Maximizing application security in the era of everything cloud

Build, scale, and secure your applications on AWS

INTRODUCTION

Navigating today's network security landscape

In this age of digital transformation, edge computing, cloud first, and cloud everything, establishing the security and availability of your application and its data is a critical mandate for every industry and segment.

Responding to this imperative involves making the right choices and following best practices across three key areas: 1) build in an environment that offers a secure infrastructure, 2) establish appropriate data protection controls, and 3) defense in depth to minimize security risks at every level.

First, protecting your applications starts with infrastructure. More specifically, it means verifying that your applications are running on infrastructure that uses sophisticated security across hardware and software. And in today's cloud-first world, this also means working with a cloud provider that delivers powerful built-in protection for secure compute across every type of instance.

Next, protect your application data. Use fine-grained security policies and layered encryption to isolate your data in transit, in use, and when stored. Ideally, these should include various forms of encryption, auditing capabilities, and identity and access management (IAM).

Finally, you will need security that remains resilient at every level, even as your applications and their data move between environments. Ideally, you should use services that can filter unauthorized traffic and rapidly detect and remediate threats and misconfigurations. You should also have robust network redundancy and global resiliency to establish availability.

While protecting your applications across these areas can be challenging, the reward is an enhanced security posture that minimizes the risk of a security event. By achieving and maintaining robust application security, you can accelerate innovation, create better experiences for customers and business users, and enhance flexibility.

In this eBook, we will outline how Amazon Web Services (AWS) enables you to capture those benefits and more, providing you with the application security needed to thrive in the modern era.

Staying ahead of security challenges

To effectively protect applications and their data, security solutions must mitigate risk while seamlessly fitting into existing IT environments. This poses multiple challenges in today's digitally connected, cloud-first world, including:

Expanded attack surface

With increasing numbers of mobile users, branch offices, data, and services located both inside and outside of the protections of traditional security appliances, organizations are struggling to keep pace and maintain the security, privacy, and integrity of their networks and cloud infrastructures. A security event can hinder your operations and slow innovation.

Complexity

Organizations use multiple point-products to handle security requirements. This often results in increasingly complex security practices and policies and difficulties scaling securely across multiple disparate solutions. Today, many organizations have prioritized simplifying and consolidating their security strategy to drive faster innovation.

Lack of integration with cloud-native services

As businesses migrate to the cloud, they are looking for feature-rich cloud-native security services that can scale to handle bursts of traffic, enable pay-as-you-go cost-efficiencies, and are already integrated with the services and security necessary to protect their environments. These factors contribute to delivering enhanced experiences for consumers and business users alike.

Protecting the way you build, run, and deploy your applications

Now that we've explored, in general terms, what it means to secure your applications—and the specific challenges you can expect to face along the way—let's look at how AWS provides a secure, trusted environment for you to build, run, and scale applications in the cloud.

Secure next-gen infrastructure

The AWS modern compute infrastructure and underlying environment for the next generation of **Amazon Elastic Compute Cloud** (Amazon EC2) instances, the **AWS Nitro System**, provides built-in security at the hardware level to continuously monitor, protect, and verify hardware and firmware. You can also run cloud-native applications more securely with the help of **AWS Graviton processors**, which are custom-built by AWS with capabilities that enable you to run cloud-native applications securely and at scale.

AWS Shield is an infrastructure-level distributed-denial-of-service (DDoS) protection service for AWS services that provides always-on network flow monitoring and in-line mitigation. When used with **Amazon CloudFront**, **Amazon Route 53**, and **AWS WAF**, AWS Shield Advanced automatically helps maintain application performance and reduce downtime during common DDoS events.

Continuous protection for your application data

Data flowing across the AWS global network is encrypted by default at the physical layer before it leaves our secured facilities. You have the option to add multiple levels of encryption to protect your applications and their data.

For stored data, **Amazon Simple Storage Service** (Amazon S3) is an object storage service that delivers unmatched security, compliance, and audit capabilities. Amazon S3 encrypts object uploads to their buckets.

For data at rest or in transit, **AWS Network and Application Protection** services enable you to enforce fine-grained security policies at every network control point across your organization. These services—such as **AWS Network Firewall**, **AWS WAF**, **AWS Shield**, and **AWS Firewall Manager**—enable you to establish an in-depth security approach with central management.

Importantly, AWS is committed to helping your organization stay ahead of threats both now and in the future. As one of the industry's largest cloud providers, AWS has broad visibility into evolving security needs across the globe. We rapidly reinvest what we've learned from this threat intelligence into managed security rules and our security services.

With AWS Network and Application Protection services, you have flexible options for how and where you build your network architecture—from defining private subnets to public internet-facing networks. You can pay as you go and only for what you need.

Enhanced security at every level

With AWS, you can easily apply a defense in depth strategy to your applications. From filtering unauthorized traffic, to rapidly detecting and remediating threats and misconfigurations, and more.

For example, many organizations are seeking specific protections against DDoS events—a common and costly digital threat that seeks to overwhelm your applications with malicious traffic. AWS Shield delivers managed protection against DDoS events, and it can be integrated with native perimeter security services to enforce network controls at the perimeter.

As your application data moves between different environments, there are several easy options available for you to encrypt your data as it moves across the AWS network—providing redundancy and resiliency through the way the **AWS Global Cloud Infrastructure** is designed.

AWS enables you to rapidly detect and remediate threats and misconfigurations across various network environments. For example, **Amazon GuardDuty** monitors activity within your AWS environments and correlates the resulting data with threat intelligence from multiple sources. This helps detect anomalies and provides additional risk context as your applications and data move throughout, into, and out of your network.

AWS Nitro System: A deeper look

The AWS Nitro System provides enhanced security that continuously monitors, protects, and verifies instance hardware and firmware. It minimizes the attack surface by offloading virtualization resources to dedicated hardware and software. Finally, its security model is locked down and prohibits administrative access—minimizing the possibility of human error and tampering.

Watch this video to learn more ›

Exploring the top use cases

In addition to the flexible built-in protections of AWS security services that can be deployed at the various network control points to augment defenses for your organization. Here are two compelling examples:

OutSystems: Protect internet-facing apps and data from external threats

As software vendor **OutSystems** grew its business, it needed a scalable security solution to further protect customers from cyber issues and reduce operational overhead. Using **AWS Shield Advanced**, a managed DDoS protection service, OutSystems successfully scaled to manage the complexity of more than 4,000 web application firewalls (WAFs) while reducing the time required to respond to malicious indicators from two hours to under five minutes.

"Using AWS services, we reduced 2 hours of work to less than 5 minutes."

Igor Antunes, Head of Security Architecture, OutSystems

Read the story ›

Baazi Games: Block malicious traffic originating from cloud workloads

Baazi Games worked with AWS to secure its serverless cloud architecture while keeping its startup business model lean and cost-efficient. Over one 8-month period, the company repelled more than 50 DDoS incidents, including major attacks coming from approximately 7,000 different IP addresses that targeted different apps on its gaming platform, website, and APIs. The company ensured business continuity even while defending against attacks that lasted up to a day.

"We saw immediate results by preventing attacks at the door, and have seen a steady decrease in DDoS activities since."

Avneet Rana, Co-Founder & CTO, Baazi Games

Read the story ›

Understanding the AWS Shared Responsibility Model

Security and compliance are shared responsibilities between AWS and its customers. Understanding the AWS Shared Responsibility Model—and effectively putting it into practice—is one of the most critical aspects of securely building, running, and deploying applications on AWS.

Our security responsibilities

AWS is responsible for the security of the cloud—that is, protecting the infrastructure that runs the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

Your security responsibilities

As an AWS customer, you are responsible for security in the cloud. Your specific responsibilities—the amount of configuration work you must perform—will be determined by the AWS Cloud services that you decide to use.

With services classified as infrastructure as a service (IaaS), such as Amazon EC2, you are required to perform necessary security configuration and management tasks for the operating system, applications, and your data. For abstracted services, such as Amazon S3, AWS operates the infrastructure layer, the operating system, and the environments, and you are responsible for managing your data (including encryption options), classifying your assets, and using IAM tools to apply the appropriate permissions.

Learn more about the AWS Shared Responsibility Model ›

Next steps

The solutions described in this eBook allow you to centrally enable a security baseline across your organization and consistently enforce protections even as new applications are created. You will be able to manage your security posture across your AWS accounts centrally, and you will be free to scale with customer demand without increasing security complexity.

Deploying AWS Network and Application Protection services not only helps protect your users, applications, and data—it can also lead to measurably better business outcomes. With enhanced security, you can conduct business with greater agility, improve customer experience, innovate with confidence—and launch new products and services faster.

In short, AWS provides your organization with the tools you need to deliver a better security posture at the edge.

Learn more about AWS Network and Application Protection services ›