AWS Guida decisionale

Scelta AWS dei servizi di sicurezza, identità e governance

Scelta AWS dei servizi di sicurezza, identità e governance: AWS Guida decisionale

Table of Contents

Guida decisionale 1
Introduzione 1
Comprendi 2
Responsabilità condivisa 2
Combina AWS strumenti e servizi 3
Considera 8
Scegliere 11
Gestione dell'identità e degli accessi 12
Protezione dei dati 12
Protezione di reti e applicazioni 13
Rilevamento e risposta 14
Governance e conformità 15
Utilizzo 16
Gestione dell'identità e degli accessi 16
Protezione dei dati 19
Protezione di reti e applicazioni 24
Rilevamento e risposta 26
Governance e conformità 31
Esplora 33
Cronologia dei documenti 35
..... xxxvi

Scelta AWS dei servizi di sicurezza, identità e governance

Fare il primo passo

È ora di leggere	27 minuti	
Scopo	Ti aiuta a determinare quali servizi di AWS sicurezza, identità e governance sono più adatti alla tua organizzazione.	
Ultimo aggiornamento	30 dicembre 2024	
Servizi coperti	• AWS Artifact • AWS Audit Manager • AWS Certificate Manager • AWS CloudHSM • AWS CloudTrail • Amazon Cognito • AWS Config • AWS Control Tower • Amazon Detective • AWS Firewall Manager • Amazon GuardDuty • AWS IAM • AWS IAM Identity Center • Amazon Inspector	• AWS KMS • Amazon Macie • AWS Network Firewall • AWS Organizations • AWS Payment Cryptography • AWS Private CA • AWS RAM • Gestione dei segreti AWS • AWS Security Hub CSPM • Amazon Security Lake • AWS Risposta agli incidenti di sicurezza • AWS Shield • AWS WAF

Introduzione

La sicurezza, l'identità e la governance nel cloud sono componenti importanti per raggiungere e mantenere l'integrità e la sicurezza dei dati e dei servizi. Ciò è particolarmente importante in quanto sempre più aziende migrano verso provider di servizi cloud come Amazon Web Services (AWS).

Questa guida ti aiuta a selezionare i servizi e gli strumenti di AWS sicurezza, identità e governance più adatti alle tue esigenze e alla tua organizzazione.

Innanzitutto, esploriamo cosa intendiamo per sicurezza, identità e governance:

- La sicurezza del cloud si riferisce all'utilizzo di misure e pratiche per proteggere le risorse digitali dalle minacce. Ciò include sia la sicurezza fisica dei data center sia le misure di sicurezza informatica per proteggersi dalle minacce online. AWS dà priorità alla sicurezza attraverso l'archiviazione crittografata dei dati, la sicurezza della rete e il monitoraggio continuo delle potenziali minacce.
- I servizi di identità consentono di gestire in modo sicuro identità, risorse e autorizzazioni in modo scalabile. AWS fornisce servizi di identità progettati per la forza lavoro e le applicazioni rivolte ai clienti e per gestire l'accesso ai carichi di lavoro e alle applicazioni.
- La governance del cloud è un insieme di regole, processi e report che guidano l'organizzazione a seguire le migliori pratiche. Puoi stabilire la governance del cloud tra AWS le tue risorse, utilizzare le migliori pratiche e gli standard integrati e automatizzare i processi di conformità e controllo. La conformità nel cloud si riferisce all'adesione a leggi e regolamenti che disciplinano la protezione dei dati e la privacy. AWS I programmi di conformità forniscono informazioni sulle certificazioni, i regolamenti e i framework a cui si allinea. AWS

Questo breve video one-and-a-half riassume in che modo AWS costruiamo una solida sicurezza alla base della nostra azienda.

Comprendi i AWS servizi di sicurezza, identità e governance

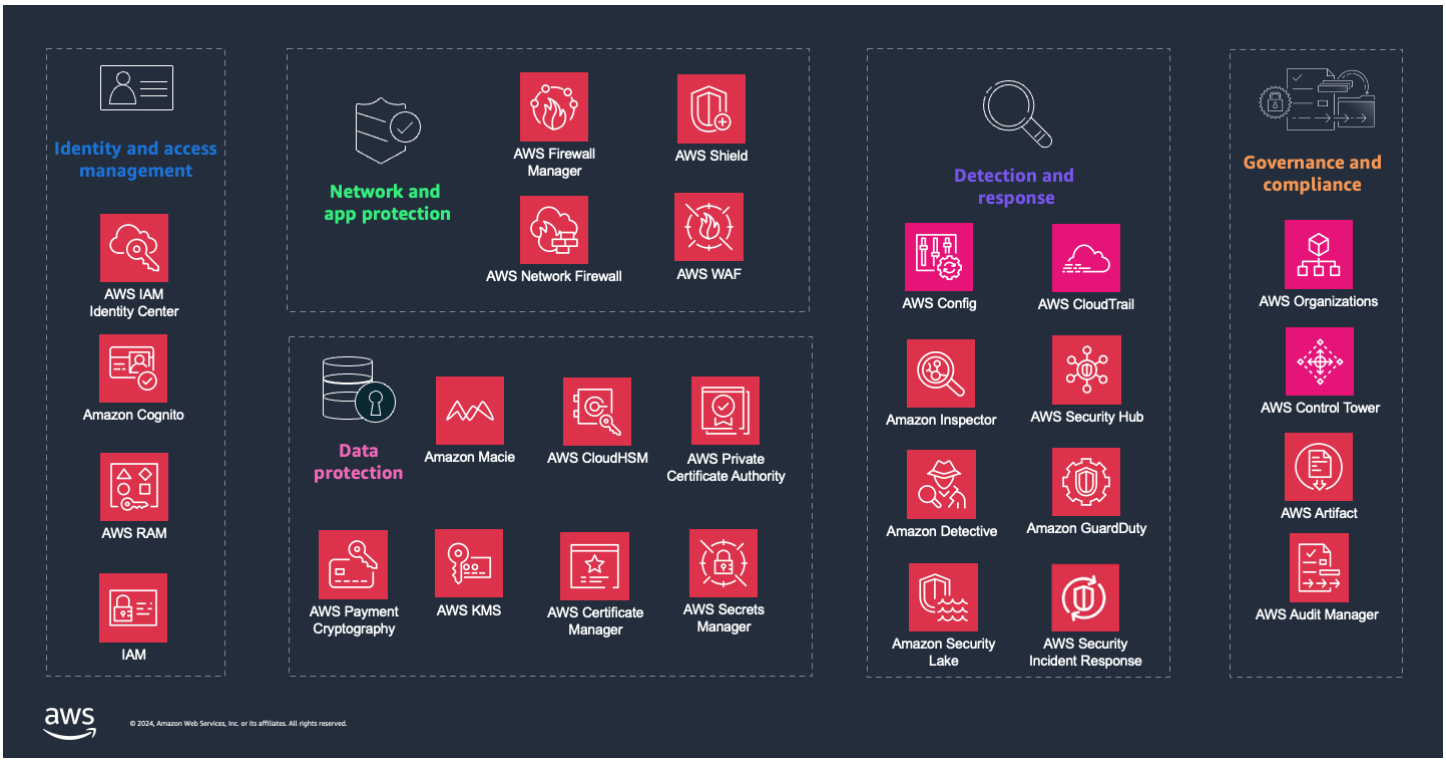
La sicurezza e la conformità sono responsabilità condivise

Prima di scegliere i servizi di AWS sicurezza, identità e governance, è importante che tu comprenda che sicurezza e conformità sono responsabilità condivise tra te e te AWS.

La natura di questa responsabilità condivisa aiuta ad alleggerire il carico operativo e offre flessibilità e controllo sulla distribuzione. Questa differenziazione di responsabilità viene comunemente definita sicurezza «del» cloud e sicurezza «nel» cloud.

Comprendendo questo modello, potete comprendere la gamma di opzioni a vostra disposizione e come quelle applicabili Servizi AWS si combinano tra loro.

Puoi combinare AWS strumenti e servizi per proteggere i tuoi carichi di lavoro



Come illustrato nel diagramma precedente, AWS offre strumenti e servizi in cinque domini per aiutarti a raggiungere e mantenere sicurezza, gestione delle identità e governance solide nel cloud. Puoi utilizzarlo Servizi AWS in questi cinque domini per aiutarti a fare quanto segue:

- Adotta un approccio multilivello per la protezione dei dati e degli ambienti
- Rafforza la tua infrastruttura cloud contro le minacce in evoluzione
- Rispetta rigorosi standard normativi

Per ulteriori informazioni sulla AWS sicurezza, inclusa la documentazione sulla sicurezza Servizi AWS, consulta la documentazione AWS sulla sicurezza.

Nelle sezioni seguenti, esaminiamo ulteriormente ogni dominio.

Comprendi i servizi di gestione delle AWS identità e degli accessi

Al centro della AWS sicurezza c'è il principio del privilegio minimo: le persone e i servizi hanno solo l'accesso di cui hanno bisogno. AWS IAM Identity Centerè consigliato Servizio AWS per gestire l'accesso degli utenti alle AWS risorse. È possibile utilizzare questo servizio per gestire l'accesso ai

propri account e le autorizzazioni all'interno di tali account, incluse le identità dei provider di identità esterni.

La tabella seguente riassume le offerte di gestione delle identità e degli accessi discusse in questa guida:

AWS IAM Identity Center

AWS IAM Identity Centerti aiuta a connettere la tua fonte di identità o a creare utenti. È possibile gestire centralmente l'accesso della forza lavoro a più applicazioni Account AWS .

Amazon Cognito

Amazon Cognito fornisce uno strumento di identità per app Web e mobili per autenticare e autorizzare gli utenti dalla directory utente integrata, dalla directory aziendale e dai provider di identità dei consumatori.

AWS RAM

AWS RAMti aiuta a condividere in modo sicuro le tue risorse all'interno dell'organizzazione e con i ruoli e gli utenti IAM. Account AWS

IAM

IAM consente un controllo sicuro e granulare sull'accesso alle risorse del carico di lavoro. AWS

Comprendi i servizi di protezione dei dati AWS

La protezione dei dati è fondamentale nel cloud e AWS fornisce servizi che aiutano a proteggere dati, account e carichi di lavoro. Ad esempio, la crittografia dei dati sia in transito che a riposo aiuta a proteggerli dall'esposizione. Con AWS Key Management Service(AWS KMS) e AWS CloudHSMpuoi creare e controllare le chiavi crittografiche che usi per proteggere i tuoi dati.

La tabella seguente riassume le offerte di protezione dei dati discusse in questa guida:

Amazon Macie

Amazon Macie rileva i dati sensibili utilizzando l'apprendimento automatico e il pattern matching e abilita la protezione automatizzata contro i rischi associati.

AWS KMS

AWS KMScrea e controlla le chiavi crittografiche che usi per proteggere i tuoi dati.

AWS CloudHSM

AWS CloudHSMfornisce moduli di sicurezza hardware ad alta disponibilità e basati sul cloud (). HSMs

AWS Certificate Manager

AWS Certificate Managergestisce la complessità della creazione, dell'archiviazione e del rinnovo di certificati e chiavi SSL/TLS X.509 pubblici e privati.

AWS Private CA

AWS Private CAconsente di creare gerarchie di autorità di certificazione private, incluse le autorità di certificazione principali e subordinate (). CAs

Gestione dei segreti AWS

Gestione dei segreti AWSconsente di gestire, recuperare e ruotare le credenziali del database, le credenziali delle applicazioni, i OAuth token, le chiavi API e altri segreti.

AWS Payment Cryptography

AWS Payment Cryptographyfornisce l'accesso alle funzioni crittografiche e alla gestione delle chiavi utilizzate nell'elaborazione dei pagamenti in conformità agli standard del settore delle carte di pagamento (PCI).

Comprendi i servizi AWS di protezione della rete e delle applicazioni

AWS offre diversi servizi per proteggere le reti e le applicazioni. AWS Shieldfornisce protezione contro gli attacchi Distributed Denial of Service (DDoS) e AWS WAFaiuta a proteggere le applicazioni Web dai comuni attacchi di sfruttamento del Web.

La tabella seguente riassume le offerte di protezione della rete e delle applicazioni illustrate in questa guida:

AWS Firewall Manager

AWS Firewall Managersemplifica le attività di amministrazione e manutenzione su più account e risorse di protezione.

AWS Network Firewall

AWS Network Firewallfornisce un firewall di rete gestito con stato e un servizio di rilevamento e prevenzione delle intrusioni con il tuo VPC.

AWS Shield

AWS Shieldfornisce protezioni contro gli attacchi DDo S per AWS le risorse a livello di rete, trasporto e applicazione.

AWS WAF

AWS WAFfornisce un firewall per applicazioni Web che consente di monitorare le richieste HTTP (S) inoltrate alle risorse protette delle applicazioni Web.

Comprendi i AWS servizi di rilevamento e risposta

AWS fornisce strumenti per aiutarvi a semplificare le operazioni di sicurezza in tutto AWS l'ambiente, compresi gli ambienti con più account. Ad esempio, puoi utilizzare Amazon GuardDuty per il rilevamento intelligente delle minacce e Amazon Detective per identificare e analizzare i risultati di sicurezza raccogliendo dati di registro. AWS Security Hub CSPMsupporta diversi standard di sicurezza e fornisce una panoramica degli avvisi di sicurezza e dello stato di conformità in tutto il mondo Account AWS. AWS CloudTrailtiene traccia delle attività degli utenti e dell'utilizzo dell'API (Application Programming Interface), un elemento fondamentale per comprendere e rispondere agli eventi di sicurezza.

La tabella seguente riassume le offerte di rilevamento e risposta discusse in questa guida:

AWS Config

AWS Configfornisce una visualizzazione dettagliata della configurazione delle AWS risorse del tuo. Account AWS

AWS CloudTrail

AWS CloudTrailregistra le azioni intraprese da un utente, ruolo o Servizio AWS.

AWS Security Hub CSPM

AWS Security Hub CSPMfornisce una visione completa dello stato di sicurezza in AWS.

Amazon GuardDuty

Amazon monitora GuardDuty continuamente i tuoi carichi di lavoro Account AWS, l'attività di runtime e i dati alla ricerca di attività dannose.

Amazon Inspector

Amazon Inspector analizza i AWS carichi di lavoro alla ricerca di vulnerabilità del software ed esposizione involontaria della rete.

Amazon Security Lake

Amazon Security Lake centralizza automaticamente i dati di sicurezza provenienti da AWS ambienti, provider SaaS, ambienti locali, fonti cloud e fonti di terze parti in un data lake.

Amazon Detective

Amazon Detective consente di analizzare, esaminare e identificare rapidamente la causa principale degli esiti di sicurezza o delle attività sospette.

AWS Security Incident Response

AWS Risposta agli incidenti di sicurezza

Ti aiuta a prepararti, rispondere e ricevere rapidamente indicazioni per aiutarti a riprenderti dagli incidenti di sicurezza.

Comprendi i servizi di AWS governance e conformità

AWS fornisce strumenti che consentono di rispettare gli standard di sicurezza, operativi, di conformità e di costo. Ad esempio, è possibile utilizzarlo AWS Control Towerper configurare e gestire un ambiente multi-account con controlli prescrittivi. Con AWS Organizations, puoi configurare una gestione basata su policy per più account all'interno della tua organizzazione.

AWS offre inoltre una visione completa dello stato di conformità e monitora continuamente l'ambiente utilizzando controlli di conformità automatizzati basati sulle AWS migliori pratiche e sugli standard di settore seguiti dall'organizzazione. Ad esempio, AWS Artifactfornisce l'accesso su richiesta ai report di conformità e AWS Audit Managerautomatizza la raccolta delle prove in modo da poter valutare più facilmente se i controlli funzionano in modo efficace.

La tabella seguente riassume le offerte di governance e conformità illustrate in questa guida:

AWS Organizations

AWS Organizationsti aiuta a consolidare più organizzazioni Account AWS in un'unica organizzazione da creare e gestire centralmente.

AWS Control Tower

AWS Control Towerti aiuta a configurare e gestire un ambiente AWS multi-account basato sulle migliori pratiche.

AWS Artifact

AWS Artifactfornisce download su richiesta di documenti di AWS sicurezza e conformità.

AWS Audit Manager

AWS Audit Manager

Ti aiuta a controllare continuamente AWS l'utilizzo per semplificare la valutazione del rischio e della conformità.

Prendi in considerazione i criteri di AWS sicurezza, identità e governance

La scelta dei servizi di sicurezza, identità e governance più adatti AWS dipende dai requisiti e dai casi d'uso specifici. La decisione di adottare un servizio AWS di sicurezza fornisce un albero decisionale che consente di decidere se l'adozione Servizi AWS per la sicurezza, l'identità e la governance è adatta alla propria organizzazione. Inoltre, ecco alcuni criteri da considerare quando si decide quali servizi utilizzare.

Security requirements and threat landscape

Conduci una valutazione completa delle vulnerabilità e delle minacce specifiche della tua organizzazione. Ciò comporta l'identificazione dei tipi di dati che gestisci, come informazioni personali sui clienti, registri finanziari o dati aziendali proprietari. Comprendi i potenziali rischi associati a ciascuno di essi.

Valuta l'architettura dell'applicazione e dell'infrastruttura. Determina se le tue applicazioni sono rivolte al pubblico e che tipo di traffico web gestiscono. Ciò influisce sulla necessità di servizi come la protezione dallo AWS WAF sfruttamento del web. Per le applicazioni interne, considera l'importanza del rilevamento interno delle minacce e del monitoraggio continuo con Amazon GuardDuty, che può identificare modelli di accesso insoliti o implementazioni non autorizzate.

Infine, considera la sofisticazione della tua attuale posizione di sicurezza e l'esperienza del tuo team di sicurezza. Se il tuo team dispone di risorse limitate, la scelta di servizi che offrono maggiore automazione e integrazione può offrirti miglioramenti efficaci della sicurezza, senza sovraccaricare il team. I servizi di AWS Shield esempio includono la protezione DDo S e AWS Security Hub CSPM il monitoraggio centralizzato della sicurezza.

Compliance and regulatory requirements

Identifica le leggi e gli standard pertinenti per il tuo settore o area geografica, come il Regolamento generale sulla protezione dei dati (GDPR), l'U.S. Health Insurance Portability and Accountability Act del 1996 (HIPAA) o il Payment Card Industry Data Security Standard (PCI DSS).

AWS offre servizi come AWS Config AWS Artifact per aiutarti a gestire la conformità a vari standard. Con AWS Config, è possibile valutare, controllare e valutare le configurazioni delle AWS risorse, semplificando la garanzia della conformità alle politiche interne e ai requisiti normativi. AWS Artifact fornisce l'accesso su richiesta AWS alla documentazione di conformità, aiutandoti con gli audit e i report di conformità.

La scelta di servizi in linea con le vostre specifiche esigenze di conformità può aiutare la vostra organizzazione a soddisfare i requisiti legali e creare un ambiente sicuro e affidabile per i vostri dati. Esplora i programmi di AWS conformità per saperne di più.

Scalability and flexibility

Considerate come crescerà la vostra organizzazione e quanto velocemente. Scegliete Servizi AWS questa soluzione per aiutare le vostre misure di sicurezza a crescere senza problemi con la vostra infrastruttura e ad adattarsi alle minacce in evoluzione.

Per aiutarti a scalare rapidamente, AWS Control Tower orchestra le funzionalità di molti altri Servizi AWS, tra cui AWS Organizations AWS IAM Identity Center, per creare una landing zone in meno di un'ora. Control Tower configura e gestisce le risorse per tuo conto.

AWS progetta inoltre molti servizi per adattarsi automaticamente al traffico e ai modelli di utilizzo di un'applicazione, come Amazon GuardDuty per il rilevamento delle minacce e AWS WAF per la protezione delle applicazioni web. Man mano che la tua azienda cresce, questi servizi crescono di pari passo, senza richiedere regolazioni manuali o causare intoppi.

Inoltre, è fondamentale poter personalizzare i controlli di sicurezza per adattarli ai requisiti aziendali e al panorama delle minacce. Prendi in considerazione la possibilità di gestire i tuoi account con AWS Organizations, in modo da poter gestire oltre 40 risorse di servizi su più account. Ciò offre ai singoli team applicativi la flessibilità e la visibilità necessarie per gestire le esigenze di sicurezza specifiche del loro carico di lavoro, garantendo al contempo la governance e la visibilità ai team di sicurezza centralizzati.

Considerare la scalabilità e la flessibilità aiuta a garantire un livello di sicurezza solido, reattivo e in grado di supportare ambienti aziendali dinamici.

Integration with existing systems

Prendi in considerazione misure di sicurezza che migliorino, anziché interrompere, le tue operazioni correnti. Ad esempio, considerate quanto segue:

- Semplifica i flussi di lavoro aggregando i dati di sicurezza e gli avvisi Servizi AWS e analizzandoli insieme ai sistemi SIEM (Security Information and Event Management) esistenti.
- Crea una visione unificata delle minacce e delle vulnerabilità alla sicurezza in entrambi gli ambienti e in locale. AWS
- Esegui AWS CloudTrail l'integrazione con le soluzioni di gestione dei log esistenti per il monitoraggio completo delle attività degli utenti e dell'utilizzo delle API nell' AWS infrastruttura e nelle applicazioni esistenti.
- Esamina i modi per ottimizzare l'utilizzo delle risorse e applicare in modo coerente le politiche di sicurezza in tutti gli ambienti. Ciò consente di ridurre il rischio di lacune nella copertura di sicurezza.

Cost and budget considerations

Esamina i modelli di prezzo per ogni servizio che stai considerando. AWS spesso addebiti in base all'utilizzo, ad esempio al numero di chiamate API, al volume di dati elaborati o alla quantità di dati archiviati. Ad esempio, Amazon GuardDuty addebita i costi in base alla quantità di dati di log analizzati per il rilevamento delle minacce, mentre le AWS WAF fatture si basano sul numero di regole implementate e sul numero di richieste Web ricevute.

Stima l'utilizzo previsto per prevedere i costi in modo accurato. Considerate sia le esigenze attuali che la crescita potenziale o i picchi della domanda. Ad esempio, la scalabilità è una caratteristica fondamentale di Servizi AWS, ma può anche portare a un aumento dei costi se non gestita con attenzione. Utilizzali Calcolatore dei prezzi AWSper modellare diversi scenari e valutarne l'impatto finanziario.

Valuta il costo totale di proprietà (TCO), che include sia i costi diretti che i costi indiretti, come il tempo e le risorse necessari per la gestione e la manutenzione. La scelta dei servizi gestiti può ridurre i costi operativi, ma potrebbe comportare un prezzo più elevato.

Infine, dai la priorità agli investimenti in sicurezza in base alla valutazione del rischio. Non tutti i servizi di sicurezza saranno altrettanto importanti per la vostra infrastruttura, quindi concentrate il budget sulle aree che avranno l'impatto più significativo sulla riduzione dei rischi e sulla garanzia

della conformità. Bilanciare l'economicità con il livello di sicurezza necessario è fondamentale per una strategia di sicurezza di successo AWS .

Organizational structure and access needs

Valuta come è strutturata e opera la tua organizzazione e in che modo le tue esigenze di accesso potrebbero variare in base al team, al progetto o all'ubicazione. Ciò influisce sul modo in cui gestisci e autentichi le identità degli utenti, assegni i ruoli e applichi i controlli di accesso in tutto l'ambiente. AWS Implementa le migliori pratiche, come l'applicazione delle autorizzazioni con privilegi minimi e la richiesta dell'autenticazione a più fattori (MFA).

La maggior parte delle organizzazioni necessita di un ambiente multi-account. Esamina le best practice per questo tipo di ambiente e valuta la possibilità di utilizzarlo AWS Organizations e aiutarti AWS Control Tower a implementarlo.

Un altro aspetto da considerare è la gestione delle credenziali e delle chiavi di accesso. Prendi in considerazione l'utilizzo di IAM Identity Center per centralizzare la gestione degli accessi su più Account AWS applicazioni aziendali, il che migliora sia la sicurezza che la comodità dell'utente. Per aiutarti a gestire senza problemi l'accesso tra gli account della tua organizzazione, IAM Identity Center si integra con. AWS Organizations

Inoltre, valuta in che modo questi servizi di gestione delle identità e degli accessi si integrano con i servizi di directory esistenti. Se disponi di un provider di identità esistente, puoi integrarlo con IAM Identity Center utilizzando SAML 2.0 o OpenID Connect (OIDC). IAM Identity Center supporta anche il provisioning System for Cross-domain Identity Management (SCIM) per aiutarti a mantenere sincronizzate le directory. Questo ti aiuta a garantire un'esperienza utente fluida e sicura durante l'accesso alle risorse. AWS

Scegli un AWS servizio di sicurezza, identità e governance

Ora che conosci i criteri per valutare le tue opzioni di sicurezza, sei pronto a scegliere quali servizi AWS di sicurezza potrebbero essere più adatti alle tue esigenze organizzative.

La tabella seguente evidenzia quali servizi sono ottimizzati per quali circostanze. Utilizza la tabella per determinare il servizio più adatto alla tua organizzazione e al tuo caso d'uso.

> **Note**
>
> [1] Si integra con AWS Security Hub CSPM (elenco completo)

[2] Si integra con Amazon GuardDuty (elenco completo)
[3] Si integra con Amazon Security Lake (elenco completo)

Scegli i servizi di gestione delle AWS identità e degli accessi

Concedi alle persone appropriate il livello di accesso appropriato a sistemi, applicazioni e dati.

Quando dovresti usarlo?	Per cosa è ottimizzato?	Servizi di sicurezza, identità e governance
Utilizza questi servizi per aiutarti a gestire e governare in modo sicuro l'accesso per clienti, forza lavoro e carichi di lavoro.	Ti aiuta a connettere la tua fonte di identità o a creare utenti. È possibile gestire centralmente l'accesso della forza lavoro a più AWS account e applicazioni.	AWS IAM Identity Center
	Ottimizzato per l'autenti cazione e l'autorizzazione degli utenti per applicazioni web e mobili.	Amazon Cognito
	Ottimizzato per la condivisione sicura delle risorse interne. AWS	AWS RAM
	Consente un controllo sicuro e preciso sull'accesso alle risorse del carico di lavoro. AWS	IAM 1

Scegli AWS i servizi di protezione dei dati

Automatizza e semplifica le attività di protezione e sicurezza dei dati che vanno dalla gestione delle chiavi e dall'individuazione di dati sensibili alla gestione delle credenziali.

Quando dovresti usarlo?	Per cosa è ottimizzato?	Servizi di protezione dei dati
Utilizzate questi servizi per aiutarvi a raggiungere e mantenere la riservatezza, l'integrità e la disponibilità dei dati sensibili archiviati ed elaborati all'interno AWS degli ambienti.	Ottimizzato per la scoperta di dati sensibili.	Amazon Macie 1
	Ottimizzato per chiavi crittografiche.	AWS KMS
	Ottimizzato per HSMs.	AWS CloudHSM
	Ottimizzato per certificati e SSL/TLS chiavi X.509 privati.	AWS Certificate Manager
	Ottimizzato per la creazione di gerarchie di autorità di certificazione private.	AWS Private CA
	Ottimizzato per credenziali di database, credenziali di applicazioni, OAuth token, chiavi API e altri segreti.	Gestione dei segreti AWS
	Ottimizzato per fornire l'accesso alle funzioni crittografiche e alla gestione delle chiavi utilizzate nell'elaborazione dei pagamenti in conformità con gli standard PCI.	AWS Payment Cryptography

Scegli i servizi AWS di protezione della rete e delle applicazioni

Proteggi centralmente le tue risorse Internet dai comuni DDo attacchi al sistema operativo e alle applicazioni.

Quando dovresti usarla?	Per cosa è ottimizzato?	Servizi di protezione di reti e applicazioni
Utilizzate questi servizi per aiutarvi ad applicare politiche di sicurezza dettagliate in ogni punto di controllo della rete.	Ottimizzato per la configura zione e la gestione centraliz zate delle regole del firewall.	AWS Firewall Manager[1]
	Ottimizzato per fornire un firewall di rete gestito e dotato di stato e un servizio di rilevamento e prevenzione delle intrusioni.	AWS Network Firewall
	Ottimizzato per la protezion e dagli attacchi DDo S per AWS le risorse a livello di rete, trasporto e applicazione.	AWS Shield
	Ottimizzato per fornire un firewall per applicazioni Web.	AWS WAF

Scegli i servizi di AWS rilevamento e risposta

Identifica e assegna continuamente priorità ai rischi per la sicurezza, integrando tempestivamente le migliori pratiche di sicurezza.

Quando dovresti usarlo?	Per cosa è ottimizzato?	Servizi di rilevamento e risposta
Utilizza questi servizi per aiutarti a rilevare e risponder e ai rischi per la sicurezza dei tuoi account, in modo da proteggere i carichi di lavoro su larga scala.	Ottimizzato per automatiz zare i controlli di sicurezza e centralizzare gli avvisi di sicurezza con integrazioni di terze parti. AWS	AWS Security Hub CSPM[2, 3]
	Ottimizzato per la valutazio ne, il controllo e la valutazio	AWS Config[1]

Quando dovresti usarlo?	Per cosa è ottimizzato?	Servizi di rilevamento e risposta
	ne della configurazione delle risorse.	
	Ottimizzato per la registrazione di eventi Servizi AWS altrui come audit trail.	AWS CloudTrail
	Ottimizzato per il rilevamento intelligente delle minacce e la reportistica dettagliata.	Amazon GuardDuty [1]
	Ottimizzato per la gestione delle vulnerabilità.	Amazon Inspector 1
	Ottimizzato per centralizzare i dati di sicurezza.	Amazon Security Lake [1]
	Ottimizzato per l'aggregazione e il riepilogo di potenziali problemi di sicurezza.	Amazon Detective [1, 2, 3]
	Ottimizzato per aiutarti a valutare i risultati, intensificare gli eventi di sicurezza e gestire i casi che richiedono la tua attenzione immediata.	AWS Risposta agli incidenti di sicurezza

Scegli i servizi di AWS governance e conformità

Stabilisci la governance del cloud per tutte le tue risorse e automatizza i processi di conformità e controllo.

Quando dovresti usarlo?	Per cosa è ottimizzato?	Servizi di governance e conformità
Utilizza questi servizi per aiutarti a implementare le migliori pratiche e soddisfare gli standard di settore durante l'utilizzo AWS.	Ottimizzato per la gestione centralizzata di più account e la fatturazione consolidata.	AWS Organizations
	Ottimizzato per fornire download su richiesta di documenti di AWS sicurezza e conformità.	AWS Artifact
	Ottimizzato per il controllo dell'utilizzo. AWS	AWS Audit Manager[1]
	Ottimizzato per la configura zione e la gestione di un ambiente AWS multi-account.	AWS Control Tower

Utilizza AWS servizi di sicurezza, identità e governance

Ora dovresti avere una chiara comprensione di ciò che fa ogni servizio di AWS sicurezza, identità e governance (e degli AWS strumenti e servizi di supporto) e quali potrebbero essere quelli giusti per te.

Per scoprire come utilizzare e saperne di più su ciascuno dei servizi di AWS sicurezza, identità e governance disponibili, abbiamo fornito un percorso per scoprire come funziona ciascuno di essi. Le sezioni seguenti forniscono collegamenti a documentazione approfondita, tutorial pratici e risorse per iniziare.

Utilizza i servizi di gestione delle identità e degli accessi AWS

Le tabelle seguenti mostrano alcune utili risorse per la gestione delle identità e degli accessi, organizzate per servizio, per aiutarti a iniziare.

AWS IAM Identity Center

- Abilitazione di AWS IAM Identity Center

  Abilita IAM Identity Center e inizia a usarlo con il tuo AWS Organizations.

  Esplora la guida
- Configura l'accesso degli utenti con la directory IAM Identity Center predefinita

  Utilizza la directory predefinita come origine dell'identità e configura e testa l'accesso degli utenti.

  Inizia con il tutorial
- Utilizzo di Active Directory come fonte di identità

  Completa la configurazione di base per l'utilizzo di Active Directory come fonte di identità IAM Identity Center.

  Inizia con il tutorial
- Configura SAML e SCIM con Okta e IAM Identity Center

  Configura una connessione SAML con Okta e IAM Identity Center.

  Inizia con il tutorial

Amazon Cognito

- Guida introduttiva ad Amazon Cognito

  Scopri le attività più comuni di Amazon Cognito.

  Esplora la guida
- Tutorial: creazione di un pool di utenti

  Crea un pool di utenti, che consente agli utenti di accedere alla tua app web o mobile.

  Inizia con il tutorial
- Tutorial: creazione di un pool di identità

Crea un pool di identità, che consente agli utenti di ottenere AWS credenziali temporanee per l'accesso Servizi AWS.

Inizia con il tutorial

- Workshop Amazon Cognito

  Fai pratica con Amazon Cognito per creare una soluzione di autenticazione per un ipotetico negozio di animali.

  Inizia con il tutorial

AWS RAM

- Iniziare con AWS RAM

  Scopri AWS RAM termini e concetti.

  Esplora la guida
- Lavorare con AWS risorse condivise

  Condividi AWS le risorse che possiedi e accedi alle AWS risorse condivise con te.

  Esplora la guida
- Gestione delle autorizzazioni nella RAM AWS

  Scopri i due tipi di autorizzazioni gestite: autorizzazioni gestite e autorizzazioni AWS gestite dai clienti.

  Esplora la guida
- Configura l'accesso dettagliato alle risorse condivise tramite AWS RAM

  Utilizza le autorizzazioni gestite dal cliente per personalizzare l'accesso alle risorse e ottenere la migliore pratica del privilegio minimo.

  Leggi il blog

IAM

- Guida introduttiva a IAM

Crea ruoli, utenti e politiche IAM utilizzando Console di gestione AWS.

Inizia con il tutorial

- Delega l'accesso tra diversi Account AWS ruoli

  Usa un ruolo per delegare l'accesso alle risorse di tua Account AWS proprietà chiamato Produzione e sviluppo.

  Inizia con il tutorial

- Crea una politica gestita dai clienti

  Utilizza il Console di gestione AWS per creare una policy gestita dai clienti e poi associala a un utente IAM del tuo Account AWS.

  Inizia con il tutorial

- Definisci le autorizzazioni per accedere alle AWS risorse in base ai tag

  Crea e testa una policy che consenta ai ruoli IAM con tag principali di accedere alle risorse con tag corrispondenti.

  Inizia con il tutorial

- Best practice per la sicurezza in IAM

  Contribuisci a proteggere AWS le tue risorse utilizzando le best practice di IAM.

  Esplora la guida

Utilizza AWS i servizi di protezione dei dati

La sezione seguente fornisce collegamenti a risorse dettagliate che descrivono la protezione AWS dei dati.

Macie

- Guida introduttiva ad Amazon Macie

  Abilita Macie per te Account AWS, valuta il tuo livello di sicurezza di Amazon S3 e configura le impostazioni e le risorse chiave per scoprire e segnalare dati sensibili nei tuoi bucket S3.

Esplora la guida

- Monitoraggio della sicurezza e della privacy dei dati con Amazon Macie

  Usa Amazon Macie per monitorare la sicurezza dei dati di Amazon S3 e valutare il tuo livello di sicurezza.

  Esplora la guida
- Analisi dei risultati di Amazon Macie

  Rivedi, analizza e gestisci i risultati di Amazon Macie.

  Esplora la guida
- Recupero di campioni di dati sensibili con i risultati di Amazon Macie

  Usa Amazon Macie per recuperare e rivelare campioni di dati sensibili riportati da singoli risultati.

  Esplora la guida
- Alla scoperta di dati sensibili con Amazon Macie

  Automatizza l'individuazione, la registrazione e il reporting di dati sensibili nel tuo patrimonio di dati Amazon S3.

  Esplora la guida

AWS KMS

- Iniziare con AWS KMS

  Gestisci le chiavi KMS di crittografia simmetrica, dalla creazione all'eliminazione.

  Esplora la guida
- Chiavi per usi speciali

  Scopri i diversi tipi di chiavi che AWS KMS supporta, oltre alle chiavi KMS con crittografia simmetrica.

  Esplora la guida
- Scalabilità delle funzionalità di crittografia a riposo con AWS KMS

Scopri le opzioni di crittografia a riposo disponibili all'interno AWS.

Esplora il workshop

AWS CloudHSM

- Iniziare con AWS CloudHSM

  Crea, inizializza e attiva un AWS CloudHSM cluster.

  Esplora la guida
- Gestione dei AWS CloudHSM cluster

  Connect al AWS CloudHSM cluster e alle varie attività amministrative relative alla gestione del cluster.

  Esplora la guida
- Gestione degli utenti e delle chiavi HSM AWS CloudHSM

  Crea utenti e chiavi HSMs nel tuo cluster.

  Esplora la guida
- Automatizza la distribuzione di un servizio web NGINX utilizzando Amazon ECS con offload TLS in CloudHSM

  Utilizzalo AWS CloudHSM per archiviare le chiavi private per i tuoi siti Web ospitati nel cloud.

  Leggi il blog

AWS Certificate Manager

- Richiesta di un certificato pubblico

  Utilizza la console AWS Certificate Manager (ACM) o AWS CLI per richiedere un certificato ACM pubblico.

  Esplora la guida
- Le migliori pratiche per AWS Certificate Manager

Scopri le migliori pratiche basate sull'esperienza reale degli attuali clienti ACM.

Esplora la guida

- Come utilizzare per AWS Certificate Manager applicare i controlli sull'emissione dei certificati

  Utilizza le chiavi di condizione IAM per assicurarti che i tuoi utenti emettano o richiedano certificati TLS in conformità con le linee guida della tua organizzazione.

  Leggi il blog

AWS Private CA

- Pianificazione dell' AWS Private CA implementazione

  AWS Private CA Preparati all'uso prima di creare un'autorità di certificazione privata.

  Esplora la guida
- AWS Private CA amministrazione

  Crea una gerarchia interamente AWS ospitata di autorità di certificazione principali e subordinate per uso interno da parte dell'organizzazione.

  Esplora la guida
- Amministrazione dei certificati

  Esegui attività di amministrazione dei certificati di base con AWS Private CA, ad esempio, l'emissione, il recupero e l'elenco di certificati privati.

  Esplora la guida
- AWS Private CA officina

  Sviluppa un'esperienza pratica con vari casi d'uso delle autorità di certificazione private.

  Esplora il workshop
- Come semplificare il provisioning dei certificati in Active Directory con AWS Private CA

  AWS Private CA Utilizzalo per fornire più facilmente certificati per utenti e macchine all'interno del tuo ambiente Microsoft Active Directory.

Leggi il blog

- Come applicare i vincoli relativi ai nomi DNS in AWS Private CA

  Applica i vincoli di nome DNS a una CA subordinata utilizzando il servizio. AWS Private CA

  Leggi il blog

Gestione dei segreti AWS

- Gestione dei segreti AWS concetti

  Esegui attività di amministrazione dei certificati di base con AWS Private CA, ad esempio, l'emissione, il recupero e l'elenco di certificati privati.

  Esplora la guida
- Imposta la rotazione alternata degli utenti per Gestione dei segreti AWS

  Imposta una rotazione alternata degli utenti per un segreto che contiene le credenziali del database.

  Esplora la guida
- Usare Gestione dei segreti AWS i segreti con Kubernetes

  Mostra i segreti di Secrets Manager come file montati nei pod Amazon EKS utilizzando AWS Secrets and Configuration Provider (ASCP).

  Esplora la guida

AWS Payment Cryptography

- Iniziare con AWS Payment Cryptography

  Crea chiavi e usale in varie operazioni crittografiche.

  Esplora la guida
- AWS Payment Cryptography FAQs

  Comprendi le basi di. AWS Payment Cryptography

Esplora il FAQs

Utilizza i servizi di protezione AWS della rete e delle applicazioni

Le tabelle seguenti forniscono collegamenti a risorse dettagliate che descrivono la protezione AWS di reti e applicazioni.

AWS Firewall Manager

- Guida introduttiva alle AWS Firewall Manager politiche

  AWS Firewall Manager Utilizzalo per attivare diversi tipi di politiche di sicurezza.

  Esplora la guida
- Come controllare e limitare continuamente i gruppi di sicurezza con AWS Firewall Manager

  AWS Firewall Manager Utilizzatelo per limitare i gruppi di sicurezza, assicurando che siano aperte solo le porte necessarie.

  Leggi il blog
- Utilizzalo AWS Firewall Manager per implementare la protezione su larga scala in AWS Organizations

  Utilizzalo AWS Firewall Manager per implementare e gestire le politiche di sicurezza in tutto il tuo. AWS Organizations

  Leggi il blog

AWS Network Firewall

- Iniziare con AWS Network Firewall

  Configura e implementa un AWS Network Firewall firewall per un VPC con un'architettura gateway Internet di base.

  Esplora la guida
- AWS Network Firewall Workshop

  Implementa AWS Network Firewall e utilizza l'infrastruttura come codice.

Esplora il workshop

- Guida pratica al motore di regole AWS Network Firewall flessibili — Parte 1

  Implementa una dimostrazione di AWS Network Firewall within your Account AWS per interagire con il suo motore di regole.

  Leggi il blog

- Guida pratica del motore di regole AWS Network Firewall flessibili — Parte 2

  Crea una politica firewall con un ordine di regole rigoroso e imposta una o più azioni predefinite.

  Leggi il blog

- Modelli di implementazione per AWS Network Firewall

  Scopri i modelli di implementazione per i casi d'uso più comuni in cui puoi aggiungere AWS Network Firewall elementi al percorso di traffico.

  Leggi il blog

- Modelli di implementazione per AWS Network Firewall i miglioramenti del routing VPC

  Utilizza primitive di routing VPC avanzate per l'inserimento AWS Network Firewall tra carichi di lavoro in diverse sottoreti dello stesso VPC.

  Leggi il blog

AWS Shield

- Come AWS Shield funziona

  Scopri come AWS Shield Standard e AWS Shield Advanced fornisci protezioni contro gli attacchi DDo S per AWS le risorse a livello di rete e trasporto (livello 3 e 4) e a livello di applicazione (livello 7).

  Esplora la guida

- Iniziare con AWS Shield Advanced

  Inizia a usare la console Shield Advanced. AWS Shield Advanced

  Esplora la guida

- AWS Shield Advanced officina

  Proteggi le risorse esposte a Internet dagli attacchi DDo S, monitora gli attacchi DDo S contro la tua infrastruttura e avvisa i team appropriati.

  Esplora il workshop

AWS WAF

- Iniziare con AWS WAF

  Configura AWS WAF, crea un ACL web e proteggi Amazon CloudFront aggiungendo regole e gruppi di regole per filtrare le richieste web.

  Inizia con il tutorial
- Analisi dei AWS WAF log in Amazon Logs CloudWatch

  Configura AWS WAF la registrazione nativa CloudWatch nei log di Amazon e visualizza e analizza i dati nei log.

  Leggi il blog
- Visualizza i AWS WAF log con una dashboard di Amazon CloudWatch

  Usa Amazon CloudWatch per monitorare e analizzare le AWS WAF attività utilizzando CloudWatch metriche, Contributor Insights e Logs Insights.

  Leggi il blog

Utilizza i servizi di AWS rilevamento e risposta

Le tabelle seguenti forniscono collegamenti a risorse dettagliate che descrivono i servizi di AWS rilevamento e risposta.

AWS Config

- Guida introduttiva con AWS Config

  Configura AWS Config e lavora con AWS SDKs.

  Esplora la guida

- Workshop su rischi e conformità

  Automatizza i controlli utilizzando AWS Config e AWS Managed Config Rules.

  Esplora il workshop
- AWS Config Libreria Rule Development Kit: crea e gestisci regole su larga scala

  Usa il Rule Development Kit (RDK) per creare una AWS Config regola personalizzata e distribuirla con. RDKLib

  Leggi il blog

AWS CloudTrail

- Visualizza la cronologia degli eventi

  Controlla l'attività delle AWS API nella tua Account AWS pagina dei servizi che supportano CloudTrail.

  Inizia con il tutorial
- Crea un percorso per registrare gli eventi di gestione

  Crea un percorso per registrare gli eventi di gestione in tutte le regioni.

  Inizia con il tutorial

AWS Security Hub CSPM

- Abilitazione AWS Security Hub CSPM

  Abilita AWS Security Hub CSPM con AWS Organizations o in un account autonomo.

  Esplora la guida
- Aggregazione tra regioni

  AWS Security Hub CSPM Risultati aggregati da più regioni di aggregazione Regioni AWS a una singola.

  Esplora la guida
- AWS Security Hub CSPM officina

Scopri come utilizzare, gestire AWS Security Hub CSPM e migliorare il livello di sicurezza dei tuoi AWS ambienti.

Esplora il workshop

- Tre modelli di utilizzo ricorrenti del Security Hub CSPM e come implementarli

  Scopri i tre modelli di AWS Security Hub CSPM utilizzo più comuni e come migliorare la tua strategia di identificazione e gestione dei risultati.

  Leggi il blog

Amazon GuardDuty

- Guida introduttiva ad Amazon GuardDuty

  Abilita Amazon GuardDuty, genera risultati di esempio e configura avvisi.

  Esplora il tutorial

- Protezione EKS in Amazon GuardDuty

  Usa Amazon GuardDuty per monitorare i log di controllo di Amazon Elastic Kubernetes Service (Amazon EKS).

  Esplora la guida

- Protezione Lambda in Amazon GuardDuty

  Identifica potenziali minacce alla sicurezza quando richiami una AWS Lambda funzione.

  Esplora la guida

- GuardDuty Protezione Amazon RDS

  Usa Amazon GuardDuty per analizzare e profilare l'attività di accesso ad Amazon Relational Database Service (Amazon RDS) per potenziali minacce di accesso ai tuoi database Amazon Aurora.

  Esplora la guida

- Protezione Amazon S3 in Amazon GuardDuty

Utilizzala GuardDuty per monitorare gli eventi CloudTrail relativi ai dati e identificare potenziali rischi per la sicurezza all'interno dei bucket S3.

Esplora la guida

- Rilevamento e risposta alle minacce con Amazon GuardDuty e Amazon Detective

  Scopri le nozioni di base di Amazon GuardDuty e Amazon Detective.

  Esplora il workshop

Amazon Inspector

- Guida introduttiva ad Amazon Inspector

  Attiva le scansioni di Amazon Inspector per comprendere i risultati nella console.

  Inizia con il tutorial

- Gestione delle vulnerabilità con Amazon Inspector

  Usa Amazon Inspector per scansionare le istanze Amazon EC2 e le immagini dei container in Amazon Elastic Container Registry (Amazon ECR) alla ricerca di vulnerabilità del software.

  Esplora il workshop

- Come scansionare EC2 AMIs utilizzando Amazon Inspector

  Crea una soluzione utilizzandone più di una Servizi AWS per scansionare le tue AMIs vulnerabilità note.

  Leggi il blog

Amazon Security Lake

- Guida introduttiva ad Amazon Security Lake

  Abilita e inizia a utilizzare Amazon Security Lake.

  Esplora la guida

- Gestione di più account con AWS Organizations

Raccogli registri di sicurezza ed eventi da più Account AWS siti.

Esplora la guida

- Inserisci, trasforma e distribuisci eventi pubblicati da Amazon Security Lake su Amazon Service OpenSearch

  Acquisisci, trasforma e distribuisci i dati di Amazon Security Lake ad Amazon OpenSearch Service per utilizzarli dai tuoi SecOps team.

  Leggi il blog

- Come visualizzare gli esiti di Amazon Security Lake con Quick

  Interroga e visualizza i dati da Amazon Security Lake utilizzando Amazon Athena e Quick.

  Leggi il blog

Amazon Detective

- Termini e concetti di Amazon Detective

  Scopri i termini e i concetti chiave importanti per comprendere Amazon Detective e come funziona.

  Esplora la guida

- Configurazione di Amazon Detective

  Abilita Amazon Detective dalla console Amazon Detective, dall'API Amazon Detective o AWS CLI.

  Esplora la guida

- Rilevamento e risposta alle minacce con Amazon GuardDuty e Amazon Detective

  Scopri le nozioni di base di Amazon GuardDuty e Amazon Detective.

  Esplora il workshop

Utilizza i servizi di AWS governance e conformità

Le tabelle seguenti forniscono collegamenti a risorse dettagliate che descrivono la governance e la conformità.

AWS Organizations

- Creazione e configurazione di un'organizzazione

  Crea la tua organizzazione e configurala con due account AWS membri.

  Inizia con il tutorial
- Servizi che funzionano con AWS Organizations

  Scopri quali servizi Servizi AWS puoi utilizzare AWS Organizations e i vantaggi derivanti dall'utilizzo di ciascun servizio a livello di organizzazione.

  Esplora la guida
- Organizzazione dell' AWS ambiente utilizzando più account

  Implementa le migliori pratiche e i consigli attuali per organizzare AWS l'ambiente generale.

  Leggete il white paper

AWS Artifact

- Iniziare con AWS Artifact

  Scarica report sulla sicurezza e sulla conformità, gestisci gli accordi legali e gestisci le notifiche.

  Esplora la guida
- Gestione degli accordi in AWS Artifact

  Utilizzalo Console di gestione AWS per rivedere, accettare e gestire gli accordi per il tuo account o la tua organizzazione.

  Esplora la guida
- Prepararsi per un audit nella AWS parte 1: AWS Audit Manager e AWS Artifact AWS Config

Servizi AWS Utilizzatelo per aiutarvi ad automatizzare la raccolta delle prove utilizzate negli audit.

Leggi il blog

AWS Audit Manager

- Abilitazione di AWS Audit Manager

  Abilita Audit Manager utilizzando Console di gestione AWS, l'API Audit Manager o il AWS CLI.

  Esplora la guida
- Tutorial per i titolari di audit: creazione di una valutazione

  Crea una valutazione utilizzando l'Audit Manager Sample Framework.

  Esplora la guida
- Tutorial per delegati: revisione di un set di controlli

  Rivedi un set di controlli che è stato condiviso con te dal proprietario di un audit in Audit Manager.

  Esplora la guida

AWS Control Tower

- Iniziare con AWS Control Tower

  Configura e avvia un ambiente multi-account, chiamato landing zone, che segue le migliori pratiche prescrittive.

  Esplora la guida
- Modernizzazione della gestione degli account con Amazon Bedrock e AWS Control Tower

  Fornisci un account con strumenti di sicurezza e sfrutta l'intelligenza artificiale generativa per accelerare il processo di configurazione e gestione. Account AWS

  Leggi il blog
- Creazione di un ambiente ben architettato AWS GovCloud (USA) con AWS Control Tower

Imposta la tua governance nelle regioni AWS GovCloud (Stati Uniti), inclusa la gestione dei AWS carichi di lavoro utilizzando le unità organizzative () OUs e. Account AWS

Leggi il blog

Esplora i servizi di AWS sicurezza, identità e governance

Editable architecture diagrams

Diagrammi di architettura di riferimento

Esplora i diagrammi dell'architettura di riferimento per aiutarti a sviluppare la tua strategia di sicurezza, identità e governance.

Esplora le architetture di riferimento per la sicurezza, l'identità e la governance

Ready-to-use code

Soluzione in evidenza

Approfondimenti sulla sicurezza su AWS

AWS Implementa codice integrato per aiutarti a visualizzare i dati in Amazon Security Lake per indagare e rispondere più rapidamente agli eventi di sicurezza.

Esplora questa soluzione

AWS Soluzioni

Esplora le soluzioni preconfigurate e implementabili e le relative guide all'imple mentazione, create da. AWS

Esplora tutte le soluzioni AWS di sicurezza, identità e governance

Documentation

White paper su sicurezza, identità e governance

Consulta i white paper per ulteriori approfond imenti e best practice sulla scelta, l'impleme ntazione e l'utilizzo dei servizi di sicurezza

AWS Blog sulla sicurezza

Esplora i post del blog che trattano casi d'uso specifici della sicurezza.

Esplora il blog AWS sulla sicurezza

, identità e governance più adatti alla tua organizzazione.

Esplora i white paper su sicurezza, identità e governance

Cronologia dei documenti

La tabella seguente descrive le modifiche importanti a questa guida decisionale. Per ricevere notifiche sugli aggiornamenti di questa guida, puoi iscriverti a un feed RSS.

Modifica	Descrizione	Data
Aggiornamento re:Invent	Sono state aggiunte informazioni su AWS Security Incident Response e. AWS Payment Cryptography Informazioni di servizio aggiornate per AWS Identity and Access Management e AWS IAM Identity Center.	30 dicembre 2024
Aggiornamento video	Video introduttivo aggiornato con un recente intervento fulmineo di RE:InForce 2024.	25 giugno 2024
Servizi di governance aggiunti	Ampliato l'ambito del documento per includere la governance, inclusa l'aggiunta di AWS CloudTrail AWS Control Tower, e AWS Organizations. Grafica aggiornata per riflettere il nuovo ambito. Migliori pratiche chiarite per l'identità. Modifiche editoriali in varie parti del documento.	7 giugno 2024
Pubblicazione iniziale	Guida pubblicata per la prima volta.	21 marzo 2024

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.