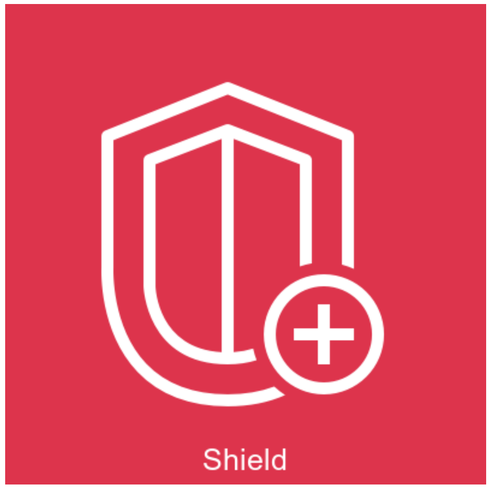
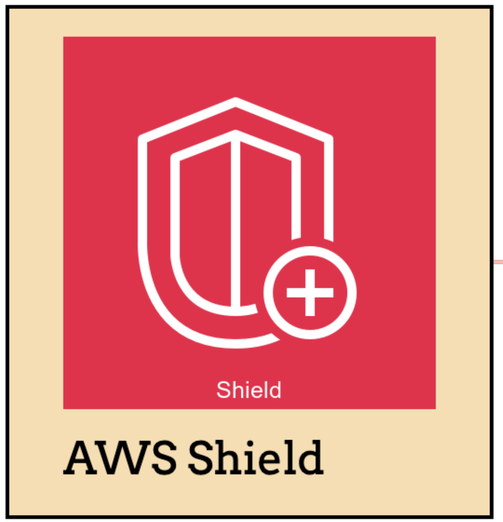
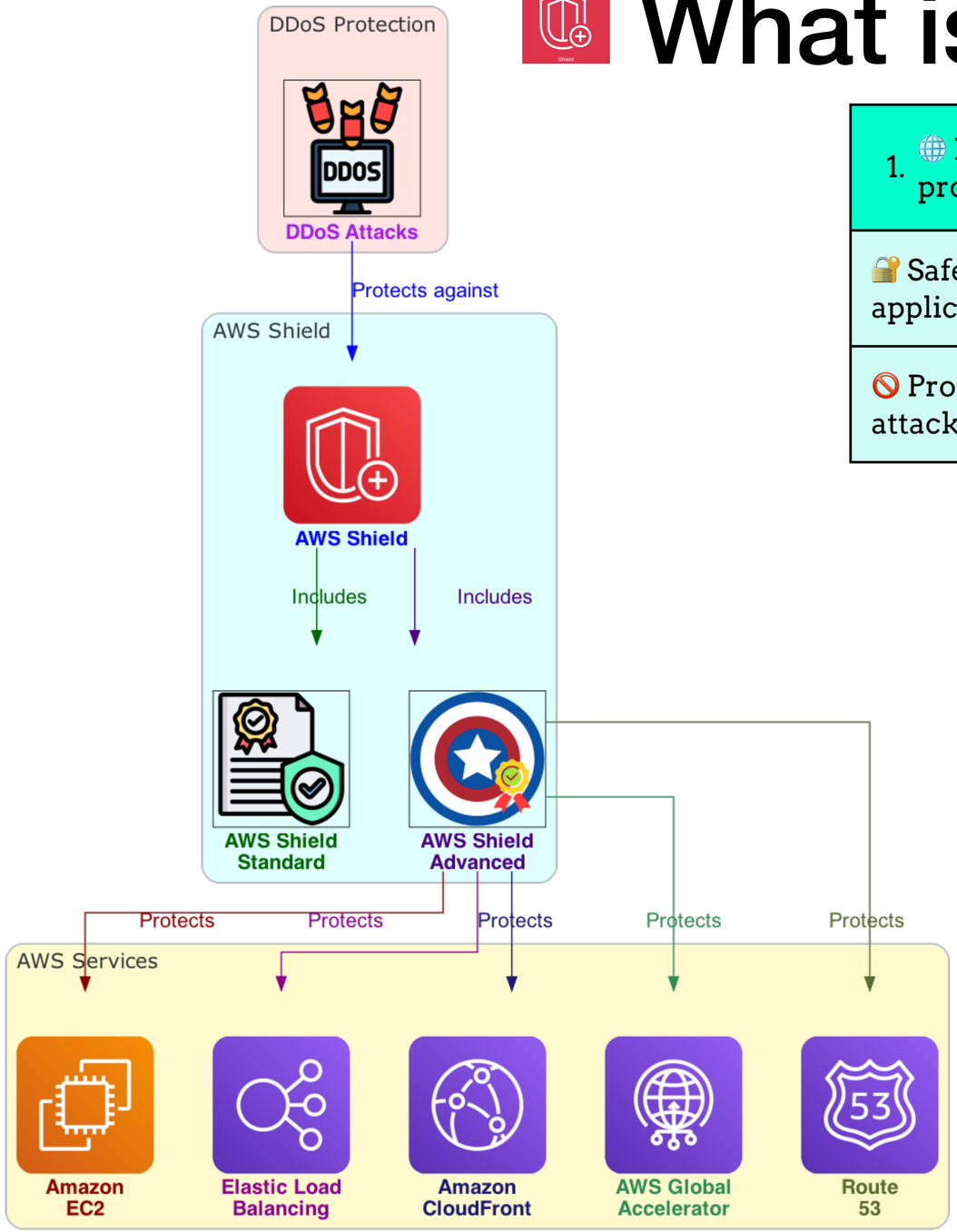


AWS Shield

Table of Contents



What is AWS Shield?



1. 🌐 Managed DDoS protection service

🔐 Safeguards AWS applications

🚫 Protects against DDoS attacks

2. 🆓 AWS Shield Standard: Free for all customers

🔓 Automatic enablement

🛡️ Basic DDoS protection

3. 💰 AWS Shield Advanced: Optional paid service

🔝 Enhanced features, benefits

🔒 Higher levels of protection

4. 🔒 Advanced protection for sophisticated attacks

🧩 Safeguards against complex attacks

📈 Handles larger-scale DDoS attacks

🔐 Ensures security, availability

5. 🎯 Supports EC2, ELB, CloudFront, Global Accelerator, Route 53

🖥️ Protects Amazon EC2

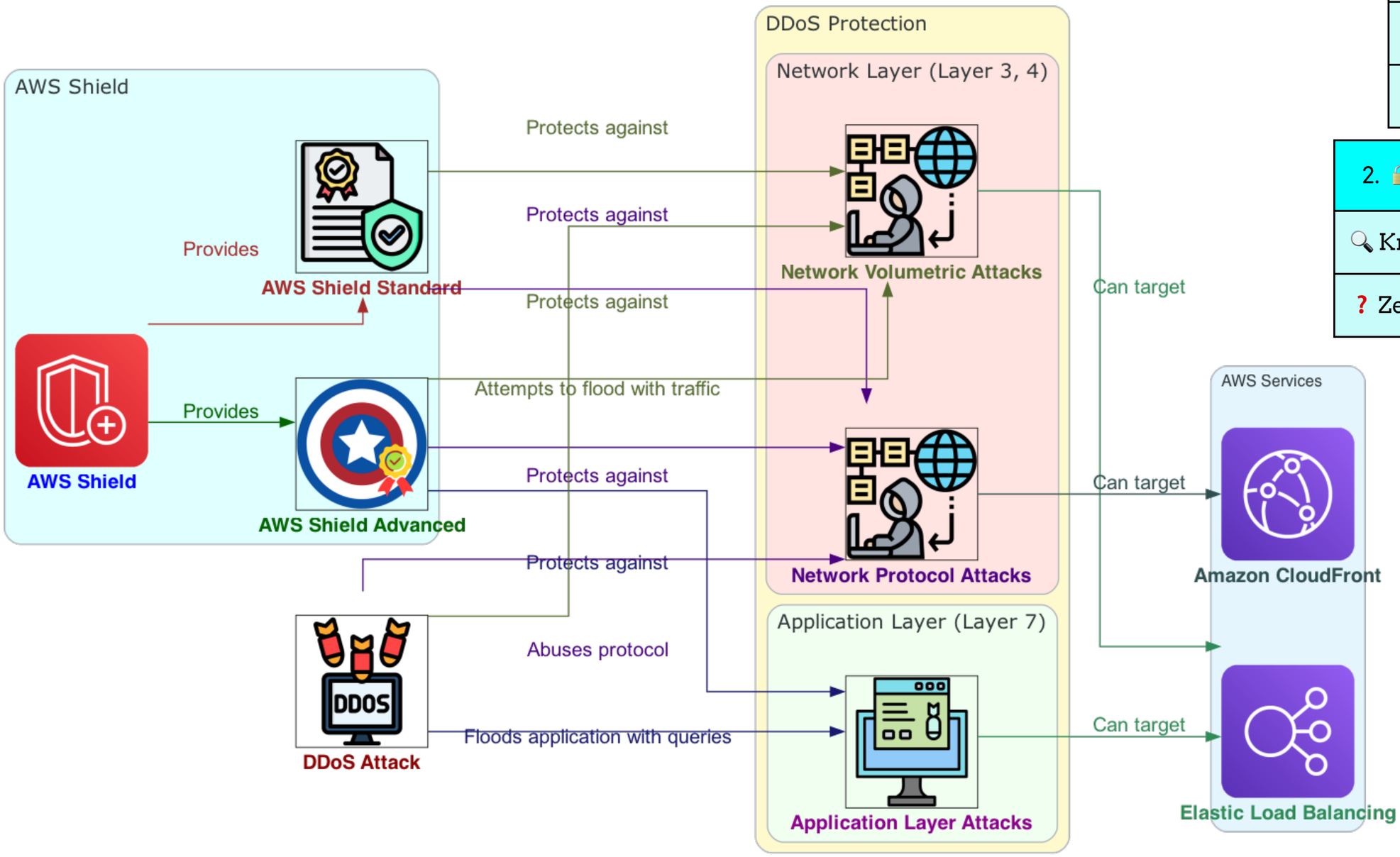
⚖️ Covers Elastic Load Balancing (ELB)

🌍 Safeguards Amazon CloudFront

🚀 Includes AWS Global Accelerator

🗺️ Extends to Amazon Route 53

How AWS Shield and Shield Advanced work



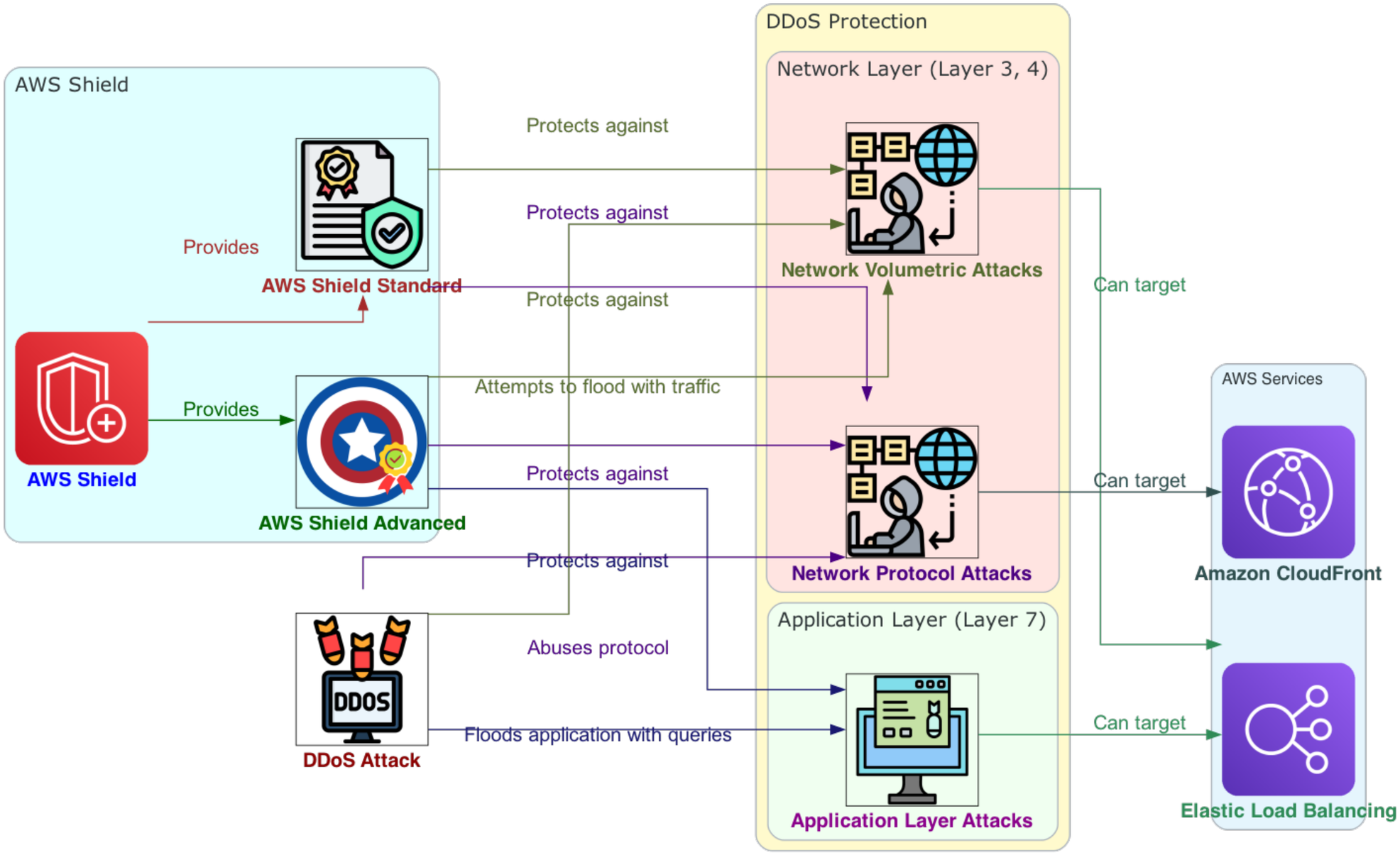
1. 🌐 Protects AWS resources
   - 🖥️ Network layer
   - 🚚 Transport layer
   - 💻 Application layer

2. 🔒 Defends against DDoS attacks
   - 🔍 Known attack vectors
   - ❓ Zero-day attack vectors

3. 🆓 Shield Standard
   - 🔓 Automatic enablement
   - 💸 Free protection
   - 🛡️ Basic DDoS protection

4. 💪 Shield Advanced
   - 💰 Optional paid service
   - 🔝 Enhanced features
   - 🔒 Higher security levels

How AWS Shield and Shield Advanced work



5. 🎯 Detects network volumetric attacks (Layer 3)

🌊 Attempts to saturate network capacity

🚫 Denies service to legitimate users

6. 🔍 Identifies network protocol attacks (Layer 4)

🌐 Example: TCP SYN floods

😨 Exhausts connection states on resources

7. 🔐 Safeguards against application layer attacks (Layer 7)

🌐 Example: Web request floods

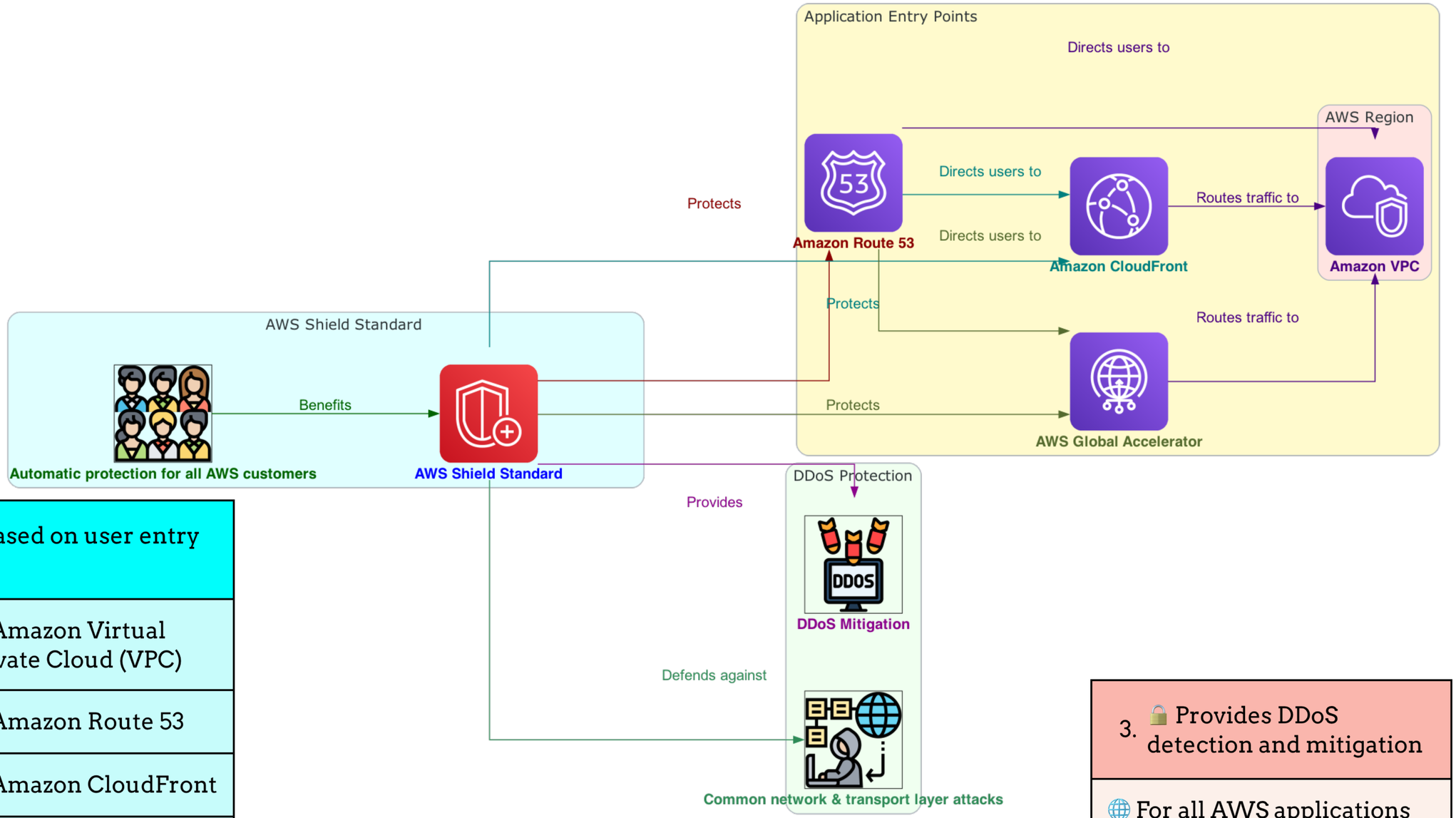
🚫 Denies service to legitimate users

AWS Shield Standard Overview

1. 🌐 Protects application perimeter

🔍 Managed threat protection service

🎯 Safeguards first point of entry



2. 🚀 Determines perimeter based on user entry point

☁️ AWS Region	🔒 Amazon Virtual Private Cloud (VPC)
🌍 Edge of AWS network	🌐 Amazon Route 53
	📡 Amazon CloudFront
	⚡ AWS Global Accelerator

3. 🔒 Provides DDoS detection and mitigation

🌐 For all AWS applications

🛡️ Protects against threats

AWS Shield Standard Overview

4. 🏗️ Application architecture influences DDoS resiliency

📐 Design decisions impact resiliency

💪 Ability to operate during an attack

5. 🆓 Automatic protection for all AWS customers

💸 No additional charge

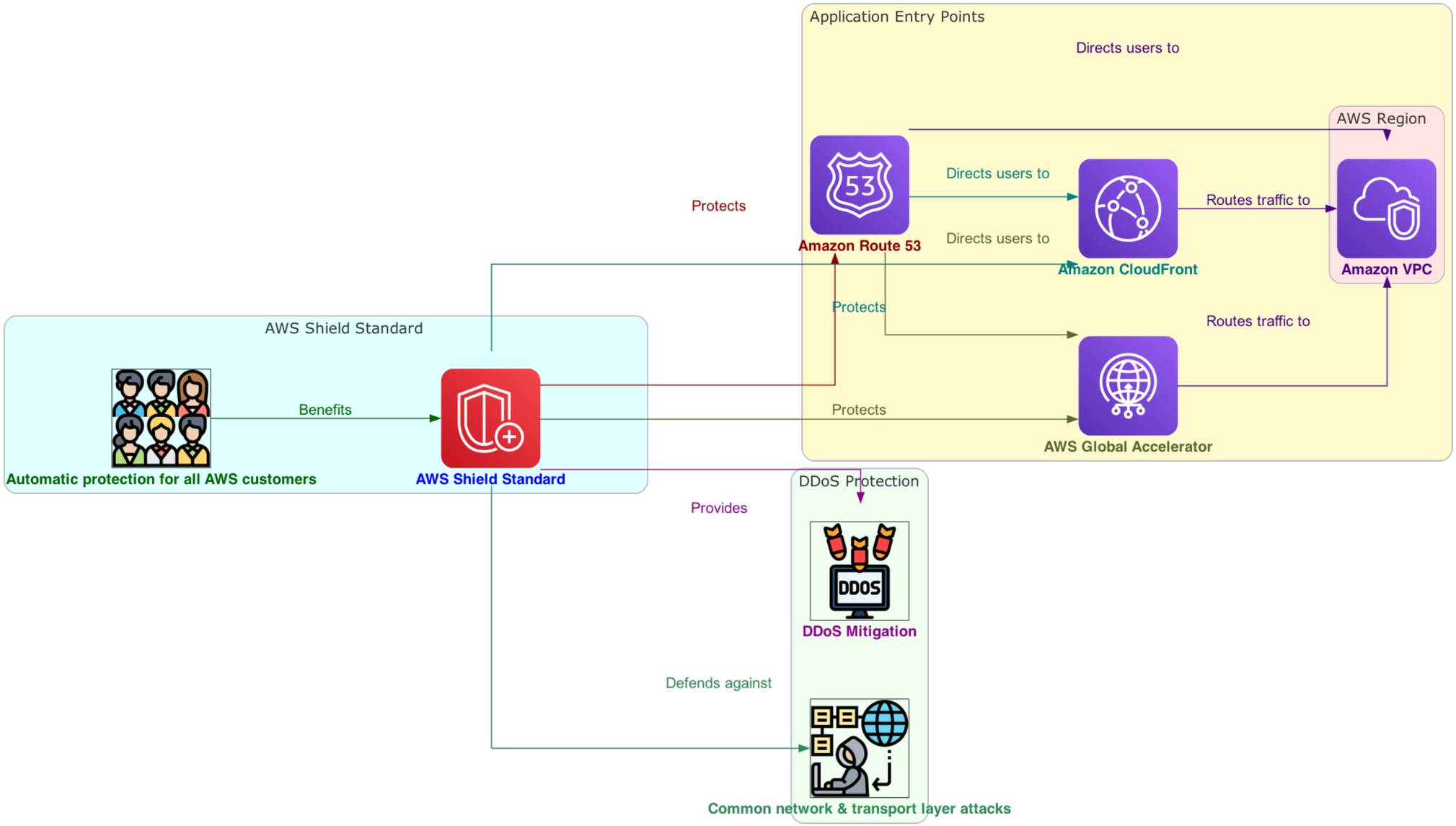
6. 🔝 Comprehensive protection

🌐 Amazon Route 53 hosted zones

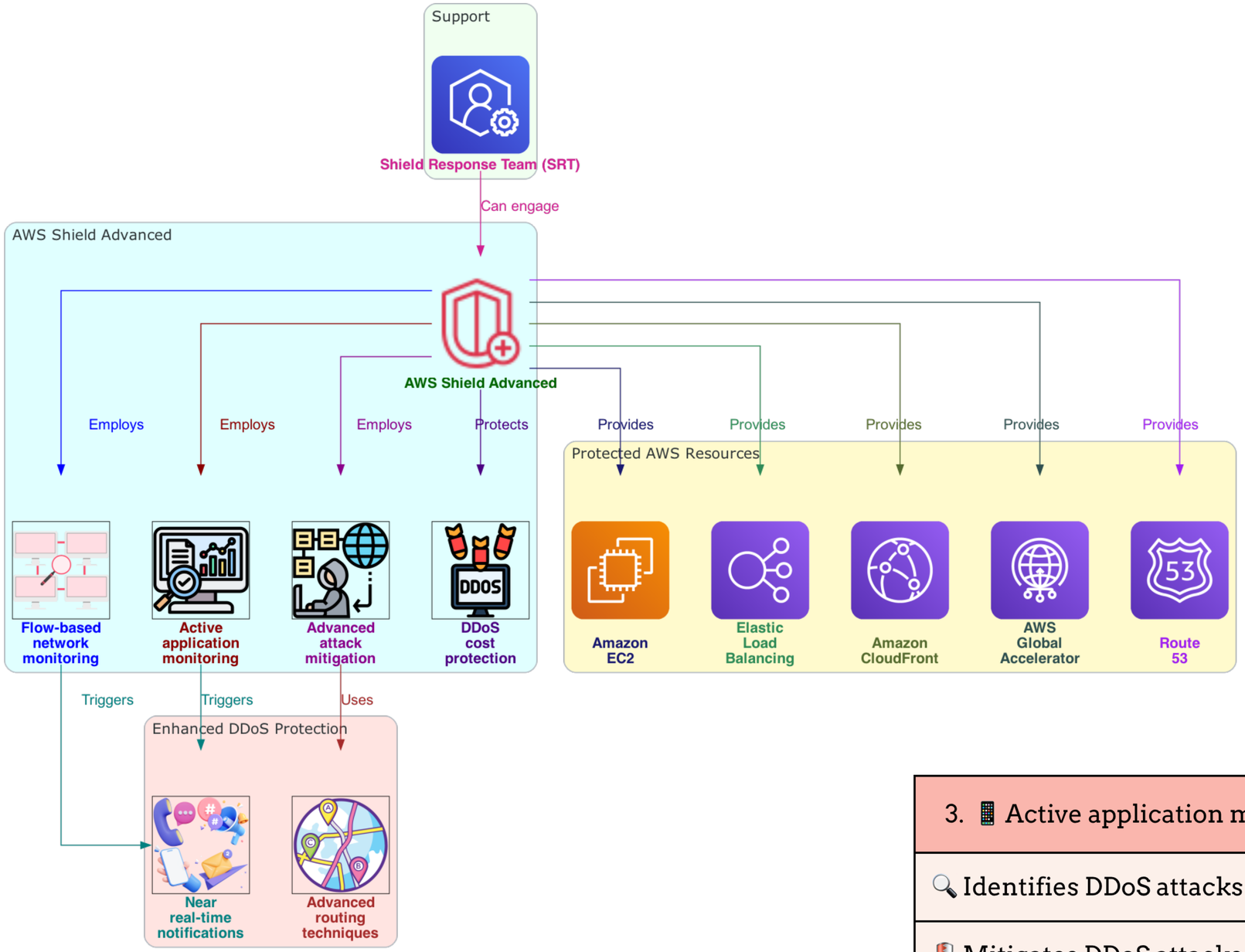
📡 Amazon CloudFront distributions

⚡ AWS Global Accelerator standard accelerators

🛡️ Against known network and transport layer attacks



AWS Shield Advanced Overview



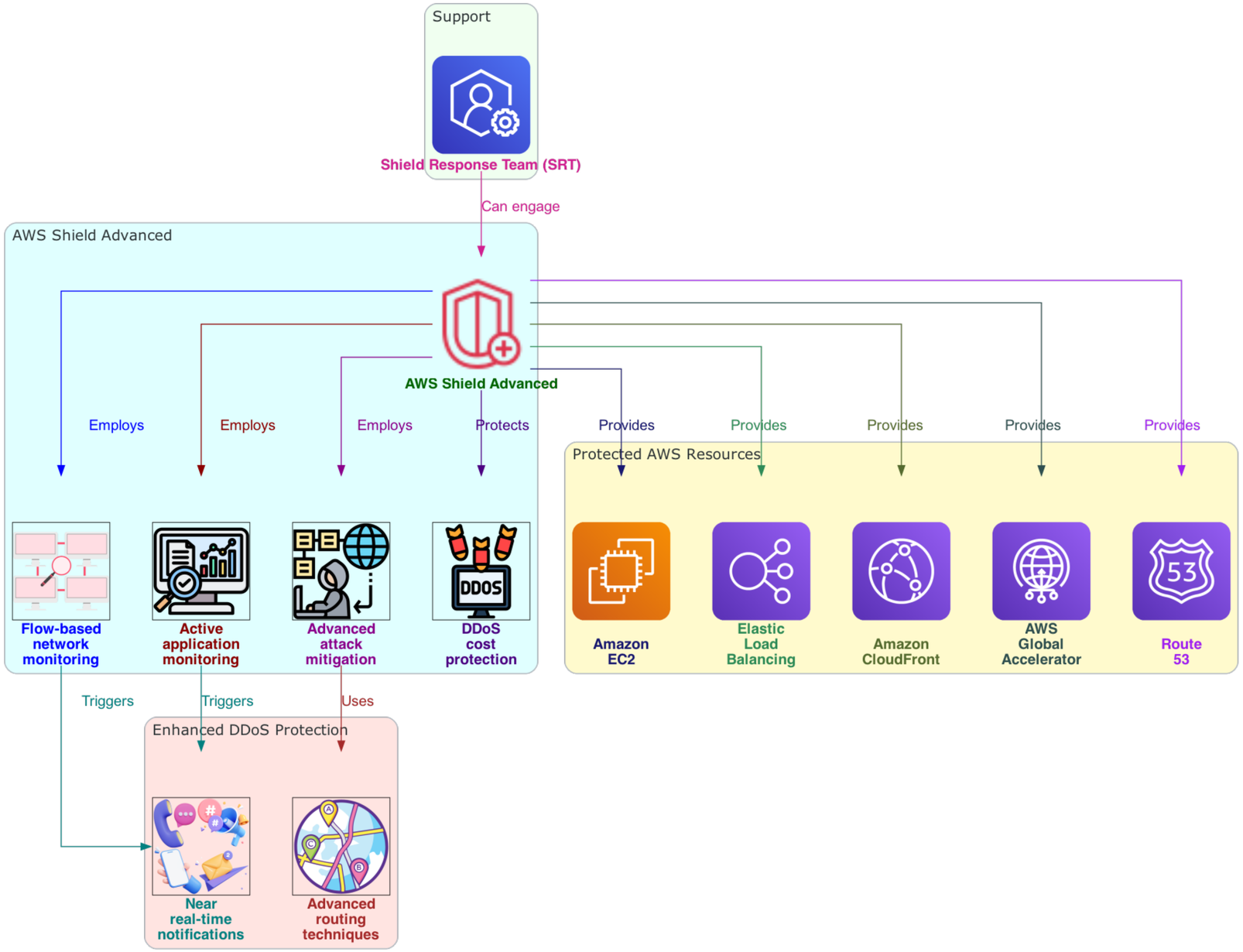
1. 🔒 Protects AWS resources
   - 🖥️ Amazon EC2
   - ⚖️ Elastic Load Balancing (ELB)
   - 🌐 Amazon CloudFront
   - ⚡ AWS Global Accelerator
   - 🗺️ Route 53

2. 🌐 Always-on, flow-based network monitoring
   - 🔍 Continuous monitoring
   - 🚨 Detects potential DDoS threats

3. 📱 Active application monitoring
   - 🔍 Identifies DDoS attacks
   - 🛡️ Mitigates DDoS attacks

4. 🚨 Near real-time notifications
   - ⏰ Timely alerts
   - 🔍 Detects potential DDoS attacks
   - 🏃 Allows quick response and mitigation

AWS Shield Advanced Overview



5. 🔧 Advanced attack mitigation and routing techniques

- 🤖 Automatically mitigates DDoS attacks
- 🗺️ Optimizes traffic routing

6. 🛠️ 24x7 Shield Response Team (SRT) support

- 💼 For Business or Enterprise customers
- ⏰ Around-the-clock support
- 🔧 Manages and mitigates application layer DDoS attacks

7. 💰 DDoS cost protection for scaling during attacks

- 🔒 Protects AWS bill against higher fees
- 📈 Due to usage spikes from protected resources
- 💸 Ensures cost control and predictability

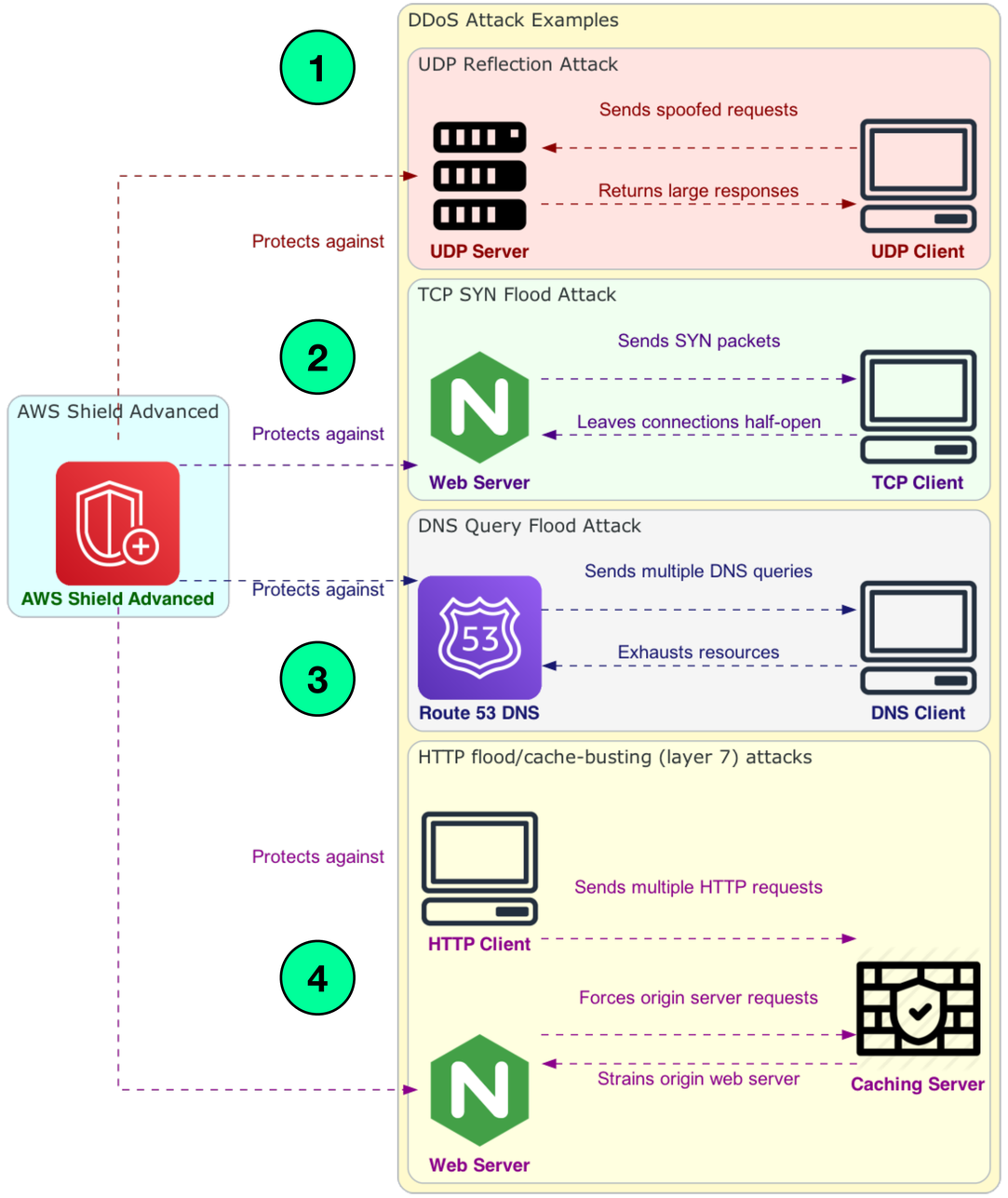
Examples of DDos Attacks

1. 🌐 User Datagram Protocol (UDP) reflection attacks
🤹 Attacker spoofs request source
📡 Uses UDP to elicit large response from server
🚦 Extra traffic slows targeted server
🚫 Prevents access for legitimate users

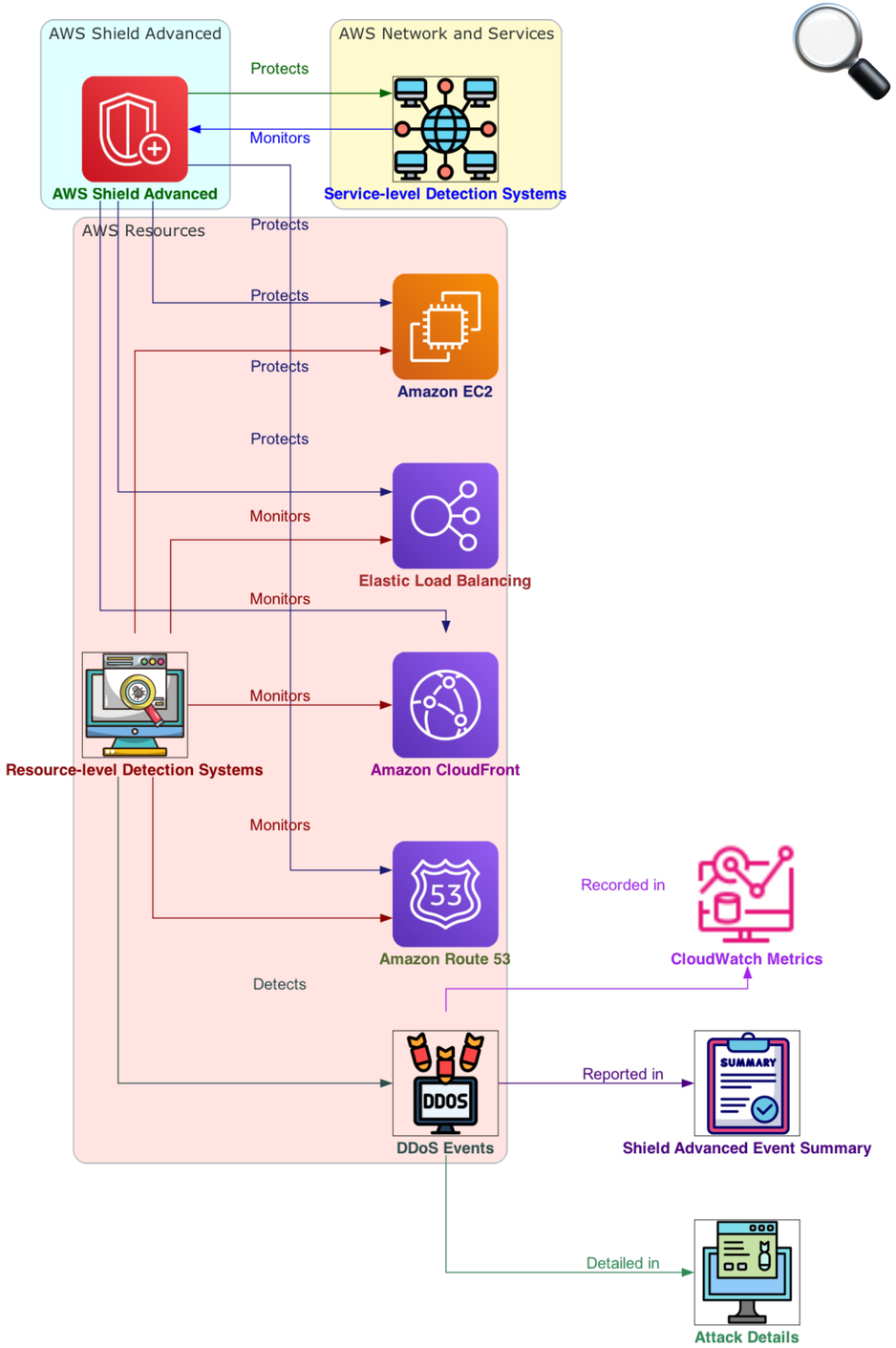
2. 🌊 TCP SYN flood
😨 Exhausts system resources
🔄 Leaves connections half-open
🤝 Exploits three-way handshake
🚫 Prevents other users from connecting

3. 🌐 DNS query flood
🔍 Attacker uses multiple DNS queries
😨 Exhausts DNS server resources
🛡️ AWS Shield Advanced protects Route 53

4. 🌊 HTTP flood/cache-busting (layer 7) attacks
🌐 Attacker sends multiple HTTP requests
😳 Requests appear from real user
💥 Cache-busting prevents use of cached content
🖥️ Forces content to be served from origin server
😨 Strains origin web server



🔍 How AWS Shield Detects Events



1. 🌐 Service-level detection systems

🔍 For AWS network and services

🎯 Ensures availability during DDoS attacks

2. 🎯 Resource-level detection systems

🔍 For individual AWS resources

🚦 Ensures traffic remains within expected parameters

3. 🛡️ Combination protects targeted resources and services

🚫 Drops known bad packets

🚨 Highlights potentially malicious traffic

✅ Prioritizes traffic from end users

4. 📊 Detected events appear in

📝 Shield Advanced event summaries

🔍 Attack details

📈 CloudWatch metrics

5. 🏷️ Events labeled with

🎯 DDoS attack vector name

📊 'Volumetric' if based on traffic volume

How AWS Shield Mitigates Events

1. 🌐 Mitigation logic varies by application architecture

🎯 Adapts based on application architecture

2. 🌍 Web and DNS use case mitigations

☁️ Amazon CloudFront

🌐 Route 53

🔒 Protects all associated services

3. 🌟 Resource-specific mitigations in AWS Regions

🏷️ Based on service and resource type

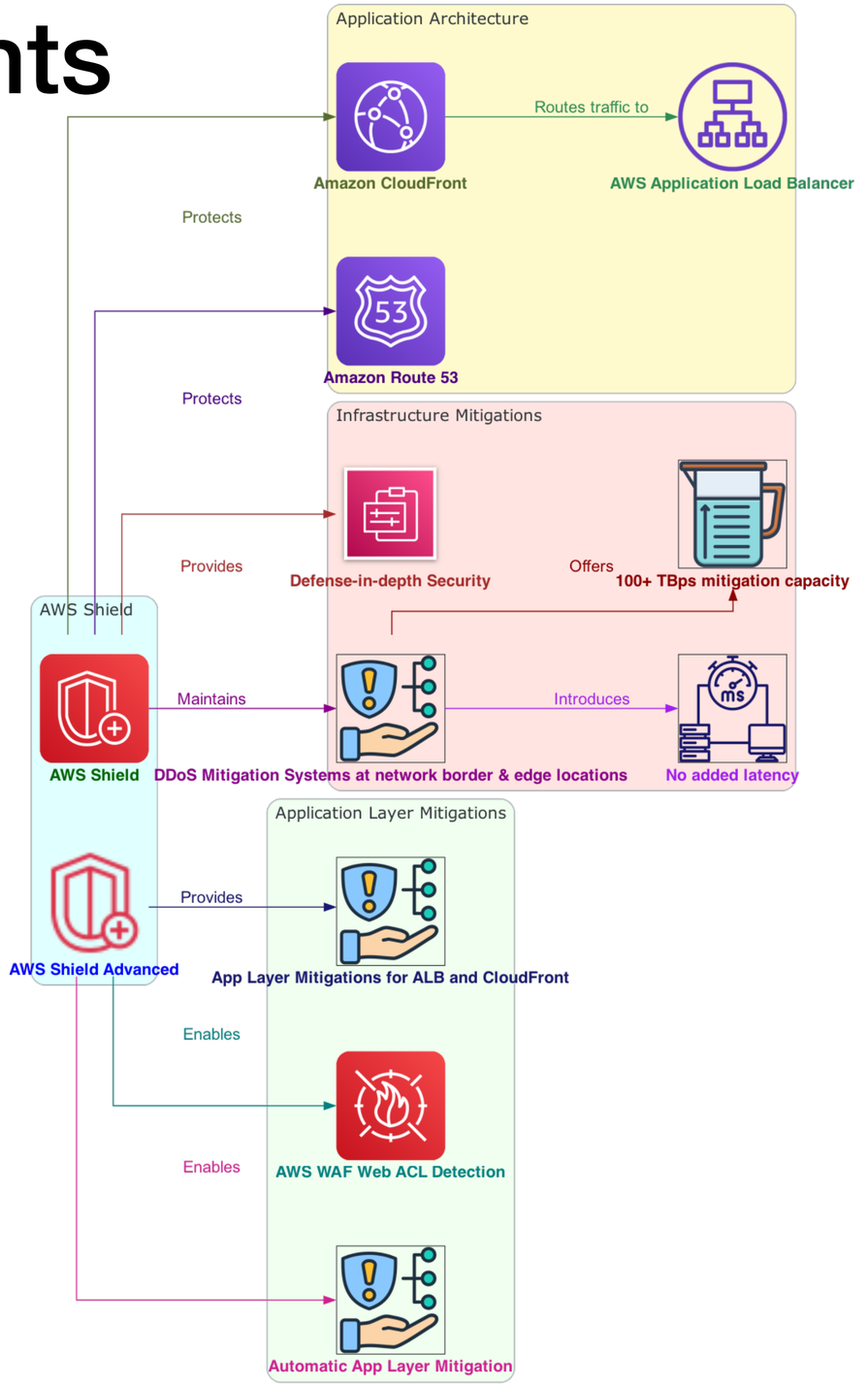
4. 🛠️ Infrastructure mitigations for layer attacks

🔒 DDoS mitigation systems

5. 🔄 DDoS mitigation systems at network border

🌐 Present at AWS network borders and edge locations

🔄 Reroutes traffic through mitigation systems



How AWS Shield Mitigates Events

6. 🚫 No additional latency or traffic rerouting

⚡ Reroutes traffic without latency

🚫 No external scrubbing centers

7. 💪 Over 100 Tbps mitigation capacity

🌐 Across all AWS Regions and edge locations

8. 🛡️ Application layer mitigations with Shield Advanced

☁️ Protects CloudFront distributions

⚖️ Protects Application Load Balancers

9. 🔒 Web ACL and automatic application layer mitigation

🤖 Enables automatic application layer mitigation

🔒 Uses AWS WAF web ACLs

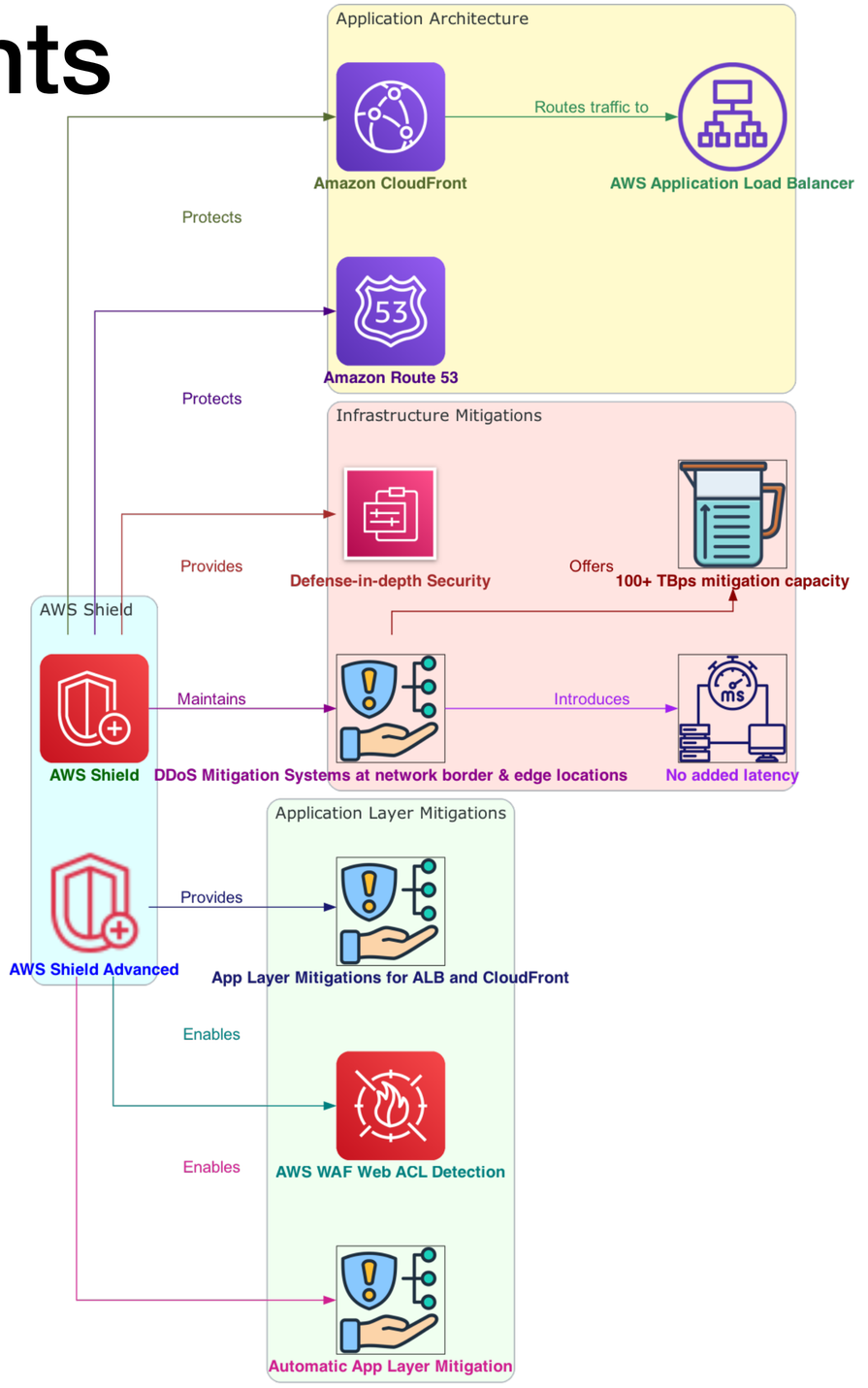
🛡️ Manages protections during DDoS attacks

10. 🚀 Custom mitigations for specific resources

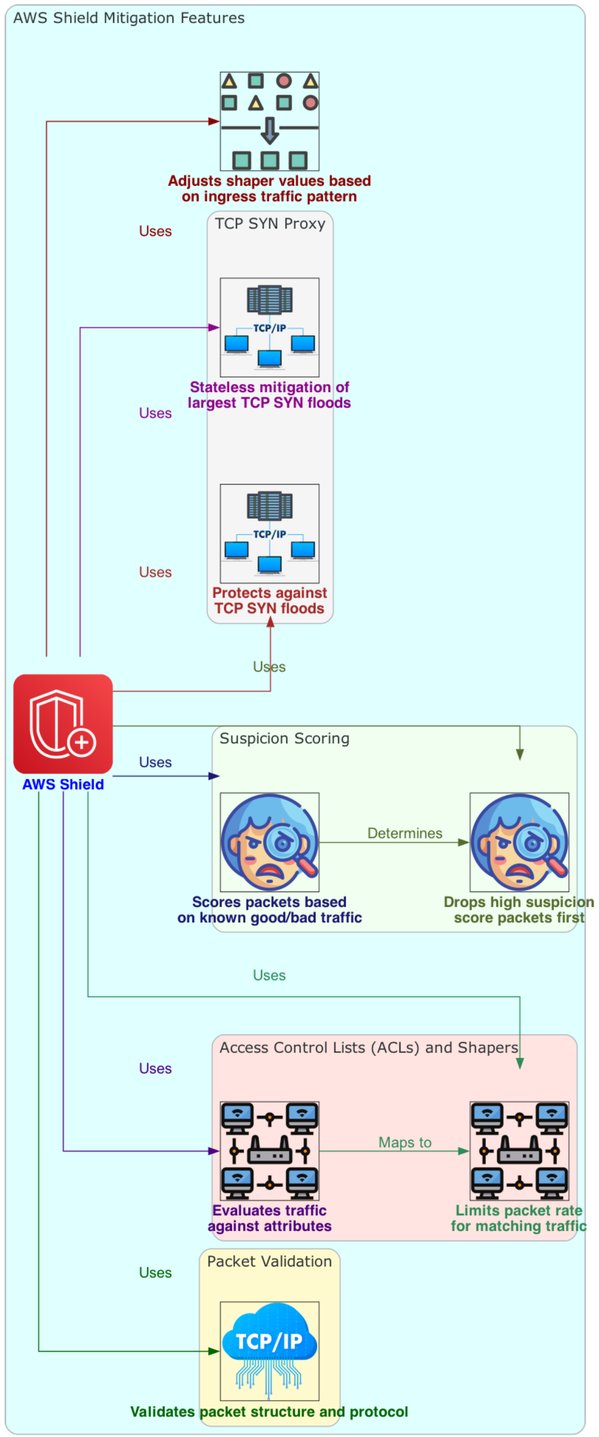
🛡️ Provides custom mitigations

🚦 Enforces rate limiting for application layer attacks

🔒 Protects specific resources



Mitigation Features

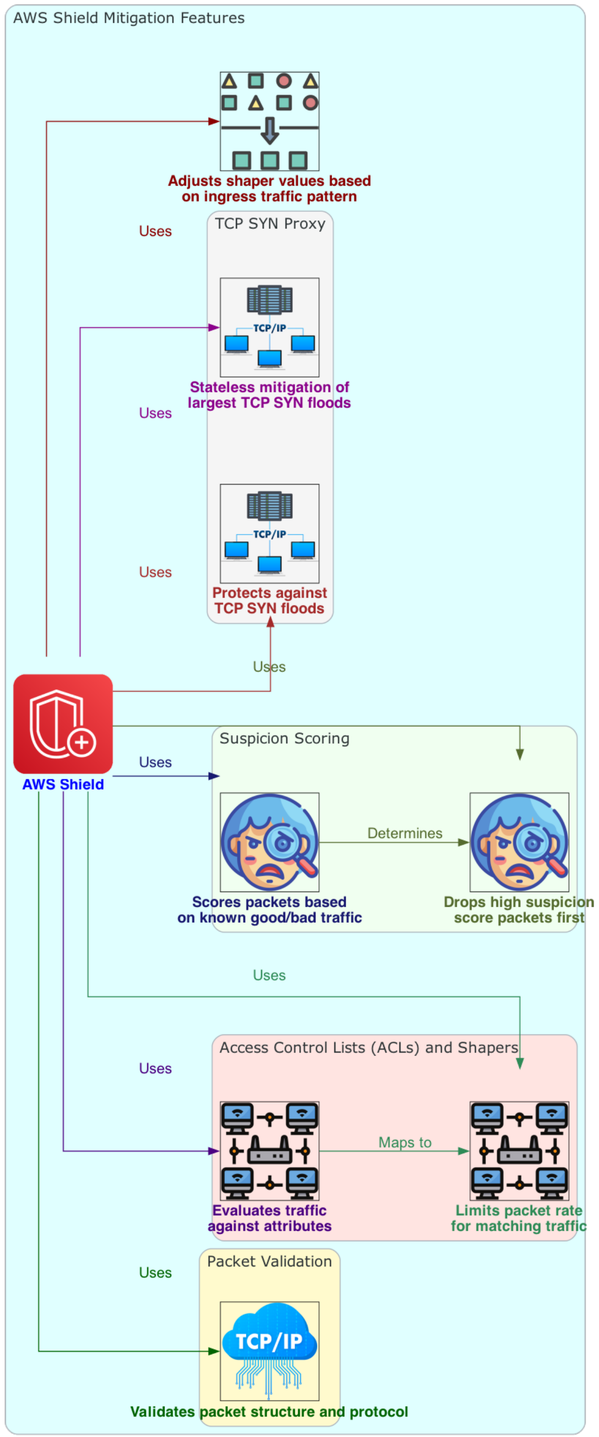


1. 📦 Packet validation
🔍 Inspects packet structure and protocol
✅ Supported protocols: IP, TCP, UDP, ICMP, DNS, NTP

2. 📝 Access Control Lists (ACLs) and shapers
🔍 ACL evaluates traffic against attributes
🚫 Drops matching traffic or maps to shaper
🚦 Shaper limits packet rate, drops excess
🎯 Dedicated rate allocations for expected/known DDoS traffic
🔍 ACL matches port, protocol, TCP flags, destination, source country, payload patterns

3. 🕵️ Suspicion scoring
📊 Scores packets based on expected traffic knowledge
👍 Lower score for known good traffic patterns
👎 Higher score for known bad traffic attributes
🚫 Drops high suspicion score packets first when rate limiting
🛡️ Mitigates known and zero-day DDoS attacks
❎ Avoids false positives

Mitigation Features



4. 🔒 TCP SYN proxy
🛡️ Protects against TCP SYN floods
🍪 Sends TCP SYN cookies to challenge new connections
📦 Stateless mitigation of largest TCP SYN flood attacks
🤝 Integrates with AWS services to hand off connection state
☁️ Available on Amazon CloudFront and Route 53

5. 📊 Rate distribution
🔄 Continuously adjusts per-location shaper values
🚦 Based on ingress traffic pattern toward protected resource
🚫 Prevents rate limiting of unevenly distributed customer traffic

Thanks for Watching