AWS pruža širok spektar sigurnosnih usluga koje vam pomažu da zaštitite svoje podatke, upravljate pristupom vašim resursima, konfigurišete sigurnosna upozorenja i automatizujete sigurnosne provere. Neke od najvažnijih AWS sigurnosnih servisa ukljucuju:

1. AWS Identity and Access Management (IAM): IAM se koristi za sigurno upravljanje pristupom AWS uslugama i resursima. Sa IAM-om, možete kreirati i upravljati AWS korisnicima i grupama, i koristiti dozvole da dozvolite i uskratite njihov pristup AWS resursima. Omogućava vam da različitim korisnicima dodelite različite dozvole za različite resurse, primenjujući princip najmanje privilegije (Least Privilege Principle),

2. AWS GuardDuty: GuardDuty je usluga za detekciju pretnji koja konstantno prati maliciozna ili neautorizovana ponašanja kako bi pomogla u zaštiti AWS naloga i aplikacija. Koristi mašinsko učenje, detekciju anomalija I sakupljene informacije da identifikuje i prioritetizuje potencijalne pretnje.

3. AWS Web Application Firewall (WAF): AWS WAF je web aplikacijski firewall koji pomaže u zaštiti web aplikacija od uobičajenih web eksploatacija koje bi mogle uticati na dostupnost aplikacija, kompromisovati sigurnost ili trošiti prekomerne resurse. AWS WAF vam daje kontrolu nad tim kako saobraćaj dolazi do vaših aplikacija tako što vam omogućava da kreirate sigurnosna pravila koja blokiraju uobičajene obrasce napada, kao što su SQL injection ili cross-site scripting (XSS).

4. AWS Key Management Service (KMS): KMS je usluga koja olakšava kreiranje i kontrolu kriptografskih ključeva koji se koriste za enkripciju podataka. Pruža centralizovanu kontrolnu tačku za upravljanje vašim kriptografskim ključevima i nudi jednostavnu integraciju sa ostalim AWS uslugama.

5. AWS Shield: AWS Shield je usluga koja pruža zaštitu od DDoS napada i koja štiti aplikacije koje se izvršavaju na AWS-u. Shield pruža stalnu detekciju i automatsko “inline” ublažavanje (deluje direktno na protok mrežnog saobraćaja, bez potrebe za bilo kakvom ručnom intervencijom) kako bi zaštitio vaše aplikacije od DDoS napada.

6. AWS Secrets Manager: AWS Secrets Manager pomaže da zaštitite pristup svojim aplikacijama, uslugama i IT resursima. Ova usluga vam omogućava da lako rotirate, upravljate i preuzimate kredencijale baze podataka, API ključeve i druge tajne tokom njihovog životnog ciklusa.

7. AWS Security Hub: AWS Security Hub vam daje sveobuhvatan pregled vaših visokoprioritetnih sigurnosnih upozorenja i statusa usklađenosti preko AWS naloga. Agregira, organizuje i prioritetizuje vaša sigurnosna upozorenja, ili nalaze, iz više AWS usluga i rešenja AWS partnera.

**AWS IAM**

AWS Identity and Access Management (IAM) je web servis koji pomaže u sigurnom kontrolisanju pristupa AWS resursima. Omogućava vam upravljanje dozvolama i kontrolu ko je autentifikovan i ovlašćen da koristi resurse na vašem AWS nalogu. Ključne karakteristike IAM-a su:

• Centralizovana kontrola pristupa: IAM omogućava centralizovano upravljanje pristupom vašim AWS resursima. Možete kreirati korisnike, grupe, uloge i definisati njihove dozvole na jednom mestu, što olakšava upravljanje i nadzor pristupa vašim resursima.

• Granularne dozvole: IAM vam omogućava da različitim korisnicima dodelite različite dozvole za različite resurse. Možete dodeliti pravila korisnicima, grupama i ulogama koje definišu ko može pristupiti kojim resursima i koje akcije mogu izvršavati. Ova granularnost omogućava vam primenu principa najmanjih privilegija, dajući korisnicima samo dozvole koje su im potrebne za izvršavanje njihovih zadataka.

• Siguran pristup AWS resursima: IAM pruža razne funkcionalnosti koje pomažu u obezbeđivanju pristupa AWS resursima. Na primer, možete primeniti Multi-Faktor Autentifikaciju (MFA) za svoje korisnike, dodajući dodatni sloj zaštite na vaš AWS nalog. IAM takođe omogućava redovno rotiranje sigurnosnih kredencijala, kao što su pristupni ključevi, kako bi se smanjio rizik od njihove kradje.

• Federacija identiteta: IAM podržava federaciju identiteta, omogućavajući korisnicima koji imaju identitete u pouzdanim eksternim sistemima, kao što su Microsoft Active Directory ili provajderi identiteta na webu, kao sto su Google ili Facebook, da pristupe AWS resursima bez potrebe za IAM korisničkim nalogom. Ovo pojednostavljuje upravljanje pristupom omogućavajući vam da upravljate korisnicima i njihovim dozvolama u vašem postojećem sistemu identiteta.

• IAM Korisnici: IAM korisnik je entitet koji kreirate u AWS-u da predstavlja osobu ili servis koji ga koristi za interakciju sa AWS-om. Korisnik u AWS-u se sastoji od imena i kredencijala.

• IAM Grupe: IAM grupa je kolekcija IAM korisnika. Grupe možete koristiti da odredite dozvole za kolekciju korisnika, što može olakšati upravljanje tim dozvolama za te korisnike.

• IAM Uloge I Pravila: IAM uloga je AWS identitet sa pravilima dozvola koja određuju šta identitet može i ne može da radi u AWS-u. Za razliku od korisnika ili grupa, uloge nemaju svoj stalni set kredencijala. Umesto toga, ako korisnik ili servis preuzme ulogu, privremene sigurnosne kredencijale se kreiraju i automatski rotiraju za tu ulogu. IAM pravilo je dokument koji definiše dozvole i može biti priključen IAM korisniku, grupi ili ulozi. Pravilo navodi koje su akcije dozvoljene ili odbijene na kojim AWS resursima.

{

"Version": "2012-10-17",

"Statement": [{

"Effect": "Allow",

"Action": [

"s3:Get\*",

"s3:List\*"

],

"Resource": "arn:aws:s3:::example\_bucket/\*"

}]

}

Policy 1: Primer IAM pravila

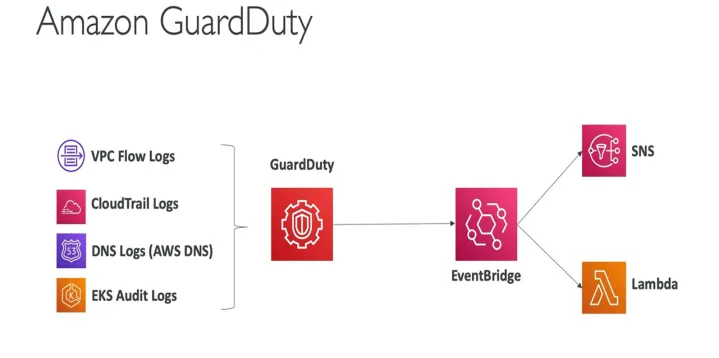
U ovom pravilu, Efekat je “Allow”, što znači da pravilo daje dozvole. Element “Action” navodi akcije koje su dozvoljene. U ovom slučaju, dozvoljene su sve akcije koje počinju sa "s3:Get" i "s3:List", što su akcije koje se odnose na čitanje podataka iz S3 korpe. Element “Resource” navodi resurse na koje se pravilo primenjuje. U ovom slučaju, pravilo se primenjuje na sve objekte u korpi "example\_bucket".

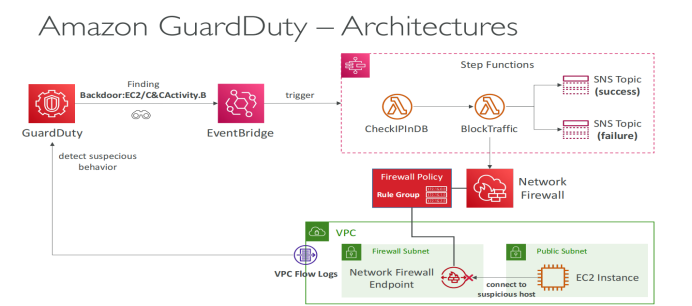
**AWS GuardDuty**

Amazon GuardDuty je servis za detekciju pretnji koji kontinuirano prati maliciozno ili neautorizovano ponašanje kako bi pomogao u zaštiti vaših AWS naloga I resursa. Koristi mašinsko učenje, detekciju anomalija i integrisanu pretnju inteligencije kako bi identifikovao i prioritetizovao potencijalne pretnje.

Ključne karakteristike GuardDuty-a:

* Kontinuirano praćenje i detekcija pretnji: GuardDuty prati neuobičajenu ili neautorizovanu aktivnost, kao što je rudarenje kriptovaluta, neuobičajene API pozive, ili potencijalno neautorizovane implementacije. Ovo pomaže da se pretnje identifikuju rano i brzo se reaguje.
* “Integrated Threat Intelligence”: GuardDuty koristi feed-ove pretnji, kao što su liste poznatih malicioznih IP adresa i domena, i primenjuje algoritme mašinskog učenja kako bi detektovao anomalije. Identifikuje poznate pretnje brže i smanjuje šanse za pogrešne detekcije.
* Detekcija pretnji na nivou naloga i resursa: GuardDuty može detektovati pretnje i neočekivano ponašanje na nivou naloga i za individualne resurse. Ovo pruža sveobuhvatni pregled vaše bezbednosne pozicije u AWS-u.
* Jednostavan za podešavanje: GuardDuty može biti omogućen sa samo nekoliko klikova u AWS Konzoli. Nema softvera ili hardvera za implementaciju ili održavanje, što ga čini jednostavnim i ekonomičnim za korišćenje.
* Centralizovana detekcija pretnji: GuardDuty može pratiti sve vaše AWS IAM naloge iz jednog, centralizovanog naloga. Ovo olakšava upravljanje i reagovanje na pretnje širom vaše celokupne AWS okoline.

Slika 1: Pojednostavljena arhitektura GuardDuty-a

Slika 2: Primer GuardDuty-a u akciji

**AWS** **WAF**

AWS WAF (Web Application Firewall) je sigurnosni servis koji pomaže u zaštiti vaših web aplikacija ili API-ja od uobičajenih web eksploatacija koje mogu uticati na dostupnost, kompromitovati sigurnost ili konzumirati prekomerne resurse. Daje vam kontrolu nad saobraćajem koji dozvoljavate ili blokirate prema vašim aplikacijama definisanjem prilagodljivih pravila za web sigurnost.

Ključne karakteristike AWS WAF-a:

* Filtriranje Web Saobraćaja: AWS WAF omogućava vam da kreirate pravila za filtriranje web zahteva na osnovu uslova kao što su IP adrese, HTTP zaglavlja, HTTP telo, ili URI stringovi. Ovo vam omogućava da blokirate uobičajene oblike napada kao što su SQL injection ili cross-site scripting (XSS).
* Održavana Pravila: AWS WAF uključuje set pravila koja održava AWS. Ova pravila mogu pomoći u zaštiti vaših aplikacija od pretnji bez potrebe da pišete svoja sigurnosna pravila.
* Bot Control: AWS WAF Bot Control vam daje vidljivost i kontrolu nad uobičajenim i rasprostranjenim bot saobraćajem koji može konzumirati prekomerne resurse, izobličiti metrike, uzrokovati pad aplikacije, ili izvršiti druge neželjene aktivnosti.
* API-ji za Automatizaciju: AWS WAF pruža API-je koji vam omogućavaju da automatizujete kreiranje i implementaciju pravila za web sigurnost. Ovo olakšava uključivanje sigurnosti u vaše razvojne i operativne procese.

AWS WAF se integriše sa nekoliko AWS servisa kako bi pružio sveobuhvatnu zaštitu za vaše aplikacije. Evo nekih ključnih integracija:

{

"Name": "BlockBadBot",

"Priority": 0,

"Statement": {

"ByteMatchStatement": {

"FieldToMatch": {

"SingleHeader": {

"Name": "User-Agent"

}

},

"PositionalConstraint": "CONTAINS",

"SearchString": "BadBot",

"TextTransformations": [

{

"Priority": 0,

"Type": "NONE"

}

]

}

},

"Action": {

"Block": {}

},

"VisibilityConfig": {

"SampledRequestsEnabled": true,

"CloudWatchMetricsEnabled": true,

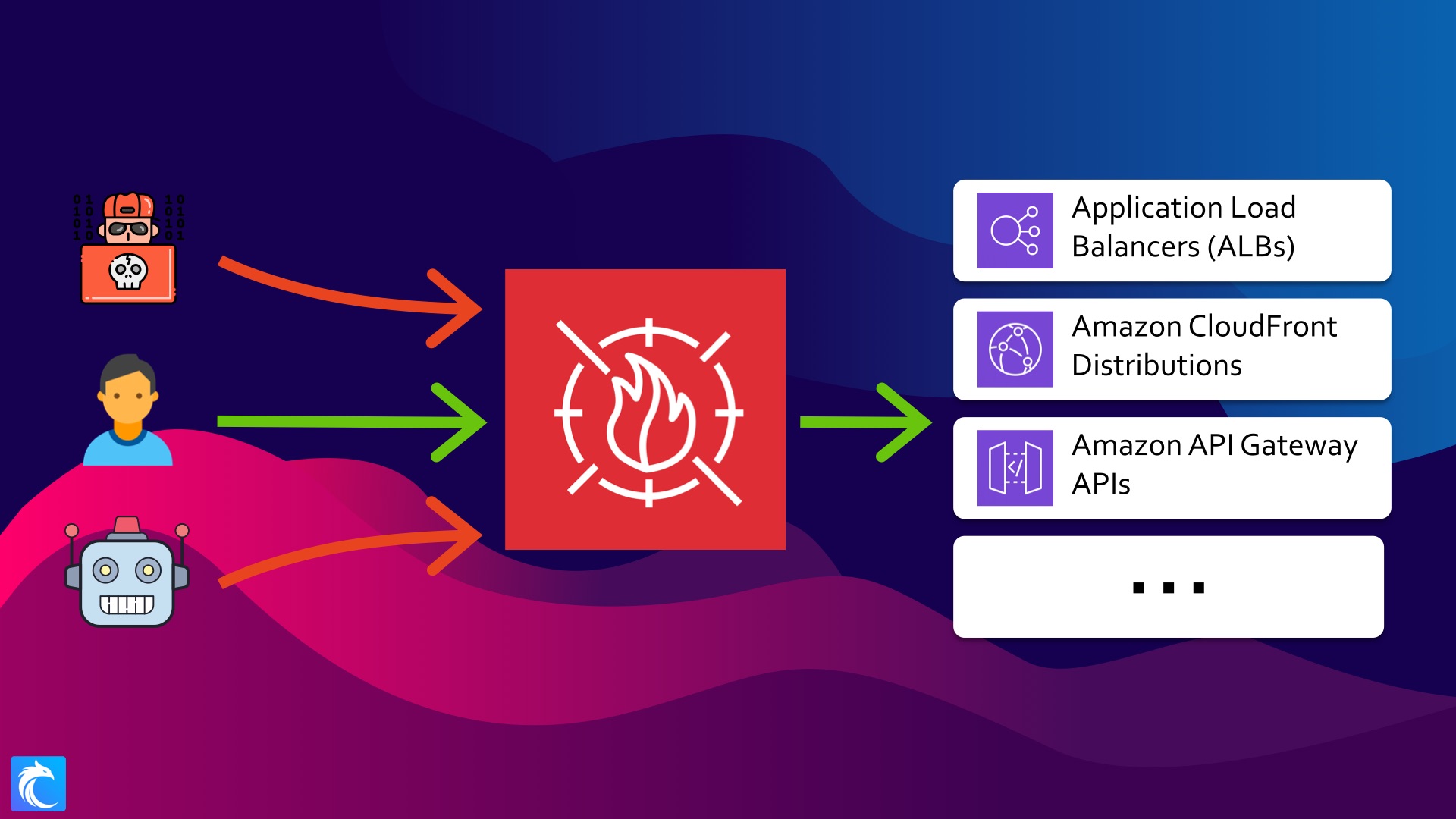
"MetricName": "BlockBadBot"

}

}

Policy 2: Primer WAF pravila

* Amazon CloudFront
* Amazon API Gateway
* AWS Application Load Balancer (ALB)
* AWS Amplify

Slika 3: Primer servisa u koje se integrise WAF

**AWS** **KMS**

AWS Key Management Service (KMS) je usluga koja olakšava kreiranje i upravljanje kriptografskim ključevima i kontrolisanje njihove upotrebe preko širokog spektra AWS servisa i u vašim aplikacijama. AWS KMS je integrisan sa ostalim AWS servisima, što olakšava šifrovanje podataka koje skladištite u ovim servisima i kontrolisanje pristupa ključevima koji ga dešifruju.

Ključne karakteristike AWS KMS-a:

* Centralizovano upravljanje ključevima: AWS KMS omogućava vam da kreirate, uvozite, rotirate, onemogućite, brišete, definišete pravila upotrebe za i proveravate upotrebu ključeva za šifrovanje koji se koriste za zaštitu vaših podataka.
* Integrisan sa AWS servisima: AWS KMS je integrisan sa širokim spektrom AWS servisa, uključujući Amazon S3, Amazon EBS, Amazon RDS, Amazon Redshift, Amazon EMR, AWS Glue, Amazon Athena i AWS CloudTrail. To znači da možete koristiti AWS KMS za šifrovanje podataka u ovim servisima.
* Revizija upotrebe ključa: AWS KMS je integrisan sa AWS CloudTrail-om kako bi pružio logove svih upotreba ključa koje mogu pomoći u ispunjavanju vaših regulatornih potreba.
* Customer master keys (CMKs): Ovo su primarni resursi u AWS KMS-u. Možete koristiti CMK za šifrovanje i dešifrovanje do 4 kilobajta (KB) podataka. CMKs se mogu takođe koristiti za generisanje, šifrovanje i dešifrovanje ključeva podataka, koji mogu šifrovati veće količine podataka.
* Ključevi podataka: Ovo su ključevi za šifrovanje koje možete koristiti za šifrovanje podataka, uključujući velike količine podataka i druge ključeve za šifrovanje podataka. Možete generisati, šifrovati i dešifrovati ključeve podataka u AWS KMS-u.
* Šifrovanje omotnica: AWS KMS podržava šifrovanje omotnica, praksu gde šifrujete plaintext podatke sa ključem podataka, a zatim šifrujete ključ podataka pod drugim ključem (kao što je CMK).

AWS Key Management Service (KMS) koristi simetričnu enkripciju kako za Customer master keys (CMKs) tako i za ključeve podataka.

Specifični algoritam koji AWS KMS koristi za simetričnu enkripciju je Advanced Encryption Standard (AES) sa veličinom ključa od 256 bita. Ovo se često naziva AES-256, i to je široko korišćeni standard za enkripciju koji pruža visok nivo sigurnosti.

Pored simetričnih CMKs, AWS KMS takođe podržava asimetrične CMKs. Asimetrični CMKs se mogu koristiti za enkripciju i dekripciju podataka, i za potpisivanje i verifikaciju poruka. Podržavaju RSA i Elliptic Curve Digital Signature Algorithm (ECDSA) parove ključeva.

Za RSA, AWS KMS podržava tri dužine ključeva: 2048 bita, 3072 bita, i 4096 bita. Za ECDSA, podržana kriva se naziva 'NIST P-256’

**AWS** **Shield**

AWS Shield je servis za zaštitu od Distributed Denial of Service (DDoS) napada koji štiti aplikacije koje rade na AWS-u. Pruža stalnu detekciju i automatski ublažavanja posledice napada kako bi se minimiziralo vreme neaktivnosti aplikacija i smanjenja latency-a, omogućavajući vašim aplikacijama da nastave sa radom tokom DDoS napada.

Postoje dva nivoa AWS Shield - Standard i Advanced.

* AWS Shield Standard je automatski uključen u vaše AWS usluge bez dodatnih troškova. Pruža zaštitu od najčešćih, često javljajućih DDoS napada kako bi odbranio vašu web stranicu ili aplikacije.
* AWS Shield Advanced je pretplatnički servis koji pruža dodatne funkcionalnosti zaštite od DDoS napada za vaše AWS resurse. Uključuje zaštitu troškova, nadoknadu troškova DDoS-a, integraciju web aplikacijskog firewall-a i pristup DDoS odgovornom timu 24/7.

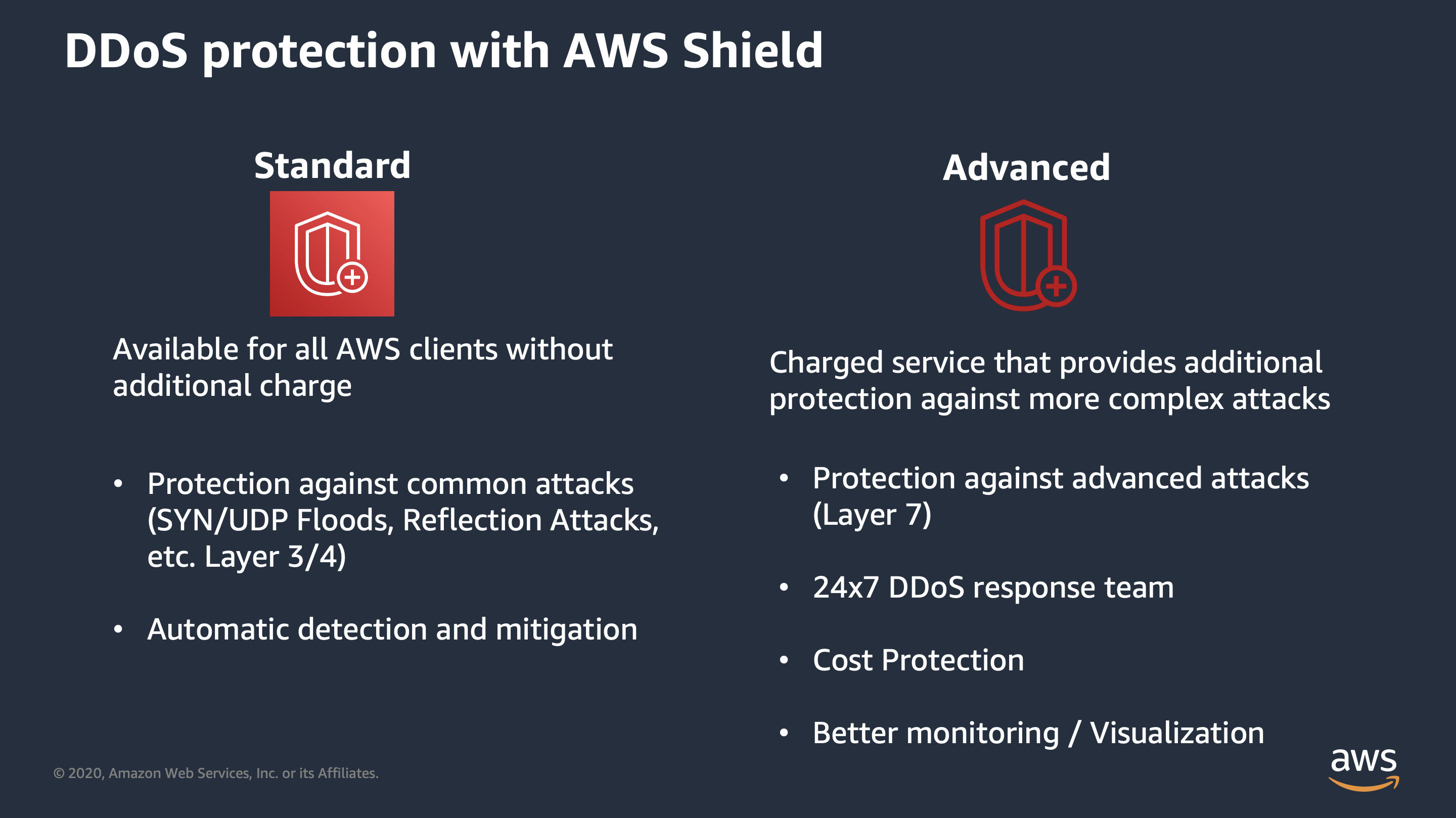
AWS Shield se prvenstveno integriše sa sledećim AWS servisima:

* Amazon CloudFront
* AWS Global Accelerator
* Amazon Route 53
* Elastic Load Balancing (ELB)
* AWS WAF

Primer kako AWS Shield radi:

Recimo da imate web aplikaciju hostovanu na AWS-u. Ova aplikacija je iza CloudFront distribucije za dostavu sadržaja vašim korisnicima.

Kada DDoS napad cilja vašu aplikaciju, AWS Shield Standard počinje da ublažava napad automatski. Koristi algoritme anomalija i druge tehnike analize za detekciju malicioznog saobraćaja. Neželjeni saobraćaj se blokira, dok se legitimni zahtevi prosleđuju vašoj aplikaciji, minimizirajući uticaj na vaše korisnike.

Slika 4: Poredjenje Shield Standard-a i Shiled Advanced-a

Ako ste pretplaćeni na AWS Shield Advanced i napad je složeniji, 24/7 AWS DDoS Response Team (DRT) se uključuje. Oni kreiraju izveštaje o incidentima, angažuju se sa vama da koordiniraju odgovor, a mogu čak i napisati prilagođena pravila ublažavanja u vaše ime