

CLOUD SECURITY

com **FORTICNP**



SÚMARIO

Introdução	2
------------------	---

Minha nuvem está segura?	3
--------------------------------	---



<i>Modelo de Responsabilidade Compartilhada</i>	4
---	---



<i>DevSecOps</i>	6
------------------------	---

Como proteger minha cloud?	7
----------------------------------	---



<i>CSPM (Cloud Security Posture Management)</i></

INTRODUÇÃO

Para atender todas as demandas atuais, as empresas necessitam ter um braço forte de tecnologia. E nesse cenário, a cibersegurança se apresenta como pilar fundamental para o bom funcionamento dos processos internos e externos, uma vez que o número de tentativas de ataques cibernéticos aumenta de forma expressiva, bem como suas complexidades.

E o Brasil é um dos países que mais sofrem desses incidentes, de acordo com um estudo da Check Point Research (CPR) a quantidade de ciberataques aumentou 37% em 2022, no mundo todo o crescimento foi de 28%.

Segundo a Fortinet, de janeiro a junho de 2022, foram 31,5 bilhões de tentativas de ataque em empresas brasileiras, sendo o segundo país mais visado da América Latina. E o principal vetor utilizado pelos cibercriminosos são os ransomwares, um tipo de malware capaz de bloquear o sistema ou a criptografia dos dados, com isso os cibercriminosos exigem dinheiro de resgate das vítimas, em troca da liberação dos dados.

Nos últimos anos tivemos casos famosos de incidentes causados por ransomware, como o da TV Record em outubro de 2022 em que foi pedido mais de US\$ 5 milhões para a devolução dos dados.

Além do perigo de ciberataques, as empresas também se preocupam com a regulamentação da Lei Geral de Proteção

Minha nuvem está segura?



Com já dito anteriormente, ao iniciar suas jornadas para a cloud, as empresas buscam implementar processos de segurança robustos, capazes de agir de forma proativa em situações de falhas ou ataques. E os casos mencionados nas páginas anteriores reforçam essa necessidade. A boa notícia é que atualmente o ambiente em cloud aparece como uma alternativa otimizada e econômica para atingir esses objetivos. Garantindo assim, que a organização possa ter uma estrutura altamente protegida, independentemente de seu tamanho.

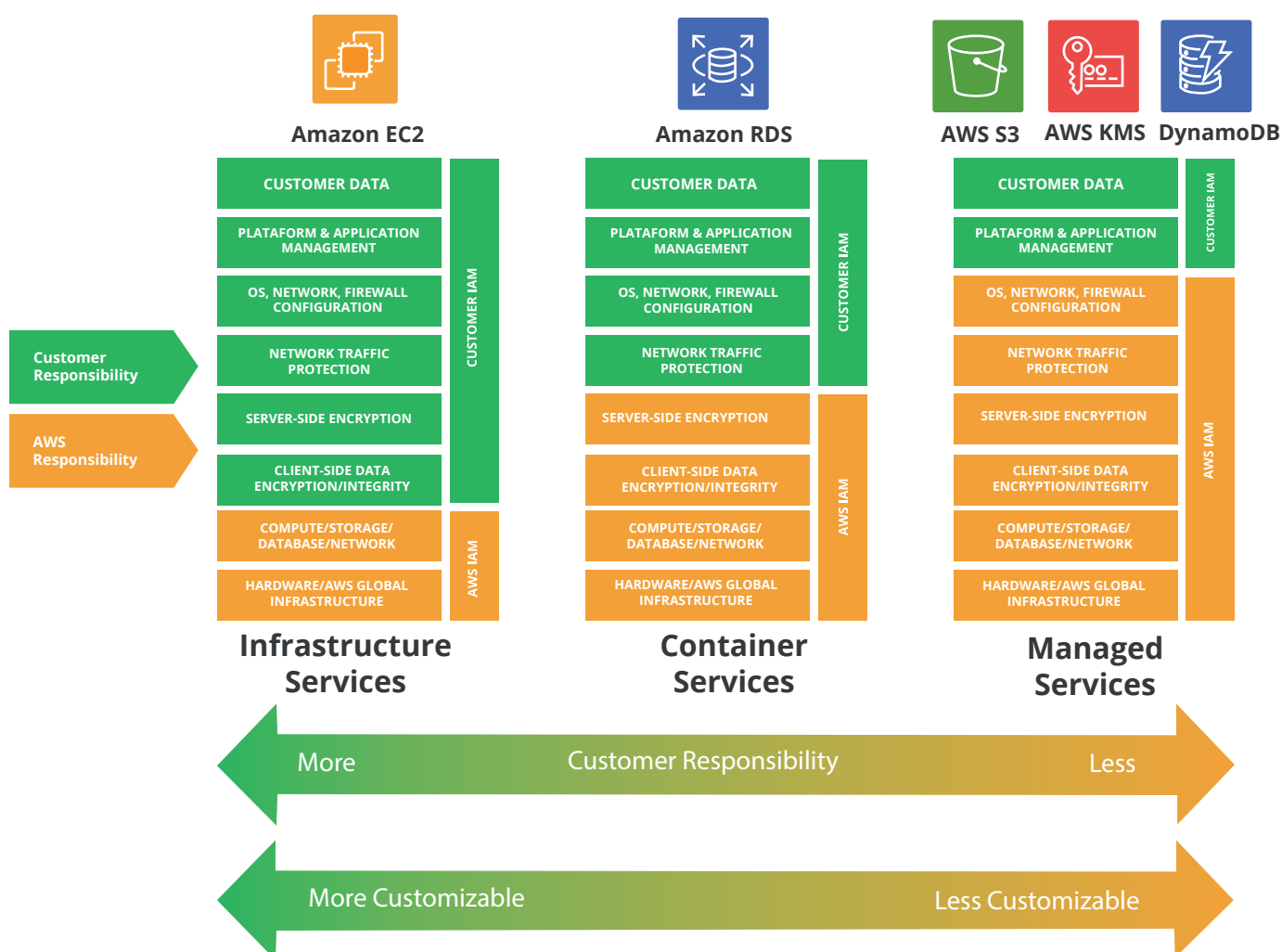
A segurança em um ambiente em cloud (Cloud Security) traz um conjunto de políticas, controles e serviços que buscam a proteção de dados, aplicações e outros dispositivos da infraestrutura. Assim

Modelo de Responsabilidade Compartilhada



Entretanto, a obrigação de manter um ambiente totalmente seguro não é obrigação apenas da plataforma. Os maiores provedores de serviços em cloud do mundo possuem um modelo de diretrizes em que delimitam as responsabilidades de se manter um ambiente seguro. O modelo de responsabilidade compartilhada detalha o que é a obrigação da plataforma, como a proteção da infraestrutura e o que é o dever do usuário na execução dos serviços, como a configuração de um firewall, por exemplo.

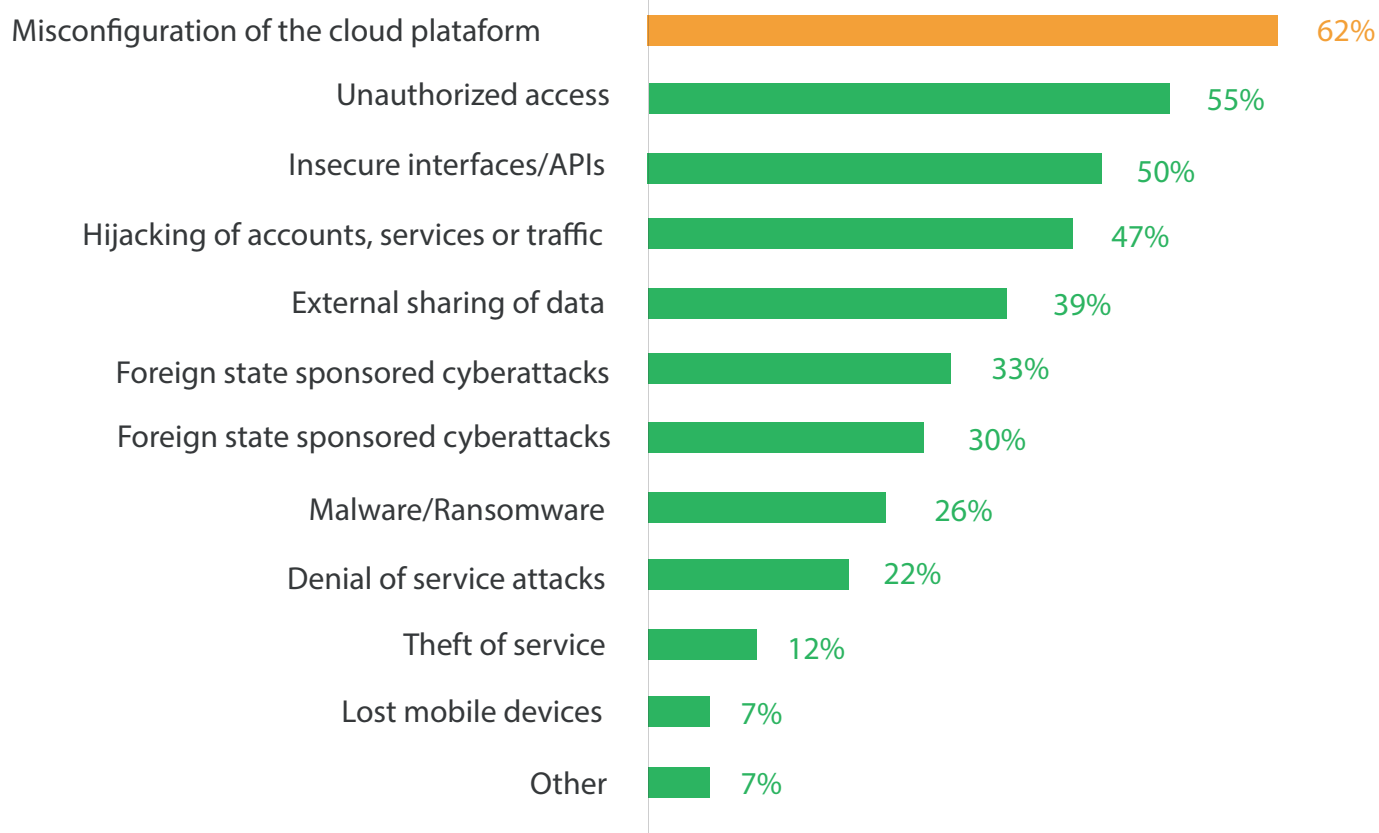
Assim, as plataformas podem oferecer o melhor serviço para o cliente e promover aquilo que todos buscam: um ambiente altamente disponível, produtivo e seguro.





Esse modelo é essencial para o bom funcionamento de um ambiente em cloud, uma vez que os três maiores riscos de segurança em cloud estão do lado do usuário, como a má configuração da estrutura, problemas no acesso a contas, e interfaces/APIs inseguras.

Biggest Cloud Security Threats





Com o aumento expressivo da importância de se implementar processos altamente seguros em uma infraestrutura de TI, surge um conceito que vem transformando a forma de pensar em desenvolvimento seguro de aplicações, principalmente para ambientes em cloud: o DevSecOps.



Todos nós já conhecemos a cultura DevOps, e como ela auxilia as empresas na construção de aplicações, com agilidade e efetividade. E seguindo essa cultura, aliado com algumas ferramentas disponibilizadas pelas plataformas, o processo de construção de aplicações para cloud foi facilitado. Mas como lidar com a segurança destes serviços? É exatamente essas possíveis fragilidades que agentes externos buscam para invadir infraestruturas.

Nesse cenário a cultura DevSecOps aparece como fator essencial para

Como proteger minha cloud?

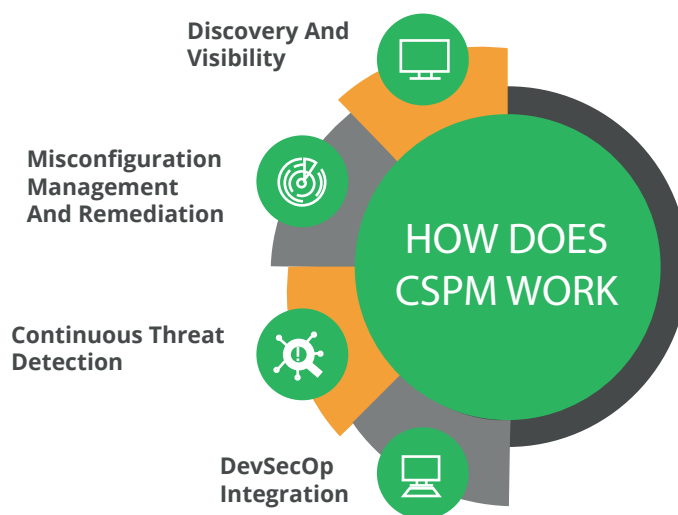


Como abordamos anteriormente, a Cloud aparece como uma das principais alternativas para as empresas implementarem uma verdadeira transformação digital e introduzir processos capazes de aumentar a segurança do ambiente como um todo. E nesse sentido, aparecem conceitos e ferramentas para auxiliar os usuários a mitigar incidentes causados por agentes internos ou externos, e nesse segmento vamos apresentar alguns deles:

CSPM (Cloud Security Posture Management)



Embora muitos considerem a tecnologia em cloud tão ou mais segura que uma estrutura on premises, é preciso ter uma postura diferente em relação à proteção dos dados e consequentemente das aplicações de um ambiente. Isso se dá devido ao modelo de responsabilidade compartilhada, que já mencionamos anteriormente, da LGPD e dos recentes incidentes em grandes empresas do mercado.



propósito desse conceito é o monitoramento contínuo da estrutura, podendo agir de forma proativa em caso de falhas e vulnerabilidade na aplicação de políticas de segurança.

As soluções CSPM agem em 4 pontos:



No processo de auditoria ou assessment da Cloud para verificação e proteção de riscos conhecidos;



No entendimento do ambiente para aplicação das melhores práticas de segurança;



No encaminhamento de soluções capazes de aumentar a proteção do ambiente;





Grandes empresas de segurança do mercado também buscam realizar investimentos para aumentar a segurança das infraestruturas presentes na cloud. Como é o caso da Fortinet, empresa líder mundial de soluções de segurança da informação. No AWS Summit São Paulo 2022, a organização apresentou o FortiCNP, uma plataforma de proteção nativa em cloud. Uma ferramenta totalmente integrada aos serviços dos maiores provedores de soluções em cloud do mundo, capaz de proteger de forma completa os workloads de uma estrutura.

Utilizando uma tecnologia patenteada, o Risk Resource Insights (RRI)™, o FortiCNP simplifica os processos de segurança da estrutura, e oferece insights para ajudar as equipes de segurança a aplicar dispositivos seguros e totalmente personalizados as necessidades do ambiente.

O FortiCNP atua em 5 pontos:



Gerenciamento de risco

SOBRE A DAREDE

A Darede é uma empresa de consultoria, especialista em serviços de TI, e com 10 anos de experiência nesse mercado. Prestamos um atendimento personalizado e de qualidade para nossos clientes, sempre em busca de obter os melhores resultados e garantindo que consigam atingir seus objetivos por meio da Cloud Computing.

A Darede é parceira nível premier da Amazon Web Services.Services (AWS), parceira nível advanced da Datadog, além de trabalhar em conjunto com grandes provedoras de TI do mundo da tecnologia.

Nossos parceiros

Em sinergia com os maiores especialistas do mercado, somos focados em resultados de eficiência para a sua empresa expandir cada vez mais os negócios.



A Darede é parceira nível Premier da AWS, além de ser a parceira mais premiada e especializada da América Latina, em 2024 ganhamos o prêmio de consultoria parce

Ao longo de sua caminhada a Darede colecionou prêmios e reconhecimentos de grandes players do mercado:





Créditos

Título do E-book: Cloud Security com FORTICNP

Autor: Darede

Produzido por: Damidia

Coordenado por: Cassius Oliveira

Design e Ilustração: Lucas Almeida Vieira

Diagramação: Lucas Almeida Vieira