

Security in GCP

Memilavi
www.memilavi.com



Security

- Security is one of the most important parts of every system
- GCP offers a lot of security measures for its resources
- It's extremely important to use those measures and follow security patterns to avoid security incidents
- We've covered most of them, here we'll summarize and emphasize some new techniques

VM Security Best Practices

- Restrict access to the VM as much as possible
- Make sure only the required ports are open to the internet
(22/1389/443/80)
- Limit access to specific IP addresses when possible
- If the VM is public facing place it behind a load balancer and make sure no public access is allowed

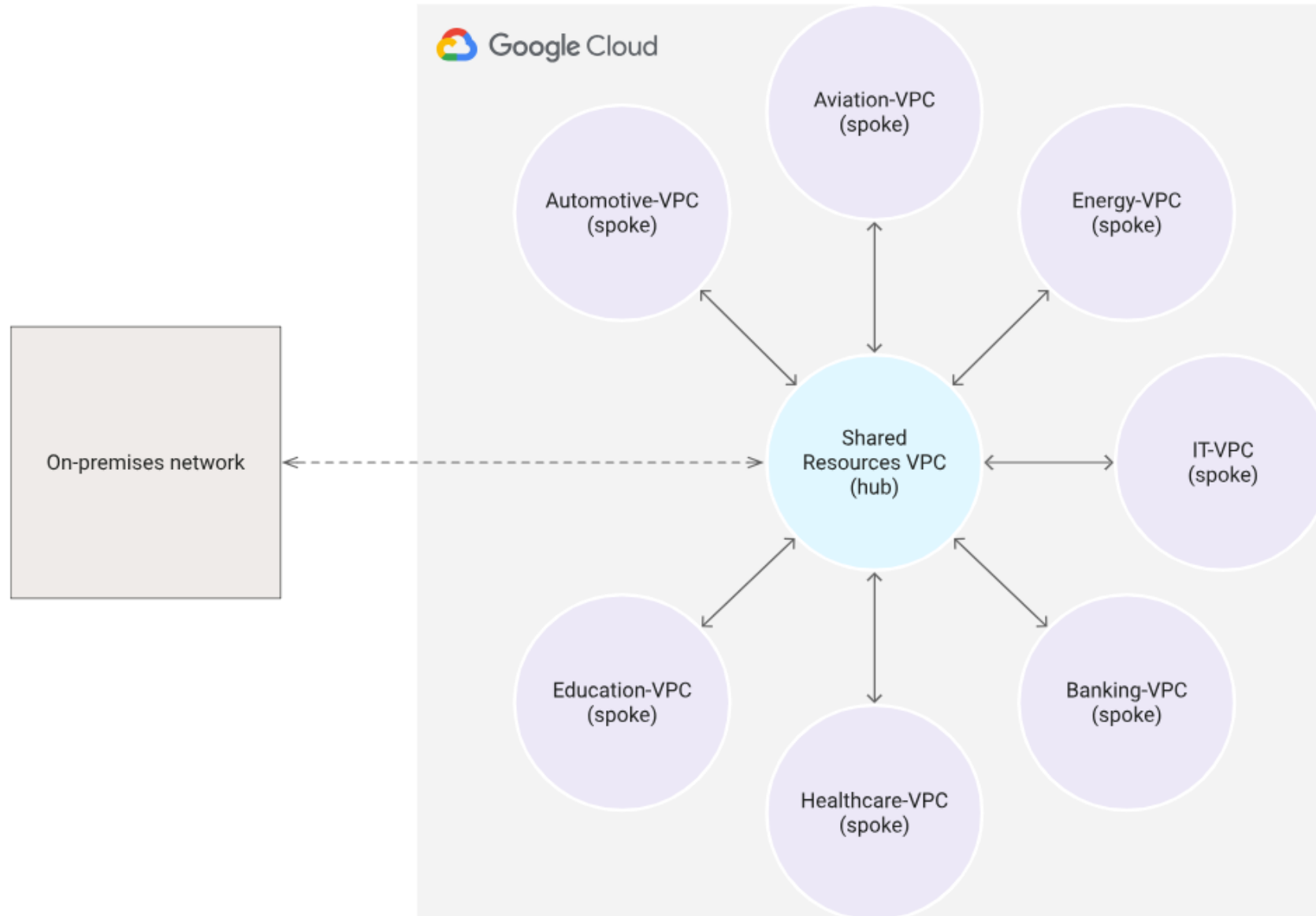
VM Security Best Practices

- Ensure operating system is fully patched and updated
- Keep backups as needed

Networking Security Best Practices

- VPC that contains private resources only – should not be exposed to the internet
- ALWAYS use Firewall Rules to restrict access to subnets
- Use Private Access to restrict access to resources
- Use the Hub-and-Spoke security model

Hub and Spoke



Database Security Best Practices

- Use encryption at rest and encryption at transit (usually On by default)
- Connect DB to relevant VPC using Private Access
- Use Firewall Rules to restrict external access

App Engine Security Best Practices

- Don't expose directly to the internet, use Load Balancer
- Make it accessible only using private IP
- Use access management engine such as Identity Platform to authenticate access

Secret Manager

- Many apps have secrets that need to be kept safely
 - Connection Strings
 - Keys
 - Certificates
 - API Keys
 - And more...

Secret Manager

- Usually kept in configuration files, configuration DB etc.
- Not really secure...
- Secret Manager solves this problem

Secret Manager

- Safely stores secrets of various types
- Restricted access – only authorized principals can access secrets
- Easily manageable
- Accessed via REST API
- Cost effective
- SLA: 99.95%



Secret Manager

- In addition to it there are also:
 - Key Management for creating, storing and managing keys
 - Certificate Manager for storing and managing certificates

Secret Manager pricing

- Based on:
 - Active secrets
 - Access operations

Secret Manager pricing

Secret Manager		
Netherlands		
Active secret versions per replica location: 100		
Access operations: 100000		
USD 5.91		

Cloud Armor

- Adds DDoS protection and WAF capabilities to your web app
- Protects against layer 7 attacks
- Mitigates OWASP top 10 risks
- Bot protection
- Allows rate limit
- Customizable

Cloud Armor

- Rich monitoring and logging
- Preview mode to understand rules effect
- IP-based and geo-based access control
- Support for hybrid and multicloud deployments
- SLA: 99.99%

Cloud Armor Editions

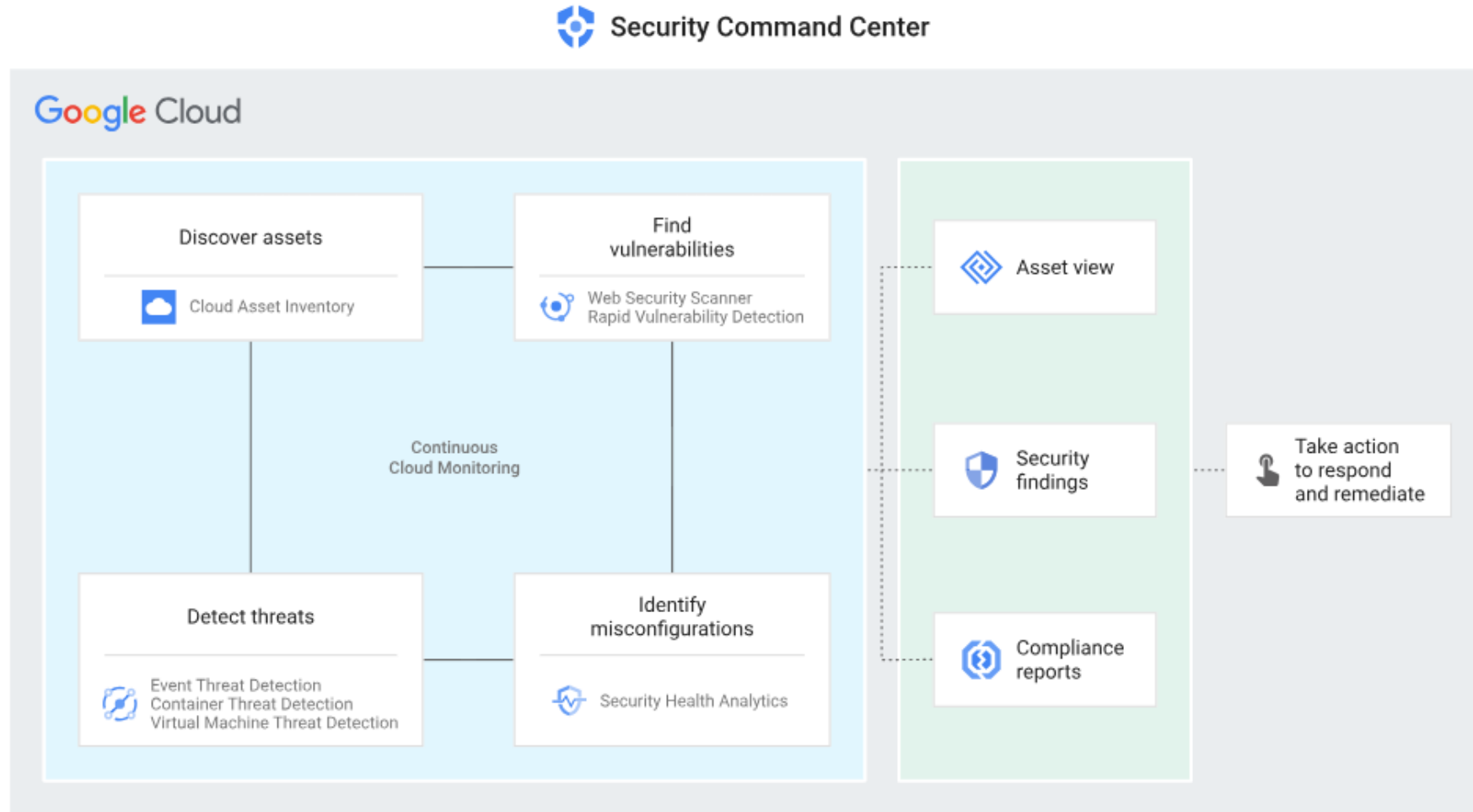
- Two editions, differ in pricing model

	Standard	Managed Protection Plus
Billing	Pay as you go	Starting at \$3,000/month
Protected resources	None	Includes first 100, additional for \$30/month
Rules	\$1/month	Included
Policy	\$5/month	Included
Requests	\$0.75/million queries	Included

Security Command Center

- Central tool for monitoring and managing security posture of the cloud environment
- Identifies misconfiguration and vulnerabilities
- Offers remediation
- Detects threats
- Monitor compliance

Security Command Center



Security Command Center

- Requires organization
- We won't work with it

Architecture: ReadIt Cloud System

