TOP CLOUD SECURITY CONCERNS OF FEDERAL AGENCIES

"Through 2022,
95%
of cloud security failures will be the customer's fault." — Gartner, Inc.

Palo Alto Networks helps agencies reduce risks in the cloud with Prisma™ Cloud security and compliance technology.

CLOUD DEPLOYMENTS

Public
aws | | Azure

Hybrid
aws | Azure | vmware®

Private
C2S/C2E | DEOS | JEDI
GOVCLOUD | milCloud | SOF

SaaS
box | GitHub | G Suite
Office 365 | salesforce | servicenow

CONCERNS AND RISKS

46%
of organizations accept traffic to Kubernetes® pods from any source[1]

65%
of reported cloud incidents between Jan. 2018 and June 2019 were due to misconfiguration[2]

In trying to protect cloud workloads:

34% of SOC teams struggle with compliance[2]

33% struggle with visibility into cloud security[2]

64%
of security pros cite data loss/leakage as their top cloud security concern[3]

PRISMA

Prisma Cloud
Comprehensive visibility, threat prevention, compliance assurance and data protection across multi-cloud environments

Prisma Cloud Compute Edition
Protection across hosts, containers and serverless deployments in any cloud and throughout the software lifecycle

VM-Series
Virtualized Next-Generation Firewalls that deliver in-line network security and threat prevention across private and public cloud environments

Prisma SaaS
Application security that provides data protection, governance and compliance to safely enable agencies to adopt SaaS

1. "5 Key Cloud Security Trends," Palo Alto Networks Unit 42, 2019.

2. "Cloudy with a Chance of Entropy," Palo Alto Networks Unit 42, 2019.

3. "2019 Cloud Security Report," Cybersecurity Insiders, 2019.