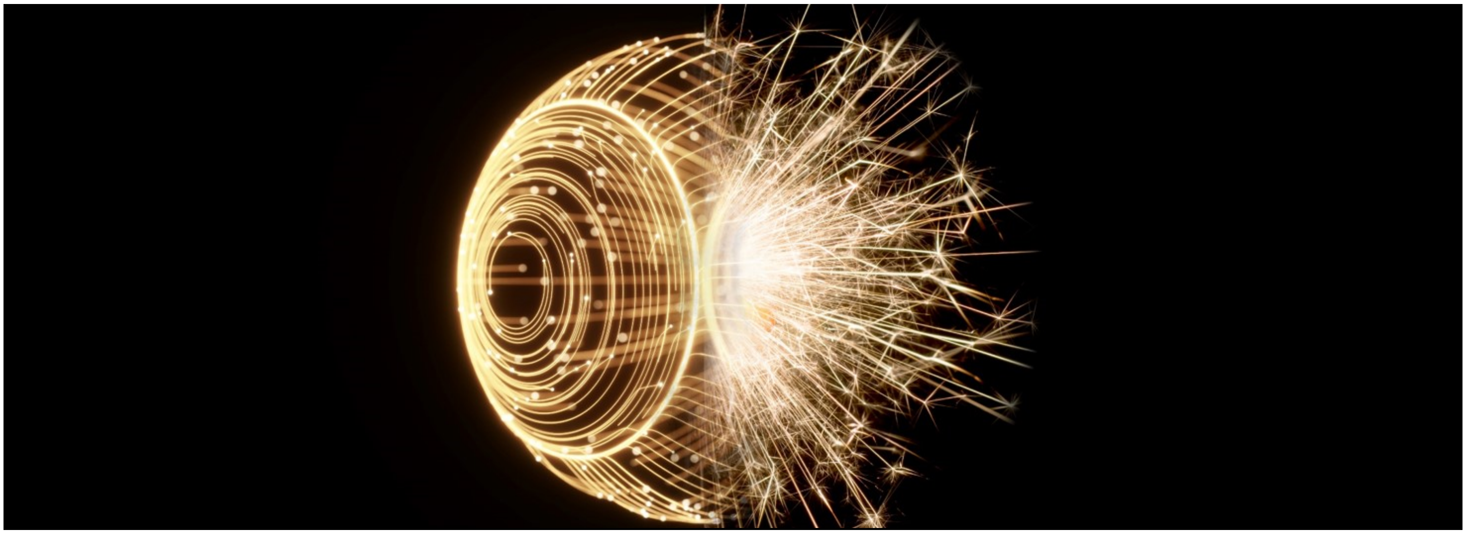


Increase IoT adoption through a secure cloud approach

A challenge

Internet of Things (IoT)-powered technologies have proliferated the modern digital world. Smart devices and sensors are able to collect and transform data into business insights more rapidly, at a lower cost, and with higher accuracy. Many businesses have realized the enormous benefit of leveraging IoT technologies to drive business decisions, and many major business processes incorporate some element of IoT.

Enterprises adopting IoT at scale will need to strategically plan to solve the cyber risk challenges associated with IoT, and also stay in compliance with increasing regulatory requirements. IoT technology exploits such as Mirai botnet and Stuxnet have resulted in significant financial loss and operational disruption over the past few years. Industry leaders and business innovators have a number of concerns—including low returns on investment (ROI), impacts to life or safety, or impacts to operations if a cyber-attack were to occur. As a result, the adoption of IoT has been slower than initially forcasted by optimistic technologists, pointing toward the need for a capability or framework to help businesses navigate through these risks, and harvest high-quality ROI.

Security is an enabler and will help increase enterprise scale adoption of IoT.

Break through the barrier

Deloitte's AWS IoT Cyber Risk Framework

To counter these threats, Deloitte Cyber Risk Services, powered by Amazon Web Services (AWS), developed an end-to-end IoT security framework. This framework is designed to help organizations establish a security-first posture, 'manage at-scale,' and leverage low-cost IoT capabilities. Deloitte's strategy to help companies push IoT adoption directly tackles cybersecurity, which is the biggest pain point in the digital cyber economy.

The AWS IoT Cyber Risk framework provides a broad approach to securing the full IoT stack.

Not only is the attack surface protected from the edge to the backend infrastructure, but a defense-in-depth approach is also applied. This approach facilitates security, vigilance, and resiliency at each layer across the IoT-based deployment.[1]

The framework outlines the capabilities the enterprise should evaluate and implement in order to have a robust security program to provide preventative, detective, and corrective controls across the IoT ecosystem, leveraging AWS native services. In addition to the capabilities outlined in the framework, it is important to extend Governance, Risk and Controls (GRC) function to the IoT ecosystem. The AWS services are highly interoperable and compatible with a customer's existing AWS cloud environment.

With the broad coverage of the security capabilities, some of the top security challenges in IoT can be effectively addressed, such as device operating system patching, improper encryption mechanisms, device default factory settings, device shadow, device event logging, distributed denial of service (DDoS) attacks, among many more. While this is a fairly comprehensive framework to start with, each enterprise needs to look at their specific use cases and evaluate if there are additional risks and requirements.

Secure

Secure means having risk prioritized controls to defend against known and emerging threats

Vigilant

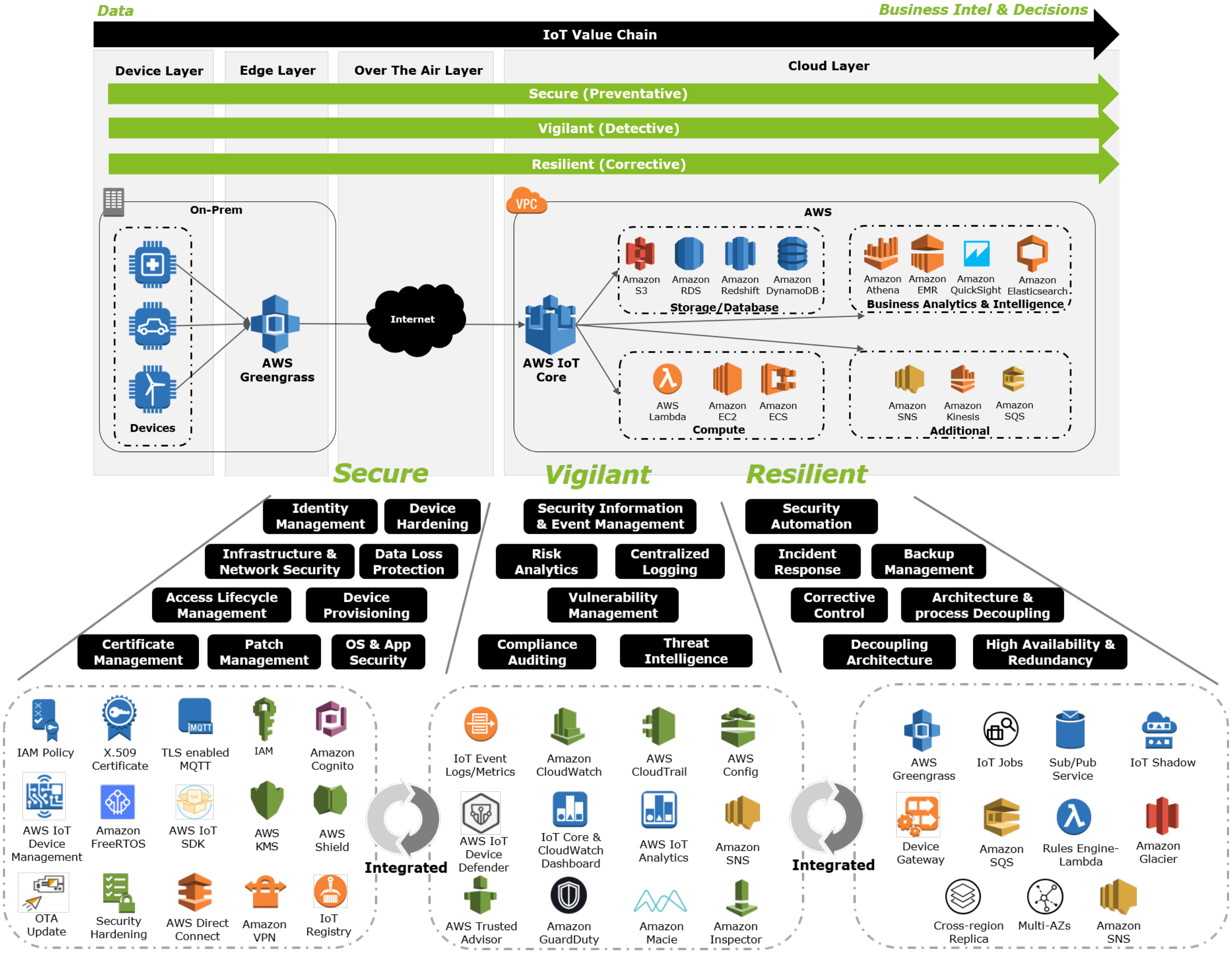
Being vigilant means having threat intelligence and situational awareness to identify harmful behavior

Resilient

Being resilient means having the ability to recover from, and reduce the impact of, cyber incidents

[1] https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Risk-Cyber-Intelligence-Center-A-new-approach-to-Cyber-Security-Juni-2017.pdf

Deloitte's IoT Cyber Risk Framework



Secure your IoT capability proactively

Preventative controls across an IoT infrastructure are imperative for creating a well-architected end-to-end security capability. The goal for architects and developers is to create an infrastructure robust enough to withstand potential cyberattacks. Deloitte's leading industry experience was leveraged to create effective security solutions, embedded with a range of preventative controls that are relevant to enterprises across a variety of industries. To this end, the Secure pillar of Deloitte's framework provides capabilities that include data loss prevention, device hardening, identity services, and network and infrastructure security.

Protect the data

IoT devices are prevalent in a range of industries across multiple unique-use cases. In some cases, the device performs minimal processing before forwarding the data upstream, while in other cases the device just acts as a data forwarder. The AWS IoT service provides secure movement of data for both data flows.

Deloitte's framework makes use of the AWS Message Queuing Telemetry Transport (MQTT) message broker and device shadow feature to encrypt communications with TLS v1.2 endeavoring to provide confidentiality of data. AWS IoT also supports a various number of cipher suites, which enable users to utilize their own choice of encryption method. By leveraging industry-leading practices, Deloitte provides a leading encryption capability reliant on native AWS services.

Lock down the environment

The security of an ecosystem is usually dependent on the weakest link. In IoT, the device/sensor is placed outside the traditional IT perimeter and sends important data to the core platform. Security starts with fundamentals, such as changing default passwords and usernames before allowing traffic from the internet, and securing devices through system hardening procedures, including changing default device service ports, like Secure Shell (SSH).

Over several years of delivering security services and capabilities, outdated operating systems have been a significant IoT concern. To that end, Deloitte often employs AWS FreeRTOS, a free microcontroller operating system, to replace outdated or insecure operating systems. Deloitte has also leveraged AWS services' free Over the Air (OTA) updates to provide consistent device updates, as well as the AWS IoT Device Management service, which supports at-scale device management.

Deloitte's experience in asset management provides valuable insight into organizing assets for maintenance and OTA updates.

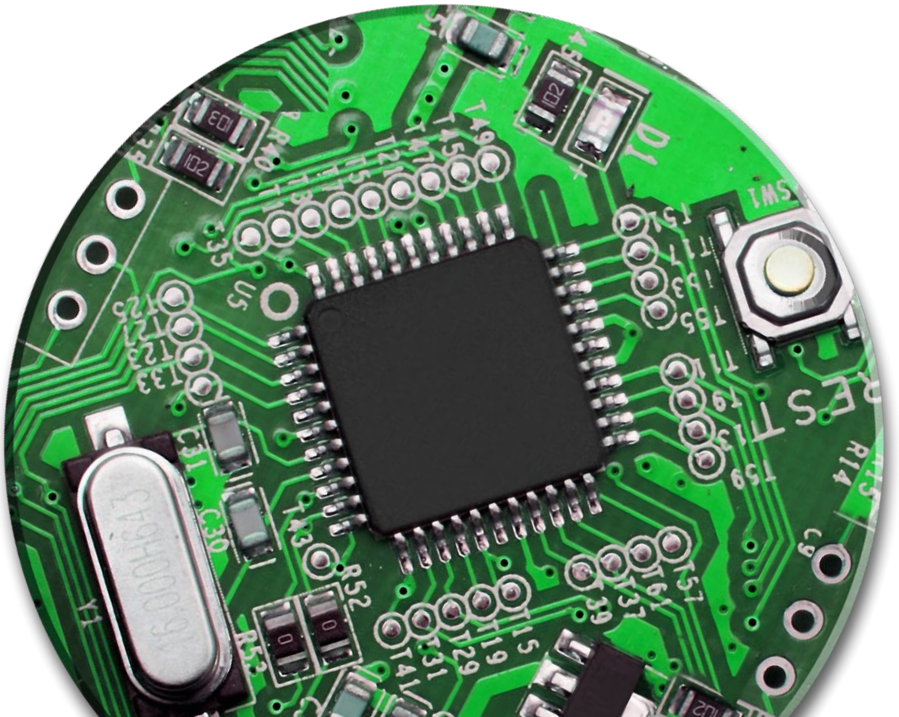
Grant permissions based on device identity

For devices to connect securely to the IoT service, authentication needs to occur at three principal levels:
(1) At the point of access to AWS, through security credentials and identity policies;
(2) when the device is onboarded to an IoT platform, using certificates and policies, and (3) when the IoT platform accesses other AWS services, through identity roles, policies, and security credentials. Deloitte leveraged native AWS services such as Amazon Cognito, the AWS IoT registry feature, AWS IoT Device Management, and federated identity services to create a rigorous device lifecycle management program.

To further increase device security, each IoT device is given a unique identity by deploying an X.509 certificate. The MQTT message broker then acts as a medium for authentication and authorization of the actions carried out. This provides a single point of access to and from the device and the IoT platform. Deloitte recommends the use of certificates by AWS IoT as a leading practice, as it reduces operational security overhead and eases management of certificates.

Route device and platform traffic properly

The AWS IoT service uses secure public endpoints residing on the edge. Device security can be further bolstered by utilizing AWS Shield, a DDoS mitigation service for public endpoints. When setting up a device with the AWS IoT Core service, AWS provides a categorization of devices based on the device using tagging and attributes of device shadow (a.k.a., the digital twin), such as light bulbs and motors. Each of these device types can then contain multiple associations, with a unique device name and defining attributes. Deloitte's framework leverages these native features to enable in-depth defense for the device endpoint. Furthermore, virtual network segmentation leveraging Virtual Private Networks (VPNs), Security Groups, and Network Access Control List (NACLs), can provide an additional layer of protection on traffic in the AWS cloud.



Be vigilant, it's always day one

Securing the configuration of IoT infrastructure is the critical first step for deploying IoT capabilities, but organizations should equally prioritize advanced detection capabilities to rapidly identify anomalous activities in their environments. Deloitte's Vigilant services integrate data sources across on-premises and AWS sources to provide security teams with contextual information that can be used to identify, detect, and respond more effectively to security threats initiated by IoT devices. Creating a truly vigilant environment includes employing security capabilities from device to cloud layers, such as centralized logging, threat intelligence,and monitoring.

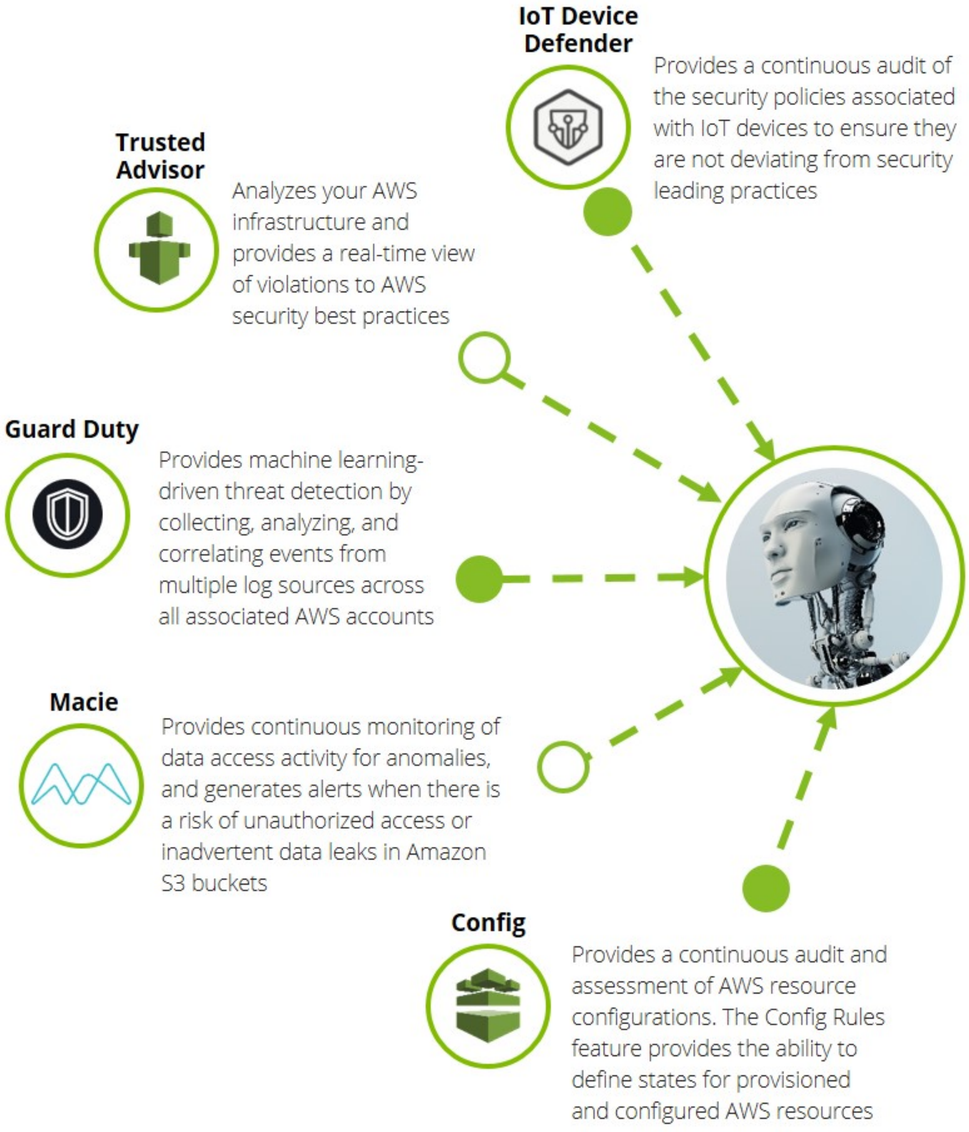
Collect evidence and track the actions of all devices

Capturing and centralizing logs can enable a truly vigilant organization. In the IoT world, these logs are spread across the platform, from device-level systems, to AWS infrastructure-level audits, data access, networks, and finally IoT- specific transmission and aggregation logs[3]. Deloitte's IoT Cyber Risk framework uses the rich log telemetry offered from AWS services to provide native log centralization by either consolidating logs into a single secure Amazon Simple Storage Service (Amazon S3) bucket (for use with third-party services), or using Amazon CloudWatch to aggregate and populate dashboards. It is important to also consider log sources external to the AWS ecosystem for a well-rounded approach to security monitoring. CloudWatch also offers a native alarm feature, allowing users to set thresholds and flags once certain criteria are met. A reliable logging capability enables effective event correlation and forensics exercises, leveraging the deployed Security Incident and Event Management (SIEM) system.

Interpret and learn the impact of each activity

The work of threat intelligence using Security Incident and Event Monitoring (SIEM) tools and services is essential to infer relationships between sequences of events, and ultimately attributing the same to malicious activity. This attribution offers actionable intelligence, enabling organizations to proactively protect against threats before they happen. In addition, Deloitte has leveraged cyber risk analytics to identify threats that have the likelihood of causing the greatest impact, empowering organizations to promptly focus on protecting the critical and vulnerable parts of the environment.

Deloitte has developed a threat intelligence capability suite using AWS native services, and third-party security products to provide broad threat intelligence for AWS IoT stacks. A portion of the services that Deloitte leverages are featured below:



IoT Device Defender

Provides a continuous audit of the security policies associated with IoT devices to ensure they are not deviating from security leading practices

Trusted Advisor

Analyzes your AWS infrastructure and provides a real-time view of violations to AWS security best practices

Guard Duty

Provides machine learning-driven threat detection by collecting, analyzing, and correlating events from multiple log sources across all associated AWS accounts

Macie

Provides continuous monitoring of data access activity for anomalies, and generates alerts when there is a risk of unauthorized access or inadvertent data leaks in Amazon S3 buckets

Config

Provides a continuous audit and assessment of AWS resource configurations. The Config Rules feature provides the ability to define states for provisioned and configured AWS resources

Watch behaviors and react Just-In-Time (JIT)

AWS detection services have the ability to send their findings to Amazon CloudWatch Events. This tool provides custom remediation functions using AWS Lambda (as part of the Deloitte's 'Resilient' procedures), and alerts management through already-existent enterprise Incident Management workflows, or Amazon Simple Notification Service (SNS) to send email or SMS alerts. Deloitte has built custom Amazon CloudWatch Dashboards to aggregate relevant metrics of AWS resources into a dashboard that reveals operational status and identifies issues at a glance, in real-time.

Deloitte's IoT Cyber Risk framework provides further value by utilizing the outputs of the threat detection services to create dashboards that assess compliance with organization's internal policies and regulatory standards. This provides visibility into the configuration of AWS resources and evaluates resource configuration changes against the desired configurations.

Approach 'no downtime' resiliency

The IoT market will likely see sizeable growth in the coming years, and AWS has spearheaded the development of services to manage the array of interconnected devices from a security and automation standpoint—the bedrock for a resilient capability. Deloitte's continued collaboration with AWS taps into the full potential AWS automation offers in designing and managing systems around an abundance of scalable, security-enabling services.

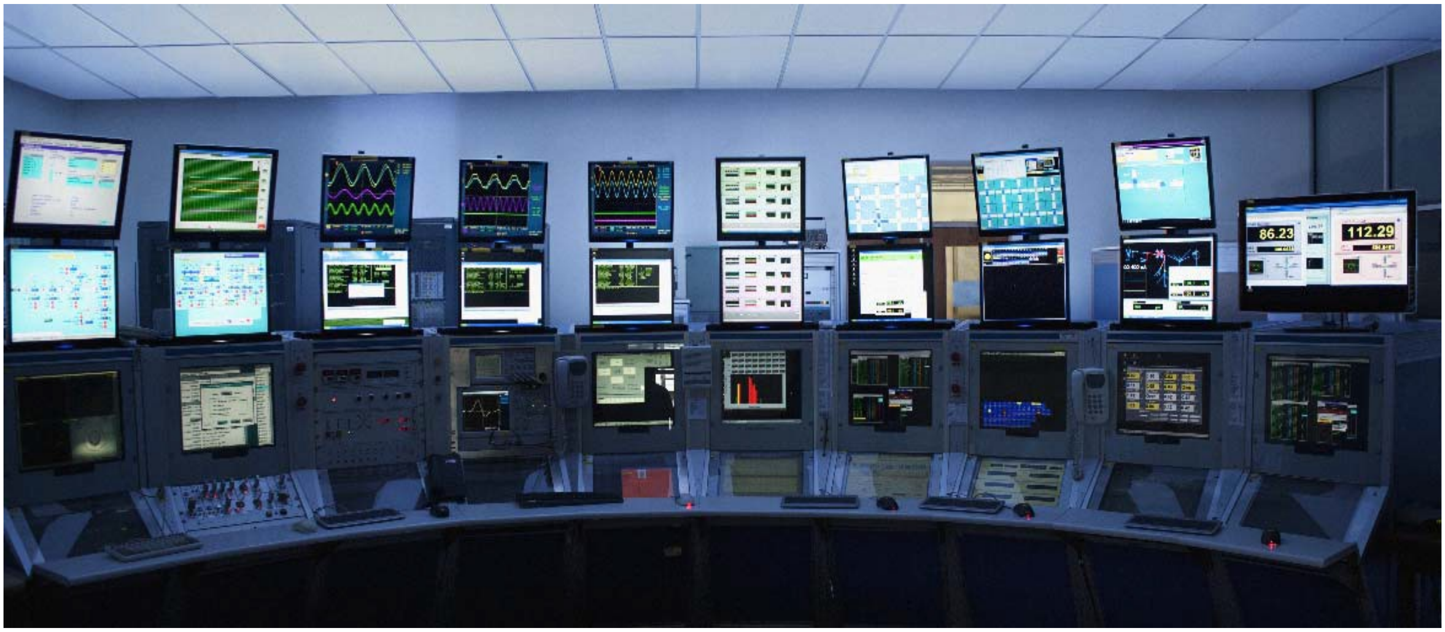
AWS provides a number of service offerings that address core security capabilities that affect resiliency, including decoupled architecture, high availability, redundancy, and security automation.

Decouple mission critical and long processes

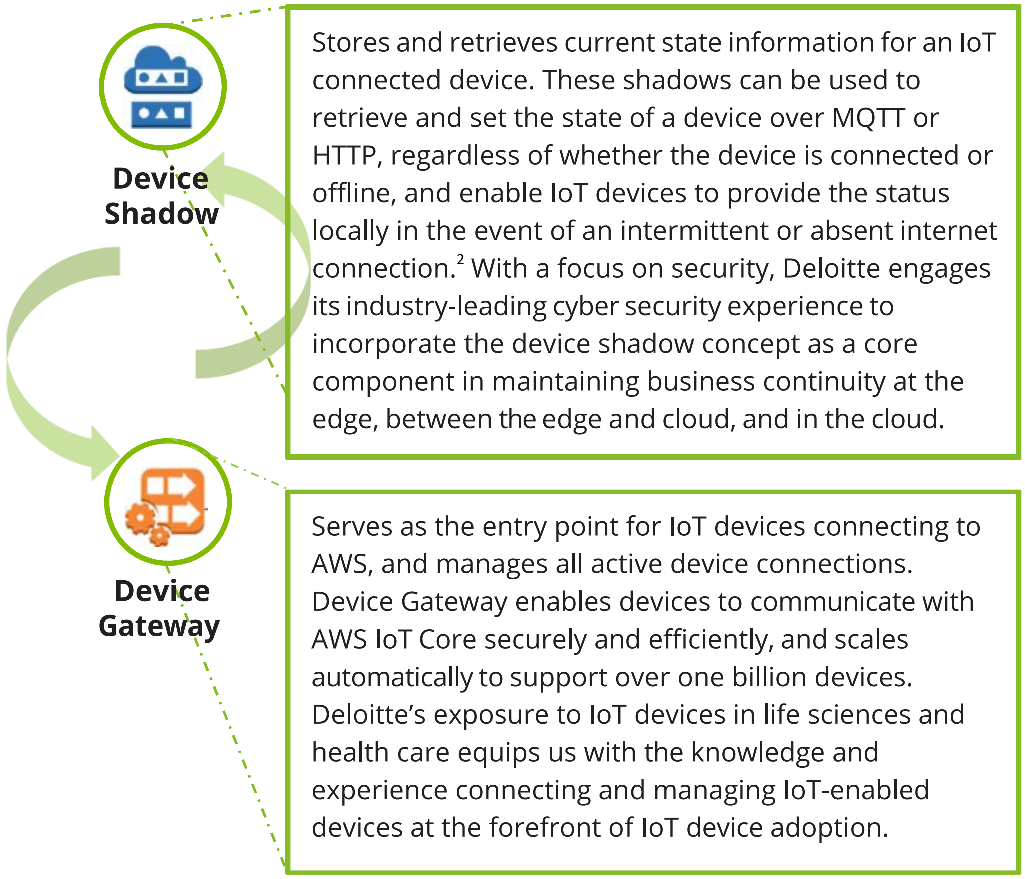
Amazon SNS and Amazon Simple Queue Service (Amazon SQS), core sub/pub messaging services, continuously provide easy-to-scale and fault-tolerant computing. These tools allow asynchronous service-to-service communication, providing event notifications for distributed applications to endpoints (e.g., subscribers) throughout a network. The sub/pub model provides flexibility to enable different IoT use cases based on business requirements, and behaves as a business logic enabler to trigger downstream integration with applications or services. The endpoints can work in parallel after reception of a message to activate processes, or buffer tasks in a queue. This decoupling is especially critical to an effective IoT capability, given that millions of devices can generate billions of requests.

Enable data resiliency

Deloitte's framework is designed to enable the creation of a resilient network, capable of responding to incidents by consistently backing up important and irreplaceable data.



With the advent of cloud computing into business operations, companies should move toward an "always-on" model of resilience, where downtime due to disruptions is reduced from minutes to seconds. AWS provides the infrastructure for companies to establish backups with low latency in the event of an external disruption, in the form of cross-region replication of virtual instances, multi-availability zone deployments, and data archiving services, like Amazon Simple Storage Service Glacier (Amazon S3 Glacier). As IoT rises to the forefront, AWS has taken steps to secure IoT devices as well. Deloitte draws experience-leveraging services like AWS IoT Device Gateway and AWS IoT Shadow to manage the exponential expansion that requires ongoing security coverage.

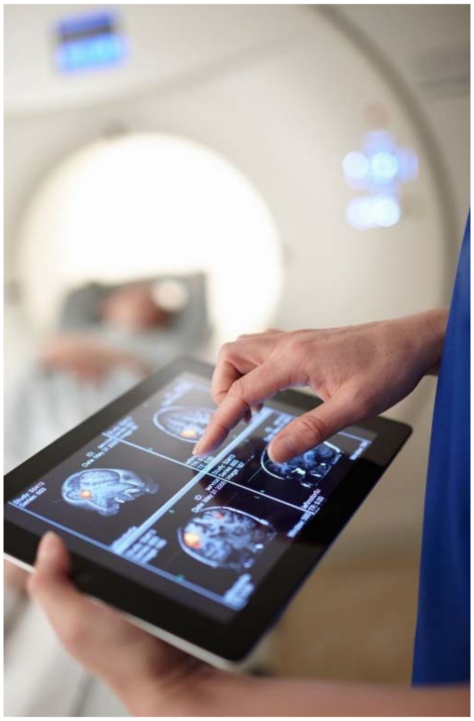


Device Shadow

Stores and retrieves current state information for an IoT connected device. These shadows can be used to retrieve and set the state of a device over MQTT or HTTP, regardless of whether the device is connected or offline, and enable IoT devices to provide the status locally in the event of an intermittent or absent internet connection.[2] With a focus on security, Deloitte engages its industry-leading cyber security experience to incorporate the device shadow concept as a core component in maintaining business continuity at the edge, between the edge and cloud, and in the cloud.

Device Gateway

Serves as the entry point for IoT devices connecting to AWS, and manages all active device connections. Device Gateway enables devices to communicate with AWS IoT Core securely and efficiently, and scales automatically to support over one billion devices. Deloitte's exposure to IoT devices in life sciences and health care equips us with the knowledge and experience connecting and managing IoT-enabled devices at the forefront of IoT device adoption.



Building a resilient network cannot granularly focus just on the device-level. Considerations and efforts need to be made across the AWS ecosystem to help achieve high availability, redundancy, and low latency cloud operations, in order to facilitate a network that can withstand cyber incidents with limited impact to the business.

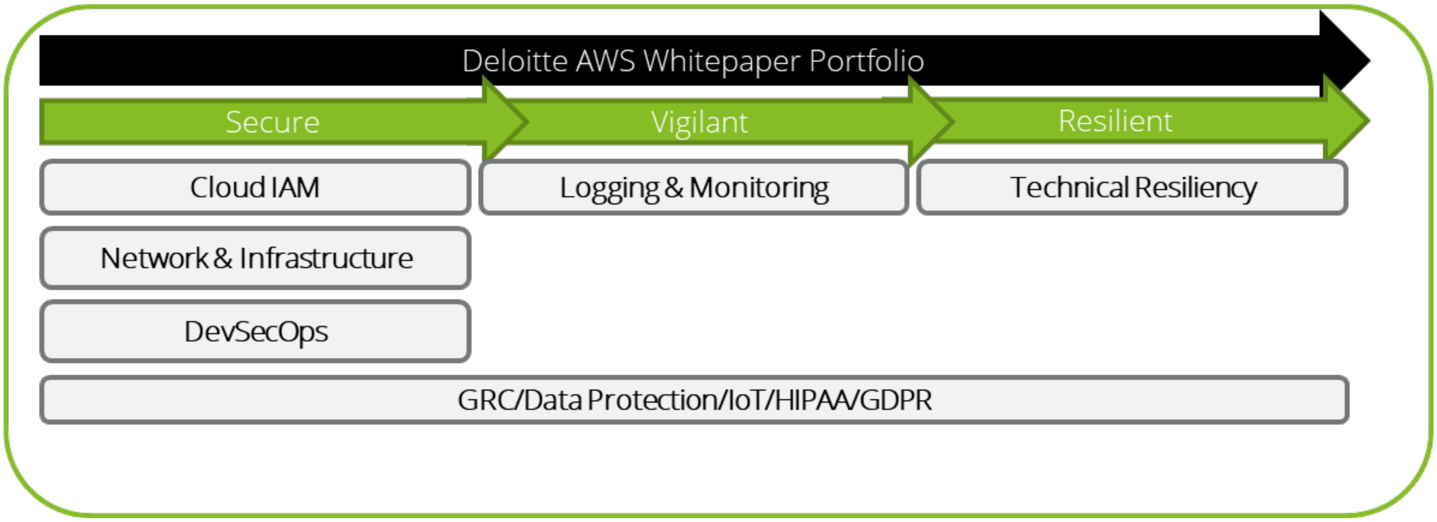
Let an AWS robot do the job

To equip and maintain a resilient network and up-to-date security patching, monitoring is imperative. Deloitte utilizes several AWS automation services to constantly monitor the security of resources and patch security holes. AWS facilitates security automation to run locally on IoT devices with services like AWS Lambda, AWS IoT Greengrass, and IoT Jobs. Making use of services like AWS Systems Manager, Deloitte possesses the tools and experience to configure automated security activities throughout the AWS IoT ecosystem. The monitoring capability can trigger auto-correction based on predefined rules and prescribed IoT jobs, thereby enhancing security automatically.

[2] https://docs.aws.amazon.com/iot/latest/developerguide/iot-security-identity.html#transport-security

The strength of the Deloitte / AWS relationship

Leveraging the Secure.Vililant.Resilient.™ framework and coupling with AWS security capabilities, Deloitte created a portfolio of whitepapers that cover the core Cyber Risk domains and tackle the top AWS security topics across industries.



Secure enabled controls are risk-prioritized and are implemented to support regulatory requirements and protect assets against known and potential threats.
Vigilant supports the establishment of monitoring and intelligence that enables the enterprise to identify and respond to unsanctioned activities – both unintentional and malicious.
Resilient enables a level of preparedness to reduce the impact of an incident and support the recovery of operations.

aws partner network

Premier
Consulting Partner

- Security Competency
- Government Competency
- Financial Services Competency
- Public Sector Partner
- MSP Partner

Our relationship brings together Deloitte's extensive industry experience in cyber and enterprise risk management with **the security-enabled cloud infrastructure of AWS**. In 2006, AWS began offering IT infrastructure services to businesses in the form of web services—now commonly known as cloud computing. Today AWS provides a highly **reliable, secure, scalable, low-cost** infrastructure that powers hundreds of thousands of businesses in 190 countries around the world, with **over a million active** customers spread across many industries and geographies.

Deloitte can help organizations adopt AWS securely and establish a security-first cloud strategy. Deloitte is a leading information technology and advisory company. Deloitte is an **APN Premier Consulting Partner and an AWS Security Competency Partner (Launch Partner)** and was one of the first eight organizations globally to achieve the **Security Competency** as a launch partner. Deloitte's vast experience in Cyber Risk, combined with its extensive experience with AWS and Cloud technologies, enable us to provide **end-to-end** security solutions.

Authors

Aaron Brown
Partner, Cyber Risk Services
Deloitte & Touche LLP
AWS Alliance Leader
aaronbrown@deloitte.com

Sean Peasley
Partner, Cyber Risk Services
Deloitte & Touche LLP
IoT Security Leader
speasley@deloitte.com

Ravi Dhaval
Manager, Cyber Risk Services
Deloitte & Touche LLP
Cloud & IoT Security Architect
rdhaval@deloitte.com

Piyum Zonooz
Global Partner Solution Architect
Amazon Web Services
pzonooz@amazon.com

Bill Chitty
Security Practice Lead
Amazon Web Services
chittyw@amazon.com

Contributors

Steve Ma
Consultant, Cyber Risk Services
Deloitte & Touche LLP

Kevin Wang
Consultant, Cyber Risk Services
Deloitte & Touche LLP

Lakshmi Modugu
Consultant, Cyber Risk Services
Deloitte & Touche LLP

Anunay Bhatt
Consultant, Cyber Risk Services
Deloitte & Touche LLP

Mark Roche
Consultant, Cyber Risk Services
Deloitte & Touche LLP

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting