Prisma Cloud and AWS

Prisma Cloud by Palo Alto Networks Is the Most Comprehensive Cloud Security Platform on the Market and Purpose Built for Amazon Web Services

The Code to Cloud Security Platform for AWS

Prisma® Cloud is a Code to Cloud™ security platform that secures every stage of the application lifecycle on AWS. Our comprehensive cloud-native platform makes it easy to prioritize and eliminate risk across the code, build, infrastructure, and runtime phases of development.

The move to the cloud has changed all aspects of the application development lifecycle—security being foremost among them. Ever-changing environments challenge developers to build and deploy at a frantic pace while security teams remain responsible for the protection and compliance of the entire lifecycle. This is why Palo Alto Networks built Prisma Cloud as one of the broadest cloud security platforms available in the market that scales with your growing business requirements on AWS.

Enforce Policy, Configuration, and Compliance Everywhere on AWS

Prisma Cloud is a full-lifecycle platform that can ensure your code is secure by design on AWS by preventing IaC misconfigurations, preventing exposed secrets, fixing open-source vulnerabilities, and securing continuous delivery pipelines. The Prisma Cloud platform reduces remediation times on AWS with cloud-native workflows that accelerate the time to fix and redeploy AWS resources. Additionally, Prisma Cloud blocks active attacks in the AWS runtime, protecting against web-based attacks and API abuse, exploitation of vulnerabilities, and defending against all types of malware, including zero-day threats.

With Prisma Cloud, you gain **1,800+** AWS configuration checks and **60+** compliance standards ready to use on AWS. Our security platform supports **30+** AWS global regions, including AWS GovCloud and AWS China so you can stay secure globally while meeting local data residency requirements.

Prisma Cloud Benefits

- **Get deep visibility and control** for your entire AWS stack across code, build, deploy, and run stages—secure everything in AWS from code to cloud.
- **Gain smarter security with Code to Cloud Intelligence and Precision AI™** by Palo Alto Networks to help discover dangerous attack paths and rapidly remediate threats and AWS misconfigurations across the lifecycle.
- **Consolidate many point tools** into Prisma Cloud to stop tool sprawl, improve operational efficiencies on AWS, and reduce security costs.
- **Prevent risks and stop breaches** in real time on AWS with a unified platform and single security framework that is prebuilt for AWS.
- **Secure your AWS estate everywhere in the world**, including AWS China and AWS GovCloud, all from a single pane of glass.

FROST & SULLIVAN

Prisma Cloud named a Leader in the Frost Radar: Cloud-Native Application Protection Platforms (CNAPP), 2023.

The Prisma Cloud Advantage on AWS in Five Steps

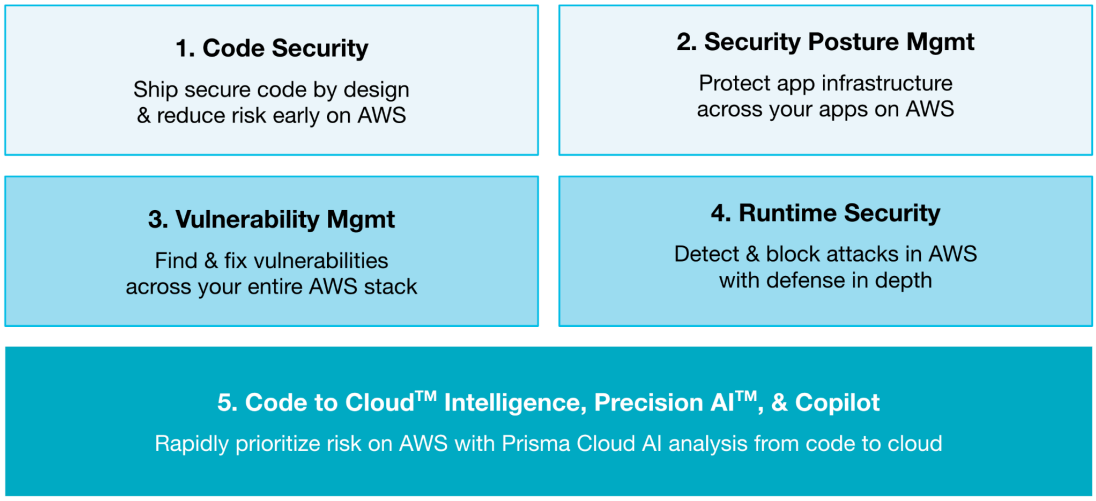


Figure 1: *Shift security left, gain posture management, and protect the runtime on AWS—all supported by intelligence and AI*

1. Ship secure code by design and eliminate alert noise with Code Security.

Prisma Cloud is your single tool for securing code across architectures and software supply chains in AWS with consistent embedded controls from build time to runtime. Shift security left and reduce time needed to address vulnerabilities by **60%**[1] with actionable feedback and guardrails to ensure only secure code goes to production. See our Code Security datasheet.

2. Find and fix misconfigurations to reduce risk across AWS with Security Posture Management for cloud, data, and AI.

Prisma Cloud delivers Visibility, Compliance and Governance for AWS configuration sensitive data, AI models, generative AI, and AWS entitlements, offering prebuilt AWS policies and **90%**[2] reduction in compliance reporting effort. See our CSPM datasheet, DSPM datasheet for AWS, and AI-SPM datasheet.

3. Find and fix flaws across AWS with vulnerability management.

Prisma Cloud helps prioritize the most impactful threats and improves remediation times by **60%**[3] by removing blind spots, prioritizing vulnerabilities with context, and managing remediation for the full AWS stack (virtual machines, containers, Kubernetes, serverless, and open-source software). See our Cloud Vulnerability Management Tipsheet.

4. Secure the AWS runtime and block attacks with defense in depth.

Prisma Cloud reduces cloud security investigation times by **48%**[4] by providing real-time advanced runtime threat detection and response with defense in depth across the full stack of AWS cloud workload types (e.g., Amazon EC2 and hosts; EKS, ECS, OpenShift containers; Fargate and Lambda functions). See our Cloud Workload Protection datasheet.

5. Modernize security with Code to Cloud Intelligence, Precision AI, and the Prisma Cloud Copilot.

Prisma Cloud with Code to Cloud Intelligence helps teams quickly prioritize risk on AWS with context, risk classification, root cause analysis, and actionable remediation steps. Powered by Precision AI from Palo Alto Networks, Prisma Cloud acts as your foundational defense for AI-first world. Eliminate expertise with a simple conversation in our Prisma Cloud Copilot. See our Code to Cloud Intelligence, Precision AI, and Copilot videos.

Prisma Cloud by Palo Alto Networks has deep AWS technical expertise, and proven customer success across multiple AWS competencies.

- ✓ **Security**
- ✓ **DevOps**
- ✓ **Containers**
- ✓ **Migration/Modernization**

We are also AWS-validated for services and programs, and a featured vendor for guidance and purpose-built use cases:

- ✓ **Amazon RDS Ready**
- ✓ **AWS Public Sector**
- ✓ **AWS Well-Architected**
- ✓ **AWS Marketplace**
- ✓ **Financial Services Security**
- ✓ **Cloud Infrastructure Security**

[1] *The Total Economic Impact Of Palo Alto Networks Prisma Cloud*, Forrester Consulting commissioned study by Palo Alto Networks, November 2023.
[2,3,4] Ibid.

Prisma Cloud Is Your Code to Cloud Security Platform Built for AWS

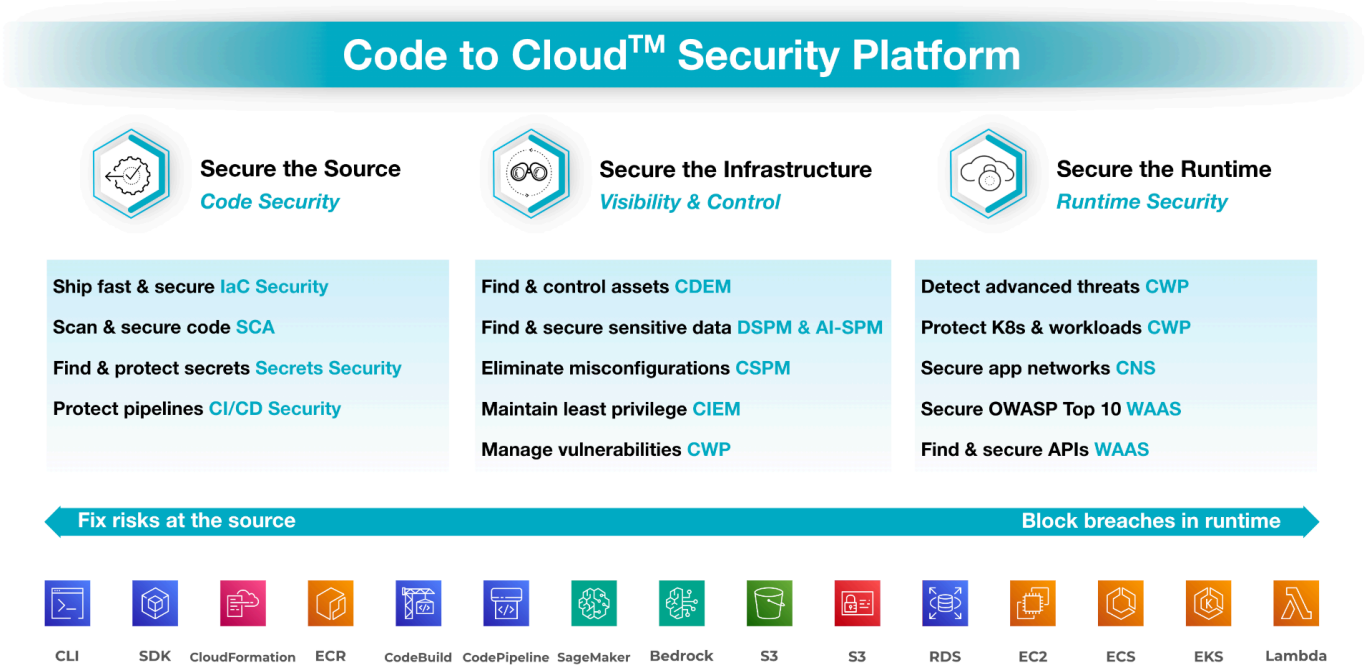


Figure 2: *The Prisma Cloud full-stack architecture protects your AWS environment from code to cloud*

Eliminate risk across the application lifecycle on AWS with full-lifecycle Prisma Cloud security that prioritizes and fixes security flaws in code, detects and blocks untrusted images before deployment, and protects applications from zero-days at runtime.

Prisma Cloud – Secure Source on AWS

Identify and fix misconfigurations on AWS with Infrastructure as Code (IaC) Security.

Detect and correct misconfigurations in **Terraform**, **AWS CloudFormation**, **Helm**, **ARM**, **Kubernetes**, and other IaC templates before deploying on AWS. Our policy as code programmatically ensures consistent security governance and remediation across your AWS environment, preventing policy drift. AppSec teams can utilize **1,600+** prebuilt policies with autofixes and smart fixes, or add custom rules. Integrate Prisma Cloud with IDEs, CI tools, and version control systems to provide feedback directly into developer tools. AWS resources are also traceable back to IaC templates and the original code modifier, allowing you to identify the correct resource and team for remediation on AWS.

Manage open-source vulnerabilities and license compliance on AWS with Software Composition Analysis.

Scan your open-source packages for vulnerabilities and help ensure license compliance to eliminate application dependency risk early in the development process. Prisma Cloud delivers the context developers need to prioritize dependency risk to the leaf node and implement fast fixes. Use our supply chain graph visualization to view a consolidated inventory of your AWS pipelines and generate a software bill of materials to reduce risk.

Find and secure exposed and vulnerable secrets across all repositories and AWS pipelines with Secrets Security.

Natively integrated into DevOps tools and workflows, Prisma Cloud makes it seamless for AWS developers to prevent secret exposure across the development lifecycle. Combining a **100+** signature-based policy library and a fine-tuned entropy model, Prisma Cloud identifies secrets in nearly any file type on AWS, including IaC templates, golden images, and Git repositories.

Harden your AWS pipelines, reduce attack surface, and protect your development environment with CI/CD Security.

Help your AppSec team protect your AWS pipelines by identifying and fixing OWASP Top 10 CI/CD Security Risks early in development. Scan code, identify vulnerabilities and secrets, and reduce infrastructure and application risk before deployment.

Prisma Cloud – Secure Infrastructure on AWS

Combat rogue AWS deployments with Cloud Discovery and Exposure Management.

Discover internet-exposed and unmanaged assets deployed across your AWS environment and convert them to managed assets protected by our CSPM capabilities. Understand what your AWS environment looks like from an attacker's point of view.

Classify and secure sensitive data and AI-powered applications with Data and AI Security Posture Management.

Gain contextual visibility into sensitive data and data flows in storage assets such as **Amazon Redshift**, **Amazon S3**, and **PostgreSQL on Amazon EC2** to detect and prevent data exfiltration, malware, and ransomware attacks across AWS regions while ensuring compliance. Further, secure your AI models and data pipelines in **Amazon SageMaker** and **Amazon Bedrock** deployments and ensure governance over models, generative AI, and AI supply chains.

Monitor, remediate, and maintain compliance for all your AWS resources with Cloud Security Posture Management.

Identify and address AWS misconfigurations promptly to reduce the risk of security breaches due to human error or misconfigured AWS resources. Prisma Cloud has an extensive library of **1,800+** built-in AWS misconfiguration checks and support for **60+** compliance frameworks and customized policies. Save time on regulatory compliance with rapid one-click reporting, monitor AWS resource changes in real time, and aid remediation teams with detailed forensic analysis.

Enforce least-privileged access to AWS infrastructure with Cloud Infrastructure Entitlement Management.

Prisma Cloud integrates with **AWS IAM Identity Center** to surface detailed information on IAM access in your AWS environment and give teams visibility into overprivileged **AWS Groups and Roles**. Continuously monitor and enforce least-privileged access for AWS resources with our role-based access control (RBAC). Remove unused privileges, restrict permissions, and even automate right-sizing of permissions with our easy-to-use “Suggest Least Privilege Access” wizard.

Manage and prioritize remediation of vulnerabilities from code to cloud on AWS with vulnerability management.

Continuously scan AWS cloud resources for vulnerabilities and prioritize them for remediation. Our Code to Cloud Traceability empowers teams to discover risks in their AWS environment with the highest potential of attack. Rapidly fix the most impactful vulnerabilities in your CI/CD pipelines before deployment to minimize your attack surface on AWS and reduce alert noise.

Prisma Cloud – Secure Runtime on AWS

Detect advanced threats, zero-day attacks, and anomalies on AWS with Cloud Threat Detection.

Gain visibility into all areas of the AWS runtime environment and identify active attacks and suspicious behavior in real time with Prisma Cloud. Our Cloud Threat Detection automates ingestion of AWS audit logs, such as **AWS CloudTrail**, and uses advanced machine learning and threat intelligence to focus investigation and remediation efforts on the most critical incidents.

Protect hosts, VMs, containers, Kubernetes, and serverless functions on AWS with Cloud Workload Protection.

Secure Linux and Windows hosts, virtual machines (**Amazon EC2**), containerized applications (**Amazon ECS**, **Amazon EKS**) with both agentless and agent-based security, and serverless (**AWS Lambda**, **AWS Fargate**). Prisma Cloud prevents configuration issues, rogue deployments, unpatched vulnerabilities, and ensures full compliance on AWS.

Secure the network on AWS that connects to your applications with Cloud Network Security.

Get end-to-end network visibility and control across your AWS application environment, understand cloud network threats, and remediate cloud network exposure with flow mapping and detailed guidance that reduces risk on AWS and simplifies security.

Defend your applications on AWS from OWASP Top 10 attacks with web application security.

Reduce the risk of web application breaches on AWS by detecting and protecting against OWASP Top 10 threats. Simplify with agent-based and agentless deployment options that locally enforces application security on AWS microservices to support scale. And, protect your applications on AWS against malicious bots, denial-of-service attacks, and unwanted access.

Discover, profile, and protect APIs from API OWASP Top 10 attacks on AWS with real-time API security.

Automatically discover APIs and API abuse on AWS in real time and secure for the API OWASP Top 10. Our risk profiling and behavioral analysis of API calls reduces breach risk, and we support virtual patching against vulnerabilities and zero days.

Code to Cloud Intelligence to Seamlessly Secure Your AWS Environment

Spend less time chasing noise in the cloud and more time fixing critical issues. Prisma Cloud with Code to Cloud intelligence automatically correlates risks that form attack paths and prioritizes issues based on impact to your specific AWS environment.

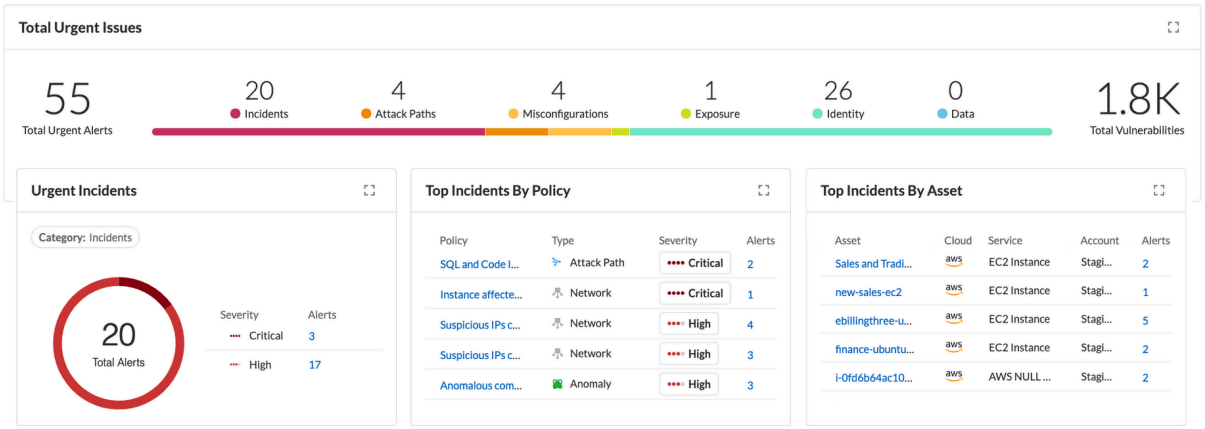


Figure 3: *The Prisma Cloud dashboard shows impactful security alerts affecting your AWS environment*

Trace attack paths with graph visualizations to uncover interconnected cloud risks in AWS.

Prisma Cloud offers visualizations of potential attack paths that automatically trace and correlate security findings across various domains—such as AWS configurations, IAM identities, sensitive data, vulnerabilities, and network flows. This deep context tracing enables teams to quickly identify and remediate attack paths without special expertise, enabling fast and advanced risk mitigation on AWS.

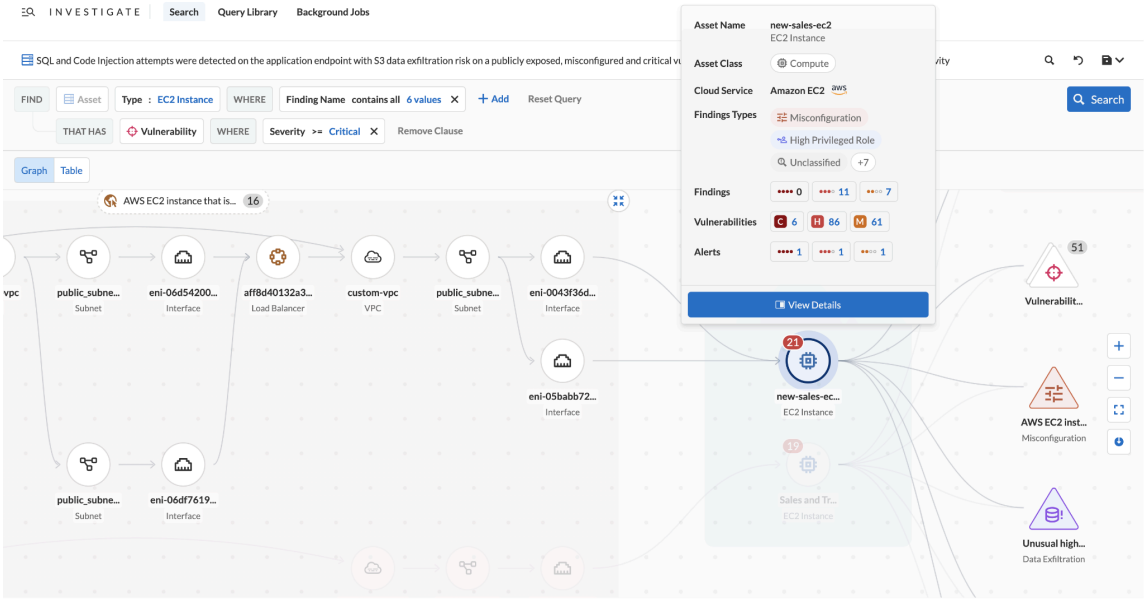


Figure 4: *Attack path in AWS traced and visualized by Prisma Cloud for investigative analysis and rapid remediation*

FROST & SULLIVAN

Prisma Cloud named a Leader in the Frost Radar: Cloud Security Posture Management (CSPM), 2024.

Continuous Monitoring Across AWS Environments

Prisma Cloud protects your AWS environment with extensive service coverage, including ingestion of over **350** AWS APIs.

Find vulnerabilities and best practice deviations with Amazon Inspector.

Ingest AWS vulnerability data and AWS security best practice deviations from **Amazon Inspector** to gain a more contextual view of risk in your AWS environment and help perform deep investigations using RQL queries.

View all your Prisma Cloud alerts in AWS Security Hub.

Integrate with **AWS Security Hub** and use it as your central console. Prisma Cloud monitors your AWS assets and sends alerts about resource misconfigurations, compliance violations, network security risks, and anomalous activities directly to your AWS Security Hub console.

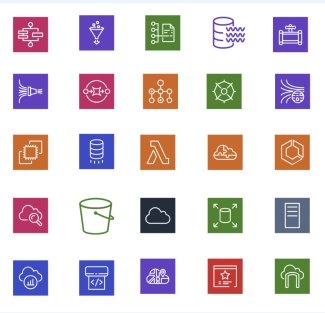
Integrate alerting with Amazon S3.

Connect with **Amazon S3** to get notifications for configuration, audit, and anomaly policy violations. You can also stream the Prisma Cloud alerts to an Amazon S3 bucket or folder.

Enhance cloud visibility with Amazon Security Lake.

Get a comprehensive view of security data with greater context using your choice of sources from cloud and on-premises environments with **Amazon Security Lake** and Prisma Cloud.

Extensive service coverage



Over 350 AWS APIs ingested

Shift security left into AWS CodeBuild and AWS CodePipeline.

Identify misconfigurations in infrastructure as code (IaC), vulnerabilities with Software Composition Analysis (SCA), license noncompliance, exposed secrets, and CI/CD pipeline risks in your AWS development platform. Integrate with **AWS CodeBuild**, Git repositories, and **AWS CodePipeline** to scan, alert, and create tickets whenever changes are pushed or triggered.

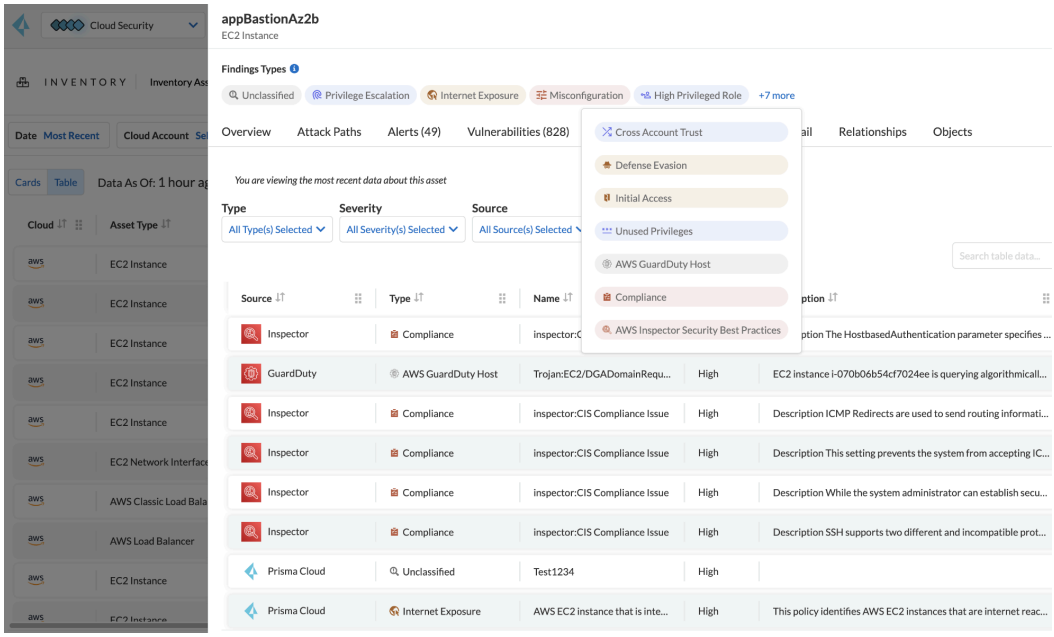


Figure 5: AWS Cloud findings are ingested into the Prisma Cloud platform for visibility and rapid remediation

FORRESTER WAVE LEADER 2024 Cloud Workload Security

Prisma Cloud named a Leader in the Forrester Wave: Cloud Workload Security, 2024.

Cloud-Native Security That Covers Your Entire Application Lifecycle on AWS

With a growing number of entities to secure and environments that constantly change, Prisma Cloud by Palo Alto Networks stands out as one of the most complete cloud security platforms to help you grow your business with AWS. No matter your industry or what your security use case is, Prisma Cloud is ready to secure it with cloud-native protections covering the full AWS stack from code to cloud.

Secure Every Stage of the Application Lifecycle

The Prisma Cloud security platform offers streamlined deployment, available for SaaS and self-hosted, with Prisma Cloud Credits that allow you to use different Prisma Cloud security modules depending on your specific need and maturity in the cloud. Using Prisma Cloud, both security and DevOps teams are able to effectively collaborate and accelerate secure cloud-native application delivery on AWS.

With code-to-cloud coverage that is prebuilt for AWS and unifying security across code, CI/CD pipeline, infrastructure, workloads, data, networks, web applications, identity, and APIs, Prisma Cloud addresses your security needs at every step of your cloud journey with AWS. Talk to your AWS representative or reach out to Palo Alto Networks for a free Prisma Cloud trial.

Prisma Cloud Security Modules	Secure Source	Secure Infrastructure	Secure Runtime
Code Security (CS) *Shift-left and secure apps by design*	✓		
Cloud Discovery and Exposure Management (CDEM) *Detect and manage rogue cloud deployments*		✓	
Data Security Posture Management (DSPM) *Classify and secure every piece of sensitive data*		✓	
AI Security Posture Management (AI-SPM) *Secure AI-powered apps through data pipelines*		✓	
Cloud Security Posture Management (CSPM) *Gain Visibility, Compliance and Governance*		✓	
Cloud Infrastructure Entitlement Management (CIEM) *Enforce least-privileged access to infrastructure*		✓	
Cloud Workload Protection (CWP) *Secure host, containers, K8s, and serverless*			✓
Web Application & API Security (WAAS) *Protect apps and APIs against web-based attacks*			✓
Cloud Network Security (CNS) *Secure the network that connects to apps*			✓

Prisma Cloud and AWS Resources

- Prisma Cloud and AWS (Environment Overview)
- Data Security Posture Management: Elevate Your Cloud Data Protection on AWS
- Executive's E-Guide to Protecting Workloads and Data on AWS
- Webinar: Elevate Your AWS Threat Intelligence with Prisma Cloud and Amazon GuardDuty
- Hands-On Lab: Palo Alto Networks – AWS Immersion Days
- Case Study (Healthcare): A Healthcare Organization's Journey to Securing Complex Clouds with Prisma Cloud
- Case Study (Financial): Modernizing Over 400 Years of Registry History with Cloud Security
- AWS Marketplace (Prisma Cloud – Annual Contract, StateRAMP Authorized)

aws **Available in AWS Marketplace**

Prisma Cloud by Palo Alto Networks offers pay-as-you-go (PAYG) and consulting partner private offers (CPPO) in **AWS Marketplace**.

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

prisma_sb_prisma-cloud-and-aws_090424