SALES/CHANNEL PLAYBOOK: **Securing the Public Cloud**

Palo Alto Networks lets organizations confidently deploy applications in the cloud by delivering the industry's most advanced security and compliance capabilities across multi-cloud environments. Delivered through inline, API- and host-based protection technologies working together, these security capabilities integrate into the application development lifecycle to make cloud security frictionless for development and security teams.

MARKET OPPORTUNITY

Gartner predicted the worldwide public cloud services market would grow 18% in 2017 to $246.8B, up from $209.2B in 2016. Infrastructure as a service, or IaaS, was projected to grow 36.8% in 2017 and reach $34.6B. Software as a service, or SaaS, was expected to increase 20.1%, reaching $46.3B in 2017. Source: "Forecast: Public Cloud Services, Worldwide, 2014-2020, 4Q16 Update."

QUALIFICATIONS

IN	OUT
Customers deploying apps on AWS, Azure or Google (leveraging IaaS and/or PaaS)	Customers whose corporate policy prohibits cloud use
Customers reducing their datacenter footprint and moving from a CapEx model to an OpEx model	Customers not using cloud applications
Customers using SaaS apps such as Office 365, Box or G Suite	–

TECHNICAL DRIVERS, BUYERS AND KEY CAPABILITIES – *SecOps, Governance, Risk & Compliance, InfoSec, NetOps*

Technical Pain Points	How We Can Address Pain Points	Customer Benefits
Challenged to ensure org data is safe from theft while enabling rapid deployment of apps in the cloud	Integrates seamlessly into the app development lifecycle; allows developers to focus on their workflow while addressing security's need to protect apps and data	Security embedded into the app dev lifecycle eliminates "friction" and enables secure app delivery at cloud speed
Cloud provider security is inadequate and legacy security slows deployment	Delivers a multi-dimensional approach for public cloud security through inline, API- and host-based protection technologies working together to minimize opportunities for attack	Avoids fragmented security tools and leverages the industry's most advanced security and compliance capabilities across multi-cloud environments
App developers are often at odds with security because it appears to slow app deployment	Accelerates multi-cloud deployments and simplifies management through deep integration with native cloud services and automation tools	Security embedded into the app dev lifecycle eliminates "friction" and enables secure app delivery at cloud speed
Public cloud breaches are often caused by human/config errors	Protects public cloud resources with continuous discovery and monitoring, storage protection, and compliance validation	Prevents app or data breaches by minimizing the risk of blind spots and automatically remediating config errors

Buzzwords: Public cloud security, data protection, cloud-first, cloud-native security, compliance, risk management, cloud workload protection, automated security, DevSecOps

BUSINESS DRIVERS, BUYERS AND KEY CAPABILITIES – *CSOs, CIOs, Cloud Architects, DevOps, Cloud App Admins*

Business Pain Points	How We Can Address Pain Points	Customer Benefits
Challenged to ensure data is safe from breaches while embedding security into the application development and deployment processes	Enables orgs to confidently deploy apps in the cloud by delivering the industry's most advanced security and compliance capabilities across multi-cloud environments	Speed app dev and business growth while preventing data loss and business downtime
Desire to reduce their physical datacenter footprint and reduce costs, allowing for more investment in innovation	Provides advanced app and data breach prevention, consistent protection across locations and clouds, and "frictionless" deployment and management	Data centers are Capex-heavy – reduce data center footprint and move confidently toward an Opex model

Buzzwords: Intellectual property, agile, speed to market, reduce Capex, business growth, compliance, customer data

MESSAGING

Executive	Management	Technical
• Confidently deploy apps in the cloud by delivering the industry's most advanced security and compliance capabilities across multi-cloud environments	• Advanced app and data breach prevention protects against data loss and business disruption • Consistent protection across multiple clouds and locations • Frictionless deployment at rapid scale	• Adopt a multi-dimensional approach for public cloud security delivered through inline, API- and host-based protection technologies working together to minimize opportunities for attack ◦ Secure inline traffic with deep visibility, segmentation, secure access and threat prevention ◦ Protect public cloud resources via API with a unique combination of continuous discovery and monitoring, storage protection, and compliance validation ◦ Block exploits, ransomware, malware and fileless attacks to minimize infected workloads • Accelerate multi-cloud deployments and simplify management through deep integration with native cloud services and automation tools

CROSS-SELL, UPSELL AND MIGRATION PATH

Professional Services opportunities include architecture definition, design and implementation; ongoing architecture modifications and adjustments; and account optimization and management (for partners).

COMPETITIVE STRATEGIES

Competitors	Top 3 Differentiators	New Differentiators
• **Native security from cloud providers:** AWS (Security Groups, WAF service, Macie), Microsoft (Network Security Groups, Application Gateway, Cloud App Security) • **Legacy security vendors:** Check Point, Fortinet, Cisco • **Cloud-focused vendors:** Trend Micro, Alert Logic, CloudCheckr, Dome9 • **Cloud Access Security Broker vendors:** Netskope, McAfee/Skyhigh Networks, Symantec, Cisco CloudLock	• Safe enablement of cloud apps by providing deep visibility for reporting and compliance, and granular controls to secure them • Automated protections to stop known and unknown threats within cloud apps • Protect public cloud resources with Evident, delivering continuous discovery and monitoring, storage protection, and compliance validation • Unique platform approach uses shared data and machine learning to automatically distribute protections across all enforcement points	• Comprehensive, consistent protection across all three major public clouds (inline, API- and host-based protection) • Advanced cloud security that seamlessly integrates into the app dev lifecycle • Central management from the cloud of physical and virtualized firewalls for policy consistency

OVERCOMING OBJECTIONS

Objection	Effective Response
WE USE NATIVE SECURITY	Native cloud security only provides basic protection and cannot address multi-cloud needs, now or in the future.
YOUR PLATFORM IS HARD TO DEPLOY IN THE CLOUD	Providing advanced threat prevention requires visibility into traffic, but using cloud provider templates and third-party tools like Terraform or Ansible, we can create fully automated/touchless deployments. We can also provide frictionless protection through an API-based approach for continuous discovery and monitoring, storage protection, and compliance validation.

PRICING

- Inline (VM-Series on Public Cloud) licensing: The VM-Series can be deployed via a BYOL, VM-Series ELA or Marketplace for Google Cloud, AWS and Azure
- API-based (Evident on Public Cloud) licensing: Evident is licensed based on the number of public cloud accounts protected – $12K per account per year

SUGGESTED CONVERSION TOOLS

Prevention Posture Assessment – PPA provides a structured assessment of prevention capabilities across all areas of the customer's architecture

Ultimate Test Drive – Cloud-dedicated UTDs provide hands-on experience with our security platform for prospects interested in protecting cloud environments

SUPPORTING MATERIALS AND LINKS

Palo Alto Networks Sales: Field Portal on Intranet

Channel Partners: Partner Portal

- Sales FAQ
- Sales Insights Training
- Customer Presentation
- Datasheets