# Zasady, polityki, procedury i usługi bezpieczeństwa w AWS

**2020 SOFTPROM** *softprom.com* | *info@softprom.com* **Amazon Web Services Partner Network ADVANCED CONSULTING PARTNER** —

## Podstawowe zasady zapewniania bezpieczeństwa w chmurze AWS

- **Wdrożenie ścisłej identyfikacji** opartej na strategii najmniejszych uprawnień (zobacz: *Strategia zarządzania dostępem w AWS*).
- **Realizacja ciągłego monitorowania**, powiadamiania i audytu w trybie czasu rzeczywistego.
- **Wdrożenie bezpieczeństwa na wszystkich poziomach:** sieciowym (VPC), równoważenia obciążenia (load balancing), maszyny wirtualnej, systemu operacyjnego, aplikacji oraz kodu źródłowego.
- **Stosowanie najlepszych praktyk** w tworzeniu bezpiecznej infrastruktury opartej na kodzie programistycznym — Infrastruktura jako Kod (AWS CloudFormation).
- **Implementacja ochrony danych** podczas ich przesyłania (w locie) i przechowywania (w spoczynku).
- **Wdrożenie narzędzi pozwalających wyeliminować czynnik ludzki**, zmniejszyć potrzebę bezpośredniego dostępu lub ręcznego przetwarzania danych.
- **Modelowanie reagowania na incydenty**, wykorzystanie narzędzi automatyzacji w celu zwiększenia profesjonalizmu, szybkości wykrywania, dochodzenia i usuwania skutków incydentów.

---

## Bezpieczeństwo w chmurze składa się z pięciu obszarów

1. **Zarządzanie tożsamością i dostępem** (*Identity and access management*)
2. **Wykrywanie** (*Detection*)
3. **Ochrona infrastruktury** (*Infrastructure protection*)
4. **Ochrona danych** (*Data protection*)

5. **Reagowanie na sytuacje awaryjne** (*Incident response*)

---

# Usługi bezpieczeństwa AWS

Poniżej przedstawiono usługi AWS mające zastosowanie w odpowiednich obszarach bezpieczeństwa.

## Zarządzanie tożsamością i dostępem

| Przykład użycia | Usługa AWS |
|---|---|
| Bezpieczne zarządzanie dostępem do usług i zasobów | AWS Identity & Access Management (IAM) |
| Chmurowa usługa logowania jednokrotnego (SSO) | AWS Single Sign-On |
| Zarządzanie tożsamością użytkowników w aplikacjach | Amazon Cognito |
| Zarządzana usługa Microsoft Active Directory | AWS Directory Service |
| Prosta i bezpieczna usługa udostępniania zasobów AWS | AWS Resource Access Manager |

## Zarządzanie i administracja

| Przykład użycia | Usługa AWS |
|---|---|
| Wszystkie konta AWS w jednym miejscu | AWS Organizations |

## Wykrywanie

| Przykład użycia | Usługa AWS |
|---|---|
| Zunifikowane centrum bezpieczeństwa i zgodności z wymaganiami | AWS Security Hub |
| Zarządzana usługa wykrywania zagrożeń | Amazon GuardDuty |
| Analiza bezpieczeństwa aplikacji | Amazon Inspector |

| | |
|---|---|
| Rejestrowanie i ocena konfiguracji zasobów AWS | AWS Config |
| Śledzenie działań użytkowników i użycia API | AWS CloudTrail |
| Zarządzanie bezpieczeństwem urządzeń Internetu Rzeczy | AWS IoT Device Defender |

## Ochrona infrastruktury

| Przykład użycia | Usługa AWS |
|---|---|
| Ochrona przed atakami DDoS | AWS Shield |
| Filtrowanie szkodliwego ruchu sieciowego | AWS Web Application Firewall (WAF) |
| Centralne zarządzanie regułami zapory sieciowej (firewalla) | AWS Firewall Manager |

## Ochrona danych

| Przykład użycia | Usługa AWS |
|---|---|
| Wykrywanie i ochrona poufnych danych na dowolną skalę | Amazon Macie |
| Przechowywanie kluczy i zarządzanie nimi | AWS Key Management Service (KMS) |
| Sprzętowy magazyn kluczy w celu spełnienia wymogów regulacyjnych | AWS CloudHSM |
| Tworzenie, wdrażanie i zarządzanie publicznymi oraz prywatnymi certyfikatami SSL/TLS | AWS Certificate Manager |
| Rotacja, pobieranie i zarządzanie poufnymi danymi (sekretami) | AWS Secrets Manager |

## Reagowanie na sytuacje awaryjne

| Przykład użycia | Usługa AWS |
|---|---|
| Analiza potencjalnych problemów z bezpieczeństwem | Amazon Detective |

| | |
|---|---|
| Szybkie, ekonomiczne i zautomatyzowane przywracanie awaryjne | CloudEndure Disaster Recovery |

### Zgodność z wymaganiami

| Przykład użycia | Usługa AWS |
|---|---|
| Bezpłatny portal samoobsługowy zapewniający dostęp na żądanie do raportów zgodności AWS | AWS Artifact |

---

## Procedury audytu bezpieczeństwa według obszarów bezpieczeństwa

Ta lista kontrolna zawiera rekomendacje dla klientów, które są zgodne z filarem bezpieczeństwa ram AWS Well-Architected Framework (*Well-Architected Framework Security Pillar*).

### Zarządzanie tożsamością i dostępem (Identity & Access Management)

1. **Zabezpiecz swoje konto AWS.** Używaj *AWS Organizations* do zarządzania swoimi kontami, korzystaj z użytkownika root wyłącznie w sytuacjach wyjątkowych z włączonym uwierzytelnianiem wieloskładnikowym (MFA) oraz skonfiguruj dane kontaktowe konta.
2. **Polegaj na scentralizowanym dostawcy tożsamości.** Scentralizuj tożsamości za pomocą *AWS Single Sign-On* lub zewnętrznego dostawcy, aby uniknąć rutynowego tworzenia użytkowników IAM lub używania długoterminowych kluczy dostępu — takie podejście ułatwia zarządzanie wieloma kontami AWS i aplikacjami federacyjnymi.
3. **Używaj wielu kont AWS do separacji obciążeń (workloads)** i etapów ich wdrażania, takich jak środowiska produkcyjne i nieprodukcyjne. Wiele kont AWS pozwala na odseparowanie danych oraz zasobów, a także umożliwia stosowanie zasad kontroli usług (*Service Control Policies*) w celu wdrożenia barier ochronnych (*guardrails*). Usługa *AWS Control Tower* może pomóc w łatwym skonfigurowaniu i zarządzaniu środowiskiem wielokontowym AWS.
4. **Przechowuj i używaj sekretów w bezpieczny sposób.** Tam, gdzie nie można użyć tymczasowych poświadczeń, takich jak tokeny z *AWS Security Token Service*,

przechowuj sekrety (np. hasła do baz danych) za pomocą usługi *AWS Secrets Manager*, która odpowiada za szyfrowanie, rotację i kontrolę dostępu.

## Wykrywanie (Detection)

1. **Włącz usługi podstawowe:** *AWS CloudTrail*, *Amazon GuardDuty* oraz *AWS Security Hub*. Dla wszystkich swoich kont AWS skonfiguruj *CloudTrail* do logowania aktywności API, używaj *GuardDuty* do ciągłego monitorowania, a *AWS Security Hub* do uzyskania kompleksowego widoku stanu bezpieczeństwa.
2. **Skonfiguruj logowanie na poziomie usług i aplikacji.** Oprócz logów aplikacji włącz logowanie na poziomie usług, takich jak *Amazon VPC Flow Logs*, *Amazon S3*, *CloudTrail* oraz logi dostępu *Elastic Load Balancer*, aby uzyskać pełny wgląd w zdarzenia. Skonfiguruj przesyłanie logów do scentralizowanego konta i chroń je przed modyfikacją lub usunięciem.
3. **Skonfiguruj monitorowanie oraz alerty i badaj zdarzenia.** Włącz *AWS Config* do śrefzenia historii zasobów oraz zarządzane reguły Config (*Config Managed Rules*) do automatycznego alarmowania lub naprawiania niepożądanych zmian. Dla wszystkich źródeł logów i zdarzeń — od *AWS CloudTrail* po *Amazon GuardDuty* i logi aplikacji — skonfiguruj alerty dla zdarzeń o wysokim priorytecie i poddawaj je analizie.

## Ochrona infrastruktury (Infrastructure Protection)

1. **Aktualizuj system operacyjny, aplikacje i kod (patching).** Używaj *AWS Systems Manager Patch Manager* do automatyzacji procesu instalowania poprawek we wszystkich systemach i kodzie, za które odpowiadasz, w tym w systemie operacyjnym, aplikacjach i zależnościach kodu.
2. **Wdróż ochronę przed rozproszoną odmową usługi (DDoS)** dla zasobów publicznych (skierowanych do Internetu). Użyj *Amazon CloudFront*, *AWS WAF* i *AWS Shield*, aby zapewnić ochronę przed atakami DDoS w warstwie 7 oraz warstwach 3 i 4.
3. **Kontroluj dostęp za pomocą grup bezpieczeństwa VPC (Security Groups) i warstw podsieci.** Używaj grup bezpieczeństwa do kontrolowania ruchu przychodzącego i wychodzącego oraz automatycznie stosuj reguły zarówno dla grup bezpieczeństwa, jak i systemów WAF przy użyciu *AWS Firewall Manager*. Grupuj różne zasoby w różnych podsieciach, aby stworzyć warstwy routingu — na przykład zasoby bazodanowe nie potrzebują bezpośredniej trasy do Internetu.

## Ochrona danych (Data Protection)

1. **Chroń dane w spoczynku (data at rest).** Używaj *AWS Key Management Service (KMS)* do ochrony danych w spoczynku w szerokiej gamie usług AWS oraz w swoich aplikacjach. Włącz domyślne szyfrowanie dla wolumenów *Amazon EBS* i kubełków *Amazon S3*.
2. **Szyfruj dane w locie (data in transit).** Włącz szyfrowanie dla całego ruchu sieciowego, w tym *Transport Layer Security (TLS)* dla kontrolowanej przez siebie infrastruktury sieciowej opartej na sieci Web, używając *AWS Certificate Manager* do zarządzania certyfikatami i ich udostępniania.
3. **Używaj mechanisms do odsuwania ludzi od danych.** Zapobiegaj bezpośredniemu dostępowi wszystkich użytkowników do wrażliwych danych i systemów. Na przykład udostępnij użytkownikom biznesowym pulpit nawigacyjny *Amazon QuickSight* zamiast bezpośredniego dostępu do bazy danych i wykonuj działania na odległość, korzystając z dokumentów automatyzacji *AWS Systems Manager* oraz funkcji *Run Command*.

### Reagowanie na incydenty (Incident Response)

1. **Upewnij się, że posiadasz plan reagowania na incydenty (IR).** Rozpocznij swój plan IR od stworzenia podręczników procedur (*runbooks*) pozwalających reagować na nieoczekiwane zdarzenia w Twoich środowiskach. Szczegółowe informacje można znaleźć w podręczniku *AWS Security Incident Response Guide*.
2. **Upewnij się, że ktoś zostanie powiadomiony o konieczności podjęcia działań w przypadku krytycznych ustaleń (findings).** Zacznij od ustaleń z *GuardDuty*. Włącz *GuardDuty* i upewnij się, że powiadomienia trafiają do osoby mającej możliwość podjęcia natychmiastowych działań. Automatyczne tworzenie zgłoszeń serwisowych (*trouble tickets*) to najlepszy sposób na zintegrowanie ustaleń *GuardDuty* z procesami operacyjnymi.
3. **Ćwicz reagowanie na zdarzenia.** Symuluj i ćwicz reagowanie na incydenty poprzez regularne organizowanie dni próbnych (*game days*), włączając wyciągnięte wnioski do planów zarządzania incydentami i stale je ulepszając.

---

## Procedury audytu bezpieczeństwa według usług AWS

### IAM

- Unikaj używania kluczy dostępu użytkownika głównego konta AWS (root account), ponieważ dają one pełny i nieograniczony dostęp do wszystkich zasobów.
- Uwierzytelnianie MFA musi być włączone dla konta root, aby zapewnić dwuskładnikową weryfikację.

- Przypisz poszczególnym użytkownikom IAM wyłącznie niezbędne uprawnienia umożliwiające logowanie.
- Upewnij się, że konta użytkowników również posiadają włączone uwierzytelnianie MFA.
- Klucze dostępu IAM (Access Keys) muszą być rotowane w regularnych odstępach czasu.
- Zapewnij silną politykę haseł dla wszystkich użytkowników.
- Przypisuj uprawnienia użytkownikom na podstawie grup użytkowników (User Groups), zamiast przypisywać je bezpośrednio do indywidualnych użytkowników IAM.
- Zapewniaj dostęp do zasobów poprzez role IAM (IAM Roles).
- Przyznawaj najmniejsze uprawnienia (least privilege) podczas tworzenia polityk IAM, niezbędne do wykonania wymaganych działań.
- Przypisuj polityki IAM do grup lub ról bezpośrednio podczas ich tworzenia.
- Jeśli to konieczne, w politykach można zdefiniować warunki (conditions), pod którymi przyznawany jest dostęp do zasobu.
- Pozbądź się niepotrzebnych poświadczeń IAM — tych, które są nieaktywne lub nieużywane.
- Używaj ról IAM, aby przyznać dostęp aplikacjom działającym na instancjach EC2.

## S3

- Upewnij się, że kubełki S3 nie są publicznie dostępne (brak publicznych uprawnień do odczytu lub zapisu); użytkownicy mogą włączyć funkcję blokowania publicznego dostępu w *Amazon S3 (block public access)*.
- Korzystaj z uprawnień na poziomie obiektów lub kubełków (object-level lub bucket-level) jako uzupełnienia polityk IAM w celu przyznawania dostępu do zasobów.
- Włącz funkcję *MFA Delete*, aby zapobiec przypadkowemu usunięciu kubełków.
- Rozważ szyfrowanie przechowywanych danych, które można wykonać na dwa sposoby: po stronie serwera (server-side) oraz po stronie klienta (client-side).
- Włącz szyfrowanie przychodzącego i wychodzącego ruchu danych za pomocą punktów końcowych SSL (SSL endpoints).
- Skonfiguruj zarządzanie cyklem życia S3 (lifecycle management) poprzez działania oparte na regułach i używaj wersjonowania (versioning) do przechowywania i odzyskiwania wielu wersji obiektu w kubełku, aby radzić sobie z przypadkowymi usunięciami.
- Upewnij się, że rejestrowanie dostępu do S3 (S3 access logging) jest włączone.
- Stale kontroluj i monitoruj kubełki S3 za pomocą metryk CloudWatch.

## EC2, VPC i EBS

- Upewnij się, że dane i wolumeny dyskowe w EBS są zaszyfrowane za pomocą algorytmu AES-256, będącego standardem branżowym.
- Ogranicz dostęp do instancji z określonych zakresów adresów IP za pomocą grup bezpieczeństwa (Security Group).
- Ogranicz zakres otwartych portów w grupach bezpieczeństwa EC2, aby zapobiec narażeniu na luki w zabezpieczeniach.
- Upewnij się, że do systemów ELB (Elastic Load Balancers) jest przypisana prawidłowa grupa bezpieczeństwa.
- Monitoruj i optymalizuj domyślne grupy bezpieczeństwa, ponieważ domyślnie zezwalają one na nieograniczony ruch przychodщий i wychodzący.
- Zapewnij ograniczony dostęp przychodzący do SSH, FTP, SMTP, MySQL, PostgreSQL, MongoDB, MSSQL, CIFS itp. wyłącznie dla autoryzowanych podmiotów.
- Używaj ról IAM do przyznawania dostępu do EC2 zamiast kluczy dostępu dla potrzeb tymczasowych.
- Jeśli używasz kluczy dostępu użytkownika IAM dla długoterminowych uprawnień, upewnij się, że nie zaszywasz kluczy bezpośrednio w kodzie, generuj różne klucze dla different aplikacji, rotuj klucze dostępu, używaj uwierzytelniania MFA i wycofuj z użycia nieużywane pary kluczy.
- Włącz i aktywuj logi przepływu VPC (VPC flow logs), aby rejestrować ruch przychodzący i wychodzący w VPC w celu lepszego monitorowania i wczesnej diagnozy.
- Usuń nieużywane wirtualne bramy prywatne (Virtual Private Gateways) i bramy internetowe VPC (VPC Internet Gateways).
- Upewnij się, że żadne punkty końcowe VPC (VPC endpoints) nie są wystawione na ryzyko, sprawdzając wartość podmiotu (principal value) w polityce.
- Upewnij się, że żadne listy ACL nie zezwalają na nieograniczony dostęp przychodzący lub wychodzący.

## CloudTrail

- Upewnij się, że usługa CloudTrail jest aktywowana we wszystkich regionach oraz dla usług globalnych, takich jak IAM, STS itp.
- Zaleca się logowanie do scentralizowanego kubełka S3.
- Upewnij się, że zarówno sama usługa CloudTrail, jak i logowanie CloudTrail są włączone dla wszystkich regionów.
- Upewnij się, że włączona jest walidacja integralności plików logów CloudTrail.
- Upewnij się, że pliki logów CloudTrail są zaszyfrowane.

## RDS

- Upewnij się, że grupy bezpieczeństwa RDS nie zezwalają na nieograniczony akses.
- Zapewnij szyfrowanie instancji i migawek (snapshots) RDS przy użyciu szyfrowania na poziomie AES-256.
- Chroń dane w locie do RDS za pomocą punktów końcowych SSL.
- Monitoruj kontrolę nad RDS przy użyciu AWS KMS i kluczy zarządzanych przez klienta (Customer Managed Keys).
- Skonfiguruj AWS Secrets Manager do automatycznej rotacji sekretów dla Amazon RDS.
- Upewnij się, że instancje bazodanowe oraz migawki RDS nie są publicznie dostępne.
- Włącz funkcję automatycznej aktualizacji mniejszych wersji (auto minor upgrade) dla RDS.

### Redshift

- Włącz parametr `require_ssl` we wszystkich klastrach Redshift, aby zminimalizować ryzyko podczas szyfrowania danych w locie dla Redshift oraz w celu bezpiecznego połączenia klienta SQL z klastrem.
- Włącz szyfrowanie klastra Redshift (Redshift Cluster encryption).
- Upewnij się, że logowanie aktywności użytkowników Redshift (Redshift user activity logging) jest włączone.
- Zapewnij szyfrowanie Redshift za pomocą kluczy KMS zarządzanych przez klienta (KMS Customer Managed Keys).
- Zaleca się, aby klastry Redshift były uruchamiane wewnątrz VPC w celu uzyskania lepszej kontroli.
- Upewnij się, że klastry Redshift nie są publicznie dostępne.

---

## Wbudowane bezpieczeństwo (Security by Design - SbD)

**Bezpieczeństwo wbudowane (SbD)** to podejście do zapewniania bezpieczeństwa, które formalizuje projektowanie konta AWS, automatyzuje systemy kontroli bezpieczeństwa i upraszcza procesy audytu. Podejście SbD, w przeciwieństwie do tradycyjnego audytu bezpieczeństwa ex-post (za miniony okres), zapewnia kontrolę bezpieczeństwa natywnie wbudowaną w proces zarządzania zasobami IT na platformie AWS. Wykorzystanie szablonów wbudowanego bezpieczeństwa (SbD) w *AWS CloudFormation* pozwala na osiągnięcie wszechstronnej i skutecznej ochrony oraz zapewnienie zgodności z wymaganiami w chmurze.

SbD to podejście do zapewniania bezpieczeństwa i zgodności z wymaganiami (compliance) na dowolną skalę, z uwzględnieniem specyfiki różnych branż, standardów i

kryteriów bezpieczeństwa. Podejście SbD w AWS można stosować przy projektowaniu funkcji bezpieczeństwa i zgodności na wszystkich etapach, co pozwala klientowi na zaprojektowanie wszystkich komponentów własnego środowiska AWS: uprawnień, logowania, relacji zaufania, wymuszonego szyfrowania, korzystania wyłącznie z zatwierdzonych obrazów maszyn (AMI) i wielu innych.

Podejście SbD pozwala zautomatyzować infrastrukturę dostępową konta AWS, niezawodnie programując bezpieczeństwo i zgodność ze standardami w używanych kontach AWS, pozostawiając w przeszłości niezgodność systemów zarządzania IT ze standardowymi wymaganiami.

## Podejście oparte na wbudowanym bezpieczeństwie (SbD)

Podejście SbD definiuje obowiązki kontrolne, zasady automatyzacji fundamentów bezpieczeństwa, ustawienia bezpieczeństwa oraz wymagania dotyczące audytu systemów zarządzania przez klienta w jego własnej infrastrukturze, systemach operacyjnych, usługach i aplikacjach działających w AWS. Oferowane przez program wytyczne, standaryzowane i powtarzalne projekty z wbudowaną automatyzacją mogą być wdrażane w typowych scenariuszach użycia, biorąc pod uwagę standardy bezpieczeństwa i wymagania audytowe w różnych branżach oraz dla różnych obciążeń roboczych.

Firma AWS zaleca stosowanie wbudowanego bezpieczeństwa i zgodności z wymaganiami na swoim koncie AWS, postępując zgodnie z poniższym czteroetapowym podejściem.

- **Etap 1. Sformułuj wymagania.** Zdefiniuj polityki i opisz systemy kontroli dziedziczone od AWS. Następnie opisz systemy kontroli stosowane przez Ciebie w środowisku AWS i określ listę reguł bezpieczeństwa, które należy wdrożyć w środowisku IT AWS.
- **Etap 2. Stwórz bezpieczne środowisko odpowiadające Twoim wymaganiom i specyfice wdrożenia.** Określ wymaganą konfigurację w postaci wartości konfiguracyjnych AWS, takich jak wymagania dotyczące szyfrowania (np. wymuszenie szyfrowania po stronie serwera dla obiektów S3), uprawnienia do zasobów (jakie role mają zastosowanie w określonych środowiskach), lista dozwolonych obrazów maszyn (na podstawie zatwierdzonych, stałych obrazów serwerowych) oraz typy obowiązkowych logów (np. wymuszenie stosowania usługi CloudTrail dla kompatybilnych zasobów).
  Ponieważ AWS oferuje wszechstronny zestaw opcji konfiguracyjnych i regularnie dodaje nowe usługi, będziesz w stanie znaleźć szablony pozwalające dostosować Twoje środowisko do określonych wymagań bezpieczeństwa. Te szablony bezpieczeństwa (w postaci szablonów *AWS CloudFormation*) dostarczają kompleksowy zestaw reguł, które można wdrażać systematycznie. Firma AWS

opracowała szablony zapewniające reguły bezpieczeństwa zgodne z różnymi strukturami bezpieczeństwa.
Dodatkową pomoc w tworzeniu bezpiecznego środowiska mogą zapewnić doświadczeni architekci AWS, specjaliści *AWS Professional Services* oraz rozwiązania naszych partnerów. Zespoły te mogą współpracować z Twoim personelem i działami audytu, aby pomóc we wdrażaniu wysokiej dotyczących bezpiecznych środowisk przygotowanych do audytów zewnętrznych.

- **Etap 3. Wdróż stworzone szablony.** *AWS Service Catalog* daje użytkownikom możliwość wymuszenia stosowania własnych szablonów w katalogu. Ten krok gwarantuje, że bezpieczne środowisko zostanie użyte podczas tworzenia jakichkolwiek nowych środowisk. Zapobiega to również tworzeniu środowisk, które nie są zgodne z ustalonymi regułami bezpieczeństwa. Wymóg obowiązkowego korzystania z określonego szablonu w katalogu daje klientom pewność, że skonfigurowane mechanizmy bezpieczeństwa będą gotowe na audyt zewnętrzny.
- **Etap 4. Wykonaj działania weryfikacyjne.** Wdrażanie w AWS za pomocą *Service Catalog* i szablonów bezpiecznego środowiska pomaga stworzyć środowisko gotowe do audytu. Reguły zdefiniowane w szablonie mogą służyć jako przewodnik po audycie. *AWS Config* umożliwia skanowanie bieżącego stanu dowolnego środowiska w celu porównania go z ustalonymi regułami bezpiecznego środowiska. Korzystanie z bezpiecznych uprawnień tylko do odczytu wraz z unikalnymi skryptami pozwala zautomatyzować zbieranie informacji na potrzeby audytu. Klienci mogą przejść od tradycyjnych, ręcznych administracyjnych środków kontroli do technicznych środków kontroli wdrażanych w sposób wymuszony, zachowując pewność, że przy prawidłowym zaprojektowaniu i zastosowaniu środki te działają w 100% przez cały czas (w przeciwieństwie do tradycyjnych metod audytu wyrywkowego i kontroli stanu w określonym punkcie czasowym).

## Znaczenie wbudowanego bezpieczeństwa

Wbudowane bezpieczeństwo umożliwia realizację następujących celów:

- Tworzenie wymuszanych funkcji, których nie mogą nadpisać użytkownicy niemający odpowiednich uprawnień;
- Organizacja niezawodnego działania systemów kontroli;
- Ciągły audyt w trybie czasu rzeczywistego;
- Stosowanie polityk zarządzania w formie skryptów programistycznych.

Wynikiem jest zautomatyzowane środowisko wspierające funkcje bezpieczeństwa, zarządzania i zgodności z konkretnymi wymaganiami. Możesz wykorzystać niezawodną implementację możliwości, które wcześniej były opisane jedynie w politykach, standardach i przepisach. Ponadto można wymuszać bezpieczeństwo i zgodność ze

standardami, co ostatecznie prowadzi do stworzenia funkcjonalnego i niezawodnego modelu zarządzania dla środowisk AWS.