eBook

Securing the Edge

Learn how industries are developing secure edge solutions with Amazon Web Services

Table of contents

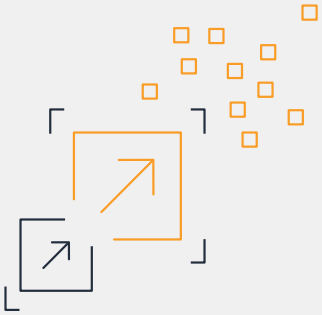
Industries advance to the edge

Services and applications have evolved from traditional on premises deployments to the cloud. Now, those cloud-based services are extending further to help companies realize opportunities at the edge. Where Internet of Things (IoT) devices and sensors used to send data to processors far away, today's edge allows IoT to compute close the point where the data is collected in near real time.

Across verticals, organizations are bringing compute closer to their endpoints, speeding up time to insights and reducing the amount of data transferred. Oil rigs use edge-powered IoT sensors to signal when it's time for maintenance, without having to connect back to the cloud. Hospitals are bringing telehealth to remote areas and relying on edge computing for solutions that connect, collect, and process medical data faster in an industry where seconds count.

As businesses increasingly adopt edge computing to solve key use cases, they also want to understand how security changes at the edge. Here are some points to keep in mind:

- **Device management:** Understand the status of all devices in your fleet to determine that they are configured securely, and updates are efficiently managed
- **Identity and access management:** Validate that robust identity management and permissions are in place so the correct people have access to the right resources and devices, in the right conditions
- **Data protection:** Categorize data based on levels of sensitivity and use encryption to protect data
- **Detection:** Continuously monitor workloads to identify potential security misconfigurations or unexpected behaviors
- **Infrastructure protection:** Define trust boundaries for networks and accounts, and verify secure system configurations and other policy-enforcement points including web application firewalls and API gateways
- **Incident response:** Implement mechanisms to respond to and mitigate security events



By 2023, there could be more than 20X as many smart devices operating at the edge, according to Gartner.

AWS for the Edge helps you unlock intelligence more securely

With Amazon Web Services (AWS) for the Edge, you can build and deploy high-performance edge applications that deliver real-time responsiveness and reduce the volume of data transferred. By extending its powerful suite of cloud services to the edge, AWS allows you to leverage familiar services in a new environment, while keeping costs down. Products built by AWS support both IoT and non-IoT deployments at the edge. AWS gives you an edge, with a more complete solution.

Secure endpoint connections. Security at the edge focuses on protecting layers for defense-in-depth. You will always control your data, including encryption, storage, movement, and retention. AWS services will help you guard identity and access, protect your data, secure your applications, and maintain compliance with regulations.

An extensive cloud infrastructure. You can run your applications on the most extensive, secure, and reliable cloud platform with the largest global footprint. On AWS, data processing and analysis is as close to your end users and devices as possible. AWS infrastructure is monitored 24/7 to help safeguard the confidentiality, integrity, and availability of your data.

A broad and deep selection of cloud services. AWS has 175+ fully-featured, integrated cloud and device services—many of which have specific edge capabilities.

A single-programming model. AWS helps you build more quickly and reduce costs with a single-programming model for the cloud. This model also applies to local devices and helps significantly shorten and reduce the cost of the development lifecycle.

Throughout this eBook, you'll find examples of how industries are building more secure edge solutions with AWS services.

Retail at the edge

Through the edge, retailers can personalize their shopping experience, sending coupons to customers' devices right as they step foot in a store, or leverage virtual reality to attract new customers. For companies to deliver innovative customer experiences like connected stores and autonomous checkouts, swift and safe transactions are critical. Retailers need to manage the status and configuration of point-of-sale and handheld devices.

AWS IoT Device Management and **AWS IoT Greengrass** help create a secure connection and keep devices up to date with the latest security patches, even when the devices are periodically disconnected. AWS IoT Greengrass seamlessly extends compute to the edge so devices can act locally on the data they generate, while still using the cloud for management, analytics, and durable storage. AWS IoT Device Management helps companies take mitigating actions such as pushing security fixes to devices.

Protect your data

AWS helps you protect your data, no matter where it resides. By extending cloud services to the edge, AWS allows retailers to safely operate with strong security infrastructure and safeguards. It used to be difficult to manage data security at the edge, as services weren't fully integrated. With AWS encryption solutions, your data at the edge is encrypted at rest and in motion. **AWS Key Management Services** (KMS) allow you to easily create and manage cryptographic keys while controlling their use in your applications and across a range of services. It's secure, resilient, and provides you with logs of key usage.

With **AWS Certificate Manager**, you'll easily be able to provision, manage, and deploy both public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates at the edge, for use with AWS services as well as your internal resources. You can manage your own encryption keys with **AWS CloudHSM**.

You can help protect all of the secrets like database passwords needed to access your edge applications and resources with **AWS Secrets Manager,** which rotates, manages, and retrieves credentials, API keys and more. You can use machine learning through **Amazon Macie** to automate discovery of sensitive data, while lowering the cost of protecting your data.

With **AWS IoT Device Defender**, you get continuous auditing of your edge IoT configurations to help you verify that they are maintaining security best practices. **AWS CloudTrail** lets you log and monitor account activity across your AWS infrastructure. **Amazon GuardDuty** monitors for malicious activity and unauthorized behavior to provide an intelligent and cost-effective threat detection service.

Manufacturing at the edge

For manufacturing, edge presents opportunities to increase operational efficiency and save money. Edge computing can help you collect, process, and analyze data to enable predictive maintenance, improve quality control, and dramatically enhance worker safety with near-real-time alerts, industrial robot fleet management, and simulation.

AWS IoT Sitewise can help you securely connect shop-floor equipment to the standard OPC-UA protocol and to powerful analytics tools in the cloud. It allows companies to monitor operations across facilities and analyze industrial equipment data. Instead of lag time while automated devices communicate with servers in the cloud, low-latency applications are extended to the edge.

Secure your applications

As manufacturers look to increase efficiency and keep costs down with edge applications, they simultaneously need greater assurance that those applications are protected. To better secure your critical web applications against security events, AWS offers several services. **AWS Web Application Firewall** (AWS WAF) lets you create security rules to protect against common cybersecurity attacks. It helps you quickly update security when issues arise, such as the detection of bad bots or vulnerability exploits. Managed rules for AWS WAF give you a quick starting point with rules that can be deployed in front of your web applications, even at the edge.

Improve the security across your edge applications with always-on detection and automatic inline mitigations from **AWS Shield Advanced**, which helps protect against Distributed Denial of Service (DDoS) attacks. You get greater availability protection when you combine AWS Shield Advanced with **Amazon Elastic Compute Cloud, Elastic Load Balancing, Amazon CloudFront, AWS Global Accelerator** and **Amazon Route 53**.

AWS Shield Advanced provides extended detection and mitigation against sophisticated DDoS attacks, with near real-time information on security events, and includes AWS WAF. You also get 24x7 access to the **AWS DDoS Response Team** and economic protection against DDoS related spikes in your workloads, including edge workloads.

Telecommunications at the edge

As edge becomes more prevalent across industries, companies increasingly rely on the ability to run low-latency applications with 5G-native security. **AWS Wavelength** extends AWS Compute at the edge of the 5G network. This way you can run applications right in the communications service providers' (CSP) datacenters, without separate contracts from each telecom provider. Developers can build the next generation of ultra-low latency applications using the same familiar and powerful AWS services, APIs, and tools they already use today. They get the same AWS benefits, like elasticity, high-availability, and pay-as-you-go pricing, while optimizing the use of their networks.

Guard identity and access

AWS Identity and Access Management (AWS IAM) and **Amazon Cognito** help companies configure secure access to their edge applications, and provide users with an easy way to sign up and sign in.

Previously, options to manage identities and access were limited at the edge—IoT devices and processes were not fully integrated, leading to potential authentication issues. AWS IAM provides multi-layer security to allow identity and access management through a seamless process. With AWS IAM, you can use pre-configured policies or utilize those as a starting point to create your own custom policies. These policies control access to configuration as well as data operations, promoting greater security.

Amazon Cognito allows you to add user sign up/sign in and control access to your web and mobile applications. Your customers have the flexibility to sign in through popular social identity providers as well as enterprise identity providers, more simply and securely. Amazon Cognito can scale to as many users as you acquire through its secure user directories. Your applications will also be able to get unique identities for users. Amazon Cognito provides enhanced security for your applications and your users. It supports multi-factor authentication and data encryption. You can define roles and map users to give your application access to the exact resources authorized for each user.

Healthcare at the edge

Healthcare organizations are seizing the opportunity to improve patient care with faster insights from ultra-low-latency applications. With edge solutions, providers have achieved local image capture and analytics, allowing for swifter coordination of care while protecting patient information. Edge applications can also help expand telehealth services to underserved areas. Now, doctors can use edge technologies to perform remote surgery using robotic assistance, relying on ultra-low-latency applications for near-real-time communication—in an area where seconds are critical.

AWS Snowball Edge allows local processing of data and secure transit to the cloud, which enables healthcare companies to maintain their HIPAA compliance requirements and secure, compliant archive to the cloud.

Meet compliance goals

In a highly regulated industry, healthcare organizations need to adhere to specific compliance demands across their workloads—even those operating at the edge. With AWS for the Edge, you inherit the benefits of built-in security controls from AWS. To aid your compliance efforts, AWS regularly achieves third-party validation for thousands of global compliance requirements that we continually monitor to help you meet standards for finance, retail, healthcare, government, and beyond. You also receive access to tools you can use to reduce your cost and time to run your own specific security assurance requirements. AWS supports more security standards and compliance certifications than any other offering, including PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171, helping customers satisfy their compliance requirements for various regulatory agencies around the globe.

To help keep you informed of the AWS security and control environment, AWS provides communication through several channels. AWS maintains listings of industry certifications and independent third-party attestations. Whitepapers and web content supply additional information on AWS security and control practices. Under NDA, you have direct access to certificates, reports, and other documentation. AWS maintains a list of AWS Services in Scope of AWS assurance programs for your reference.

Get started with AWS for the Edge today!

Learn more about AWS for the Edge and find resources to help you build and deploy your AWS edge solution in the AWS Partner Network.