Os contentores ABSTRACT surgiram como uma alternativa leve às máquinas virtuais que oferecem um melhor apoio à arquitectura dos microserviços.

Embora sejam considerados o método padronizado para a implementação de micro-serviços, desempenhando um papel importante nos campos emergentes da computação em nuvem, tais como malhas de serviços, os estudos de mercado mostram que a segurança dos contentores é a principal preocupação e barreira à adopção para muitas empresas. Neste artigo, pesquisamos a literatura sobre segurança e soluções em contentores. Concluímos quatro casos de uso generalizado que devem cobrir os requisitos de segurança dentro do cenário de ameaça dos contentores de acolhimento. Verificámos que os três primeiros casos de utilização utilizam uma solução baseada em software que se baseia principalmente em funcionalidades de kernel Linux e módulos de segurança Linux .

O último caso de utilização baseia-se em soluções baseadas em hardware, tais como módulos de plataforma confiáveis e suporte de plataforma confiável . Esperamos que a nossa análise ajude os investigadores a compreender os requisitos de segurança dos contentores e a obter uma imagem mais clara de possíveis vulnerabilidades e ataques. INDEX TERMS Containers, Docker, contentores Linux, virtualização ao nível do SO, virtualização leve, segurança, levantamento. As máquinas virtuais proporcionam uma excelente segurança.

No entanto, o seu isolamento de segurança cria um estrangulamento para o total de VMs que podem funcionar num servidor, porque cada VM deve ter a sua própria cópia do sistema operativo , bibliotecas, recursos dedicados, e aplicações. A virtualização baseada em contentores emergiu como uma alternativa leve aos VMs. Muitos contentores podem partilhar o mesmo OS kernel em vez de terem uma cópia dedicada para cada um deles como nos VMs. Muitas tecnologias de contentores estão disponíveis tais como LXC, OpenVZ, LinuxVserver, sendo o Docker o predominante.

Os contentores são uma opção mais plausível para os micro-vices do que os VMs, devido aos numerosos benefícios tais como serem leves, rápidos, mais fáceis de implementar, e permitirem uma melhor utilização de recursos e controlo de versões. Os contentores estão a ser utilizados para diferentes aplicações tais como serviços de Internet das Coisas , carros inteligentes, computação de nevoeiro, malhas de serviço, e assim por diante [3]-[8]. Os contentores são considerados o padrão para implantar micro-serviços e aplicações na nuvem [10]. Os contentores são também importantes para o futuro da computação em nuvem e espera-se que o seu valor de mercado atinja 2,7 mil milhões de dólares até 2020 [11], [12], [12].

Embora existam vários inquéritos que abordam as VMs, não se concentram em questões de segurança de contentores

Uma vez que os VMs se baseiam na partilha do kernel do SO entre eles, enquanto cada VM tem o seu próprio kernel, a segurança do contentor é diferente da do seu homólogo VM, uma vez que se baseia em diferentes suportes arquitectónicos e turais. Assim, a compreensão das ameaças e soluções de segurança dos contentores é muito importante devido à falta de revisões sistemáticas sobre elas na literatura. Por exemplo, o suporte de plataforma de confiança por exemplo, Intel Software Guard Extensions é utilizado principalmente para permitir o funcionamento de contentores num anfitrião não confiável, assim o seguimento desses diferentes casos de utilização pode ser frustrante para o leitor. Isto deverá ajudar os leitores a compreender melhor as questões de segurança sobre os contentores e os mecanismos disponíveis para os proteger.

Na Secção IV, apresentamos os mecanismos de protecção de software e hardware utilizados para garantir a segurança dos con- tinadores. Na Secção V é apresentada uma discussão sobre

vulnerabilidades de contentores, explorações, ferramentas de dis- cobertura, e normas relevantes. Nesta secção, apresentamos material de fundo sobre arquitecturas de contenção, bem como arquitecturas monolíticas e de microserviços. Diferentes nomes são usados para se referir a contentores na ture literária- incluindo virtualização de nível de SO e virtualização leve- alização.

Docker, LXC, e RKT são exemplos de gestores de contentores. Muitos estudos concentram-se no Docker porque é o ambiente predominante de tempo de execução de contentores. Em segundo lugar, os contentores podem ser iniciados e parados quase instantaneamente enquanto os VMs precisam de tempo considerável para iniciar [3]. Os contentores também provaram ser mais eficientes do que as VMs para algumas aplicações tais como microserviços, porque são leves e não requerem uma cópia completa do SO para cada imagem.

No entanto, os contentores ainda necessitam de um núcleo totalmente funcional que é partilhado entre diferentes contentores. Além disso, a concepção dos microserviços sublinha a importância dos contentores de estado efémero, em que qualquer persistência de dados vai para outro armazenamento ou serviço de dados. Os contentores são considerados a forma padrão de implementar os microserviços na nuvem [10]. Muitas compa- nies oferecem serviços de contentores que permitem uma grande variedade de aplicações contentorizadas para vários mercados [20].

SO anfitrião introduz muitas questões de segurança, o que as torna menos seguras do que as VM [21]. A vista da ave de uma pilha de contentores é necessária porque a implantação depende de várias partes.

Tecnologias de empilhamento e realização de contentores. [23] apresentaram um sur- vey sobre as ferramentas disponíveis para a gestão de contentores. Classificaram diferentes soluções, tanto na literatura académica como na indústria, bem como cartografaram-nas de acordo com os requisitos baseados num estudo de caso que forneceram. Contrário da utilização de uma arquitectura monolítica, que requer a reescrita de todas as partes.

Embora as aplicações monolíticas possam correr dentro de um recipiente, é altamente recomendada a utilização de arquitectura de microserviço quando se utilizam recipientes [25]. As arquitecturas Microservice revolucionaram a forma como os cátions são construídos hoje em dia. Executar cada micro-serviço num VM separado não é eficiente porque os VMs são pesados em comparação com os contentores [25]. Os contentores são alternativas importantes aos VM e têm uma série de benefícios sobre eles, especialmente no perfor- mance e no tamanho.

O advento dos contentores realçou a importância das arquitecturas de microserviço em relação às arquitecturas mono-litíticas mais antigas. Contudo, os contentores são afectados por numerosas questões de segurança que constituem os principais obstáculos à sua adopção pelas empresas. [24] apresentaram um estudo recente sobre a emergência de micro-serviços e como o seu desenvolvimento melhorou os inconvenientes da arquitectura monolítica. Ocasionalmente, baseámo-nos em pesquisas não publicadas ou publicadas sob formas não comerciais, tais como relatórios, declarações políticas, etc. Tais artigos foram incluídos porque a investigação sobre recipientes é um campo intrinsecamente prático que é dominado pela indústria e é publicado em diferentes fontes em linha.