PRISMA CLOUD | paloalto NETWORKS

Shift Left and Enable DevSecOps

Integrate security across the entire development lifecycle

Most modern organizations realize the value of shifting security left in the development lifecycle—especially as applications are becoming collections of microservices and functions, and everything is getting defined as code. Developers use a vast array of tools to build and deploy cloud native applications, and operationalizing security controls that work seamlessly across these tools remains a challenge.

Meanwhile, although static code analysis tools have existed for many years, they have a reputation for being difficult to use. To enable a culture of DevSecOps, a practical way to shift security left across the entire development lifecycle is essential.

Start with Shifting Left

During the build phase, Prisma® Cloud enables developers to scan virtual machine images, container images, Pivotal Application Service (PAS) droplets, and serverless functions for vulnerabilities and unsecure configurations using native security plugins for integrated development environments (IDEs), source code management (SCM), and continuous integration/continuous development (CI/CD) that seamlessly integrate into existing tools.

Prisma Cloud also enables you to scan your infrastructure-as-code (IaC) templates to find unsecure configurations used with Terraform®, CloudFormation, Kubernetes manifests, and similar technologies. Additionally, Prisma Cloud gives security teams the control to fail a build based on vulnerability or compliance issues, preventing unsecure software from progressing farther in the pipeline and instead forcing the developer to resolve the issues. **As cloud native environments become more automated, it's critical to ensure security teams can set and enforce quality gates in the pipeline**.

Secure the Deployment

While shifting left and enforcing security at the build phase is crucial, it's equally important to ensure any host operating systems, container images, PAS droplets, and serverless functions are free of new vulnerabilities that may have been discovered after the build. By scanning any container registry or serverless repository and enforcing trusted code sources, Prisma Cloud ensures that even code that has passed the build quality gate is free of security issues when it's time to deploy. If your defined security requirements are not met, Prisma Cloud can again stop the deployment. This way, **no matter when or where a build was done, you can feel confident you're only deploying secure code**.

Use Comprehensive Risk Prioritization and Runtime Protection

With vulnerable code unable to reach production, your overall attack surface is greatly reduced. To complement this, Prisma Cloud provides comprehensive runtime security, automatically ranking every issue by risk severity as well as how it impacts your unique usage and environment. Furthermore, Prisma Cloud uses metadata from an application (during the CI stage) along with tags to automatically notify the specific developer who created the application, directly within whichever development tooling they're already using.

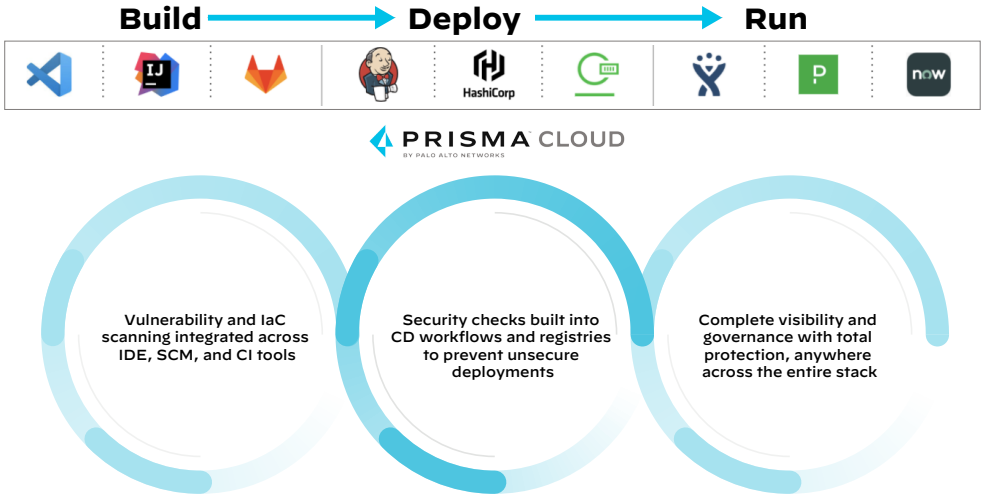

Figure 1: Examples of common Prisma Cloud integrations[1]

Prisma Cloud provides risk prioritization for any running environment so security teams can continuously monitor all their cloud native infrastructure and apps and quickly prioritize remediation efforts. By automatically informing developers when they must fix and redeploy their code, only Prisma Cloud makes DevSecOps a reality.

1. The current list of DevOps integrations can be found in the Prisma Cloud documentation.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com