



Check Point[®]
SOFTWARE TECHNOLOGIES LTD

DIAGNÓSTICO DO HOME OFFICE S/A

O impacto deste novo ambiente
“corporativo” interconectado

Claudio Bannwart

Country Manager

CHECK POINT BRASIL

O Coronavírus mudou drasticamente o funcionamento das organizações

01

**FUNCIONÁRIOS
MUDAM PARA
TRABALHO
REMOTO**

02

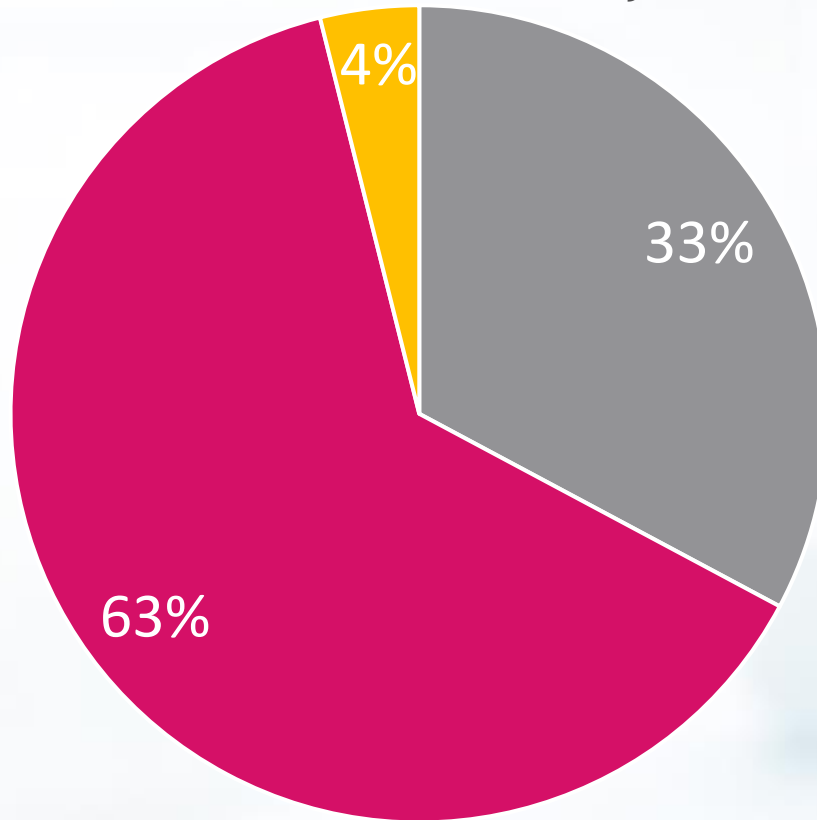
**FOCO EM
“CUSTOMER
CENTRICITY” E
EMPATIA**

03

**TRANSFORMAÇÃO
DIGITAL
ACCELERADA**

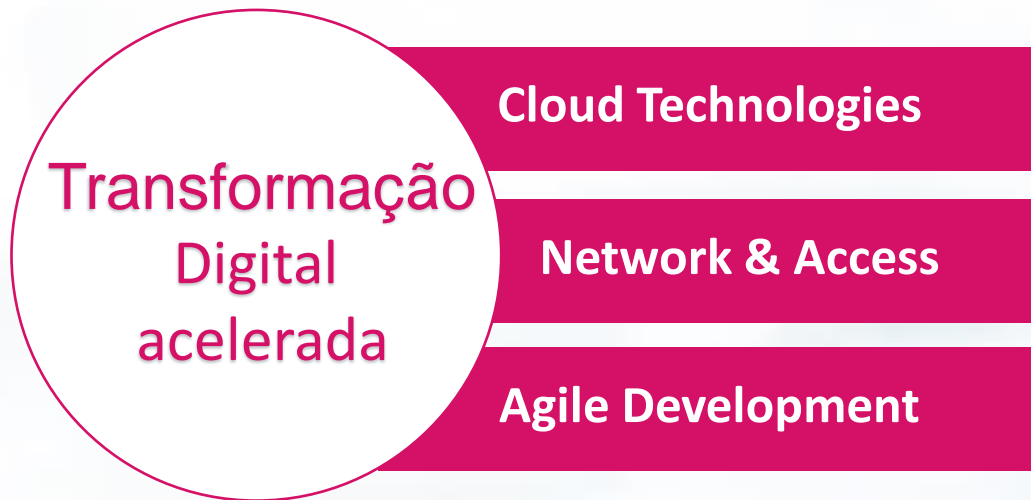
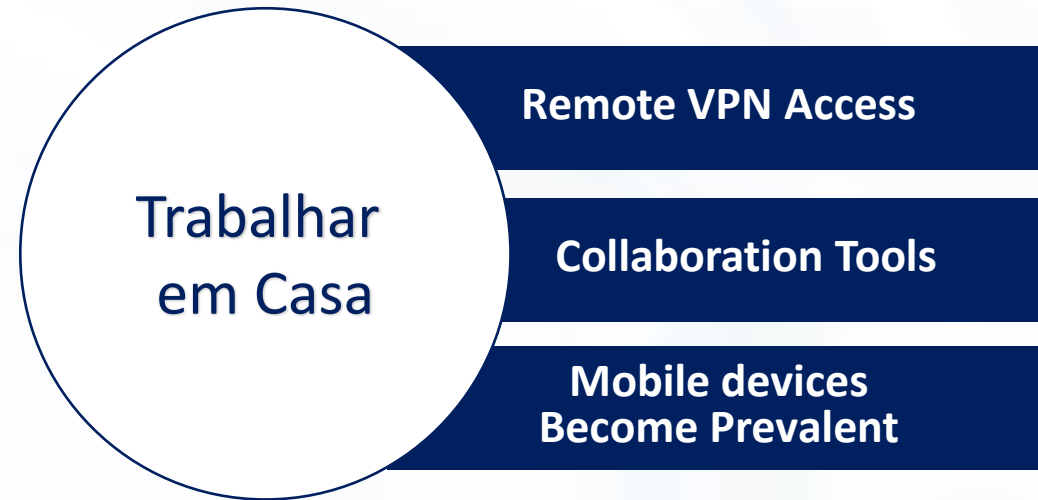
96% acreditam que aspectos do Coronavírus chegaram para ficar

Qual das opções a seguir melhor descreve sua abordagem para avançar na situação atual?



- The impact of coronavirus is permanent and we plan to act accordingly
- We will return to more normal life in the coming months, some aspects of the coronavirus impact will stay
- We believe we will soon return to the pre-coronavirus era with no lasting impact on day to day life

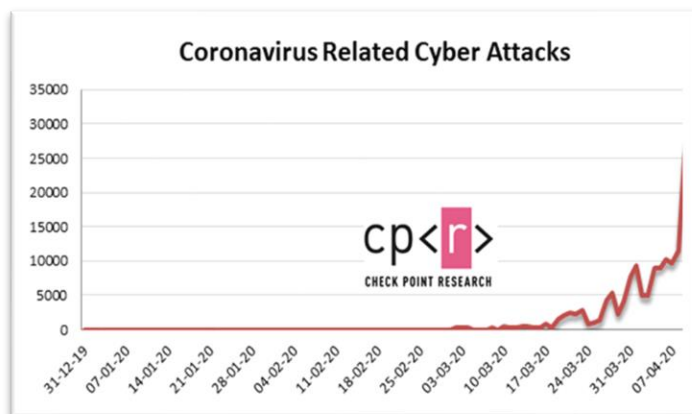
O impacto do Coronavírus nos ambientes de TI



O que resultou em um sério aumento de ciberataques

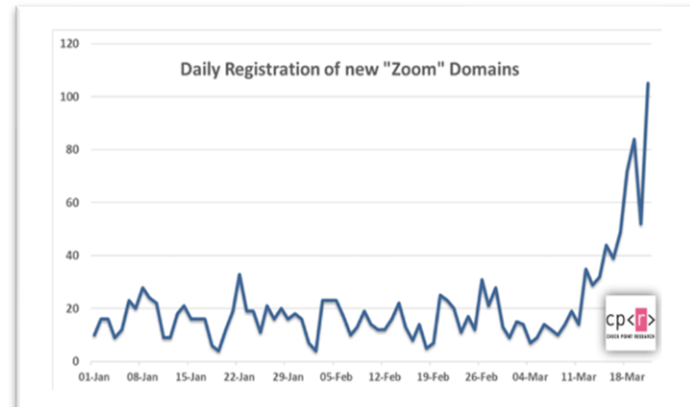
Ascensão Crítica em ciberataques

20.000 ataques diários
94% ataques de phishing



Alvo Domínios ZOOM

6.500 novos domínios
4% suspeitos



Apps Móveis Disfarçados

16 apps maliciosos
Disseminação Malware



Perguntamos aos 271 profissionais de segurança de TI...

Quais foram os **EFEITOS MAIS IMPORTANTES** na segurança de TI?

O que melhor funcionou para eles ao **APLICAR O NOVO NORMAL?**

Quais são as principais **PREOCUPAÇÕES ATUALMENTE?**

Como eles acreditam que o futuro cibernético se parecerá e quais são suas **PRINCIPAIS PREOCUPAÇÕES DAQUI PARA FRENTE?**

Quais são seus principais **PROJETOS FUTUROS DE CIBER-SEGURANÇA?**

148 Clientes, prospects e parceiros (25 deles são C-Level), 123 funcionários de vendas (em contato com os clientes)

Desafio imediato dos profissionais de segurança de TI: cuidar da conectividade e do acesso remoto em grande escala

Quais foram os efeitos mais importantes da pandemia do Coronavírus em seus ativos de TI?

The need to move to remote workforce

86%

Acceleration of digital technology projects

34%

Shift to Customer empathy at scale
(connectivity, interaction, experience,
support)

32%

Rapid adoption of cloud technologies

24%

Zoom Meeting

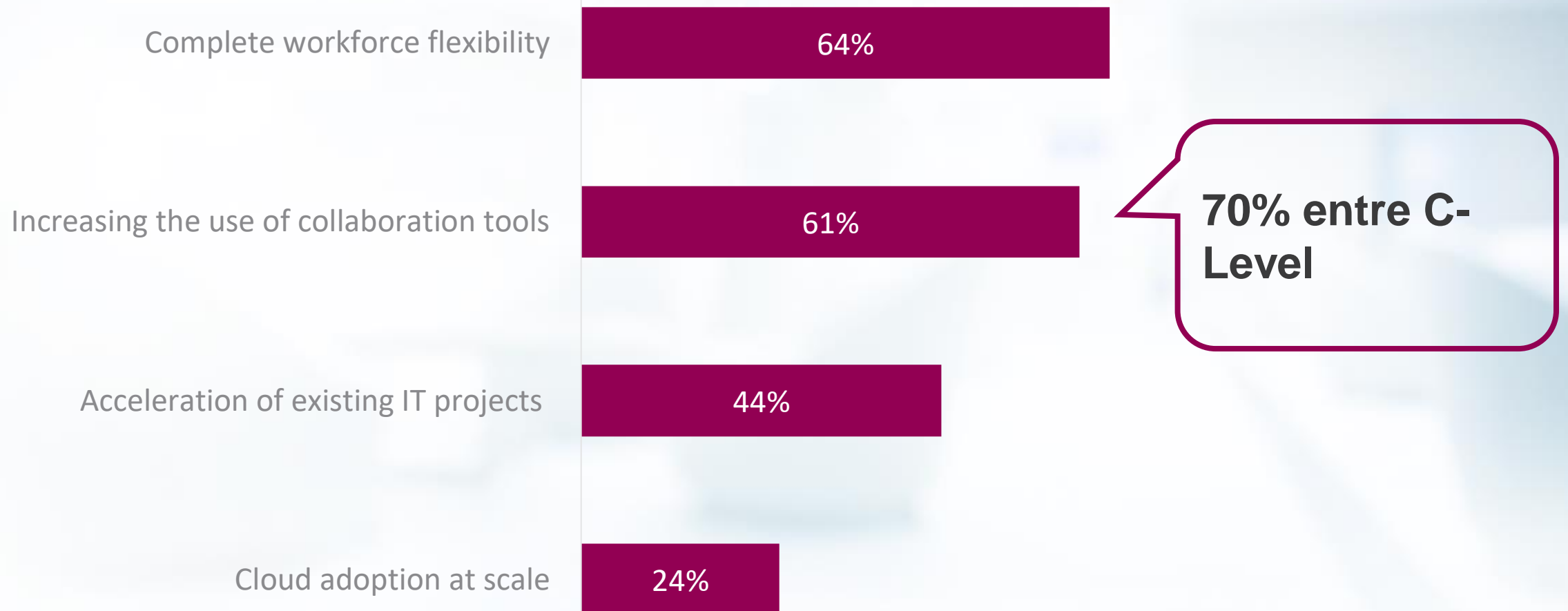
Audio only

With video



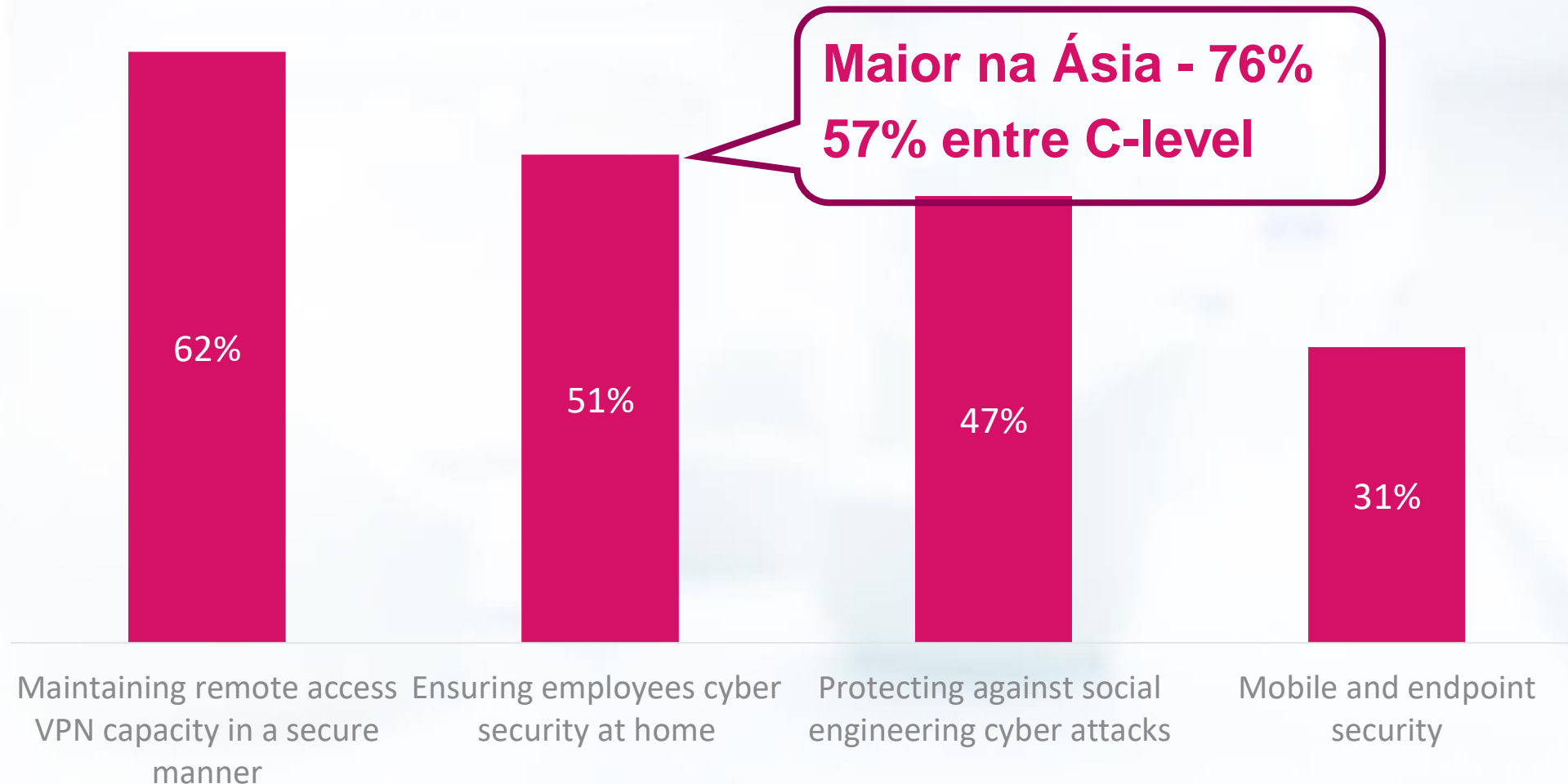
Flexibilidade e colaboração da força de trabalho percebida como base para a continuidade dos negócios

O que funcionou melhor durante o surto para alcançar a continuidade dos negócios?



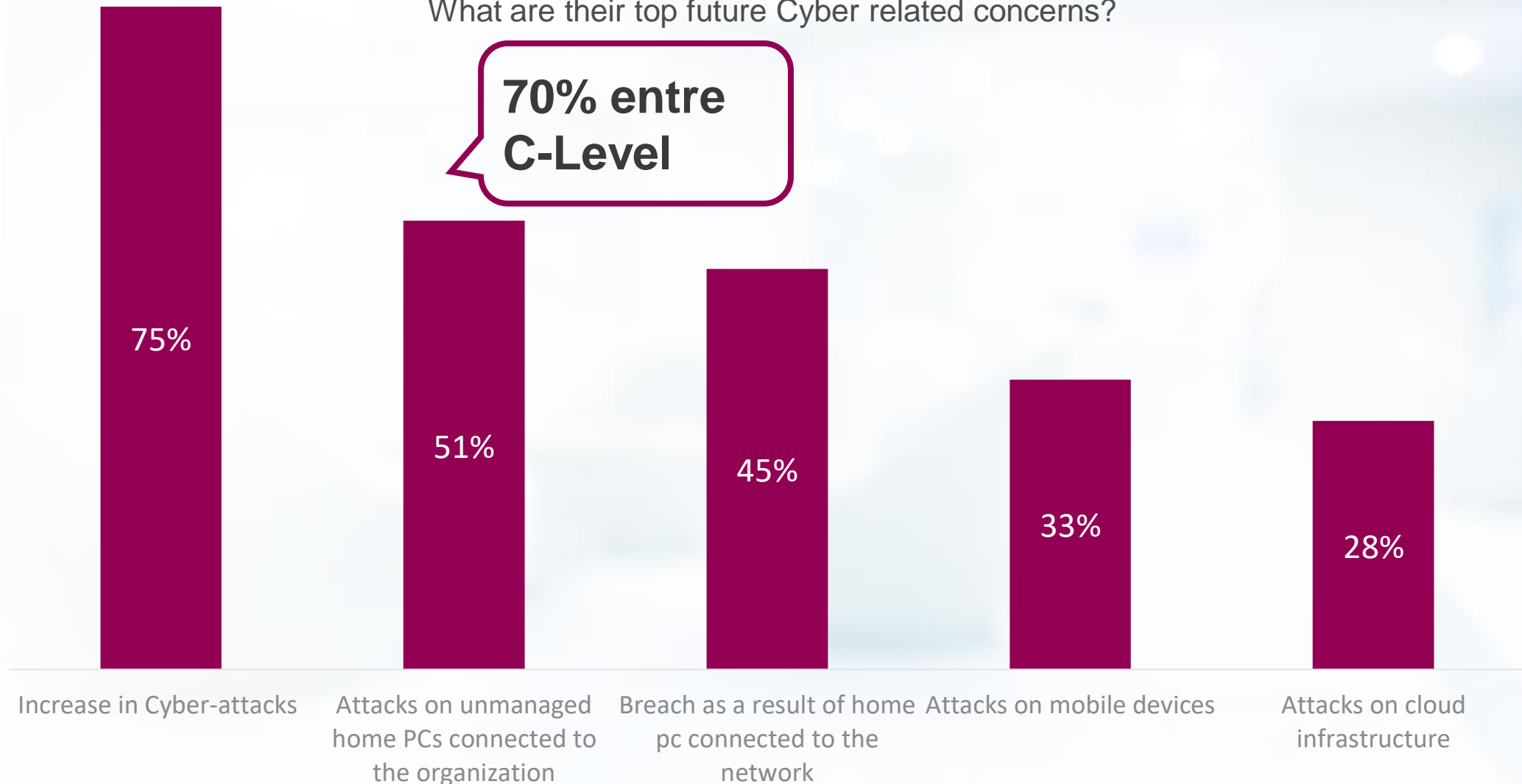
Profissionais estão mais preocupados em **proteger a força de trabalho remota** (incluindo o elemento humano)

Quais são as suas principais preocupações de segurança relacionadas ao Coronavírus?



Maior preocupação com o aumento de ciberataques no futuro

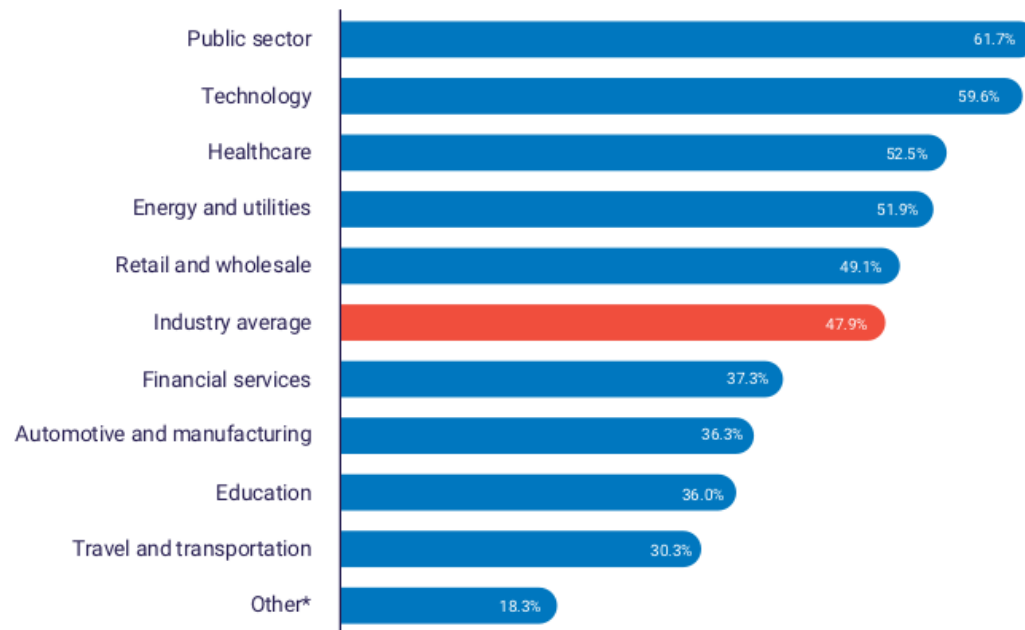
What are their top future Cyber related concerns?



Infraestrutura Obsoleta

Em 2017, 13,1% dos ativos de rede eram antiquados ou obsoletos; no ano passado, esse total alcançou 47,9%. Os dados da pesquisa indicam que dispositivos obsoletos têm, em média, 42,2 vulnerabilidades por equipamento, enquanto os antiquados têm 26,8 e os novos 19,4.

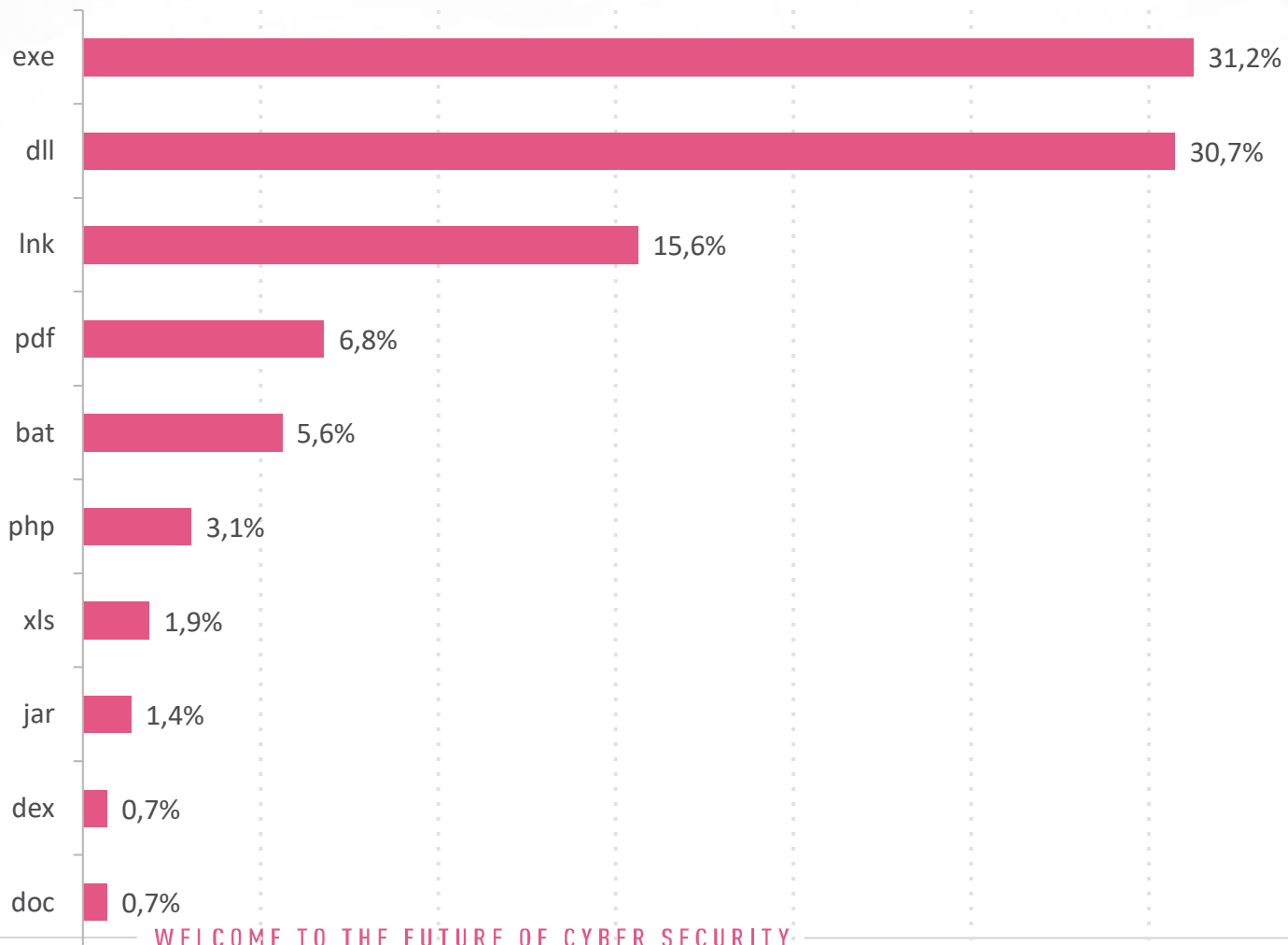
Ageing and obsolete devices – ranked by industry



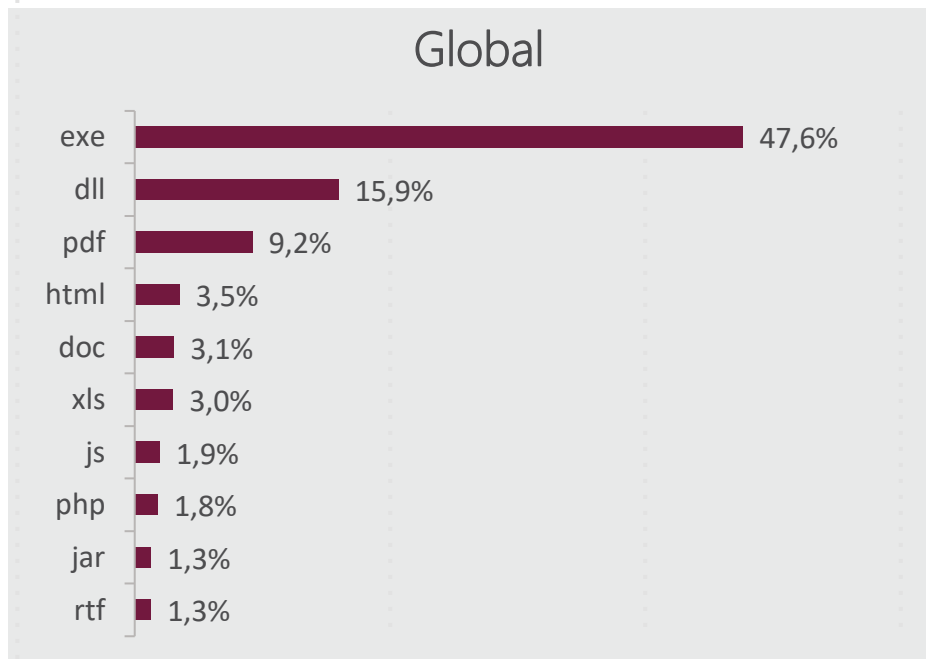
Source: 2020 Global Network Insights', da NTT

Top Malicious File Types, Web- Last 30 Days

Brazil

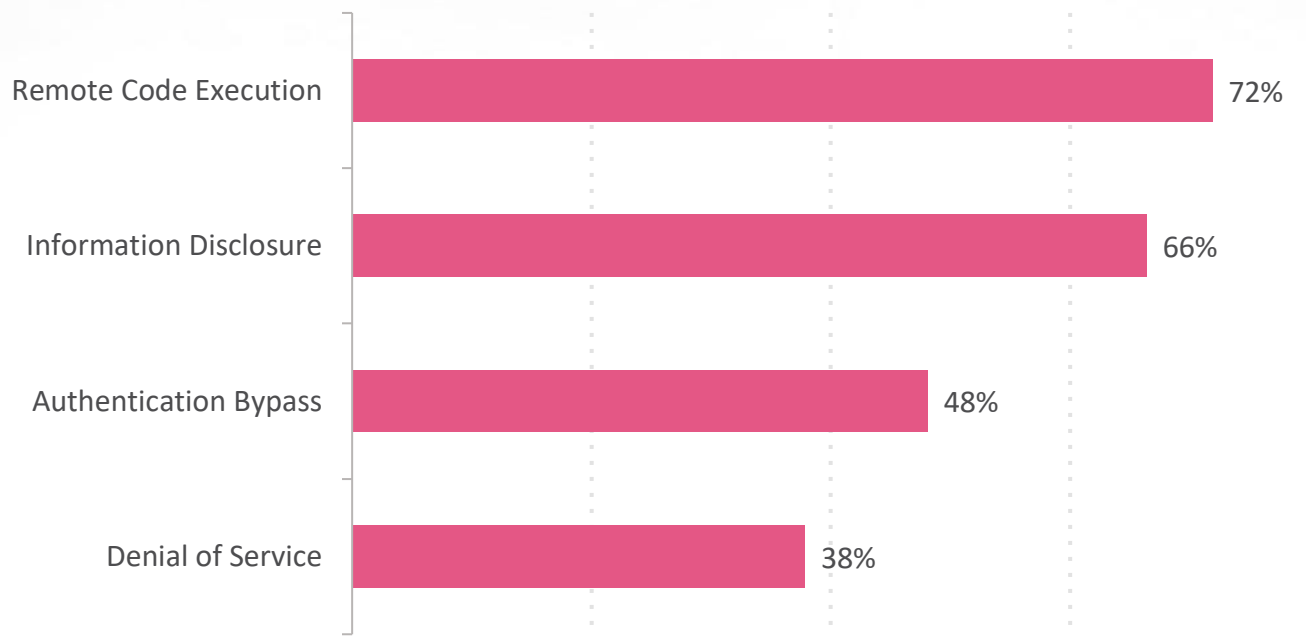


Global

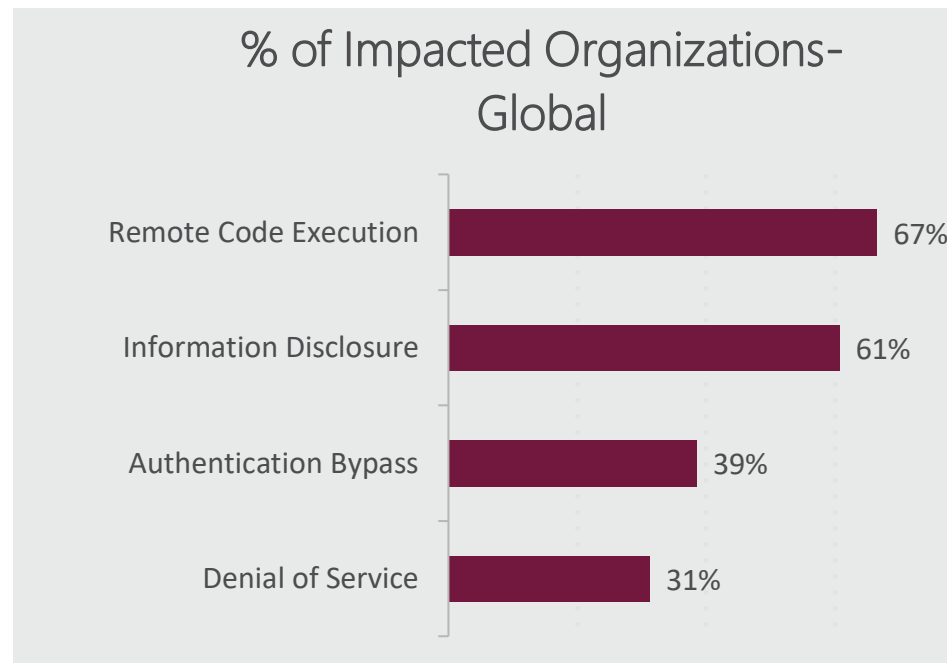


Top Vulnerability Exploit types - Last 30 Days

% of Impacted Organizations- Brazil



% of Impacted Organizations- Global



A pandemia desaparecerá / O efeito cibernético ficará



A pandemia desaparecerá. O efeito cibernético ficará.

O que as empresas devem focar para a segurança do novo normal



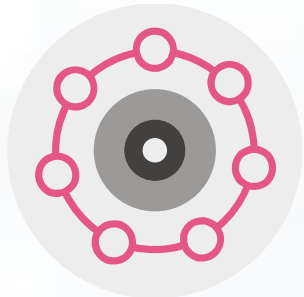
PREVENÇÃO EM TEMPO REAL

Prevenir é o melhor que tratamento



PROTEJA TUDO

Mobile, Endpoint, IoT, Cloud



CONSOLIDAÇÃO E VISIBILIDADE

Eliminar pontos cego de infecção



SWIFT e AGILE

Proteção com um clique de um botão

Como permanecer seguro?

Change	Effect	Risk	Top Process/Technologies to mitigate (partial list)
Working from home	Personal mobile and computers provided access to corporate networks	Data breach (e.g. key logger, screen logger on pc/mobile)	<ol style="list-style-type: none"> 1. Implementation of endpoint security and hygiene with compliance check (latest patches, AV...) 2. User training awareness (e.g. phishing simulation) 3. Mobile threat defense on mobile
Rapid move to cloud	Speed of deployment on the expense of security	Basic security controls can lead to data loss and manipulation	<ol style="list-style-type: none"> 1. Invest in Cloud Security posture management 2. Deploy workload security for containers and serverless apps. 3. Real time prevention of threats with IaaS security
Critical infrastructure	Allowing critical infrastructure remote access	Critical infrastructure breach	<ol style="list-style-type: none"> 1. IoT security for IoT devices 2. bolster network security posture with red team ... 3. OT security with Scada enforcement
Increased network capacity	More throughput is needed to address data in motion	Lack of service Network is down	<ol style="list-style-type: none"> 1. Invest in network security that scales according to needs 2. All protections must be enabled while keeping business continuity 3. Scalable secure remote access

1

Há uma nova arquitetura de TI que deve ser protegida.

2

A pandemia desaparecerá. O efeito cibernético ficará.

3

**Agora seus dados estão em todo o lugar.
E sua cibersegurança?**

4

Seu mundo mudou. Proteja-o.

5

Treinar/Educar o funcionário/usuário.

6

Foco na informação que transita de maneira diferente, rápida e por muitos dispositivos móveis e de IoT.

7

Múltiplos vetores de ataque a partir do home office.

8

Nuvem onipresente: aceleração dos negócios, processo de transformação digital, configuração e segurança.



Check Point[®]
SOFTWARE TECHNOLOGIES LTD

PERGUNTAS / RESPOSTAS

OBRIGADO!