

Ransomware: O backup seguro é a sua última linha de defesa



Everton Cardoso
Systems Engineer

O ransomware democratizou o roubo de dados



- Nunca vai acontecer comigo
- Meus dados não são valiosos
- Sou pequeno demais para ser atacado
- Nossa segurança é boa o suficiente
- Eu tenho seguro virtual

Você acha que suas chances são boas?

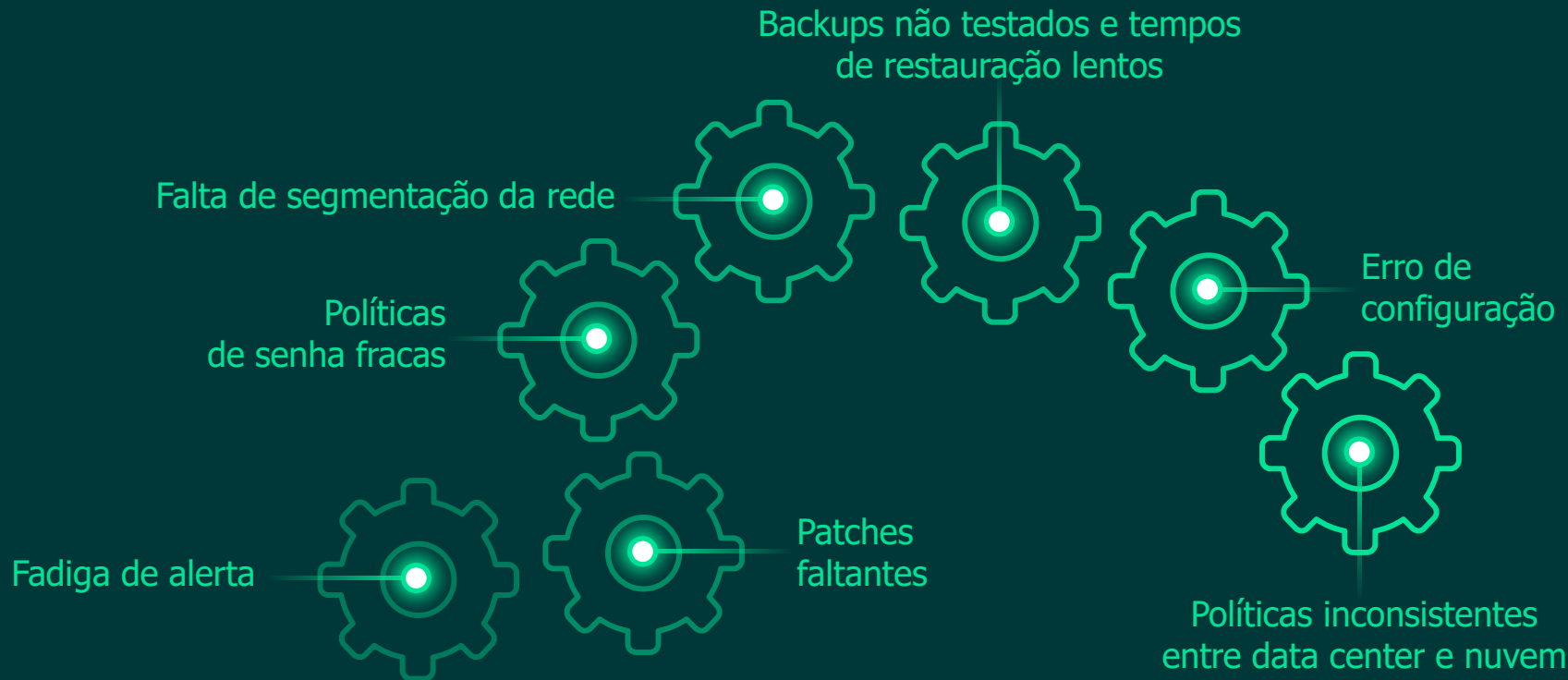
Agentes maliciosos podem fazer **infinitas** tentativas para entrar e só precisam acertar uma vez

Os defensores têm **UMA** chance de bloquear ataques e precisam estar certos 100% do tempo



Por que o ransomware é eficaz?

Pessoas, processos, tecnologia



Falta de preparação = \$\$

- Resgate pago em média: **US\$ 170 mil**
- Perda de dados em média: **35%**
- Custo total do ataque: **US\$ 1,85 milhão**

Extorsão em alta, de **3%** em 2020
para **7%** em 2021



<https://news.sophos.com/en-us/2021/04/27/the-state-of-ransomware-2021/>

O ransomware
é um **desastre**



Ransomware: a solução deve...



- Ser **flexível** para atender aos seus requisitos
- Fornecer **visibilidade**, porque não é possível proteger o que não se pode ver
- Permitir **testes e verificação** para que seus dados estejam lá quando você precisar
- Ser criada para **recuperação rápida e confiável**, porque a recuperação deve ser sempre melhor do que o resgate

Flexibilidade oferece operações mais fáceis

A Veeam é definida por software e agnóstica em relação ao storage:

- 1 Implantação: Escolha o servidor, o storage e a nuvem mais adequados para seu negócio
- 2 Reduza custos: Escale os componentes de forma independente
- 3 Prepare para o futuro: Evite ficar preso ao fornecedor e evolua para enfrentar ameaças futuras



Imutabilidade confiável



Scale-out Backup
Repository

Veeam
READY

Repository

Veeam
READY

Object

Veeam
READY

Object with
Immutability

Performance Tier



DAS




NAS



Appliance
de deduplicação



Repositório
fortalecido

Imutabilidade 
do começo ao fim

- Baseada em políticas
- Transparente
- Eficiência de espaço;
- Autossuficiente
- Sem custos adicionais

Capacity Tier



Compatível com S3



Storage de
Objeto IBM



Google
Cloud Platform



Amazon S3



Armazenamento
de Blob do
Microsoft Azure



Amazon S3
Glacier



Armazenamento
de Blob do
Microsoft Azure

Melhores práticas para proteção contra ransomware



Três cópias
diferentes
de dados



Duas mídias
diferentes



Uma cópia
externa

veeAM



Uma delas:
isolada ou
imutável e off-line



Sem erros após
o teste automatizado
de backup e verificação
de recuperabilidade

Detecte problemas com a verificação de backups

Para se recuperar do ransomware, seus ativos devem ser **PROTEGIDOS**

- Garanta que todos os ativos estejam protegidos com relatórios automatizados
- Certifique-se de que as tarefas de proteção estão sendo executadas e concluídas
- Receba alertas e aja automaticamente quando problemas forem detectados



Detecte sinais de ransomware

Procure os sinais e seja alertado automaticamente

Alarmes prontos

- Alarme de possível atividade de ransomware
- Alarme de tamanho suspeito de backup incremental

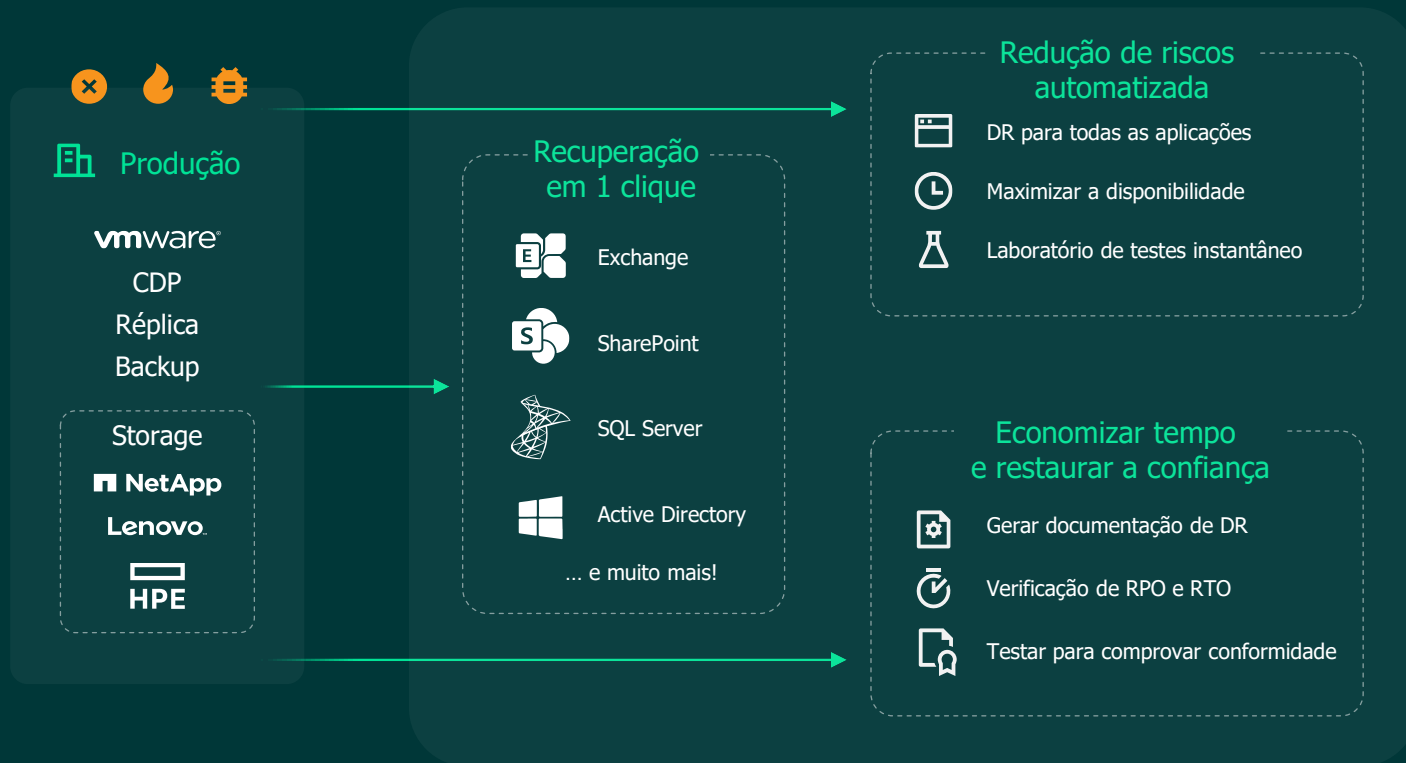
Use outros recursos de monitoramento para:

- Monitoramento de desempenho da rede
- Criação de alarmes com base em métricas de desempenho específicas
- Encontrar máquinas virtuais (VMs) desprotegidas



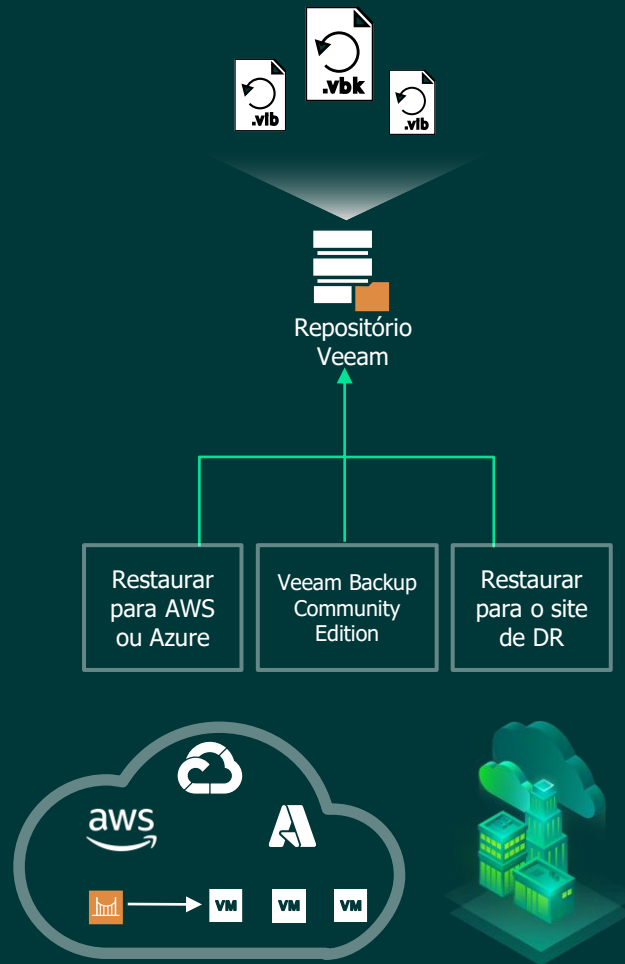
Reduzir o risco com testes e verificação

Prove que está pronto para os desastres



Mobilidade de dados

- ✓ Fazer backup, recuperar, migrar para, de ou dentro de qualquer ambiente, com um formato de dados realmente portátil
- ✓ Modernizar o storage, movendo os dados para fornecer o nível certo de disponibilidade com o menor custo
- ✓ Liberar a movimentação de dados para onde você precisa deles, sempre que forem necessários, entre nuvens e sem cobranças
- ✓ Manter a continuidade dos negócios, não importa onde os seus dados fiquem armazenados



Recuperação instantânea em escala

General options

File-level recovery (Windows)	V2V conversion to vSphere/Hyper-V	Full VM restore	VM files restore	Multi-VM Instant Recovery	VM hard disk restore
Failover to a replica VM	File-level recovery (Multi-OS)	Quick Rollback	U-AIR restore	Restore from a replica VM	Replicate VM from a backup
		Instant VM disk recovery	Staged Restore	Secure Restore	Data Integration API
				Instant first-class disk recovery	Instant DB recovery

Veeam Explorers

Active Directory	Exchange	Teams
Export container/object	Restore system objects/GPO	Save data
Restore a deleted container/object	Restore a changed container/object	Send data
	Restore folder/item/mailbox	Save file/as ZIP
	Export to PST file	Send post/file
		Restore team/channel/tab/post/file
		Export post
SharePoint	OneDrive	Oracle
Save library/document	Send library/document	Save folder/document
Restore library/list/document/site	Export library	Send document
	Restore folder/document	Restore the latest state
	Copy data to same/different user	Restore to a specific point in time
		Restore to a specific transaction
		Restore from Oracle RMAN backup
		Restore from Oracle RMAN backup
SQL		
Restore the latest point	Restore to specific time/transaction	Restore/export DB schema
	Restore/export DB schema	Export latest or point-in-time state
		Publish latest or point-in-time state
		Export as MDF/BAK

Agents

Agent Backup to a Hyper-V VM	Guest OS files/folders/volumes	Agent Linux	Agent Windows
Agent Mac	Export a point as a virtual disk	P2C conversion	Application-level restore

Network Shares

Restore entire file share	Rollback to a point in time
Restore files and folders	Restore permissions and security attributes
Instant share publishing	

91 **veeam**

Recovery scenarios with Veeam Backup & Replication v11

Backup Enterprise Manager

1-click VM/file restore	Virtual disk restore	Launch failover plan	Restore of vCD infrastructure
Exchange item restore	SQL/Oracle DB restore	Self-service Restore Portal	Restore via RESTful API

vCloud Director

Instant VM Recovery into vApp/vSphere	Full restore into vApp/vSphere	vCloud vApp restore	Linked Clone VMs to vCD
---------------------------------------	--------------------------------	---------------------	-------------------------

Tape

Full VM to infrastructure	Files from tape	Backup from tape	Tenant restore
---------------------------	-----------------	------------------	----------------

Extra

Restore via PowerShell	Extract utility	File restore audit	Restore under user context
------------------------	-----------------	--------------------	----------------------------

Cloud

Restore from "deleted" VCC backups	Restore from object storage	Restore from the VCC Provider	C2V conversion via "external" repo
	Partial/full site failover	Restore to Azure VM/AWS EC2	

Explorer for Storage Snapshots

Guest files (Windows/Multi-OS)	Instant VM/disk Recovery	SQL/Oracle DB restore	Exchange/SP/AD item restore
--------------------------------	--------------------------	-----------------------	-----------------------------

A solução contra ransomware da Veeam



Veeam Backup & Replication™



Veeam ONE™



Veeam Disaster Recovery Orchestrator



Kasten K10 da Veeam



Proteção Contra Ransomware

O **backup** seguro é a sua última linha de **defesa**



Backup

Imutabilidade confiável

Verificação de backups

Regra 3-2-1-1-0



Recuperação

Recuperação instantânea em escala

Restauração Segura

Orquestração de DR

Definido por software.

Sem aprisionamento com hardware proprietário

A Veeam ajuda os clientes a proteger dados



Perda
de dados real

33% - 2018

25% - 2020



Tempo de
inatividade

41% - 2018

24% - 2020



Perda de
produtividade

28% - 2018

21% - 2020



Recuperação
de dados

Mais recuperados

91+% dos dados

Fonte: <https://www.veeam.com/wp-ransomware-retrospective-2021.html>

Saiba mais sobre a recuperação rápida e confiável

Ransomware Prevention Kit

Secure Backup is your last line of Defense

- NEW! Proprietary white paper
- Deep dive webinar
- Free 30-day trial



veeam

5 Ransomware Protection Best Practices

Veeam's definitive guide to data protection

Rick Vanover
Senior Director,
Product Strategy, Veeam Software

Edwin Weijndema
Global Technology
Product Strategy, Veeam Software



veeam

2021 Ransomware Retrospective



veeam

Ransomware in 2022: 7 Capabilities You Need for Rapid and Reliable Recovery

Dave Russell,
Vice President, Enterprise
Strategy, Veeam Software

Jeff Reichard,
Senior Director, Enterprise
Strategy, Veeam Software

Chris Hoff,
Data Protection &
Ransomware Marketing
Manager, Veeam Software



A Veeam está trabalhando muito



Veeam Availability Suite &
Veeam Backup & Replication **v11a**



Veeam Backup *for AWS* **v4**
Veeam Backup *for Azure* **v3**
Veeam Backup *for Google Cloud* **v2**



Veeam DR Orchestrator **v5**
Kasten K10 by Veeam **4.5**



Qualquer nuvem. **Do seu jeito**

PRIVADA | PÚBLICA | HÍBRIDA | MÚLTIPLA | COMO UM SERVIÇO

VEEAMON 2022

A conferência do ano sobre proteção de dados moderna

De 16 a 19 de maio
Las Vegas e virtual



V12



Ransomware



Kubernetes



AWS/Azure/Google



Salesforce



Microsoft 365

Virtual

Acesse de qualquer lugar!

GRÁTIS

Presencial

Passe da conferência

\$1,199

QUANTIDADE LIMITADA!

Apenas 1.500 vagas disponíveis

Treinamento e certificação

+ US\$ 1.599

VMCE e VMCA

De 14 a 16 de maio

Aprenda com especialistas da Veeam



Anand Eswaran

Diretor executivo (CEO),
Veeam Software



Danny Allan

Diretor de tecnologia (CTO)
e Vice-presidente sênior,
Estratégia de Produtos, Veeam Software



Anton Gostev

Vice-presidente sênior, Gerenciamento de produtos,
Veeam Software



Rick Vanover

Diretor Sênior, Estratégia de Produtos,
Veeam Software



Registre-se e faça login
entre 4 e 18 de maio
para uma chance de ganhar
uma caixa de SnackMagic.

**INSCREVA-SE
AGORA**

Obrigado

veeam