As mudanças nas ameaças e a segurança de dados

Bem Vindos!

- Use o chat para perguntas (Preciso de perguntas)
- Qualquer duvida não hesite em perguntar!
- Por favor nos avise se tiver qualquer problemas de áudio / vídeo

Rodrigo Gazola

rodrigo.gazola@addee.com.br

I am a MSP

♥ BACKUP

linkedin.com/in/rodrigogazola

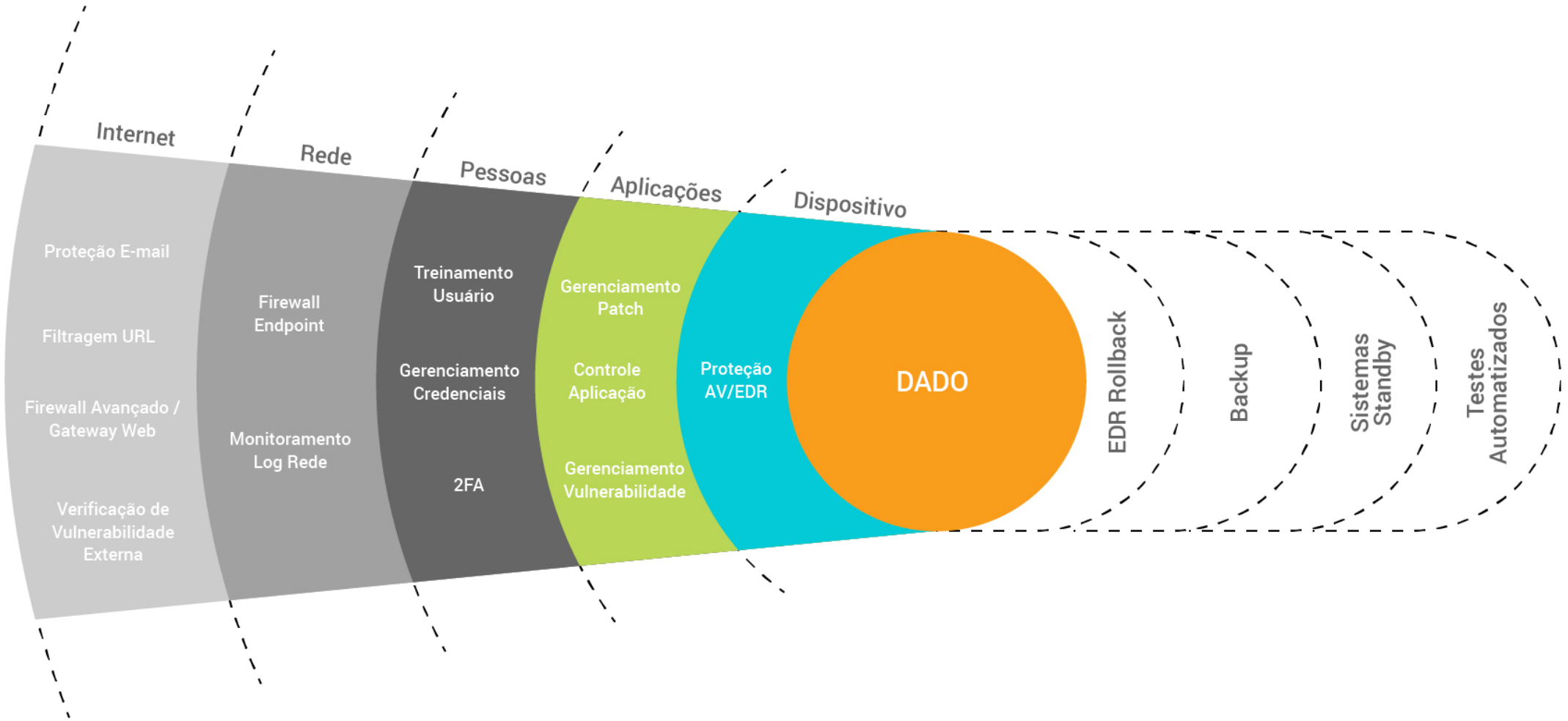
Cristiano Fermo

cristiano@clsinfo.com.br

Diretor

https://www.linkedin.com/in/cristiano-fermo-3b613441/

Prevenção < DADOS > Recuperação



Credenciais

Backup

Prevenção

Recuperação

Gerenciamento de Patch

EDR

Usuário

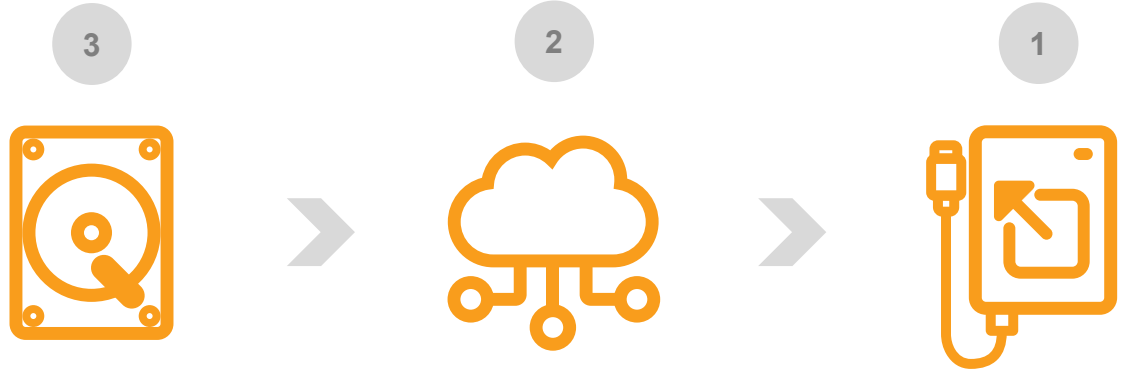
Politica de segurança SEM treinamento de usuário não faz sentido

Backup – # 1 > Recuperação

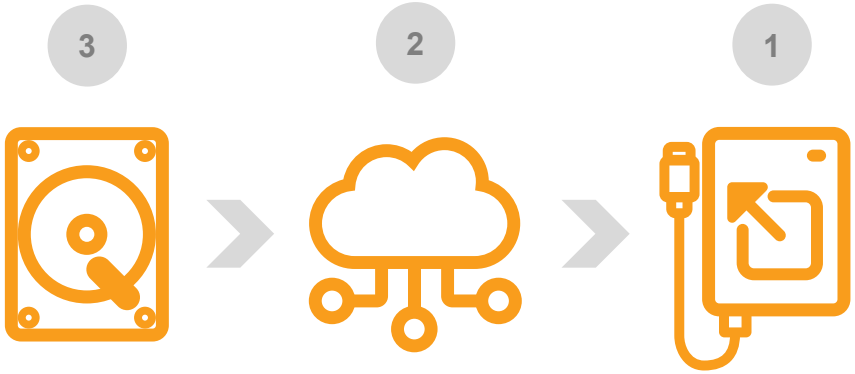
BACKUP

ADDEE+

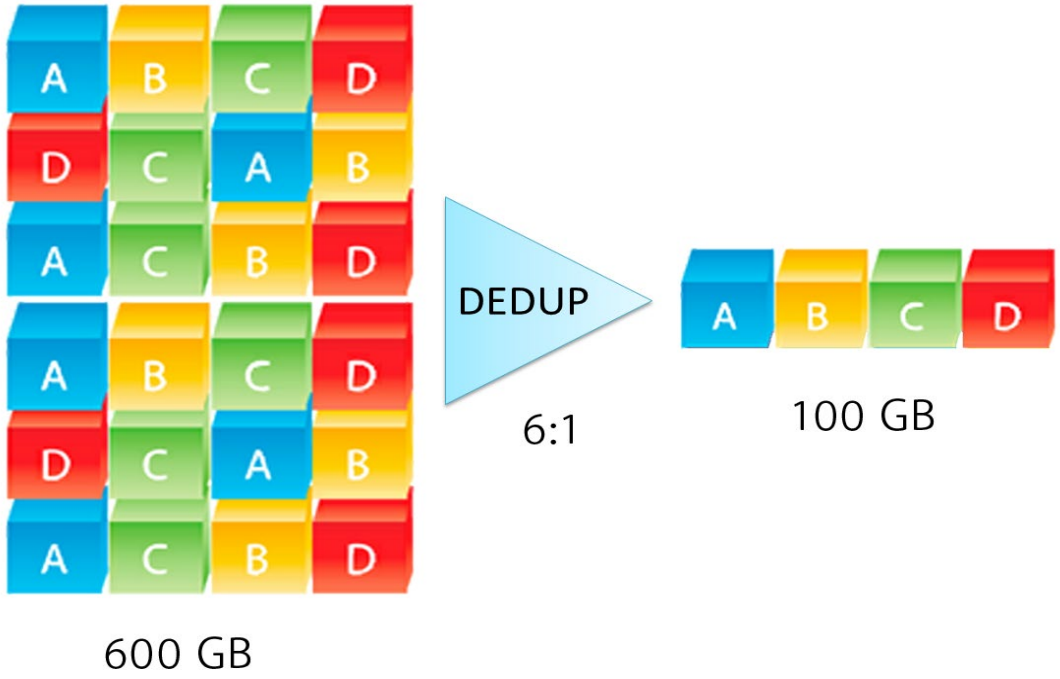
Backup é tudo igual ?



3x2x1 x (0)



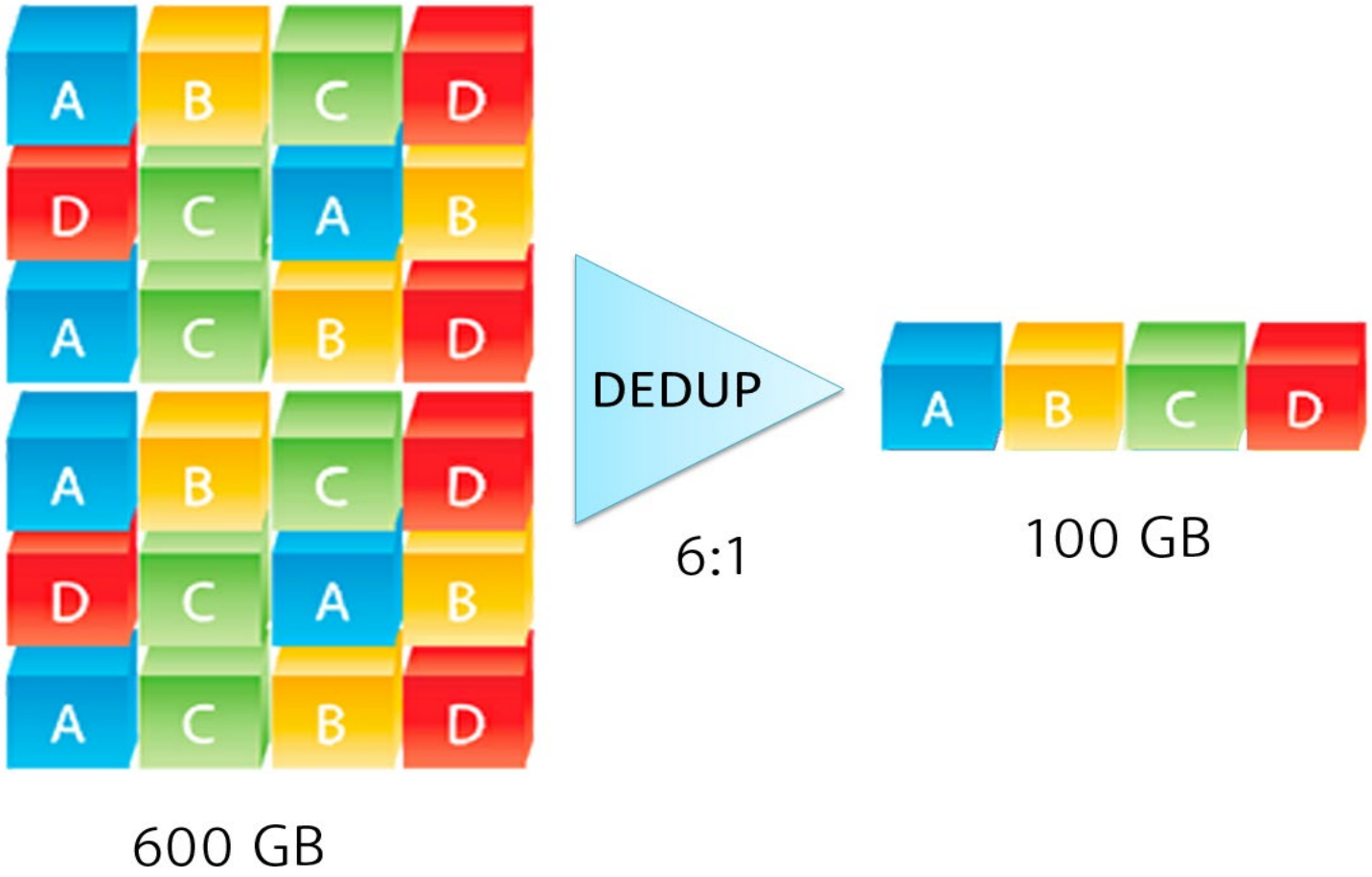
Desduplicação



Conceito 3x2x1 (0)

3 = Cópias de Dados **2** = Locais Diferentes **1** = Off Site

Desduplicação Dados

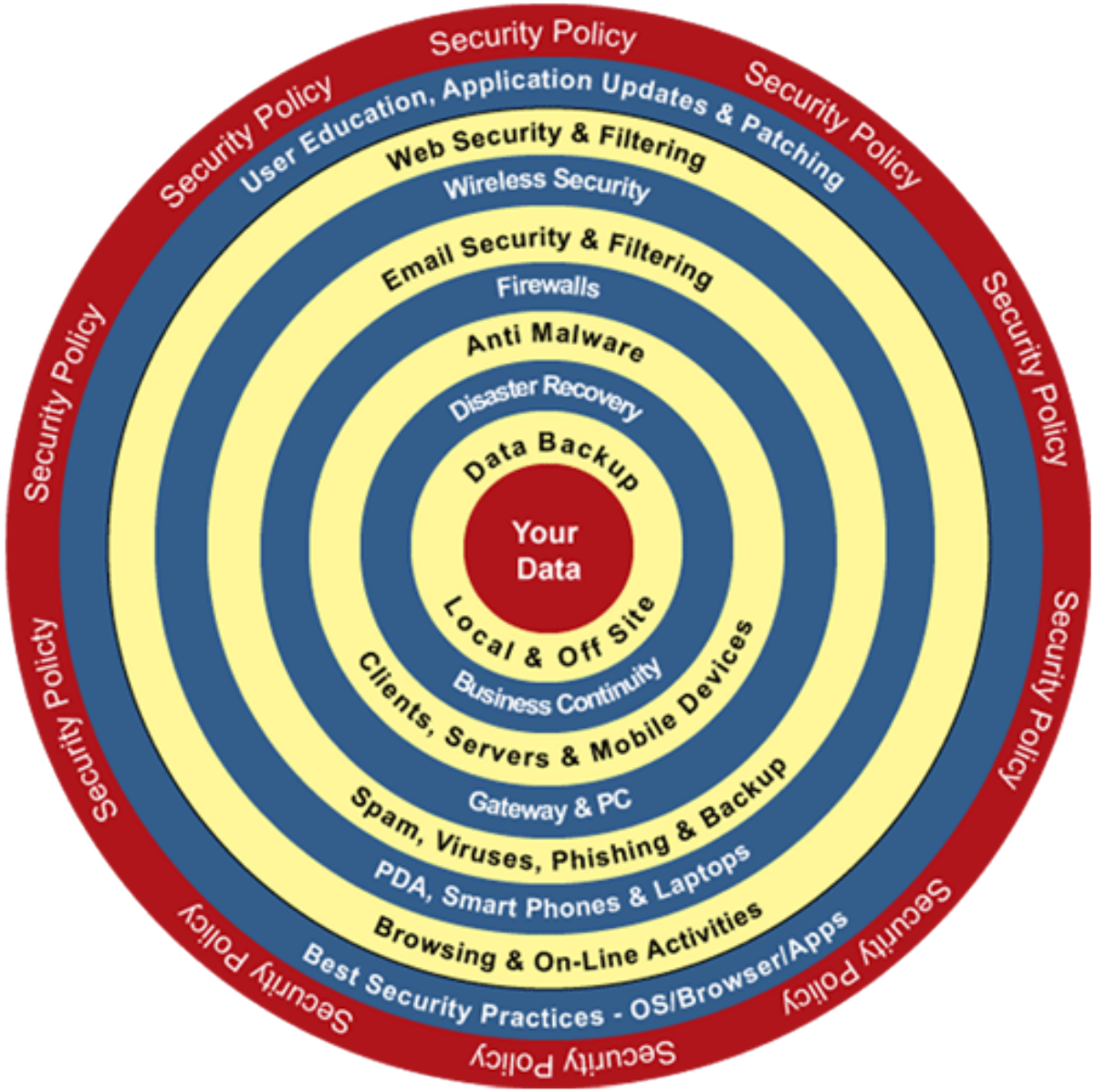


Vídeo
BACKUP x DESDUPLICAÇÃO
na pratica

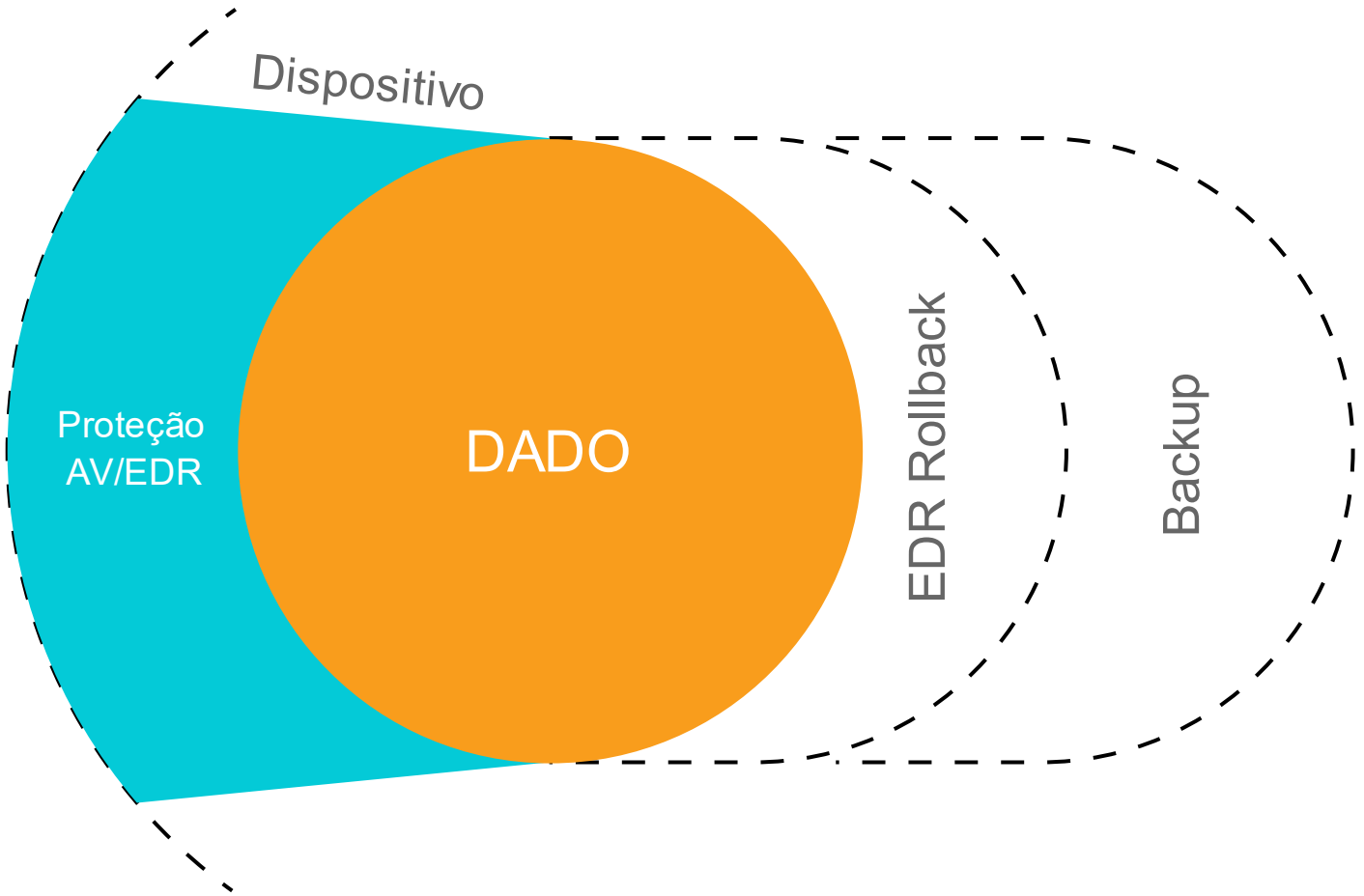
Vídeo
Restauração x DESDUPLICAÇÃO

EDR – # 2 > Recuperação

Camadas Segurança



Primeira Camada da Recuperação



Proteção ao longo do tempo

Ciclo de vida da ameaça

Proteção Avançada

- Isolamento Network – Execução
- File System > Rollback - Pós
- Registry rollback - Pós
- Histórico Ataques - Pós

Novas AMEAÇAS x AV

A evolução do malware

- AV é baseado em assinatura
- Os novos malware sabem como evitar / não ser detectado pelo AV
- As ameaças evoluem rapidamente

ADDEE+

Ameaças que “escapam” do AV

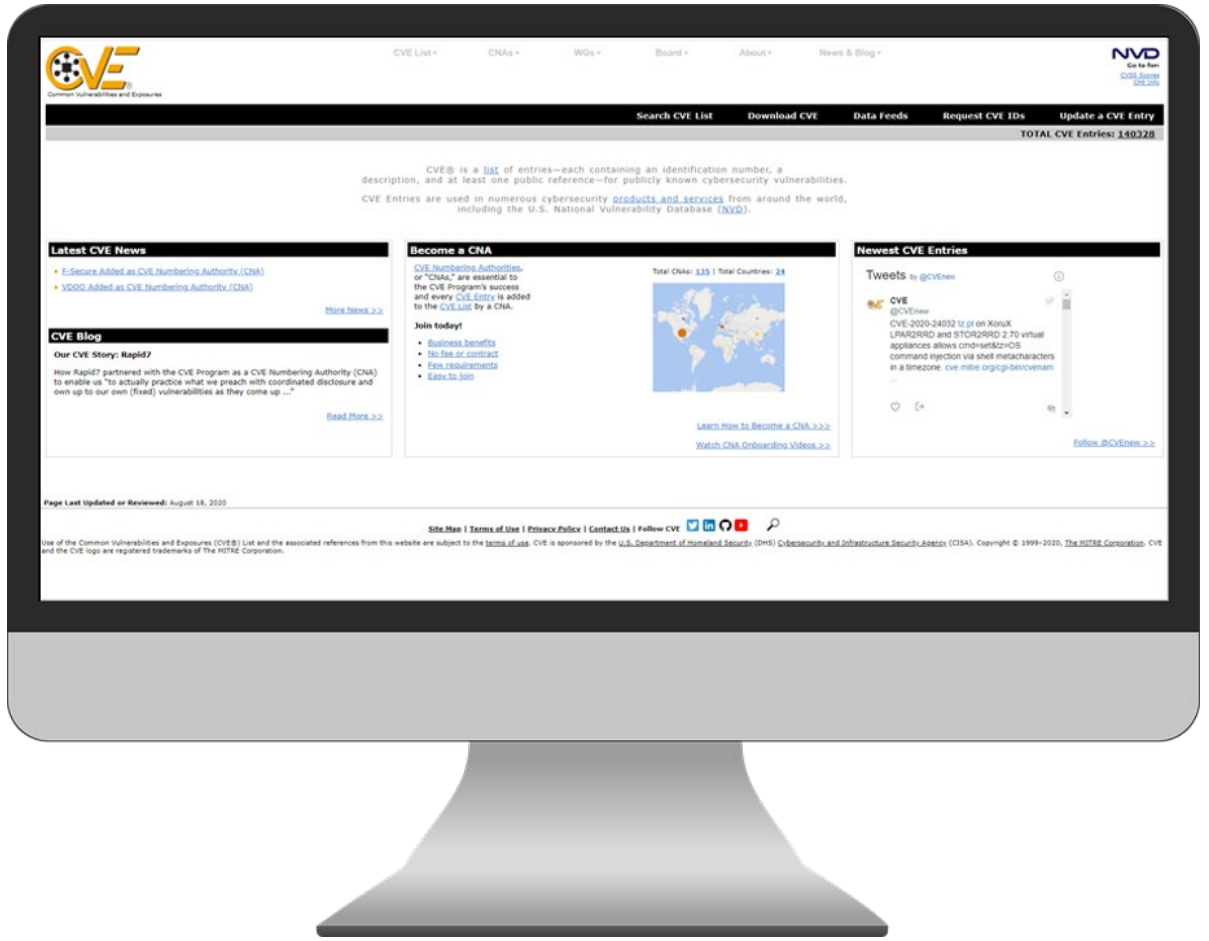
- Polimórfico
- Documentos Armados
- Download Induzido
- Ataque sem Arquivo
- Malware Ofuscado

E-book

5 Ameaças cibernéticas que escapam do AV

https://materiais.addee.com.br/cinco-ameacas-ciberneticas

Proteção Avançada



Proteção Avançada

O que o EDR tem a ver com as CVE

Proteção Avançada

Características EDR

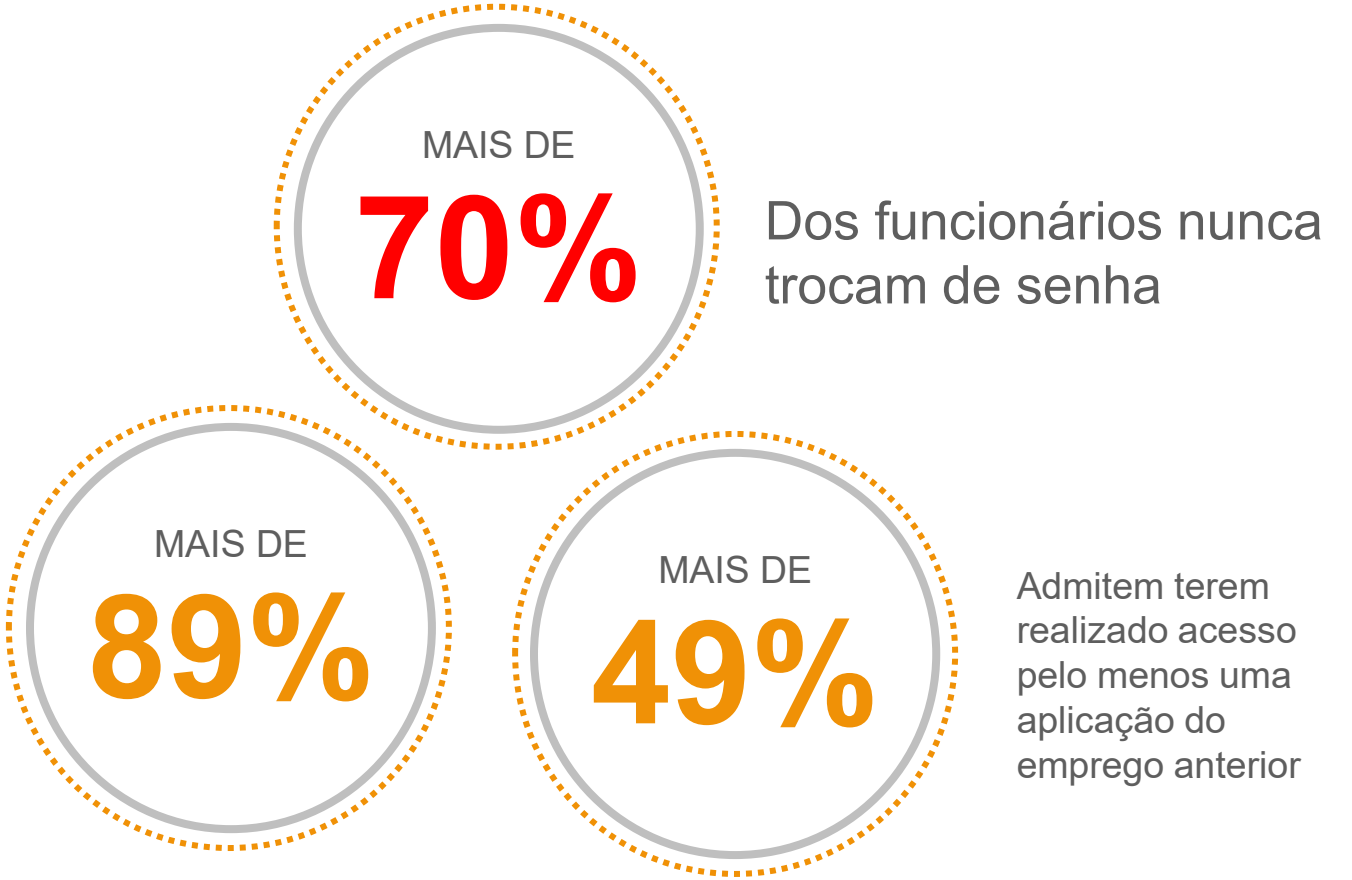
- Interface Rede
- Rollback
- **Agente**

Vídeo
EDR ROLL BACKUP

Credenciais – # 1 > Prevenção

Gerenciamento Credenciais

O gerenciamento precário de senhas pode criar um risco significativo para os negócios, especialmente quando funcionários saem da empresa.



https://enterprise.verizon.com/resources/reports/dbir/

Quais as recomendações?

1

Siga o princípio do menor privilégio possível

2

Revogue acesso e realize auditoria em uso de credenciais após um desligamento

3

Crie uma rotatividade periódica de senhas

4

Automatize o gerenciamento de senhas e documentação

E-book

https://materiais.addee.com.br/melhor-defesa-contra-cibercrime

Esta é a sua senha?

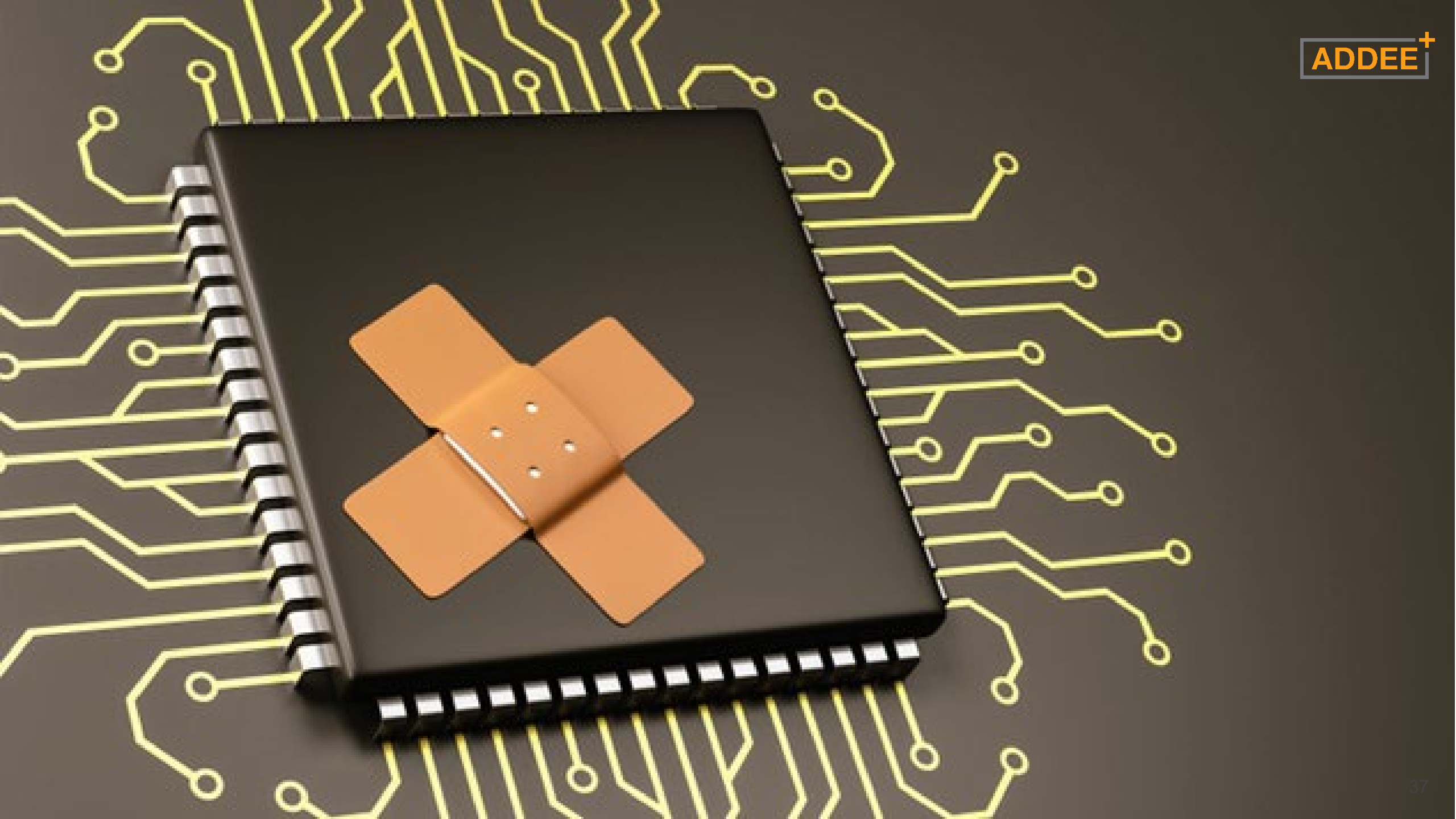
- 123456
- 123456789
- qwerty
- Senha
- 111111
- 12345678
- Abc123
- 123456
- Password1
- 12354
- 1234567890
- 123123
- 000000
- iloveyou
- 1234
- 1q2w3e4r5t
- qwertyuiop
- 123
- monkey
- dragon


Password
IXIFTY
Sign In
Username
Password
Login

Patch – # 2 > Prevenção

ADDEE+

PATCHES


ADDEE+

Práticas Recomendadas - Patch

1. Avalie seu “portifólio”
2. Priorize as atualizações
3. Cubra Tudo
4. Formalize / Crie um processo recorrente

Q&A

Perguntas e Respostas

OBRIGADO