# Cloud Native Application Protection Platform

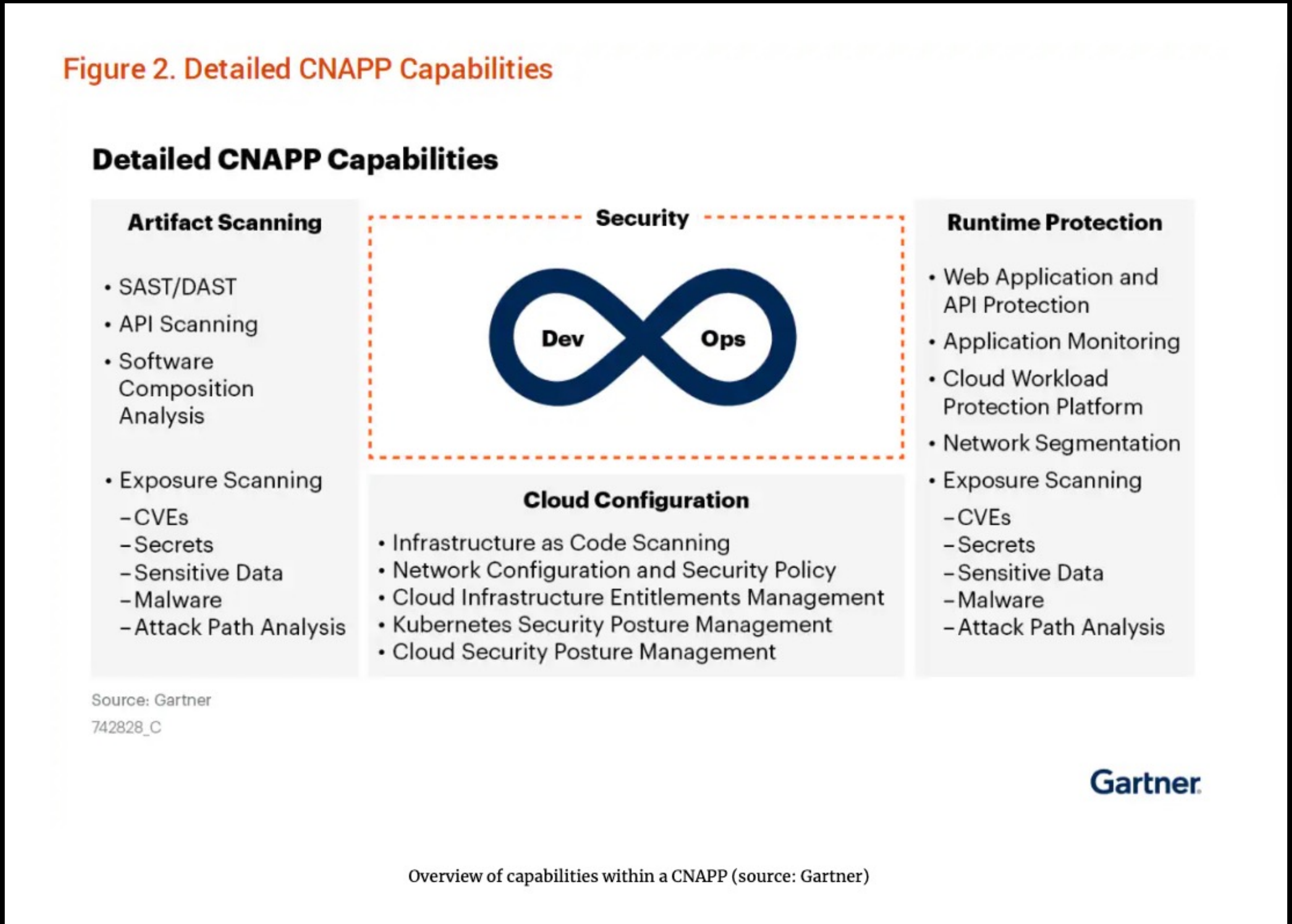


Figure 2. Detailed CNAPP Capabilities

## Detailed CNAPP Capabilities

**Artifact Scanning**

- SAST/DAST
- API Scanning
- Software Composition Analysis
- Exposure Scanning
  - CVEs
  - Secrets
  - Sensitive Data
  - Malware
  - Attack Path Analysis

**Security**

**Cloud Configuration**

- Infrastructure as Code Scanning
- Network Configuration and Security Policy
- Cloud Infrastructure Entitlements Management
- Kubernetes Security Posture Management
- Cloud Security Posture Management

**Runtime Protection**

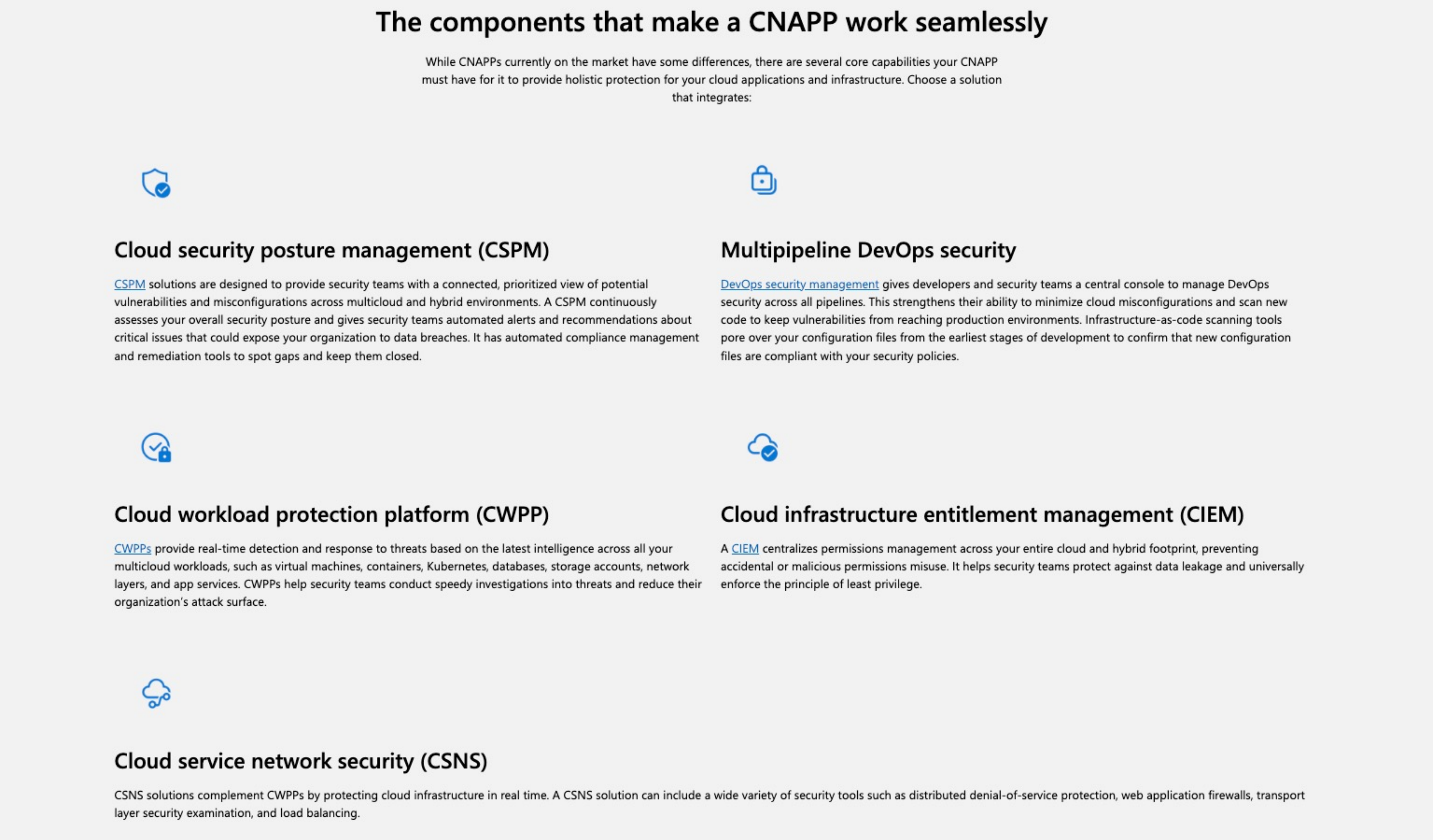
- Web Application and API Protection
- Application Monitoring
- Cloud Workload Protection Platform
- Network Segmentation
- Exposure Scanning
  - CVEs
  - Secrets
  - Sensitive Data
  - Malware
  - Attack Path Analysis

Source: Gartner
742828_C

Gartner

Overview of capabilities within a CNAPP (source: Gartner)

[Get to Know Cloud Native Application Protection Platforms (paloaltonetworks.com)]



## The components that make a CNAPP work seamlessly

While CNAPPs currently on the market have some differences, there are several core capabilities your CNAPP must have for it to provide holistic protection for your cloud applications and infrastructure. Choose a solution that integrates:

### Cloud security posture management (CSPM)

CSPM solutions are designed to provide security teams with a connected, prioritized view of potential vulnerabilities and misconfigurations across multicloud and hybrid environments. A CSPM continuously assesses your overall security posture and gives security teams automated alerts and recommendations about critical issues that could expose your organization to data breaches. It has automated compliance management and remediation tools to spot gaps and keep them closed.

### Multipipeline DevOps security

DevOps security management gives developers and security teams a central console to manage DevOps security across all pipelines. This strengthens their ability to minimize cloud misconfigurations and scan new code to keep vulnerabilities from reaching production environments. Infrastructure-as-code scanning tools pore over your configuration files from the earliest stages of development to confirm that new configuration files are compliant with your security policies.

### Cloud workload protection platform (CWPP)

CWPPs provide real-time detection and response to threats based on the latest intelligence across all your multicloud workloads, such as virtual machines, containers, Kubernetes, databases, storage accounts, network layers, and app services. CWPPs help security teams conduct speedy investigations into threats and reduce their organization's attack surface.

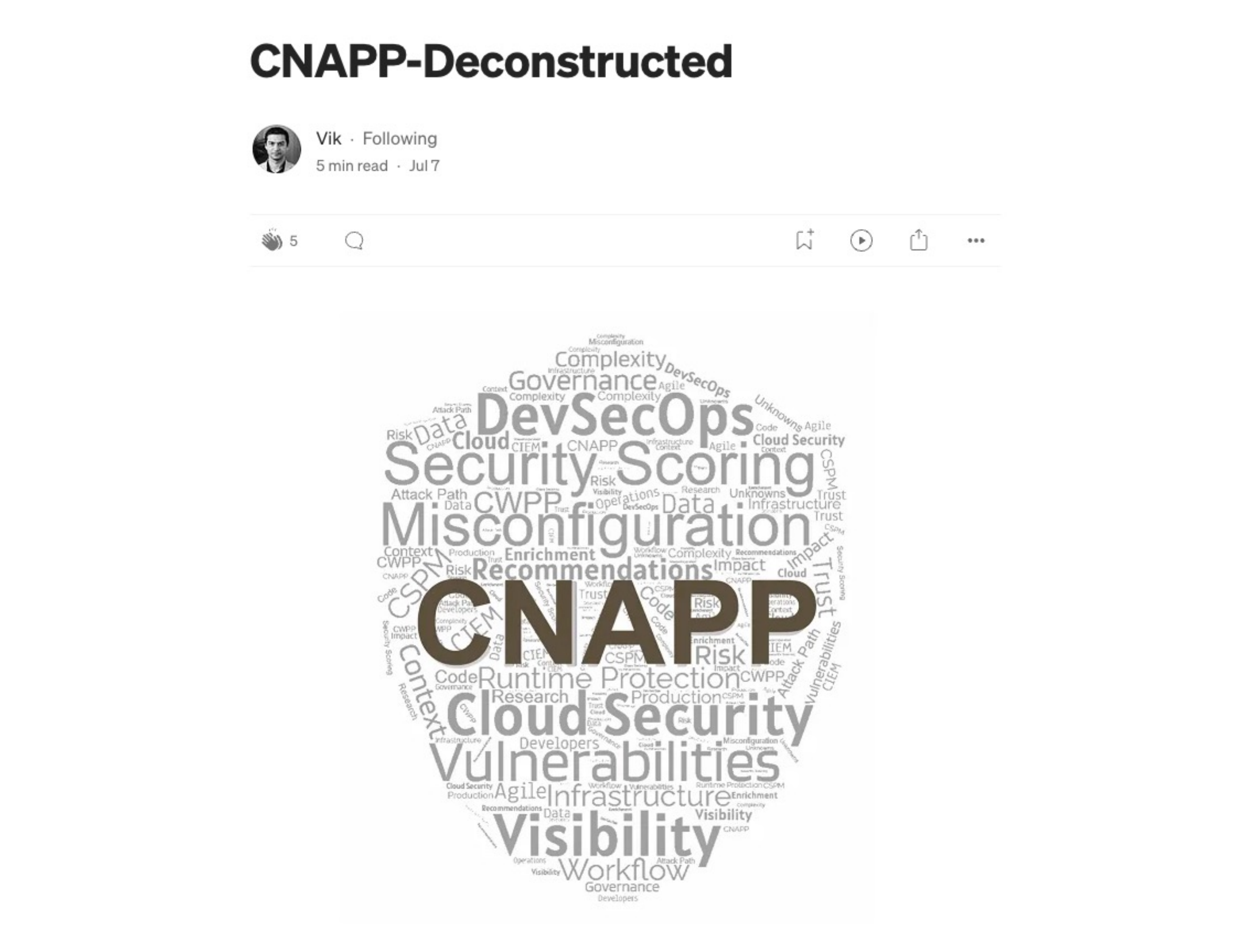
### Cloud infrastructure entitlement management (CIEM)

A CIEM centralizes permissions management across your entire cloud and hybrid footprint, preventing accidental or malicious permissions misuse. It helps security teams protect against data leakage and universally enforce the principle of least privilege.

### Cloud service network security (CSNS)

CSNS solutions complement CWPPs by protecting cloud infrastructure in real time. A CSNS solution can include a wide variety of security tools such as distributed denial-of-service protection, web application firewalls, transport layer security examination, and load balancing.

What Is a CNAPP? | Microsoft Security

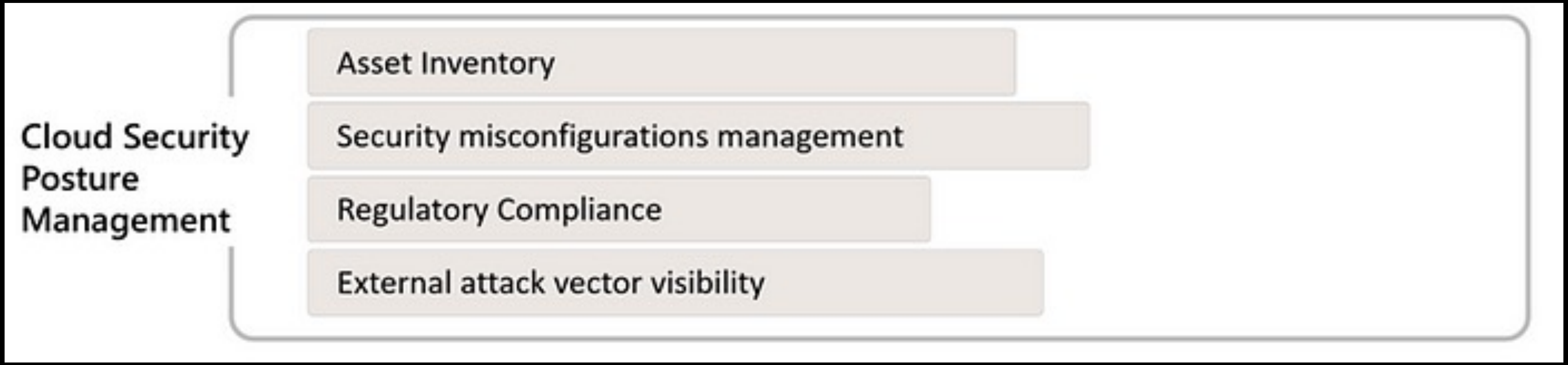


# CNAPP-Deconstructed

Vik · Following

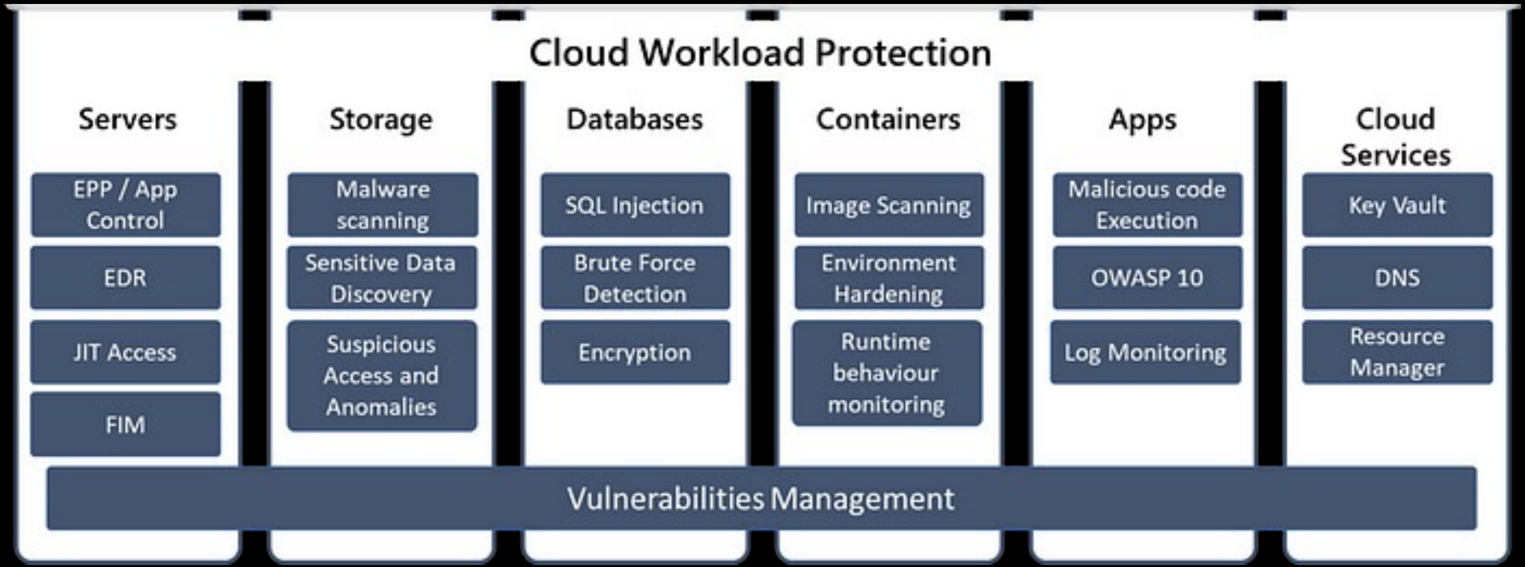
5 min read · Jul 7

[CNAPP-Deconstructed. The current state of cloud security | by Vik | Medium]()



Cloud Security Posture Management

- Asset Inventory
- Security misconfigurations management
- Regulatory Compliance
- External attack vector visibility

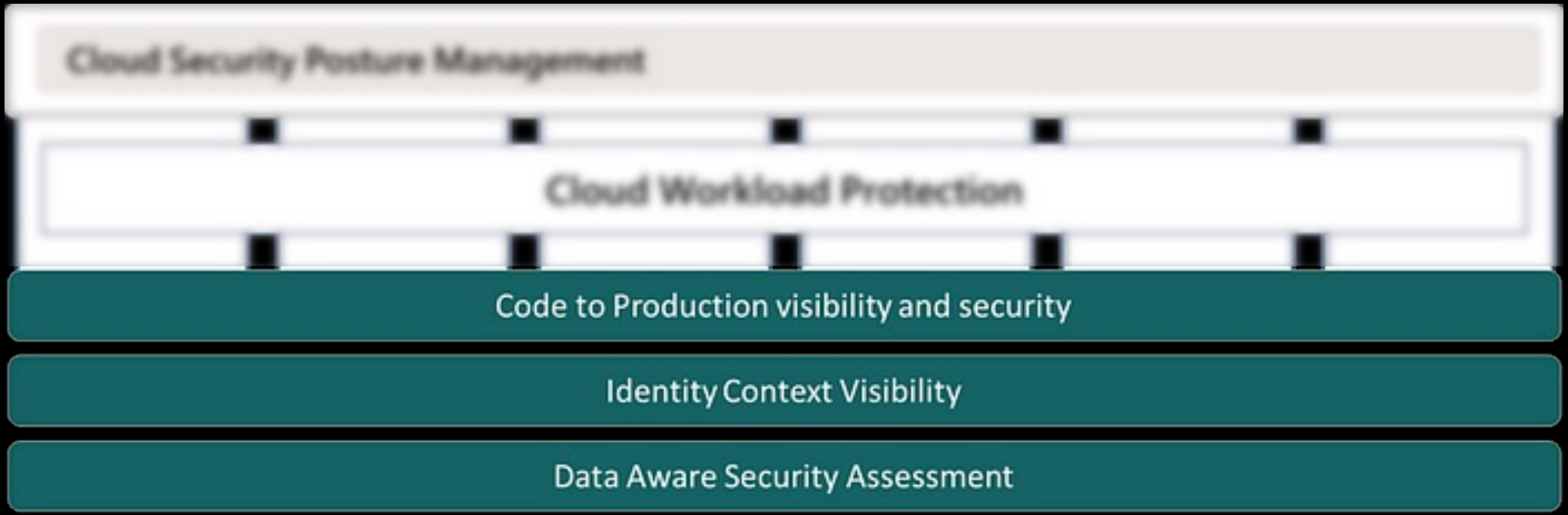


Cloud Workload Protection

| Servers | Storage | Databases | Containers | Apps | Cloud Services |
|---|---|---|---|---|---|
| EPP / App Control | Malware scanning | SQL Injection | Image Scanning | Malicious code Execution | Key Vault |
| EDR | Sensitive Data Discovery | Brute Force Detection | Environment Hardening | OWASP 10 | DNS |
| JIT Access | Suspicious Access and Anomalies | Encryption | Runtime behaviour monitoring | Log Monitoring | Resource Manager |
| FIM | | | | | |

Vulnerabilities Management

[CNAPP-Deconstructed. The current state of cloud security | by Vik | Medium]



Cloud Security Posture Management

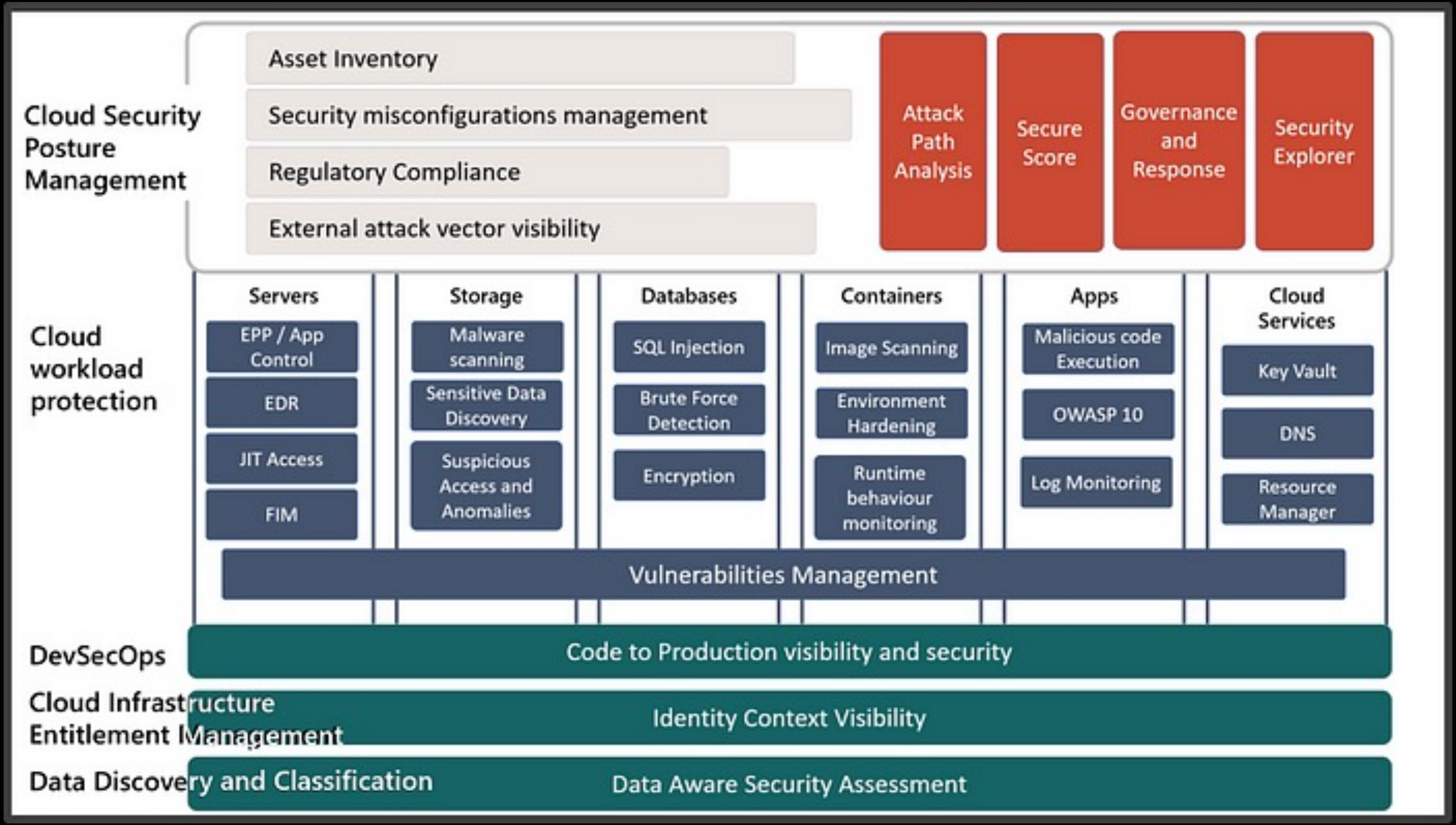
Cloud Workload Protection

Code to Production visibility and security

Identity Context Visibility

Data Aware Security Assessment

[CNAPP-Deconstructed. The current state of cloud security | by Vik | Medium]



Cloud Security Posture Management

- Asset Inventory
- Security misconfigurations management
- Regulatory Compliance
- External attack vector visibility

Attack Path Analysis

Secure Score

Governance and Response

Security Explorer

Cloud workload protection

| Servers | Storage | Databases | Containers | Apps | Cloud Services |
|---|---|---|---|---|---|
| EPP / App Control | Malware scanning | SQL Injection | Image Scanning | Malicious code Execution | Key Vault |
| EDR | Sensitive Data Discovery | Brute Force Detection | Environment Hardening | OWASP 10 | DNS |
| JIT Access | Suspicious Access and Anomalies | Encryption | Runtime behaviour monitoring | Log Monitoring | Resource Manager |
| FIM | | | | | |

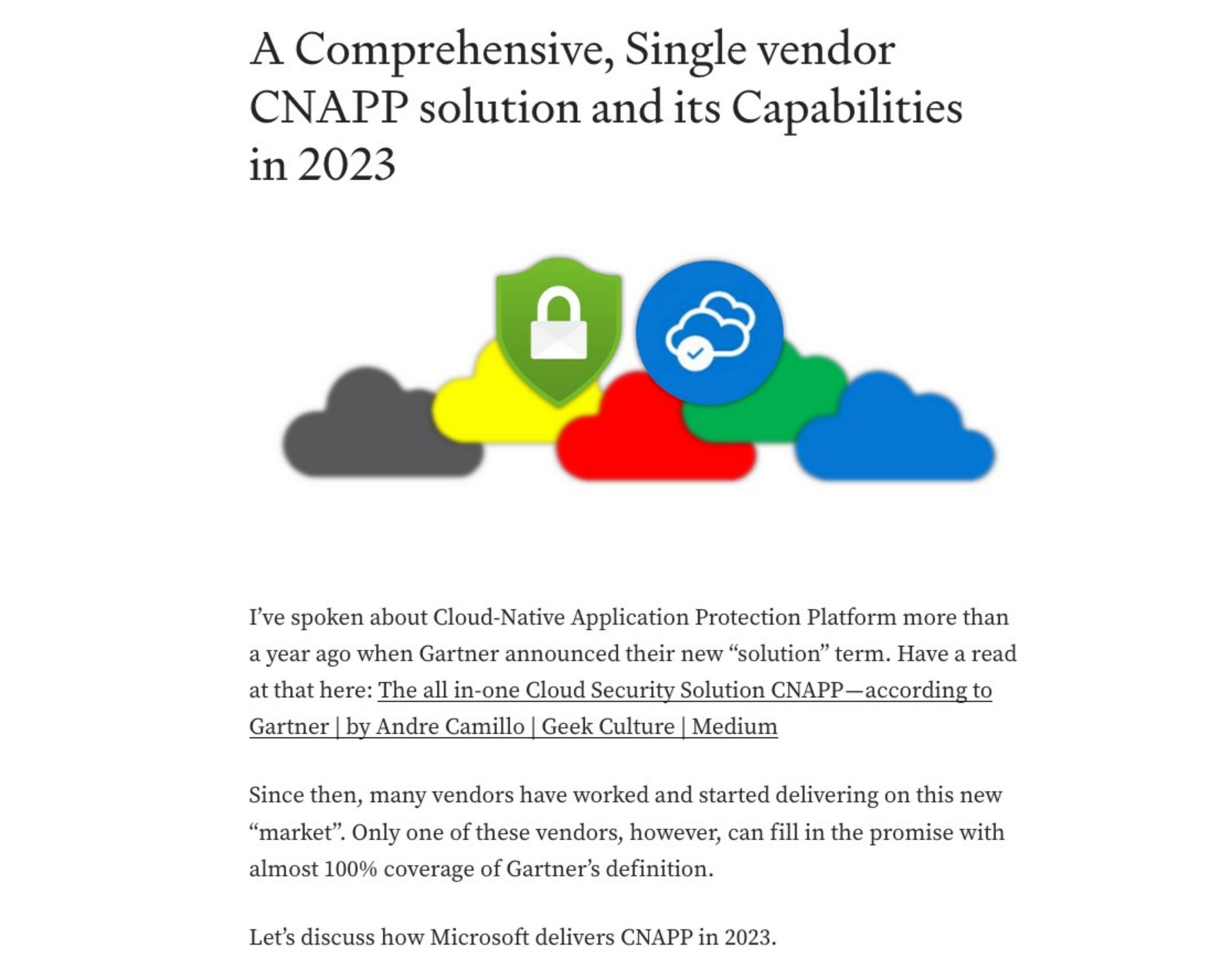
Vulnerabilities Management

DevSecOps: Code to Production visibility and security

Cloud Infrastructure Entitlement Management: Identity Context Visibility

Data Discovery and Classification: Data Aware Security Assessment

[CNAPP-Deconstructed. The current state of cloud security | by Vik | Medium]



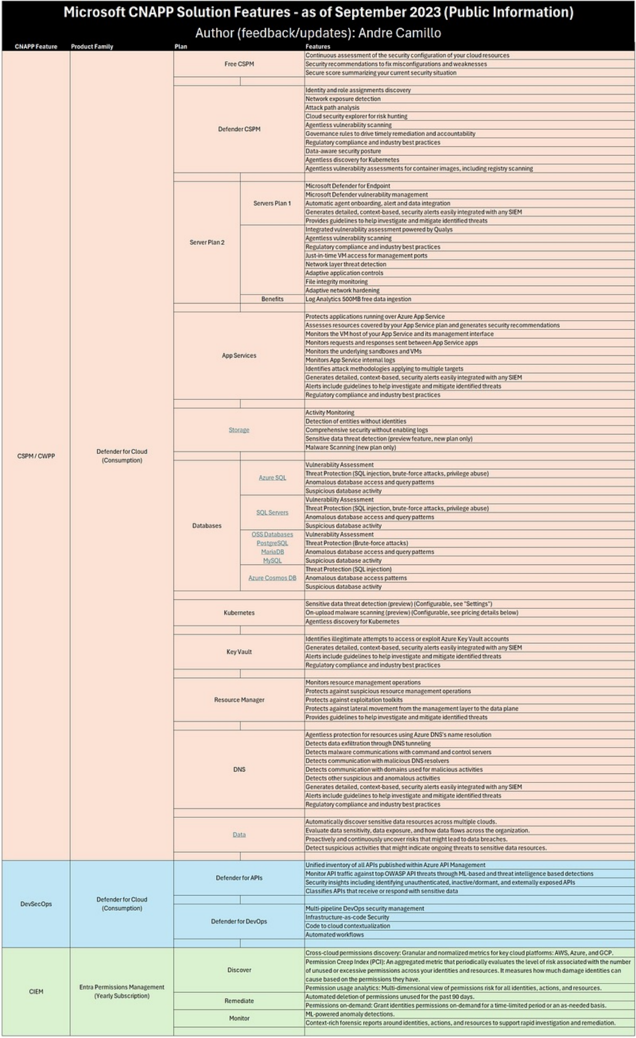
# A Comprehensive, Single vendor CNAPP solution and its Capabilities in 2023

I've spoken about Cloud-Native Application Protection Platform more than a year ago when Gartner announced their new "solution" term. Have a read at that here: The all in-one Cloud Security Solution CNAPP—according to Gartner | by Andre Camillo | Geek Culture | Medium

Since then, many vendors have worked and started delivering on this new "market". Only one of these vendors, however, can fill in the promise with almost 100% coverage of Gartner's definition.

Let's discuss how Microsoft delivers CNAPP in 2023.

Andre Camillo – Medium

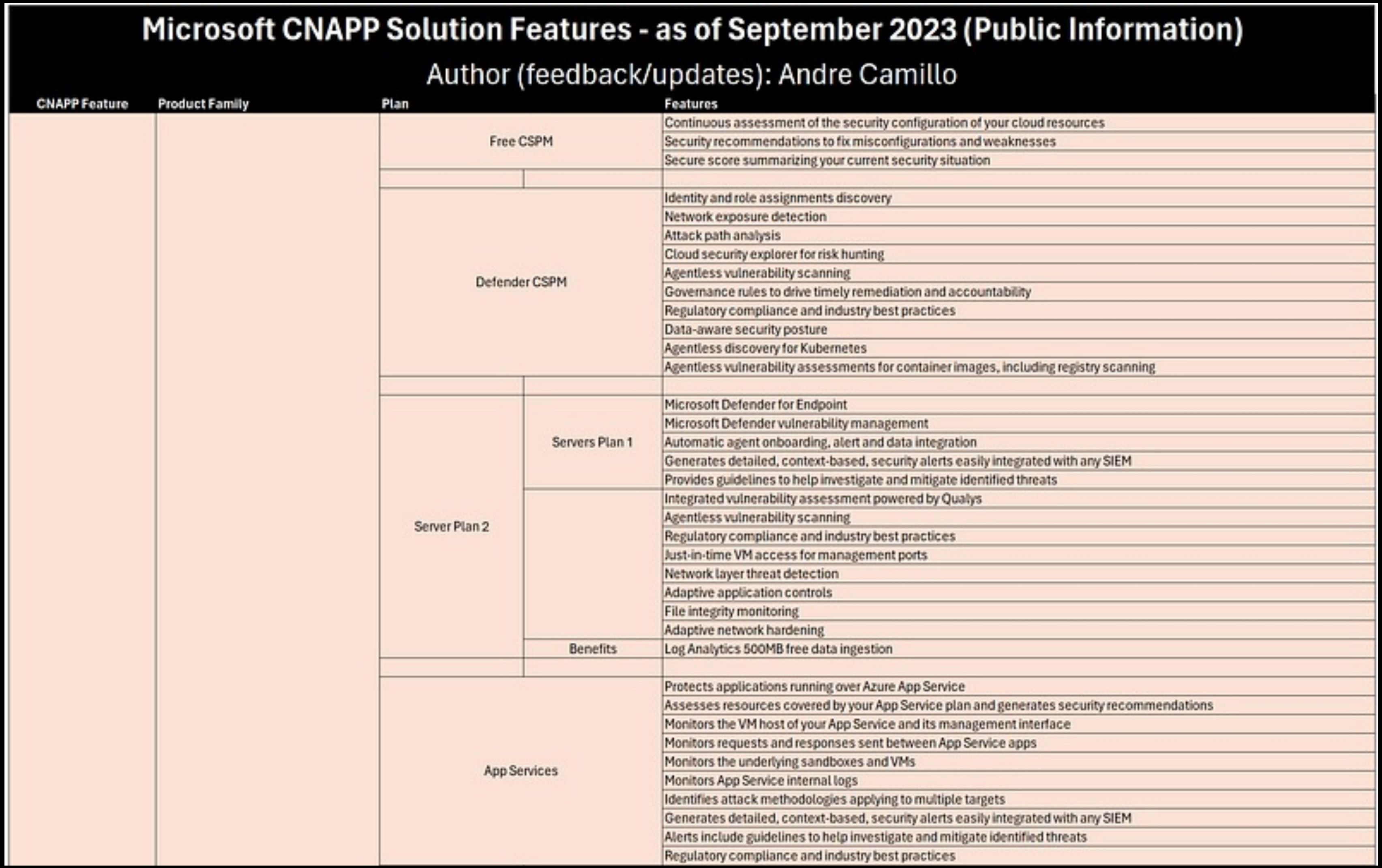


## Microsoft CNAPP Solution Features - as of September 2023 (Public Information)

Author (feedback/updates): Andre Camillo

| CNAPP Feature | Product Family | Plan | | Features |
|---|---|---|---|---|
| CSPM / CWPP | Defender for Cloud (Consumption) | Free CSPM | | Continuous assessment of the security configuration of your cloud resources |
| | | | | Security recommendations to fix misconfigurations and weaknesses |
| | | | | Secure score summarizing your current security situation |
| | | | | |
| | | Defender CSPM | | Identity and role assignments discovery |
| | | | | Network exposure detection |
| | | | | Attack path analysis |
| | | | | Cloud security explorer for risk hunting |
| | | | | Agentless vulnerability scanning |
| | | | | Governance rules to drive timely remediation and accountability |
| | | | | Regulatory compliance and industry best practices |
| | | | | Data-aware security posture |
| | | | | Agentless discovery for Kubernetes |
| | | | | Agentless vulnerability assessments for container images, including registry scanning |
| | | | | |
| | | Server Plan 2 | Servers Plan 1 | Microsoft Defender for Endpoint |
| | | | | Microsoft Defender vulnerability management |
| | | | | Automatic agent onboarding, alert and data integration |
| | | | | Generates detailed, context-based, security alerts easily integrated with any SIEM |
| | | | | Provides guidelines to help investigate and mitigate identified threats |
| | | | | Integrated vulnerability assessment powered by Qualys |
| | | | | Agentless vulnerability scanning |
| | | | | Regulatory compliance and industry best practices |
| | | | | Just-in-time VM access for management ports |
| | | | | Network layer threat detection |
| | | | | Adaptive application controls |
| | | | | File integrity monitoring |
| | | | | Adaptive network hardening |
| | | | Benefits | Log Analytics 500MB free data ingestion |
| | | | | |
| | | App Services | | Protects applications running over Azure App Service |
| | | | | Assesses resources covered by your App Service plan and generates security recommendations |
| | | | | Monitors the VM host of your App Service and its management interface |
| | | | | Monitors requests and responses sent between App Service apps |
| | | | | Monitors the underlying sandboxes and VMs |
| | | | | Monitors App Service internal logs |
| | | | | Identifies attack methodologies applying to multiple targets |
| | | | | Generates detailed, context-based, security alerts easily integrated with any SIEM |
| | | | | Alerts include guidelines to help investigate and mitigate identified threats |
| | | | | Regulatory compliance and industry best practices |
| | | | | |
| | | Storage | | Activity Monitoring |
| | | | | Detection of entities without identities |
| | | | | Comprehensive security without enabling logs |
| | | | | Sensitive data threat detection (preview feature, new plan only) |
| | | | | Malware Scanning (new plan only) |
| | | | | |
| | | Databases | Azure SQL | Vulnerability Assessment |
| | | | | Threat Protection (SQL injection, brute-force attacks, privilege abuse) |
| | | | | Anomalous database access and query patterns |
| | | | | Suspicious database activity |
| | | | SQL Servers | Vulnerability Assessment |
| | | | | Threat Protection (SQL injection, brute-force attacks, privilege abuse) |
| | | | | Anomalous database access and query patterns |
| | | | | Suspicious database activity |
| | | | OSS Databases<br>PostgreSQL<br>MariaDB<br>MySQL | Vulnerability Assessment |
| | | | | Threat Protection (Brute-force attacks) |
| | | | | Anomalous database access and query patterns |
| | | | | Suspicious database activity |
| | | | Azure Cosmos DB | Threat Protection (SQL injection) |
| | | | | Anomalous database access patterns |
| | | | | Suspicious database activity |
| | | | | |
| | | Kubernetes | | Sensitive data threat detection (preview) (Configurable, see "Settings") |
| | | | | On-upload malware scanning (preview) (Configurable, see pricing details below) |
| | | | | Agentless discovery for Kubernetes |
| | | | | |
| | | Key Vault | | Identifies illegitimate attempts to access or exploit Azure Key Vault accounts |
| | | | | Generates detailed, context-based, security alerts easily integrated with any SIEM |
| | | | | Alerts include guidelines to help investigate and mitigate identified threats |
| | | | | Regulatory compliance and industry best practices |
| | | | | |
| | | Resource Manager | | Monitors resource management operations |
| | | | | Protects against suspicious resource management operations |
| | | | | Protects against exploitation toolkits |
| | | | | Protects against lateral movement from the management layer to the data plane |
| | | | | Provides guidelines to help investigate and mitigate identified threats |
| | | | | |
| | | DNS | | Agentless protection for resources using Azure DNS's name resolution |
| | | | | Detects data exfiltration through DNS tunneling |
| | | | | Detects malware communications with command and control servers |
| | | | | Detects communication with malicious DNS resolvers |
| | | | | Detects communication with domains used for malicious activities |
| | | | | Detects other suspicious and anomalous activities |
| | | | | Generates detailed, context-based, security alerts easily integrated with any SIEM |
| | | | | Alerts include guidelines to help investigate and mitigate identified threats |
| | | | | Regulatory compliance and industry best practices |
| | | | | |
| | | Data | | Automatically discover sensitive data resources across multiple clouds. |
| | | | | Evaluate data sensitivity, data exposure, and how data flows across the organization. |
| | | | | Proactively and continuously uncover risks that might lead to data breaches. |
| | | | | Detect suspicious activities that might indicate ongoing threats to sensitive data resources. |
| | | | | |
| DevSecOps | Defender for Cloud (Consumption) | Defender for APIs | | Unified inventory of all APIs published within Azure API Management |
| | | | | Monitor API traffic against top OWASP API threats through ML-based and threat intelligence based detections |
| | | | | Security insights including identifying unauthenticated, inactive/dormant, and externally exposed APIs |
| | | | | Classifies APIs that receive or respond with sensitive data |
| | | | | |
| | | Defender for DevOps | | Multi-pipeline DevOps security management |
| | | | | Infrastructure-as-code Security |
| | | | | Code to cloud contextualization |
| | | | | Automated workflows |
| | | | | |
| CIEM | Entra Permissions Management (Yearly Subscription) | Discover | | Cross-cloud permissions discovery: Granular and normalized metrics for key cloud platforms: AWS, Azure, and GCP. |
| | | | | Permission Creep Index (PCI): An aggregated metric that periodically evaluates the level of risk associated with the number of unused or excessive permissions across your identities and resources. It measures how much damage identities can cause based on the permissions they have. |
| | | | | Permission usage analytics: Multi-dimensional view of permissions risk for all identities, actions, and resources. |
| | | Remediate | | Automated deletion of permissions unused for the past 90 days. |
| | | | | Permissions on-demand: Grant identities permissions on-demand for a time-limited period or an as-needed basis. |
| | | Monitor | | ML-powered anomaly detections. |
| | | | | Context-rich forensic reports around identities, actions, and resources to support rapid investigation and remediation. |
| | | | | |

Andre Camillo – Medium

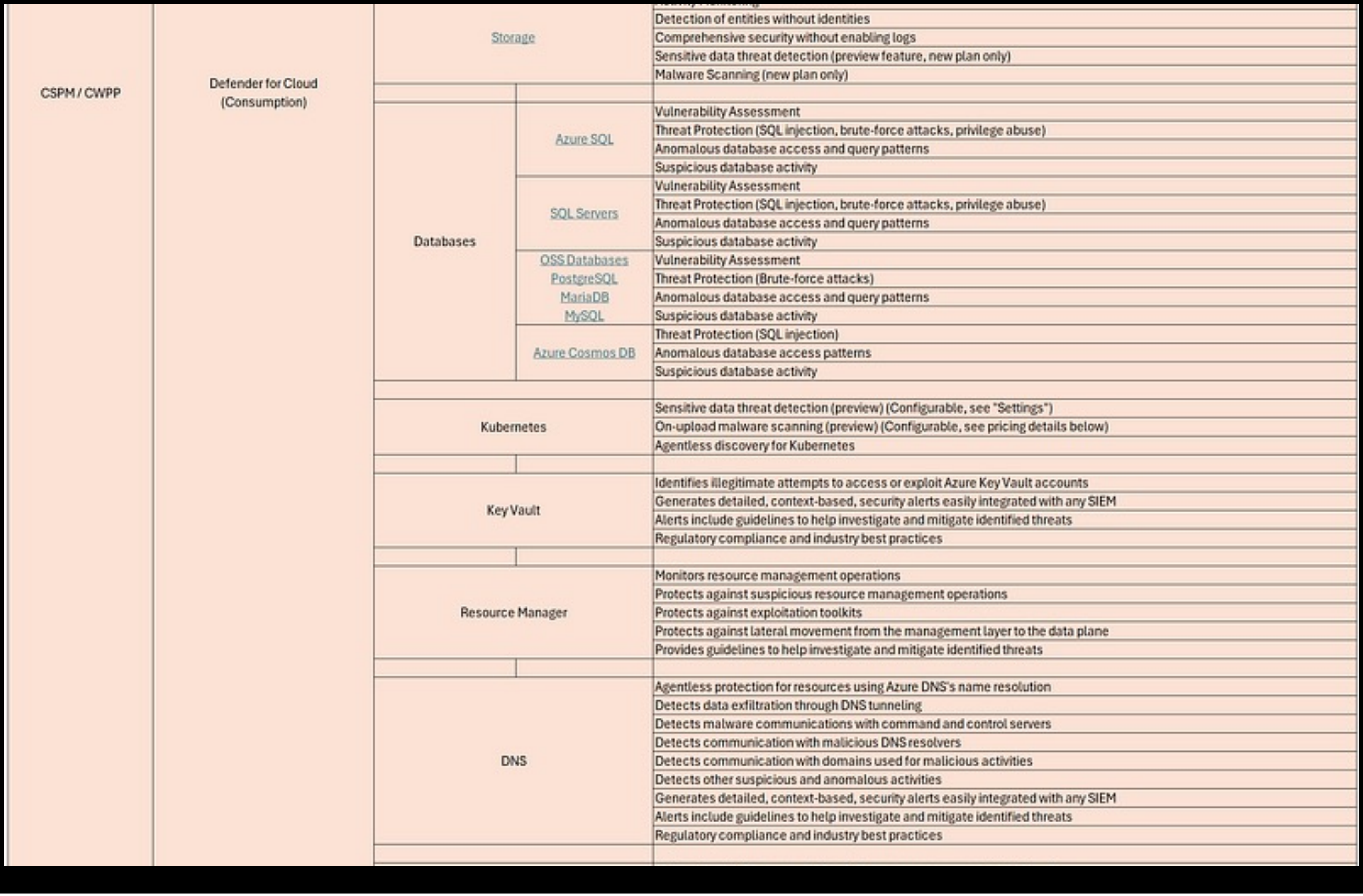


## Microsoft CNAPP Solution Features - as of September 2023 (Public Information)

Author (feedback/updates): Andre Camillo

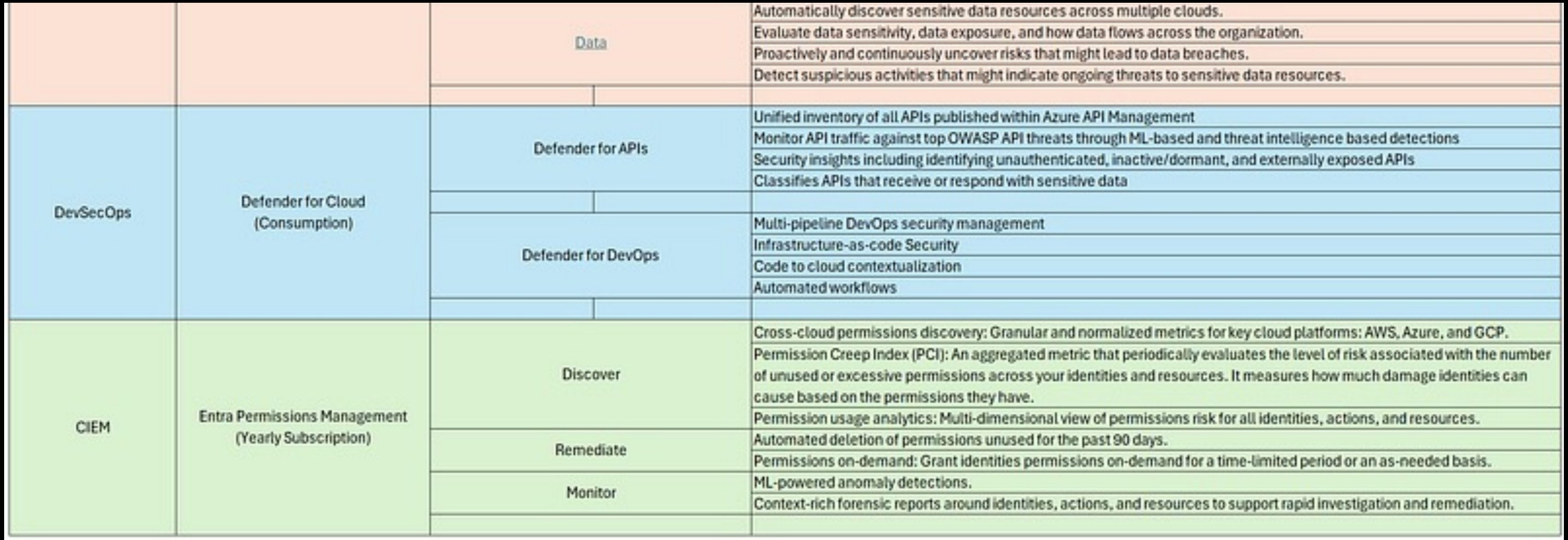
| CNAPP Feature | Product Family | Plan | | Features |
|---|---|---|---|---|
| | | Free CSPM | | Continuous assessment of the security configuration of your cloud resources |
| | | | | Security recommendations to fix misconfigurations and weaknesses |
| | | | | Secure score summarizing your current security situation |
| | | | | |
| | | Defender CSPM | | Identity and role assignments discovery |
| | | | | Network exposure detection |
| | | | | Attack path analysis |
| | | | | Cloud security explorer for risk hunting |
| | | | | Agentless vulnerability scanning |
| | | | | Governance rules to drive timely remediation and accountability |
| | | | | Regulatory compliance and industry best practices |
| | | | | Data-aware security posture |
| | | | | Agentless discovery for Kubernetes |
| | | | | Agentless vulnerability assessments for container images, including registry scanning |
| | | | | |
| | | Server Plan 2 | Servers Plan 1 | Microsoft Defender for Endpoint |
| | | | | Microsoft Defender vulnerability management |
| | | | | Automatic agent onboarding, alert and data integration |
| | | | | Generates detailed, context-based, security alerts easily integrated with any SIEM |
| | | | | Provides guidelines to help investigate and mitigate identified threats |
| | | | | Integrated vulnerability assessment powered by Qualys |
| | | | | Agentless vulnerability scanning |
| | | | | Regulatory compliance and industry best practices |
| | | | | Just-in-time VM access for management ports |
| | | | | Network layer threat detection |
| | | | | Adaptive application controls |
| | | | | File integrity monitoring |
| | | | | Adaptive network hardening |
| | | | Benefits | Log Analytics 500MB free data ingestion |
| | | | | |
| | | App Services | | Protects applications running over Azure App Service |
| | | | | Assesses resources covered by your App Service plan and generates security recommendations |
| | | | | Monitors the VM host of your App Service and its management interface |
| | | | | Monitors requests and responses sent between App Service apps |
| | | | | Monitors the underlying sandboxes and VMs |
| | | | | Monitors App Service internal logs |
| | | | | Identifies attack methodologies applying to multiple targets |
| | | | | Generates detailed, context-based, security alerts easily integrated with any SIEM |
| | | | | Alerts include guidelines to help investigate and mitigate identified threats |
| | | | | Regulatory compliance and industry best practices |

Andre Camillo – Medium



| | | | | |
|---|---|---|---|---|
| CSPM / CWPP | Defender for Cloud (Consumption) | Storage | | Detection of entities without identities |
| | | | | Comprehensive security without enabling logs |
| | | | | Sensitive data threat detection (preview feature, new plan only) |
| | | | | Malware Scanning (new plan only) |
| | | | | |
| | | Databases | Azure SQL | Vulnerability Assessment |
| | | | | Threat Protection (SQL injection, brute-force attacks, privilege abuse) |
| | | | | Anomalous database access and query patterns |
| | | | | Suspicious database activity |
| | | | SQL Servers | Vulnerability Assessment |
| | | | | Threat Protection (SQL injection, brute-force attacks, privilege abuse) |
| | | | | Anomalous database access and query patterns |
| | | | | Suspicious database activity |
| | | | OSS Databases<br>PostgreSQL<br>MariaDB<br>MySQL | Vulnerability Assessment |
| | | | | Threat Protection (Brute-force attacks) |
| | | | | Anomalous database access and query patterns |
| | | | | Suspicious database activity |
| | | | Azure Cosmos DB | Threat Protection (SQL injection) |
| | | | | Anomalous database access patterns |
| | | | | Suspicious database activity |
| | | | | |
| | | Kubernetes | | Sensitive data threat detection (preview) (Configurable, see "Settings") |
| | | | | On-upload malware scanning (preview) (Configurable, see pricing details below) |
| | | | | Agentless discovery for Kubernetes |
| | | | | |
| | | Key Vault | | Identifies illegitimate attempts to access or exploit Azure Key Vault accounts |
| | | | | Generates detailed, context-based, security alerts easily integrated with any SIEM |
| | | | | Alerts include guidelines to help investigate and mitigate identified threats |
| | | | | Regulatory compliance and industry best practices |
| | | | | |
| | | Resource Manager | | Monitors resource management operations |
| | | | | Protects against suspicious resource management operations |
| | | | | Protects against exploitation toolkits |
| | | | | Protects against lateral movement from the management layer to the data plane |
| | | | | Provides guidelines to help investigate and mitigate identified threats |
| | | | | |
| | | DNS | | Agentless protection for resources using Azure DNS's name resolution |
| | | | | Detects data exfiltration through DNS tunneling |
| | | | | Detects malware communications with command and control servers |
| | | | | Detects communication with malicious DNS resolvers |
| | | | | Detects communication with domains used for malicious activities |
| | | | | Detects other suspicious and anomalous activities |
| | | | | Generates detailed, context-based, security alerts easily integrated with any SIEM |
| | | | | Alerts include guidelines to help investigate and mitigate identified threats |
| | | | | Regulatory compliance and industry best practices |
| | | | | |

Andre Camillo – Medium



| | | | |
|---|---|---|---|
| | | Data | Automatically discover sensitive data resources across multiple clouds. |
| | | | Evaluate data sensitivity, data exposure, and how data flows across the organization. |
| | | | Proactively and continuously uncover risks that might lead to data breaches. |
| | | | Detect suspicious activities that might indicate ongoing threats to sensitive data resources. |
| | | | |
| DevSecOps | Defender for Cloud (Consumption) | Defender for APIs | Unified inventory of all APIs published within Azure API Management |
| | | | Monitor API traffic against top OWASP API threats through ML-based and threat intelligence based detections |
| | | | Security insights including identifying unauthenticated, inactive/dormant, and externally exposed APIs |
| | | | Classifies APIs that receive or respond with sensitive data |
| | | | |
| | | Defender for DevOps | Multi-pipeline DevOps security management |
| | | | Infrastructure-as-code Security |
| | | | Code to cloud contextualization |
| | | | Automated workflows |
| | | | |
| CIEM | Entra Permissions Management (Yearly Subscription) | Discover | Cross-cloud permissions discovery: Granular and normalized metrics for key cloud platforms: AWS, Azure, and GCP. |
| | | | Permission Creep Index (PCI): An aggregated metric that periodically evaluates the level of risk associated with the number of unused or excessive permissions across your identities and resources. It measures how much damage identities can cause based on the permissions they have. |
| | | | Permission usage analytics: Multi-dimensional view of permissions risk for all identities, actions, and resources. |
| | | Remediate | Automated deletion of permissions unused for the past 90 days. |
| | | | Permissions on-demand: Grant identities permissions on-demand for a time-limited period or an as-needed basis. |
| | | Monitor | ML-powered anomaly detections. |
| | | | Context-rich forensic reports around identities, actions, and resources to support rapid investigation and remediation. |
| | | | |

Andre Camillo – Medium