

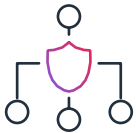


SECURITY: THE FOUNDATION OF AWS

# How AWS embeds a culture of security into every aspect of its business

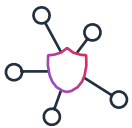
Security lives and breathes at the core of Amazon Web Services (AWS), filtering through to every aspect of our business. From weekly CEO and CISO security alignment meetings to empowering employees to escalate security issues, security is paramount to every decision, action, and outcome. In addition to inheriting our world-class security controls, our customers benefit from the proactive AWS security culture that supports continuous collaboration.

## 4 key principles to strengthen security culture



### Building security into organizational structure

Security permeates from the top of AWS, with senior-level executive leadership playing an active role in supporting security initiatives. Across the organization, business leaders own the security for their services and are in control of their functionality.



### Distributing security expertise across AWS

At AWS, our customers have come to expect and rely on the highest standard of security. Within the product teams, the **Security Guardians program** trains, develops, and empowers service team developers to ensure that new services, products, and features are built and shipped securely to customers.



### Putting the power of security in everyone's hands

At AWS, security is everyone's job, playing an important role in how every employee approaches work. Built into every product road map, engineering plan, and weekly stand-up meeting, product and service teams are accountable for their own service's security. Across AWS, employees are encouraged to identify security issues and escalate as needed.

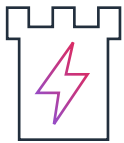


### Leveraging innovation to scale security

Our culture of innovation enables security to scale. Every scenario is tested to prove systems are secure. Automated reasoning tools ask critical questions about infrastructure to detect any misconfigurations, providing higher assurance in cloud security.

# 22.5%

fewer medium- and high-severity security findings were generated during the security review process with the Security Guardians program<sup>1</sup>



## AWS Nitro System—security by design

This pioneering platform is leveraged for all modern AWS compute instances. It is designed to protect customer code and data from unauthorized access during processing. This unique architecture means no one, not even the most privileged admins within AWS, can access a customer's workloads or data running on Amazon EC2 instances.

[Learn more](#)

**“At AWS, we made an intentional choice for the security team to report directly to the CEO. The goal was to build security into the structural fabric of how AWS makes decisions.”<sup>1</sup>**

Stephen Schmidt, Chief Security Officer, Amazon

**“Cloud computing is some of the most critical infrastructure we have, as it hosts sensitive data and powers business operations across our economy. It is imperative that cloud service providers prioritize security and build it in by design.”<sup>2</sup>**

Robert Silvers, DHS Under Secretary of Policy, CSRB Chair

## Optimize security to drive business success

As the technological landscape continually evolves with new solutions, such as generative artificial intelligence (AI), we continue to innovate our security services to help ensure our customers are always secure. Discover how your organization can benefit from optimizing security to move fast, stay secure, and enable digital transformation.

[Learn more about AWS Security >](#)

<sup>1</sup> “How AWS built the Security Guardians program, a mechanism to distribute security ownership,” AWS Security Blog, August 2023

<sup>2</sup> “Cyber Safety Review Board Releases Report on Microsoft Online Exchange Incident from Summer 2023,” Homeland Security Press Release, April 2024