoT solution, including device hardware and firmware, on-premises and in-cloud systems and software, and processes such as device manufacturing, shipping, and provisioning.

Cloud security best practices

The best IoT security solutions are rooted in cloud security. Cloud architecture offers intrinsic security provisions and best practices, providing a strong foundation for powerful, easy-to-manage IoT protection. Follow these best practices when securing your IoT solutions in the cloud:

1. **Understand your shared responsibility:** Know your role vs. the role of your vendors and partners in maintaining the security of your devices. These roles should be documented upfront, and you should strive to vet and select trusted partners and vendors with security practices that align well with the goals of your business.

2. **Implement a strong identity foundation:** Use the ***principle of least privilege*** and enforce separation of duties with appropriate authorization for each interaction. Centralize privilege management and reduce—or even eliminate—reliance on long-term credentials.

3. **Enable traceability:** Monitor, alert, and audit actions and changes to your environment in real time. Integrate logs and metrics with systems to automatically respond and take action.

4. **Apply security at all layers:** Rather than only focusing on protection of a single outer layer, apply a defense-in-depth approach with other security controls. Apply to all layers (e.g., edge network, virtual private cloud (VPC), subnet, load balancer, every instance, operating system, and application).

5. **Automate security best practices:** Automated software-based security mechanisms to improve your ability to scale securely, rapidly, and cost-effectively. Create secure architectures—including the implementation of controls—that are defined and managed as code in version-controlled templates.

6. **Protect data in transit and at rest:** Separate your data into sensitivity levels and use mechanisms—such as encryption, tokenization, and access control—where appropriate.

7. **Keep people away from data:** Create mechanisms and tools to reduce or eliminate the need for direct access or manual processing of data. This lowers the risks of loss, modification, and other human errors when handling sensitive data.

8. **Prepare for security events:** Create an incident management process that aligns to your organizational requirements. Run incident response simulations and use tools with automation to increase your speed for detection, investigation, and recovery. For more on building an incident response process, view the AWS Security Incident Response Guide.

Learn security best practices for a well-architected AWS Cloud »

Explore AWS Cloud security offerings and best practices in depth »

Key term definition

Principle of least privilege–A security best practice of only granting your identities the least number of privileges required to perform their intended operations within expected contexts.

IoT security best practices

Ideally, you could rely on a publicly known and reusable list of cloud security practices for every building block in your IoT ecosystem, and these principles would perfectly align with your unique requirements and constraints. In reality, however, at least some of the IoT security burden must fall on your shoulders.

Not to worry, though—the following best practices will help you protect your business and IoT ecosystem, from design and implementation to ongoing operations and management. In addition to the best practices themselves, we've provided a list of high-level recommendations following each rule. These recommendations are not an exhaustive list, and they are only meant to clarify the underlying concepts behind each rule.

1. Provision devices and systems with unique identities and credentials

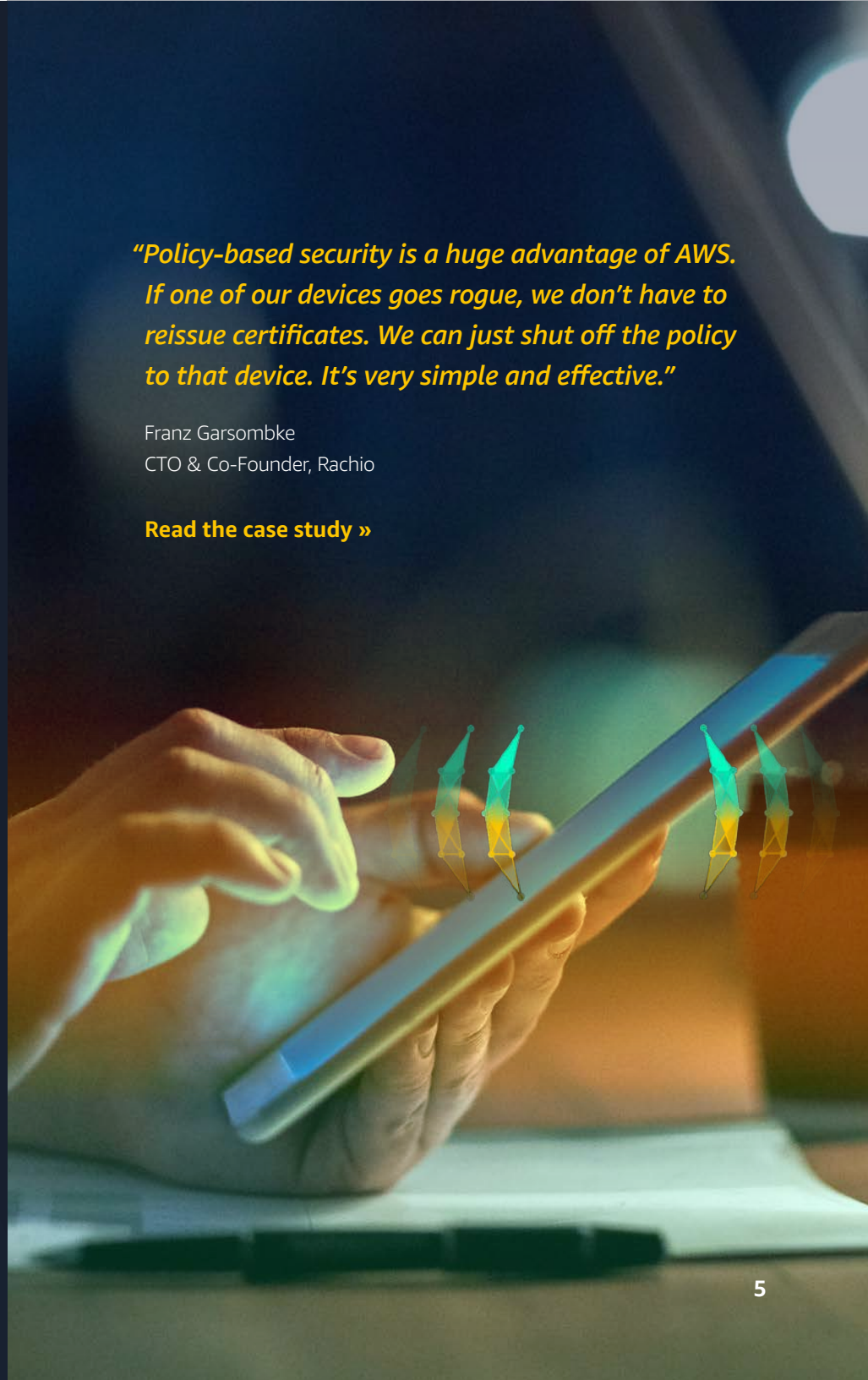
- Assign unique identities to all devices and on-premises or in-cloud systems.
- Assign unique and cryptographic credentials such as X.509 certificates to each identity.
- Create mechanisms to facilitate the generation, distribution, rotation, and revocation of credentials.
- Opt to use hardware-protected modules such as trusted platform modules (TPMs) or hardware security modules (HSMs) for storing credentials and performing authentication operations.
- Create mechanisms to securely manage access to IoT services and resources.

2. Apply authentication and access control mechanisms

- Establish clear trust boundaries based on your ***threat model*** and enforce access controls on all access outside those boundaries.
- Identify and mitigate issues with entry points that are vulnerable to forging or spoofing identities and unauthorized escalation of privileges.
- Consider deploying services that let you authenticate identities without hard-coding passwords, tokens, or other secrets.
- If your threat model includes potential physical access to devices by unauthorized actors, tamper-proof your device hardware and disable any unused hardware interfaces physically and/or at the firmware or operating system layer.
- Create mechanisms to assess credentials and privileges at regular intervals and whenever their associated identities transition through lifecycle events.
- Enforce resource consumption limits and practice throttling to protect the availability of shared resources.

Key term definition

Threat model–A living document that catalogs relevant potential threats to your IoT ecosystem with corresponding mitigations and accepted risks. Also includes a full inventory of all of your assets, the systems that interact with them, their threat boundaries, and their entry points.



"Policy-based security is a huge advantage of AWS. If one of our devices goes rogue, we don't have to reissue certificates. We can just shut off the policy to that device. It's very simple and effective."

Franz Garsombke
CTO & Co-Founder, Rachio

Read the case study »

"Amazon FreeRTOS is an exciting leap forward for our business and our customers. Dev teams can now focus their energy on the application and not the plumbing, messaging, or security. Instead, they choose the board, the chip, and connect to AWS IoT seamlessly."

Seb Chakraborty
CTO, British Gas HIVE

Read the case study »

3. Use cryptographic network protocols

- Use proven, trusted IoT software development kits (SDKs) to securely connect your devices to the cloud.
- Protect the confidentiality and integrity of inbound and outbound short- and long-range network communication channels for data transfers, monitoring, administration, provisioning, and deployments.
- Protect the integrity of data—regardless of classification level—by using cryptographic network protocols to detect any unauthorized modification.
- For resource-constrained devices that cannot support cryptographic network protocols, limit network activity to short-range connections within network-level trust boundaries (as identified in your threat model).
- Employ open and standard cryptographic network protocols that the security community publicly and continuously vets and conduct peer reviews.
    - Using cryptographic primitives, such as one-way hash functions or encryption functions, cannot replace cryptographic protocols for protecting data in transit. Cryptographic protocols consider contextual information required for enforcing data transportation security controls.
    - Cryptographic protocols provide security controls such as recipient authentication, secure cryptographic key exchange or negotiation, and message order integrity and successful message delivery verification.
- Consider running your devices on open and well-maintained operating systems—such as FreeRTOS—that allow you to easily and continuously add security functionalities and applications.

4. Create continuous update and deployment mechanisms

- Use cryptographic network protocols for transferring ***deployment artifacts***.
- Apply and verify digital signatures on distributed deployment artifacts.
- Apply a default configuration for deploying security updates and patches automatically.
- Employ authentication and access controls on deployment artifact repositories and their distribution systems.
- Maintain an inventory of the deployed software across your IoT ecosystem, including versions and patch status.
- Monitor status of deployments and investigate any failed or stalled deployments.
- Use version control mechanisms to prevent unauthorized actors from forcing firmware or software downgrades.
- Maintain notification mechanisms to immediately alert stakeholders when your infrastructure can't deploy security updates to your fleet.
- Create mechanisms to identify and replace constrained devices that are not capable of receiving updates.
- Create detection and response mechanisms to handle unauthorized changes in deployed software or firmware.

Key term definition

Deployment artifacts–All source code, configuration, and binary files that users need for secure and reliable installation of software or firmware on IoT devices or general-purpose hosts.

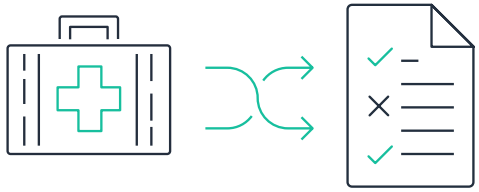
5. Deploy security auditing and monitoring mechanisms

- Deploy auditing and monitoring mechanisms to continuously collect and report activity metrics and logs from across your IoT ecosystem.
- Monitor on-device and related off-device activities, such as network traffic and entry points, process execution, and system interactions, for any unexpected behavior.
- Use logs to further monitor events and troubleshoot issues.
- Maintain and regularly exercise a security incident response plan, along with containment and recovery mechanisms.
    - This should be in correspondence to the technical skill level of your IoT element operators and their deployment and ownership model.
- Keep a record of security actions taken by user, role, or service.

"AWS IoT…provides device behavior monitoring that is a must-have for any IoT company that is building a secure infrastructure."

Franz Garsombke
CTO & Co-Founder, Rachio

Read the case study »



6. Build continuous health checks for security mechanisms

- Continuously check that your security controls and systems are intact by using mechanisms such as ***canary tests***.
- Verify that security controls prevent unauthorized access and maintain their integrity in the event of external dependency or internal system failures.
- Test your IoT devices to ensure they maintain their security controls in the event of failures such as:
    - Low or fluctuating battery power
    - Low memory or processing resources
    - Malfunctioning physical sensors or other attached devices
    - Ingestion of malformed inputs, including sensed data
    - Absence of network connection or intermittent connectivity

Key term definition

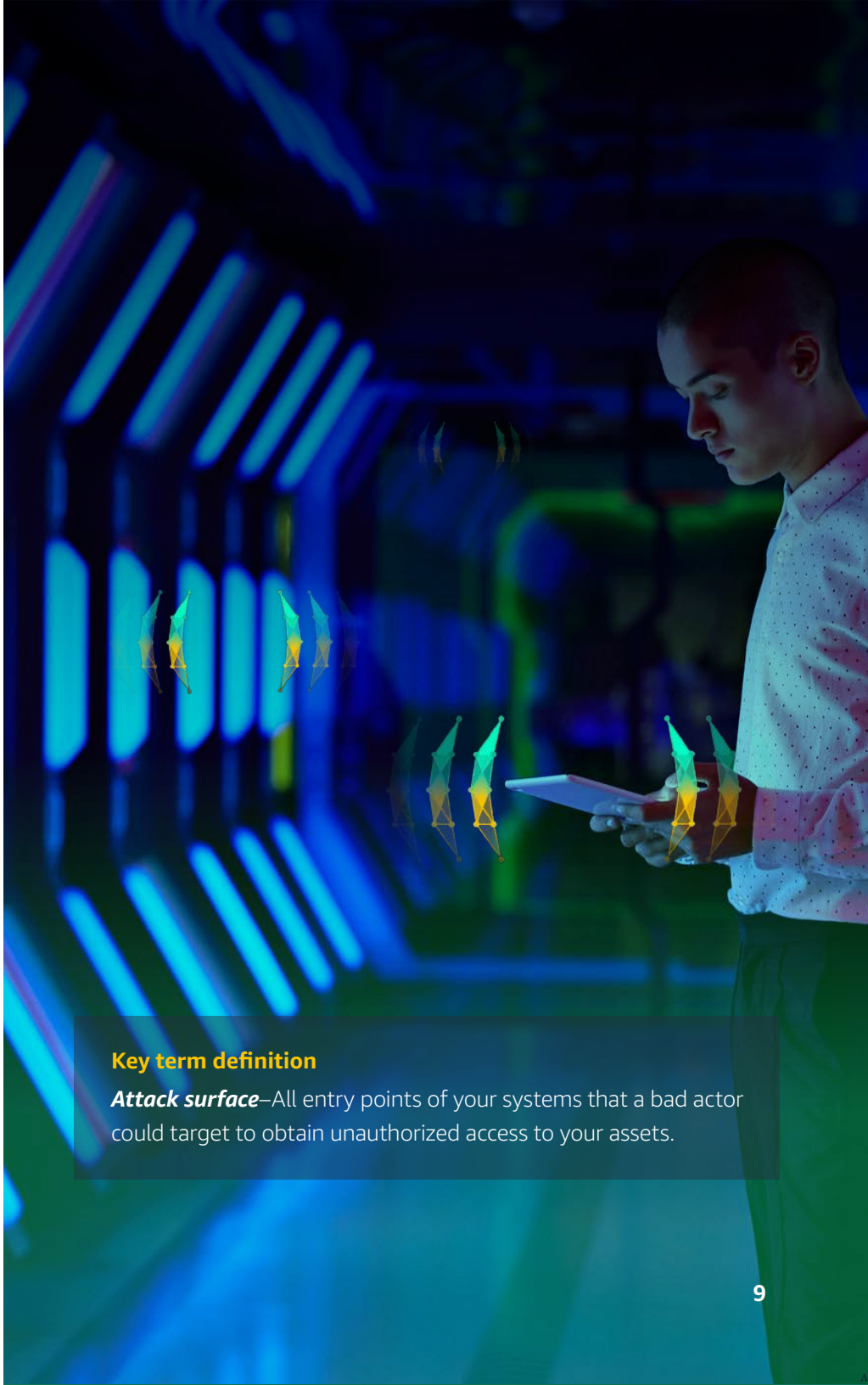
Canary test–A software test in which programming code changes are pushed to a small number of end users who have not volunteered to test anything, with the goal of ensuring code changes are transparent and work in a real-world environment.

7. Proactively assess the impact of potential security events

- Create and maintain a threat model that encompasses all assets and systems and is informed by your shared responsibility model.
- Identify and measure the impact of a possible security event on your IoT devices, their sensed environment and actuation systems, their associated on-premises and cloud infrastructure, human operators and supply chain systems, and processes.
- Consider different elements of security events such as scale, sophistication, and level of unauthorized access to assess potential impact. Create corresponding in-depth layers of prevention, detection, containment, and recovery.
- Provision your devices and field gateways with credentials that grant only the required privileges.

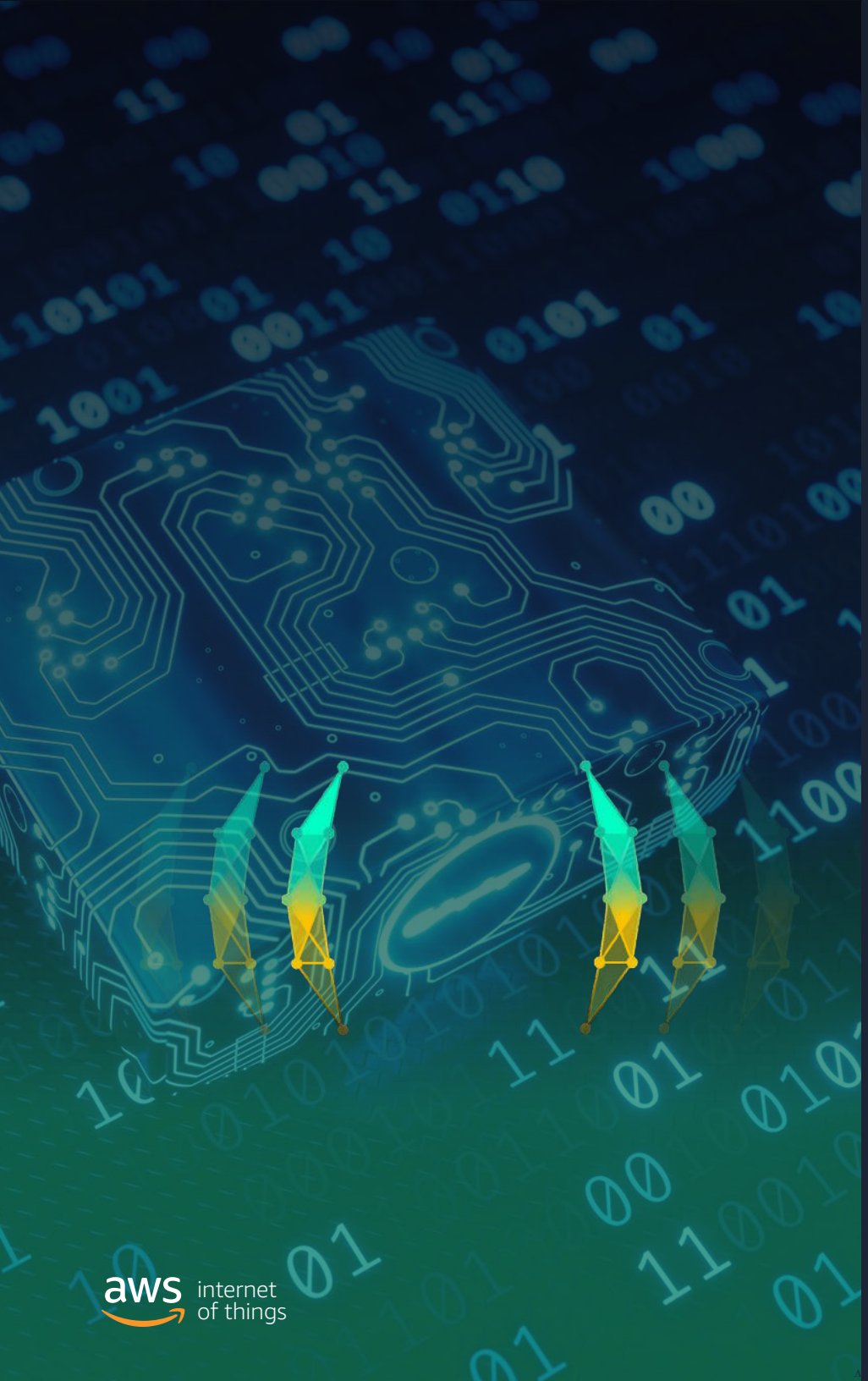
8. Minimize the attack surface of your IoT ecosystem

- Identify and eliminate unused entry points on your devices, field gateways, and backend systems.
- Disable unused device sensors, actuators, services, and/or their unused functions.
- Disable unused functionality or insecure-by-default configurations in your dependencies.
- Use the least possible number of dependencies, such as third-party libraries and network services.
- Employ secure-by-default configurations across your IoT ecosystem.
- Only add well-maintained dependencies and establish a mechanism to keep them up to date.
- Regularly review and identify attack surface minimization opportunities as your IoT ecosystem evolves.



Key term definition

Attack surface–All entry points of your systems that a bad actor could target to obtain unauthorized access to your assets.



aws internet of things

9. Avoid unnecessary data access, storage, and transmission

- Identify and classify data collected throughout your IoT ecosystem and learn its corresponding business use cases.
- Identify and execute on opportunities to stop collecting unused data or adjusting its granularity and retention time.
- Consider using tokenization and one-way cryptographic hashing wherever you don't need specific data in its entirety.
- Consider using asymmetric cryptography to protect data at rest on IoT devices—and devices that are only responsible for temporarily collecting and batching data—and periodically submit the data to other systems for processing.
- Only store and transmit data to central systems with strong ownership and strict security controls.
- Follow the principle of least privilege in granting access to any collected data.
- Identify and consider the unique capabilities of your IoT devices.
    - This could include mobility, actuation, sensory data collection and transmission, and ownership transfers that impact your regulatory and legal compliance.
- Consider privacy and transparency expectations of your customers and corresponding legal requirements in the jurisdictions where you manufacture, distribute, and operate your IoT devices and systems.
- Codify and publish your customer-facing privacy notice.

10. Monitor vulnerability disclosure and threat intelligence sources

- Stay informed about disclosed vulnerabilities, adversarial techniques, tactics, and procedures used in recent attack campaigns and assess their potential impact.
- Correlate information from vulnerability disclosures and threat intelligence with your auditing events, configurations, and metadata.
    - This will help you detect any trends of involvement or abuse of your infrastructure in the context of ongoing adversarial campaigns
- Create a vulnerability disclosure program for your IoT solutions to facilitate engagement with security researchers and encourage their responsible disclosure of potential security issues.

How AWS can help

Amazon Web Services (AWS) combines cloud services and edge software to deliver a truly end-to-end IoT security solution. AWS IoT provides you with the easiest, quickest, and most cost-effective path toward comprehensive, continuous, scalable IoT security.

AWS Cloud Security

AWS has been architected to be the most flexible and secure cloud computing environment available today. Our core infrastructure is built to satisfy the security requirements for military, global banks, and other high-sensitivity organizations. AWS uses the same secure hardware and software to build and operate each of our regions, so all of our customers benefit from the only commercial cloud that has had its service offerings and associated supply chain vetted and accepted as secure enough for top-secret workloads. This is backed by a deep set of cloud security tools, with more than 200 security, compliance, and governance services and key features.

Our shared responsibility model places the majority of the security burden on our shoulders, so you can stay focused on your business. AWS manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. You are responsible for building secure applications—but we can help you with that as well.

AWS provides a wide variety of best practices documents, encryption tools, and other guidance you can leverage in delivering application-level security measures. In addition, the AWS Partners Network offers hundreds of tools and features to help you meet your security objectives—ranging from network security, configuration management, access control, and data encryption.

Learn more by visiting the AWS Cloud Security resource page »

AWS IoT Security

In the cloud, AWS IoT provides preventative security mechanisms, like device identity and authentication, encryption, and access control to device data. At the edge, AWS IoT Greengrass authenticates and encrypts device data for both local and cloud communications—so that data is never exchanged between devices and the cloud without proven identity.

In addition, AWS IoT Device Defender continuously monitors and audits security configurations for compliance with security best practices and delivers alerts, so you can take actions—such as pushing a security fix to a device—to mitigate potential issues and risks. And to further support corporate governance and security regulations, AWS IoT stores device history 24 times longer than other offerings.

More details on security provisions for each of our IoT services are listed on the right. Click the links for in-depth information on each solution.

"AWS IoT Device Defender …is the easiest, quickest, and most cost-effective way for us to achieve and scale a high level of device security and anomaly detection. This protects our customers from service interruptions and [our] reputation for excellent customer service."

Peter Huisman
CTO, SolarNow

Read the case study »

AWS IoT Services

Amazon FreeRTOS is an operating system for microcontrollers that comes with libraries to help secure device data and connections.

AWS IoT Greengrass authenticates and encrypts device data for both local and cloud communications.

AWS IoT Core allows you to easily and securely connect your devices to the cloud by providing authentication and end-to-end encryption.

AWS IoT Device Defender is a fully managed service that helps you secure your IoT device fleet.

AWS IoT Device Management enables you to securely onboard, organize, monitor, and remotely manage IoT devices at scale.

AWS IoT Analytics is a fully managed service that makes it easy to run and operationalize sophisticated analytics on massive volumes of IoT data.

AWS IoT SiteWise is a managed service that makes it easy to collect and organize data from industrial equipment at scale.

AWS IoT Events helps you detect and respond to events from IoT sensors and applications.

AWS IoT Things Graph is a service that makes it easy to visually connect different devices and web services to build IoT applications.

Analyst Awards

AWS has won a number of awards for its IoT security offerings, including:

- IoT World "Best Security Solution" for AWS IoT Device Defender
- Frost & Sullivan Global IoT Platforms Market—Growth Innovation Leadership Radar Award
- IoT Eclipse 2019 IoT Developer Report—#1 IoT Cloud Platform

Conclusion

Enable the internet of (protected) things

Now that you have a better understanding of the shared relationship between cloud security and IoT security—and you're armed with proven best practices for both—it's time to start taking real steps toward safeguarding your devices, their connections, and their data. Visit the AWS IoT webpage now to access links to helpful resources, customer success stories, and guidance for specific use cases.

Get started on AWS »

Legal notice

This document is published for informational purposes only and does not serve as nor imply any guarantee of any measure of security or protection of devices, data, or any and all other assets. AWS recommends you consult with security experts both within and outside your organization before taking any actions recommended or detailed within this document.

For more information, review the AWS Service Terms »