CHEQUER Common Evaluation Chart - CNAPP

Numbering	Category	Item	Subitem	Evaluation Details	Importance	Score
1-1		Artifact Scanning	Software Composition Analysis (SCA)	Supports open source library scan	High	
1-2				Supports scanning sub-libraries within libraries in SBOM	Mid	
1-3			Shift Left Security	Supports SAST(Static Application Security Testing)	Low	
1-4				Supports DAST(Dynamic Application Security Testing)	Low	
1-5				Supports automated scans (via API)	Low	
1-6				Supports scanning code vulnerabilities (CVE, CWE from Github, Gitlab)	Mid	
1-7				Supports secret scan	Mid	
1-8				Supports scanning without processing GitHub Action workflows	Low	
1-9				Supports scanning for Infrastructure as Code (IaC)	Mid	
1-10				Supports scanning registries and their images	Mid	
1-11				Supports IDE plugins (such as VS Code, IntelliJ, Eclipse, GoLand, PyCharm)	Mid	
2-1		Cloud Connections	Multi-Cloud Support	Supports various cloud service providers - AWS, GCP, Azure, etc.	High	
2-2				Supports private/on-prem clouds	Low	
2-3				Supports multi-cloud integrations and asset identifications - VM, Container - IaaS, PaaS, SaaS	High	
2-4				Supports comprenhensive monitoring and risk correlative analysis - cross account & cross cloud lateral movement risks	High	
3-1		CWPP (Cloud Workload Protection Platform)	Workload Protection	Supports detecting vulnerabilities and risks even on turned-off workloads	High	
3-2				Supports agentless scanning	High	
3-3				Includes Kubernetes in scopes	Mid	
3-4				Supports manually triggering CVE scan	Mid	
3-5				Supports CVE scans for OS and Runtimes	High	
3-6				Supports vulnerability/risk prioritization based on their contexts	High	
3-7			Cloud Detection & Response	Supports scanning vulnerabilities on workloads (which includes EC2, S3, EKS, ECR, RDS) along with real-time malware scanning capability	High	
3-8				Supports reputation intelligence linking - VirusTotal, CISCO Talos, X-Force, Sophos, etc.	Mid	

CHEQUER Common Evaluation Chart - CNAPP

Numbering	Category	Item	Subitem	Evaluation Details	Importance	Score
3-9	Features			Supports container forensics through snapshots and monitoring (incident analysis)	Mid	
4-1		CSPM (Cloud Security Posture Management)	Compliance Frameworks	Supports security compliance management by mapping cloud configuration status to security frameworks and controls - ISO 27001/27017/27701, SOC2, GDPR, PCI-DSS, etc.	High	
4-2				Supports CIS Benchmarks based frameworks extended to OS, Softwares - Host OS (Amazon Linux / Ubuntu, etc.) - Software (Docker, Nginx, Apache, etc.)	High	
4-3				Provides local compliance frameworks such as ISMS-P standards	Mid	
4-4			Custom Frameworks	Supports creating custom frameworks from scratch	Mid	
4-5				Supports adding user-defined security controls and/or editing controls from existing frameworks after duplication	Mid	
5-1		CIEM (Cloud Infrastructure Entitlement Management)	Identity and Access Management	Supports discovering overall cloud IAM asset and their risks - Users and groups - Roles and policies - Access keys	High	
5-2				Supports policy optimization for which are assigned with excessive administrative rights	High	
6-1		DSPM (Data Security Posture Management)	Sensitive Data	Supports detecting PII(Personal Identifiable Information) and its exposure	High	
6-2				Must define its residency for sensitive data and must be storing PIIs with risks in masked versions (not the original)	High	
6-3				Supports detecting other sensitive data such as keys/tokens/secrets	High	
7-1		API Security	API & API Risk Discovery	Supports unmanaged(Shadow/Zombie) API discovery	High	
7-2				Supports identifying API misconfigurations, vulnerabilities and risks	High	
7-3				Supports identifying PII exposure from API endpoints	High	
7-4				Supports OWASP top 10 & OWASP API top 10	High	
8-1		Additional Features	Remediations	Provides appropriate and specific remediation guides for each vulnerability and asset	High	
8-2				Supports auto remediation	Mid	
8-3			Tagging	Supports collecting tags from all cloud assets	High	
8-4				Supports dynamic tagging for identified risks from analysis	High	
8-5				Supports custom tagging applicable to assets from multiple clouds	Mid	

CHEQUER Common Evaluation Chart - CNAPP

Numbering	Category	Item	Subitem	Evaluation Details	Importance	Score
9-1	Services	Security Configuration	3rd Party IdP Integration	Supports SAML/OIDC protocol for integration with Okta	High	
9-2				Supports SCIM protocol for user lifecyle provisioning	High	
9-3			Authorization Management	Supports RBAC(Role-Based Access Control) / GBAC(Group-Based Access Control)	High	
9-4			Multi-Factor Authentication (MFA)	Supports MFA for local accounts	High	
9-5			Network ACL Support	Supports Network ACL(NACL) via setting whitelists/trusted IPs	High	
			BYOK	Supports BYOK to promote strong control over sensitive data and applications		
9-6			Logging	Supports audit logging	High	
9-7				Supports recording sytem logs	High	
10-1		Convenience	Deployment	Supports cloud account integration with agentless method	High	
10-2				Supports deployment without any impact on existing cloud assets	High	
10-3			UI/UX	Supports visibility with comprehensive dashboards	High	
10-4				Supports asset inventory and risk management and makes them easier via integration with OpenAI or else	Mid	
10-5				Supports creating and saving custom filters for asset, vulnerability and risk views	Mid	
10-6				Supports customizing risk levels	Mid	
10-7				Supports listing applications, installed packages, running services on each asset	Mid	
10-8				Provides easy-to-comprehend guides	Mid	
10-9			Integration Modules	Supports integration with Compliance and Risk Managment platform such as Vanta	Mid	
10-10				Supports integration with communication tools such as Jira, Slack, etc.	High	
10-11				Supports SIEM integration such as Splunk, Datadog, etc.	High	
10-12				Supports various 3rd-party integration natively from the solution	Low	
10-13			Tenant Separation	Supports separation by projects or tenants	High	
10-14			Reports	Supports reports in email/pdf format and their scheduling	High	
10-15			Customer Support	Provides CS channels to easily open cases when issues occur	Mid	
10-16				Provides Customer Success channel which helps following up with feature enhancement requests, etc.	Mid	
10-17			Rest API / CLI / SDK / SDK	Provides various external APIs which users can utilize for log collection, orchestration and for other security purposes	High	

CHEQUER Common Evaluation Chart - CNAPP

Numbering	Category	Item	Subitem	Evaluation Details	Importance	Score
10-18			Rest API / CLI / CDK / SDK	Supports authorization management on APIs	Mid	
10-19				Supports CLI	Mid	
10-20			Localization	Supports Korean language for its UI, guides	Low	