Visão geral sobre Segurança da Informação em Cloud

Bruno Leal
bruno.leal@unesp.br

Vazamentos

A hacker gained access to 100 million Capital One credit card applications and accounts

By Rob McLean, CNN Business

Updated 2117 GMT (0517 HKT) July 30, 2019

Imperva: Data Breach Caused by Cloud Misconfiguration

by Tara Seals

October 11, 2019

Hackers were able to steal an AWS administrative API key housed in a compute instance left exposed to the public internet.

11/22/2019
11:30 AM

DARK Reading

1.2B Records Exposed in Massive Server Leak

A single server leaked 4 terabytes of personal data, including social media profiles, work histories, and home and mobile phone numbers.

Principais Ameaças

42%

Unauthorized access

42%

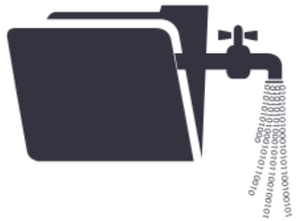
Insecure interfaces/APIs

40%

Misconfiguration of the cloud platform/ wrong setup

Fonte: Check Point Cloud Security Challenges, Solutions, and Trends 2019

Barreiras para adoção de Cloud



29%

Data security, loss & leakage risks

28%

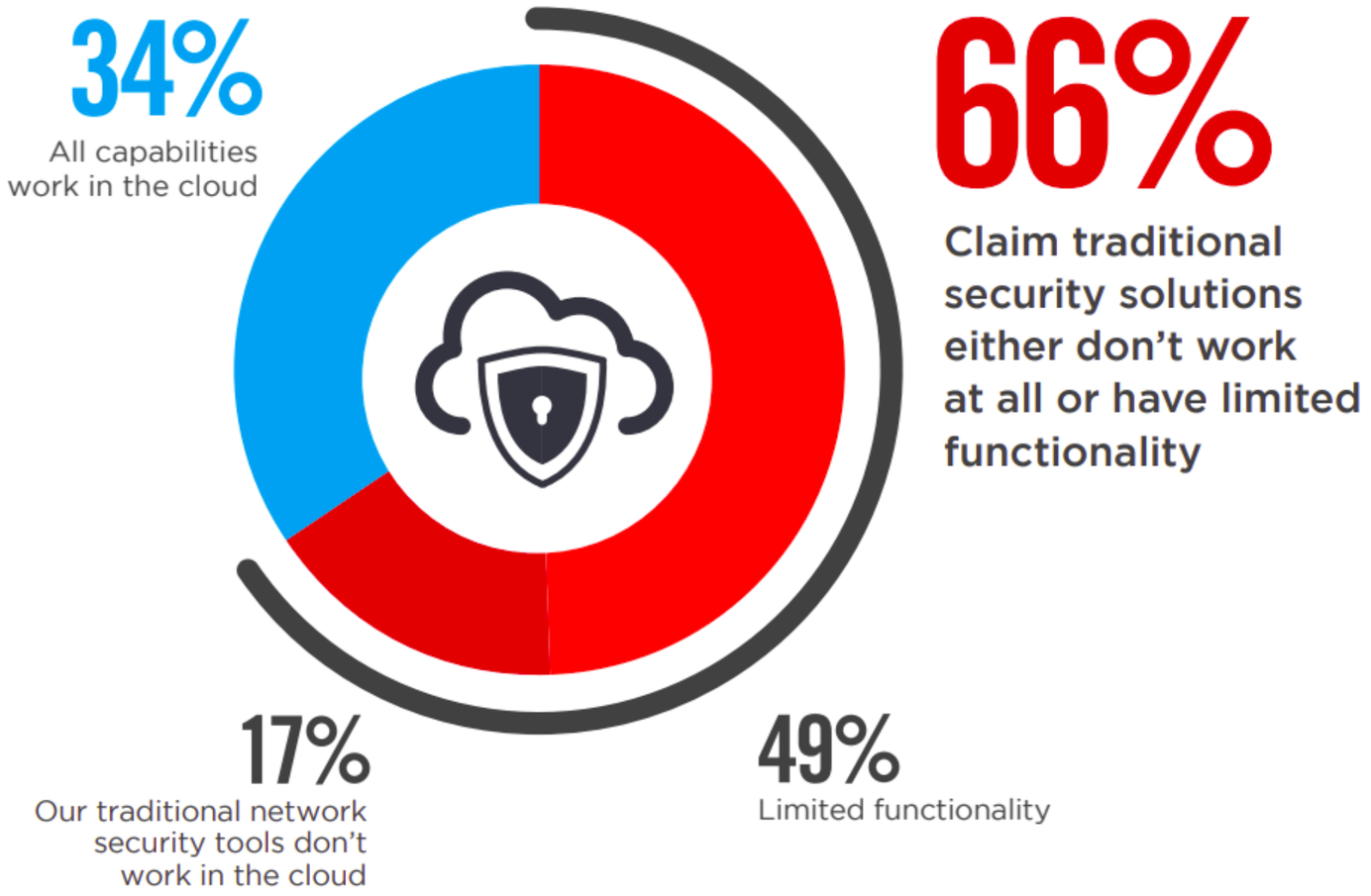
General security risks

26%

Lack of budget

Fonte: Check Point Cloud Security Challenges, Solutions, and Trends 2019

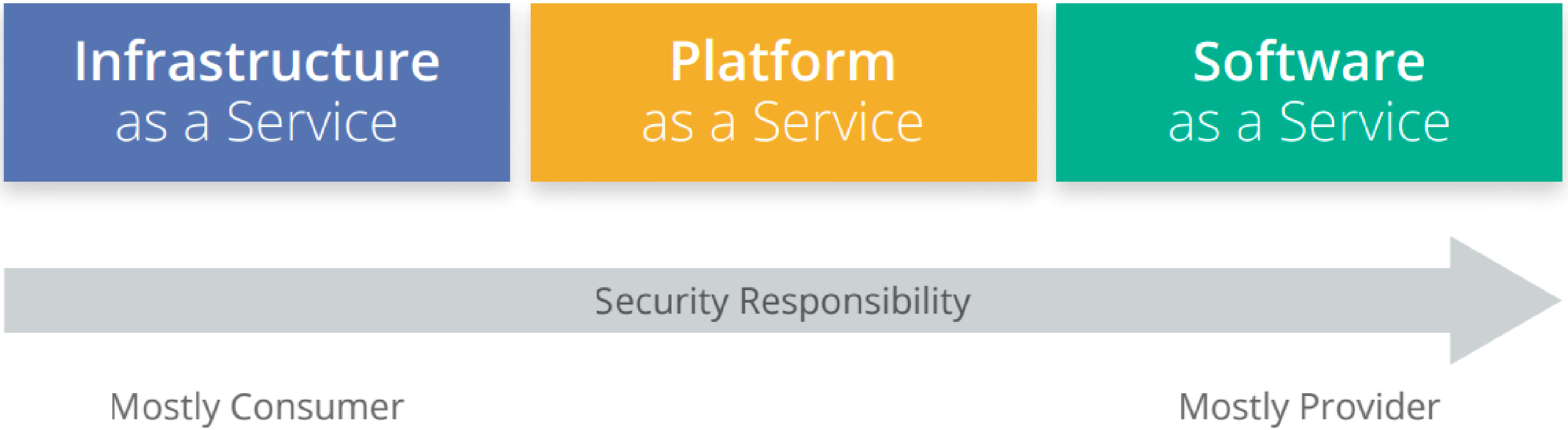
Segurança Tradicional



Fonte: Check Point Cloud Security Challenges, Solutions, and Trends 2019

Segurança em Cloud

- Modelo de Segurança Compartilhada



Software as a Service - SaaS

- Cloud Provider
  - Responsável por quase toda a segurança;
  - Usuário não pode alterar o funcionamento da aplicação;
- Cloud User
  - Controle de acesso por meio da aplicação.

Platform as a Service - PaaS

- Cloud Provider
  - Responsável pela segurança da plataforma;
- Cloud User
  - Responsável por tudo que é implementado;
  - Configuração dos recursos de segurança disponíveis.

Infrastructure as a Service - IaaS

- Cloud Provider
  - Responsável pela segurança da infraestrutura;
- Cloud User
  - Responsável por tudo o que constrói na infraestrutura.

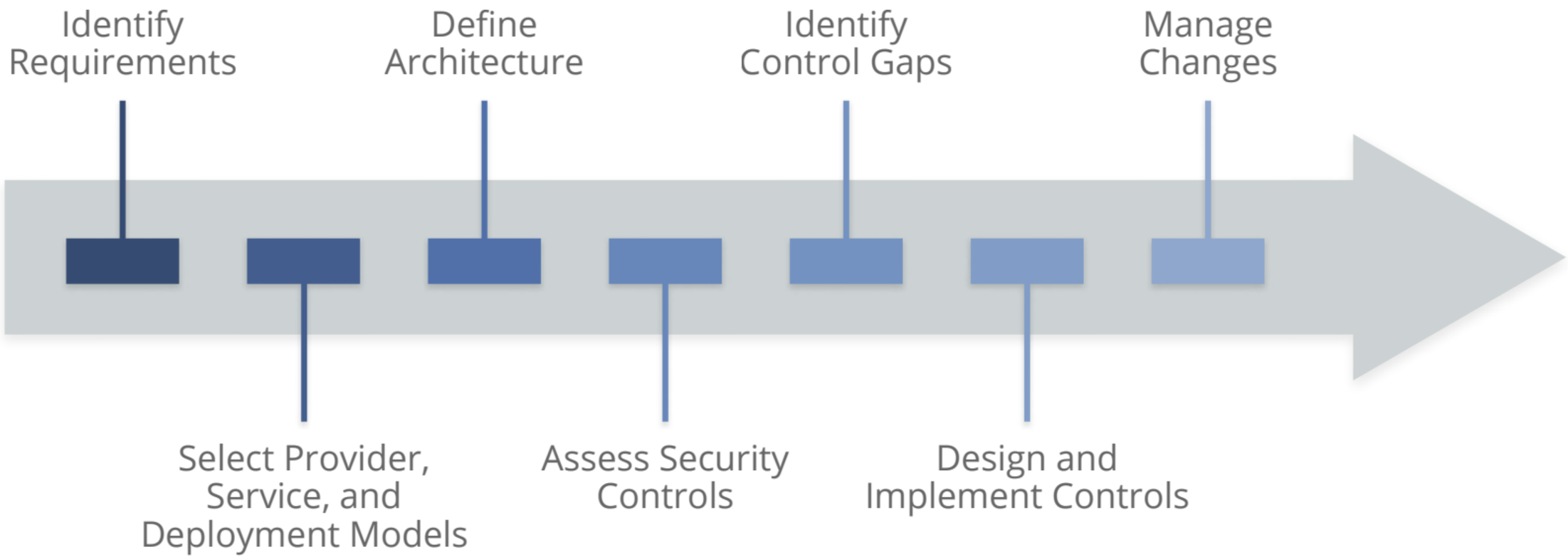
Padrões e Políticas Segurança (1)

- Cloud Security Alliance;

- Devem ser avaliados de acordo com cada projeto
  - Conheça bem o provedor e a arquitetura.

Padrões e Políticas Segurança (2)

- Por onde começar:



Padrões e Políticas Segurança (3)

- Alguns guias:
  - Cloud Controls Matrix v3.0.1
    - https://downloads.cloudsecurityalliance.org/initiatives/ccm/CSA_CCM_v3.0.1-FedRAMP_5.2.15.xlsx
  - Security Guidance v4
    - https://cloudsecurityalliance.org/artifacts/security-guidance-v4/
  - Guidelines on Security and Privacy in Public Cloud Computing
    - https://csrc.nist.gov/publications/detail/sp/800-144/final

Pentest em Cloud

- Os mesmos desafios e ferramentas
  - Scan - nmap;
  - Exploração - metasploit;
  - Pós-exploração - meterpreter;

Pentest em Cloud

- E mais...
  - Scan por buckets vulneravéis - AWSBucketDump;
  - Interação via AWS CLI;
  - Scout Suite;
  - Pacu Framework.

Desafios

- Profissionais para implantar segurança em Cloud;
- DevSecOps;
- Definição de políticas de segurança;
- Validação da segurança;
- Responsabilidade solidária.

Obrigado!
Dúvidas?

Contato

Bruno Leal

bruno.leal@unesp.br

LinkedIn: /in/lealbrunof

Telegram: @lealbrunof

Key ID: FEFB7512