

Palo Alto Complete Triggers

Briona Adams



Guiding Customer Conversations

- Understanding CSPM
- Effectively Articulate the value of MDC
- Targeting the Customer
 - Highest likelihood Azure Customer – Azure is the dominant cloud
 - AWS Customer – AWS is the dominant cloud
 - No Azure Consumption
- Respond to High Level Objections to using Microsoft Security Solutions
- Highlight the Benefits of MDC for Azure Customers
- Highlight the Benefits of MDC for Non Azure/AWS Customers
- Impact of CloudKnox and RiskIQ Acquisitions
- Key Investment areas for MDC
- Roadmap for MDC (acknowledge gaps and highlight what MS is going to narrow gaps in key areas)
- Resource Listing

Microsoft Defender for Cloud can protect all these resources and workloads:

- Defender for Servers
- Defender for App Service
- Defender for ARM
- Defender for DNS
- Defender Containers
- Defender for Key Vault
- Defender for Storage
- Defender for SQL
- Defender for MySQL
- Defender for MariaDB
- Defender for PostgreSQL
- Defender for Azure Cosmos DB

Prisma is limited to

Capability	Description	MDC	Prisma Cloud	Comments
CSPM – Recommendations	Resource coverage & depth	2	5	
CSPM – Compliance	Out-of-the-box standards coverage & depth	1	5	
CWP – IaaS	VMs	4	2 (without Cortex EPP)	MDE is leader
CWP – PaaS	Storage, SQL etc.	--	3	
CWP – Containers		3	5	
CWP – Serverless	Functions, App Services	--	5	
CWP – Service Layer		--	2	
Shift-Left security	CI/CD & dev tools	--	5	
API Security		--	5	
Micro-segmentation	Identity-based	--	5	
CIEM		--	3	PANW CIEM is AWS only
Data classification and Governance	DLP, Classification (Purview)	5	3	Purview classification is a differentiator

Capability	Description	MDC	Prisma Cloud	Comments
CSPM – Recommendations	Resource coverage & depth	5	3	
CSPM – Compliance	Out-of-the-box standards coverage & depth	5	4	We have better depth, PANW cover more standards
CWP – IaaS	VMs	5	2 (without Cortex EPP)	MDE is leader
CWP – PaaS	Storage, SQL etc.	5		
CWP – Containers		3	5	
CWP – Serverless	Functions, App Services	2	5	
CWP – Service Layer	ARM, DNS, KV	5	2	
Shift-Left security	CI/CD & dev tools	--	5	
API Security		--	5	
Micro-segmentation	Identity-based	--	5	
CIEM		--	--	PANW CIEM is AWS only
Data classification and Governance		5	--	PANW DLP is AWS only

Highlighting the Benefits of MDC versus Prisma (Azure Customers)

Prisma

- Does not run in Azure.
 - It runs only in AWS or GCP.
 - To monitor Azure resources, data must be transmitted out of Azure.
- Does not have a true PAYG pricing model on GCP
- Does not protect as many Azure resource types as Microsoft Defender for Cloud
- Does not integrate/leverage many Azure services. Customers cannot benefit from their Azure investment and expertise.

Microsoft Defender for Cloud Benefits (Azure Customers)

	Microsoft Defender for Cloud	Prisma
Ease of onboarding	Automatic Discovery and frictionless onboarding for AKS clusters and ACR registries	Agent deployment on the cluster, is customer responsibility
Ease of management	Zero configuration for Container VA and threat detection (no policy decisions)	Prisma Cloud ships with an empty runtime policy, disabling runtime defense entirely. Manual steps need to be taken to enable it on each cluster and define policy rules.
Native/1 st party solution	<ul style="list-style-type: none"> Defender profile is embedded as part of AKS RP (<i>coming soon- can be enabled via AKS onboarding</i>). Defender VA is embedded in every ACR registry and scan images based on ACR activity Security findings are available via the AKS \ ACR resources 	What would we say about Prisma here?
Agentless threat detection	Kubernetes audit events based on KubeAudit logs are automatically streamed from AKS to MDC via Azure backbone without onboarding, configuration or customer cost.	Prisma collects Kubernetes audit events either through configuring Kubernetes audit sink (deprecated feature) or through integration with Log Analytics which requires per cluster configuration and can be significant Azure costs to the customer.
Azure Arc	Is Azure Arc worth mentioning as a benefit for coverage on On-Prem?	



Microsoft Defender for Cloud Benefits (Azure Customers)

	Microsoft Defender for Cloud	Prisma
Fileless Attack Detection	Uses automated memory forensic techniques to identify fileless attack toolkits, techniques, and behaviors. Fileless Attack Detection periodically scans Kubernetes runtime and extracts insights directly from the memory of the running processes. It can find evidence of exploitation, code injection and execution of malicious payloads.	Prisma doesn't have a similar capability. *Need to understand what Prisma's comparable solution is for fileless attack detection. What does Prisma do?
Linux process threats	Provides broad coverage for Linux process threats. *Need to quantify what broad coverage means.*	Prisma's process based runtime detection coverage is missing a lot of the Linux attack matrix techniques which are relevant also for containerized environment *Need to quantify or restate "missing a lot".
MITRE matrix for product evaluation and coverage	Microsoft Defender for Cloud, has an advantage being primary contributor to the MITRE attack matrix for containers, which is starting to become a common tool for customer evaluations	Is there a Prisma standard here for MITRE matrix? What is the true MDC advantage versus Prisma here?
Runtime model accuracy	Uses anomaly-based detections, learned across clusters and tenants, combined with signature and rule-based detections that are proven to expose real threats and remove false positives.	Alerts based on Prisma's runtime models (learning container baseline behavior) are noisy/generate many false positives and hard to manage at scale. *This sounds subjective, is this based on customer feedback. How can we make this more evidence/data rooted?

Objection Handling

Every security conversation is a compete and objection handling conversation

A big part of forming a reliable and complete diagnosis is listening. Beyond the symptoms their own organizations are experiencing, many ITDMs and technology leaders will also challenge you with doubts, objections, and especially competitors. And you should listen carefully to these concerns.

 <p>Objection</p>	<p>Prisma Cloud claims that with Prisma 3.0 it can provide agentless scanning i.e., requires no agents to be installed to collect relevant security data. I can see many advantages to this approach.</p> <p>Doesn't Defender for Cloud require agents? If so, why should I not choose Prisma Cloud?</p>	<p>Response</p> 	<ol style="list-style-type: none">1. Defender for Cloud requires agents and extension—for some, but not all, resources.2. The installation of these agents and extensions can be automated with auto-provisioning. Auto-provisioning reduces management overhead by installing all required agents and extensions on existing and new machines to ensure faster security coverage for all supported resources.3. Sometimes <i>APIs alone are not sufficient</i>—agents are required to gather all the required security information. That's why Prisma Cloud continues to support agents.
<p>Objection</p>	<p>Prisma Cloud claims it can provide CWPP and CSPM for resources in AWS, Azure, Google Cloud, Oracle Cloud (OCI) and Alibaba Cloud.</p> <p>I plan to use multiple clouds, doesn't Microsoft just protect Azure? Should I not choose Prisma Cloud over Defender for Cloud?</p>	<p>Response</p>	<p>Microsoft Defender for Cloud equally provides capabilities to protect cloud resources in Azure, AWS, GCP and on-premises. While CSPM capabilities for Azure and AWS are natively integrated, CWPP setup requires configuration. These articles describe how to connect Defender for Cloud to non-Azure machines, your AWS accounts, and your GCP accounts.</p> <p>For example, here's what Cloud Defender can do for your AWS accounts:</p> <ul style="list-style-type: none">• You can extend Defender for Cloud's CSPM features to your AWS resources. This <i>agentless plan</i> assesses your AWS resources according to AWS-specific security recommendations and these are included in your secure score. The resources will also be assessed for compliance with built-in standards specific to AWS (AWS CIS, AWS PCI DSS, and AWS Foundational Security Best Practices). Defender for Cloud's asset inventory page is a multicloud enabled feature helping you manage your AWS resources alongside your Azure resources.• Microsoft Defender for Containers extends the container threat detection and advanced defenses of Defender for Kubernetes to your Amazon EKS clusters.• Microsoft Defender for Servers brings threat detection and advanced defenses to your Windows and Linux EC2 instances. This plan includes the integrated license for Microsoft Defender for Endpoint, security baselines and OS level assessments, vulnerability assessment scanning, adaptive application controls (AAC), file integrity monitoring (FIM), and more.

Pricing Comparison

Prisma Cloud Enterprise Edition Pricing

Prisma Cloud prices are not public. Pricing is composed of modules. Each module has its own capacity unit and is charged per capacity unit. Units can be bought in increments of 100. Usage is measured based on the number of units consumed every hour, which roll up to daily, weekly, monthly, and quarterly averages.

Prisma Cloud pricing is less predictable, while Defender for Cloud offers a [pricing calculator](#) and [workbooks](#) to aid spend planning.

- Microsoft Defender for Cloud [public pricing page](#)
- Free: CSPM capabilities are free
- Paid: CWPP uses a workload-specific pay-as-you-go model

Prisma Cloud Module	Capacity Unit	Unit Price
Cloud Security Posture Management (CSPPM)		
Visibility, Compliance & Governance	Per instance of the following list of resources: <ul style="list-style-type: none"> • Amazon/AWS: EC2, RDS, Redshift, ELB, NAT gateway • Azure: Virtual Machines, SQL DB, PostgreSQL, SQL Managed Instance, Load Balancer • Google Cloud: GCE, Cloud SQL, Load Balancer, Cloud NAT • Alibaba Cloud: ECS • Oracle Cloud Infrastructure: Compute 	1 Prisma Cloud Credit per instance
Threat Detection (incl. in Enterprise Edition)	N/A	0
Data Security (for Amazon S3)	Per 33GB of Exposure, Sensitive and Malware scan (Full scan) <ul style="list-style-type: none"> • For Full scan, public exposure scanning will be charged for 200GB per credit for all selected data, while only classifiable data will be charged for 33GB per credit 	1
	Per 200GB of public exposure scan	1
Cloud Workload Protection (CWP)		
Host Security	Per Host Defender deployed	1
Container Security	Per Container Defender deployed	7
	Per Container Defender: App-Embedded deployed	1
Serverless Security	Per 6 Defender Functions (Serverless Defenders or Scanned Functions)	1
Web Application and API Security	Per Defender running Web Application and API Security	30

Release calendar H1 2022

Q1 2022

Public Preview announcements

Native support for Google Cloud Platform (GCP) – CSPM & CWP

- Native support for GCP CSPM
- Out-of-the-box security recommendation, aligned to CIS for GCP
- Protect GCP workloads including onboarding VM protection and K8s protection

Defender for Cosmos DB (part of Defender for Databases) - CWP

- Microsoft Defender for Cosmos DB helps organizations protect Cosmos DBs by providing cloud-native means to prevent, detect, and respond to threats quickly

Security Governance - CSPM

- Help organizations manage the process of improving security posture in their organization:
 - Enable organizations to easily identify owners & estimated timing for recommendation resolution
 - Define and track organization-wide “campaigns” on specific high-priority items

Vulnerability assessment for Windows container images

- Extending Defender for Containers VA capabilities to automatically scan Windows container images for known vulnerabilities.

Q2 2022

Public Preview announcements

Contextual CSPM

- Context-aware CSPM for optimized prioritization of recommendations that includes integrations with RiskIQ and CloudKnox

Defender for DevOps - CWP

A new offering that supports the shift-left strategy of organizations and will allow developers and security professionals to identify preventable security and quality issues early in development to defend unintended vulnerabilities from reaching production.

Antimalware for Storage - CWP

- Protect your storage estate from malware distribution and help meet compliance requirements using built-in malware scan at scale for storage accounts.

Vulnerability Assessment for Container images in AWS

- Extending Defender for Containers VA capabilities to automatically scan Linux container images stored in ECR for known vulnerabilities.