



# Prisma Cloud

Monitor posture, detect and respond to threats, and maintain compliance in US government multi-cloud environments

US federal government agencies are embracing [Cloud Smart](#) to reduce the cost of shared service delivery, deliver services more quickly, and engage citizens in the digital age. Prisma® Cloud enables agencies to gain visibility, ensure compliance, detect and respond to threats, and automate remediation across multi-cloud environments. From a single console, agencies can monitor security posture, prevent misconfigurations, and detect vulnerabilities and other threats that might lead to data leaks. They can maintain consistent security across cloud service providers while dramatically reducing alert volume, configuration errors, and the need for multiple security tools.

The cloud security posture management (CSPM) capabilities of Prisma Cloud are part of a FedRAMP Moderate Authorized environment.



## Comprehensive CSPM for a Multi-Cloud Reality

Effective cloud security requires complete visibility into every deployed resource as well as absolute confidence in their configuration and compliance status. As agencies adopt cloud native methodologies and gain the flexibility of multi-cloud architectures, stitching together security data from disparate, siloed tools becomes a considerable obstacle. DevOps and cyber teams need a simpler way to monitor and enforce consistent, compliant security across clouds.

Prisma Cloud takes a unique approach to CSPM, going beyond mere compliance or configuration management. Vulnerability intelligence from cloud service providers and third-party sources, such as Qualys and Tenable, provides deep, granular context with every alert. Integrated Infrastructure-as-Code (IaC) scanning prevents insecure IaC configurations.

The following CSPM capabilities of Prisma Cloud are part of a FedRAMP Moderate Authorized environment that runs on AWS® GovCloud (US). These capabilities are part of a comprehensive cloud security platform that enables integrators and agencies to meet the US Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) program. For more information on how Palo Alto Networks meets CDM capabilities, please read [this datasheet](#).

### Visibility, Compliance, and Governance

#### Cloud Asset Inventory

Prisma Cloud delivers comprehensive visibility and control over the security posture of every deployed resource across AWS, Microsoft Azure®, and Google Cloud environments. While some solutions simply aggregate asset data, Prisma Cloud analyzes and normalizes disparate data sources to provide unmatched risk clarity.











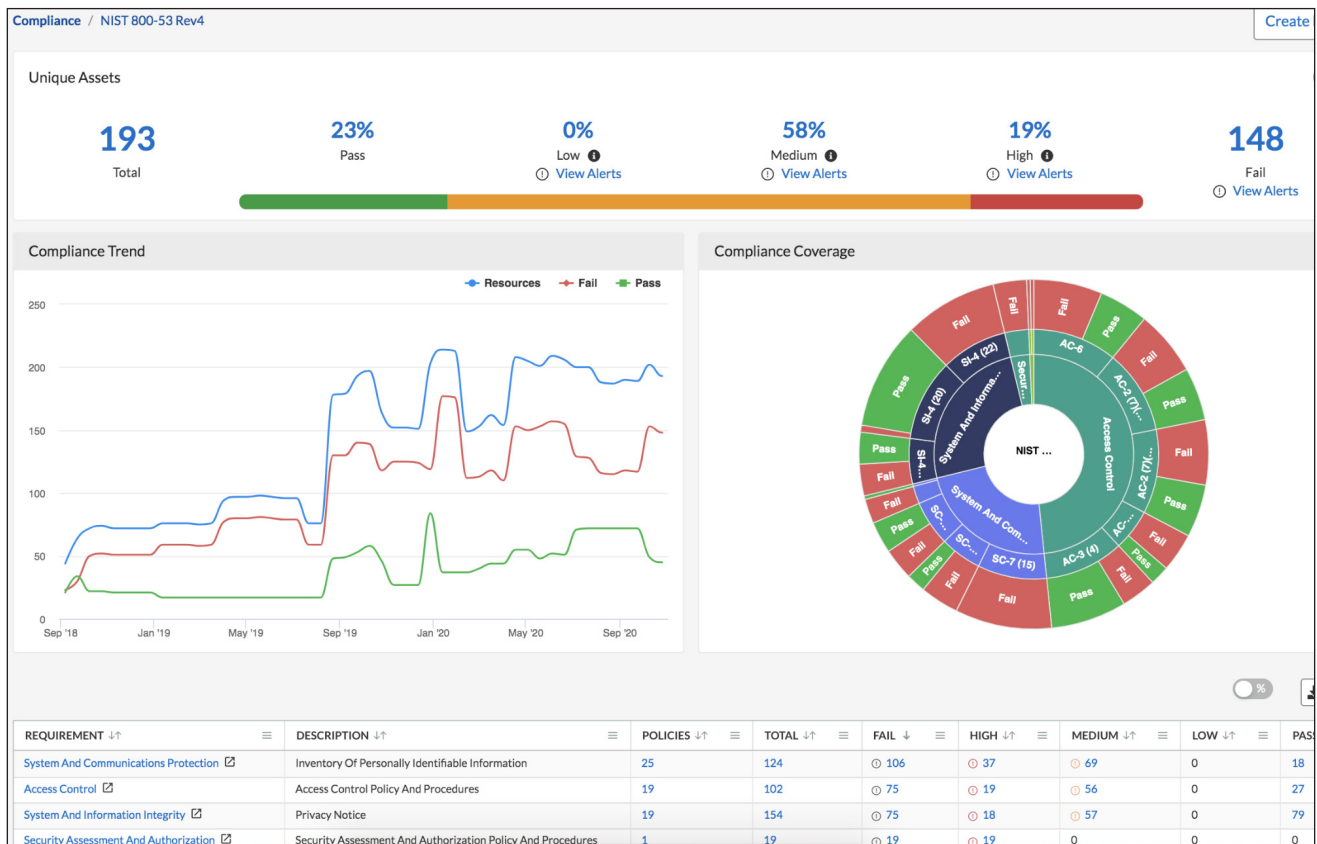
	Amazon EFS	aws	24	0	24	0	24	0	0%
	AWS Secrets Manager	aws	7	7	0	0	0	0	100%
	Amazon EKS	aws	1	0	1	0	1	0	0%
	Amazon SQS	aws	5	0	5	0	5	0	0%
	Amazon S3	aws	66	0	66	66	0	0	0%
	Azure Virtual Network	azure	120	87	33	18	15	0	73%
	Azure Network Watcher	azure	31	31	0	0	0	0	100%
	Azure Resource Manager	azure	9	7	2	0	0	2	78%
	Azure Policy	azure	3	3	0	0	0	0	100%
	Azure SQL Database	azure	2	0	2	2	0	0	0%
	Azure Compute	azure	31	17	14	5	9	0	55%
	Azure Storage	azure	13	0	13	1	12	0	0%
	Azure App Service	azure	1	1	0	0	0	0	100%
	Azure Security Center	azure	2	0	2	0	2	0	0%
	Google Resource Manager	gcp	114	91	23	12	11	0	80%

Figure 1: Asset inventory

## Compliance Monitoring and Reporting

Prisma Cloud continuously monitors compliance posture across all your cloud environments and supports one-click reporting from a single console. More than 15 compliance frameworks are included out of the box, and you can build additional custom frameworks.



**Figure 2: Compliance dashboard**

## Infrastructure-as-Code (IaC) Scanning

Prisma Cloud enables users to scan IaC templates for vulnerabilities and build cloud-agnostic policies for the build and runtime development phases.

**Add Config Policy**

1 Details — 2 Build Your Rule — 3 Compliance Standards — 4 Remediation

Policy Name \*

IaC Vulnerability Scan

Policy Subtype \*

☐ Run ☒ Build

Description

Scan IaC templates for vulnerabilities

Severity \*

High

Labels

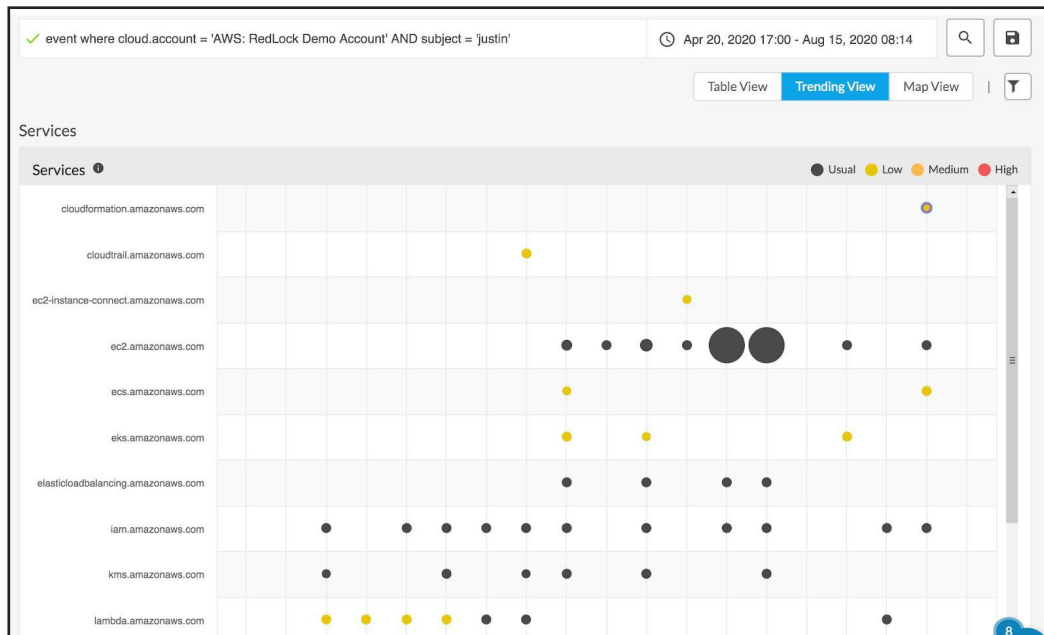
CloudFormation

**Figure 3: Custom IaC policy creation**

## Threat Detection

### User and Entity Behavior Analytics (UEBA)

Prisma Cloud analyzes millions of audit events, and then uses machine learning to detect anomalous activities that could signal account compromises, insider threats, stolen access keys, and other potentially malicious user activities that could threaten data security.



**Figure 4: Anomalous activity tracker**

### Network Anomaly Detection

Prisma Cloud monitors cloud environments for unusual network behavior and can detect unusual server port or protocol activity, including port scans and port sweeps that probe servers or hosts for open ports.

Back

Filter(s): Policy Type = Anomaly

Port scan activity (External)

Identifies port scan attempts by inspecting inbound network traffic to your cloud environment. A host outside your environment is scanning one of your cloud hosts. Port scans are a type of discovery attack where a source host is probing a target host across multiple ports, to find out what services are running and to uncover vulnerabilities associated with those services.

Recommendation

1. Review the list of scanned ports to determine the ones to be closed. Reducing the number of ports available decreases the opportunities for adversaries to compromise your cloud resources.

2. Please review and fix any violating policy associated with the target host in the alert, as reported by Prisma Cloud.

Violating Resources

Modern Table (Beta)

Remediate

	ALERT ID	RESOURCE NAME	ACCOUNT	REGION	ALERT STATUS	RATING	OPTIONS								
<input checked="" type="checkbox"/>	P-45094	188.166.186.209	Azure: RedLock Demo Account	Azure East US	Open	N/A	<div><div></div><div></div><div></div></div>								
<table><tr><th>SOURCE HOST</th><th>SOURCE LOCATION</th><th>TARGET HOST</th><th>TARGET PORT COUNT</th></tr><tr><td>188.166.186.209</td><td>Singapore</td><td>Bastion-Host-2</td><td>1000</td></tr></table>								SOURCE HOST	SOURCE LOCATION	TARGET HOST	TARGET PORT COUNT	188.166.186.209	Singapore	Bastion-Host-2	1000
SOURCE HOST	SOURCE LOCATION	TARGET HOST	TARGET PORT COUNT												
188.166.186.209	Singapore	Bastion-Host-2	1000												
<input type="checkbox"/>	P-44786	185.39.10.14	Azure: RedLock Demo Account	Azure West US	Open	N/A	<div><div></div><div></div><div></div></div>								
<input type="checkbox"/>	P-44700	93.174.93.68	Azure: RedLock Demo Account	Azure East US	Open	N/A	<div><div></div><div></div><div></div></div>								
<input type="checkbox"/>	P-44405	93.174.93.68	Azure: RedLock Demo Account	Azure West US	Open	N/A	<div><div></div><div></div><div></div></div>								
<input type="checkbox"/>	P-44404	93.174.93.68	Azure: RedLock Demo Account	Azure West US	Open	N/A	<div><div></div><div></div><div></div></div>								
<input type="checkbox"/>	P-44403	185.39.10.54	Azure: RedLock Demo Account	Azure East US	Open	N/A	<div><div></div><div></div><div></div></div>								
<input type="checkbox"/>	P-44354	89.248.172.196	Azure: RedLock Demo Account	Azure East US	Open	N/A	<div><div></div><div></div><div></div></div>								
<input type="checkbox"/>	P-44282	89.248.172.196	Azure: RedLock Demo Account	Azure West US	Open	N/A	<div><div></div><div></div><div></div></div>								
<input type="checkbox"/>	P-44281	89.248.172.196	Azure: RedLock Demo Account	Azure West US	Open	N/A	<div><div></div><div></div><div></div></div>								
<input type="checkbox"/>	P-44280	80.82.77.214	Azure: RedLock Demo Account	Azure East US	Open	N/A	<div><div></div><div></div><div></div></div>								
<input type="checkbox"/>	P-43973	89.248.168.62	Azure: RedLock Demo Account	Azure West US	Open	N/A	<div><div></div><div></div><div></div></div>								
<input type="checkbox"/>	P-43972	185.39.10.14	Azure: RedLock Demo Account	Azure West US	Open	N/A	<div><div></div><div></div><div></div></div>								
<input type="checkbox"/>	P-43971	185.39.10.25	Azure: RedLock Demo Account	Azure East US	Open	N/A	<div><div></div><div></div><div></div></div>								

**Figure 5: Port scan activity detail**

## Automated Investigation and Response

Prisma Cloud provides automated remediation, detailed forensics, and correlation capabilities. Insights combined from workloads, networks, user activity, data, and configurations accelerate incident investigation and response.

The screenshot displays the 'Violating Resources' section in the Prisma Cloud console. It features a table with columns for Alert ID, Resource Name, Account, and Options. A modal window is open, showing a warning about the impact of a remediation command and the specific CLI command to be executed.

Alert ID	Resource Name	Account	Options
P-45089	EC2ContainerService-default-test-EcsSecurityGroup-UUD683S3Z3T4	AWS: RedLo	Remediate
P-44971	launch-wizard-8		
P-44964	launch-wizard-7		
P-44617	launch-wizard-6		
P-44607	k8s-elb-a90cc32b		
P-44585	terraform-202007		
P-44279	launch-wizard-4		
P-44278	launch-wizard-5		
P-44246	Red Hat Enterpris		
P-44239	Red Hat Enterpris		
P-43969	launch-wizard-3		

**Running this command may have an adverse impact on your application**

"This CLI command requires 'ec2:RevokeSecurityGroupIngress' permission. Successful execution will update the security group to revoke the ingress rule records open to internet either on IPv4 or on IPv6 protocol." To resolve the alert from Prisma Cloud's console, add the permission.

Copy to Clipboard

```
aws --region us-east-2 ec2 revoke-security-group-ingress --group-id sg-0c7777a30125a8180 --ip-permissions [{"IpProtocol": "tcp", "FromPort": 80, "ToPort": 80, "IpRanges": [{"CidrIp": "0.0.0.0/0"}]}];
```

View Resource Config

Execute Command

**Figure 6:** Automated investigation detail

## About Prisma Cloud and the US Government

Hundreds of civilian and defense agencies, departments, bureaus, and offices trust Palo Alto Networks to safeguard their operations, data, and missions. Agencies use Prisma Cloud capabilities, both on-premises and in the cloud, to protect their data, applications, and workloads.

- For examples of how governments self-host [Prisma Cloud Compute Edition](#) and rapidly build as well as deploy secure cloud applications, watch our [DevSecOps in a Mission-Critical Environment](#) webinar.
- For more information on FedRAMP Authorized services from Palo Alto Networks, visit [paloaltonetworks.com/security-for-government/fedramp](https://paloaltonetworks.com/security-for-government/fedramp).
- Prisma Cloud and other Palo Alto Networks products and services assist agencies in adhering to CDM program requirements. For more information, read our [CDM at a Glance](#) datasheet.
- For more information on how Palo Alto Networks serves the needs of the US government, visit [paloaltonetworks.com/us-federal](https://paloaltonetworks.com/us-federal).