



GUIA DE INTEGRAÇÃO

# AUMENTE SUA RESILIÊNCIA CIBERNÉTICA

COM O COMMVAULT CLOUD®  
CLEANROOM™ RECOVERY

# SUMÁRIO

03 O QUE É UM  
CLEANROOM?

04 POR QUE VOCÊ  
PRECISA DE UM?

05 PRINCIPAIS CASOS DE USO PARA  
AMBIENTES DE CLEANROOM

06 COMMVault® CLOUD  
CLEANROOM™ RECOVERY

07 DETALHES DE  
INTEGRAÇÃO

08 ETAPAS PARA INICIAR A  
RECUPERAÇÃO EM CLEANROOM

09 SERVIÇOS DE  
CLEANROOM

10 DETALHAMENTO  
DE CUSTOS

# O QUE É UM CLEANROOM?

Um cleanroom, também conhecido como Ambiente de Recuperação Isolado, não é apenas um espaço fisicamente seguro.

É uma fortaleza de proteção de dados, uma abordagem abrangente para a recuperação cibernética. Trata-se de um ambiente seguro e independente, cuidadosamente planejado e executado, com processos estabelecidos, melhores práticas, testes e procedimentos bem definidos.

A tecnologia por trás de um cleanroom não é mágica; seu verdadeiro poder está na capacidade de reunir esses diversos elementos em uma unidade coesa e eficaz, aumentando a segurança e a proteção dos seus dados.



# POR QUE VOCÊ PRECISA DE UM?

Os ciberataques aumentaram e se intensificaram drasticamente nos últimos anos, representando uma ameaça significativa e imediata para organizações de todos os setores.

Esses ataques podem ter consequências devastadoras, incluindo violações de dados, perdas financeiras e danos irreparáveis à reputação. A urgência em proteger seus dados nunca foi tão grande. A maioria dos ciberataques começa sem malware. Isso significa que os invasores ainda conseguirão obter acesso, independentemente de quão forte seja a defesa de segurança na linha de frente.

Hoje, os invasores não “invadem” mais sistemas.

**Eles fazem login.**



De acordo com o IBM Security Group, uma vez que o invasor obtém acesso, o tempo médio de permanência em uma empresa é de

**204 DIAS<sup>1</sup>**

**Nos primeiros**

**84 MINUTOS,**

**os invasores se movem lateralmente.** Isso significa que, durante esses 204 dias, eles se deslocam silenciosamente pelo ambiente, explorando e aproveitando vulnerabilidades. Esse período é conhecido como left of bang, um termo usado para descrever o período antes de o impacto total de um evento ser sentido.

Quando os invasores executam o evento de criptografia, conhecido como “bang”, o dano é tão abrangente que, em média, leva

**21 DIAS**

**para restaurar sistemas críticos.** Os dias gastos analisando e recuperando-se do ciberataque são chamados de right of bang, um termo usado para descrever o período após o impacto total do evento.

Empresas que não possuem uma opção de recuperação e decidem pagar o resgate não têm melhores resultados.

**Mais de**

**90% DAS EMPRESAS**

que pagam o resgate não recuperam todos os seus dados; **em média, recuperam menos de 70% dos dados.**

No entanto, você pode ter confiança na recuperação de dados com a tecnologia de cleanroom. As empresas estão descobrindo que os tempos de descriptografia

**EXCEDEM EM MUITO**

**o tempo que levaria para restaurar a partir de backups,** tornando a tecnologia de cleanroom uma solução mais eficaz e eficiente. Empresas que pagam o resgate são atacadas novamente dentro de um mês, pois ainda operam em um ambiente comprometido.

# PRINCIPAIS CASOS DE USO PARA AMBIENTES DE CLEANROOM

Um ambiente de cleanroom é essencial para estratégias de recuperação cibernética. Ele oferece um espaço econômico e flexível para testes, além de uma área segura para analisar, restaurar e corrigir sistemas afetados por ciberataques. Cleanrooms proporcionam uma recuperação mais rápida, minimizam a perda de dados e aumentam a resiliência contra ameaças cibernéticas.

**A seguir, alguns casos de uso críticos de um cleanroom na recuperação cibernética:**



## Testes Contínuos do Plano de Recuperação Cibernética

- ✓ As organizações podem utilizar o cleanroom para simular ciberataques e avaliar seus planos de resposta a incidentes, identificando e corrigindo possíveis falhas antes de enfrentar um ataque real.
- ✓ Exercícios regulares em um ambiente de cleanroom ajudam as equipes de segurança e TI a se manterem preparadas e a aprimorar continuamente o plano de recuperação cibernética para ataques reais.



## Resposta a Incidentes e Forense: Análise Pós-Incidente

- ✓ O cleanroom oferece um ambiente controlado para que analistas forenses investiguem a linha do tempo do ataque, identifiquem sua origem e coletem evidências para possíveis processos legais.
- ✓ O cleanroom permite desenvolver, testar e implementar correções de segurança em um ambiente seguro e controlado antes de aplicá-las aos sistemas de produção.



## Recuperação Segura de Dados

- ✓ Um cleanroom pode extrair cópias limpas de dados críticos a partir de backups não infectados, mesmo que parte dos dados dos sistemas de produção esteja comprometida.
- ✓ Quando a integridade do ambiente de produção é questionada, o cleanroom oferece um local seguro para iniciar a recuperação enquanto o ambiente está sendo remediado.
- ✓ Os cleanrooms fornecem um ambiente seguro para iniciar a recuperação durante a correção do ambiente de produção quando há dúvidas sobre sua integridade.

# COMMVAULT® CLOUD CLEANROOM™ RECOVERY

O Cleanroom Recovery oferece um ambiente de recuperação isolado, seguro, limpo e acessível sob demanda para testar planos de recuperação cibernética, realizar análises forenses seguras e garantir a continuidade dos negócios sem interrupções.

A solução da Commvault permite recuperar workloads de qualquer local para um cleanroom seguro e isolado na nuvem, aumentando sua resiliência e prontidão cibernética.

**Nossos principais diferenciais incluem:**

- ✓

### Portabilidade Any-to-Any

Permite a recuperação de qualquer workload de qualquer local para outro. Tradicionalmente, aplicações e dados de diferentes sistemas exigiam a duplicação de todos os ambientes para teste e recuperação.
- ✓

### Redução de Custos e Complexidade

Possibilita a utilização de uma abordagem flexível de cleanroom, reduzindo custos e complexidade. Pague apenas pelo que você precisa, quando precisar.
- ✓

### Plano de Controle Somente Leitura

Iniciamos a recuperação em cleanroom com um plano de controle somente leitura para impedir acessos caso o ambiente de produção esteja comprometido.
- ✓

### Tecnologia de IA/ML

Utiliza tecnologia de IA/ML para identificar e selecionar automaticamente pontos de recuperação confiáveis.

✗

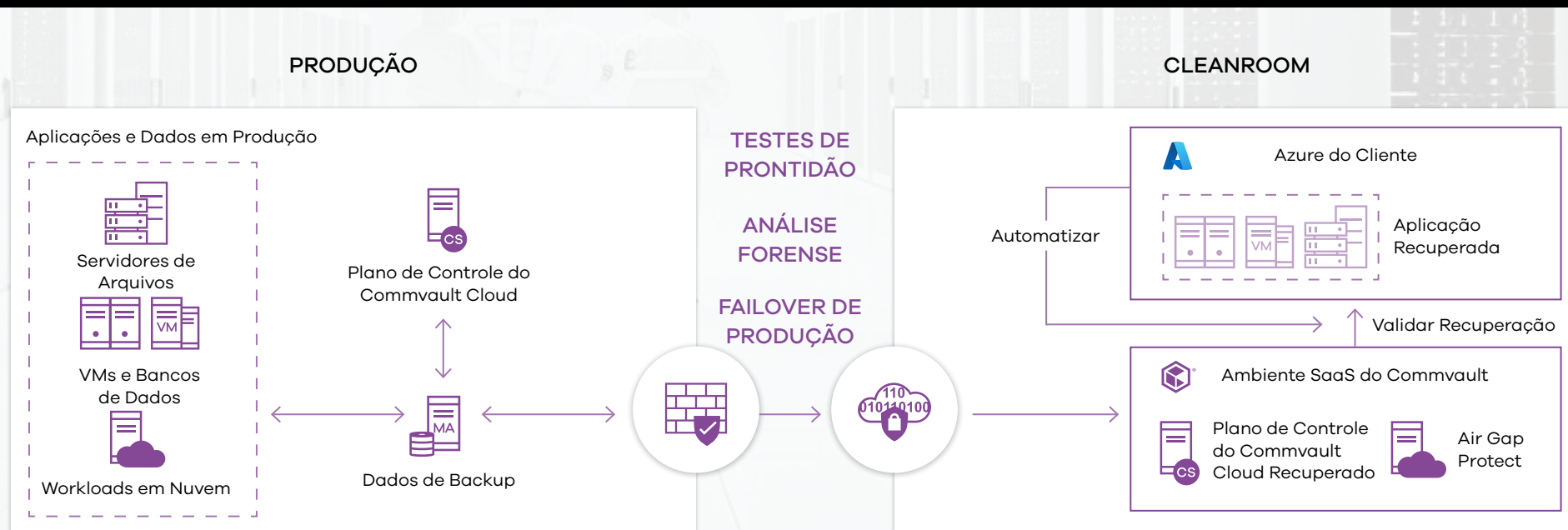
### Cleanrooms Tradicionais

Os métodos tradicionais de cleanroom costumam ser caros e complexos para muitas organizações. Outras soluções de segurança de dados com ofertas semelhantes são limitadas à recuperação de desastres e restritas a um conjunto limitado de workloads e opções de recuperação.

# DETALHES DE INTEGRAÇÃO

O Commvault Cleanroom Recovery automatiza a recuperação do Control Plane do Commvault Cloud em um tenant SaaS do Commvault Cloud. Em seguida, automatiza a recuperação de máquinas virtuais a partir do Commvault Cloud Air Gap Protect para um tenant Azure fornecido pelo cliente, com base nos grupos de recuperação definidos.

A Figura 5 (abaixo) ilustra como seria o ambiente de um cliente atualmente utilizando o software da Commvault. O Control Plane recuperado estará na mesma região do armazenamento Air Gap Protect (por exemplo, US Central), e o ambiente de destino deve estar na mesma região.



As VMs recuperadas serão automaticamente removidas (excluídas do ambiente de cleanroom de destino) quatro dias após a recuperação do control plane. As VMs recuperadas podem ser mantidas por mais tempo mediante contato com o suporte da Commvault. Clientes que desejam migrar as VMs recuperadas para produção podem trabalhar com os serviços profissionais da Commvault e com provedores de serviços locais.

# ETAPAS PARA INICIAR A RECUPERAÇÃO EM CLEANROOM

## ETAPA 01

### Recuperar o Control Plane

Acesse [cloud.commvault.com](https://cloud.commvault.com) e inicie o processo de recuperação do control plane. Você receberá e-mails notificando o início e a conclusão da recuperação do control plane.

## ETAPA 02

### Preparar o Ambiente de Recuperação

Crie um tenant Azure separado.

## ETAPA 03

### Adicionar o Hipervisor de Destino no Azure

Acesse a interface (UI) do Commvault recém-recuperada e adicione o hipervisor do Azure como destino de recuperação.

## ETAPA 04

### Adicionar um Destino de Recuperação em Cleanroom

Acesse a interface do Commvault e crie o destino de recuperação apontando para o ambiente Azure criado na Etapa 02.

## ETAPA 05

### Criar um Grupo de Recuperação

Crie um grupo de recuperação e adicione os workloads que deseja recuperar ou selecione um grupo de recuperação já existente e inicie a recuperação.

# SERVIÇOS DE CLEANROOM

A Commvault oferece um conjunto de serviços de Cleanroom para projetar, implementar, testar e, quando necessário, responder a incidentes. Ao utilizar os serviços da Commvault, você pode ter confiança de que nossos especialistas trazem anos de experiência com o Commvault Cloud para ajudar a desenvolver sua estratégia de recuperação e trabalhar com você para que esteja preparado no caso de um ciberataque.

Esta tabela detalha os benefícios e o escopo dos serviços de Design & Implementação de Cleanroom, Testes de Prontidão e Resposta a Incidentes.

SERVIÇO	BENEFÍCIOS	ESCOPO
Design e Implementação	✓ Planejar e construir a capacidade de recuperar rapidamente ativos de produção em um ambiente de recuperação isolado na nuvem.	<p><b>Planejar e Configurar os Recursos do Commvault</b></p> <ul style="list-style-type: none"> <li>• Serviço de Validação de Recuperação do CommServe</li> <li>• Air Gap Protect</li> <li>• Recuperação de Aplicações em Cleanroom</li> </ul> <p><b>Testes Iniciais</b></p> <ul style="list-style-type: none"> <li>• Teste de Recuperação do Control Plane</li> <li>• Teste de Grupo de Recuperação</li> </ul>
Testes de Prontidão	✓ Aumentar a confiança da equipe de TI na capacidade de recuperação após um ciberataque por meio de testes regulares do plano de recuperação em cleanroom e sua atualização conforme necessário.	<p><b>Recuperação do Control Plane</b></p> <ul style="list-style-type: none"> <li>• Recuperar o control plane</li> <li>• Executar um teste de restauração</li> <li>• Exportar evidências</li> </ul> <p><b>Teste de Recuperação</b></p> <ul style="list-style-type: none"> <li>• Executar failover do control plane</li> <li>• Restaurar grupo(s) de recuperação no Azure conforme necessário para análise</li> </ul>
Resposta a Incidentes	✓ Recuperar rapidamente ativos de produção em um ambiente isolado para análises forenses durante a recuperação de um ciberataque.	<p><b>Recuperação em Cleanroom</b></p> <ul style="list-style-type: none"> <li>• Executar failover do control plane</li> <li>• Restaurar grupo(s) de recuperação no Azure conforme necessário para análise</li> </ul>

# DETALHAMENTO DE CUSTOS

## O que é necessário para realizar a compra?

O Cleanroom Recovery é vendido em incrementos de 10 TB. Para determinar a medida de 10 TB, o cliente configura os dados em um Grupo de Recuperação com base nos terabytes de front-end.

Por exemplo, se um cliente configurar 100 TB de dados nos grupos de recuperação (com base no tamanho dos dados no momento da configuração), deverá adquirir 10 unidades. Se o cliente precisar configurar 104 TB de dados, deverá adquirir 11 unidades. Um SKU de 10 unidades custa US\$ 1.590.

## Para utilizar o Commvault Cloud Cleanroom Recovery, os clientes precisam de:

- SKU de Cleanroom Recovery
- Air Gap Protect
- Backup & Recovery (de qualquer um dos pacotes)
  - Para software: versão 11.34.13 ou superior
  - Para SaaS: versão 11.36 ou superior
- Qualquer um dos níveis do Commvault Cloud — Operational Recovery, Autonomous Recovery, Cyber Recovery

---

Agende uma reunião com seu parceiro hoje mesmo para saber mais sobre como você pode aumentar sua resiliência com o Cleanroom Recovery.

[commvault.com](https://commvault.com) | 888.746.3849 | [get-info@commvault.com](mailto:get-info@commvault.com)

