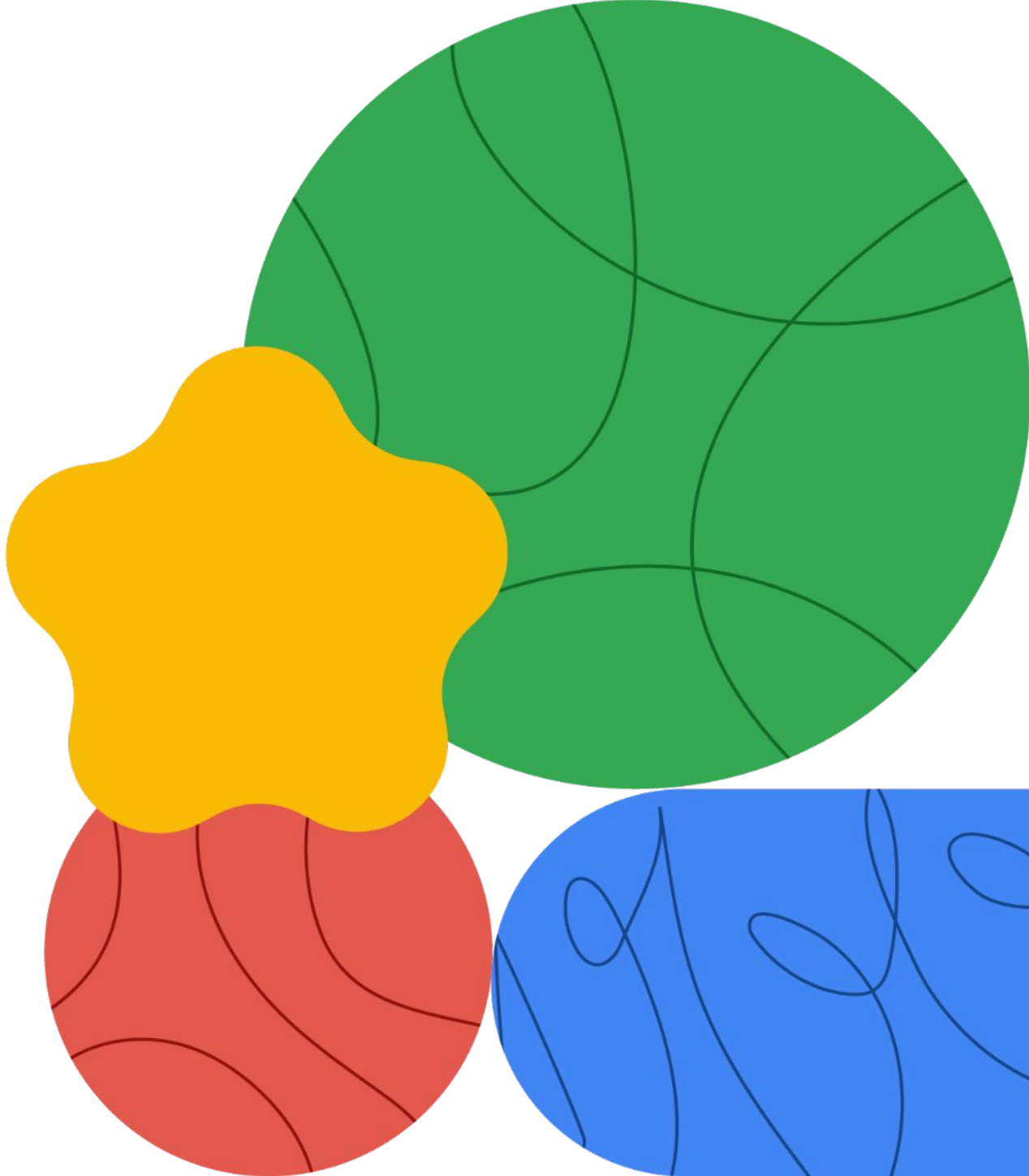
Google Cloud

Networking in Google Cloud

Distributed Denial of Service Attacks (DDoS) Protection



Today's agenda

01 How DDoS attacks work

02 Google Cloud mitigations

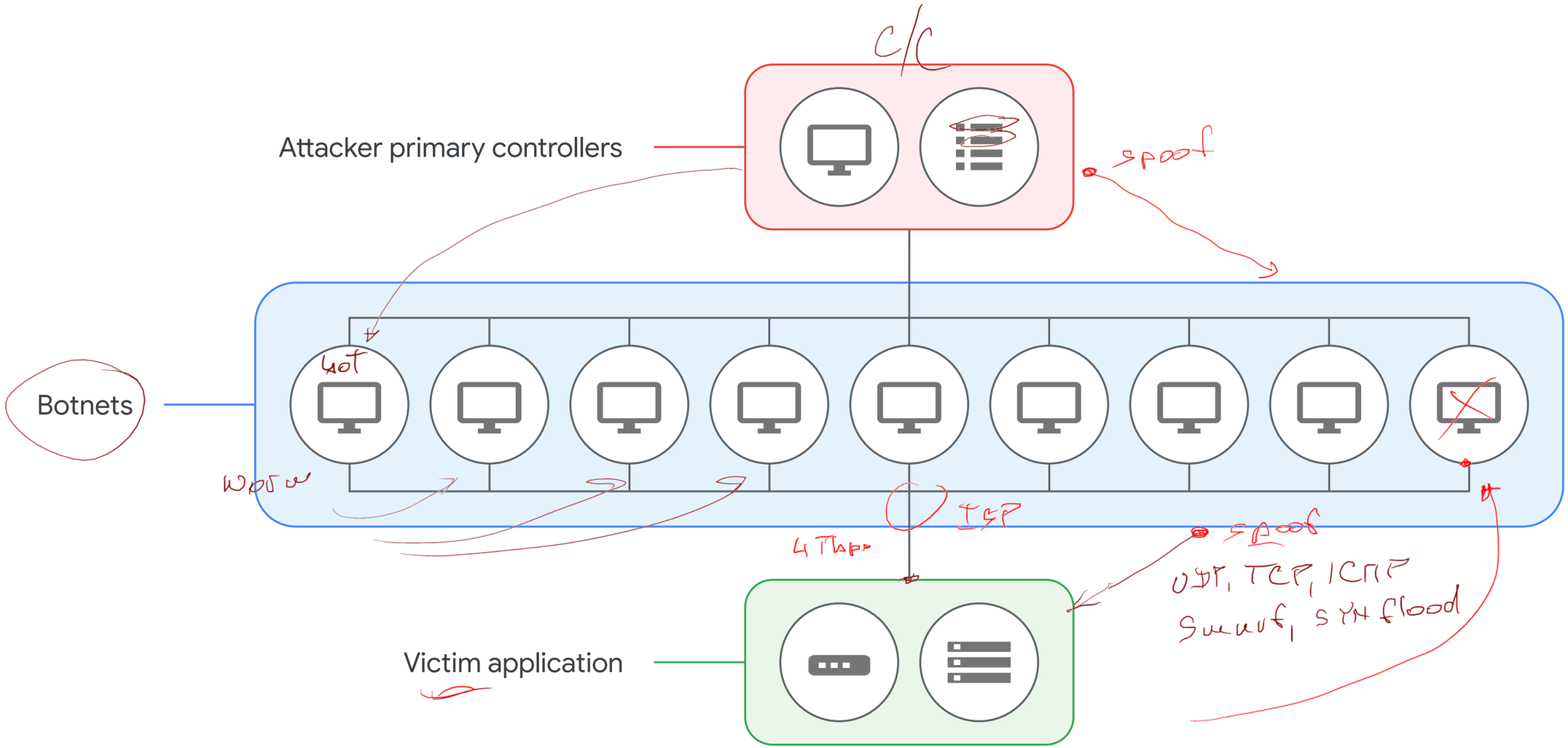
03 Types of complementary partner products

04 Lab: Configuring Traffic Blocklisting with Google Cloud Armor

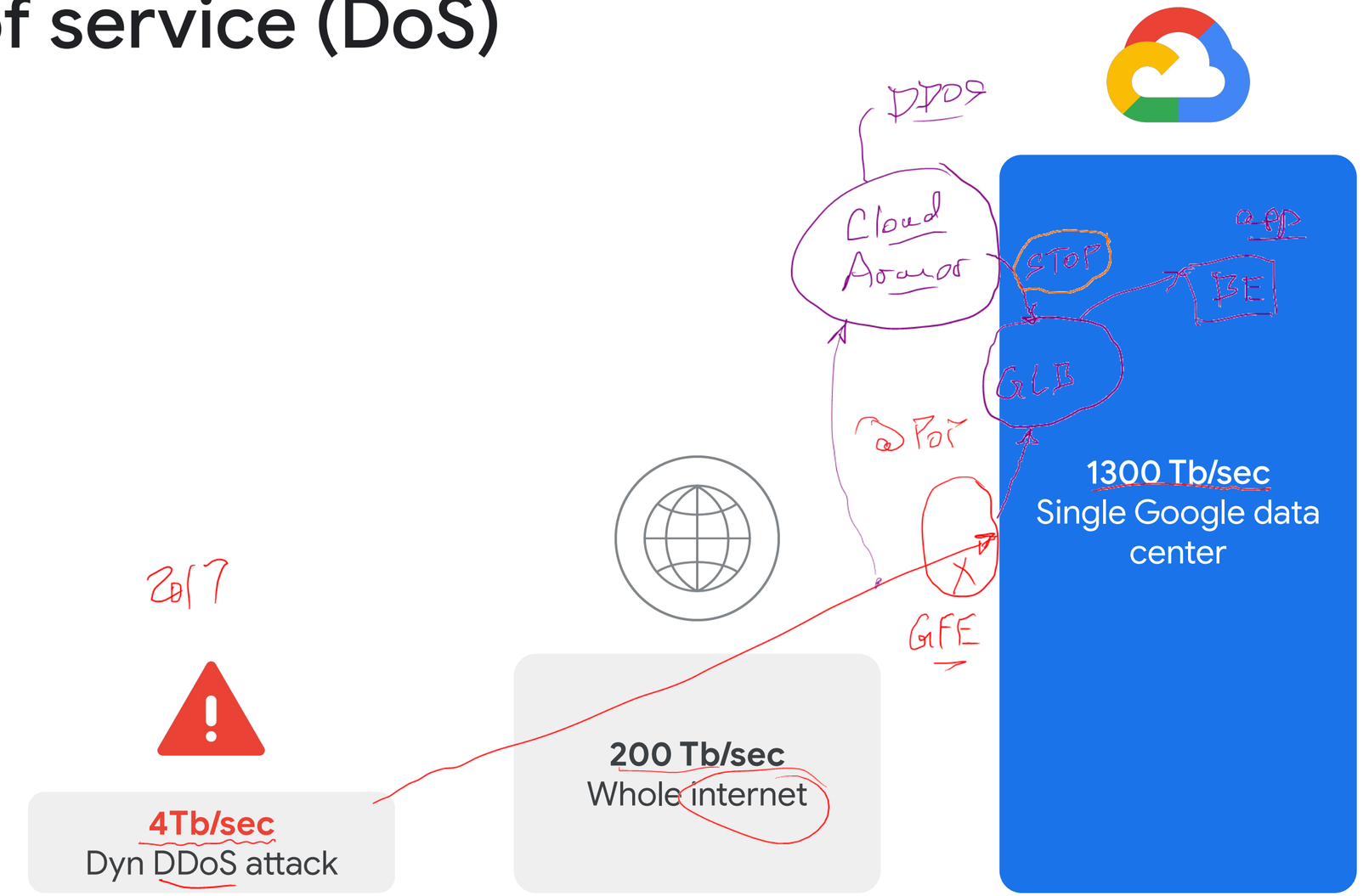
05 Quiz

Distributed denial-of-service (DDoS) attacks attempt to make your online application unavailable by overwhelming it with traffic from multiple sources.

DDoS attacks

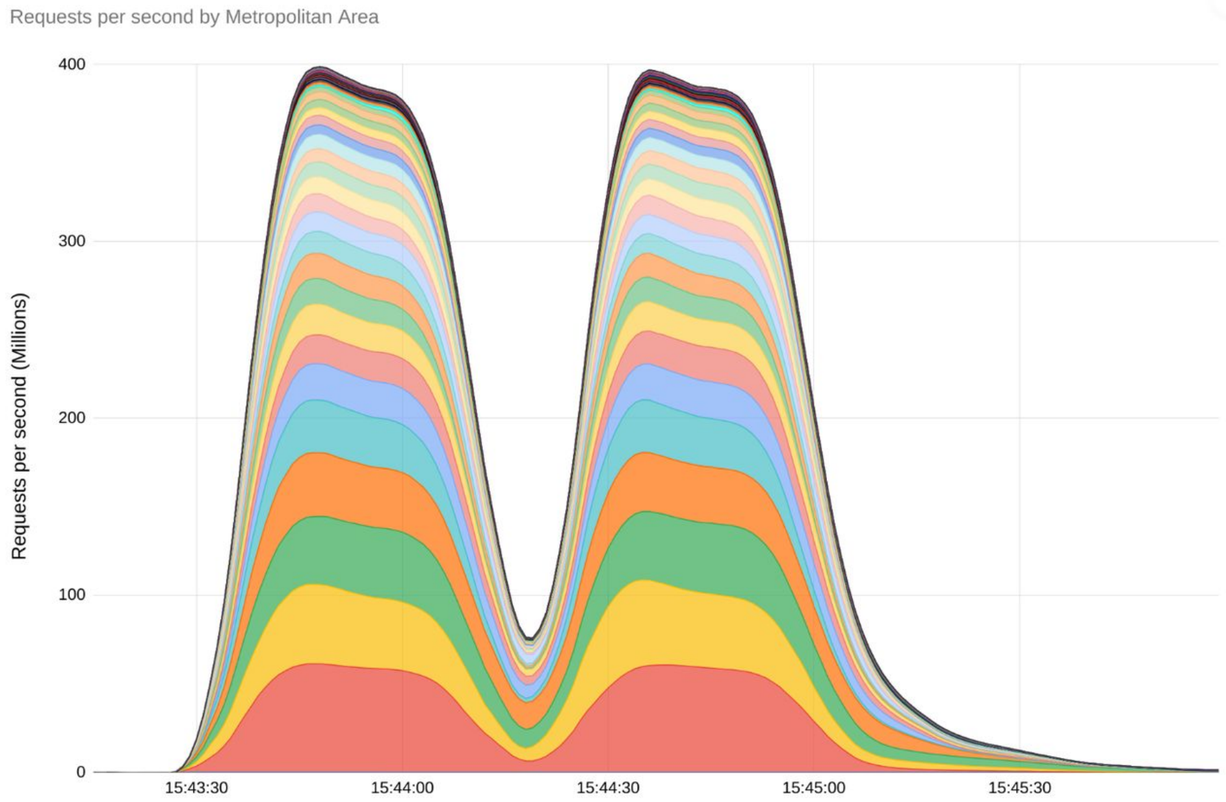


Denial of service (DoS)



DDoS attacks are growing in frequency and size

- Aug 2022: Google blocks a record breaking 46M requests-per-second (rps) attack.
- Aug 2023: we stopped an even larger DDoS attack—7½ times larger— of 398M rps.



Today's agenda

01 How DDoS attacks work

02 Google Cloud mitigations

03 Types of complementary partner products

04 Lab: Configuring Traffic Blocklisting with Google Cloud Armor

05 Quiz

DDoS attacks are increasing

- Kai is looking to handle the increasing sophistication of modern attacks.
- Kai needs a scalable, cloud-based solution that is cost effective and does not require contracts or long-term agreements.
- Kai needs a solution that can effectively defend their website without impacting performance.

Successful DDoS mitigation strategies have many layers

Defence in Depth

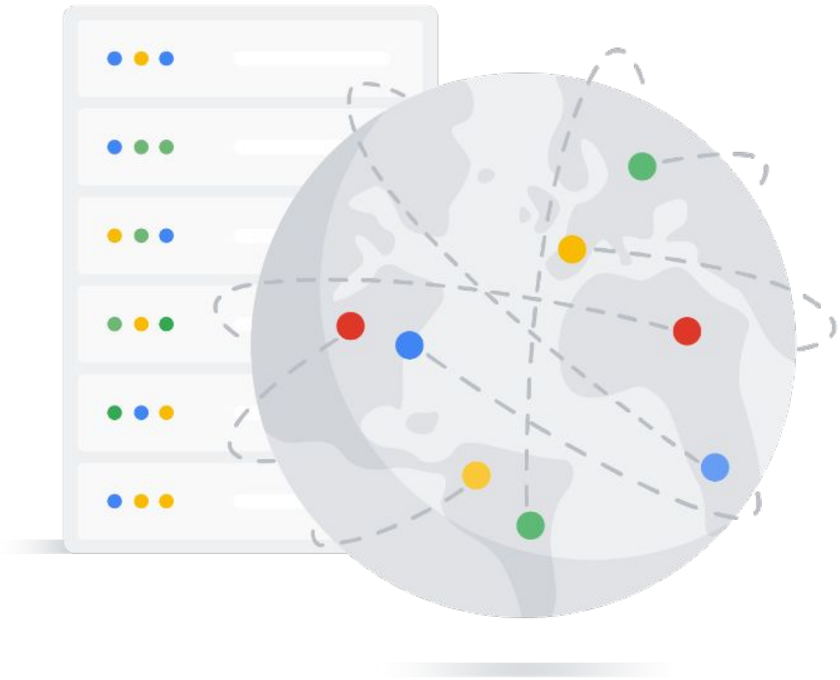
Load balancing	Using proxy-based load balancing to distribute load across resources.
Attack surface	Reducing the attack surface by reducing externally facing resources.
Internal traffic	Isolating internal traffic from the outside world by restricting access.
API management	Monitoring and managing APIs to spot and throttle DDoS attacks.
CDN offloading	Offloading static content to a CDN to minimize impact.
Specialized DDoS protection	Deploying applications that specifically provide deeper DDoS protection.

Leveraging Cloud Load Balancing

Cloud Load Balancing provides built-in defense against infrastructure DDoS attacks.

- No additional configuration is required to activate this DDoS defense.

- It leverages Google's central DDoS mitigation service.
  - If the system detects an attack, it can configure load balancers to drop or throttle traffic.



Reducing the attack surface

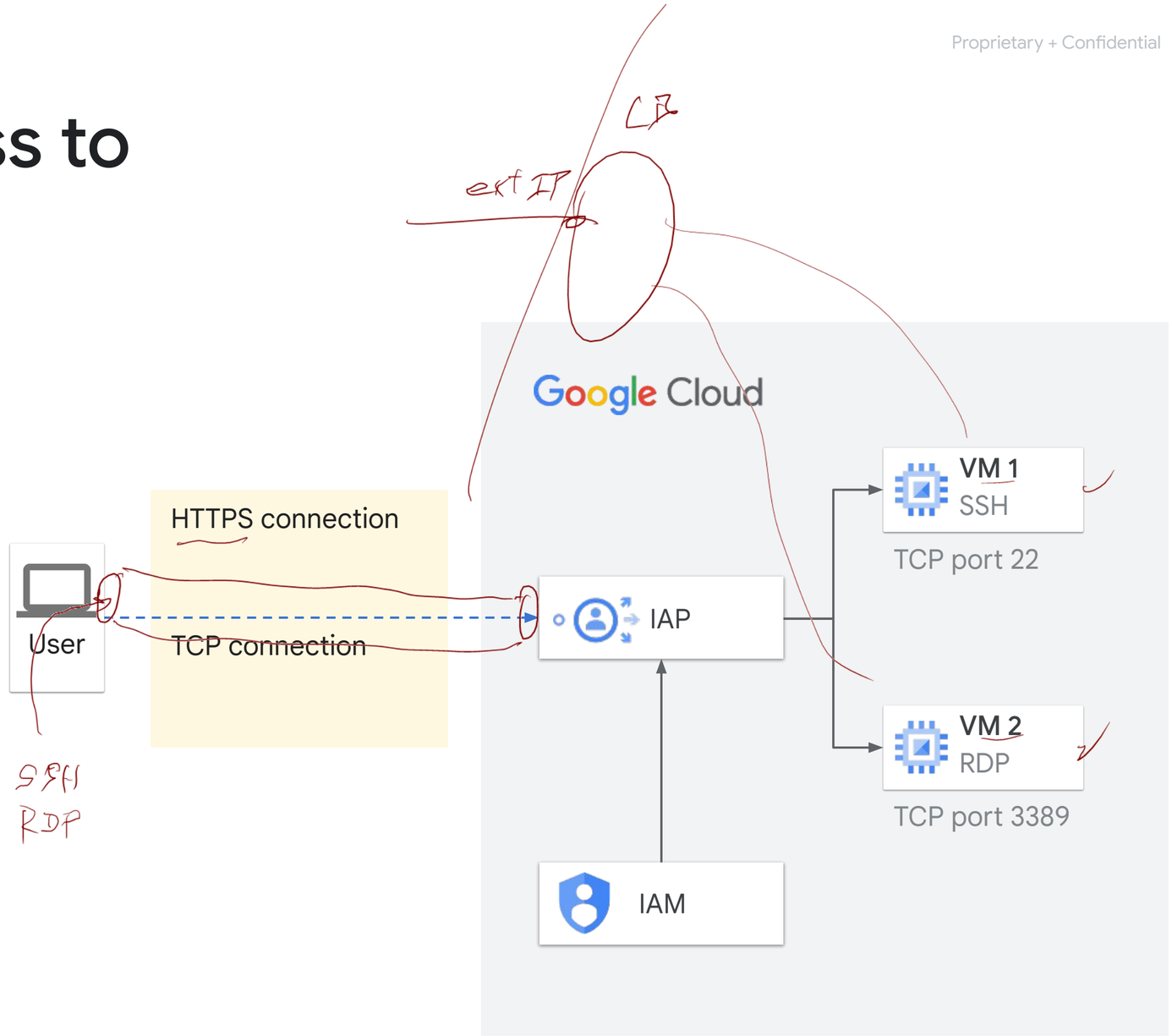
Attack surface:

Total data entry or extraction points that an unauthorized user could use in an environment..

- Isolate machines within VPCs.
- Set up firewall rules to block unused ports.
- Use firewall rules to block unwanted sources.
- Use firewall tags and service accounts to control targets.

Restricting public access to internal traffic

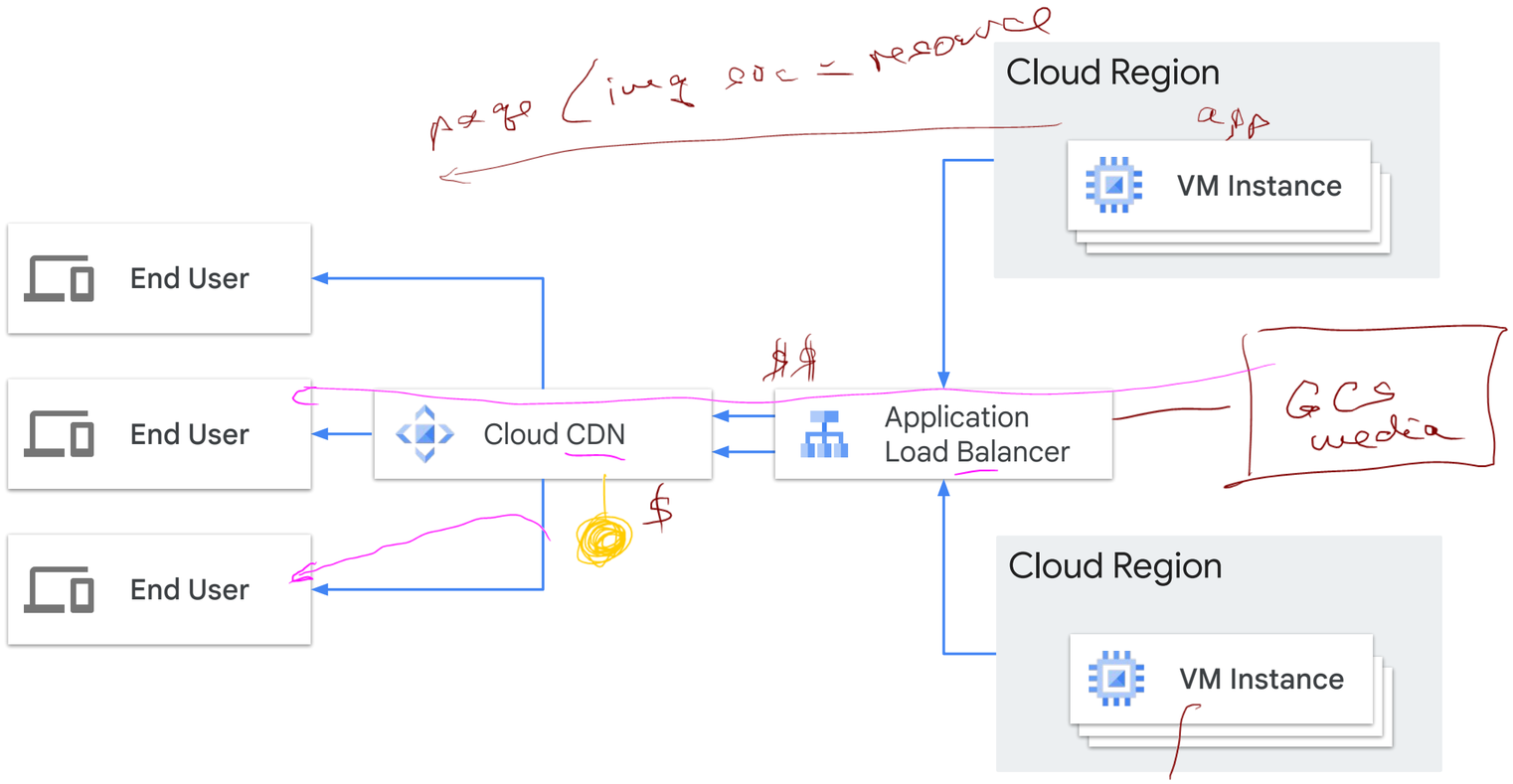
- Don't give machines public IPs unnecessarily.
- Use Identity-Aware Proxy or bastion hosts to limit machines exposed to the internet.
- Use internal load balancers for internal services.



Using Cloud CDN

Caches content between your users and your servers.

- Requests for cached content are routed to POPs.
- Google's massive infrastructure can absorb attacks.



API management and monitoring

- Create an API gateway to manage your backend services.
  - Throttle requests to limit requests from clients.
  - Control access to APIs from a single location.
  - Monitor API usage.
- You can use Apigee to create API gateways.

Extensible Service Proxy (ESP) is based on NGINX
Envoy proxy

Google Cloud Armor

Mitigate infrastructure DDoS attacks with the global external Application Load Balancer.

Allow and block traffic, and rate limit based on IP, Geo, and custom match parameters (L3-L7 etc).

Defend against application layer attacks with **OWASP Top 10.**

Telemetry: Decisions logged to Cloud Logging and Monitoring dashboard, and Cloud Security Command Center.

Configure policy

Name *
cloud-armor-policy
Lowercase letters, numbers, hyphens allowed

Description

Policy type

- (•) Backend security policy
- ( ) Edge security policy
- ( ) Network edge security policy

Scope

- (•) Global
- ( ) Regional

Default rule action

Action *
Deny

Response code *
403 (Forbidden)

Apply policy to targets (optional)

Targets are Google Cloud Platform resources that you want to control access to.
You can only use non-CDN HTTP(S) load balancer backend services as targets.

Type 1
Load balancer backend ser...

Backend Service target 1 *

Filter Type to filter

web-backend
Load balancer: web-lb

+ ADD TARGET

You can also add/edit targets after the p

NEXT STEP

RULES | TARGETS | LOGS

Rules are evaluated by priority: Lower numbers are evaluated first. Learn more

ADD RULE | DELETE | MORE

Filter Enter property name or value

Action	Type	Match	Description	Priority
Deny (403)	IP addresses/ranges	* (All IP addresses)	Default rule, higher priority overrides it	2,147,483,647

Other Google Cloud Armor features

Supports a variety of load balancers:

- Global external Application Load Balancer
- Regional external Application Load Balancer
- Classic Application Load Balancer
- External proxy Network Load Balancer
- External passthrough Network Load Balancer

Supports:

- Rate limiting
- Adaptive protection
- Google Cloud Armor bot management with reCAPTCHA Enterprise
- Custom rules language

Cloud Armor Enterprise

Feature	Standard	Cloud Armor Enterprise	
		Paygo	Annual
Billing method	Pay as You Go	Pay as You Go	Subscription with 12-month commitment
Billing access	Per project	Per project	Per billing account
Cloud Armor WAF	Per policy, per rule, per request	Included	Included
Advanced network DDoS	No	Yes	Yes
Network edge security policy	No	Yes	Yes
Threat Intelligence	No	Yes	Yes
Adaptive Protection	Alert Only	Yes	Yes
DDoS Response	No	No	Yes* (w/premium support)
DDoS Bill Protection	No	No	Yes

Today's agenda

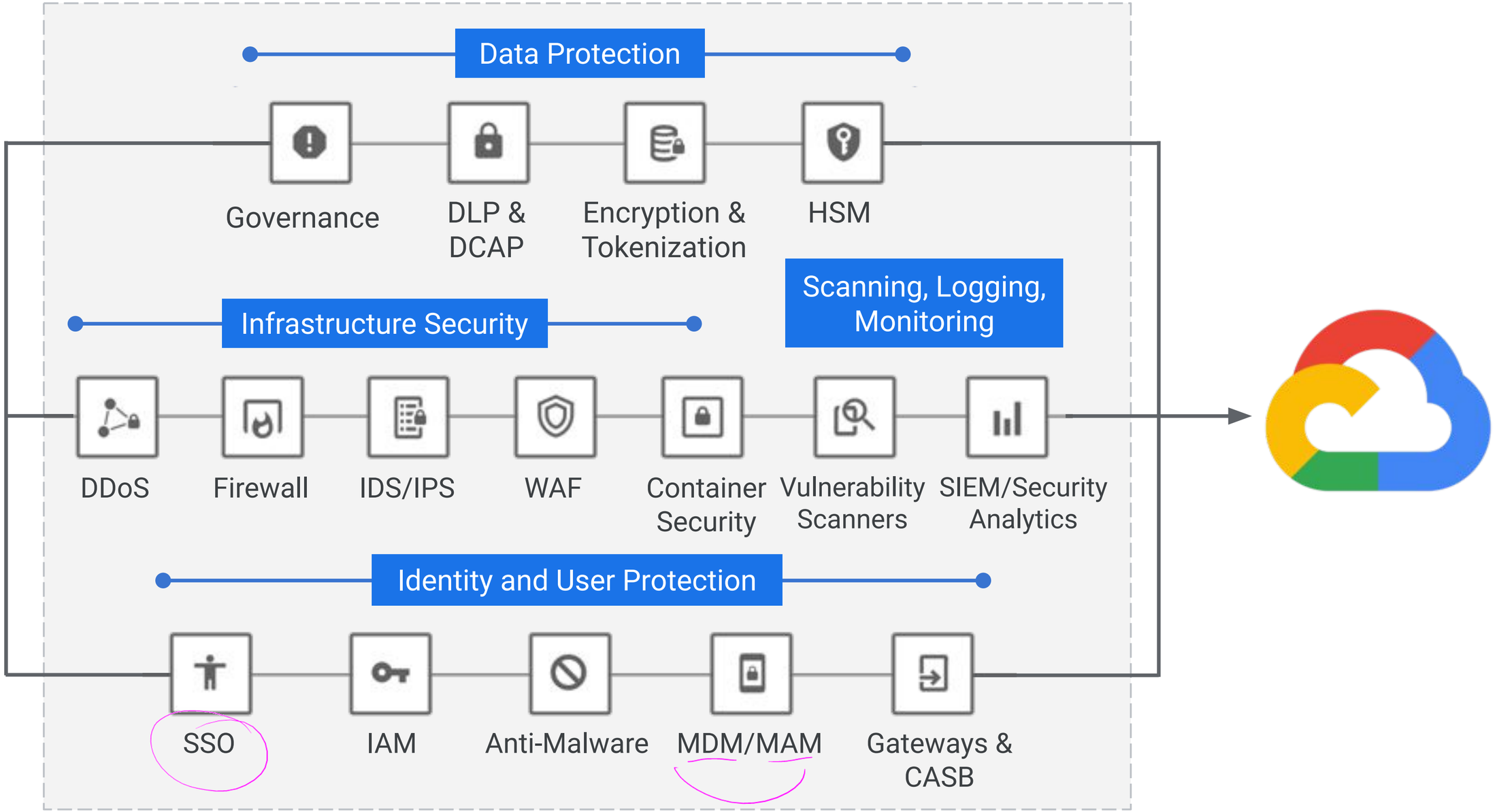
01 How DDoS attacks work

02 Google Cloud mitigations

03 Types of complementary partner products

04 Lab: Configuring Traffic Blocklisting with Google Cloud Armor

05 Quiz



Infrastructure protection partners

https://cloud.google.com/security/partners/

Data protection partners

https://cloud.google.com/security/partners/

Logging and monitoring partners

https://cloud.google.com/security/partners/

Configuration, vulnerability, risk, and compliance

https://cloud.google.com/security/partners/

Today's agenda

01 How DDoS attacks work

02 Google Cloud mitigations

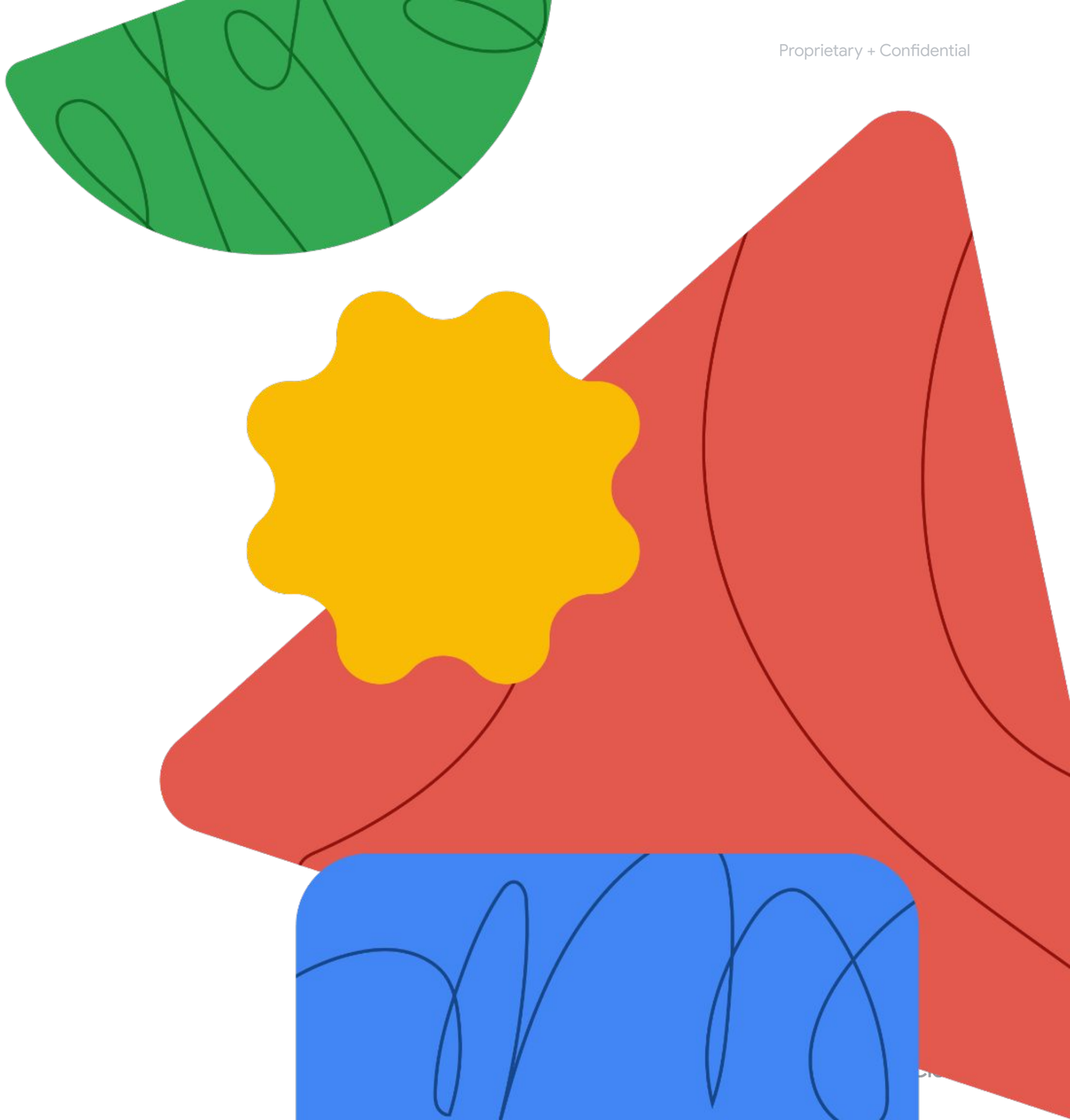
03 Types of complementary partner products

04 Lab: Configuring Traffic Blocklisting with Google Cloud Armor

05 Quiz

Lab intro

Configuring Traffic Blocklisting with Google Cloud Armor



Today's agenda

01 How DDoS attacks work

02 Google Cloud mitigations

03 Types of complementary partner products

04 Lab: Configuring Traffic Blocklisting with Google Cloud Armor

05 Quiz

Quiz | Question 1

Question

Which Google Cloud service provides defense against infrastructure and application Distributed Denial of Service (DDoS) attacks?

A. Cloud CDN

B. Cloud Load Balancing

C. Cloud Armor

D. Cloud DNS

Quiz | Question 1

Answer

Which Google Cloud service provides defense against infrastructure and application Distributed Denial of Service (DDoS) attacks?

A. Cloud CDN

B. Cloud Load Balancing

C. Cloud Armor

D. Cloud DNS

Quiz | Question 2

Question

Which two of the following statements are true about Google Cloud Armor?

A. Google Cloud Armor is not currently compatible with any third-party partner security products.

B. Google Cloud Armor enforces access control based on IPv4 and IPv6 addresses or CIDRs.

C. Google Cloud Armor is a ransomware defense service.

D. Google Cloud Armor protection is delivered at the edge of Google's network.

Quiz | Question 2

Answer

Which two of the following statements are true about Google Cloud Armor?

A. Google Cloud Armor currently is not compatible with any third-party partner security products.

B. Google Cloud Armor enforces access control based on IPv4 and IPv6 addresses or CIDRs. 

C. Google Cloud Armor is a ransomware defense service.

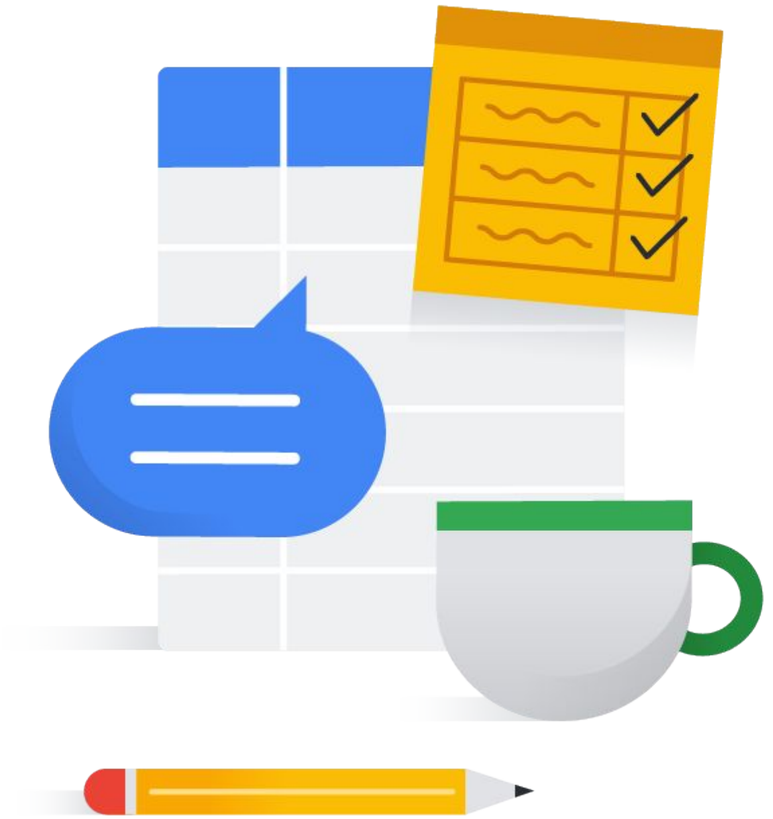
D. Google Cloud Armor protection is delivered at the edge of Google's network. 

Let’s ask Gemini

Instruct the user on creating a Cloud Armor security policy.

Explain how Google Cloud Armor works to protect against DDoS attacks.

Debrief



Thank you.