Effective Cloud Security and Compliance in Financial Services

Insights from Palo Alto Networks and AWS

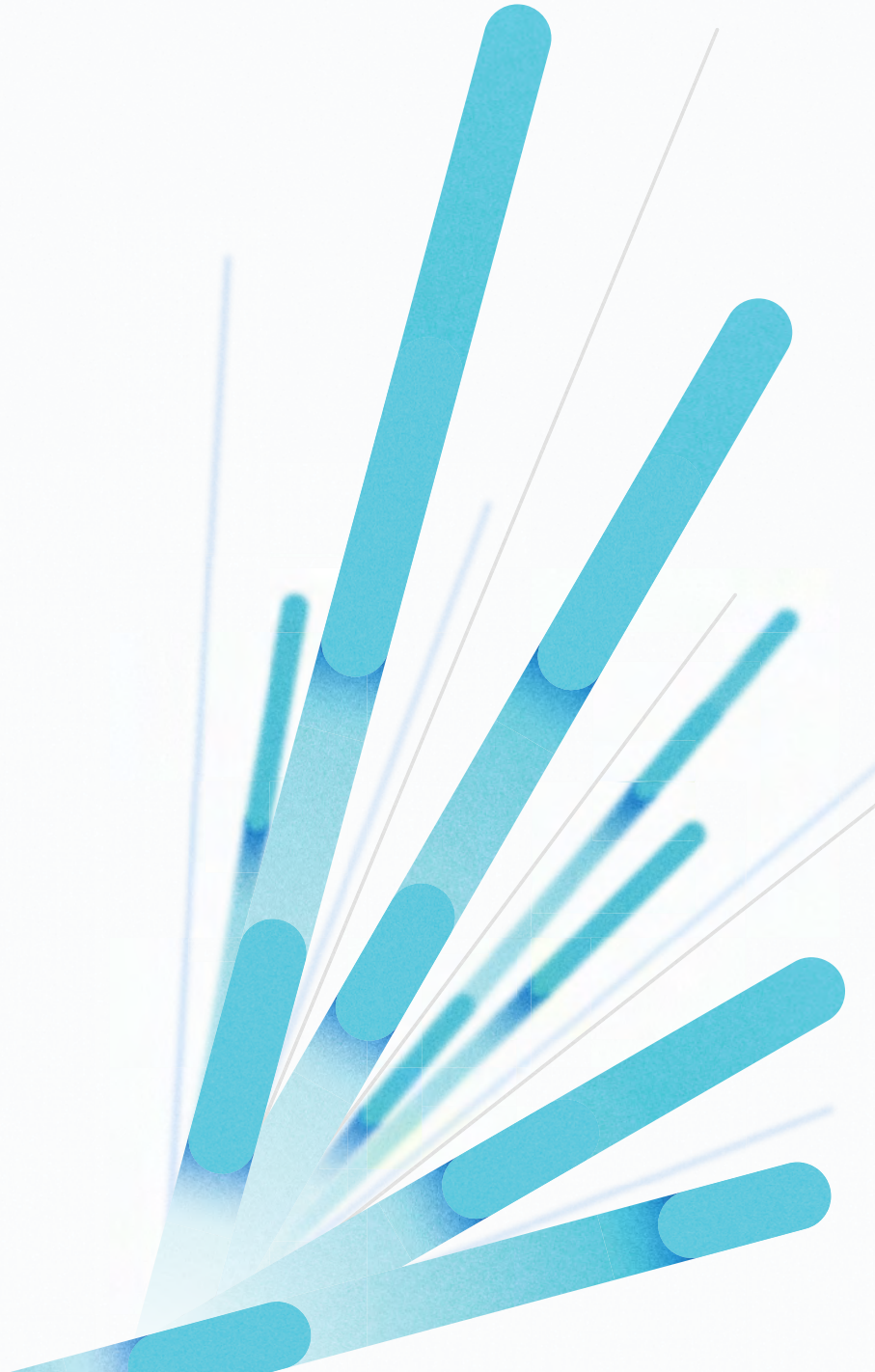


Table of contents

Tackle common FinServ security questions around cloud adoption

The COVID-19 pandemic forced all companies to accelerate their cloud adoption, regardless of how regulated or risk averse their respective industry. The need for work-from-home environments pushed companies already undergoing their cloud adoption journey to rethink how they use the cloud to enable remote access and capabilities for every facet of their business.

Financial services (FinServ) organizations responded quickly to ensure business as usual for financial customers with the realization that the industry-wide shift to the cloud also meant a race to developing a whole new way to do business as usual.

Amazon Web Services (AWS) offers innovative technologies that financial services organizations can use to create new value and truly differentiate themselves in a busy market.

However, FinServ organizations often have five critical questions about security and compliance:

1. How do I **stay on top of emerging security threats** and potential attacks?
2. How do I **better understand my organization's role in cloud security**?
3. How do I **ensure that my cloud environment is secure** and configured properly at all times?
4. Can my cloud provider help me **satisfy industry and regulatory requirements**—even as they change?
5. What can I do to **empower my developer teams** to move fast AND stay secure?

To confidently address these questions, FinServ organizations need partners who deeply understand their industry and cloud technology. Palo Alto Networks, together with AWS, can provide FinServ organizations access to key capabilities that enable the speed and agility you need in the face of today's ever-changing threat landscape. Palo Alto Networks and AWS offer the broadest set of integrated security capabilities to help with every stage of the cloud adoption journey. This eBook presents the partners' combined perspective to help you address your most pressing cloud security issues and plan for your future with confidence.

paloalto NETWORKS | aws

Stay on top of emerging security threats

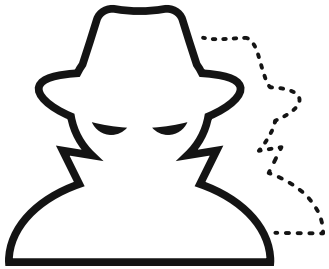
The cloud environment constantly changes. On one hand, it seems like every day a new threat, cyberattack, or piece of malware emerges threatening your business and customers. On the other hand, AWS constantly rolls out new services and features that offer valuable opportunities for innovation and efficiency.

Security events and threats continue to center around three primary areas:

- **Data Breaches** from external or internal attacks, which result in hundreds of millions of stolen accounts and exposure of sensitive data
- **Account hijacking** in which malicious hackers launch any number of attacks, including denial of service and ransomware, into an environment
- **Cloud misconfigurations**, or risks customers unknowingly create for themselves through the policies and permissions they enact (or fail to enact) over users, data, and applications in the cloud. By 2025, Gartner projects 99% of cloud security failures will be the customers' fault.

The AWS Shared Responsibility Model defines roles and responsibilities that AWS and its customers assume in the cloud. Reviewing the model helps reinforce awareness of available AWS resources to support security and compliance and also helps avoid confusion about where responsibility starts and ends.

AWS continuously updates security features of its services, referred to as 'Security OF the Cloud.' It offers native tools to help you stay abreast of changing regulations. For example, the self-service portal for AWS compliance reports, AWS Artifact, provides access to AWS auditor-issued reports, certifications, accreditations, and other third-party attestations across a variety of global, regional, and industry specific security standards and regulations.



Better understand your role in cloud security

As a customer in the shared responsibility model, you are responsible for security IN the cloud, which includes activities like defining data and application permissions and configuring networks and firewalls. But you're never alone. AWS provides best practice documentation, encryption tools, and guidance you can use to help you choose the right security measures for your business needs. You can also enlist the help of AWS Security Partners, such as Palo Alto Networks, that create solutions to integrate seamlessly with AWS to deliver comprehensive security and control coverage.

Prisma Cloud from Palo Alto Networks provides a comprehensive, cloud native security platform (CNSP) to help you manage security and compliance across multiple public clouds, private clouds, and hybrid environments including on-premises data centers. The integrated solution helps secure the entire cloud stack—from your infrastructure-as-a-service (IaaS) deployments on Amazon Elastic Compute Cloud (Amazon EC2), to Platform-as-a-Service (PaaS) solutions like Amazon Redshift, Amazon Elastic Container Service (Amazon ECS), and Amazon Lambda functions.

With Prisma Cloud, you also get full visibility into AWS Identity and Access Management (IAM) settings to oversee users and roles and easily apply the principle of least privileges to control who can access which data. Simple changes like removing excessive permissions can greatly reduce the attack surface.

Keep cloud environment secure with a trusted security partner

Palo Alto Networks runs a dedicated Cloud Security Research team exclusively within Prisma Cloud. The team continuously monitors all the new services and features being launched by AWS and develops security best practices. It is responsible for all the security guardrails delivered through Prisma Cloud as OOB policies.

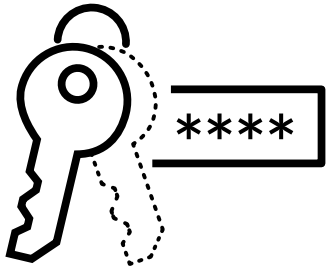
Additionally, Unit 42 at Palo Alto Networks, influences Prisma Cloud security guardrails and policies. Unit 42 includes over 200 global threat intelligence researchers with world-class expertise in adversary tools, techniques, and develops comprehensive Incident Response and Recovery capabilities in addition to proactive cloud security assessments. You can apply this research and insight automatically through the proverbial single pane of glass when you use Prisma Cloud to monitor and secure your entire cloud footprint.

750+

OOB POLICIES AND COUNTING

EXTEND YOUR ZERO TRUST ARCHITECTURE TO AWS TO HELP YOU DEPLOY AND ITERATE FASTER

Palo Alto Networks recently launched identity-based, micro-segmentation capabilities for east-west traffic to help your institution adopt containers and microservices while controlling access and preventing lateral movement of an attacker.



paloalto NETWORKS | aws

Meet industry and compliance requirements

FinServ organizations need to monitor the security and compliance posture of all their environments in real-time and against historical trends as part of appropriate governance. Tracking and meeting regulations, like PCI, GDPR, and local data privacy laws, requires coordination between services designed by cloud providers and solutions built and configured by cloud partners.

When it comes to Security OF the Cloud, AWS experts continuously monitor industry trends to understand potential issues, develop regulatory and authority relationships to stay abreast of emerging requirements, and hone long-term strategies to help meet customer security assurance needs. As an AWS customer, you can leverage that strong foundation by using AWS Partner solutions with AWS services to protect your application logic and data IN the Cloud.

Prisma Cloud for AWS provides visibility into how your workloads track against compliance requirements. The Palo Alto Networks team uses industry benchmarks like NIST and CIS, as well as regulatory standards like HIPAA and PCI to provide continuous compliance posture monitoring and one-click reporting. From this central system, you can easily investigate and auto-remediate compliance violations.

Comprehensive coverage for 20+ compliance standards

CIS, GDPR, HIPAA, ISO-27001, NIST-800, PCI-DSS, SOC 2

Empower developers to build fast AND secure

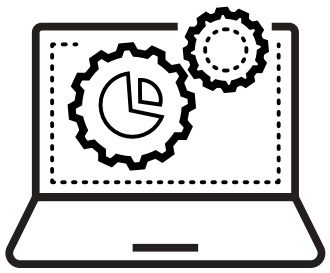
In today's cloud-based workplace, application development can move fast which enables your financial institution to be responsive, but also begs the question, "what are you doing to ensure developers can build quickly while maintaining strong security practices and adhering to governance policies?"

Ideally, everyone owns security—not just those with "Security" in their job title. This change requires a shift-left mentality across the organization to make security an integrated, automated component of DevSecOps processes and a central focus for your culture.

One of the best ways to raise the security culture of your organization and ensure security becomes an integral part of technology development and business enablement, is to embed security into development. When the most desirable action for developers is also the most secure action, everyone wins. Using automation to replace manual or ad hoc processes goes a long way to supporting a SecDevOps approach to to app development. Automation improves your overall control environment and increases your speed and agility, so you realize business value faster without risking security or compliance.

Palo Alto Networks continuously helps customers embed security and compliance checks early and often across the application development cycle. With Prisma Cloud, automated security scans are embedded into all your favorite CI/CD tools and used on AWS to accelerate developer productivity and time to market.

Deliver releases faster and prevent security lapses by applying a consistent set of security checks for your AWS CloudFormation templates and TerraForm scripts through the build-to-release process supported by Prisma Cloud.



paloalto NETWORKS | aws

Get started with Prisma Cloud on AWS

Together, Palo Alto Networks and AWS provide comprehensive security for the cloud. Palo Alto Networks offerings complement native AWS services across all solution areas, helping you protect your most mission critical and sensitive cloud applications.

With Prisma Cloud, you get enhanced visibility, security, and compliance across your entire AWS environment. Its native integrations allow you to extend AWS services, such as AWS Security Hub, AWS Control Tower, AWS Inspector, Amazon GuardDuty, AWS CloudTrail, and AWS Lambda, so you can process and act on cloud security events at the speed of modern business.

Help your financial services organization meet the demands of tomorrow's cloud-driven market. Run Prisma Cloud by Palo Alto Networks on AWS. Palo Alto Networks has:

- 4 AWS Competencies
- 8 AWS Marketplace solutions
- 500+ mutual customers in 12 months

Learn more about the Palo Alto Networks and AWS partnership.

Explore Palo Alto Networks solutions in the AWS Marketplace.