Prisma Cloud
At a Glance

Protect Applications from Code to Cloud

Prisma® Cloud is a cloud-native application protection platform (CNAPP) designed to protect applications across any public, private, hybrid, or multicloud environment. Unlike a collection of point products, Prisma Cloud integrates a broad set of security capabilities into a single platform to deliver unified, best-in-class security. The benefits of our approach include reduced risk, fewer breaches, better Dev-Sec collaboration, increased efficiency, and improved compliance and security posture.

Risk Prevention

Prevent risks and misconfigurations from entering production.

Visibility and Control

Establish continuous visibility and control across your cloud environment.

Runtime Protection

Enable real-time protection for cloud workloads, web applications, and APIs.

Figure 1: Prisma Cloud's unified Code to Cloud™ approach

Prisma Cloud Use Cases

Risk Prevention

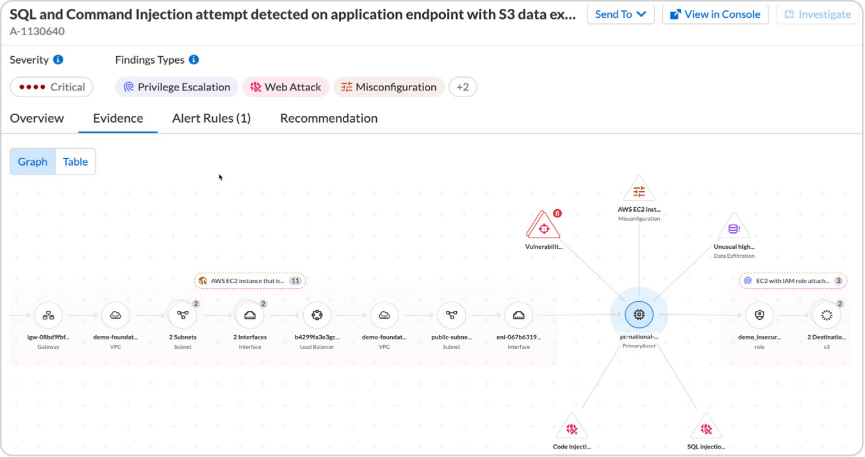
Shift left and secure applications by design. Prisma Cloud integrates with engineering ecosystems to prevent risks and misconfigurations from entering production, offering:

- **Infrastructure-as-Code (IaC) security:** Identify and fix misconfigurations in Terraform, CloudFormation, ARM, Kubernetes, and other IaC templates.
- **Secrets security:** Find and secure exposed and vulnerable secrets across all files in repositories and CI/CD pipelines.
- **CI/CD security:** Harden CI/CD pipelines, reduce the attack surface, and protect your application development environment.
- **Software composition analysis:** Address open source vulnerabilities and license compliance issues with context-aware prioritization.

Visibility and Control

Gain continuous visibility and control over cloud misconfigurations, identity and access, data, vulnerabilities, and API endpoints across your cloud environment. Prisma Cloud secures cloud infrastructure, delivering:

- **Cloud security posture management (CSPM):** Monitor posture, detect and remediate risks, and maintain compliance.
- **Cloud infrastructure entitlement (CIEM):** Gain control over permissions across multicloud environments.
- **Agentless workload scanning:** Scan hosts, containers, Kubernetes, and serverless for vulnerabilities and threats.
- **Cloud data security:** Identify sensitive data and scan for malware across public cloud storage.
- **API visibility:** Discover, profile, and protect APIs across cloud-native applications.
- **Cloud discovery and exposure management:** Increase visibility and control over unknown, unmanaged cloud assets exposed to the internet.



SQL and Command Injection attempt detected on application endpoint with S3 data ex...
A-1130640

Severity: ●●●● Critical

Findings Types: Privilege Escalation, Web Attack, Misconfiguration, +2

Figure 2: Attack Path Analysis

Prisma Cloud
At a Glance

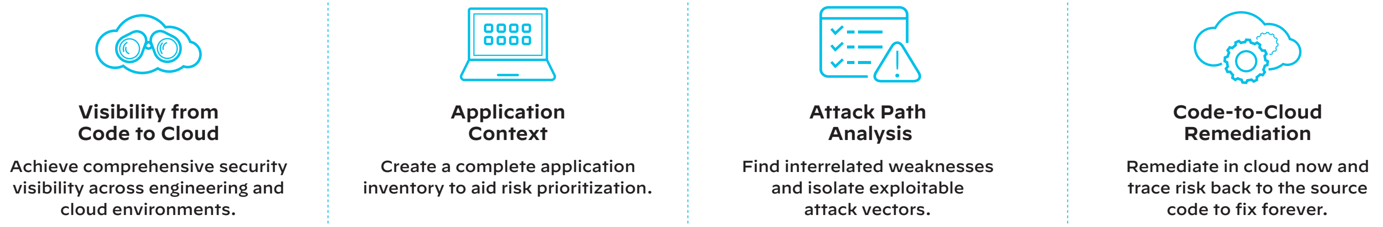
Runtime Protection

Block breaches in runtime and protect applications against attacks. Prisma Cloud delivers threat protection across public and private clouds, including:

- **Cloud threat detection:** Detect advanced threats, zero-day attacks, and anomalies across multicloud environments.
- **Host security:** Secure cloud VMs for any public or private cloud.
- **Container security:** Secure containers and Kubernetes platforms on any public or private cloud.
- **Serverless security:** Secure serverless functions across the full application lifecycle.
- **Web application and API security:** Protect web applications and APIs across any public or private cloud.

Code to Cloud Intelligence

Our unique approach is powered by Code to Cloud intelligence, connecting insights from the developer environment through application runtime to reduce risk and prevent breaches. Prisma Cloud contextualizes alerts, prioritizes critical risks, and offers remediation guidance.



Visibility from Code to Cloud

Achieve comprehensive security visibility across engineering and cloud environments.

Application Context

Create a complete application inventory to aid risk prioritization.

Attack Path Analysis

Find interrelated weaknesses and isolate exploitable attack vectors.

Code-to-Cloud Remediation

Remediate in cloud now and trace risk back to the source code to fix forever.

Figure 3: Code to Cloud intelligence

> "Everything is so easy with Palo Alto Networks. The native integration is seamless, the visibility is complete, and the automation takes care of the vast majority of monitoring. There's no impact on our resources either."

– Oussama Benzaouia, CISO, Teads

Read the full case study.

> "The Palo Alto Networks portfolio makes sense on every level. Instead of relying on point security solutions, we have a suite of best-practice, interconnected security technologies that are proven to deliver. Our team can focus on value-add tasks, confident that critical security processes are running in the background, protecting our new digital infrastructure."

– Bob Bowden, Security Architect, Registers of Scotland

Read the full case study.