snyk | aws

CHEATSHEET

DevSecOps requires AppSec and CloudSec to work together to understand the full context of application and cloud risk, from code to cloud, and back. Snyk's integration with AWS Security Hub allows security practitioners to manage security events from various sources in a more streamlined way, feeding alerts into a central location for security teams to analyze and prioritize security findings based on vulnerability severity, breaking down silos of responsibility between application and cloud security to create a true DevSecOps program.

	Application Security Posture Management (ASPM)	Cloud Security Posture Management (CSPM)
Description	ASPM is the process of continuously managing the security posture of your applications by identifying, prioritizing, and mitigating potential risk within your application fleet. Incorporating security tooling like Snyk throughout the SDLC ensures that security is considered from design to development to deployment of production workloads.	CSPM is the process of adhering to cloud security best practices and compliance standards. As organizations migrate more resources and data to the cloud, ensuring that those environments are configured securely becomes paramount. CSPM tools like AWS Security Hub fill this need by providing continuous oversight and automated checks against best practices and compliance standards.
Visibility	Identify all the applications and software assets in your AWS environment to ensure you don't miss any security risks.	Develop a comprehensive view of your AWS resources and their relationships, as well as potential security issues.
Find, Prioritize, and Fix	Implement automated security controls to continuously scan all the components of your applications for vulnerabilities, including source code, open source packages, containers images, and IaC configs. Combine application and business context to prioritize fixes.	Implement automated security controls to continuously find and fix misconfigurations in cloud services that can leave your AWS environment open to malicious actors.
Continuous Monitoring	Continuously monitor your running applications and provide engineering and security stakeholders with reports on coverage gaps and potential risk. Comprehensive reporting capabilities in ASPM tooling will also help technical teams provide the visibility executive stakeholders need to ensure applications are always secure.	Send real-time alerts to the right teams whenever critical misconfigurations are identified and create notification and response workflows to manage those security risks. Comprehensive reporting capabilities in CSPM tooling will also help technical teams provide the visibility executive stakeholders need to ensure customer data is always secure.
Compliance	Check that your AppSec program ensures that security controls are adequate and covers the right assets against popular regulatory standards such as GDPR, HIPAA, and PCI DSS. Continuously enable these risks to be automatically identified and addressed.	Check your cloud environment against popular regulatory standards such as AWS Well-Architected, GDPR, HIPAA, PCI-DSS, and more, ensuring that cloud configurations are in line with both internal and industry regulations.
Continuous Security	Incorporate continuous security checks throughout the SDLC to ensure that security is considered from the very first line of code.	Leverage AWS services and API functionalities to integrate findings and recommendations from tools like AWS Security Hub into your CI/CD pipeline, ensuring that security checks are part of your development and deployment processes.

Learn more about how Snyk and AWS power modern DevSecOps practices by booking a demo, or signing up for a free Snyk account directly from the AWS Marketplace.

aws Available in AWS Marketplace