

# Inovações de resiliência cibernética baseadas em IA

Reduza o caos da recuperação de ameaças cibernéticas.

## Introdução

As interrupções cibernéticas agora são inevitáveis, causando desafios para empresas em todo o mundo. Mais de 65%<sup>1</sup> das empresas sofreram uma violação cibernética nos últimos dois anos. O aumento das ameaças cibernéticas, o impacto e os custos associados aos tempos de inatividade, e a evolução das demandas das regulamentações governamentais ressaltam a necessidade de uma **solução de resiliência cibernética** mais simples, inteligente e rápida.

## O estado da recuperação cibernética

O processo de recuperação cibernética permanece complexo, ineficiente e cheio de incertezas. Pode ser caótico, exigindo colaboração entre várias organizações, e geralmente fica nas mãos da TI, que se vê sobrecarregada e pouco treinada. O tempo médio de recuperação aumentou para 19 dias, de 15,7 dias em 2022 e 6,7 dias em 2021<sup>2</sup>. Em 2023, apenas 35% das organizações afirmaram que podem se recuperar em um mês, uma queda significativa de 52% em 2022<sup>2</sup>. Algumas organizações enfrentam tempos de recuperação que se estendem por até três meses.

O impacto financeiro e de reputação das capacidades de recuperação inadequadas é profundo. As interrupções cibernéticas podem custar mais de 2,73 milhões de dólares por incidente<sup>2</sup>, quase o dobro nos últimos 2 anos, com custos adicionais afetando a integridade da marca e a confiança do público. Por exemplo, a recente interrupção cibernética da MGM Resorts levou 10 dias para se recuperar e foi estimada em quase 100 milhões de dólares. Incidentes públicos, como o ataque de ransomware no [Aeroporto de Seattle](#), destacam ainda mais os impactos sociais, incluindo interrupções operacionais e inconvenientes para o cliente.

## A necessidade de resiliência cibernética eficaz

As organizações devem proteger os dados em ambientes complexos aproveitando as soluções baseadas em IA que aumentam a segurança e facilitam a recuperação, especialmente quando a equipe está sobrecarregada e mal treinada. A recuperação rápida e confiável

## Principais desafios na recuperação cibernética:

- **Falta de recuperação automatizada:** muitas organizações têm dificuldade em desenvolver modelos de recuperação que incorporem automação para diferentes níveis de recuperação. Os modelos de recuperação podem ajudar a reduzir o caos e a confusão de uma recuperação cibernética.
- **Coordenação de várias equipes:** a recuperação eficaz requer colaboração entre as equipes de TI, gerenciamento de dados e segurança e, possivelmente, outras.
- **Gerenciamento de ameaças e malwares:** garantir que os dados recuperados estejam livres de malware ou vulnerabilidades.
- **Restauração da plataforma de backup:** restaurar uma plataforma de backup comprometida é essencial se ela tiver sido o alvo.
- **Identificação de pontos de dados:** encontrar o ponto de recuperação ideal entre 90.000 pontos de dados em potencial pode ser difícil.
- **Ambiente de recuperação limpo:** restaurar dados em um ambiente "limpo" para evitar a reintrodução de ameaças.
- **Escassez de habilidades:** a escassez de profissionais de TI especializados agrava os desafios de recuperação, com 45% dos líderes de TI citando a falta de habilidades em segurança de dados e 29% notando que a experiência em proteção de dados é insuficiente.

é essencial para reduzir o tempo de inatividade e proteger a reputação organizacional. Uma solução eficaz de resiliência cibernética deve ser fácil de usar, inteligente e transparente, permitindo uma recuperação mais simples e rápida, além de aderir às regulamentações em evolução.

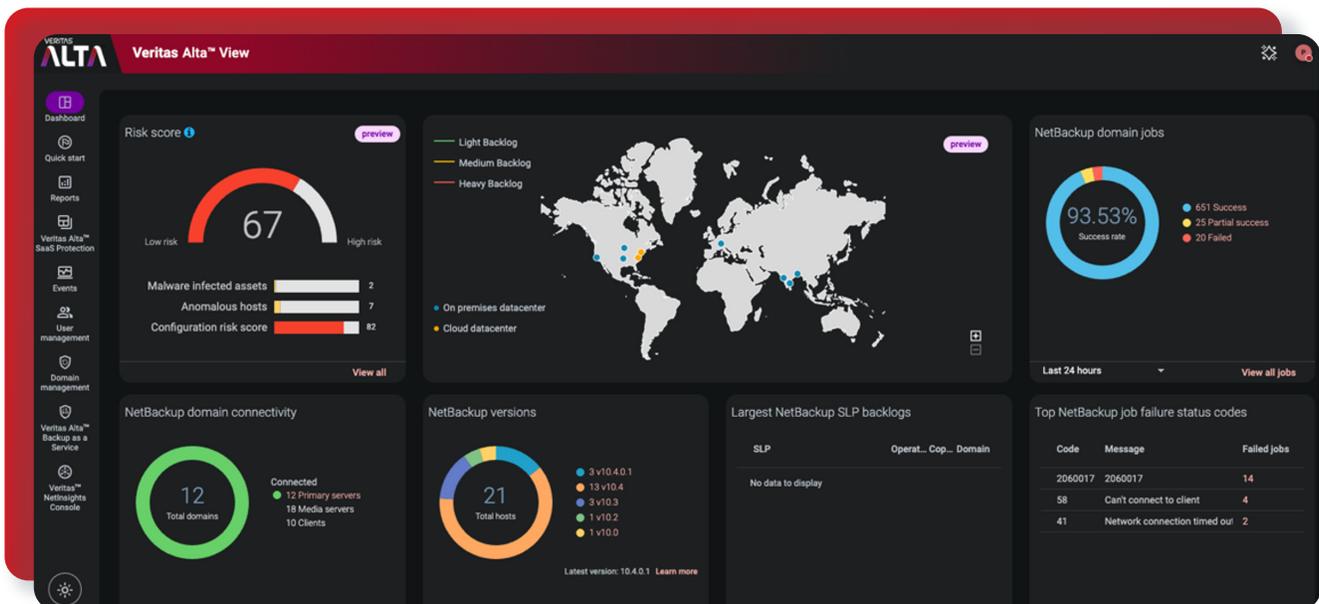
## Soluções da Veritas para maior resiliência cibernética

A Veritas Technologies é líder em segurança cibernética há muito tempo, aproveitando a base sólida da estrutura do National Institute of Standards and Technology (NIST) para oferecer soluções escaláveis de resiliência cibernética. Os princípios fundamentais dessa estrutura — identificar, proteger, detectar, responder e recuperar — têm sido fundamentais para orientar a forma como a Veritas aborda o desenvolvimento de soluções robustas e escaláveis que atendam às necessidades de grandes empresas. Ao aderir a esses fundamentos, a Veritas fornece consistentemente tecnologias que não apenas protegem os dados, mas também garantem uma rápida recuperação após um incidente, oferecendo uma vantagem essencial em uma escala que os concorrentes lutam para igualar.

Com base nessa base estabelecida, as inovações recentes da Veritas continuam aprimorando suas capacidades de resiliência cibernética, tornando-as mais simples, mais inteligentes e mais rápidas. Esses novos desenvolvimentos se concentram em aprimorar a automação, melhorar a inteligência contra ameaças e simplificar as práticas de gerenciamento para oferecer estratégias de proteção mais proativas e preditivas. Por exemplo, o Veritas Alta™ Copilot introduz a automação inteligente para reduzir significativamente os tempos de recuperação e a intervenção manual. Essa evolução das ofertas da Veritas foi projetada não apenas para acompanhar a evolução do cenário de ameaças, mas para estabelecer novos padrões do setor em termos de simplicidade e velocidade de recuperação. Essas melhorias refletem uma mudança estratégica voltada a soluções mais integradas e fáceis de usar, que minimizam a complexidade e maximizam a eficiência e o controle, garantindo que a Veritas permaneça na vanguarda do setor de proteção de dados.

### Mais simples

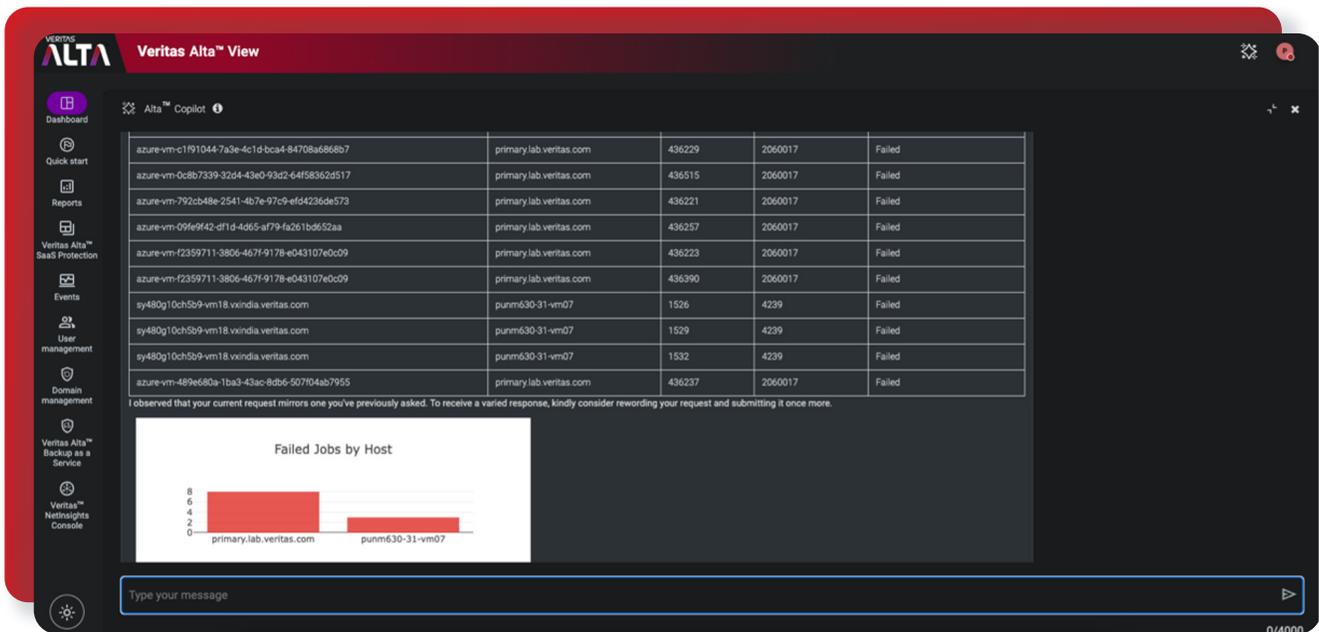
- **Experiência de usuário aprimorada:** a nova interface de usuário da Veritas Alta oferece uma interface moderna e intuitiva, que simplifica o gerenciamento de dados e facilita a navegação.



- **Criação automatizada de políticas de proteção:** facilita o desenvolvimento e a aplicação de políticas de segurança usando IA para sugerir e implementar estratégias ideais de proteção de dados.
- **Auditoria e proteção de ativos não detectados:** aprimora os recursos de descoberta e proteção de ativos de dados não detectados anteriormente, garantindo segurança abrangente.

## Mais inteligente

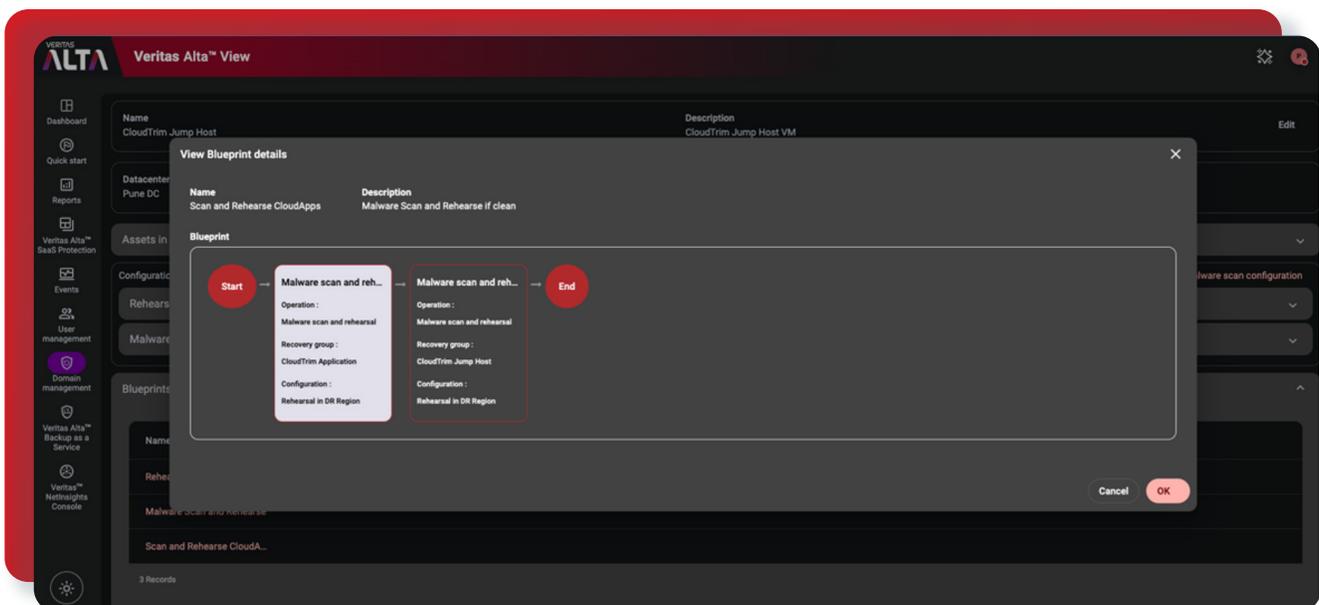
- **Análise inteligente de falhas em tarefas de backup:** usa IA para fornecer insights a fim de identificar e tratar as causas básicas das falhas de backup, garantindo uma proteção consistente dos dados.



- **Detecção aprimorada de malware com inteligência artificial:** usa inteligência artificial avançada para detectar e mitigar ameaças com eficácia em todos os ativos de dados.
- **Caça acelerada de ameaças e análise de raio de explosão:** acelera a detecção de ameaças e limita possíveis danos, aproveitando a detecção de malware baseada em hash e a indexação eficiente de arquivos.

## Mais rápida

- **Recomendações de pontos de recuperação inteligentes:** aproveita análises avançadas para recomendar pontos de recuperação ideais, equilibrando velocidade e integridade dos dados.
- **Modelos de recuperação orquestrados:** oferece fluxos de trabalho automatizados e definidos pelo cliente para recuperação, personalizáveis para se alinharem aos objetivos específicos de recuperação e aos requisitos de conformidade.



- **Recuperação flexível entre nuvens:** facilita a recuperação de dados em vários ambientes de nuvem, garantindo a continuidade dos negócios durante interrupções ou ataques específicos da nuvem.
- **Avaliação de segurança e pontuação de risco de alto nível:** fornece uma visão abrangente da postura de segurança, avaliando fatores como frequência de backup e possíveis vulnerabilidades.

## Conclusão

A Veritas continua sendo pioneira em resiliência cibernética, oferecendo soluções mais simples, inteligentes e rápidas. Essas soluções simplificam as operações, aceleram os tempos de recuperação e garantem a conformidade com as regulamentações do setor. As ferramentas da Veritas permitem que as organizações lidem com as complexidades da recuperação cibernética com mais eficiência, garantindo operações contínuas e protegendo sua reputação contra ameaças futuras. Ao adotar as soluções da Veritas, as empresas podem proteger seus dados, se recuperar rapidamente de incidentes cibernéticos e demonstrar forte resiliência cibernética, mantendo assim a eficácia operacional e garantindo a confiança das partes interessadas.

Para obter mais informações sobre como a Veritas pode aprimorar sua estratégia de resiliência cibernética, visite [veritas.com/pt/br/alta/view](https://www.veritas.com/pt/br/alta/view) ou entre em contato conosco hoje mesmo.

1. Veritas [https://www.veritas.com/content/dam/www/pt/documents/analyst-report/AR\\_veritas\\_data\\_risk\\_management\\_report\\_2023.pdf](https://www.veritas.com/content/dam/www/pt/documents/analyst-report/AR_veritas_data_risk_management_report_2023.pdf)
2. Statista: <https://www.statista.com/statistics/1422159/us-healthcare-ransomware-attacks-downtime-average-by-days/>

## Sobre a Veritas

A Veritas Technologies é líder em gerenciamento de dados em várias nuvens. Mais de 80 mil clientes, incluindo 91% das empresas da Fortune 100, confiam na Veritas para ajudar a garantir a proteção, capacidade de recuperação e conformidade de seus dados. A Veritas tem uma reputação de confiabilidade em escala, o que oferece a resiliência de que seus clientes precisam contra as interrupções ameaçadas por ataques cibernéticos, como ransomware. Nenhum outro fornecedor é capaz de igualar a capacidade de execução da Veritas, com suporte para mais de 800 fontes de dados, mais de 100 sistemas operacionais e mais de 1.400 destinos de armazenamento por meio de uma abordagem única e unificada. Com tecnologia de escala de nuvem, a Veritas está entregando hoje sua estratégia de gerenciamento autônomo de dados, que reduz a sobrecarga operacional e, ao mesmo tempo, oferece maior valor. Saiba mais em [www.veritas.com/pt/br](https://www.veritas.com/pt/br). Siga-nos no X em [@veritastechllc](https://twitter.com/veritastechllc).

# VERITAS™

2625 Augustine Drive  
Santa Clara, CA 95054  
+1 (866) 837 4827  
[veritas.com/pt/br](https://www.veritas.com/pt/br)

Para obter informações de contato globais, visite: [www.veritas.com/pt/br/company/contact](https://www.veritas.com/pt/br/company/contact)