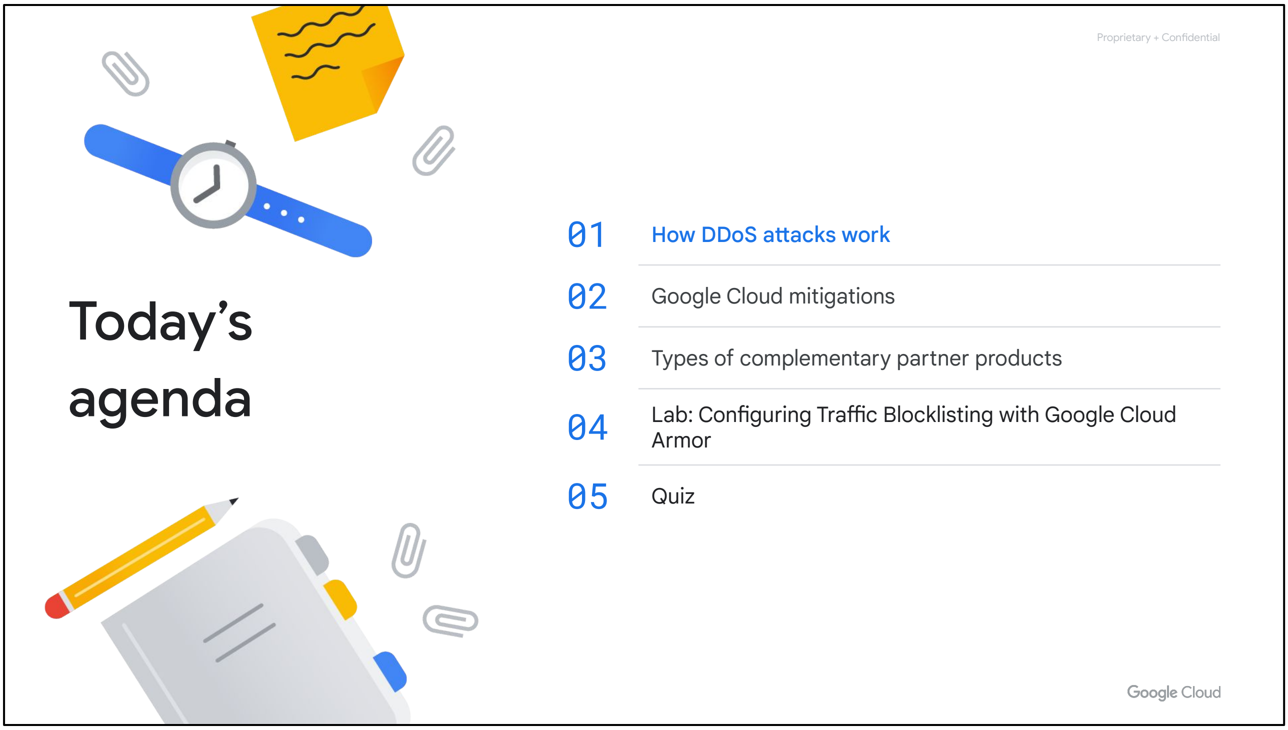
Google Cloud

Networking in Google Cloud

Distributed Denial of Service Attacks (DDoS) Protection

Welcome to the Distributed Denial of Service Attacks (DDoS) Protection module.



Proprietary + Confidential

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

Google Cloud

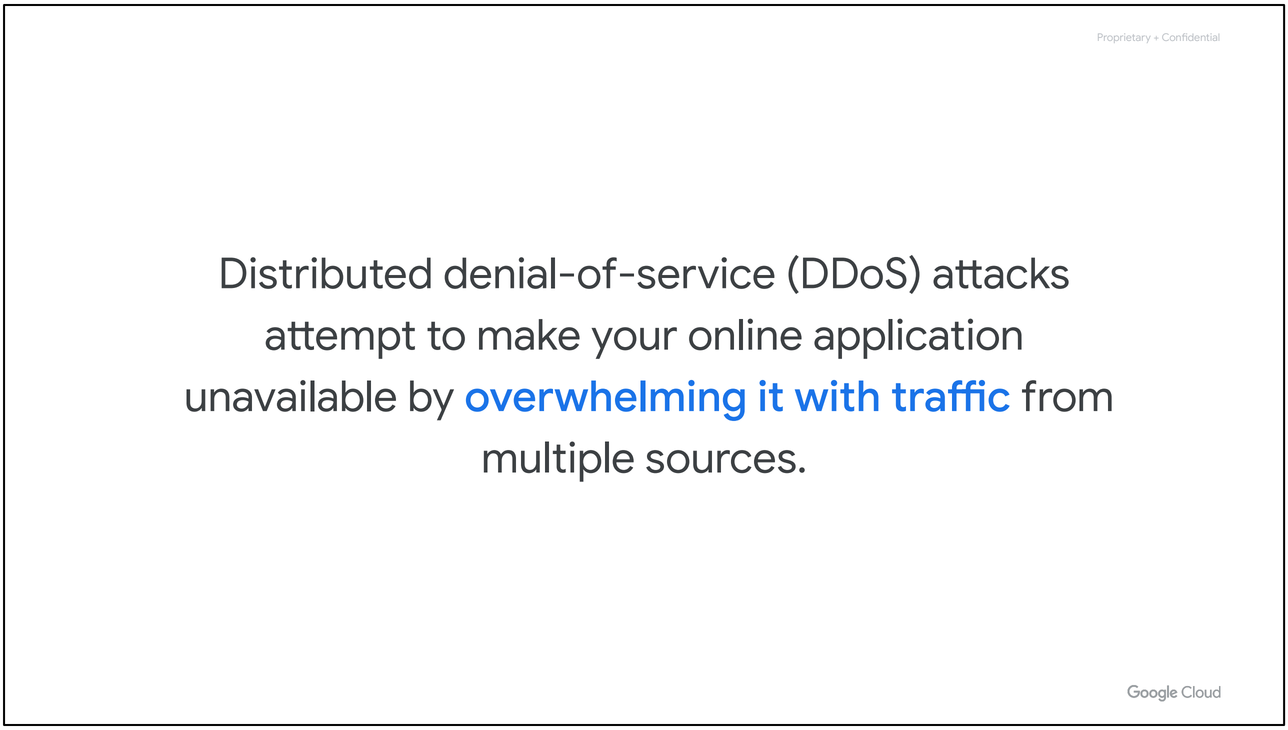
Distributed denial of service attacks are a major concern today. They can have a huge—and potentially fatal—impact on businesses if the business is not adequately prepared.

We will start this module with a quick discussion on how DDoS attacks work.

And then, we will review some DDoS mitigation techniques that are provided by Google Cloud.

Then, we will finish up with a review of complementary partner products and a lab where you will get a chance to see some DDoS mitigations in action.

OK, let's get started!



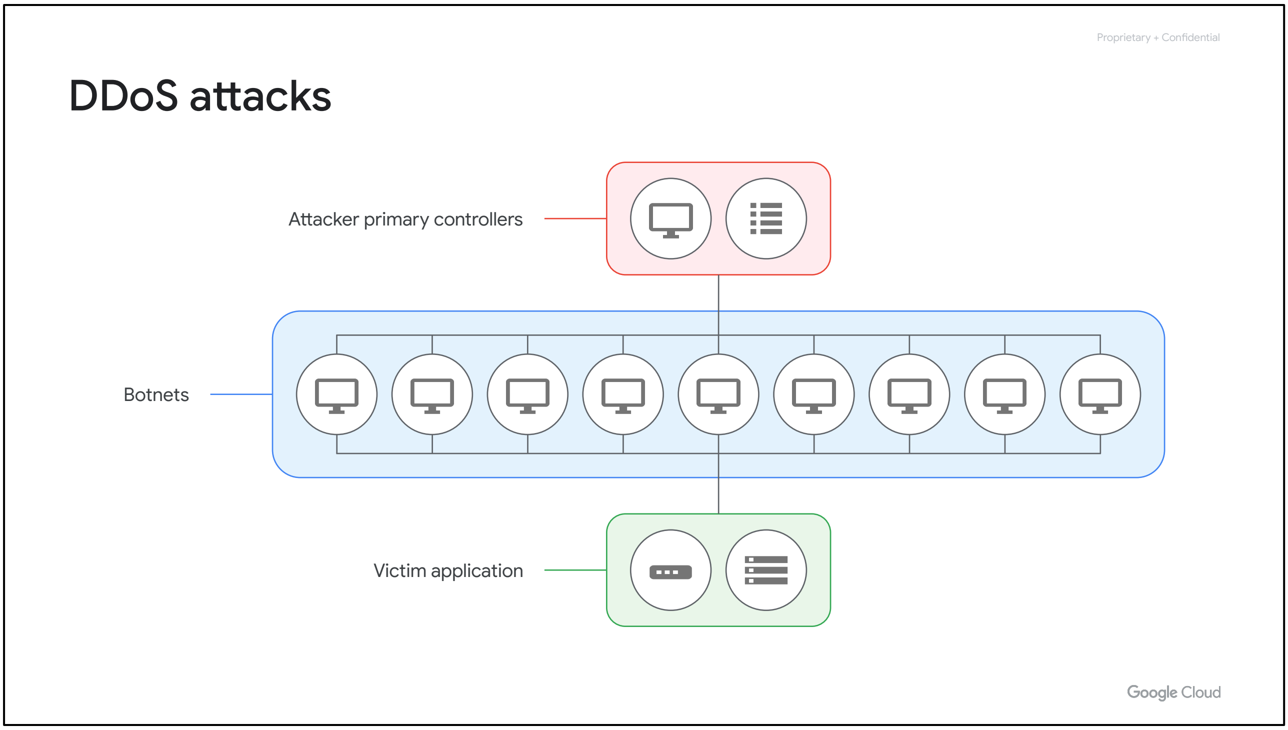
Proprietary + Confidential

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

Google Cloud

A distributed denial-of-service (or DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic from multiple sources.

Essentially, it is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. DDoS attacks can come from individuals, cybercriminal groups, or can even be state-sponsored.

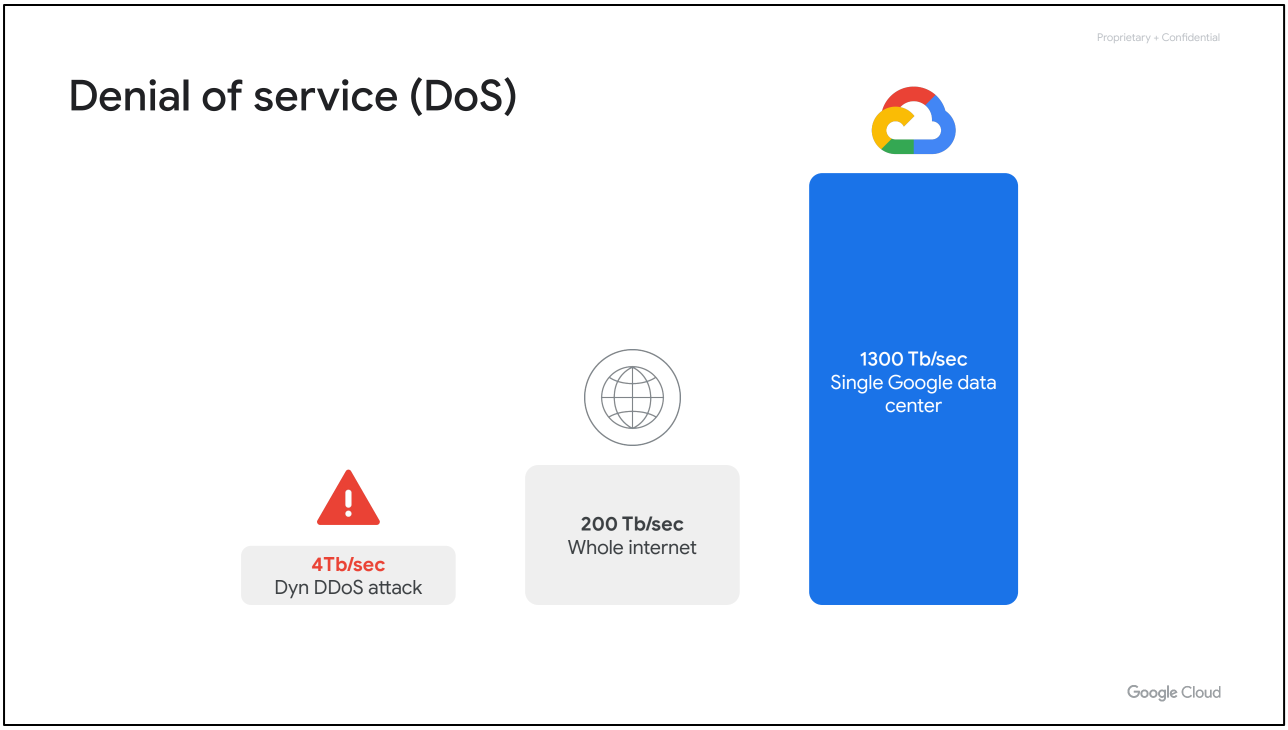


Proprietary + Confidential

DDoS attacks

Google Cloud

In the diagram, attackers build networks of infected computers, known as 'botnets', by spreading malicious software through emails, websites, and social media. Once infected, these machines can be controlled remotely without their owners' knowledge. They are then used like an army to launch an attack against any target. Some botnets are millions of machines strong.



Proprietary + Confidential

Denial of service (DoS)

4Tb/sec
Dyn DDoS attack

200 Tb/sec
Whole internet

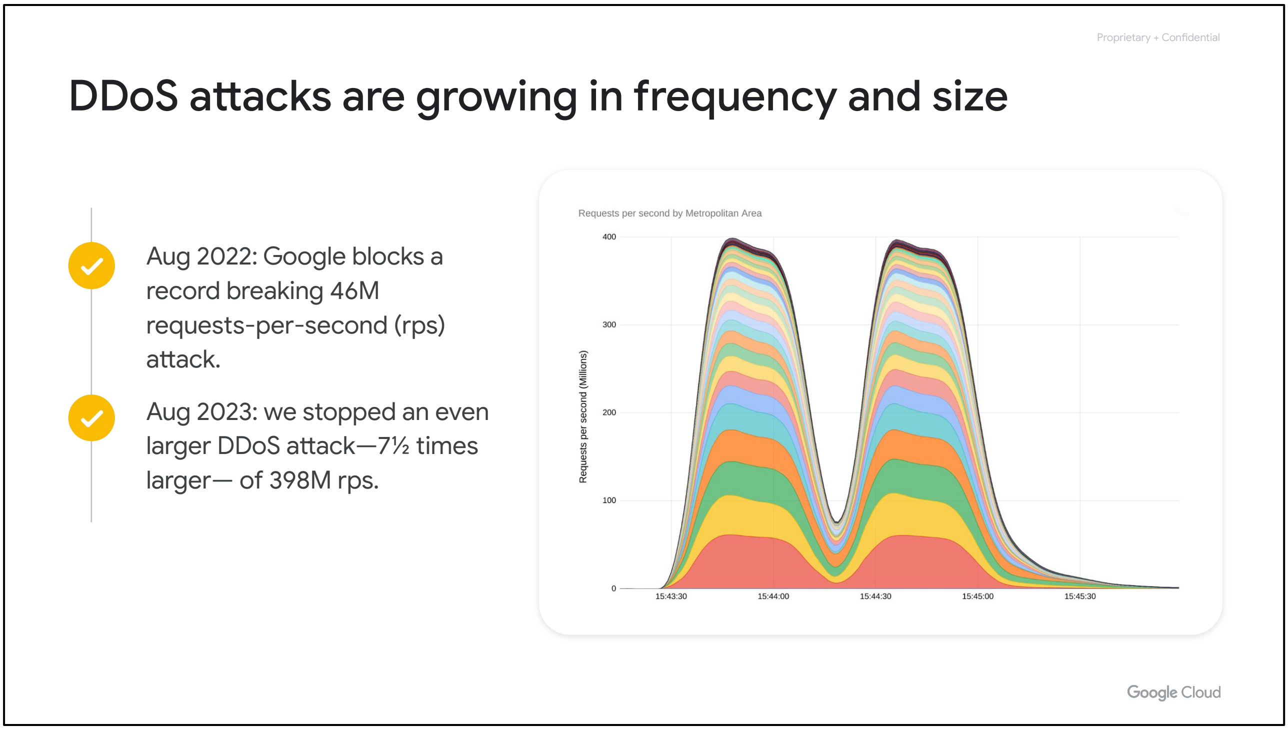
1300 Tb/sec
Single Google data center

Google Cloud

For context, a large attack in 2017 had a strength of around four terabit per second.

For reference, the whole internet has a bisection bandwidth of 200 terabits per second.

Now, when you compare this to a single Google data center, which has a bisection bandwidth of 1,300 terabits per second, you can see we have internal capacity many times that of any traffic load we can anticipate. This means that, when there is an attack, we have time to isolate it and address it.



Proprietary + Confidential

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.

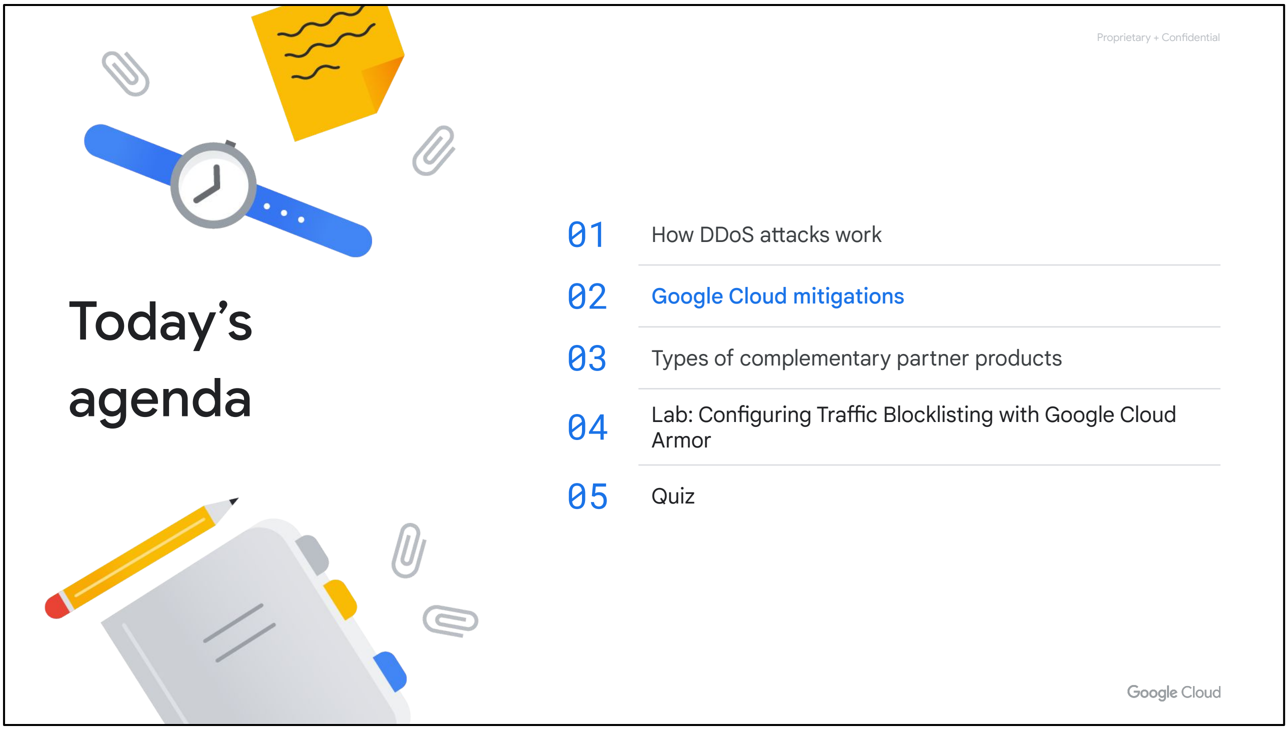
Over the past few years, Google has observed that distributed denial-of-service (DDoS) attacks are increasing in frequency and growing in size exponentially.

On August, 2022, a Google Cloud Armor customer was targeted with a series of HTTPS DDoS attacks which peaked at 46 million requests per second. This is the largest layer 7 DDoS reported to date—at least 76% larger than the previously reported record.

In August 2023, we stopped an even larger DDoS attack—7½ times larger—398M rps.

Cloud Armor blocked the attack ensuring the customer's service stayed online and continued serving their end-users.

Find more details of this attack in the link in the speaker notes:
Link:
https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-at-46-million-rps



Proprietary + Confidential

Today's agenda

01 How DDoS attacks work

02 **Google Cloud mitigations**

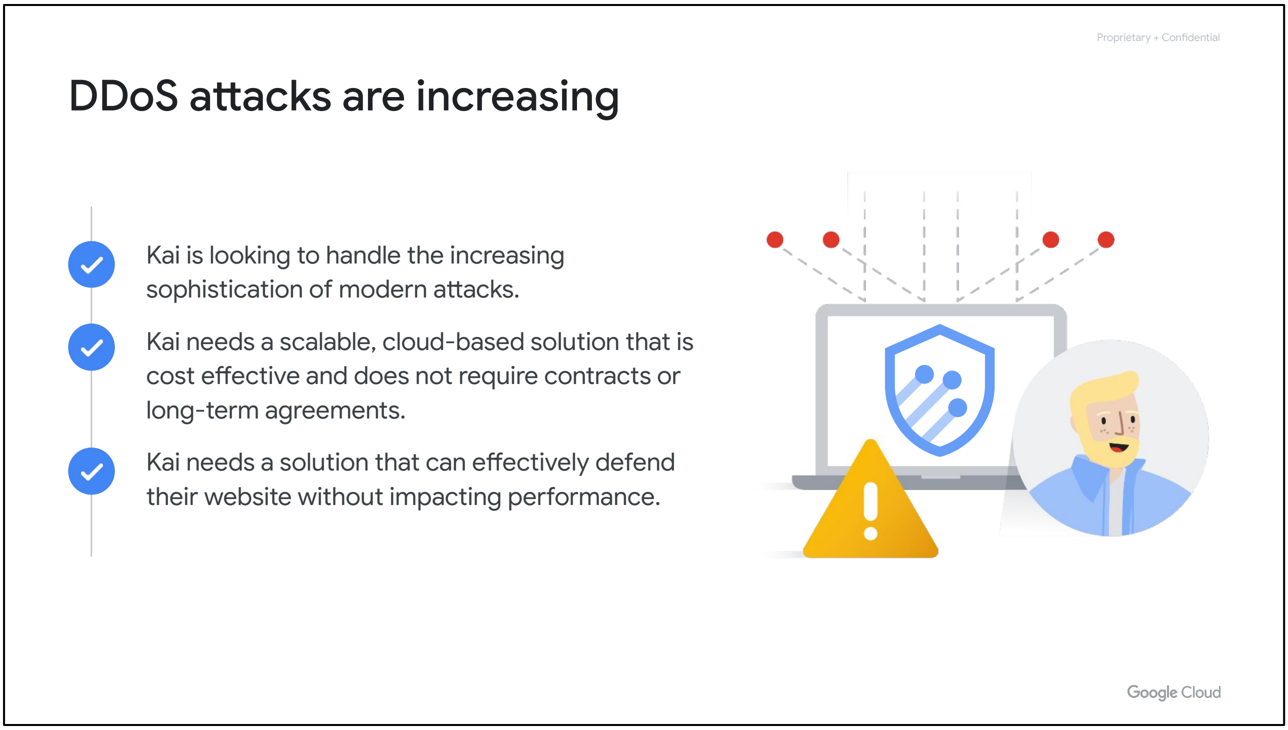
03 Types of complementary partner products

04 Lab: Configuring Traffic Blocklisting with Google Cloud Armor

05 Quiz

Google Cloud

Now let's review some DDoS mitigation techniques that are provided by Google Cloud.



Proprietary + Confidential

DDoS attacks are increasing

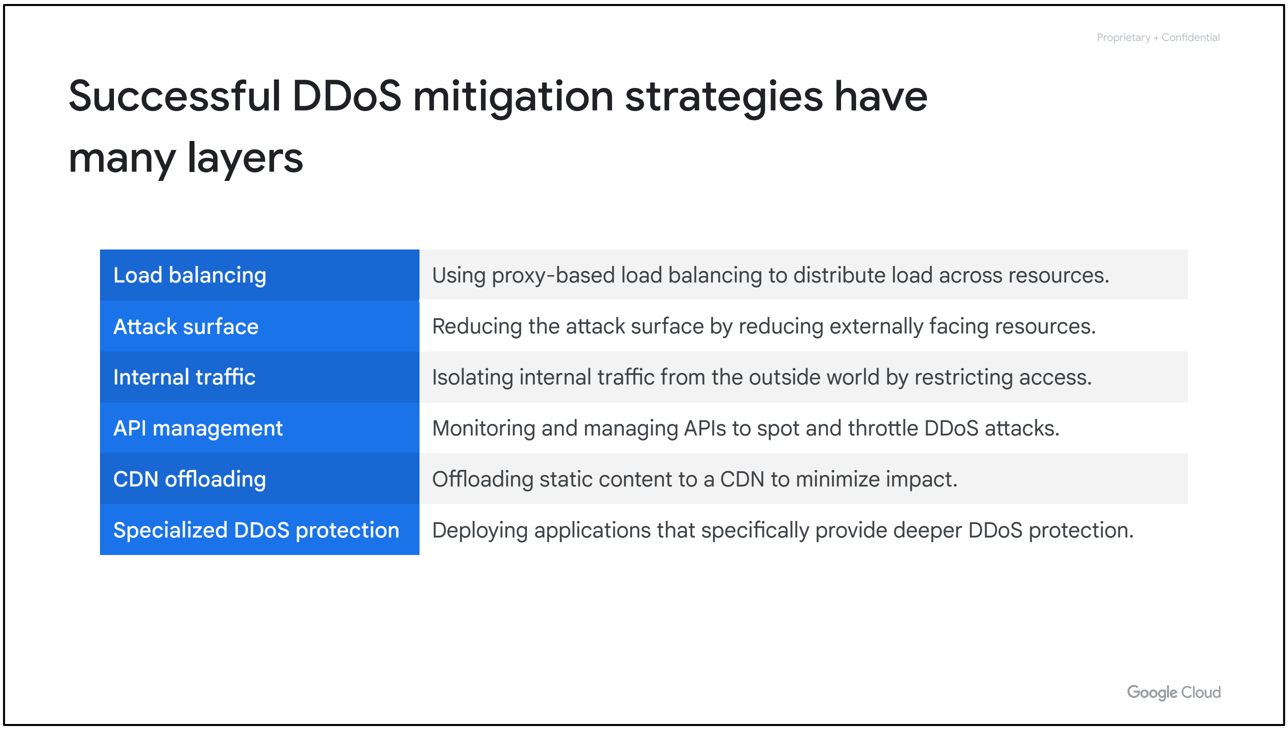
- ✓ Kai is looking to handle the increasing sophistication of modern attacks.
- ✓ Kai needs a scalable, cloud-based solution that is cost effective and does not require contracts or long-term agreements.
- ✓ Kai needs a solution that can effectively defend their website without impacting performance.

Google Cloud

Kai is a network engineer at Cymbal Corporation. Their current DDoS solution is outdated and resource-intensive, struggling to handle the increasing traffic volume and sophistication of modern attacks. Kai needs a scalable, cloud-based solution that is cost effective and does not require contracts or long-term agreements.

A solution that can effectively defend their website without impacting performance.

Let us see the ways you can address this challenge.



Proprietary + Confidential

Successful DDoS mitigation strategies have many layers

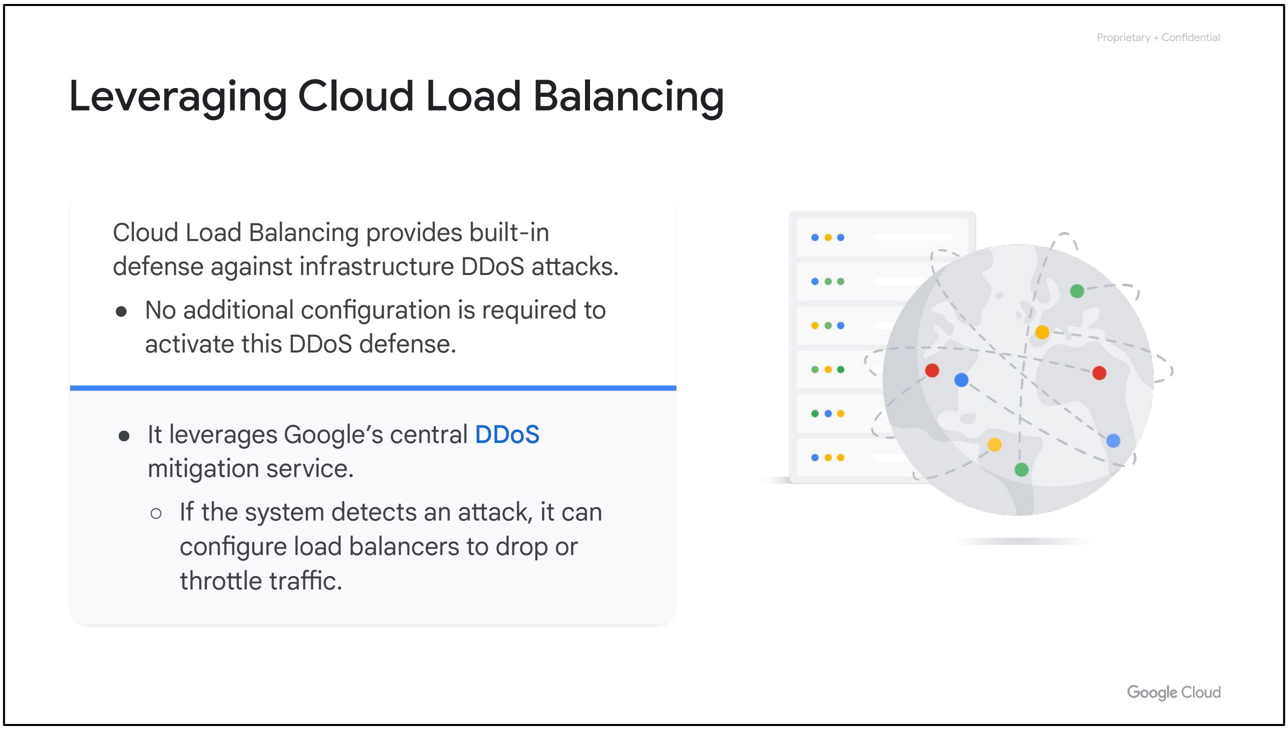
Load balancing	Using proxy-based load balancing to distribute load across resources.
Attack surface	Reducing the attack surface by reducing externally facing resources.
Internal traffic	Isolating internal traffic from the outside world by restricting access.
API management	Monitoring and managing APIs 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.

Creating secure applications requires a multi-faceted approach which has been customized to fit your business' needs, vulnerabilities, and resources. Properly understanding the different options available when facing a DDoS attack can help your organization create a plan to minimize the impact.

Let's look at these generalized strategies in more detail and discuss how Google Cloud helps you implement them.

In this lesson, you will learn more about:

- Leveraging Cloud Load Balancing.
- Reducing the network attack surface.
- Isolating internal traffic.
- Using Cloud CDN.
- Using API management and monitoring.
- Leveraging the Google Cloud Armor defense service.



Proprietary + Confidential

Leveraging Cloud Load Balancing

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

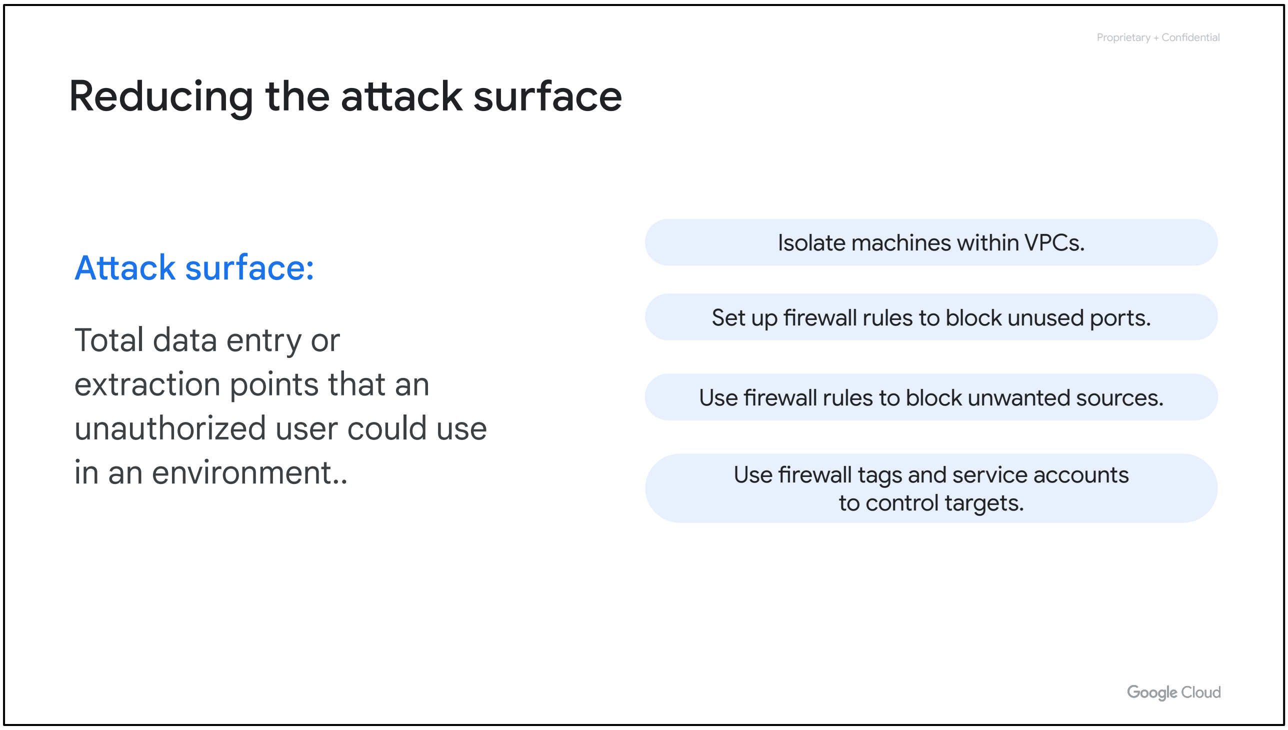
- No additional configuration is required to activate this DDoS defense.

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

Google Cloud

Cloud Load Balancing provides built-in defense against infrastructure DDoS attacks—and no additional configuration is needed. Placing a load balancer in front of your services will filter known-bad traffic streams before they reach your resources. Google Cloud offers load balancing at layer 4 (the transport layer, such as TCP or UDP) and layer 7 (the application layer, generally HTTP or HTTPS). The layer 4 load balancers automatically protect against things like UDP floods and TCP SYN floods. The layer 7 load balancers provide layer 4 protection plus protection from connection-based attacks like Slowloris.

Google Cloud load balancers leverage Google's global DoS mitigation service. If the system detects an attack, it will automatically configure the load balancers to drop or throttle traffic.



Proprietary + Confidential

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.

Google Cloud

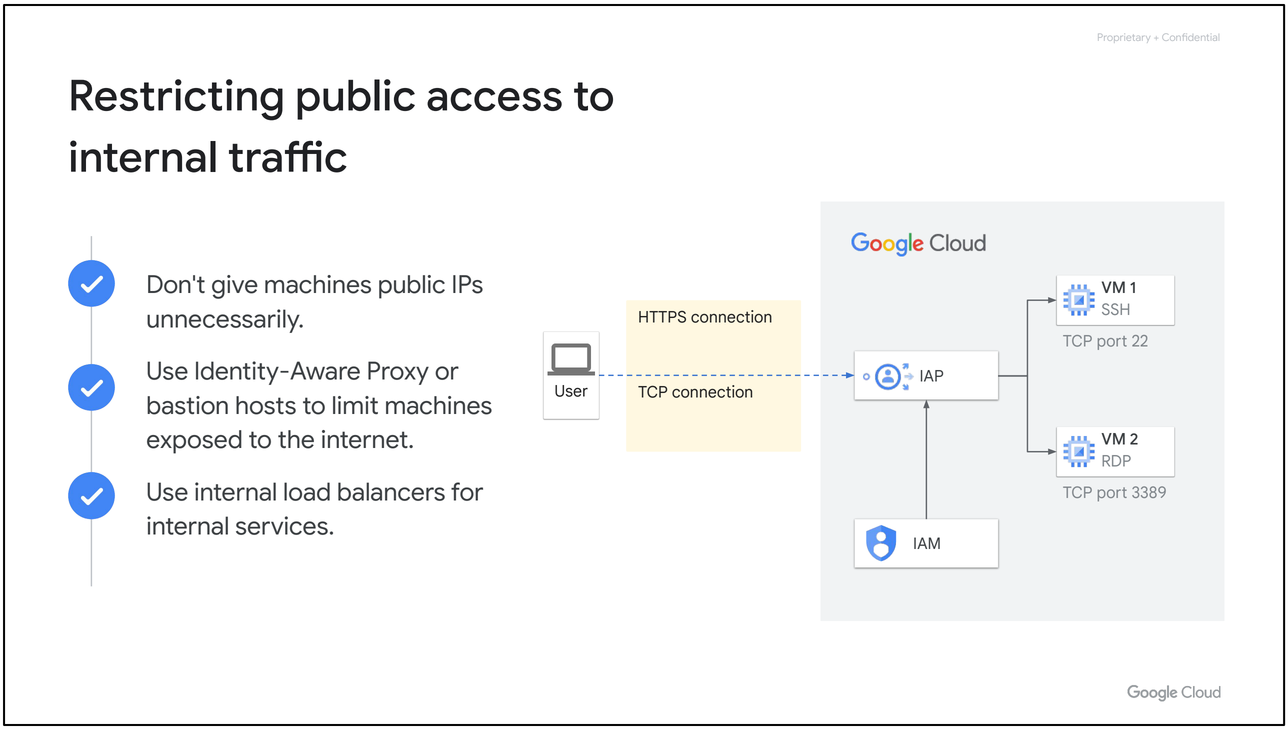
An attack surface of a software environment is the sum of the different points where an unauthorized user can try to enter data to or extract data from this environment. Keeping the attack surface as small as possible is a basic security measure.

Reducing the attack surface means reducing how much exposure your VMs have to the internet. You should host Compute Engine resources that require network communication on the same VPC network. If the resources aren't related and don't require network communication among themselves, consider hosting them on different VPC networks. For most applications implemented in Google Cloud, Google also recommends creating separate subnets within a network for each tier of an application (for example, web front end, services layer, and database backend). That is because subnetting is a convenient way to implement inter-network firewall restrictions.

You can control individual ingress and egress traffic for compute resources using firewall rules.

Be sure you are blocking both unused ports as well as unwanted sources.

Remember, you can use firewall tags and service accounts to help control which targets to use for firewall rules.



Proprietary + Confidential

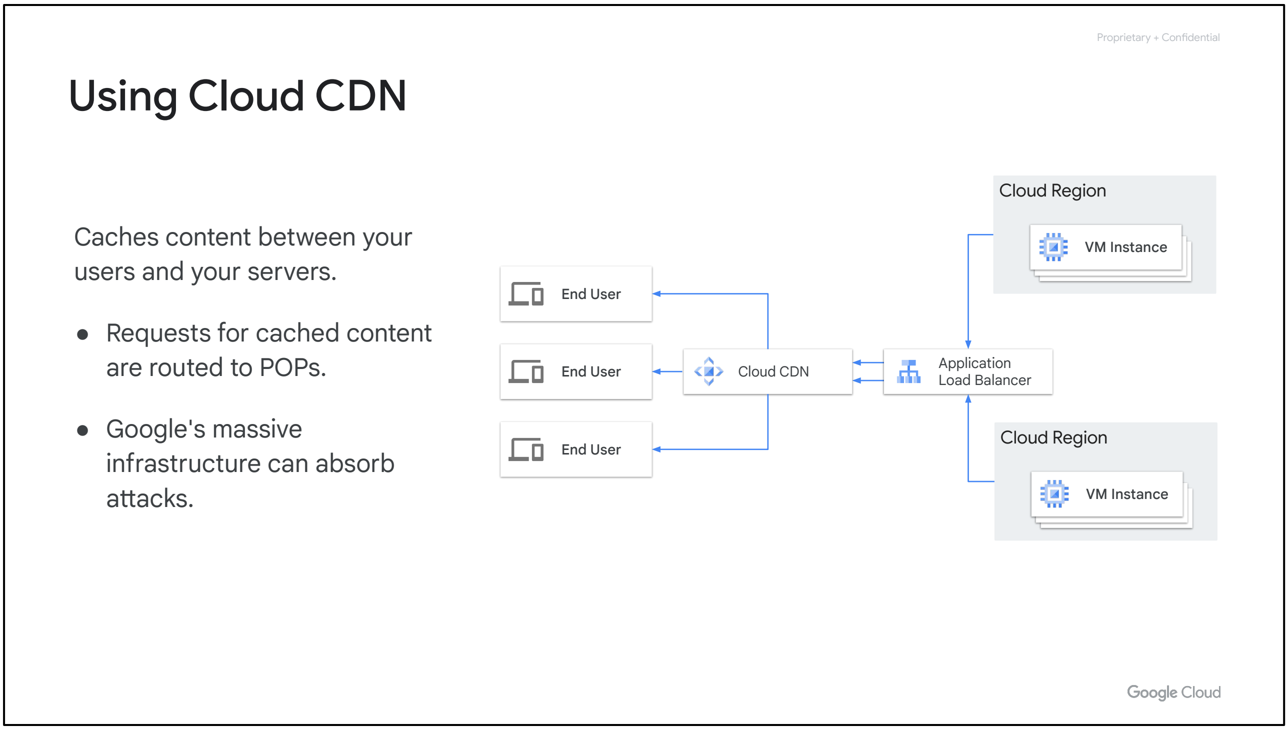
Restricting public access to internal traffic

- ✓ 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.

Google Cloud

It is also important to ensure you restrict external traffic within your VPCs. Virtual machines should not be given public IP addresses unnecessarily.

Even if you need to connect to the VM from the internet, leveraging solutions like Identity-Aware Proxy or bastion hosts can help restrict the internal traffic. You can also connect your on-premise network with your VPC network using VPN IPsec Tunnels or Dedicated Interconnect.



Proprietary + Confidential

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.

End User

End User

End User

Cloud CDN

Application Load Balancer

Cloud Region

VM Instance

Cloud Region

VM Instance

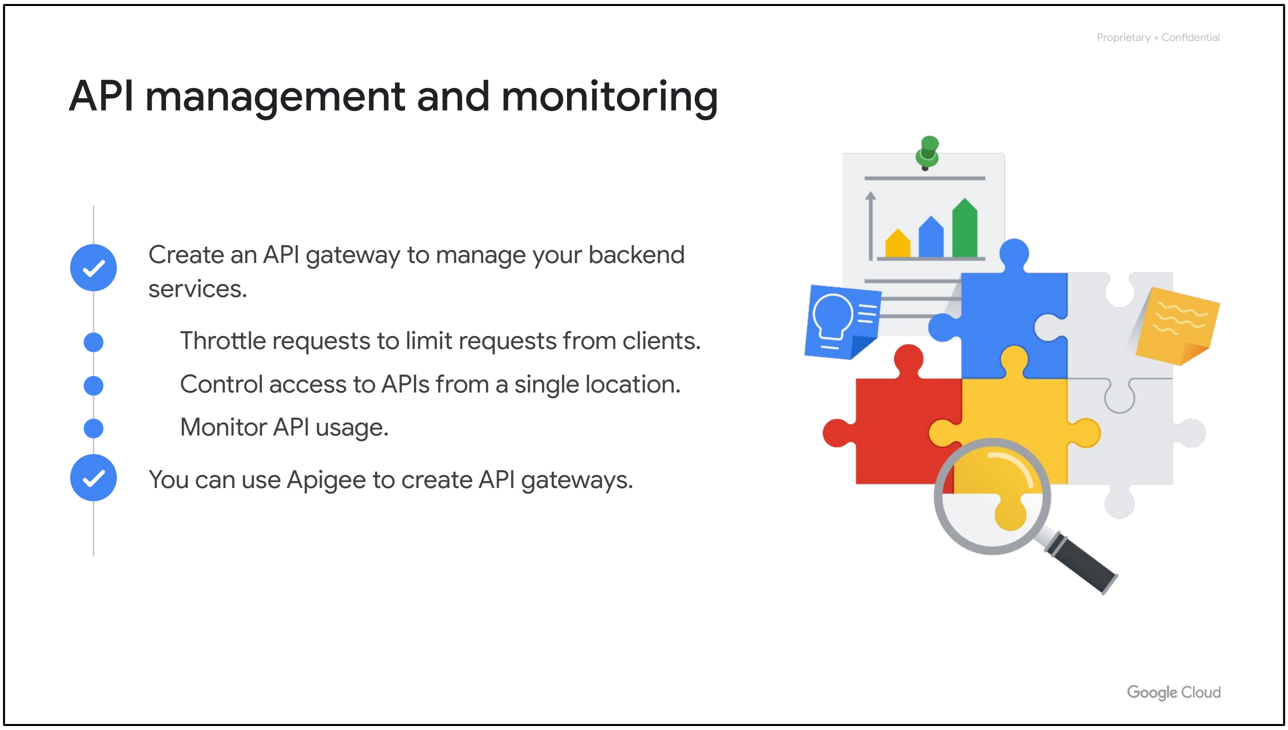
Google Cloud

Google’s Cloud Content Delivery Network (or CDN) is used to cache web content at over 90 edge locations, or points of presence (POPs), around the globe.

Cloud CDN provides very similar protection as Google’s load balancers. In addition, requests for your content are routed to Google’s POPs (points of presence) rather than directly to your resources.

Thus, Google Cloud’s resilient network infrastructure absorbs the brunt of attacks.

This also naturally reduces the load on your resources even when there are no attacks.



Proprietary + Confidential

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.

Google Cloud

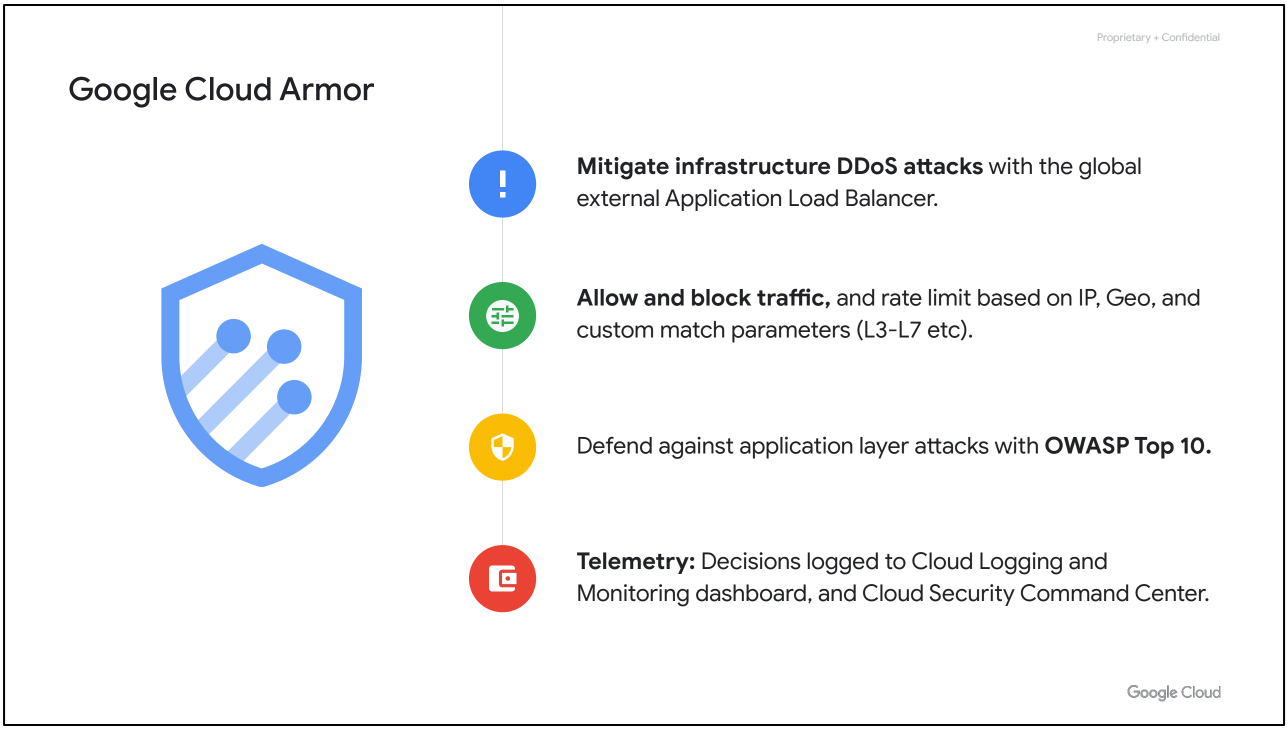
For IT, network, and DevOps teams, allowing access to backend services is often required to facilitate interactions between applications, services, customers, and business partners.

This access can also introduce vulnerabilities and challenges.

Putting an API gateway, or API management, in front of your backend services can help prevent denial of service attacks by:

- Throttling requests to limit the number of requests per client.
- Controlling access to API from a single centralized location.
- Adding the ability to monitor and track all API usage.

In Google Cloud, use Apigee for implementing API management.



Proprietary + Confidential

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.

Google Cloud

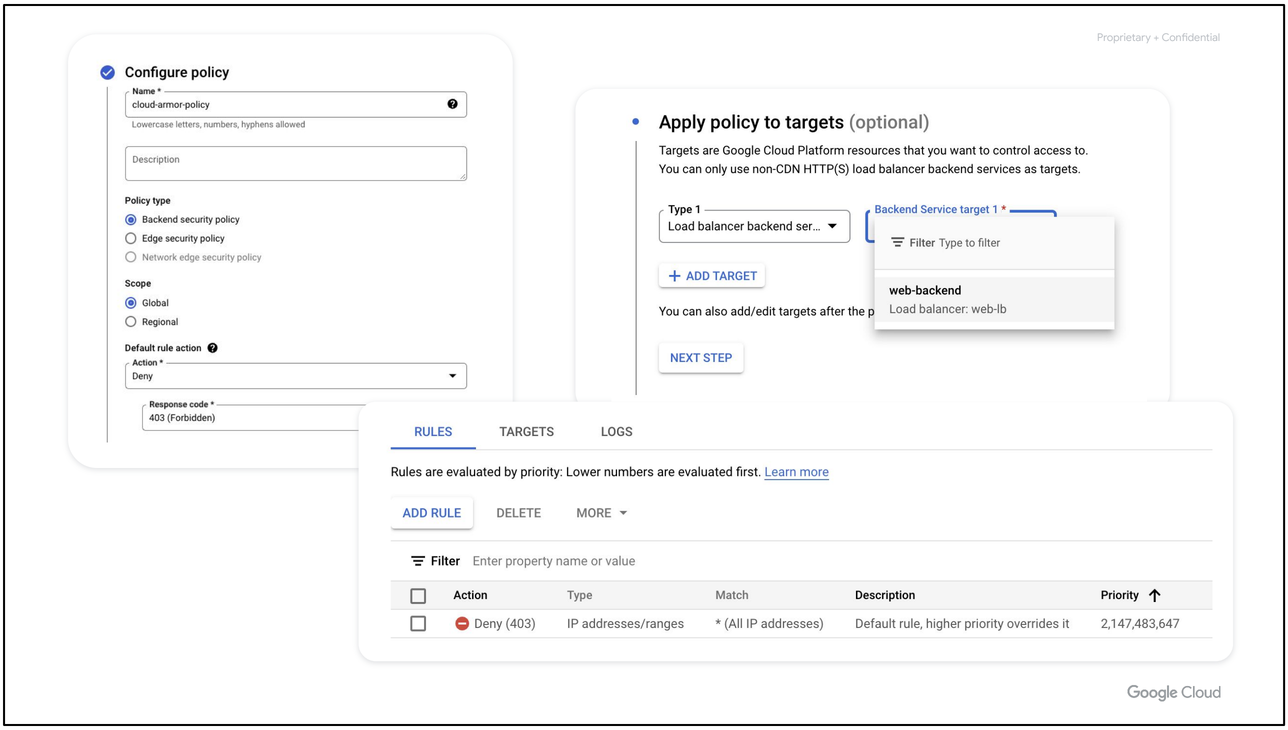
Google Cloud Armor is a DDoS and application defense service. It delivers defense at scale against infrastructure and web application Distributed Denial of Service (DDoS) attacks using Google's global infrastructure and security systems. Similar to CDNs, Google Cloud Armor protection is delivered at the edge of Google's network and can block attacks close to their source before they have a chance of affecting your applications. Google Cloud Armor works with the global external Application Load Balancer to provide built-in defenses against infrastructure DDoS attacks.

It defends against both network-layer (L3/L4) and application-layer (L7) DDoS attacks, safeguarding your services from being overwhelmed by malicious traffic.

Google Cloud Armor comes with pre-defined rulesets specifically designed to protect against the OWASP Top 10 web application vulnerabilities. These include common threats like SQL injection (SQLi), cross-site scripting (XSS), and insecure deserialization.

You can easily configure Google Cloud Armor to block traffic originating from specific countries or regions. This is helpful for preventing attacks from known malicious sources or complying with regional regulations.

Google Cloud Armor also provides detailed logs for analysis and monitoring of traffic patterns and potential security threats.



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

You can also add/edit targets after the p

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

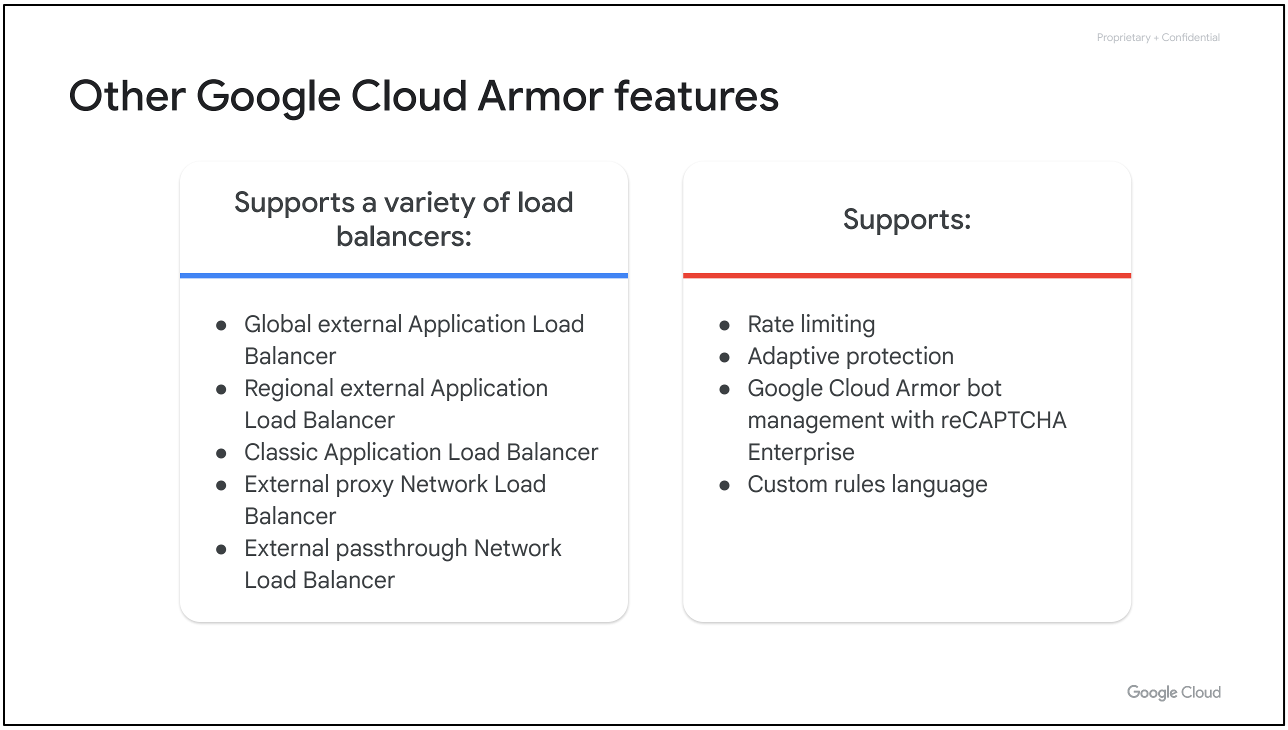
Filter Enter property name or value

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

Google Cloud Armor defense is customized using a security policy which can contain one or more rules.

Rules tell your security policy what to do (the action), when to do it (the condition), and where to apply the rule (the target).

Google Cloud Armor also provides several predefined rules to defend against cross-site scripting (XSS) and SQL injection (SQLi) application-aware attacks.



Proprietary + Confidential

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

Google Cloud

Google Cloud Armor also provides the following features:

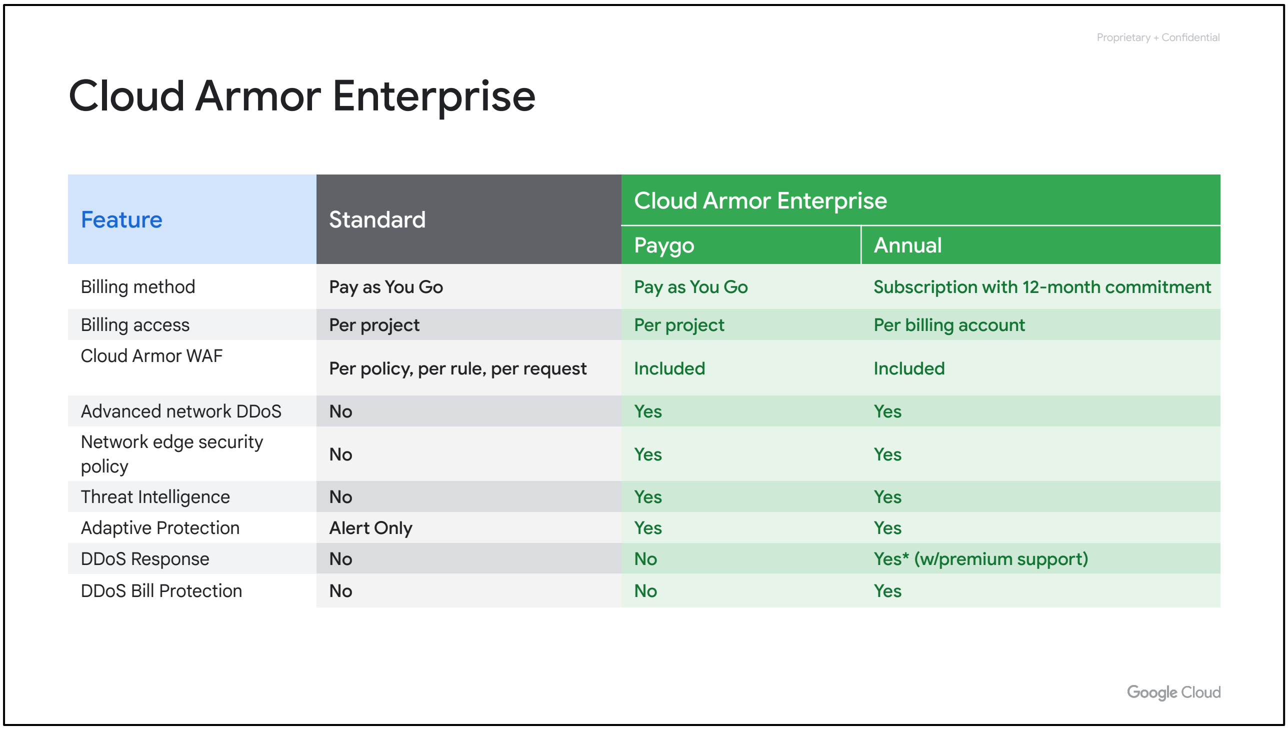
- **Variety of load balancer support:** Google Cloud Armor now supports a variety of load balancers:
  - Global external Application Load Balancer
  - Regional external Application Load Balancer
  - Classic Application Load Balancer
  - External proxy Network Load Balancer
  - External passthrough Network Load Balancer
- **Rate limiting:** rate-based rules help you protect your applications from a large volume of requests that flood your instances and block access for legitimate users.
- **Adaptive protection:** helps you protect your Google Cloud applications, websites, and services against L7 distributed denial-of-service (DDoS) attacks such as HTTP floods and other high-frequency layer 7 (application-level) malicious activity.
- **Cloud Armor bot management with reCAPTCHA Enterprise:** helps you evaluate and act on incoming requests that might be from automated clients.
- **Custom rules language:** enables you to define prioritized rules with configurable match conditions and actions in a security policy.

For the latest Google Cloud Armor updates, check out the Google Cloud Armor release notes.

- **Link:** cloud.google.com/armor/docs/release-notes

To explore Google Cloud Armor features further, check out the **Securing your Network with Cloud Armor** quest.

- **Link:** https://www.cloudskillsboost.google/course_templates/785



Proprietary + Confidential

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

Google Cloud

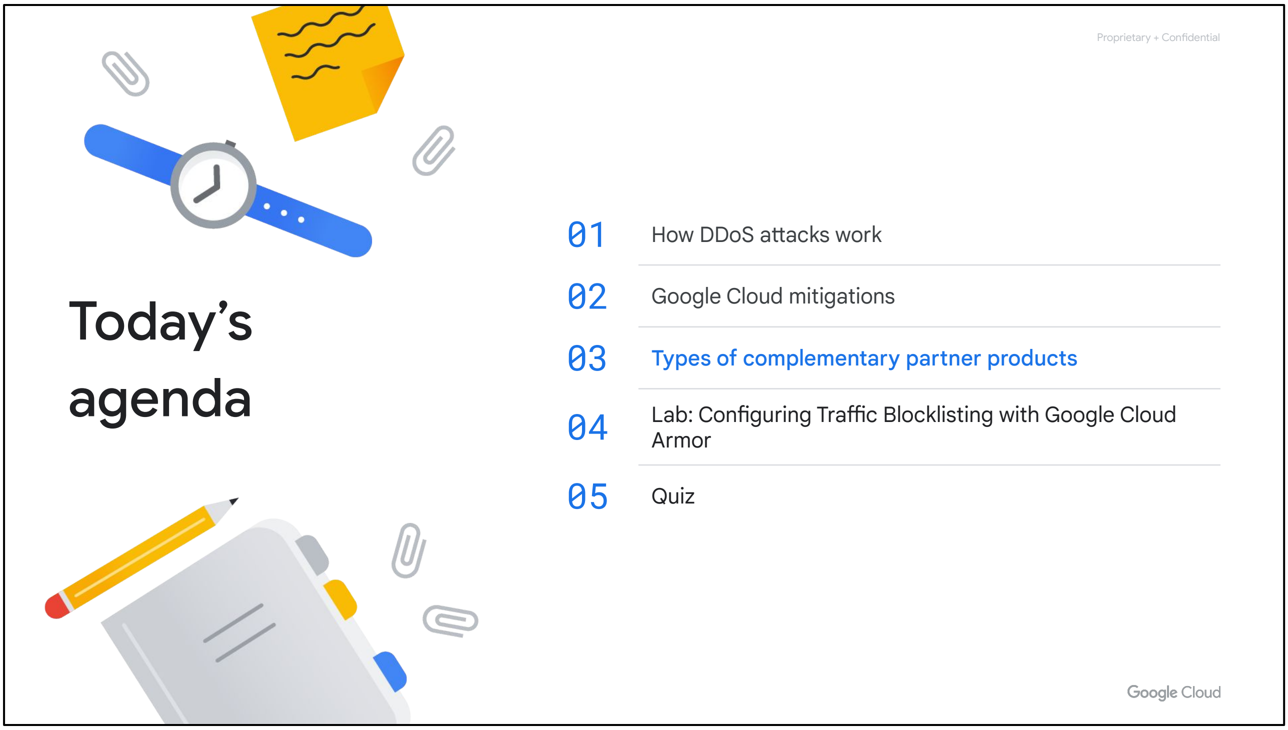
Cloud Armor Enterprise expands upon Google Cloud Armor Standard, providing enhanced security capabilities for your applications and infrastructure.

It offers flexible pricing models—annual for predictable budgeting or pay-as-you-go for scalability. Cloud Armor Enterprise includes unlimited access to the Web Application Firewall (WAF), covering rules, policies, and requests for comprehensive and simplified protection.

Proactive security is bolstered by curated third-party IP lists and Google Threat Intelligence insights, keeping you ahead of emerging threats. The service employs advanced protection mechanisms, including machine learning-powered Adaptive Protection for Layer 7 and robust defenses against DDoS attacks for pass-through endpoints.

If you opt for the annual plan, you'll gain access to DDoS bill protection and expert support from the DDoS response team, as well as in-depth visibility into DDoS attack patterns to help you strengthen your security posture.

Cloud Armor Enterprise equips you with a robust and adaptable security toolkit to defend against the ever-changing threat landscape and keep your digital assets secure.



Proprietary + Confidential

Today's agenda

01 How DDoS attacks work

02 Google Cloud mitigations

03 Types of complementary partner products

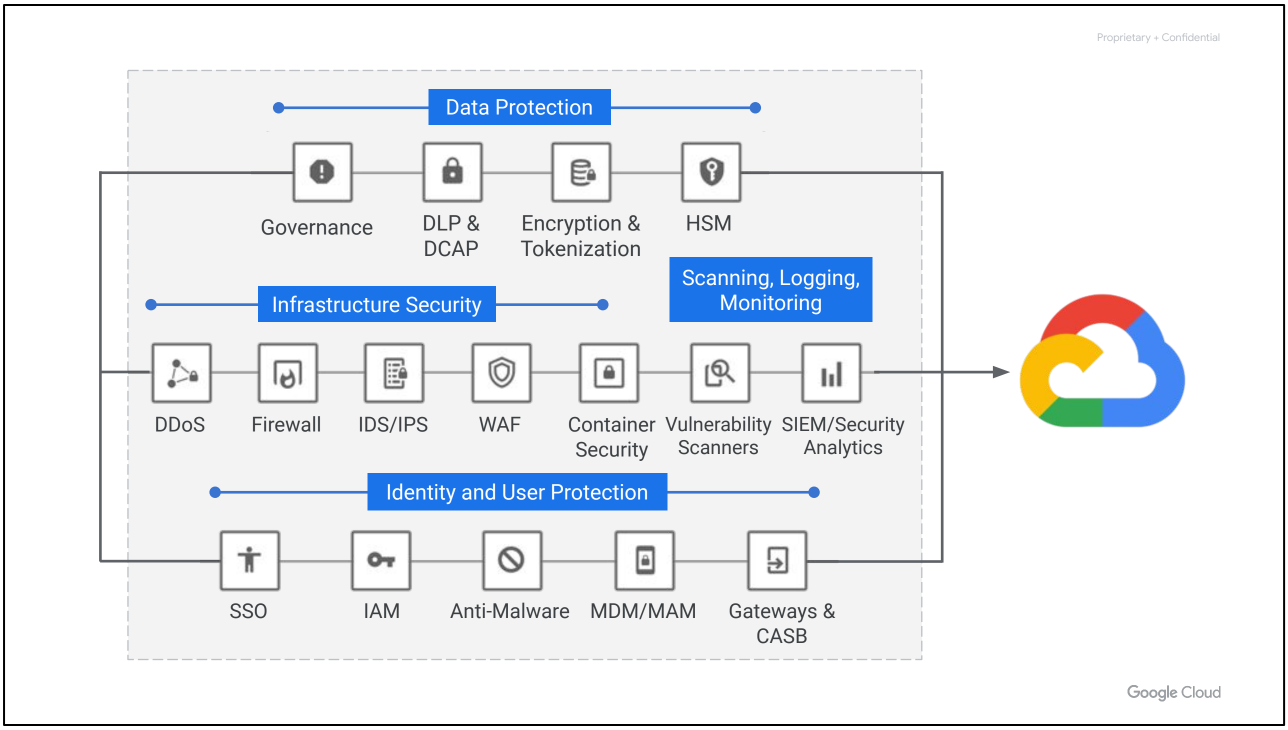
04 Lab: Configuring Traffic Blocklisting with Google Cloud Armor

05 Quiz

As you have seen, here at Google, we offer some of the best in class platform security, but we did not stop there.

Google also partners with a number of security-centric firms.

In this section, we will review some of the complementary partner products.



Proprietary + Confidential

Data Protection

Governance

DLP & DCAP

Encryption & Tokenization

HSM

Infrastructure Security

Scanning, Logging, Monitoring

DDoS

Firewall

IDS/IPS

WAF

Container Security

Vulnerability Scanners

SIEM/Security Analytics

Identity and User Protection

SSO

IAM

Anti-Malware

MDM/MAM

Gateways & CASB

Google Cloud

There are several different categories of security in our security ecosystem:

Data protection, which includes things like:

- Governance
- Data loss prevention
- Data-centric audit and protection
- Encryption
- Hardware security modules

Infrastructure protection, which includes:

- DDoS protection
- Network and application firewalls
- Intrusion detection and prevention
- Container security

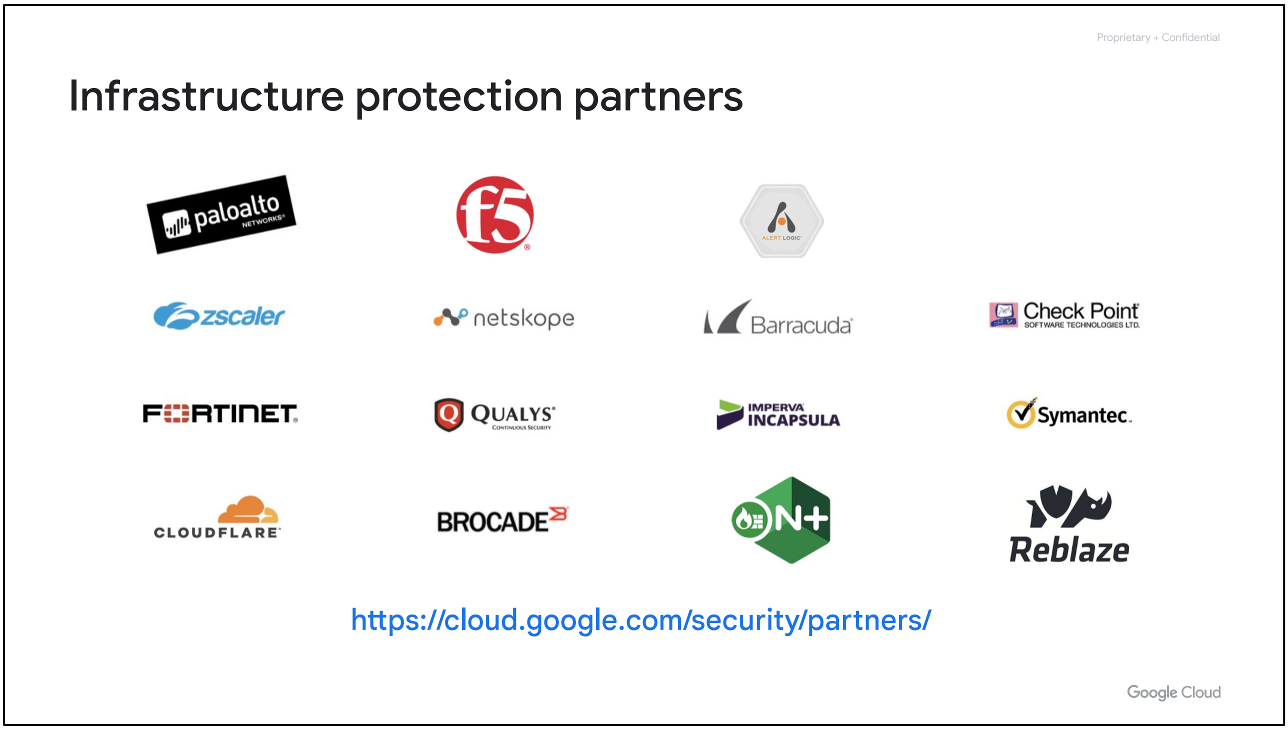
Scanning, logging, and monitoring, which includes a vulnerability scanner and security and information management tools.

Identity and user protection, which includes:

- Single sign on
- Identity and Access Management
- Anti-malware
- Mobile device and application management

- Cloud access security brokers

Configuration, vulnerability, risk, and compliance protection across all areas of your infrastructure.



Proprietary + Confidential

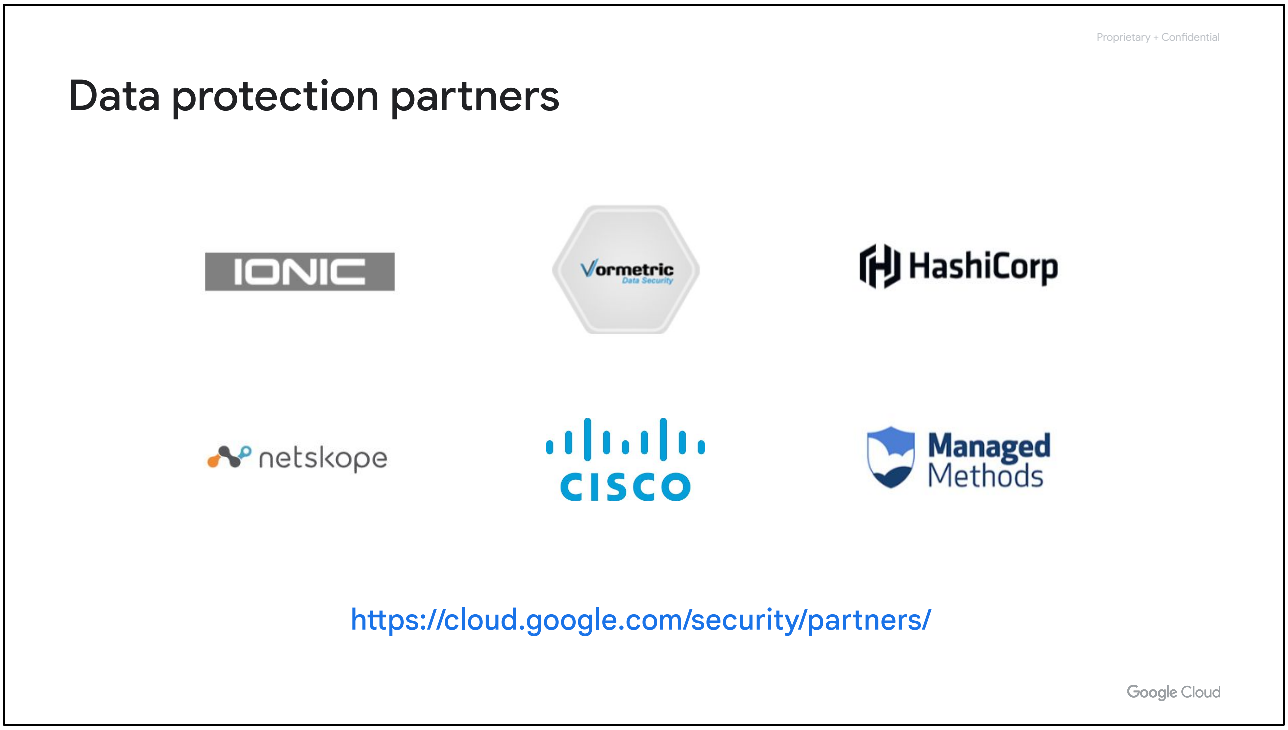
Infrastructure protection partners

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

Google Cloud

Infrastructure protection helps protect your cloud infrastructure and applications from cyberattacks. There are many industry leaders that provide services that can be leveraged from Google Cloud covering a wide range of solutions, including:

- Next generation firewalls
- Web application firewalls
- Web proxies and cloud gateways
- Server endpoint protection
- Distributed denial of service
- And container security



Proprietary + Confidential

Data protection partners

IONIC

Vormetric Data Security

HashiCorp

netskope

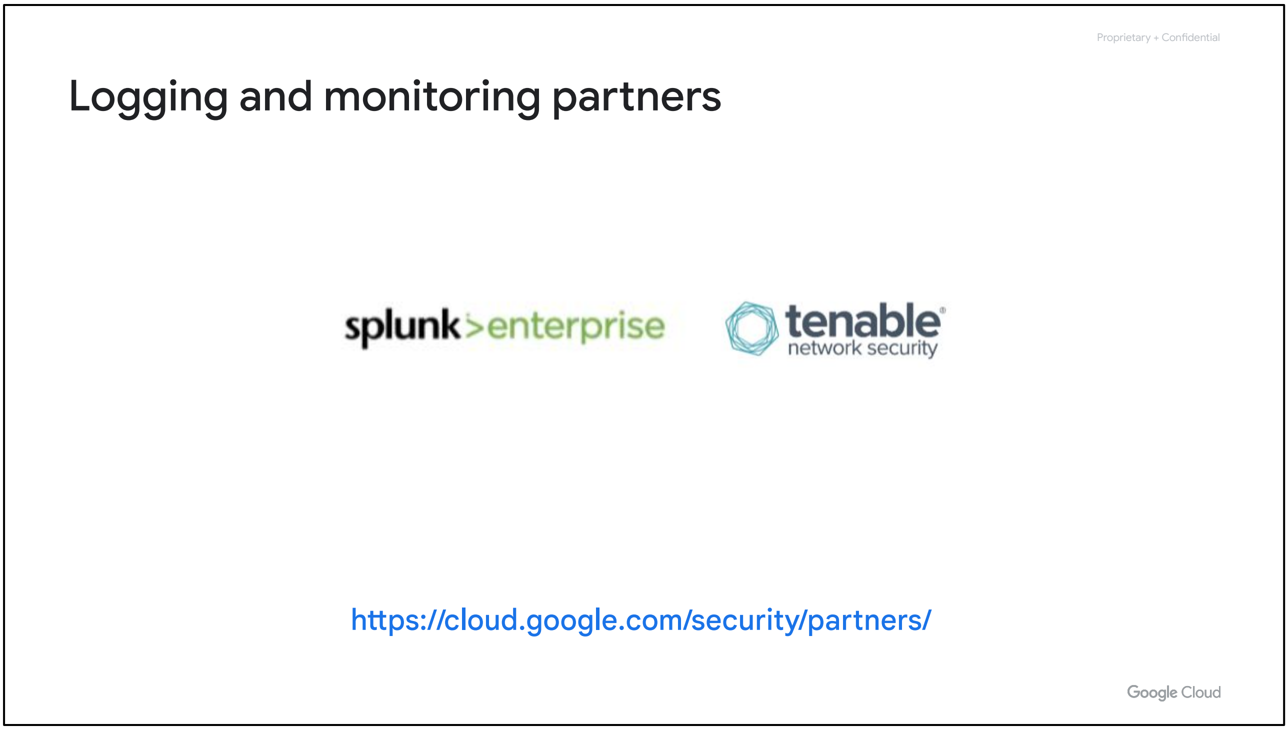
CISCO

Managed Methods

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

Google Cloud

Data protection partners can help protect your data from unauthorized access, as well as internal and external threats through encryption, key management, and policy-driven data loss prevention controls.



Proprietary + Confidential

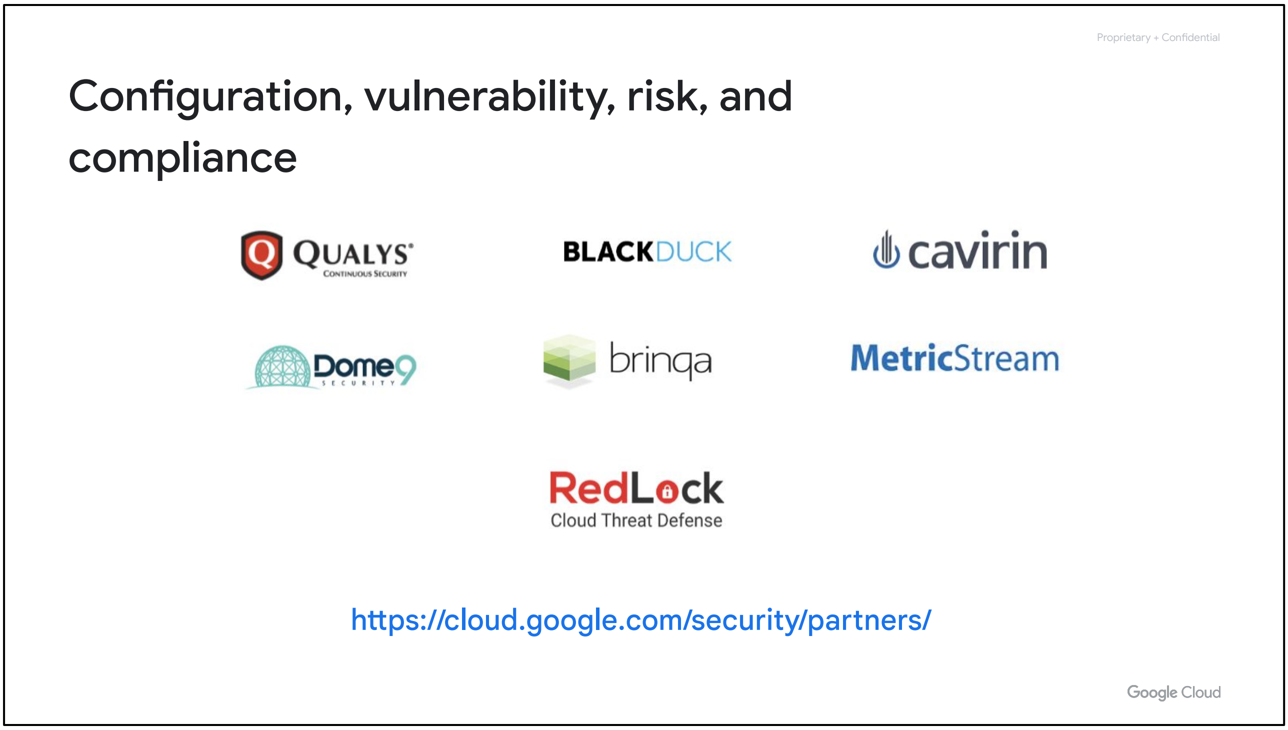
Logging and monitoring partners

splunk>enterprise

tenable network security

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

Logging and monitoring partners help enable visibility and auditability of user and system activities in your infrastructure, while providing policy-driven alerting and reporting.



Proprietary + Confidential

Configuration, vulnerability, risk, and compliance

QUALYS
CONTINUOUS SECURITY

BLACKDUCK

cavirin

Dome9
SECURITY

brinqa

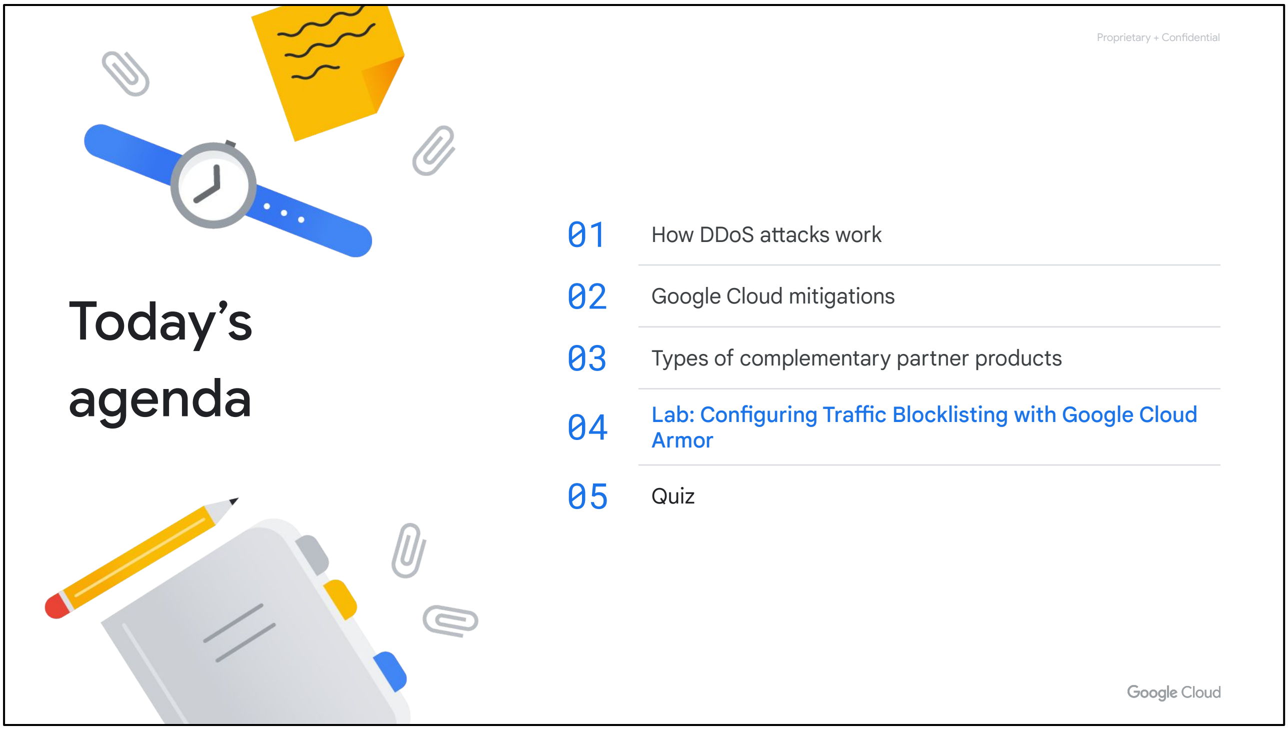
MetricStream

RedLock
Cloud Threat Defense

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

Google Cloud

Configuration, vulnerability, risk, and compliance partners can facilitate the visualization and inspection of your network and application deployments for vulnerabilities, security, and compliance risks, and assist with remediation.



Proprietary + Confidential

Today's agenda

01 How DDoS attacks work

02 Google Cloud mitigations

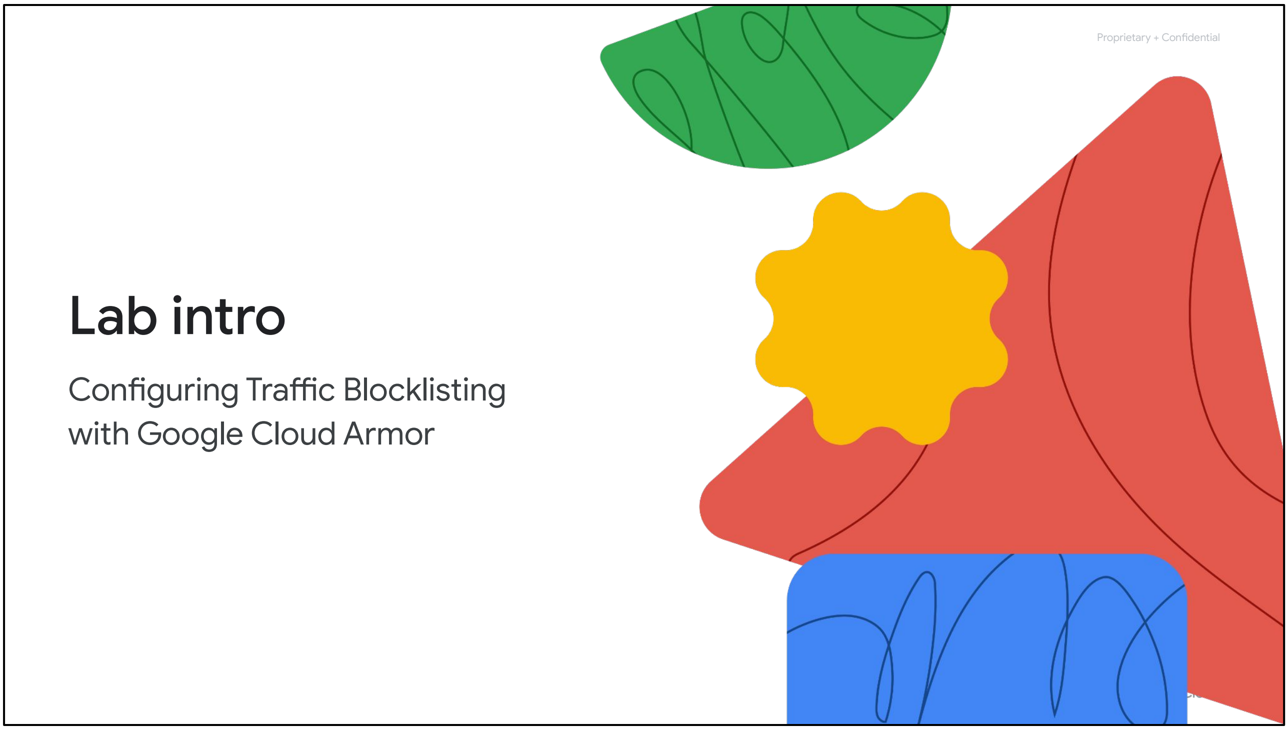
03 Types of complementary partner products

04 Lab: Configuring Traffic Blocklisting with Google Cloud Armor

05 Quiz

Google Cloud

Next, you will see Google Cloud Armor in action.



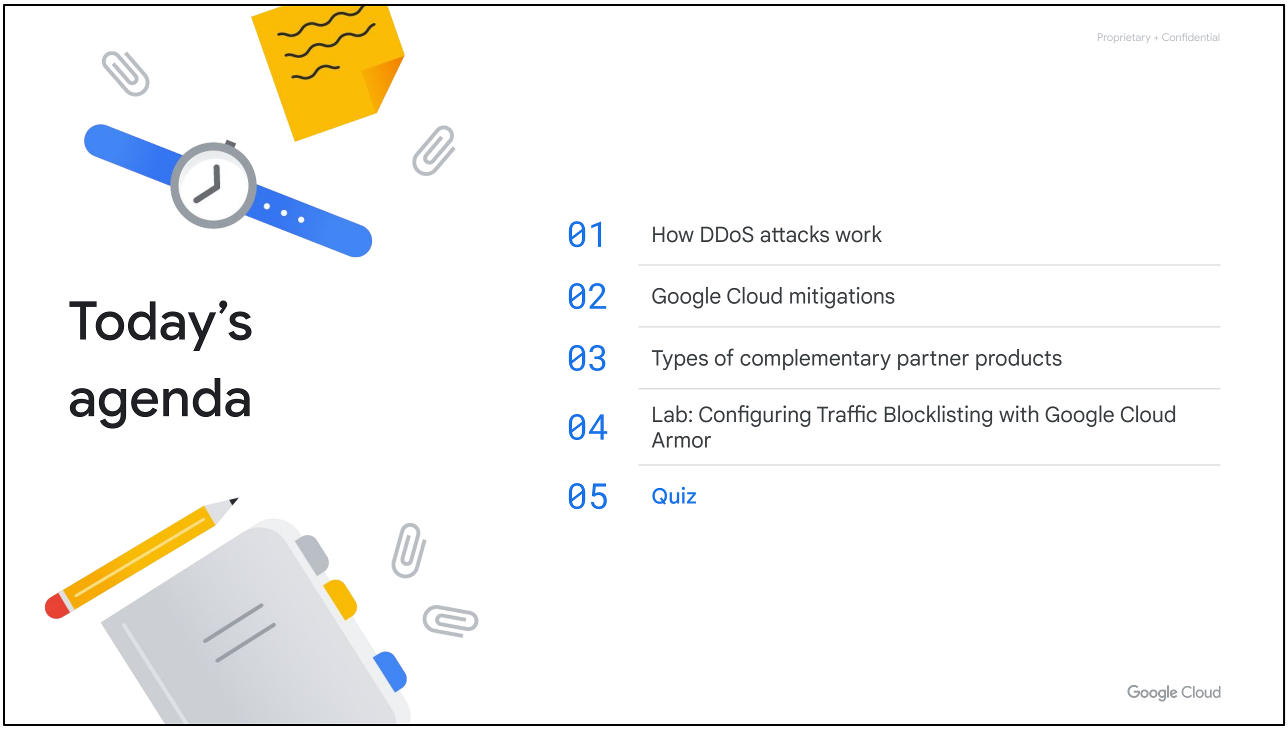
Proprietary + Confidential

Lab intro

Configuring Traffic Blocklisting with Google Cloud Armor

In this lab, you will perform the following tasks:

- Configure an Application Load Balancer for a simple web application,
- And use Google Cloud Armor to blocklist an IP address and restrict access to an Application Load Balancer



Proprietary + Confidential

Today's agenda

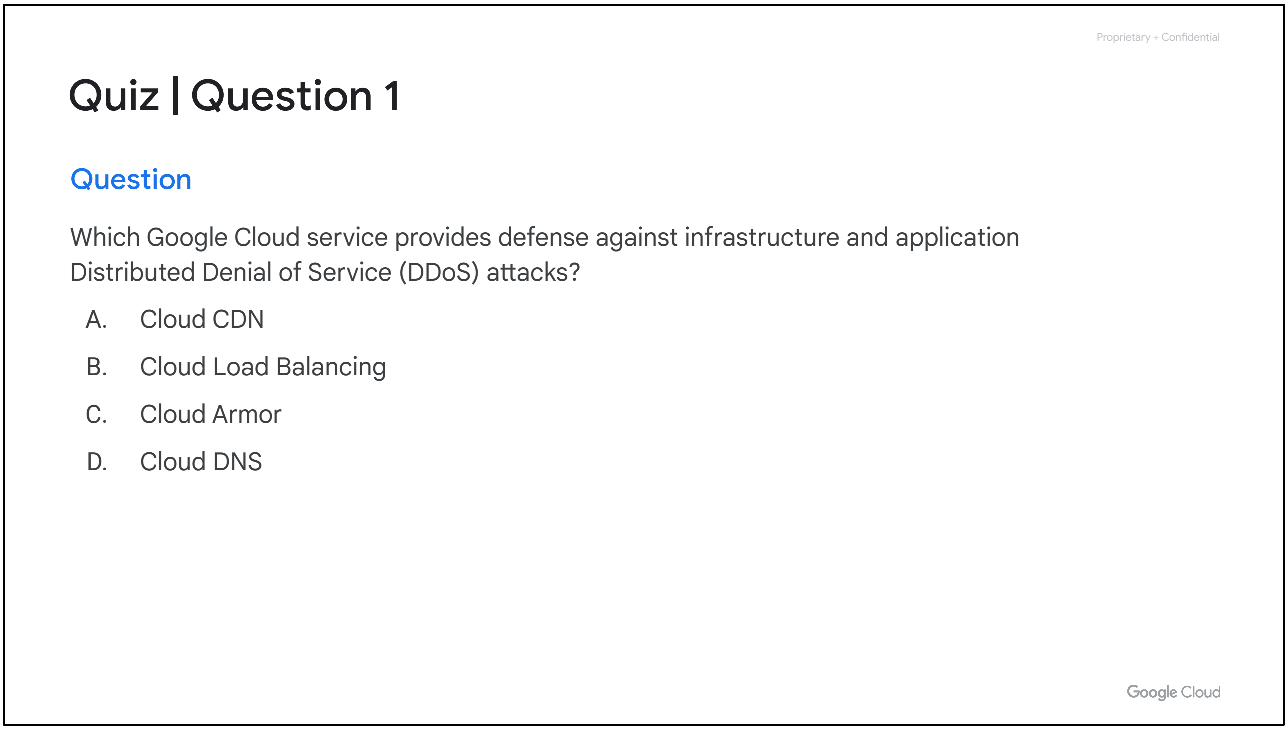
01 How DDoS attacks work

02 Google Cloud mitigations

03 Types of complementary partner products

04 Lab: Configuring Traffic Blocklisting with Google Cloud Armor

05 Quiz



Proprietary + Confidential

Quiz | Question 1

Question

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

A. Cloud CDN

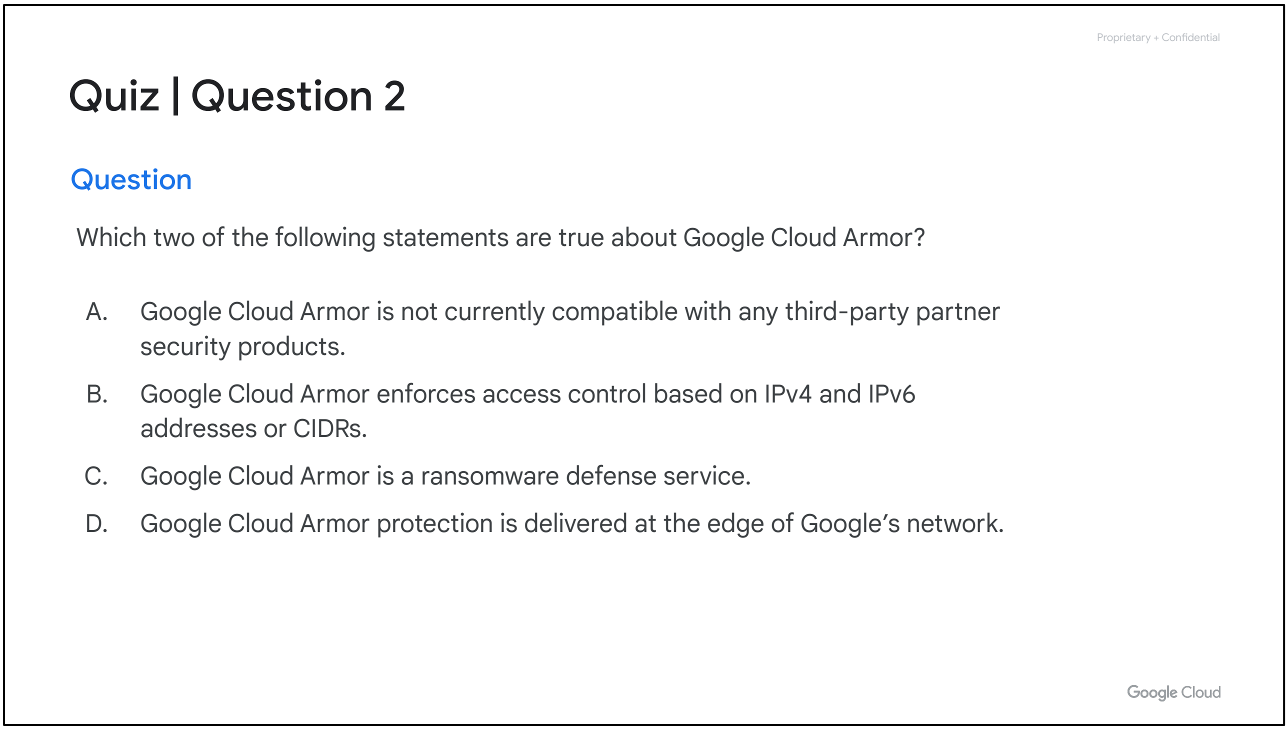
B. Cloud Load Balancing

C. Cloud Armor

D. Cloud DNS

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

(a) Cloud CDN
(b) Cloud Load Balancing
(c) Google Cloud Armor
(d) Cloud DNS



Proprietary + Confidential

Quiz | Question 2

Question

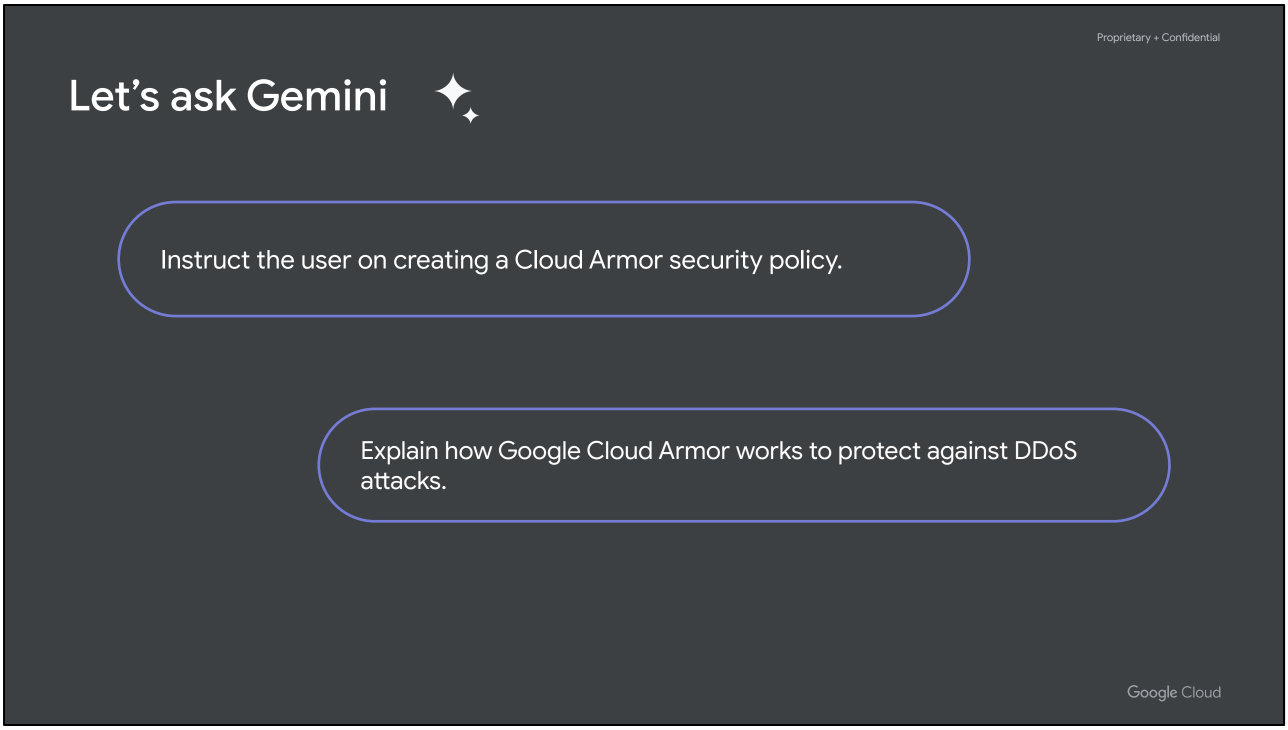
Which two of the following statements are true about Google Cloud Armor?

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.



Proprietary + Confidential

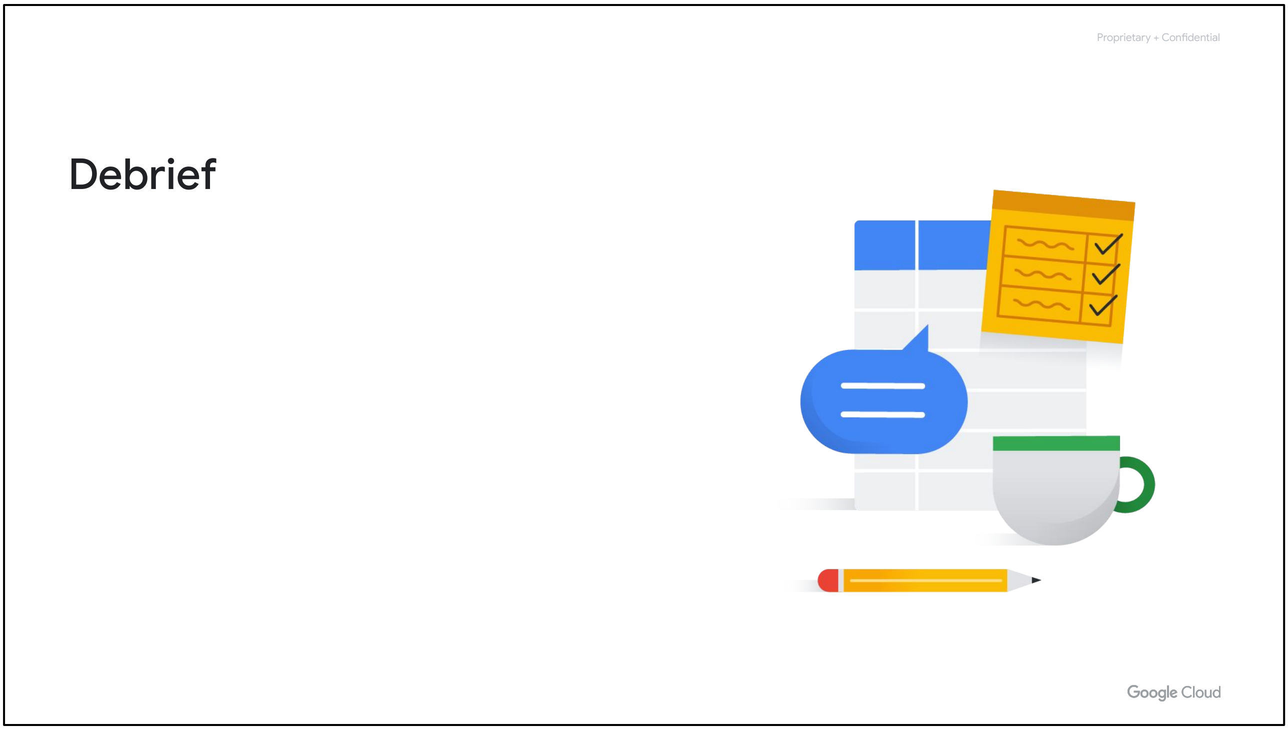
Let’s ask Gemini

Instruct the user on creating a Cloud Armor security policy.

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

Google Cloud

This concludes the module on DDoS protection. Before we wrap up, let's explore some useful Gemini prompts that can help you with related questions. The slide displays a few sample prompts to get you started.



Proprietary + Confidential

Debrief

Google Cloud

This module provided a comprehensive overview of Distributed Denial of Service (DDoS) attacks, their mechanisms, and how Google Cloud Armor effectively mitigates them. You learned about the various types of DDoS attacks and Google Cloud's multi-layered protection approach. Additionally, you explored complementary partner products that can enhance your defense strategy. In the hands-on lab, you configured Traffic Blocklisting with Google Cloud Armor, and a quiz reinforced your understanding of the key concepts covered in this module.

Thank you.

THANK YOU