BRASP Cyber Cloud

Segurança completa para todas as camadas dos seus dados

- *Segurança*
- *Backup e DR*
- *Gerenciamento*
- *Monitoramento*

Conheça com a BRASP um novo conceito em Serviços de Proteção de Dados e Backup!

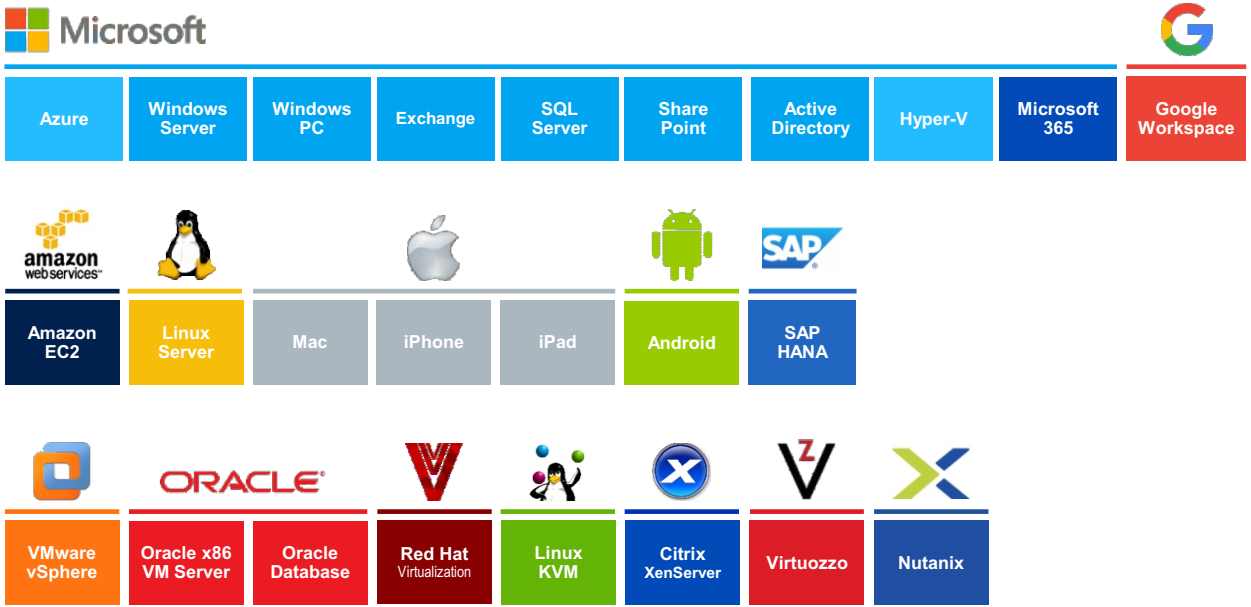
BRASP Cyber Cloud

Seguro, econômico e expansível de acordo com as suas necessidades!

- *Melhoria da segurança*
- *Redução dos custos de TI*
- *Níveis de serviço mais elevados*

Advanced Packs: Segurança, Gestão, Backup, Recuperação de Desastres

Proteção para mais de 20 plataformas em uma única solução.



Agilizamos a entrega de proteção de dados com integração total, tudo em uma só ferramenta!

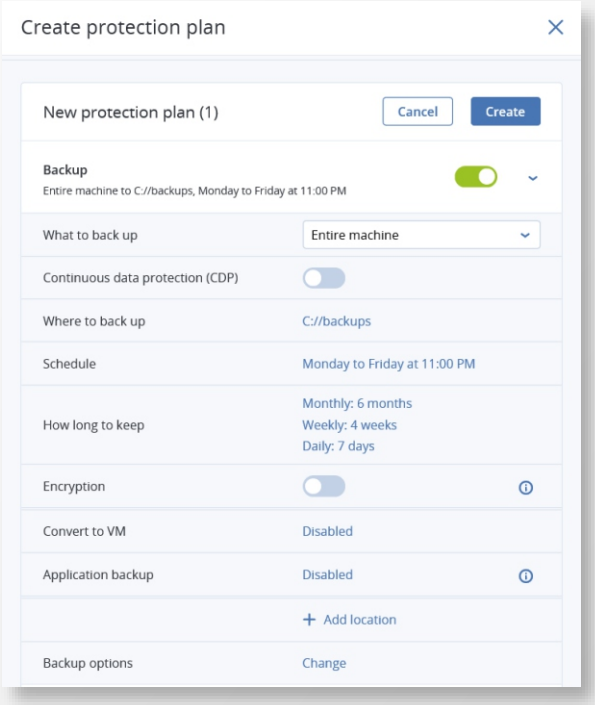
Backups a nível de arquivo e imagem completa

Faça backup de arquivos individuais ou proteja seu negócio inteiro com apenas alguns cliques.

Backup em nível de arquivo: Use essa opção para proteger dados específicos, reduzir o tamanho do backup e economizar espaço de armazenamento.

Backup de imagem completa: Faça backup facilmente de todo o sistema como um único arquivo, garantindo restaurações de bare metal.

Em caso de desastre de dados, você pode facilmente restaurar todas as informações para o novo hardware!



Porque?

Garanta a continuidade dos seus negócios com opções flexíveis de backup e evite o tempo de inatividade e a perda de dados.

Opções de armazenamento flexíveis

Armazenamento nuvem

Google Cloud Platform

Acronis Cyber Cloud Storage

Azure

Três opções de armazenamento em nuvem

aws

IBM Cloud

Alibaba Cloud

Outras nuvens públicas
(via Acronis Cyber Backup Gateway)

Seu próprio armazenamento em nuvem

Armazenamento local

Discos locais

SMB/CIFS/DFS and NFS shares

Acronis Cyber Infrastructure

Garanta a conformidade e a presença local

Escolha entre 26 data centers em todo o mundo para armazenar dados hospedados na Acronis, Google Cloud e Microsoft Azure

20+6

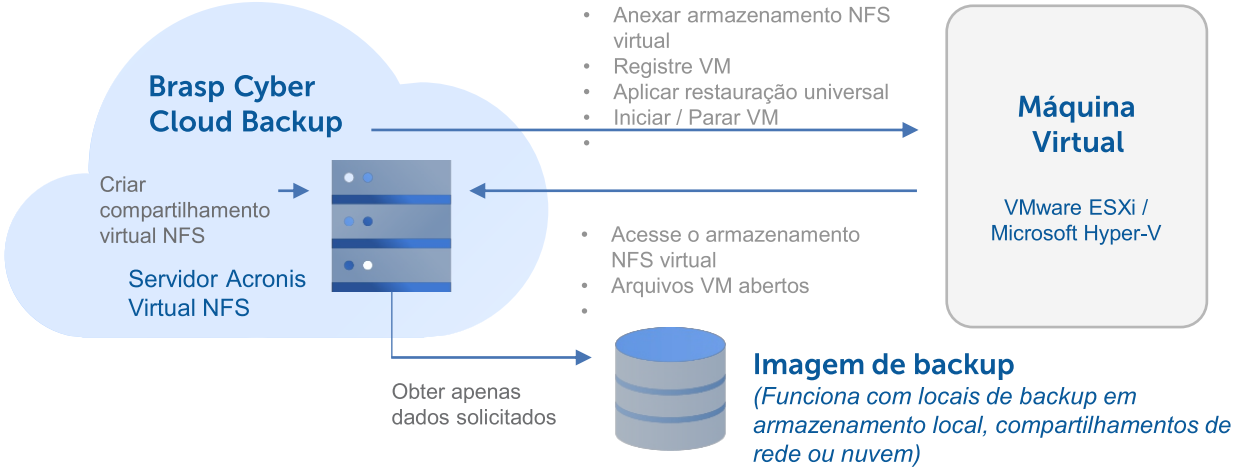
DATA CENTERS

Forte presença na Ásia - Pacífico:
Cingapura, Japão, Austrália

O melhor RTO com Instant Recovery

O Instant Restore é uma tecnologia patenteada que permite recuperar sistemas em segundos, iniciando qualquer sistema Windows ou Linux (físico ou virtual) diretamente do armazenamento de backup no host Microsoft Hyper-V ou VMware vSphere ESXi existente– sem mover dados.

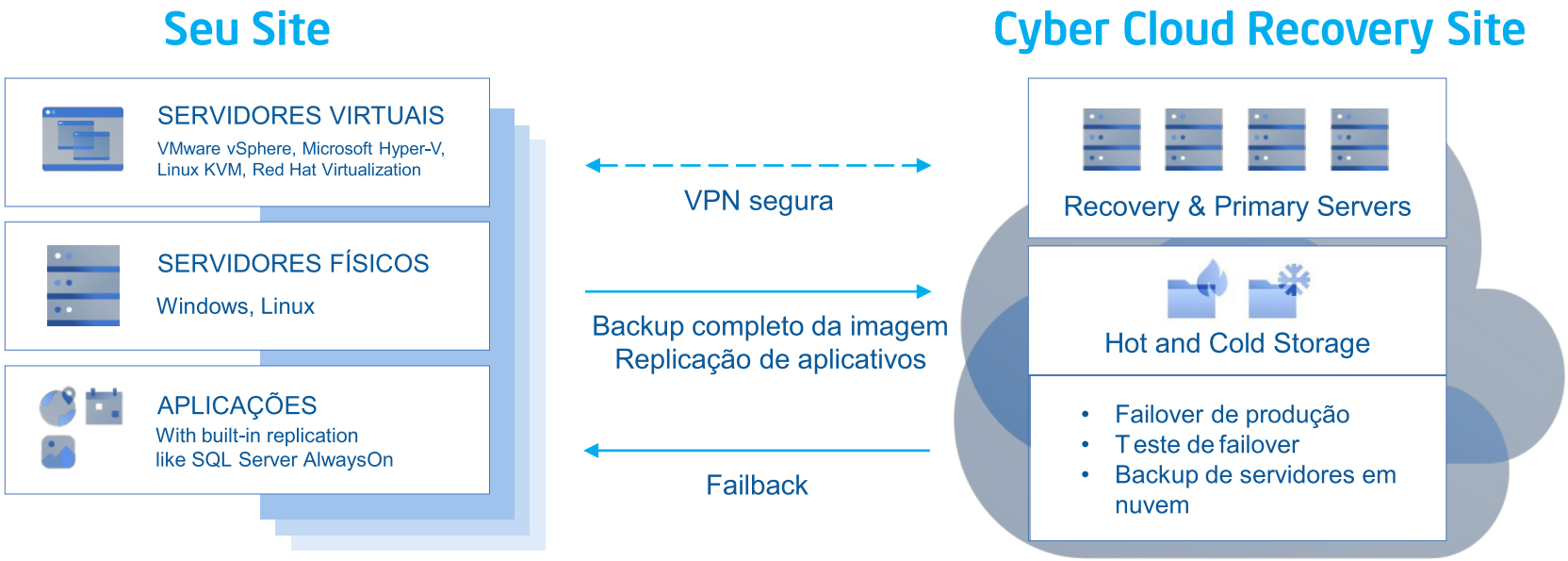
Como funciona:



Benefícios

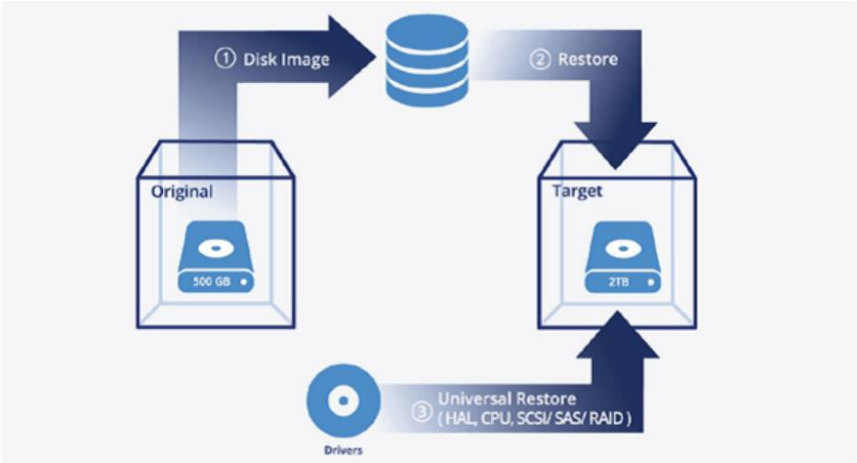
- RTO em segundos!
- Recuperar qualquer servidor virtual, físico, em nuvem, Windows ou Linux.
- Redução do consumo de rede

Disaster Recovery no Brasp Cyber Cloud | Cloud Recovery Site



Universal Restore

- Restaurar sistemas Windows e Linux para hardware diferente.
- Recuperação rápida e fácil do sistema para hardware diferente, incluindo ambientes físicos, virtuais ou em nuvem – Bare Metal.
- Depois de recuperar uma imagem de disco como está, o Universal Restore analisa a nova plataforma de hardware e sintoniza as configurações do Windows ou Linux para corresponder aos novos requisitos.



Porque?

- Garanta uma migração rápida e fácil do sistema com alguns cliques.
- Reduzir os RTOs.
- Minimizar o tempo de inatividade.

Recursos anti-malware estendidos

Brasp Cyber Cloud Protect

Brasp Cyber Cloud Backup

Active Protection

Anti-ransomware, anti-cryptojacking, AI- and ML-enabled

+

Static AI analyzer

Detecção on-access e sob demanda

Anti malware engine

Qualquer malware (detecção de nuvem e local)

Motor comportamental

Detecção no acesso

Integração nativa com o Windows Security Center

Porque? Prevenção ativa do tempo de inatividade e perda de dados, não apenas recuperação após um ataque.

Proteção em IA contra malware de dia zero

Proteção anti-malware para Windows, Linux e macOS

Detecção de ransomware e recuperação de dados.

Detecção de processos de criptomining.

Proteção em tempo real e varredura sob demanda.

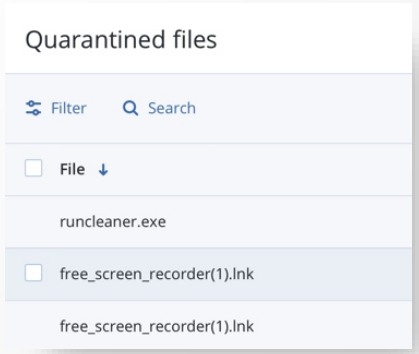
Autoproteção: Proteger os componentes do Acronis (por exemplo, registro, parada de serviço, proteção de arquivos Acronis).

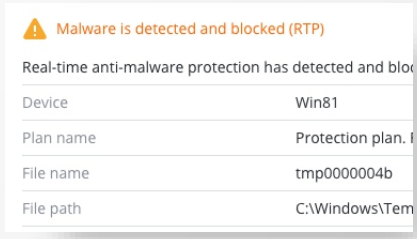
Proteção de pastas de rede: proteja os dados em pastas compartilhadas em sua máquina contra ransomware.

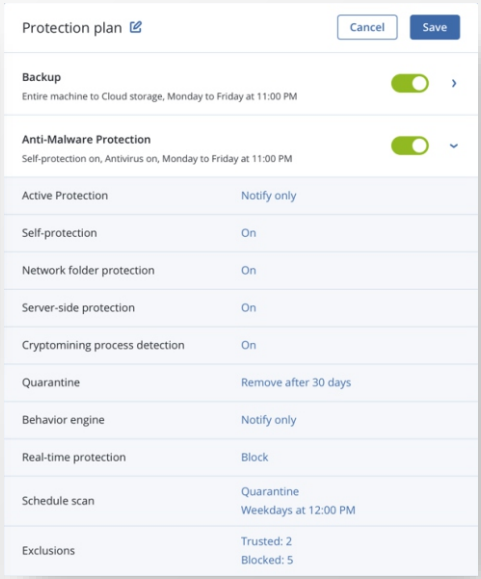
Proteção do lado do servidor: proteja os dados em pastas compartilhadas dentro de sua rede contra ransomware.

Quarentena de arquivos.

Gerenciamento de exclusões: Especifique processos que não serão considerados malware; excluir pastas onde as alterações de arquivo não serão monitoradas; selecionar arquivos e pastas onde a digitalização programada não será executada.



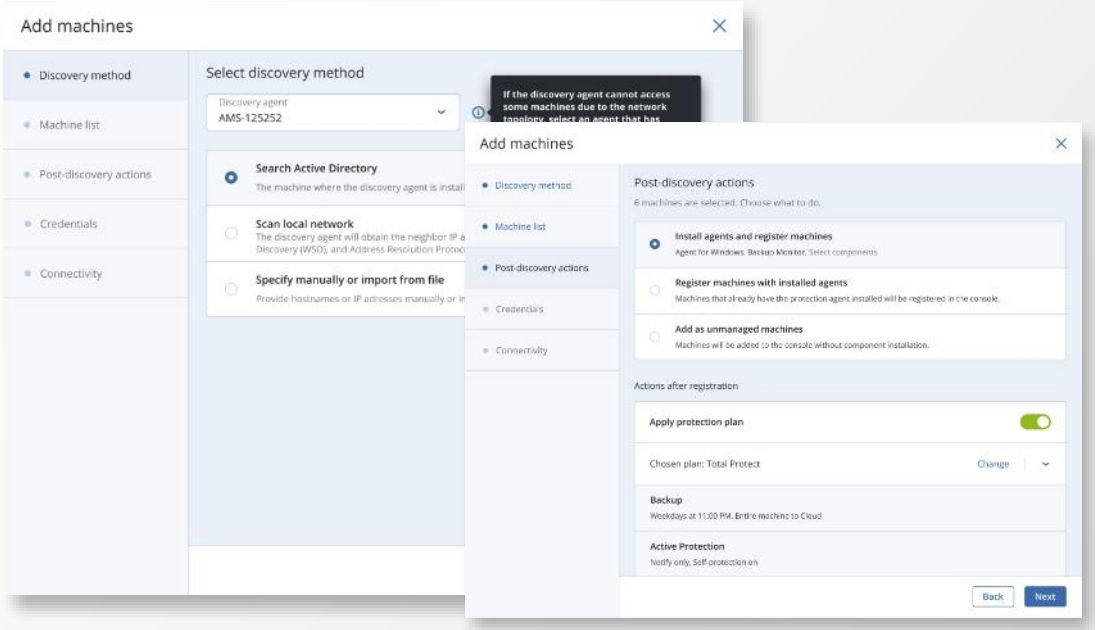




Descoberta e instalação remota de agentes

Simplifique o processo de instalação de vários agentes ao mesmo tempo – tanto na nuvem quanto no local

- Descoberta baseada em rede
- Descoberta baseada em Active Directory
- Importe uma lista de computadores do arquivo
- Aplique automaticamente um plano de proteção
- Instalações de agentes remotos em lote com um assistente de descoberta

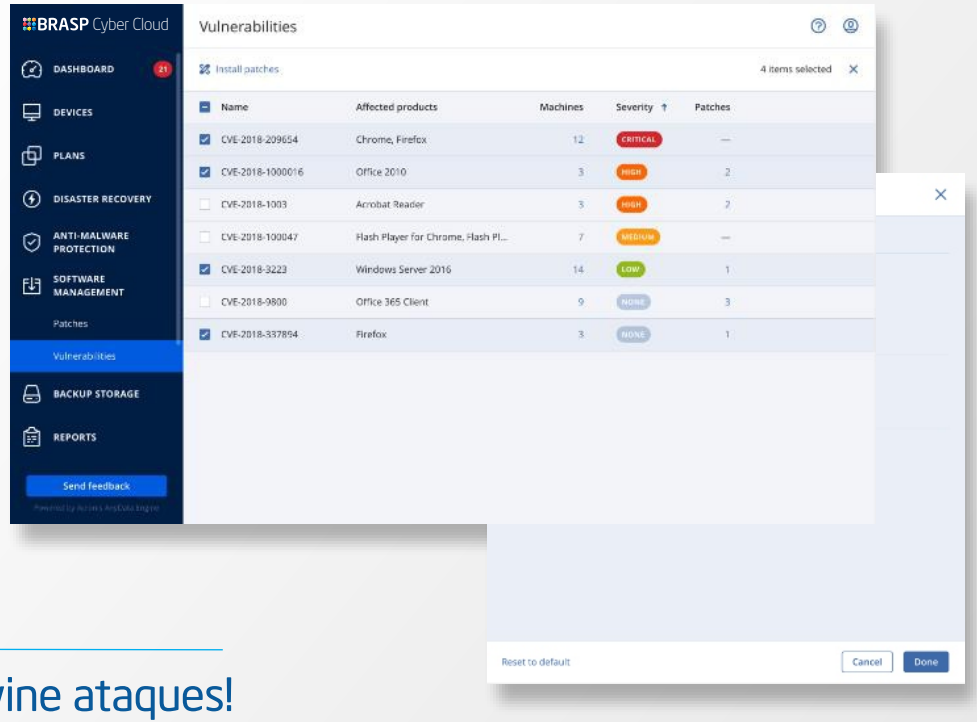


Porque ? Mais fácil e mais rápido no embarque. Menos recursos necessários. Proteção completa.

Avaliações de vulnerabilidade

Descubra um problema antes que seja um problema

- Atualizações contínuas e diárias do banco de dados de vulnerabilidades e gerenciamento de patches da Acronis.
- Suporte para:
  a) Estações de trabalho– Windows 7 e posterior
  b) Servidor– Windows Server 2008R2 e posterior
  c) Microsoft Office (2010 e mais) e componentes relacionados
  d) .NET Framework eaplicativosde servidor
  e) Adobe, Oracle Java
- Navegadorese outrossoftwares.



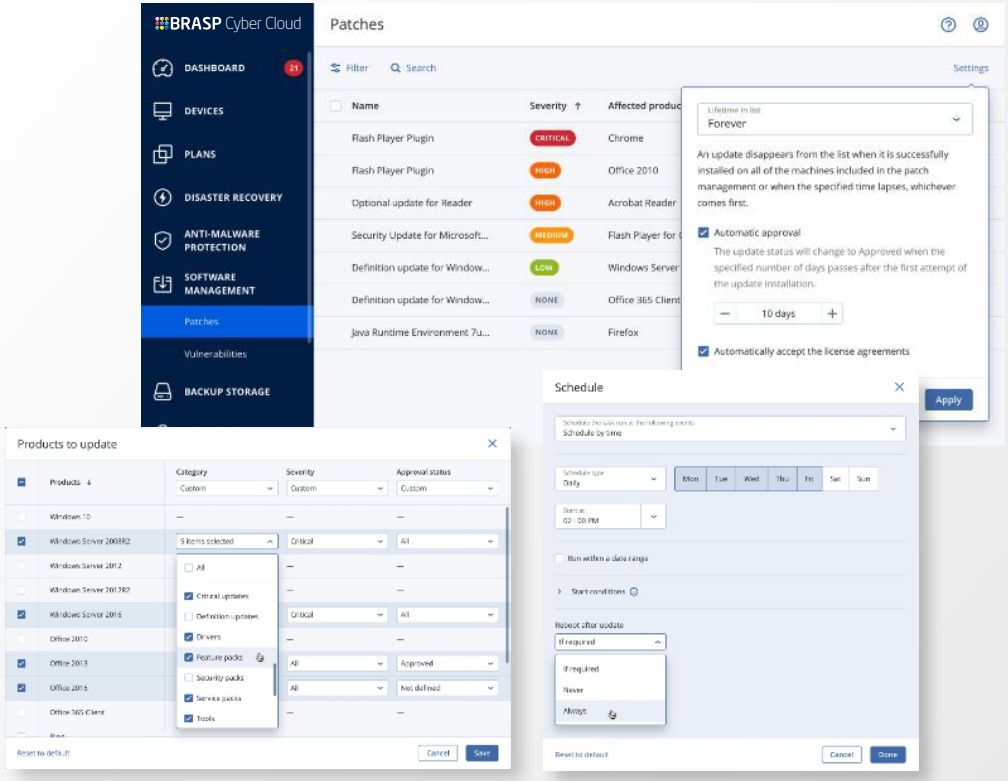
Porque? Mitiga potenciais ameaças e previne ataques!

Gerenciamento de patches

Corrija o problema antes que o problema aconteça.

O banco de dados de vulnerabilidades contém 12 869 Vulnerabilidades e Exposições Comuns, 250 -300 novos CVEs semanais

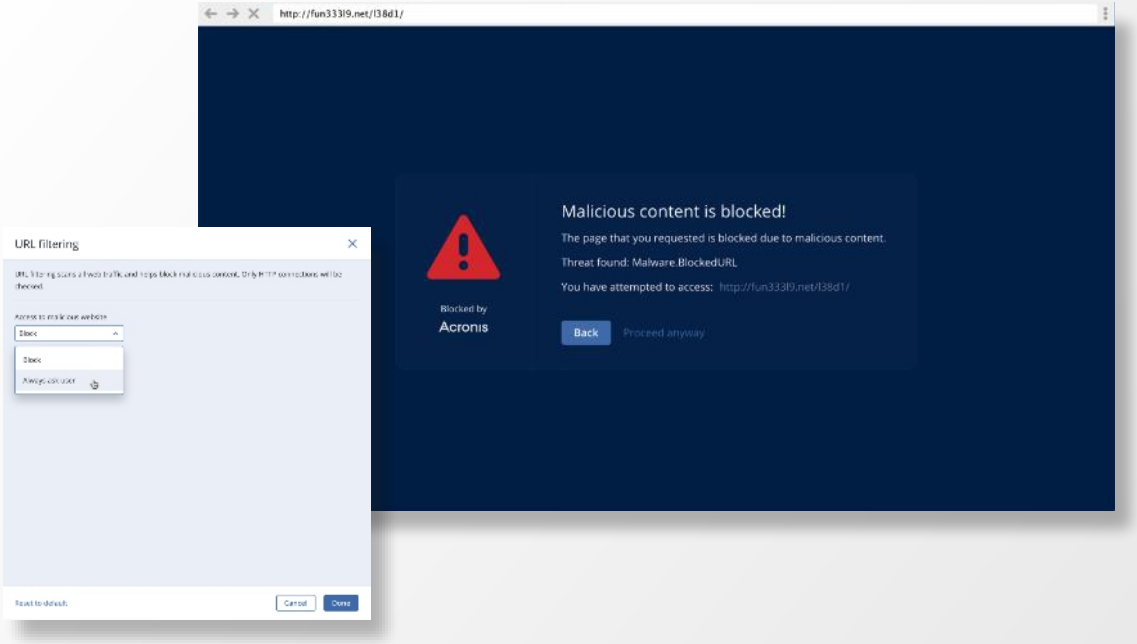
- **Aprovação automática de patches**
- **Implantação em um cronograma**
- **Implantação manual**
- **Opções flexíveis de reinicialização e janela de manutenção**
- **Implantação em estágio**
- **Todas as atualizações do Windows, incluindo o MS Office e os aplicativos Win10**



Porque? Automatiza a proteção, mitiga potenciais ameaças, previne ataques. (Equifax & WannaCry)

Filtragem de URL. Controle o acesso a URLs maliciosas

A filtragem de URL permite controlar o acesso a sites da Internet, permitindo ou negando acesso a sites específicos com base em informações contidas em uma lista de URL.

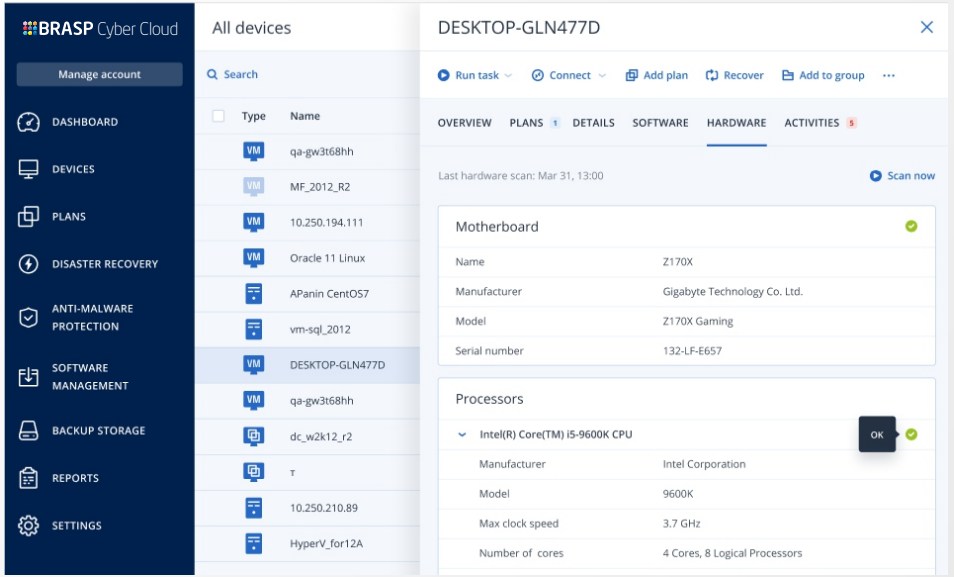


- **Banco de dados de terceiros**
- **Interceptor HTTP/HTTPS interno**
- **Listas preto/branco para URLs**
- **Análise de carga para URLs maliciosos**

Porque? Prevenção de ataques através de sites maliciosos/hackeados, melhor conformidade e produtividade.

Inventário de hardware

- Descubra todos os ativos de hardware em todos os endpoints protegidos da organização (por exemplo, CPU, GPU, motherboard, RAM, adaptadores de rede, etc.)
- Obtenha informações atualizadas sobre ativos de hardware
  - As varreduras regulares podem ser agendadas para serem executadas automaticamente
  - As varreduras sob demanda podem ser acionadas manualmente
  - Obtenha informações detalhadas sobre ativos de hardware, como modelo, fabricante, número de série, etc.
  - Navegue por todos os ativos de hardware, ou pesquise por vários critérios: modelo de processador, núcleos de processador, tamanho total do disco, capacidade de memória
  - Gere relatórios de inventário de hardware



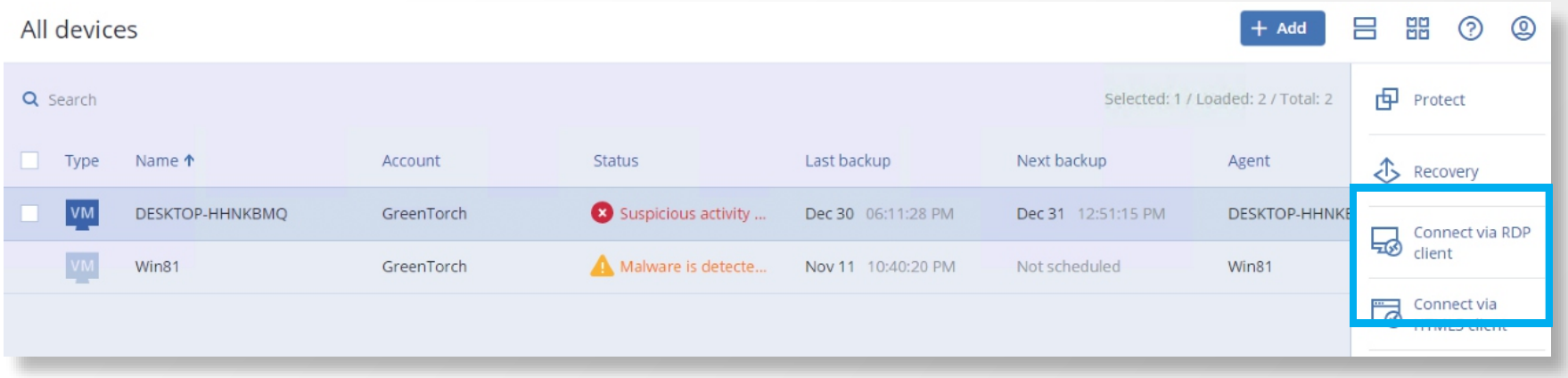
Porque? Economize tempo e esforço com informações atualizadas de inventário de hardware.

Desktop remoto e assistência remota

Opere remotamente qualquer endpoint como se você estivesse perto do dispositivo!

Conecte-se a máquinas remotas mesmo atrás de um firewall ou em uma rede privada sem alterar as configurações de firewall ou estabelecer VPN adicional.

Permita que seu time técnico visualize a tela do usuário, ajude com tarefas específicas ou corrija problemas.

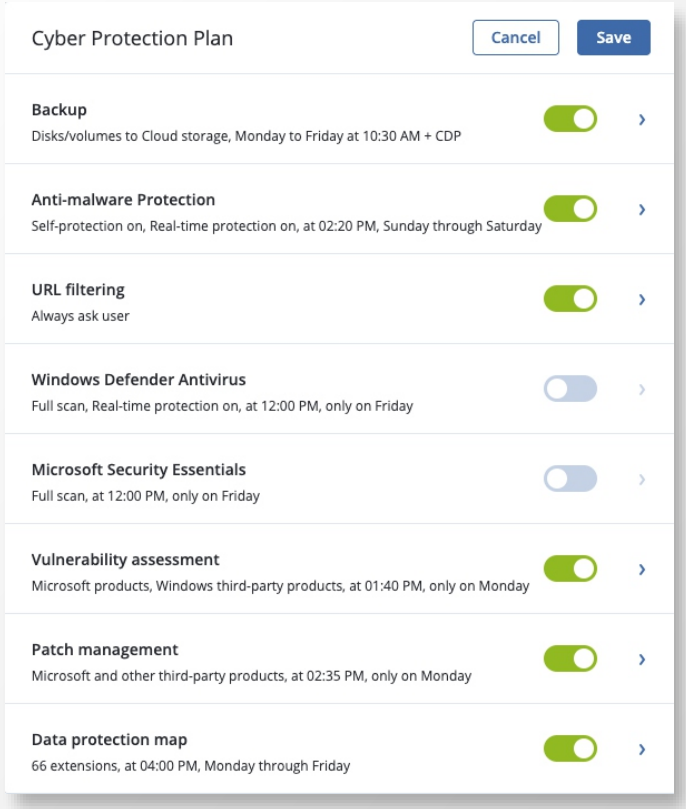


Porque? Menos ferramentas, além de menos esforço para se conectar, e tempos de reação mais rápidos, custos reduzidos.

Um plano de proteção!

Abrange todos os aspectos de proteção cibernética :

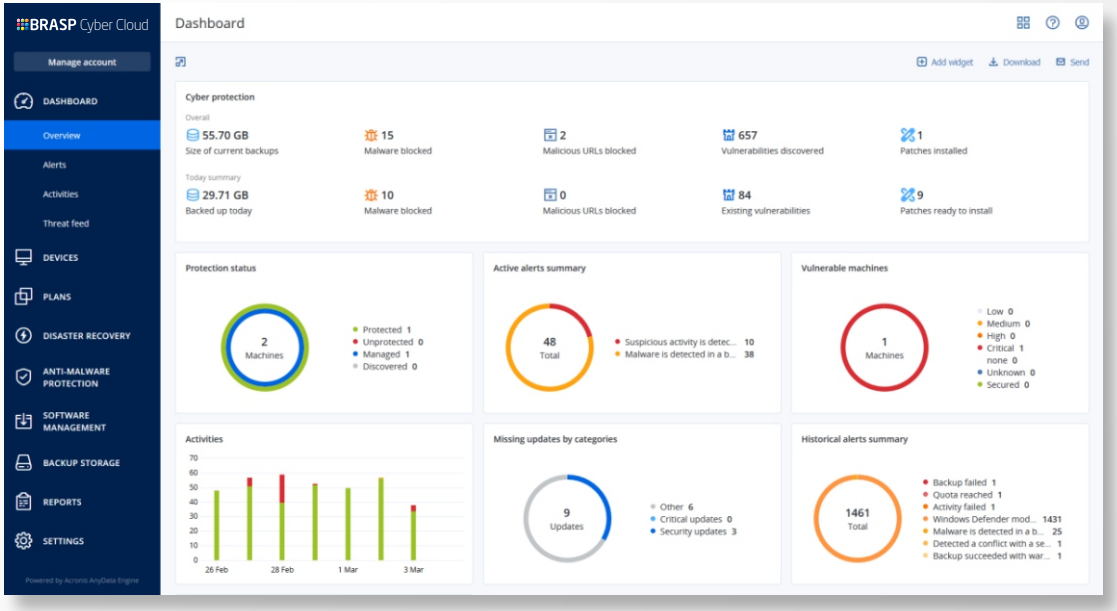
- **Backup**
- **Proteção anti-malware**
- **Recuperação de desastres**
- **Filtragem de URL**
- **Avaliações de vulnerabilidades**
- **Gerenciamento de patches**
- **Descoberta de dados (via mapa de proteção de dados)**
- **Gerenciamento do Microsoft Defender Antivirus Microsoft Security Essentials**



Porque? Melhor proteção com menos esforço, automatizada!

Monitoramento e relatórios flexíveis

- Monitoramento de saúde por hardware (HDD, SSD)
- Controle de atualizações ausentes
- Painel com Widgets personalizáveis
- Identifique rapidamente os problemas
- Acesso rápido às ações de gestão



Porque? Console única, operações mais rápidas, ajuda a demonstrar valor de MSP e simplificar renovações.

Cyber Protect Cloud

Advanced Backup:

- ✓ Proteção contínua de dados
- ✓ Suporte de backup para clusters de servidores SQL da Microsoft, Clusters Microsoft Exchange, Oracle DB, SAP HANA
- ✓ Mapa de proteção de dados e relatórios de conformidade
- ✓ Relatórios de backup agendados

Advanced Disaster Recovery:

- ✓ Falha de produção e teste para Acronis Cloud
- ✓ Runbooks: orquestração de recuperação de desastres
- ✓ Opção de implantação sem VPN
- ✓ Suporte a VPN Multisite IPsec, VPN aberto local-a-site L2
- ✓ Vários modelos
- ✓ Configuração de DNS personalizada

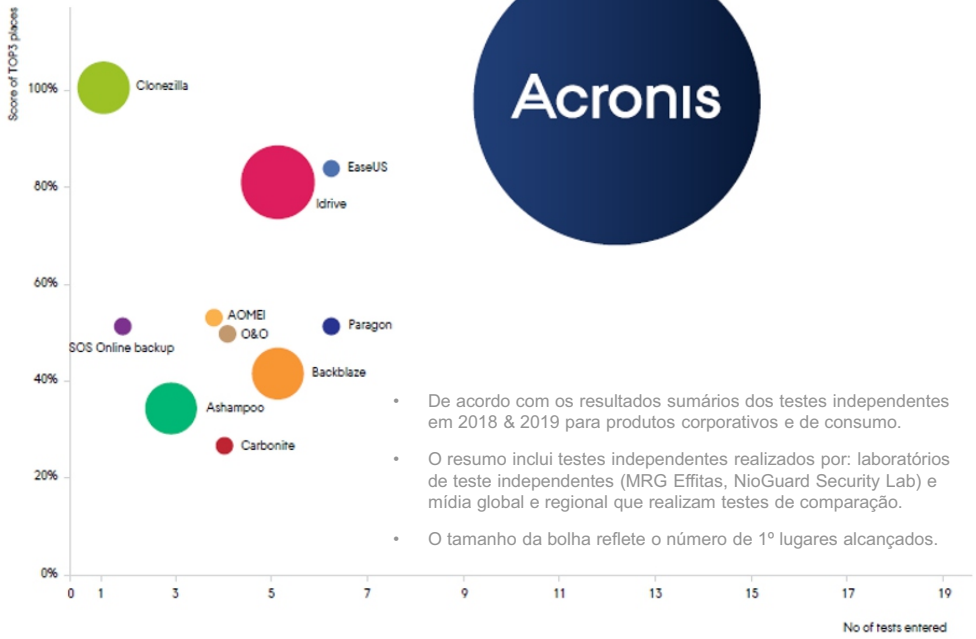
Advanced Security:

- ✓ Filtragem de URL
- ✓ Prevenção de exploração
- ✓ Antivirus com detecção aprimorada baseada em assinaturas
- ✓ Varreduras anti-malware de dados na Nuvem Acronis: Remova a carga nos endpoins e garanta backups sem malware
- ✓ Dados forenses em backups
- ✓ Planos de proteção inteligente
- ✓ Lista automática de permissões
- ✓ Recuperação segura: atualizações de definição de AV e varreduras anti-malware como parte do processo de recuperação para evitar a recorrência de ameaças
- ✓ Limpeza remota do dispositivo
- ✓ Gerenciamento anti-malware do Windows

Advanced Management:

- ✓ Gerenciamento automatizado de patches
- ✓ Inventário de software
- ✓ Monitor de saúde de Discos
- ✓ Patches à prova de falhas
- ✓ Agendamento de relatórios

Líder em resultados de testes independentes



Acronis

- De acordo com os resultados sumários dos testes independentes em 2018 & 2019 para produtos corporativos e de consumo.
- O resumo inclui testes independentes realizados por: laboratórios de teste independentes (MRG Effitas, NioGuard Security Lab) e mídia global e regional que realizam testes de comparação.
- O tamanho da bolha reflete o número de 1º lugares alcançados.

SME 2020-21 DCIG TOP 5 ANTI-RANSOMWARE BACKUP

Gold Self-Protection Award Anti-Malware Test Lab

vb 100 VIRUS virusbtn.com

AV TEST APPROVED BACKUP & DATA SECURITY SOFTWARE av-test.org 04/2017

AV TEST APPROVED CORPORATE ENDPOINT PROTECTION WINDOWS TOP PRODUCT av-test.org 02/2019

MRG Effitas CERTIFIED

BRASP Cyber Cloud | Acronis