Whitepaper da AWS

Introdução à segurança da AWS

Introdução à segurança da AWS: Whitepaper da AWS

Table of Contents

Introdução à segurança da AWS

Data de publicação: 11 de novembro de 2021 (Revisões do documento)

Resumo

A Amazon Web Services (AWS) fornece uma plataforma de computação em nuvem escalável, de alta confiabilidade e disponibilidade, com ferramentas que permitem executar uma grande variedade de aplicações. Ajudar a proteger a confidencialidade, a integridade e a disponibilidade de sistemas e dados é de suma importância para a AWS, assim como também é importante manter a confiança dos clientes. Este documento é uma introdução à abordagem de segurança da AWS, incluindo os controles no ambiente da AWS e alguns dos produtos e recursos disponíveis para atender aos objetivos de segurança dos clientes.

Segurança da infraestrutura da AWS

A infraestrutura da AWS foi projetada para ser um dos ambientes de computação em nuvem mais flexíveis e seguros disponíveis no momento. Ela foi desenvolvida para oferecer uma plataforma extremamente escalável e altamente confiável que permite aos clientes implantar aplicações e dados com rapidez e segurança.

Essa infraestrutura é criada e gerenciada não somente de acordo com práticas recomendadas e padrões de segurança, mas também com as necessidades exclusivas da nuvem. A AWS usa controles redundantes e em camadas, validação e testes contínuos, além de uma automação substancial, para garantir que a infraestrutura subjacente seja monitorada e protegida 24 horas por dia, 7 dias por semana. Além disso, a AWS garante que esses controles sejam replicados em cada novo datacenter ou serviço.

Todos os clientes da AWS podem se beneficiar com um datacenter e uma arquitetura de rede criados para atender aos requisitos dos clientes com as maiores exigências de segurança. Isso significa que você obterá uma infraestrutura resiliente e projetada para alta segurança, sem o gasto de capital e as despesas operacionais de um datacenter tradicional.

A AWS opera em um modelo de responsabilidade de segurança compartilhada, no qual ela é responsável pela segurança da infraestrutura de nuvem subjacente e você tem a incumbência de proteger as workloads que implanta na AWS (Figura 1). Isso oferece a flexibilidade e a agilidade de que você precisa para implementar os controles de segurança mais apropriados para suas funções de negócios no ambiente da AWS. Você pode restringir com rigor o acesso aos ambientes que processam dados confidenciais ou implantar controles menos restritos para as informações que desejar tornar públicas.

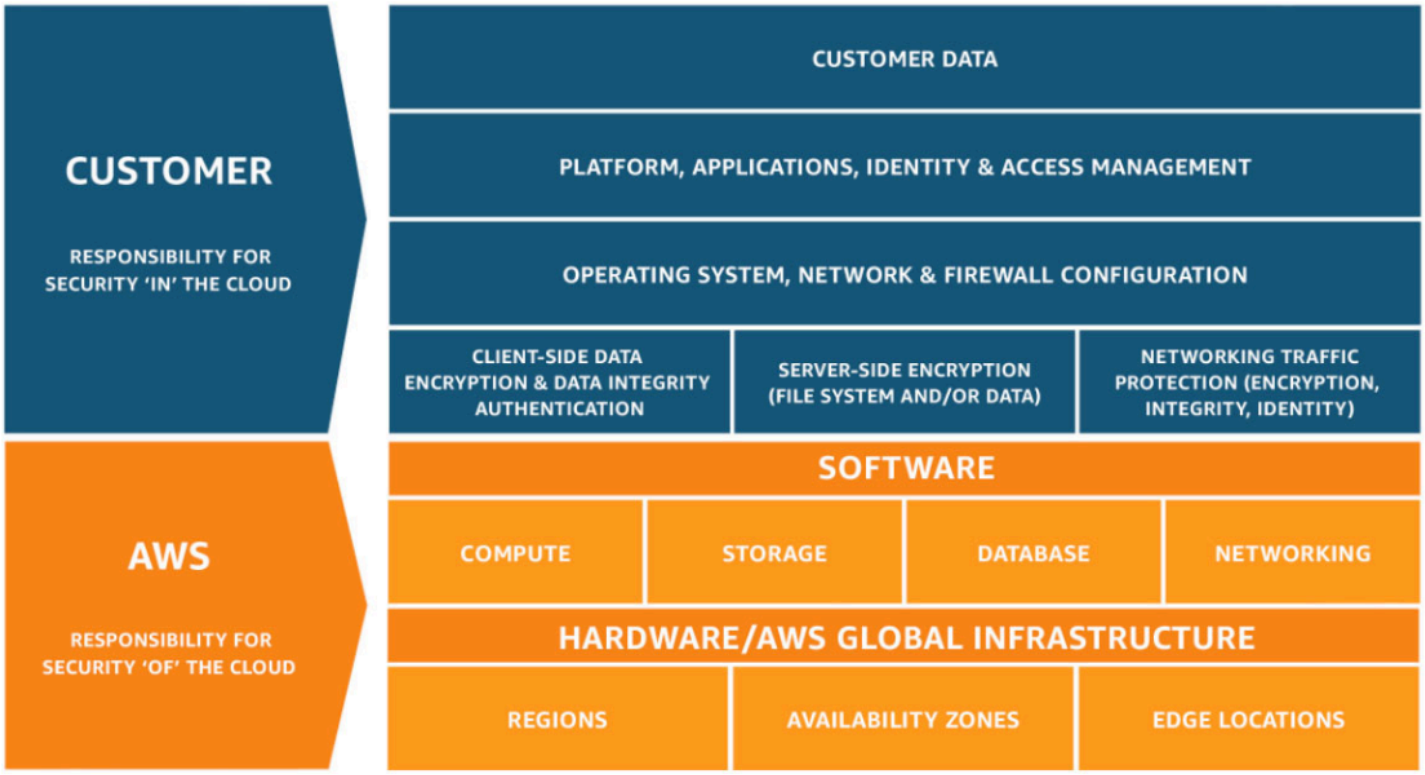

Figura 1: Modelo de responsabilidade de segurança compartilhada da AWS

Produtos e recursos de segurança

A AWS e seus parceiros oferecem uma ampla variedade de ferramentas e recursos para ajudar você a atingir seus objetivos de segurança. Essas ferramentas refletem os controles bem conhecidos que você implanta em seus ambientes on-premises. A AWS fornece ferramentas e recursos de segurança que abrangem segurança de rede, gerenciamento de configuração, controle de acesso e segurança de dados. Além disso, a AWS oferece ferramentas de monitoramento e registro em log para proporcionar total visibilidade do que está acontecendo no ambiente.

Tópicos

Infraestrutura de segurança

A AWS oferece diversos recursos e serviços de segurança para aumentar a privacidade e controlar o acesso à rede. Estes são alguns exemplos:

- Firewalls de rede integrados à Amazon VPC que permitem criar redes privadas e controlar o acesso às instâncias e aplicações. Os clientes podem controlar a criptografia em trânsito com TLS nos serviços da AWS.
- Opções de conectividade que permitem conexões privadas, ou dedicadas, em seu escritório ou no ambiente on-premise.
- Tecnologias de mitigação de DDoS aplicáveis às camadas 3, 4 e 7. Elas podem ser implementadas como parte das estratégias de entrega de aplicações e conteúdo.
- Criptografia automática de todo o tráfego nas redes globais e regionais da AWS entre instalações protegidas da AWS.

Gerenciamento de inventário e configuração

A AWS oferece diversas ferramentas para agilizar seu trabalho e, ao mesmo tempo, garantir que seus recursos de nuvem estejam em conformidade com os padrões e as práticas recomendadas. Estes são alguns exemplos:

- Ferramentas de implantação para gerenciar a criação e a desativação de recursos da AWS de acordo com os padrões da organização.
- Ferramentas de gerenciamento de inventário e configuração para identificar recursos da AWS e, depois, rastrear e gerenciar as alterações desses recursos ao longo do tempo.
- Ferramentas de definição e gerenciamento de modelos para criar máquinas virtuais padrão, pré-configuradas e reforçadas para instâncias do EC2.

Criptografia de dados

A AWS permite adicionar uma camada de segurança a seus dados em repouso na nuvem, fornecendo recursos de criptografia escaláveis e eficientes. Estes são alguns exemplos:

- Recursos de criptografia de dados em repouso disponíveis na maioria dos serviços da AWS, como o Amazon EBS, o Amazon S3, o Amazon RDS, o Amazon Redshift, o Amazon ElastiCache, o AWS Lambda e o Amazon SageMaker
- Opções flexíveis de gerenciamento de chaves, incluindo o AWS Key Management Service, que permitem a você optar entre o gerenciamento das chaves de criptografia pela AWS ou manter o controle completo sobre suas próprias chaves
- Armazenamento de chaves criptográficas dedicado e baseado em hardware usando o AWS CloudHSM, para ajudar você a cumprir seus requisitos de conformidade
- Filas de mensagens criptografadas para a transmissão de dados confidenciais usando criptografia no lado do servidor (SSE) para Amazon SQS.

Além disso, a AWS fornece APIs para você integrar criptografia e proteção de dados a qualquer serviço que desenvolver ou implantar em um ambiente da AWS.

Identidade e controle de acesso

A AWS oferece recursos para você definir, reforçar e gerenciar políticas de acesso de usuários nos serviços da AWS. Estes são alguns exemplos:

- O AWS Identity and Access Management (IAM) permite definir contas de usuários individuais com permissões em todos os recursos da AWS. O AWS Multi-Factor Authentication se destina a contas com privilégios de acesso e inclui opções para autenticadores baseados em software e hardware. O IAM pode ser usado para conceder a seus funcionários e suas aplicações acesso federado ao Console de gerenciamento da AWS e APIs de serviços da AWS usando seus sistemas de identidade atuais, como o Microsoft Active Directory ou outra oferta de parceiros.
- O AWS Directory Service permite a integração e a federação com diretórios corporativos para reduzir a sobrecarga administrativa e melhorar a experiência do usuário final.
- O AWS Single Sign-On (AWS SSO) possibilita o gerenciamento centralizado do acesso SSO e das permissões de usuário em todas as suas contas do AWS Organizations.

A AWS fornece integração nativa a gerenciamento de identidade e acesso, além de integração à API com qualquer um de seus serviços e aplicações.

Monitoramento e registro em log

A AWS oferece ferramentas e recursos que permitem ver o que está acontecendo no ambiente da AWS. Estes são alguns exemplos:

- Com o AWS CloudTrail, você pode monitorar as implantações da AWS na nuvem obtendo um histórico de chamadas de APIs da AWS em sua conta, incluindo as chamadas feitas por meio do Console de gerenciamento da AWS, dos AWS SDKs, das ferramentas da linha de comando e dos serviços mais gerais da AWS. Também é possível identificar os usuários e as contas que chamaram APIs da AWS para serviços que oferecem suporte ao CloudTrail, o endereço IP de origem dessas chamadas e quando as chamadas ocorreram.
- O Amazon CloudWatch oferece uma solução de monitoramento confiável, escalável e flexível que você pode começar a usar em questão de minutos. Não é mais necessário configurar, gerenciar e escalar a própria infraestrutura e os sistemas de monitoramento.
- O Amazon GuardDuty é um serviço de detecção de ameaças que monitora continuamente atividades mal-intencionadas e comportamentos não autorizados para proteger suas contas e workloads da AWS. O Amazon GuardDuty expõe notificações via Amazon CloudWatch, para que você possa acionar uma resposta automatizada ou notificar uma pessoa.

Estes recursos e ferramentas oferecem a visibilidade de que você precisa para identificar os problemas antes que eles afetem os negócios e permitem melhorar os procedimentos de segurança de seu ambiente, além de reduzir o perfil de risco.

Produtos de segurança no AWS Marketplace

Migrar workloads de produção para a AWS pode ajudar as organizações a melhorar a agilidade, a escalabilidade, a inovação e a economia de custos e, ao mesmo tempo, manter um ambiente seguro. O AWS Marketplace oferece produtos de segurança líderes do setor que são equivalentes, idênticos ou integrados aos controles existentes em seus ambientes on-premises. Esses produtos complementam os serviços da Nuvem AWS já existentes para que os clientes possam implantar uma arquitetura de segurança abrangente e obter uma experiência mais uniforme na nuvem e no ambiente on-premises.

Orientações de segurança

A AWS oferece aos clientes orientações e conhecimento técnico por meio de ferramentas online, recursos, suporte e serviços profissionais fornecidos pela AWS e seus parceiros.

O AWS Trusted Advisor é uma ferramenta online que atua como um especialista de nuvem personalizado, ajudando você a configurar seus recursos para seguir as práticas recomendadas. O Trusted Advisor inspeciona seu ambiente da AWS para ajudar a fechar lacunas de segurança e encontra oportunidades para reduzir os custos, melhorar a performance do sistema e aumentar a confiabilidade.

As equipes de contas da AWS atuam como o primeiro ponto de contato, orientando os processos de implantação e implementação e indicando os recursos certos para resolver os problemas de segurança que podem surgir.

O AWS Enterprise Support presta assistência com tempo de resposta de 15 minutos e está disponível 24 horas por dia, 7 dias por semana, por telefone, chat ou e-mail, e dispõe de um gerente técnico da conta dedicado. Esse serviço de concierge garante que os problemas dos clientes sejam resolvidos com a maior rapidez possível.

A Rede de Parceiros da AWS oferece centenas de produtos líderes do setor que são equivalentes, idênticos ou se integram aos controles existentes nos ambientes on-premises. Esses produtos complementam os serviços da AWS existentes para você poder implantar uma arquitetura de segurança abrangente e obter uma experiência mais uniforme na nuvem e no ambiente on-premises. Contamos também com centenas de parceiros de consultoria da AWS certificados no mundo inteiro para ajudar a atender a suas necessidades de segurança e conformidade.

O AWS Professional Services inclui uma prática especializada de segurança, risco e conformidade para ajudar você a desenvolver confiança e capacidade técnica ao migrar suas workloads mais confidenciais para a Nuvem AWS. O AWS Professional Services ajuda os clientes a desenvolver políticas e práticas de segurança com base em estruturas comprovadas, além de ajudar a garantir que o design de segurança do cliente atenda a requisitos de conformidade internos e externos.

O AWS Marketplace é um catálogo digital com milhares de ofertas de software de provedores independentes (ISVs). Ele facilita a localização, o teste, a compra e a implantação de softwares que podem ser executados na AWS. Os produtos de segurança do AWS Marketplace complementam os serviços da AWS para que você possa implantar uma arquitetura de segurança abrangente e obter uma experiência mais uniforme na nuvem e nos ambientes on-premises.

Os boletins de segurança da AWS são informativos que abordam as vulnerabilidades e as ameaças atuais, permitindo aos clientes trabalhar com especialistas em segurança da AWS para resolver questões como denúncias de abusos, vulnerabilidades e testes de penetração. Também temos recursos online para relatório de vulnerabilidade.

A documentação de segurança da AWS mostra como configurar os serviços da AWS para atender a seus objetivos de segurança e conformidade. Os clientes da AWS se beneficiam de um datacenter e de uma arquitetura de rede criados para atender aos requisitos das empresas com as maiores exigências de segurança.

O AWS Well-Architected Framework ajuda os arquitetos de nuvem a criar uma infraestrutura segura, de alta performance, resiliente e eficiente para suas aplicações. O AWS Well-Architected Framework inclui um pilar de segurança que se concentra em proteger informações e sistemas. Os tópicos principais incluem a confidencialidade e a integridade de dados, a identificação e o gerenciamento das atividades que podem ser realizadas pelos usuários com o gerenciamento de privilégios, a proteção de sistemas e o estabelecimento de controles para detectar ocorrências no âmbito da segurança. Os clientes podem usar o AWS Well-Architected Tool no Console de gerenciamento da AWS ou contratar os serviços de um dos parceiros da AWS (APN) para ajudá-los.

O AWS Well-Architected Tool ajuda você a analisar o estado das workloads e as compara às práticas recomendadas de arquitetura mais recentes da AWS. Essa ferramenta gratuita está disponível no Console de gerenciamento da AWS. Para usá-la, basta responder a um conjunto de perguntas sobre excelência operacional, segurança, confiabilidade, eficiência de performance e otimização de custos. Depois, o AWS Well-Architected Tool fornece um plano sobre como projetar a arquitetura de nuvem usando as práticas recomendadas estabelecidas.

Conformidade

A conformidade da AWS capacita os clientes a entender os controles robustos disponíveis para manter a segurança e a proteção dos dados na Nuvem AWS. Quando os sistemas são criados na Nuvem AWS, a AWS e os clientes compartilham responsabilidades de conformidade. Os ambientes de computação da AWS são continuamente auditados, com certificações de organismos de acreditação em regiões geográficas e verticais, incluindo SOC 1/SSAE 16/ISAE 3402 (anteriormente SAS 70), SOC 2, SOC 3, ISO 9001/ISO 27001, FedRAMP, DoD SRG e PCI DSS Nível 1.i. Além disso, a AWS também tem programas de garantia que fornecem modelos e mapeamentos de controle para ajudar os clientes a estabelecer a conformidade de seus ambientes em execução na AWS. Para obter uma lista completa de programas, consulte Programas de conformidade da AWS.

Confirmamos que todos os serviços da AWS podem ser usados em conformidade com o RGPD. Isso significa que, além de se beneficiar com todas as medidas que a AWS já toma para manter a segurança dos serviços, os clientes podem implantar serviços da AWS como parte de seus planos de conformidade com o RGPD. A AWS oferece um anexo de processamento de dados em conformidade com o RGPD (DPA do RGPD) para que você possa cumprir suas obrigações contratuais em relação a esse regulamento. O DPA do RGPD da AWS é incorporado aos Termos de Serviço da AWS e se aplica automaticamente a todos os clientes em todo o mundo que exigem a conformidade da AWS com o RGPD. A Amazon.com, Inc. é certificada nos termos do Privacy Shield entre UE e EUA, e a AWS tem a cobertura dessa certificação. Isso ajuda os clientes que optam por transferir dados pessoais para os EUA a atender a suas obrigações de proteção de dados. A certificação da Amazon.com, Inc. pode ser encontrada no site do Privacy Shield entre UE e EUA: https://www.privacyshield.gov/list

Com a operação em um ambiente credenciado, os clientes reduzem o escopo e os custos das auditorias que precisam realizar. A AWS passa continuamente por avaliações de sua infraestrutura subjacente, incluindo a segurança física e do ambiente de hardware e datacenters, para que os clientes possam aproveitar essas certificações e simplesmente herdar esses controles.

Em um datacenter tradicional, as atividades comuns de conformidade são geralmente manuais e periódicas. Essas tarefas incluem a verificação de configurações de ativos e a elaboração do relatório de atividades administrativas. Além disso, os relatórios resultantes ficam desatualizados antes mesmo de serem publicados. Operar em um ambiente da AWS permite que os clientes aproveitem ferramentas incorporadas e automatizadas, como o AWS Security Hub CSPM, o AWS Config e o AWS CloudTrail para validar a conformidade. Essas ferramentas reduzem o esforço necessário para realizar auditorias, já que essas tarefas se tornam rotineiras, contínuas

e automatizadas. Com a redução de gastos em atividades manuais, você pode elevar o papel da conformidade em sua empresa, transformando o que era uma carga administrativa necessária em um elemento que gerencia seu risco e melhora seus procedimentos de segurança.

Leitura adicional

Para obter mais informações, consulte os seguintes recursos:

Para obter informações sobre…	Consulte
Principais tópicos, áreas de pesquisa e oportunidades de treinamento em segurança de nuvem na AWS	Aprendizado sobre segurança na Nuvem AWS
AWS Cloud Adoption Framework, que organiza as orientações em seis áreas de concentração: negócios, pessoas, governança, plataforma, segurança e operações	AWS Cloud Adoption Framework
Controles específicos disponíveis na AWS e instruções sobre como integrar a AWS à estrutura de trabalho	Amazon Web Services: risco e conformidade
Práticas recomendadas de segurança, identidade e conformidade	Práticas recomendadas de segurança, identidade e conformidade
Pilar Segurança – AWS Well-Architected Framework	Pilar Segurança – AWS Well-Architected Framework

Revisões do documento

Para ser notificado sobre atualizações deste whitepaper, inscreva-se no RSS feed.

update-history-change	update-history-description	update-history-date
Whitepaper atualizado	Atualizado com links para leitura adicional.	11 de novembro de 2021
Whitepaper atualizado	Atualização dos serviços, recursos e tecnologias mais recentes.	22 de janeiro de 2020
Publicação inicial	Introdução à segurança da AWS publicada.	1º de julho de 2015

Avisos

Os clientes são responsáveis por fazer sua própria avaliação independente das informações neste documento. Este documento é: (a) fornecido apenas para fins informativos, (b) representa as ofertas e práticas de produtos atuais da AWS, que estão sujeitas a alterações sem aviso prévio e (c) não cria nenhum compromisso ou garantia da AWS e suas afiliadas, fornecedores ou licenciadores. Os produtos ou serviços da AWS são fornecidos no “estado em que se encontram”, sem garantias, declarações ou condições de qualquer tipo, explícitas ou implícitas. As responsabilidades e obrigações da AWS com seus clientes são regidas por contratos da AWS, e este documento não modifica nem faz parte de nenhum contrato entre a AWS e seus clientes.