CyberTech Report

CISCO SECURE

Nuvem: inovações, tendências e soluções

#10 | ABRIL | 2022

Sumário

Este report conta com o apoio da Cisco Secure.

cisco SECURE

Para navegar pelos capítulos deste estudo, **clique nos botões na margem superior**. A qualquer momento, **clique no logo do Distrito no canto inferior direito para voltar a esta página.**

Metodologia

As startups delineadas no report foram selecionadas a partir de um trabalho minucioso de pesquisa e consulta ao banco de dados de startups proprietário do Distrito. Também foram realizadas consultas a bancos abertos e informações públicas do governo.

As startups foram examinadas individualmente para verificar adequação ao tema do report e aos critérios de seleção estabelecidos. São eles:

- **Ter a inovação no centro do negócio, seja na base tecnológica, no modelo de negócios ou na proposta de valor;**
- **Estar em atividade no momento da realização do estudo, medida pelo status do site e atividade em redes sociais;**
- **Desempenhar atividade diretamente relacionada ao setor estudado;**
- **Ter nacionalidade brasileira e operar atualmente no Brasil.**

O trabalho de definição das categorias foi baseado em análise da literatura relevante e das classificações utilizadas amplamente no mercado, no Brasil e no mundo.

A definição da categoria a que pertence cada startup foi feita por nossa equipe, e, quando uma startup opera em mais de uma categoria, a situamos na que interpretamos como sua atividade principal ou de maior visibilidade.

Também temos uma preocupação em incluir somente aquilo que consideramos startups—e, por mais que nosso critério para defini-las seja bastante amplo, excluímos alguns tipos de negócio que, embora muitas vezes se autodenominam startups, acabam fugindo do conceito. Isso inclui empresas que têm como característica principal serem:

- **Software Houses (desenvolvimento de software sob demanda);**
- **Consultorias;**
- **Agências de marketing, publicidade e design.**

Enfatizamos aqui que os números expostos podem sofrer alterações conforme a evolução da acurácia das informações e maior capacidade de interação com as próprias startups ao longo do tempo.

Entrevistados

Juan Marino
Cybersecurity Sales Strategy Manager LATAM
Cisco

Pedro Pisa
Diretor Executivo
Solvimm

Thiago Caserta
Founder & CSO
Kumulus

Américo de Paula
Head of Solutions Architecture LATAM
Amazon Web Services

Introdução

Introdução

Engana-se quem pensa que a computação na nuvem é um conceito recente. O uso de uma representação cartunesca daquilo que costumamos ver ao olhar para o céu já era usado por empresas de tecnologia desde os anos 70 e 80 — mas, claro, em um contexto bem diferente do que conhecemos agora. A palavra era uma metáfora usada para se referir, de forma mais acessível, a própria internet, implicando uma simplificação de diagramas que demonstravam como vários endpoints de uma vasta rede eram conectados, de forma simultânea, a um serviço disponível em outra máquina (servidor).

Foi só em meados de 1993 que a palavra "cloud" começou a ser utilizada por grandes corporações — incluindo a Apple e a operadora de telefone móvel AT&T — como sinônimo de tecnologias de computação distribuída, especificamente para se referir a, respectivamente, seus produtos Telescript (linguagem de programação que quis “matar” o Java ao possibilitar a execução de aplicações web sem a necessidade da instalação de um cliente local) e PersonalLink (serviço de notícias, previsão meteorológica e email para PDAs escrito na linguagem Telescript).

A computação na nuvem como conhecemos hoje só nasceu mesmo nos anos 2000. Hoje, entendemos o conceito como a disponibilidade de poder computacional (tanto para processamento e armazenamento) sob demanda e sem a gestão direta do usuário, o que acarreta em diversos benefícios óbvios como redução de custos operacionais e acesso remoto a aplicações, serviços, dados e arquivos.

Os anos seguintes ficaram marcados por um gigantesco *buzz* no mercado; parte por conta das próprias campanhas de mídia das corporações que já ofereciam tal tecnologia, parte por conta da cobertura midiática que posicionava a nuvem como “o futuro”. E, se no início existia resistência por parte das empresas de migrar para esse modelo, a transformação digital acelerada que estamos vivendo ao longo dos últimos dois ou três anos fez com uma verdade ficasse bastante clara: por ser flexível, acessível e escalável, a nuvem é sim uma grande aliada para a maioria das corporações.

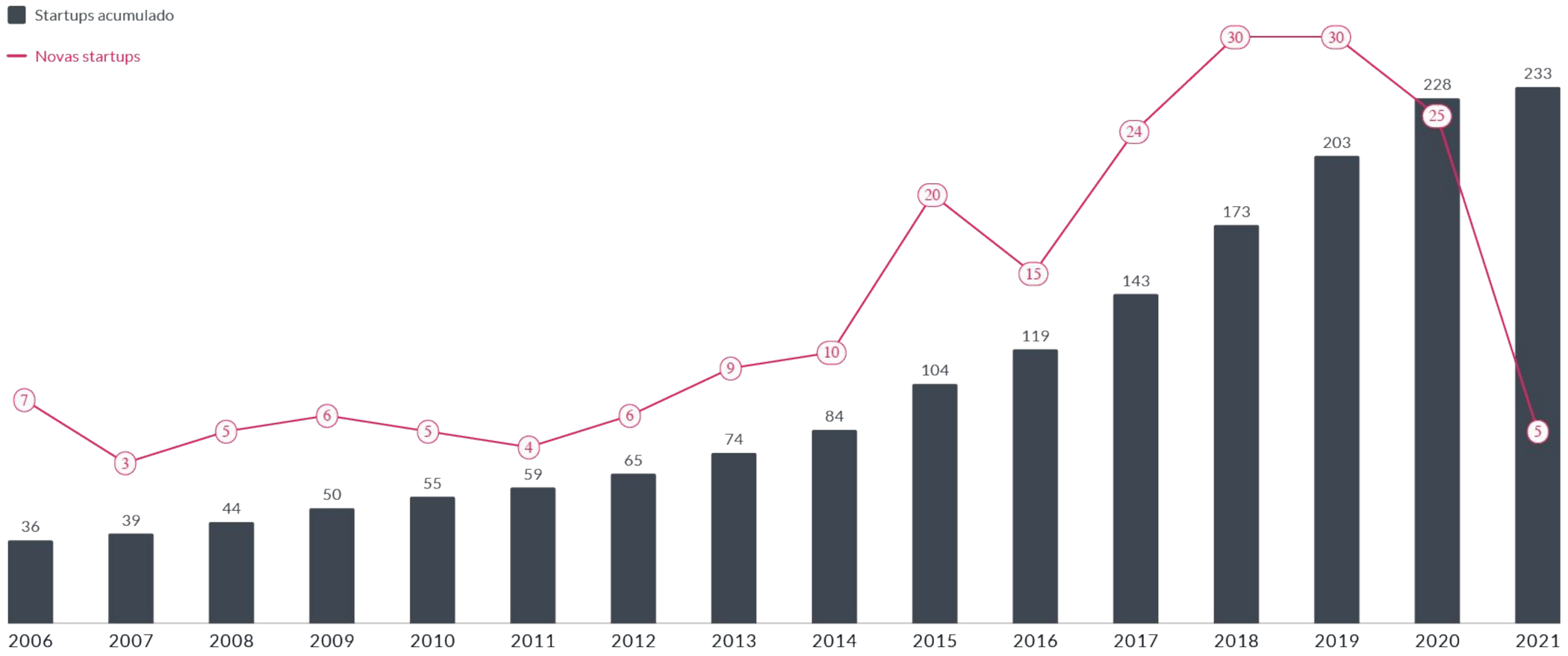
Contudo, novas arquiteturas de computação exigem novas estratégias de proteção contra ameaças cibernéticas. Ambientes na nuvem possuem peculiaridades que nem sempre os CISOS e equipes de segurança da informação sabem lidar. Ao mesmo tempo, a própria computação na nuvem vem se provando uma arma excelente para dar força às soluções de cibersegurança, possibilitando a criação de novas plataformas que blindam sua rede contra os meliantes virtuais.

Afinal, qual é o futuro da nuvem? Quais são os desafios que precisamos enfrentar e quais oportunidades temos em nossa frente? Esta edição do CyberTech Report visa responder essas e outras questões.

Boa leitura!

Ecossistemas Cybertech

Evolução Cybertechs



Highlights

233
Startups

12
Categorias

9.000
Funcionários empregados

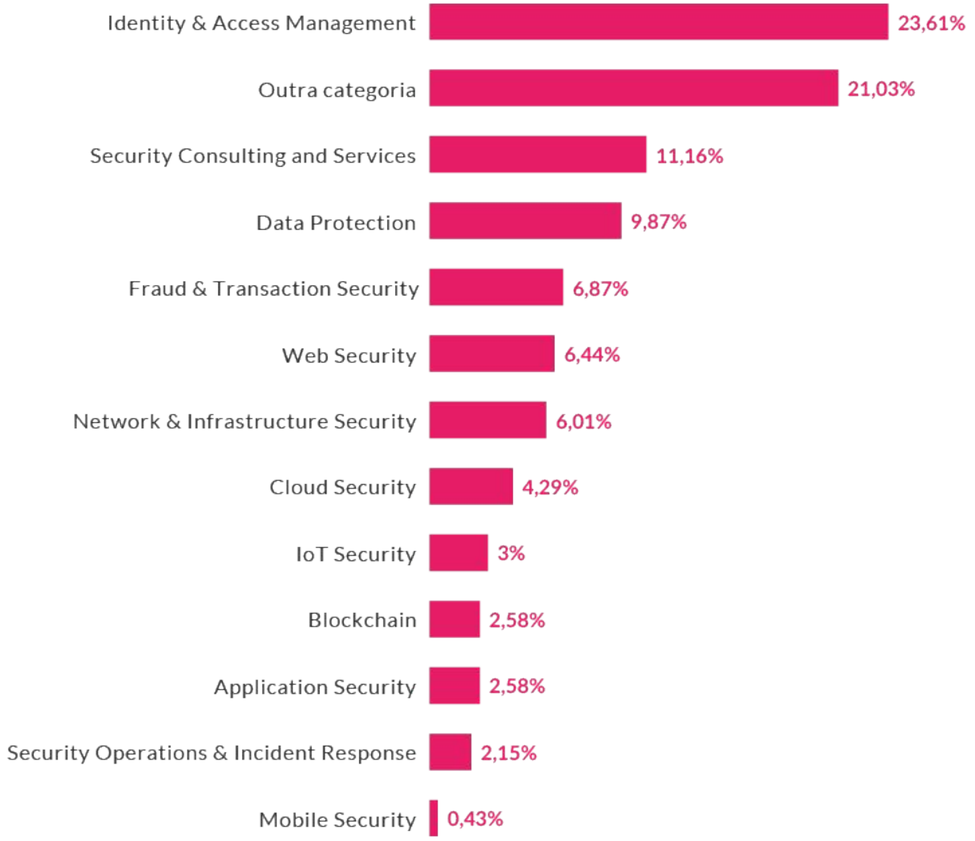
75
Startups com investimento recebido

US$ 412,5M
Investimento recebido desde 2013

US$ 294M
Investimento recebido nos últimos 2 anos

15
M&A's desde 2012

Divisão Cybertechs por categoria



RADAR: CYBERTECHS

DISTRITO

Data protection

36ZERO · a2f · ADDERE SOLUTIONS · beAnalytic · CLAVIS · DADOS LEGAIS · dogma · ethquo · GLOBAL DATA BANK · guardSI · Intelivix · IT2SGROUP · leadcomm · LOGS360 · MODULO · NETTIME · sentnella · PHISHX · Privacy tools · PRIVALLY · riskex · SAFE WAY · senhasegura · SENSR. · Simply. · ST3TAILOR · FlashSafe

Cloud Security

ADTsys · BrasilCloud · DDMX · nuvic · RedeHost · CleanCloud

Mobile Security

BluePex

Security Consulting and Services

SOTO · CECyber · Collision · CROMISOFT · Deep.bbl · DESEC · ESTUARIO · HACK3R_RANGERS · IBLISS · iCybersec · INFOSAFE · INtroduce · SOLVIMM · nova8 · OPTRA SECURITY · REDBELT · RUSTCON · STRONG SECURITY · TEMPEST · Unbroken Cyber Security

Fraud & Transaction Security

B2e Group · bigdatacorp. · BrScan · CQuantt · EXATO DIGITAL BETA · ZAIG · infodatos · konduto · legiti · MOST · Neoway · VIVALISTO · NeuroBanco · NEXTCODE · TRANSFERO SWISS AG

Network, Infrastructure Security

CONNECT · ISM · lumiun CLOUD MANAGED NETWORK · munio SECURITY · oktopus · ProFUSION embedded systems · StartLink · TI Safe · Virti · WEDOIT Working Together · Ztec

Security Operations & Incident Response

AXUR · gocache next-gen CDN

RADAR: CYBERTECHS

DISTRITO

Identity & Access Management

acert · AIKNOW · akiyama · Assine Online · autentique · AutoSeg · BeCloudx · BRy Tecnologia · CH tecnologia · Formalizar e-signature · FULLFace A sua segurança é você · griaule big data biometrics · GrupoCloud · GRYFO · HDDBOX · contract · ID ESSENTIALS · idwall · MEERKAT · NATOSAFE · nexti · nTokens · DITI · payface · qriar · QualiSign · PONT marcação móvel · unike · UNISEC Segurança, tecnologia e conforto · VSOFT · welcome · COMBATE A FRAUDE · contraktor · CRED DEFENSE · D4S · FIVE VALIDATION · mavie · INOVACODE · JURIDOC · Let's Work · .ai · SHIELDER · SimpleID IDENTIDADE CONFIRMADA! · SVATECH smart video analytics · T-SHIELD · UNICO

IoT Security

GAVB · LATOS · Ochain · TrackerThings · POLSEC · PREVISIOWN · ROBBIOT

Governance, Risk and Compliance

GAT InfoSec · NeuralMind · certo · REFINARIA DE DADOS

Application Security

Berghem Smart Information Security · CONVISO · BugHunt

Blockchain

2LEDGER · c4 4D4 .4 · amachains · bitshopp · BLOCKc · BlockNobre · BLOCO1 · bom valor · MARKETPLACE · COSMOS · CRIPTONOMIA · EOSRIO · Go Blockchain · GoBlock · growthTech · InspireIP · ORIGINALMY BLOCKCHAIN · QUAN · rhizom · safe TRACE · health · GoLedger · HubChain

Web Security

apura · AuditSafe · CromiWAF cyber defense · ERRORSEC · <u> · XLabs | ON SECURITY · SITE BLINDADO · Gatefy · UPX TECHNOLOGIES · XLabs · MBSEC

Nuvem: o êxodo e suas consequências

Contexto e Panorama Nacional

Um novo lugar para chamar de lar

Embora o agente infeccioso tenha um papel importante nesse fenômeno, não podemos dar ao novo coronavírus (SARS-CoV2) todo o crédito pela migração massiva das empresas para infraestruturas na nuvem. Uma pesquisa realizada pela SAS Brasil em maio de 2019 (muito antes da pandemia atingir seus níveis críticos) com quase 300 executivos c-level na América Latina apontou que 80% das empresas já pretendia adotar tal tecnologia dentro dos 12 meses subsequentes.

Os motivos apontados eram óbvios: **agilidade, inovação e crescimento exponencial, tudo isso com um custo reduzido** se compararmos com os investimentos necessários para ampliar uma central de servidores (data center) tradicional (on-premise). Porém, se essa ambição não era tida como prioridade, o caos causado pela COVID-19 acelerou esse êxodo.

Da noite para o dia, tornou-se necessário entregar aplicações de forma eficiente para colaboradores que estavam trabalhando remotamente em isolamento social. As corporações também tiveram que se apressar para digitalizar a oferta de seus produtos e serviços para o consumidor final, efetivamente pivotando seu core business para uma estratégia focada 100% no ambiente virtual.

Foi o momento perfeito para a nuvem brilhar. Corporações de todo porte e segmento poderiam escalar seu poder computacional e trabalhar com computação distribuída a uma fração do custo dos servidores on-premise.

Agora, com os ânimos mais controlados e a pandemia tendo se tornado uma endemia, uma nova pesquisa da Sky.One divulgada em março deste ano apresentou alguns números bem interessantes em relação a tal movimentação. O estudo constatou que **87% das empresas brasileiras que migraram para a nuvem são de pequeno porte (até 50 colaboradores)**, estatística que ajuda a desmistificar de vez a visão retrógrada de que a tecnologia é exclusiva para corporações de grande porte.

“Os custos de migração acabam sendo mais baratos que o investimento em uma infraestrutura de TI local, por exemplo. Isto, somado aos benefícios que a nuvem traz como escalabilidade, disponibilidade, agilidade e segurança. Ao final, a migração para a nuvem é muito mais rentável para as empresas, não apenas as pequenas, mas de todos os portes e verticais”, explicou Roberto Arruda, diretor de receita da Sky.One.

Traduzindo, a jornada para a nuvem é muito mais simples quando feita “do zero” do que quando é necessário migrar uma infraestrutura legada de grande porte.

Por outro lado, surgem as preocupações com a segurança cibernética: afinal, quanto menor é a empresa, menor é a sua equipe de SI e menos experiência os seus membros costumam ter com novas arquiteturas computacionais.

Está chovendo dados

Embora as estatísticas apresentadas anteriormente referem-se especificamente ao Brasil, não demorou muito para que o êxodo das empresas para a nuvem sem o devido preparo começasse a apresentar alguns efeitos preocupantes. De acordo com a mais recente edição do relatório IDC State of Cloud Security, **98% das corporações com sede nos Estados Unidos sofreram pelo menos um incidente de vazamento de dados em ambientes na nuvem** ao longo dos 18 meses anteriores.

Embora não tenhamos uma inteligência similar específica para o mercado brasileiro, a gigantesca quantidade de manchetes alertando sobre vazamentos em serviços e empresas nacionais não deixa dúvidas que o problema é igualmente preocupante em nosso país.

Os motivos para tais exposições indevidas são diversos, mas os participantes do estudo elencaram os maiores desafios de proteger informações sensíveis na nuvem.

Maiores desafios na nuvem

Caminhando para um futuro híbrido

Juan Marino
Cybersecurity Sales Strategy Manager LATAM
Cisco

Os benefícios da computação na nuvem são conhecidos por qualquer profissional da área da tecnologia. Contudo, se mesmo há alguns anos já enxergávamos empresas cometendo erros de segurança ao usar esse tipo de infraestrutura, a transformação digital acelerada causada pela pandemia da COVID-19 fez com que um número ainda maior de empresas (incluindo as de pequeno e médio porte) adotassem serviços de cloud sem o devido preparo para lidar com suas peculiaridades. Ao mesmo tempo, não param de surgir startups oferecendo soluções de segurança na nuvem. Como a Cisco enxerga todo esse cenário?
O presente e o futuro próximo requerem uma abordagem híbrida. O trabalho é híbrido, parte remoto, parte no escritório. A infraestrutura de TI é híbrida, parte tendo se movido para a nuvem e parte tendo se mantido on-premise, e a segurança também é híbrida. Deve-se tomar cuidado para não cair em posições radicais sob a promessa de soluções mágicas de segurança na nuvem, no terminal ou em qualquer outro lugar.

A resposta é "e". Como sempre, a segurança é construída em camadas e, embora diferentes empresas de diferentes tamanhos não tenham o mesmo nível de sofisticação em seus recursos de segurança, todas elas exigem uma combinação de tecnologias que, em parte, podem ser fornecidas como um serviço em nuvem.

Alguns requerem a instalação em dispositivos finais e na rede. Em outras palavras, estamos falando de uma abordagem de plataforma que a Cisco vem construindo há mais de uma década. Acreditamos que a resiliência é possível para organizações de todos os setores e tamanhos com a combinação certa de produtos e serviços.

A segurança na nuvem e a partir da nuvem são definitivamente uma peça chave e estamos acompanhando nossos clientes nessa transformação. Uma boa segurança depende de boas decisões e nesta equação é fundamental confiar nos fornecedores de tecnologia uma estratégia clara e transparente. →

Todos sabemos que há um déficit de profissionais de segurança cibernética no mundo inteiro. Quando falamos especificamente sobre cloud computing, torna-se ainda mais raro encontrar especialistas no assunto, o que agrava tal problema. Como podemos mitigar esse gap a curto prazo, auxiliando empresas de todos os portes e setores a trilhar uma jornada segura para a nuvem mesmo com essa falta de mão-de-obra?
Para muitas organizações, especialmente as de menor porte, é difícil e até proibitivo ter profissionais de segurança cibernética capazes de levar adiante a gestão e operação da segurança. Por isso, o desenvolvimento de serviços de segurança gerenciados pelo ecossistema de parceiros, integradores de tecnologia, é essencial.

Há avanços nessa direção, embora ainda haja um longo caminho a percorrer. Por outro lado, na Cisco, estamos mitigando essa lacuna de talentos fornecendo serviços profissionais em todo o ciclo de gerenciamento de segurança cibernética e até mesmo na resposta a incidentes. Por último, mas não menos importante, cabe destacar a contribuição histórica que a Cisco Networking Academy tem feito na formação de profissionais. Nos últimos anos, observamos um interesse crescente no treinamento de segurança cibernética, e os alunos do Cisco NetAcad estão aproveitando nossas ofertas de educação nessas áreas.

Ao mesmo tempo em que a nuvem se provou uma tecnologia crucial para a transformação digital das empresas, seja através de infraestruturas-como-serviço (IaaS) ou pelos softwares-como-serviço (SaaS), ela também está revolucionando a própria segurança da informação. Estamos vislumbrando o nascimento de conceitos como virtualização em nuvem de áreas de trabalho, arquitetura SASE, XDR etc. Como a Cisco Secure, enquanto player líder no segmento, utiliza a nuvem para fornecer soluções de segurança disruptivas ao mercado?
A Cisco construiu suas soluções de segurança na nuvem seguindo as tendências do mercado e com uma abordagem de plataforma aberta, entendendo que a chave para uma segurança eficaz está na capacidade de integrar soluções não apenas dentro do mesmo fabricante, mas também com tecnologias de terceiros.

Desta forma, garantimos aos clientes maior proteção do investimento, interoperabilidade e eficiência.

Outro diferencial está no investimento da Cisco em construir data centers distribuídos pelo mundo com os mais altos padrões de qualidade e segurança para garantir o melhor desempenho e confiabilidade para os nossos clientes.

Poderíamos destacar outras iniciativas da Cisco para proteger o mercado de computação na nuvem?
Vale destacar uma das recentes adições ao portfólio, com a solução Cisco Secure Cloud Insights, que permite ampliar a visibilidade em ambientes multicloud resolvendo um dos desafios mais complexos para profissionais de segurança e TI, que é entender o uso de recursos dinâmicos na nuvem no intuito de verificar →

Caminhando para um futuro híbrido

Juan Marino
Cybersecurity Sales Strategy Manager LATAM
Cisco

as configurações de segurança para minimizar a superfície de ataque de forma eficaz e em conformidade com as legislações.

Por fim, como você enxerga o mercado de computação na nuvem para os próximos anos, falando sobre tendências, desafios e oportunidades para esse setor?
Vemos um aprofundamento da adoção da nuvem tanto para a computação quanto para serviços de TI e segurança. O mercado exige maior simplicidade e consolidação com as quais vemos uma tendência contra a fragmentação. Os principais players, como a Cisco, capazes de consolidar serviços de rede, computação, colaboração e segurança são os mais bem posicionados para atender as necessidades do mercado.

.

Caminhando para um futuro híbrido

Juan Marino
Cybersecurity Sales Strategy Manager LATAM
Cisco

Investimento em startups de cloud security cresce no Brasil

Embora a capacitação de mão-de-obra especializada seja a melhor alternativa em um mundo utópico, já discutimos, em edições anteriores do CyberTech Report, as dificuldades que o mercado enfrenta para inserir novos talentos no mercado. Felizmente, a adoção massiva da nuvem como infraestrutura computacional tem impulsionado o nascimento de diversas startups que oferecem soluções de segurança específicas para esse tipo de ambiente.

Estamos falando de plataformas que auxiliam times de segurança a ter maior visibilidade sobre sua (ou suas, no caso de uma abordagem multicloud) nuvem, entendendo exatamente os gaps existentes em sua estratégia de proteção, auxiliando na correta configuração de privilégios de acesso e até mesmo ajudando a reduzir custos cortando o uso desnecessário de poder computacional ou armazenamento de dados contratado.

O gráfico ao lado mostra **o volume de investimento e número de deals de acordo com o estágio de aporte recebido por startups brasileiras de cloud security ao longo dos últimos anos**. Hoje, nossa base de inteligência Cyber Digital Hub monitora 10 startups do segmento que, juntas, empregam 166 funcionários e estão localizadas sobretudo no estado de São Paulo.

Naturalmente, todas elas possuem um modelo de negócios business-to-business (B2B).

Investimentos e deals por estágio

	Nº de deals	Investimento (em milhões de US$)
Anjo	8	3,1 mi
Private Equity	1	1,6 mi
Pré-Seed	17	3,4 mi
Seed	29	19,1 mi
Series A	11	33,5 mi
Series B	5	168,6 mi
Series C	3	159,6 mi
Series D+	1	100 mi

Equilibrando agilidade e segurança

Pedro Pisa
Diretor Executivo
Solvimm

Como a Solvimm enxerga o atual uso da tecnologia da computação na nuvem por parte das empresas brasileiras? Temos consciência de que a maior parte das corporações que migraram para infraestruturas cloud nos últimos anos são de pequeno e médio porte. Elas realmente estão preparadas para trabalhar com tal ambiente e suas peculiaridades?
A computação em nuvem facilitou e revolucionou o mercado de inovação brasileiro. Principalmente para novos negócios, a tecnologia permite testar com muito mais rapidez e menor custo, promovendo inovação e ciclos rápidos de melhorias.

É muito raro vermos projetos de inovação que não se utilizam da computação em nuvem. E essa agilidade e facilidade em criar ambientes, muitas vezes faz com que as empresas priorizem a velocidade em detrimento da segurança.

O que observamos no mercado é que muitas empresas focam apenas em fazer as suas aplicações funcionarem na Internet, sem foco na construção de mecanismos de proteção de dados e de confiabilidade das aplicações.

Como vocês auxiliam essas empresas a fazerem um uso mais seguro da computação na nuvem, evitando intrusões de criminosos cibernéticos e vazamentos de dados, por exemplo?
Na Solvimm, acreditamos que não é necessário escolhermos entre agilidade e segurança. Com as ferramentas disponíveis na computação em nuvem, é possível ter os dois.

A jornada dos nossos clientes começa com uma revisão completa dos ambientes das suas aplicações, identificando os principais riscos em termos de tecnologia, processos e formação das pessoas da empresa. Em seguida, começamos uma caminhada de melhoria contínua a quatro mãos com nossos clientes, incluindo workshops para a equipe, mentorias para estruturar as aplicações com maior segurança, confiabilidade e desempenho, squads de implementação das melhorias e processos de manutenção e suporte dos ambientes já existentes.

Com esse processo, nossos clientes focam nos riscos mais prioritários para o negócio de cada um deles, visualizando ao longo do tempo as melhorias de segurança enquanto ainda agilizam a sua própria operação. →

O mercado de soluções de segurança para nuvem vem crescendo exponencialmente, o que naturalmente gera uma maior competitividade no mercado. Quais diferenciais da Solvimm você citaria em comparação com outras startups com o mesmo core business?
A Solvimm foca na atenção personalizada ao negócio de cada cliente. Embora nos apoiamos em ferramentas, procedimentos e automações para agilizar a entrega, nossa equipe é treinada e certificada para entregar as soluções adequadas à realidade de cada cliente.

Como prova da nossa competência, possuímos o reconhecimento da Amazon Web Services (AWS) como Well Architected Partner e também especializações em serviços ligados a automação de segurança nos ambientes, como o AWS Config e o AWS CloudFormation.

Em nossa gestão com os clientes, entendemos que segurança é a prioridade zero em todos os projetos e construímos fortes relações de confiança com nossos clientes buscando a melhoria contínua nesse quesito.

Para a Solvimm, como a nuvem está ajudando a criar novas soluções inovadoras e arquiteturas inéditas de segurança cibernética? Como tal tecnologia impulsiona a inovação e quais são suas perspectivas para os próximos anos?
Quando falamos sobre a união de agilidade e segurança, o principal que precisamos fazer é repensar o papel das equipes de segurança das empresas. Durante muito tempo, essas equipes eram envolvidas na revisão do ambiente e na autorização ou não de determinada tecnologia, construindo manuais de inúmeras páginas que nunca eram lidas. Esse processo era demorado e, muitas vezes, falho, pois quando o time de segurança era envolvido, muitas vezes já não havia tempo para as correções necessárias.

Com a computação em nuvem, devido a toda a infraestrutura ser programável, as regras de segurança também podem ser programáveis. Chegamos, assim, no conceito de Segurança como Código.

O novo papel dos times de segurança é desenvolver as regras de segurança e conformidade previamente nos ambientes de desenvolvimento e homologação.

Assim, é possível que os desenvolvedores já criem as aplicações cientes das regras de segurança e, caso as aplicações não sejam aprovadas nessas regras, isso será percebido no próprio ambiente de produção, com validações instantâneas e automáticas. Dessa forma, a computação em nuvem cria a possibilidade de auditoria contínua e em tempo real, o que permite que as aplicações sejam criadas já com a segurança adequada, promovendo Agilidade e Segurança Cibernética.

Equilibrando agilidade e segurança

Pedro Pisa
Diretor Executivo
Solvimm

kumulus

Nome: Kumulus

Local: Campinas, SP

Ano de fundação: 2017

Público: B2B

Sobre

Embora o seu modelo de negócio não seja exclusivamente focado em computação na nuvem, a Kumulus é uma startup nacional que chama atenção por se posicionar como uma agente de transformação digital que utiliza tal tecnologia como apoio para criar estratégias disruptivas aos seus clientes, independentemente do porte ou segmento da empresa interessada.

Fundada por ex-engenheiros da Microsoft em 2017, a companhia também oferece serviços de data & analytics, machine learning, modernização de aplicações e assim por diante. Falando especificamente de soluções para a nuvem, além de auxiliar seus parceiros em toda a jornada de migração para o novo ambiente, a marca também oferece gestão de segurança da infraestrutura com suporte 24/7.

A equipe da Kumulus consegue identificar pontos de vulnerabilidade, auxiliar na correta configuração e automatizar diversas tarefas para que a empresa possa se concentrar em seu core business, sem a necessidade de ter mão-de-obra interna especializada.

A maior acionista da Kumulus é a multinacional Logicalis, que, em 2020, adquiriu 30% da companhia para aumentar seu portfólio global de serviços gerenciados para a nuvem. Posteriormente, em 2021, a Logicalis aumentou ainda mais sua participação, se tornando acionista majoritária da startup brasileira.

“A migração para a nuvem ganhou força no último ano e tende a ter ainda mais tração daqui para frente. No período em que atuamos juntos, a Kumulus mostrou que é uma empresa sólida, com conhecimento de alto nível e que pode contribuir com a aceleração das agendas da transformação digital na base de clientes da Logicalis, não só no Brasil, mas também na América Latina”, comentou Rodrigo Parreira, CEO da Logicalis para a América Latina.

A nuvem como meio para a transformação digital

Thiago Caserta
Founder & CSO
Kumulus

A Kumulus é uma startup nacional que se especializou em acompanhar a jornada das empresas para a nuvem e oferecer serviços gerenciados de administração de ambientes e segurança dos próprios. Primeiramente, como vocês enxergam esse período de transformação digital acelerada, na qual empresas de todos os portes resolveram adotar a nuvem para digitalizar a entrega de seus produtos e serviços? Como tal período foi encarado pela Kumulus?
Costumamos dizer aqui na Kumulus que a transformação digital é, em primeiro lugar, uma transformação cultural, uma mudança de mindset que as organizações precisam adotar devido aos fenômenos da nova economia e da globalização digital. É interessante notar que, devido a tais fenômenos, mudanças estruturais na nossa sociedade ocorreram, tanto nos hábitos de consumo como de trabalho.

Com o aumento vertiginoso da utilização de devices, como smartphones e tablets, é possível dizer que essa transformação não é apenas necessária, mas obrigatória para que as empresas permaneçam relevantes. Um exemplo que gosto de utilizar são os dos próprios clientes das empresas.

Considerando a visão convencional de mercado, os clientes são meros atores passivos com os quais as empresas possuem relacionamento.

Em uma era digital, porém, avançamos para um mundo dominado por um conceito conhecido como rede de clientes. Nesse contexto, todos os clientes ou potenciais clientes de uma organização se conectam e interagem com a sua marca de forma dinâmica e contínua.

Hoje, os clientes são influenciadores uns dos outros, com o poder de construir ou destruir a reputação de empresas e marcas, mostrando assim o claro poder que possuem no âmbito do consumo.

A utilização das plataformas digitais, as quais se tornaram possíveis graças ao avanço tecnológico, muito alavancado pelas capacidades da nuvem, também afetam a maneira como os consumidores procuram, analisam, compram e utilizam os produtos e serviços de uma determinada empresa, bem como interagem e se mantêm conectados com as organizações.

Isso força as empresas a repensarem a forma de atrair novos clientes e reter os já existentes, seja através do uso eficiente das redes sociais, plataformas de busca, lojas online e até mesmo seus diversos canais de comunicação, que podem utilizar tecnologias de inteligência artificial, por exemplo, para garantir um atendimento mais assertivo. →

Também notamos uma mudança no nível de agilidade exigido pela nova economia. Quanto tempo estamos dispostos a esperar por um táxi hoje em dia? Alguns minutos talvez! Isso tem relação com essa mudança de hábito que a tecnologia impulsionou, a qual permite que hoje solicitemos um transporte terrestre, como um táxi, com apenas alguns toques do nosso smartphone, conectando com o carro disponível mais próximo baseado na nossa localização geográfica.

Essa "falta de paciência", característica presente na atual sociedade digital, é que vem exigindo a agilidade na transformação das empresas. As empresas precisam lançar novidades, precisam estar em mais canais, precisam corrigir bugs de maneira mais rápida.

No fim do dia, a tecnologia é meio para essa transformação, mas o objetivo principal da organização sempre será o de se adaptar ao mundo cada vez mais digital em que vivemos hoje.

O mesmo se passa no ambiente de trabalho. Podemos dizer que a pandemia do COVID-19 acelerou essa mesma transformação mencionada sobre os hábitos de consumo — o aumento no volume de transações via plataformas de delivery como iFood e Rappi representa bem isso —, mas principalmente no modelo de trabalho.

Como se adaptar aos conceitos remote first, home office e organizações híbridas? Utilizando de maneira eficiente a tecnologia disponível hoje, principalmente quando destacamos a capacidade que a nuvem possui de disponibilizar de maneira rápida e eficiente exatamente aquilo que minha organização necessita, sejam soluções de colaboração que permitam a extensão do escritório físico, com mais segurança e de forma mais ágil, ou aplicativos para agendamento de mesa no escritório devido ao distanciamento físico praticado até então.

Com essa visão em mente, notamos que o que ocorreu foi uma percepção acelerada das organizações para implementarem tais mudanças estruturais, as quais possibilitam que essas organizações se adaptem à atual era digital que vivemos. A Kumulus encara esse período como uma onda de transformação natural e necessária e, como agentes da transformação digital, temos a oportunidade de apoiar centenas de organizações a utilizarem a o melhor da tecnologia, que é meio, da maneira mais efetiva possível, para que elas possam alcançar melhores resultados nessa nova economia.

Você poderia detalhar como funcionam as soluções e ofertas da Kumulus para auxiliar a jornada das empresas para a nuvem e mitigar as ameaças que existem nesse tipo de ambiente?
Somos agentes da transformação digital. Nos consideramos *enablers*, ou seja, facilitadores para que os objetivos dos nossos clientes sejam alcançados.

Para nós, o nosso sucesso é medido pelo resultado que os clientes dos nossos clientes terão com as soluções que implementamos, gerenciamos e suportamos. →

A nuvem como meio para a transformação digital

Thiago Caserta
Founder & CSO
Kumulus

→ Nosso portfólio se baseia em dois pilares principais de transformação:

A transformação da cultura/mindset, a qual chamamos de Agile Transformation, e um segundo pilar que é a tecnologia em si. Desses dois pilares principais, oferecemos soluções personalizadas para cada tipo de cliente, baseado nas suas principais dores, tamanho, setor e outras características que avaliamos durante os primeiros engajamentos que temos com cada empresa.

Hoje atendemos empresas de diversos tamanhos e segmentos, e temos apoiado não apenas na jornada para a nuvem, mas na estruturação de um plano estratégico de transformação digital, que envolve, além da nuvem em si, soluções com foco em Data Analytics, Application Modernization, DevOps e Modern Workplace.

A nuvem possui o conceito de gestão compartilhada. Os grandes players desse mercado, como Microsoft, Amazon e Google são responsáveis por prover os recursos computacionais necessários para armazenar e processar as cargas de trabalho de empresas em todo o mundo. Quando falamos de segurança, diversas camadas de proteção já são fornecidas por essas mesmas empresas, como segurança e redundância física dos recursos, isolamento e segregação dos ambientes de cada cliente, certificações internacionais de segurança e compliance, além de toda a infraestrutura necessária para suportar os maiores negócios do mundo, com milhares de profissionais monitorando e gerenciando tais recursos.

Por outro lado, cabe a cada empresa fazer a gestão do seu lado da ponta, seja das suas próprias aplicações, que foram configuradas através dos serviços de nuvem, como seus dados são armazenados e utilizados, bem como entender as premissas de segurança necessária para o seu negócio.

Dessa forma, podemos dizer que muitas vezes se faz necessário o apoio de parceiros estratégicos, como a Kumulus, que apoiam as organizações fornecendo essa camada adicional de segurança, através de soluções que atuarão no nível das aplicações e soluções utilizadas por cada cliente. Essas soluções podem partir de um simples antivírus que deverá ser instalado nos servidores virtuais do cliente até soluções de monitoramento e segurança contra ameaças como um Web Application Firewall (WAF), um time de especialistas em segurança que atuarão em escala 24x7 dentro de um centro de operação de segurança (SOC), entre outros.

É prudente concluir que, pelo seu *core business*, a Kumulus possui experiência em ajudar empresas de todos os segmentos e portes na jornada para a nuvem. Na visão de vocês, quais são os principais riscos dessa jornada (quando feita sem o apoio devido) e quais são os principais erros que as corporações adotam ao decidir por usar tal tecnologia?
Os maiores equívocos durante essa jornada estão relacionados com o entendimento correto da dor e a forma como a empresa busca realizar essa transformação e/ou um foco muito grande na tecnologia que ele deseja utilizar, do que na solução em si. →

A nuvem como meio para a transformação digital

Thiago Caserta
Founder & CSO
Kumulus

Para elucidar, podemos pensar numa empresa que está buscando uma solução para melhorar o atendimento aos seus clientes através de canais digitais. Essa não é necessariamente a dor do cliente, talvez o cliente simplesmente não é entendido durante o atendimento, mas, baseado nessa percepção, essa empresa resolve criar um chatbot para que o seu cliente tenha um contato *self-service* a qualquer hora do dia para que ele tire dúvidas, por exemplo.

Se o cliente não estiver buscando isso e, de fato, o problema tenha relação com a compreensão do seu problema, uma simples solução que responde as perguntas mais comuns através de um chat pode deixá-lo mais frustrado, gerando maior insatisfação. No fim do dia, notamos que essa empresa criou apenas uma barreira adicional, pois ela focou demasiadamente numa percepção de dor que não era a dor principal, ou olhou apenas a tecnologia em si ("quero ser uma organização inovadora, vou criar um chatbot").

É muito comum ouvirmos no mercado empresas que querem ir para nuvem, que querem ter um data lake, buscam trabalhar com machine learning, mas elas acabam deixando de lado a visão de que essas tecnologias são apenas o meio.

O grande segredo para uma jornada de sucesso é entender para onde a organização está indo, do ponto de vista de mudanças estruturais, culturais e de processos, que eventualmente vão gerar maior atratividade, qualidade, e outros benefícios e diferenciais para o seu cliente final e aí sim compreender quais tecnologias e soluções deverão ser adotadas para atingir esse resultado.

No geral, podemos dizer que a nuvem é o alicerce de tudo. Não temos dúvidas de que fará muito mais sentido utilizar as tecnologias em nuvem por inúmeros motivos já conhecidos, como elasticidade, escalabilidade, acesso a tecnologias avançadas pagando pelo tempo de uso e de acordo com a necessidade e tamanho da empresa, porém a premissa principal é entender como de fato essa jornada se encaixa para a minha empresa. Claro que uma empresa poderia simplesmente fazer uma migração da sua infraestrutura on-premise para a nuvem, e isso já poderia ser considerado parte de um plano de jornada para a nuvem.

Mas, levando em consideração os aspectos da transformação digital mencionados em outras respostas, a re-arquitetura do ambiente tecnológico atual, a definição de novas soluções necessárias, bem como a otimização da operação, com certeza deve considerar essa visão de mapear e entender os principais desafios que a empresa busca atender, para que ela se mantenha relevante no mercado em que atua.

É possível perceber que a Kumulus carrega consigo, em seu DNA, uma forte ligação com a inovação e fomento de outras startups em geral. Como se dá essa relação da marca com a inovação aberta e incentivo a novos empreendedores? Vocês possuem e/ou participam de programas e iniciativas relacionadas ao assunto?
Por sermos especializados em transformação digital, a Kumulus está sempre envolvida em iniciativas de inovação. →

A nuvem como meio para a transformação digital

Thiago Caserta
Founder & CSO
Kumulus

Temos orgulho de ter em nosso hall de clientes startups como Neon, Dentro da História, Netshow.me, além de ter apoiado diversas outras startups e empreendedores a darem o pontapé inicial nas definições do seu stack tecnológico.

Em geral, nós atuamos muito próximo dos próprios empreendedores desses negócios ou o CTO da startup. Além de ter participado como membro da Associação Brasileira de Startups e patrocinado eventos como o CASE (Conferência Anual de Startups e Empreendedorismo), nós atuamos diretamente com nossos parceiros de tecnologia, como Microsoft e Google, em programas de incentivo às empresas Digital Natives e startups no geral, além de participarmos e organizarmos hackathons que buscam desenvolver novas soluções a partir de tecnologias em nuvem.

A nuvem como meio para a transformação digital

Thiago Caserta
Founder & CSO
Kumulus

Investimentos disparam ao redor do globo

Panorama Internacional

E o prêmio vai para...

A importância da soluções de segurança na nuvem se torna ainda mais clara quando analisamos o cenário internacional. Conforme um levantamento já realizado anteriormente pelo Distrito através de radares globais de mercado, **"Segurança de Infraestrutura na Nuvem" foi o modelo de negócio que mais recebeu investimentos ao longo de 2021, movimentando, sozinho, nada menos do que US$ 3,3 bilhões** ao redor do globo. Ficam em segundo e terceiro lugar, respectivamente, "Segurança de Endpoint" com US$ 1,1 bilhão e Gestão de Identidade e Acesso (IAM) com US$ 737 milhões.

Estamos falando de startups que auxiliam empresas — sejam elas outras startups que estão começando a usar a nuvem ou corporações de grande porte que procuram migrar sua infraestrutura legada — a identificar eventuais riscos em seu ambiente remoto. Também estão inclusas nesse escopo as ferramentas que oferecem camadas adicionais de proteção para infraestruturas-como-serviço, indo além dos recursos oferecidos de forma nativa pelos prestadores de serviço.

Por fim, a categoria também engloba terceirização de gerenciamento de ambientes de cloud computing, no modelo que conhecemos como provedor de serviços gerenciados de segurança (Managed Security Services Provider ou MSSP).

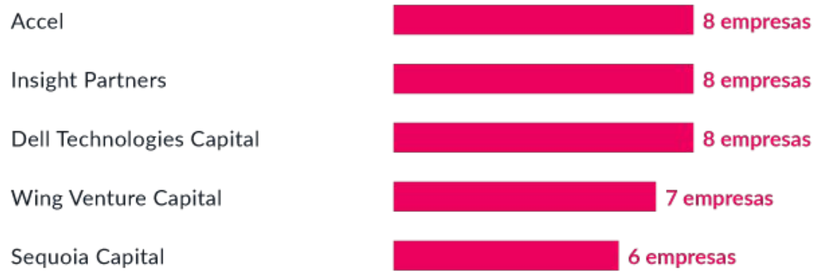
Modelos de negócio em cibersegurança com maior investimento em 2021

Pandemia dispara preocupações

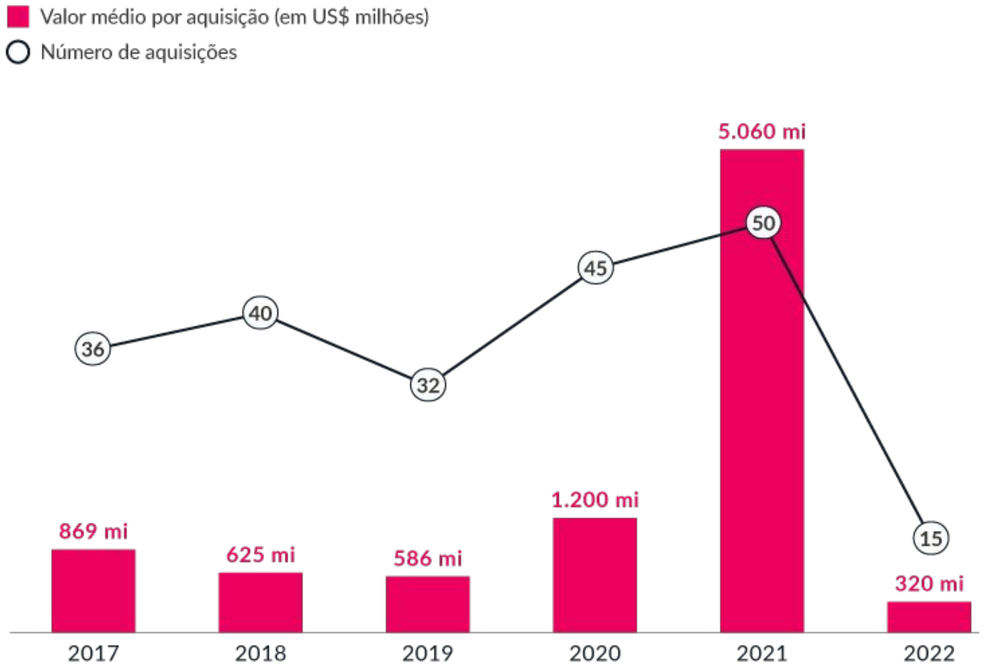
Se analisarmos as rodadas de investimento em startups de segurança na nuvem ano-a-ano, perceberemos que houve uma alta vertiginosa em 2021. Não é à toa: este foi o ano em que, embora a pandemia do novo coronavírus estivesse começando a se tornar mais branda (com o início dos programas de imunização e queda no número de casos mortais), as empresas que migraram para infraestruturas de cloud computing em 2020 (em pleno "pico do incêndio") começaram a perceber as dificuldades e ameaças que rondam tal ambiente.

Como resultado, **o ano seguinte ficou marcado por um interesse generalizado em soluções que pudessem automatizar grande parte dos desafios e dificuldades** enfrentadas pelas empresas na hora de lidar com tais ambientes. Ainda é cedo para palpitar, mas a tendência é que os investimentos em 2022 sigam com números expressivos.

Investidores mais ativos e nº de empresas investidas



Evolução nos investimentos e nº de rodadas



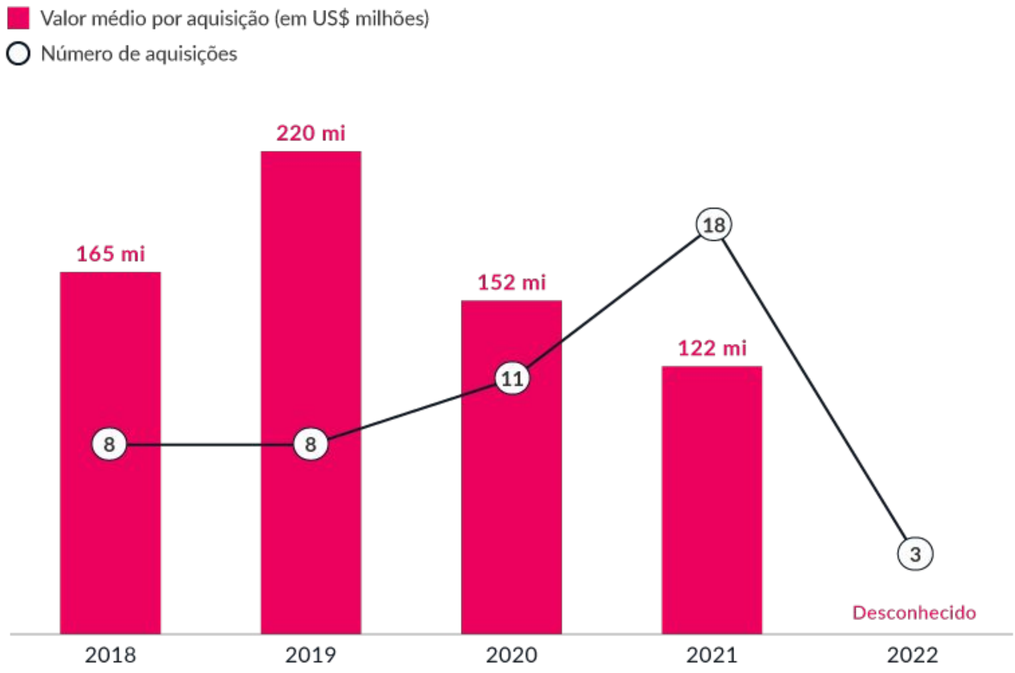
Aquisições: quantidade sobe, valor cai

Outro fenômeno interessante a ser observado é que, cada vez mais, startups promissoras do setor de cloud security estão sendo adquiridas por empresas de grande porte — geralmente, provedoras de soluções de segurança com tradição e renome no mercado. Afinal, é mais fácil embutir em seu portfólio uma nova ferramenta de alta demanda no mercado do que desenvolver algo do zero. As próprias provedoras de soluções de computação na nuvem também estão se tornando compradoras fervorosas de novas soluções de segurança para infraestruturas-como-serviço.

Porém, ao mesmo tempo em que o número de aquisições está claramente subindo, **o valor médio de cada transação está se tornando mais baixo**. Isso pode ser explicado pelo fato de que as startups adquiridas costumam estar em um estágio menor de maturidade, possuindo assim um valor menor de mercado.

Se por um lado isso pode ser encarado como uma tendência monopolista, por outro, podemos enxergar essa tendência como uma excelente oportunidade para novos empreendedores que desejam fundar novas startups e conseguir exits em tempo recorde. Tudo depende de sua estratégia de mercado.

Aquisições de startups de cloud security



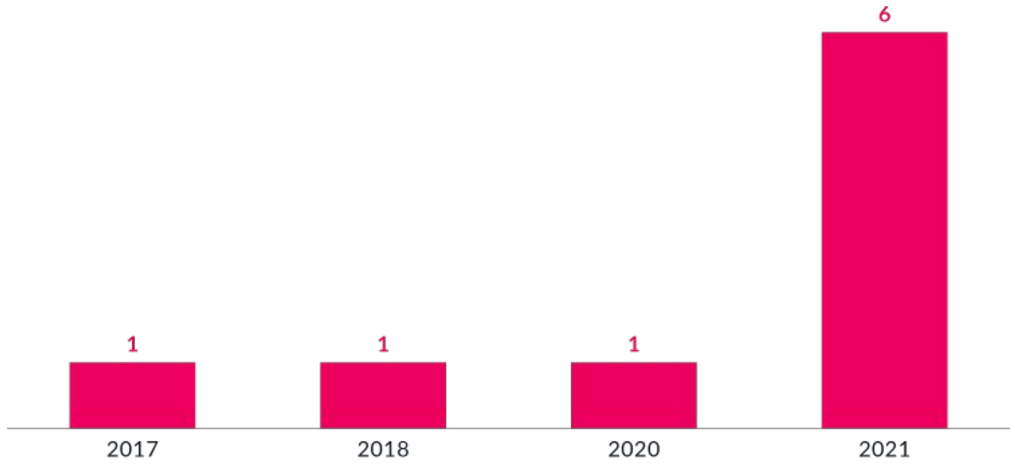
Unicórnios que voam sobre as nuvens

Ao redor do globo, temos um total de **9 startups de cloud security que atingiram o status de unicórnio**. Claro, trata-se de um número pequeno se compararmos com o cenário empreendedor de outras verticais tecnológicas, mas é importante frisar, novamente, que grande parte das startups desse segmento acabam se dissipando em fusões ou aquisições. Logo, trata-se de uma quantia expressiva.

Além disso, em consonância com a tendência de maiores investimentos em 2021, não é surpresa alguma perceber que esse foi o ano em que tivemos o maior nascimento de unicórnios. Confira a lista de startups com tal status:

- **Illumio:** fundada em 2013 nos EUA, captou um total de US$ 566 milhões em aporte e se encontra em Series F
- **Netskope:** fundada em 2012 nos EUA, captou um total de US$ 1,04 bilhão em aporte e se encontra em Series H
- **Artic Wolf:** fundada em 2012 nos EUA, captou um total de US$ 500 milhões em aporte e se encontra em Series F
- **Lacework:** fundada em 2015 nos EUA, captou um total de US$ 1,9 bilhões em aporte e se encontra em Series D
- **Aqua Security:** fundada em 2015 nos EUA, captou um total de US$ 1,9 bilhões em aporte e se encontra em Series D
- **Wiz:** fundada em 2020 em Israel, captou um total de US$ 600 milhões em aporte e se encontra em Series C
- **Orca Security:** fundada em 2019 em Israel, captou um total de US$ 632 milhões em aporte e se encontra em Series C
- **Sysdig:** fundada em 2013 nos EUA, captou um total de US$ 744 milhões em aporte e se encontra em Series G
- **Aviatrix:** fundada em 2014 nos EUA, captou um total de US$ 346 milhões em aporte e se encontra em Series E

Nascimento de unicórnios por ano



Nome: Netskope

Local: Santa Clara, EUA

Ano de fundação: 2012

Público: B2B

Sobre

Podemos considerar a Netskope como startup mais bem-sucedida no segmento de segurança para computação na nuvem. Tendo participado de oito rodadas de investimento, ela atualmente encontra-se no estágio de Series H e já conseguiu nada menos do que US$ 1,04 bilhão em investimentos — o que lhe concede status de unicórnio, que ostenta desde 2018.

Com atuação em diversos países (incluindo o Brasil), a empresa oferece uma vasta gama de soluções para quem deseja proteger sua infraestrutura na nuvem. Entre os destaques, podemos citar seu cloud access security broker (CASB), que é considerada referência entre outras ferramentas similares. UM CASB nada mais é do que uma espécie de “corretor” que lhe auxilia a ter maior visibilidade e controle sobre as diversas aplicações e infraestruturas no caso de uma abordagem multicloud.

Já a Netskope Cloud XD é uma plataforma completa, tudo-em-um, que promete oferecer "visibilidade inigualável" em tempo real sobre tudo o que acontece em ambientes na nuvem, detecando ameaças e protegendo dados a partir de qualquer local e qualquer dispositivo.

Ela pode ser integrada com outras ferramentas de segurança, incluindo soluções de compartilhamento de inteligência cibernética, SIEM/SOAR e assim por diante.

Por fim, vale destacar que a Netskope também conta com soluções de segurança que utilizam a nuvem como mecanismo central. Um bom exemplo é o Netskope Cloud Firewall, que utiliza políticas de regras baseadas na nuvem para facilitar uma administração centralizada de redes híbridas.

Iniciativas da líder de mercado

Américo de Paula
Head of Solutions Architecture LATAM
Amazon Web Services

A Amazon Web Services é a maior suíte de soluções em nuvem do mundo, ostentando o maior market share desse mercado. Trata-se da primeira opção de muitas empresas e profissionais que procuram adotar a cloud computing em seu processo de transformação digital. Ao mesmo tempo, como resultado natural dessa popularidade, a maioria das violações de dados na nuvem que vemos são de ambientes mal configurados da AWS. O que a empresa faz para promover um uso mais seguro e consciente dessa tecnologia?
A AWS tem a plataforma de nuvem mais abrangente e amplamente adotada do mundo e conta com mais de 200 serviços completos nas mais diversas áreas, como Security, Compute, Networking, Analytics e AI/ML. Nossos números são importantes e a segurança de dados é nossa principal preocupação e prioridade.

Nossas ofertas de serviços são respaldadas por mais de 280 ferramentas de segurança, compliance e governança. Todos os 117 serviços da AWS que armazenam dados de clientes oferecem a capacidade de criptografar esses dados automaticamente, além do suporte a 98 padrões de segurança e certificações de conformidade, incluindo PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2 e NIST 800-171, que oferecemos para ajudar os nossos clientes a atender aos requisitos de conformidade de praticamente todas as agências reguladoras ao redor do mundo.

Temos um modelo de responsabilidade compartilhada com todos os clientes, pois de nada adianta ter a casa com todos os dispositivos de segurança mais atuais do mercado e deixar a porta aberta. A segurança se dá em parceria. A AWS gerencia e controla os componentes do sistema operacional host e da camada de virtualização até a segurança física das instalações nas quais os serviços operam, e os nossos clientes são responsáveis por construir aplicações seguras.

Os clientes mantêm a propriedade e o controle de todo o conteúdo armazenado na AWS. A AWS fornece todos os mecanismos, mas somente os próprios clientes podem decidir criptografar ou não seus dados e quais dados, exatamente, criptografar. →

A busca por segurança é um trabalho constante de vigilância e atualização. Para diminuir os riscos de nossos clientes “deixarem a porta aberta”, além de ferramentas de criptografia, oferecemos uma ampla variedade de documentos de práticas recomendadas e outras orientações que eles podem aproveitar ao fornecer medidas de segurança em nível de aplicação.

Além disso, os parceiros da AWS oferecem centenas de ferramentas e recursos para ajudar os clientes a cumprir seus objetivos de segurança, que vão desde segurança de rede, gerenciamento de configuração, controle de acesso e criptografia de dados. Todos os setores nos quais a segurança é uma questão crítica, como finanças, saúde, governo e energia, estão cada vez mais confiando no poder da nuvem.

A AWS foi projetada para ser o ambiente de computação em nuvem mais flexível e seguro disponível. Segurança sempre será nossa prioridade.

Nossa infraestrutura atende organizações militares e bancos globais, por exemplo, sendo aceita como segura para cargas de trabalho estritamente secretas.

São diversas as iniciativas da AWS para promover o uso da computação na nuvem por parte de startups e fomentar a inovação através de tal tecnologia. Quais são essas principais iniciativas e como a empresa se posiciona no que tange ao cenário global de inovação? De quais outras formas a AWS se comunica e interage com o empreendedorismo digital?
A AWS está no Brasil há 10 anos e, se pensarmos nas startups que surgiram neste período, muitas teriam tido muita dificuldade em se desenvolver sem os valores acessíveis, dinamismo e inovação viabilizados pela nuvem. Alguns data centers custariam milhões de reais, valor impraticável para quem está começando. Não somos simplesmente implementadores de tecnologia, apenas diminuindo os custos e melhorando o time-to-market.

Na verdade, a atuação da AWS auxilia na operação dos negócios, colocando os dados no centro de tudo, possibilitando mais inovação ao permitir que os clientes ousem, testem mais propostas, falhem, aperfeiçoem os modelos, testem novamente e, assim, evoluam. A nuvem, desde o início, tem sido o berço da inovação ao permitir que ideias ganhem vida a um preço muito baixo.

C6 Bank, Quinto Andar, iFood, PicPay, Nubank, Hotmart, EBANX e Gympass são alguns exemplos de startups que começaram e estão conosco. No Brasil e no mundo, boa parte das startups começou na nuvem e a maioria delas começa na AWS. Temos grande parte dos unicórnios brasileiros na nossa nuvem.

Nossas novas gerações de chips diminuem de 25% a 40% os custos da nuvem, o que é um grande diferencial para atrair startups que trabalham com machine learning e precisam de cargas de trabalho mais custo-efetivas. As startups também estão consumindo mais VR e AR, que se somam a visualização em 3D, machine learning, inteligência artificial e IoT entre as soluções que têm sido buscadas. →

Iniciativas da líder de mercado

Américo de Paula
Head of Solutions Architecture LATAM
Amazon Web Services

A AWS conta com várias iniciativas voltadas a startups, como o programa AWS Activate, que oferece às startups uma série de benefícios, incluindo créditos AWS — somente no ano passado, fornecemos mais de US$ 1 bilhão em créditos por meio do programa para ajudar as startups a crescer e escalar seus negócios, e um total de mais de US$ 4 bilhões em créditos para mais de 170 mil startups ao longo dos sete anos desde o lançamento do AWS Activate.

Temos ainda o AWS EdStart, uma aceleradora de startups de tecnologia educacional que foi projetada para ajudar os empreendedores a construir a próxima geração de soluções de aprendizado on-line, análise e gerenciamento de campus na nuvem AWS. Oferece benefícios como suporte financeiro por meio de créditos em serviços AWS, treinamento técnico e suporte, acesso a uma comunidade global de especialistas em EdTech e muito mais.

As startups também podem contar com o AWS Startup Mentorship, que oferece mentoria de experts; APN Global Startup Program, que apoia startups em rápido crescimento por meio de validação técnica, apoio em go-to-market e habilitação de vendas; AWS Cost Optimization, que permite às startups otimizar seus gastos com serviços na nuvem.

Em março de 2022, a AWS também lançou o AWS Space Accelerator, que auxilia startups que usam a nuvem para reimaginar missões espaciais comerciais e governamentais, e o AWS Sustainable Cities Accelerator, que oferece suporte a startups que criam soluções de mobilidade e transporte para aumentar a sustentabilidade de centros urbanos de rápido crescimento.

Iniciativas da líder de mercado

Américo de Paula
Head of Solutions Architecture LATAM
Amazon Web Services

Sabemos que há uma falta de mão-de-obra generalizada de profissionais capacitados em segurança cibernética. Quando falamos sobre computação na nuvem, é ainda mais difícil encontrar mão-de-obra especializada. Como a AWS enxerga esse cenário e quais são as perspectivas para o futuro? Mais do que simplesmente capacitar profissionais, a empresa está empenhada em automatizar recursos de segurança para usuários da nuvem?

Encaramos o desafio da mão-de-obra especializada em cibersegurança com nossos vários tipos de treinamentos. A AWS continua a investir na qualificação local de desenvolvedores, alunos e na próxima geração de líderes de TI por meio de programas como AWS Academy, AWS Educate, AWS re/Start, AWS Skill Builder e todo o programa de Treinamentos & Certificações.

Esses programas educacionais da AWS ajudam estudantes de todas as origens e experiências a se preparar para carreiras na nuvem. Com apoio de iniciativas públicas e privadas, de cursos universitários a programas de treinamento em tempo integral e conteúdo de aprendizado individualizado, esses programas oferecem →

acesso às habilidades para iniciar uma carreira na nuvem.

Globalmente, estamos comprometidos a capacitar 29 milhões de pessoas em nuvem até 2025. E só no Brasil, já treinamos 200 mil pessoas em nuvem desde 2017.

Uma parte, em cibersegurança, exatamente a segunda maior habilidade digital que será demandada pelas organizações brasileiras em 2025, de acordo com o Estudo Global de Habilidades Digitais da AWS.

No entanto, as competências em cibersegurança, como a capacidade de implementar medidas para sanar ameaças e vulnerabilidades de segurança digital, fazem parte da formação ou estão sendo ensinadas para apenas 13% dos trabalhadores técnicos e não-técnicos brasileiros que participaram do estudo.

De 2020 ao fim deste ano, a AWS terá investido R$ 1 bilhão no desenvolvimento e expansão da nossa região na América Latina, localizada no Estado de São Paulo e que também dá suporte a iniciativas educacionais no Brasil. Nesse esforço, visamos atingir 100 mil empregos técnicos nos próximos 5 anos.

Quanto à automatização, a AWS conta com ferramentas para visibilidade e controle do ambiente - através dessa visibilidade é possível fazer a automatização de tarefas de segurança que auxiliam na redução de erros humanos de configuração, o que oferece mais tempo para que as equipes de Segurança da Informação se concentrem em outros trabalhos cruciais para as empresas.

Contamos com uma ampla variedade de soluções profundamente integradas que podem ser combinadas para automatizar tarefas de forma simples, usando, por exemplo, o AWS Lambda – código em linguagens de programação de mercado, sem necessidade de subir um servidor ou documentos de automação.

O Systems Manager inclui mais de 100 documentos de automação pré-configurados que os nossos clientes podem usar especificando parâmetros na execução, e se integra com outros serviços da AWS para, por exemplo, detectar e mudar a política de acesso de um “Bucket” público do S3 (serviço de armazenamento) para privado. Os serviços da AWS possuem APIs para interação, facilitando a automação e o trabalho da equipe de segurança em estreita colaboração com as equipes de desenvolvedores e operações para criar e implementar o código de maneira mais rápida e segura. Agile, DevOps e CI/CD são práticas fundamentais para a maioria dos profissionais de segurança.

As ameaças à segurança da informação continuam evoluindo continuamente, tornando as tarefas de proteção e segurança proativas e reativas difíceis, com alto custo de implementação e gastando muito tempo dos profissionais de segurança. Definir rotinas automatizadas para estas respostas, seguindo boas práticas de segurança e de conformidade baseadas em padrões de mercado, é um compromisso que temos junto aos clientes. →

Iniciativas da líder de mercado

Américo de Paula
Head of Solutions Architecture LATAM
Amazon Web Services

→ Falando especificamente do Brasil, qual é a estratégia da AWS para atender o público local? Vocês percebem peculiaridades nesse mercado e na América Latina em geral? Se sim, existem programas específicos para fomentar a inovação e a segurança no uso da computação na nuvem no continente?

Apenas cinco anos depois da fundação da AWS em Seattle (EUA), chegamos ao Brasil, o que já demonstrava a nossa visão do potencial do país. Isso foi em 2011, quando o Estado de São Paulo recebeu a oitava região AWS do mundo e sabíamos, desde o início, que investir em uma região é um compromisso de longo prazo, que envolve milhares de racks e servidores, entre outros investimentos maciços.

A nuvem foi essencial para a transformação digital das empresas, governos e instituições nesses 10 anos e a AWS tem um compromisso com as organizações brasileiras de ajudá-las em suas jornadas na nuvem.

Em recente estudo intitulado "A computação em nuvem na América Latina", a Global Data destacou a expectativa de que o mercado de nuvem chegue a US$ 11 bilhões na América Latina até 2025, com uma receita cumulativa de US$ 41,1 bilhões entre 2021 e 2025.

O estudo apontou que o futuro da nuvem corporativa na América Latina será híbrido conforme empresas de todos os portes buscarem formas de aproveitar os benefícios das nuvens públicas e privadas. Essa movimentação continuará a levar ao crescimento da computação em nuvem no curto e no médio prazo. Além disso, com o crescimento da adoção da IoT em processos empresariais críticos, a necessidade de uma análise dos dados na borda da rede começa a ganhar força.

O estudo também aponta que a migração das empresas para o modelo de negócios de IaaS híbrida na nuvem e a adoção crescente de soluções de infraestrutura como serviço (IaaS) por empresas de pequeno e médio porte impulsionam o mercado de IaaS da América Latina, que terá um crescimento aproximado de 24% de CAGR entre 2020 e 2025 chegando a quase US$ 5,5 bilhões ao final do período.

O segmento de plataforma como serviço (PaaS) é o mercado com crescimento mais rápido na região, com um CAGR de 30% durante o mesmo período.

Iniciativas da líder de mercado

Américo de Paula
Head of Solutions Architecture LATAM
Amazon Web Services

Tendências

Não adianta resistir: a nuvem não é o futuro, é o presente!

Apesar de tudo, a conclusão que podemos chegar neste relatório é bastante simples — a nuvem não é o futuro, ela é o presente. Independentemente do porte, segmento ou modelo de negócio, toda empresa pode (e deve!) usufruir dos benefícios da cloud computing caso queira participar desse amplo processo de transformação digital pelo qual o mundo está passando. Porém, **é importante que a adoção da nuvem não seja encarada como uma simples "modernização da infraestrutura para entrar na moda"**; sua adoção deve ser norteada por um sentido bem claro.

Seja para otimizar a entrega de serviços digitais para seus consumidores finais, seja para aprimorar o fluxo de trabalho de sua empresa no modelo híbrido — enfim, alcançar a nuvem é o meio, e não o fim. É necessário enxergar essa tecnologia como uma facilitadora da inovação.

Porém, a jornada para esse tipo de ambiente deve ser cerceada com cuidados apropriados. Embora a maioria das provedoras de infraestrutura-como-serviço já ofereçam soluções embarcadas de segurança e recursos gratuitos de treinamento, isso nem sempre é o suficiente para garantir que a sua marca não sofra um incidente por conta da falta de experiência.

Por conta disso, **as plataformas e soluções de cloud security são cada vez mais importantes**, automatizando tarefas e reduzindo a necessidade de mão-de-obra especializada — que, infelizmente, ainda é escassa e não podemos esperar a resolução desse problema.

Por conta disso, a tendência é que **investimentos em soluções de cloud security continuem crescendo a todo vapor** acompanhando a adoção da nuvem por um número cada vez maior de empresas ao redor do mundo. Até mesmo as big techs já perceberam que vale a pena investir nesse setor. Podemos estimar que, ao longo de 2022, o número de deals, fusões e aquisições será igual ou até mesmo superior ao registrado no ano passado.

Infelizmente, com uma concorrência forte no estrangeiro, as startups brasileiras naturalmente vão enfrentar certa dificuldade para escalar seu negócio e internacionalizar suas operações — caso este seja o seu plano, claro. Ainda assim, há muita demanda nacional por clientes que preferem recorrer a soluções nacionais. Ou seja: trata-se de um mercado promissor e lucrativo, independentemente da situação.

A nuvem como impulsionadora de cibersegurança

Por fim, também vale ressaltar que a computação na nuvem está possibilitando a criação de uma série de soluções e arquiteturas de segurança inéditas no mercado e que são apropriadas para o "novo normal". O **Secure Access Service Edge (SASE) e o Extended Detection and Response (XDR) são dois excelentes exemplos disso**, tornando suas redes híbridas ainda mais seguras e correlacionando com maior agilidade dados sobre ameaças nas mais diversas camadas de proteção.

Ou seja: mais do que ser uma tecnologia que serve como infraestrutura para otimizar a entrega de aplicações, recursos e poder computacional, a nuvem também está revolucionando o próprio mercado de segurança cibernética ao permitir a entrega de maior inteligência, rapidez e eficiência no monitoramento de riscos. Com tudo isso, não há dúvidas de que a nuvem veio para ficar.

Cybertechs

Glossário de categorias

Categorias

NETWORK & INFRASTRUCTURE SECURITY
Companhias que apliquem processos de proteção da infraestrutura da rede, instalando medidas preventivas para negar acessos não-autorizados, modificações, exclusões e roubo de recursos e dados. Essas medidas de segurança podem incluir controle de acesso, segurança de aplicativos , firewalls, redes virtuais privadas (VPN), análise comportamental, sistemas de prevenção de intrusão e segurança sem fio. Se relaciona com a camada física de transmissão e conexão. Também englobamos soluções de endpoint e messaging security nesta categoria.

WEB SECURITY
Medidas e protocolos de proteção que empresas utilizam para proteger suas organizações de criminosos e ameaças que usam a web como canal. Se relaciona com a camada não-física de segurança, o que engloba internet e segurança de sites.

APPLICATION SECURITY
Medidas de segurança que impedem o roubo/sequestro de dados e códigos dentro de dentro de aplicativos e plataformas.

DATA PROTECTION
Engloba empresas e serviços responsáveis pela proteção de informações sensíveis à empresa (banco de dados, informações de corporações) pelo enquadramento (compliance) às regulamentações de proteção de dados..

MOBILE SECURITY
Empresas que atuam com produtos e serviços voltados a garantir a segurança de dispositivos móveis, independente de seu sistema operacional. Via de regra, são companhias que visam a proteção contra ameaças associadas à conexões wireless.

SECURITY OPERATIONS & INCIDENT RESPONSE
Empresas que desenvolvem soluções estruturadas para responder a vazamentos de dados ou ciberataques. A solução visa minimizar os impactos de ataques cibernéticos já realizados, possibilitando um controle da situação com o menor tempo e custo.

IOT SECURITY
Empresas que atuam com segurança relacionada a internet das coisas, aparelhos e networks que estão conectados entre si.

Categorias

IDENTITY & ACCESS MANAGEMENT
Empresas que desenvolvem soluções que garantem a veracidade das informações e identidades de todas as partes envolvidas em um processo. Aqui se encontram empresas de Identidade como Serviço, que capturam, armazenam e asseguram a veracidade do usuário, e companhias de assinatura digital, que trazem inovação e segurança para todo o ciclo de documentos.

BLOCKCHAIN
Blockchain-as-a-Service (BaaS) são empresas que possibilitam o desenvolvimento de produtos digitais com a tecnologia blockchain, instalando, hospedando e/ou mantendo redes desse tipo em nome de outras organizações.

FRAUD & TRANSACTION SECURITY
Empresas que aplicam tecnologias de análise de dados para gerar avaliações e insights sobre clientes, permitindo mapear riscos, analisar a conformidade com leis e regulamentações e se prevenir contra perdas, desvio, fraude e ataques cibernéticos.

SECURITY CONSULTING & SERVICES
Refere-se às startups que prestam serviços para testar e/ou aprimorar serviços de cibersegurança. Um bom exemplo aqui são as empresas que atuam com simulações de ataques cibernéticos (pentest ou teste de intrusão) como forma de identificar possíveis falhas nos sistemas.

GOVERNANCE, RISK AND COMPLIANCE
Soluções GRC (Governança, Risco e Compliance) são compostas por ferramentas que abrangem a gestão de riscos, governança corporativa e práticas de auditoria e controle, com o objetivo de garantir a conformidade com leis, regulamentos, frameworks e padrões de boas práticas.

CLOUD SECURITY
Cloud security refere-se às iniciativas que atuam com políticas, tecnologias, aplicativos e outros mecanismos de controle utilizados para proteger IP virtualizado, dados, aplicativos, serviços e a infraestrutura associada de computação em nuvem.

Agradecimentos

Este report conta com o apoio da:

Cybertech Report