AWS SECURITY

5 ways a secure cloud infrastructure drives innovation

Inspire confidence and activate creativity with AWS infrastructure and security services

Table of contents

INTRODUCTION

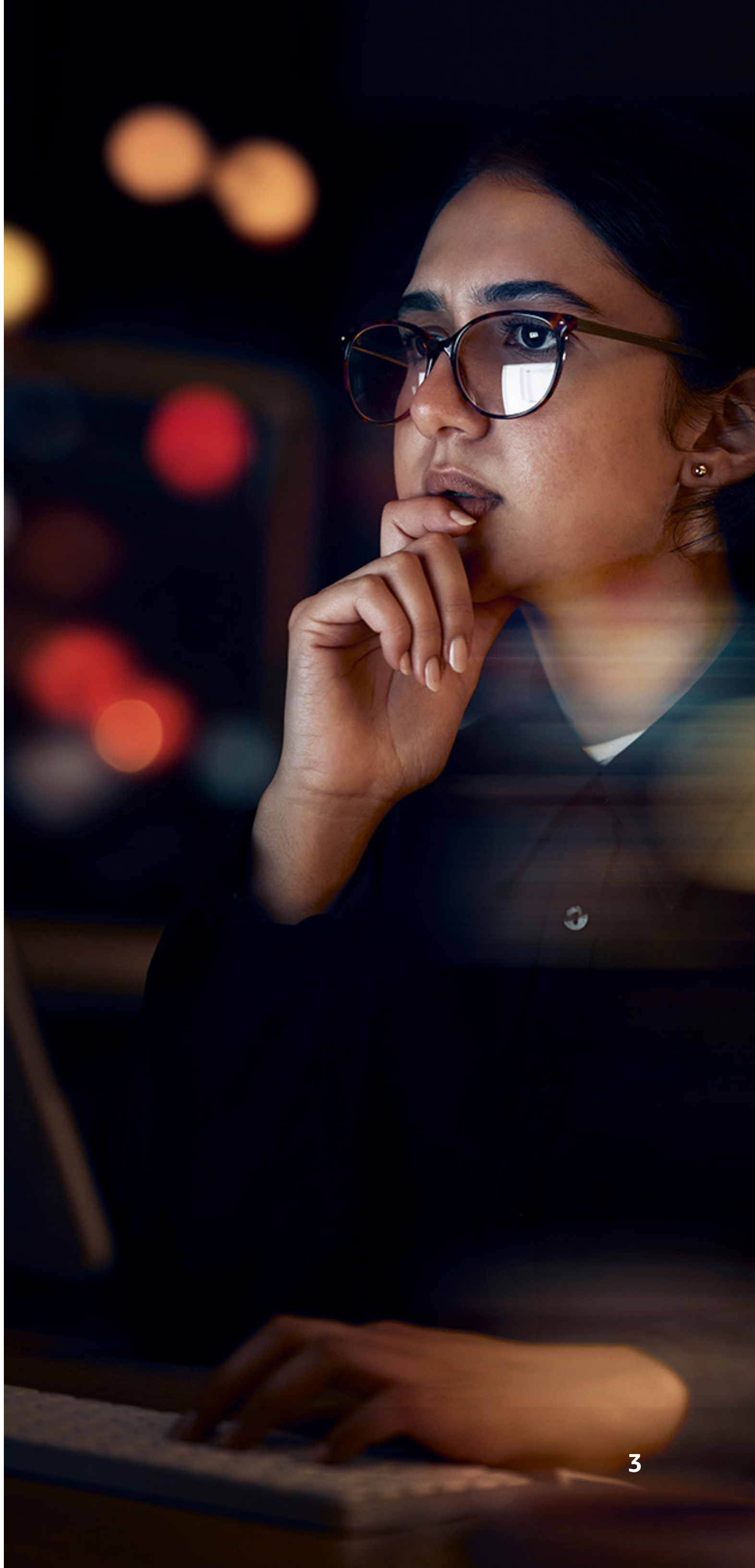
Reinforce a culture of innovation with a commitment to secure infrastructure

Even in times of economic uncertainty, organizations need to continue innovating to drive differentiation and competitive advantage. Innovation allows businesses to discover those operational efficiencies and new streams of revenue. Many factors can affect the ability to innovate quickly and at scale, and they can vary according to company size and industry. But one element stands universally critical: security.

Modern organizations must move fast and experiment, but do so in a secure way from the start. Yet traditional development processes put security at the end. This can create the impression that security is a bottleneck or barrier to innovation.

Building a proactive security strategy on top of a secure cloud infrastructure means integrating security into the innovation process from the start. Over time, security can catalyze, foster, and reinforce a culture of innovation that continuously improves production, quality, agility, risk management, and resource optimization.

Driven by a proactive security strategy and built on a secure, scalable infrastructure, organizations can spark innovation that helps them succeed in today's economic climate—and thrive as the future unfolds.



5 ways a secure cloud infrastructure drives innovation

In this section, we will explore customer stories that demonstrate how your organization can accelerate innovation with secure cloud infrastructure.

1

Moving fast, staying secure

Trusted, resilient cloud infrastructure provides the secure guardrails that allow your teams the freedom to move faster, which can lead to shorter production cycles. Building securely should be the path of least resistance—with no trade-off between security and speed.

Southwest Airlines invests in its security posture with AWS

By allowing Amazon Web Services (AWS) to manage infrastructure on its behalf with the **AWS Shared Responsibility Model** and using built-for-cloud elements to gather security insights, **Southwest Airlines** gained the freedom to focus on building innovative applications—not managing infrastructure.

Previously, it took Southwest five to six weeks to implement new security controls. Now, that process takes only one week. The airline also reduced the time needed for development ideation, production, and activation from years to weeks or months.

Read the full success story ›

Southwest®

"If our security system is not running, we're not flying. So having the robust security posture and capabilities we achieve on AWS is critical for us."

Jon Barcellona, Former Cybersecurity Engineering Director at Southwest Airlines

Payble accelerates path to CDR compliance by collaborating with AWS Partners

In 2020, Australia enacted the Consumer Data Right (CDR) initiative, which mandated that any organization wishing to receive open banking data must be approved as an accredited data recipient (ADR). As a financial services startup operating in Australia, **Payble** needed to access the benefits of CDR compliance as quickly as possible—but the path was complex and time-consuming.

Working with AWS Partners, Payble completed the ADR application six months faster than the industry average, ultimately building an audit-ready CDR environment in only four weeks.

Read the full success story ›

Payble™

"By using our solution's automation capabilities, Payble didn't have to start from scratch when trying to understand CDR rules and create security policies. Instead, they could move quickly and effectively on the entire process."

Sandeep Kumar, CEO of Astero, an AWS Partner

2
Focusing on customer outcomes

By building on a secure cloud infrastructure, you can help mitigate security events, automate protection, and strengthen the security of your applications—enabling application owners to focus on what is important for their customers. This can lead to less downtime, better customer experiences, and a higher quality bar for your products and services.

Dropbox layers AWS security services to scale its signature service protection

Dropbox acquired the electronic signature and storage solution HelloSign in 2019. HelloSign grew quickly to more than 80,000 customers in 2021 and recognized the importance of protecting its customers' personally identifiable information (PII) and payment card information data. The company wanted to make its service both secure and highly available, which required protecting its services from distributed-denial-of-service (DDoS) events and other security threats.

HelloSign used **AWS WAF** to filter traffic before it hit the company's web servers—mitigating incidents in only 15–30 minutes. It also used AWS WAF to create customized rules that proactively block common security event patterns and apply geographic or country-specific blocks to areas under US sanctions.

AWS WAF and other AWS security services helped HelloSign avert 12 DDoS events, save roughly 120 hours of work per week through automation, achieve visibility into its security posture, and implement security best practices.

Read the full success story ›

Dropbox Sign

"Using AWS, we were able to mature our security model and automate manual processes. We saved about a million dollars per year in triage time for security operations, staffing, and licensing costs."

Mark Dorsi, Former Director of Security at HelloSign

3

Increasing agility

A secure cloud allows your business to innovate and move with agility and availability to meet ever-changing customer demands, economic conditions, and threat landscapes. With the right mix of secure infrastructure and cloud-based services, you can continually help enforce your security controls by automating infrastructure and application security checks and enabling faster, safer testing and deployment.

ZS delivers always-on security best practices using AWS security services

ZS Associates (ZS), a management consulting and technology firm focused on transforming global healthcare, sought to create greater visibility and simplify management of its security posture. The company's global client base faced diverse, complex, and demanding security challenges, intensifying the need for ZS to develop methods of protecting its customers that could be rolled out in fast, highly scalable ways.

Using AWS, ZS built a scalable, comprehensive security landscape that automated time-consuming manual security procedures and eased the rollout of cloud architecture for its clients. The solution saved ZS thousands of hours per month in security management and allowed ZS to onboard clients three times faster.

Incorporating AWS security allowed ZS to improve its agility, helping the company free up resources to tap into innovative analytics and machine learning (ML) capabilities. Today, the company's employees use these cutting-edge technologies to work collaboratively with clients and help them solve their toughest challenges.

Read the full success story ›

ZS

> **"Using AWS helps give us central visibility. It's always on and always live. It's changing our whole mindset."**

Rujuswami Gandhi, Former Director of Cloud Services at ZS Associates

4

Managing and minimizing risk

Innovative cloud solutions can help automate tasks in novel ways, reducing human configuration errors and simplifying how your security team collaborates with developers and operations teams. Among other benefits, this helps improve risk management by empowering you to create and deploy code faster and more securely.

For example, by employing technologies like ML, your cloud provider can enable you to discover, classify, and protect sensitive data—automatically and continuously.

If you work in a hybrid environment, you should prioritize the choice of information management and security tools built to integrate with the cloud. This allows the cloud to act as a seamless and secure extension of your on-premises environments.

OutSystems strengthens security posture using AWS Shield Advanced

As software vendor **OutSystems** grew its business, it needed a scalable security solution for its cloud service to further protect customers from cyber issues while reducing operational overhead. The company looked to AWS for centralized security management, so it could offer protection at scale while limiting manual interventions.

Using services like **AWS Shield Advanced**, a managed DDoS, OutSystems successfully scaled to manage the complexity of more than 4,000 web application firewalls (WAFs). It also reduced the response time after detecting a malicious event from approximately two hours to under five minutes. OutSystems paired AWS Shield Advanced with **AWS Firewall Manager**, a security management service for centrally configuring and managing firewall rules across accounts and applications. OutSystems used both services to manage the complexity of security solutions while improving response time.

OutSystems worked closely with AWS teams to address challenges and meet customer needs. Its team continues to implement additional capabilities of AWS Firewall Manager to fine-tune its security solution and better protect its customers.

Read the full success story ›

outsystems

> **"Using AWS services, we can manage the security posture of all customers from a central place by deploying rules that are specific to our technology and blocking malicious events. We also have the granularity to address very specific challenges."**
>
> Igor Antunes, Former Head of Security Architecture at OutSystems

5

Optimizing resources

By reducing costs for infrastructure and storage and allowing your teams to redirect technology resources previously dedicated to infrastructure management, you can make better use of those resources. With secure, cost-efficient access to powerful infrastructure and compute services at AWS, you can optimize your resources further through advanced analytics and AI-powered solutions.

Panasonic Avionics improves security and compliance with AWS

Driven by increased customer demand, **Panasonic Avionics**—a leading supplier of in-flight entertainment and communications solutions for airlines—needed to go beyond the limits of its existing on-premises infrastructure. Working with an AWS Partner, the company embarked on a phased digital transformation journey to the cloud.

Throughout the process, Panasonic Avionics pursued the principal objective of verifying that the transformed cloud data system was fully secure. The company used a broad palette of AWS security services to help it continuously monitor for threats, organize and prioritize response actions from a single hub, and much more.

With powerful, secure AWS architecture and AWS security services now supporting its every move, Panasonic Avionics can make much more efficient use of its resources. Its infrastructure costs are 86 percent lower, and it pays 78 percent less for data storage. The company can quickly analyze its data to derive insights, creating virtually endless business value. And tasks that once took weeks or months are now completed in hours or days, leading to increased innovation and productivity.

Read the full success story ›

Panasonic

> **"We've been able to churn out more software and features—built on and powered by AWS—faster than ever before. And our customers have noticed. They're excited about working with us."**

Anand Desikan, Former Head of Platform Services at Panasonic Avionics

How AWS helps organizations innovate securely

Secure cloud infrastructure is only part of the innovation equation. In this section, we will explore how AWS can help you design and implement a layered, proactive security strategy that inspires confidence and activates creativity.

Build, run, and scale on the most secure infrastructure

By choosing AWS, you inherit cloud and network architecture built to help satisfy the most security-sensitive organizations. From built-in capabilities, such as default encryption at the physical layer, to fully isolated regional infrastructure partitions, AWS is architected to be the most secure environment to build, run, and scale applications in the cloud.

Leading organizations trust AWS to help them secure their data, protect their reputations, and mitigate risk, because we're continuously innovating to develop powerful infrastructure that remains reliably secure—even as the threat landscape evolves.

AWS infrastructure features that strengthen your security include:

AWS Nitro System: Enjoy built-in security that continuously monitors, protects, and verifies hardware and firmware across the underlying foundation for the next generation of **Amazon Elastic Compute Cloud (Amazon EC2)** instances.

AWS Nitro Enclaves: Create additional isolation to protect and securely process highly sensitive data within Amazon EC2 instances—while significantly reducing the attack surface area.

AWS Graviton Processors: Run cloud-native applications with enhanced security, always-on memory encryption, dedicated caches for every vCPU, and support for pointer authentication—while enjoying the best price performance on Amazon EC2.

Protect your application data

AWS helps our customers meet Zero Trust requirements, implement data security policies, encrypt data, and monitor and audit data—while maintaining data ownership.

With AWS, you control your data by determining where it is stored, how it is secured, and who has access to it. We enable fine-grained security policies and layered encryption to isolate your data in transit, in use, and when stored. And AWS continuously raises the bar on privacy safeguards with services and features that allow you to implement your own privacy controls, including advanced access, encryption, and logging features. We prohibit—and our systems are designed to prevent—unrequested remote access by AWS personnel to your data for any purpose, including service maintenance. The only exceptions are when our access is required to prevent fraud and abuse or to comply with the law.

AWS infrastructure features that help protect your data include:

Amazon Simple Storage Service (Amazon S3) Storage Lens: Receive actionable recommendations to apply data protection best practices and optimize costs while gaining organization-wide visibility into object storage usage and activity trends.

Amazon CloudWatch: Observe and monitor resources and applications running on AWS, on premises, or in other clouds to detect anomalies, perform root cause analysis, set alarms, and take automated actions.

Improve security at every level

AWS enables you to further enhance security—and stay ahead of new and evolving threats—with the ability to add additional layers of protection quickly, efficiently, and at scale. Use a wide range of AWS services and features to filter unauthorized traffic, rapidly detect threats and misconfigurations, and remediate issues quickly or automatically.

AWS services that enhance your security include:

AWS Network and Application Protection: Enforce fine-grained security policies at every network control point with services that inspect and filter traffic to help prevent unauthorized resource access.

AWS Shield: Boost application availability and responsiveness with managed DDoS protection.

AWS WAF: Protect your web applications from common exploits and bots that can affect availability, compromise security, or consume excessive resources.

AWS Network Firewall: Deploy network firewall security for your virtual private clouds (VPCs) and define firewall rules that provide fine-grained control over network traffic.

Amazon GuardDuty: Protect your AWS environment with continuous monitoring of your AWS accounts and workloads for malicious activity.

Drive speed and agility with AI and automation

AWS provides organization-wide controls that automate infrastructure and application security checks to continually enforce security and compliance controls. Customers can then implement automated reasoning tools to mathematically prove the highest levels of security.

AWS services that can help drive agility include:

Amazon GuardDuty: More accurately isolate and alert suspicious user behavior with predictions powered by ML.

Amazon Inspector: Through deep semantic analysis of your application code, use this service—which features machine learning models and automated reasoning—to help identify code vulnerabilities and provide guidance you can use as part of remediation.

Amazon Detective: Automatically generate a narrative of an issue helping to bring a broader perspective and more security knowledge to the user.

NEXT STEPS

Start innovating securely with next-generation infrastructure

Throughout this eBook, we've highlighted the importance of tying meaningful innovation to reliable infrastructure security. Driven by proactive security strategies and building on secure, scalable infrastructure, organizations like Southwest Airlines, OutSystems, and Panasonic Avionics have enabled the innovation culture that helps them adapt and succeed in today's unpredictable, ever-changing economic climate.

Start innovating securely with AWS to unleash greater innovation across your business.

Learn more about AWS infrastructure security ›

Discover the ways AWS can help you focus on secure innovation with more than 200 fully featured services, including serverless and ML capabilities. **Take advantage of the AWS Free Tier** and get free, hands-on experience with AWS services.