CLOUD SECURITY POWERED BY PALO ALTO NETWORKS PRISMA CLOUD

paloalto NETWORKS

Infosys®
Navigate your next

Cloud adoption, while it was revolutionizing business and IT for enterprises with all the benefits it offered, has now been fast-tracked by the pandemic to create the perfect digitization storm. This digitization storm has made cloud migration a must have technology objective. The dynamic nature of cloud landscape, lack of cloud skills, half-baked cloud migrations and shared responsibility model in cloud have opened up a lot of unknown and potential risks. Ensuring continuous evaluation and governance of enterprise security controls and regulatory baselines is a mandate. Today with majority of companies adopting a multi-cloud strategy, security governance challenges have only multiplied. To fight and overcome all these challenges, creating end to end visibility into all cloud assets and workflows is critical. With the desired visibility being established, the expected posture definition can be created for each workload so as to ensure complete cloud-native application security.
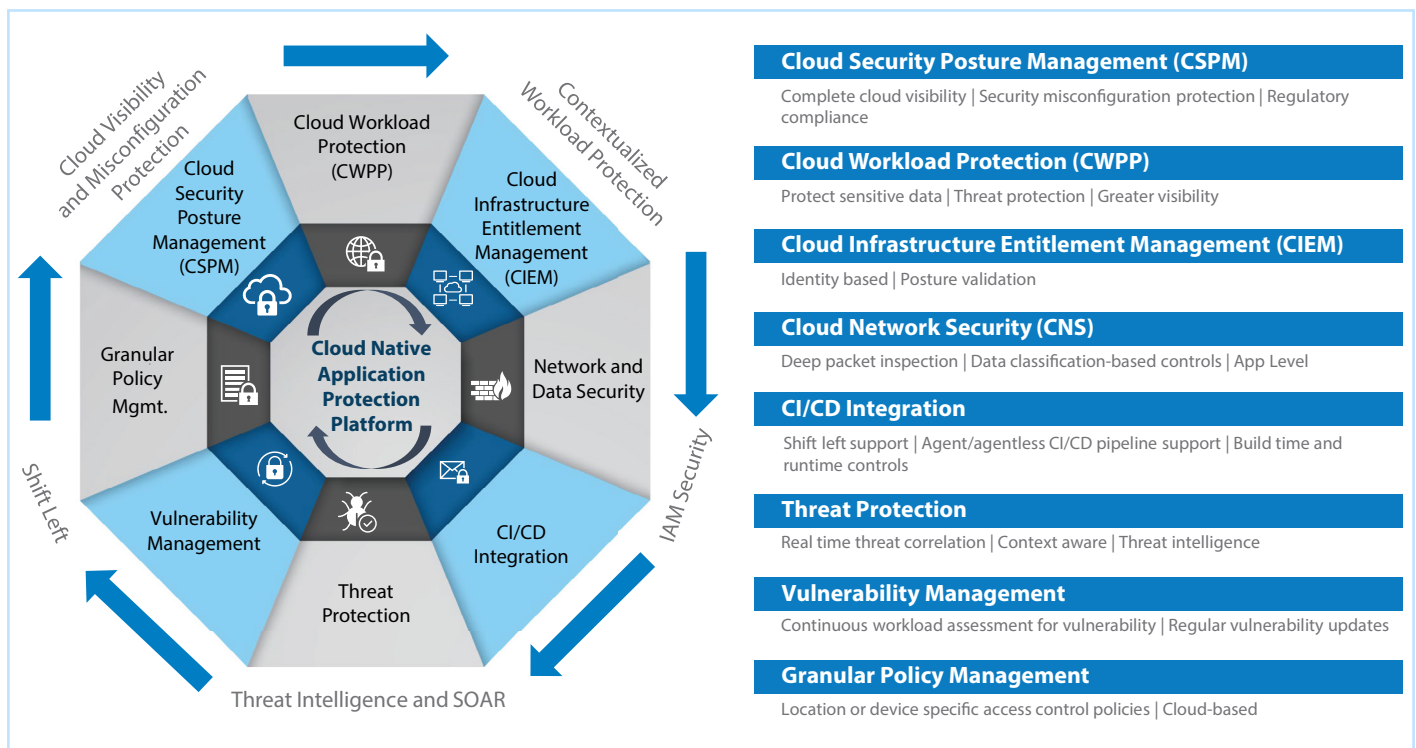
Definition

The 2021 Gartner® Hype Cycle™ for Cloud Security defines Cloud Native Application Protection Platforms (CNAPPs) as an integrated set of security and compliance capabilities designed to help secure and protect cloud-native applications across development and production. CNAPPs consolidate a large number of previously siloed capabilities, including container scanning, cloud security posture management, infrastructure as code scanning, cloud infrastructure entitlements management and runtime cloud workload protection platforms.
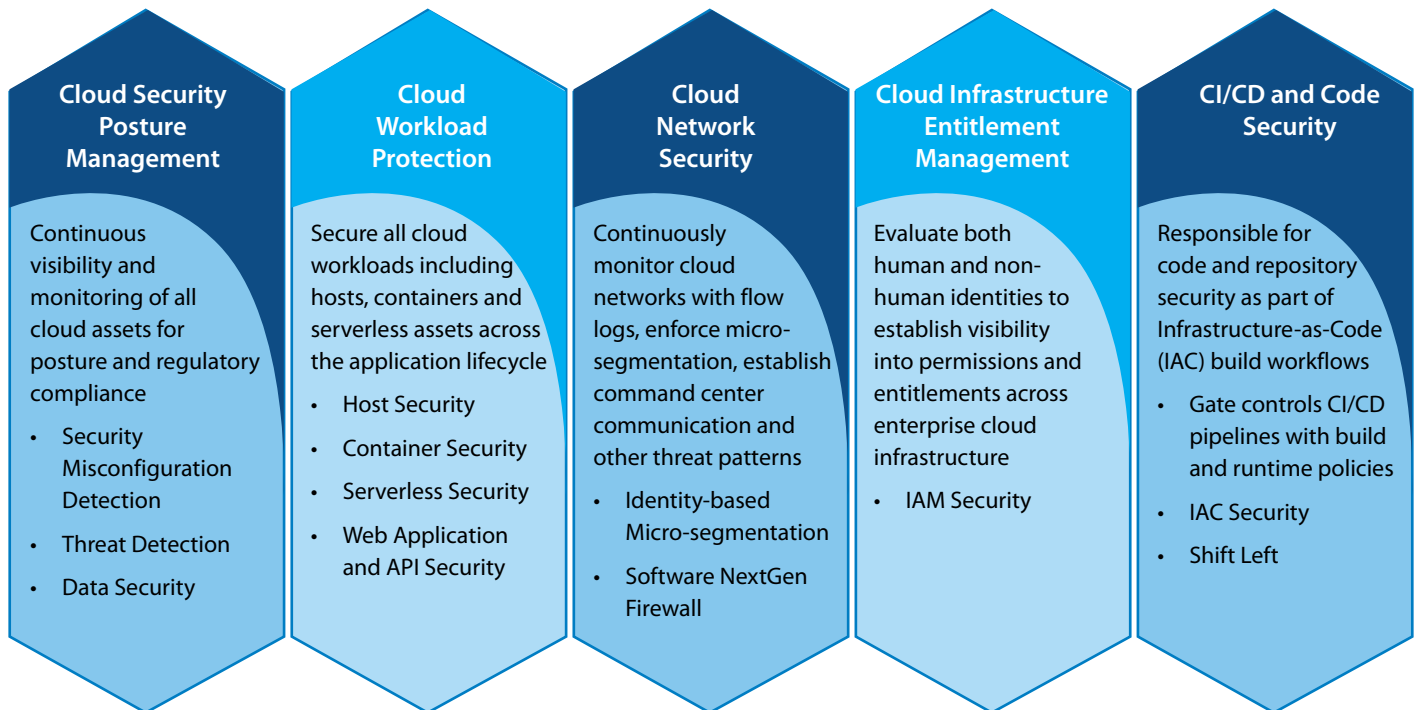
Unraveling CNAPP

CNAPP aims to integrate and centralize the otherwise distributed security functions into a single user platform interface. By partnering with Palo Alto Networks, we aim to utilize the Prisma Cloud technology to deliver solid and all-encompassing CNAPP. Its functionality includes Cloud Security Posture Management (CSPM), Cloud Workload Protection Platform (CWPP), Cloud Infrastructure Entitlement Management(CIEM), Cloud Network Security(CNS), Infrastructure as Code(IAC) and CI/CD Security. A full stack security is the primary delivery principle that creates and protects all cloud assets and workflows. This platform will ensure true partnership between DevOps and security infrastructure teams to provide enterprises cloud native and DevSecOps approach to cloud security management.

CNAPP Features and Capabilities

Cloud Security Posture Management (CSPM)
Complete cloud visibility | Security misconfiguration protection | Regulatory compliance

Cloud Workload Protection (CWPP)
Protect sensitive data | Threat protection | Greater visibility

Cloud Infrastructure Entitlement Management (CIEM)
Identity based | Posture validation

Cloud Network Security (CNS)
Deep packet inspection | Data classification-based controls | App Level

CI/CD Integration
Shift left support | Agent/agentless CI/CD pipeline support | Build time and runtime controls

Threat Protection
Real time threat correlation | Context aware | Threat intelligence

Vulnerability Management
Continuous workload assessment for vulnerability | Regular vulnerability updates

Granular Policy Management
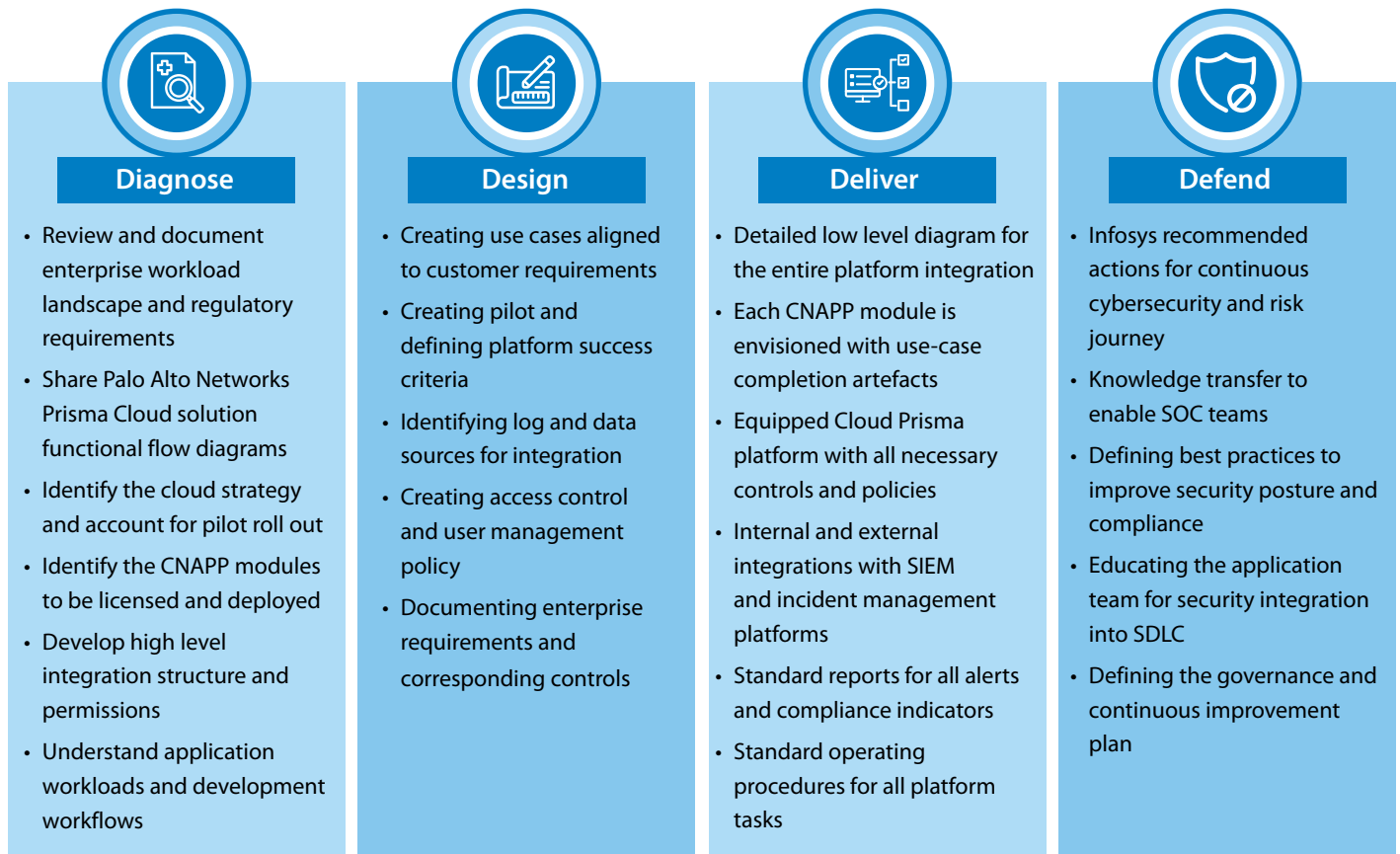Location or device specific access control policies | Cloud-based

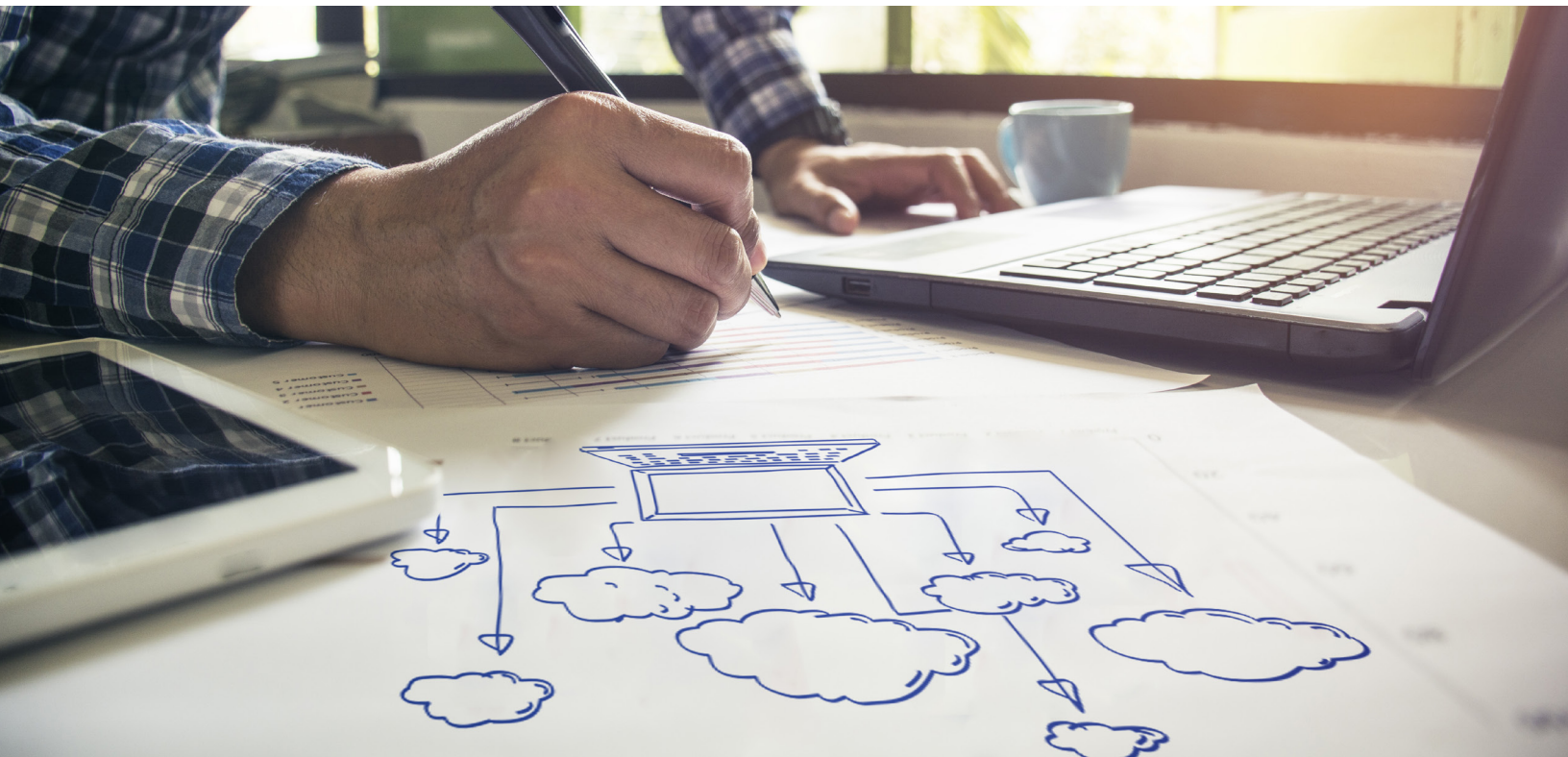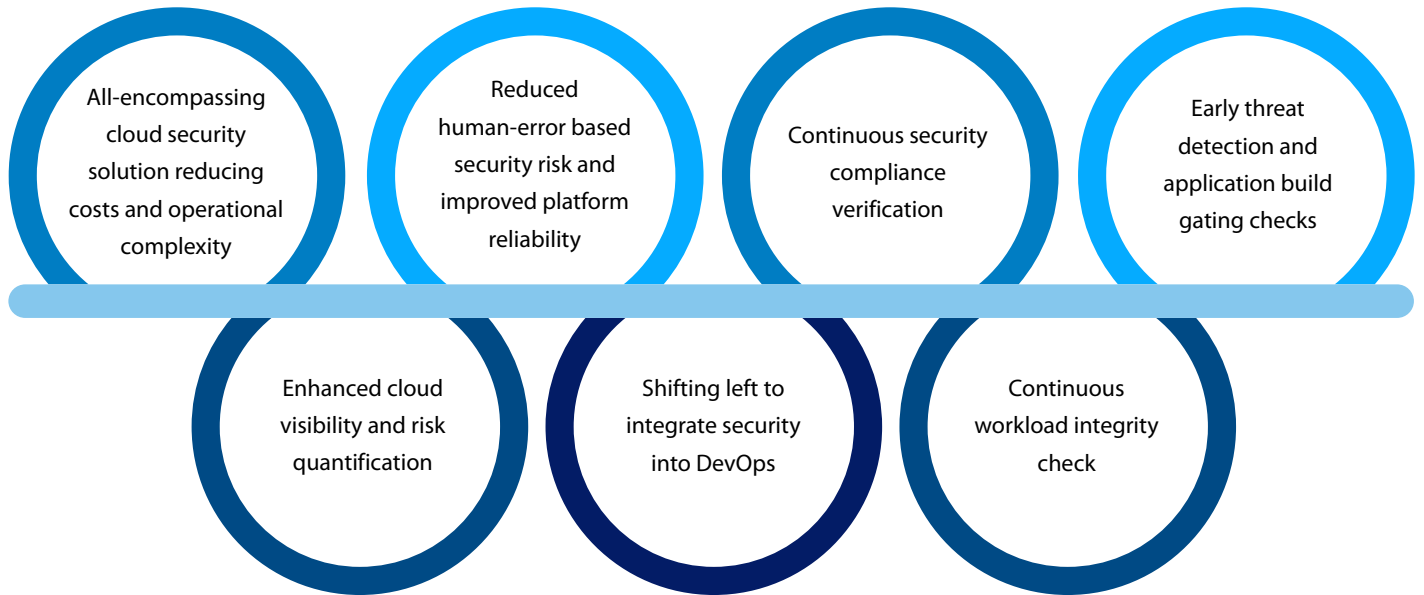# Infosys and Palo Alto Networks' CNAPP Offerings

With our global strategic partnership with Palo Alto Networks, we will utilize the Cloud Security industry experience and experts to align with the technology benefits provided by Palo Alto Networks Prisma Cloud platform to deliver one holistic and modular security platform which covers all aspects of cloud infrastructure security baselining and regulatory compliance.

Cloud Security Posture Management

Continuous visibility and monitoring of all cloud assets for posture and regulatory compliance

- Security Misconfiguration Detection
- Threat Detection
- Data Security

Cloud Workload Protection

Secure all cloud workloads including hosts, containers and serverless assets across the application lifecycle

- Host Security
- Container Security
- Serverless Security
- Web Application and API Security

Cloud Network Security

Continuously monitor cloud networks with flow logs, enforce micro-segmentation, establish command center communication and other threat patterns

- Identity-based Micro-segmentation
- Software NextGen Firewall

Cloud Infrastructure Entitlement Management

Evaluate both human and non-human identities to establish visibility into permissions and entitlements across enterprise cloud infrastructure

- IAM Security

CI/CD and Code Security

Responsible for code and repository security as part of Infrastructure-as-Code (IAC) build workflows

- Gate controls CI/CD pipelines with build and runtime policies
- IAC Security
- Shift Left

Comprehensive services aligned with Infosys 4D approach

Diagnose

- Review and document enterprise workload landscape and regulatory requirements
- Share Palo Alto Networks Prisma Cloud solution functional flow diagrams
- Identify the cloud strategy and account for pilot roll out
- Identify the CNAPP modules to be licensed and deployed
- Develop high level integration structure and permissions
- Understand application workloads and development workflows

Design

- Creating use cases aligned to customer requirements
- Creating pilot and defining platform success criteria
- Identifying log and data sources for integration
- Creating access control and user management policy
- Documenting enterprise requirements and corresponding controls

Deliver

- Detailed low level diagram for the entire platform integration
- Each CNAPP module is envisioned with use-case completion artefacts
- Equipped Cloud Prisma platform with all necessary controls and policies
- Internal and external integrations with SIEM and incident management platforms
- Standard reports for all alerts and compliance indicators
- Standard operating procedures for all platform tasks

Defend

- Infosys recommended actions for continuous cybersecurity and risk journey
- Knowledge transfer to enable SOC teams
- Defining best practices to improve security posture and compliance
- Educating the application team for security integration into SDLC
- Defining the governance and continuous improvement plan

Assured Benefits

- All-encompassing cloud security solution reducing costs and operational complexity
- Reduced human-error based security risk and improved platform reliability
- Continuous security compliance verification
- Early threat detection and application build gating checks
- Enhanced cloud visibility and risk quantification
- Shifting left to integrate security into DevOps
- Continuous workload integrity check

For more information, contact askus@infosys.com

Infosys®
Navigate your next

Infosys.com | NYSE: INFY

Stay Connected