

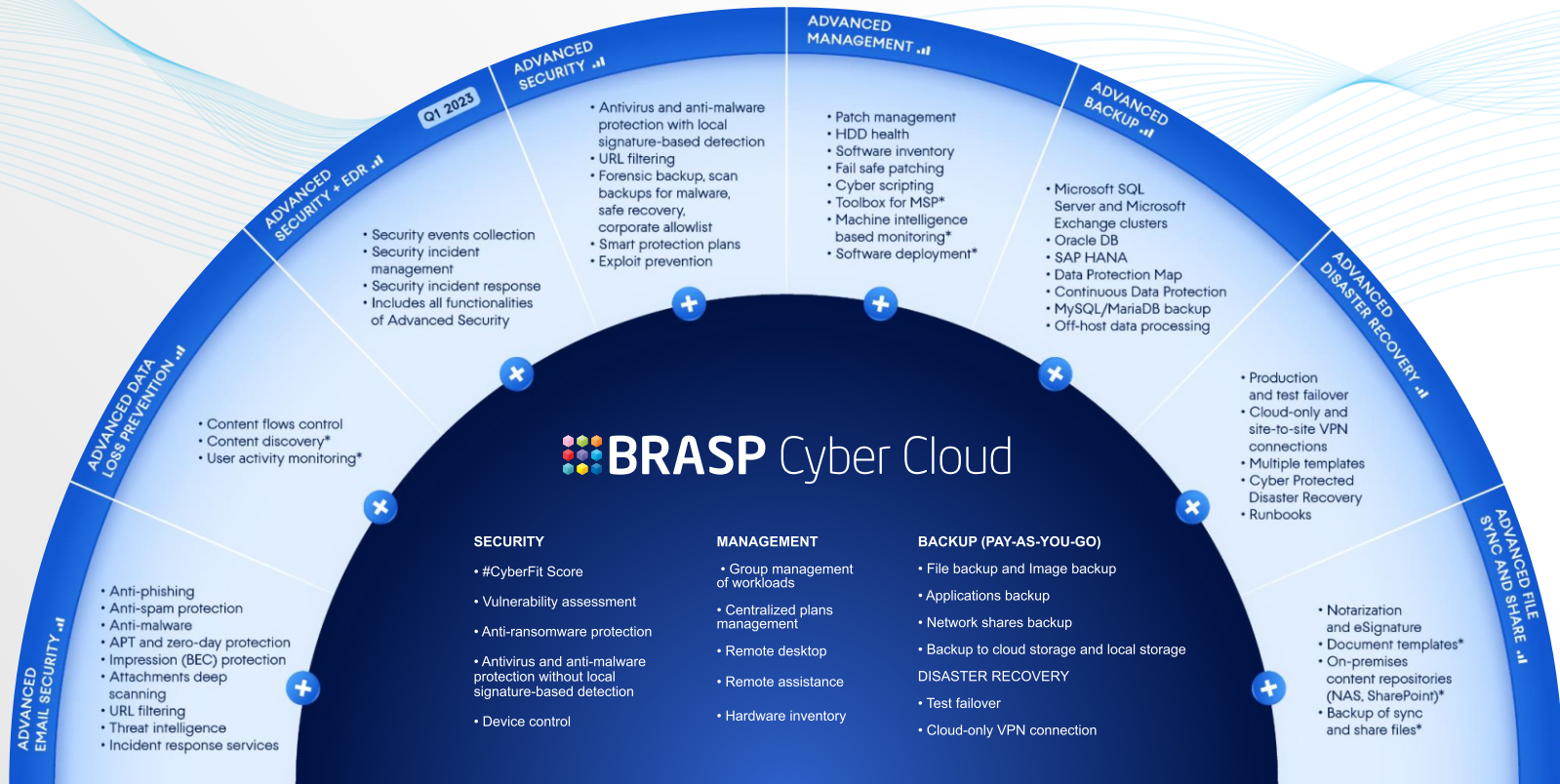
BRASP Cyber Cloud

*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

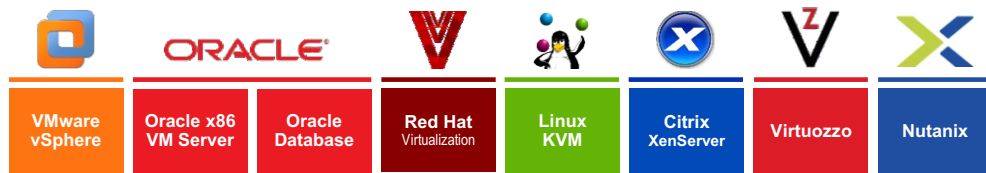
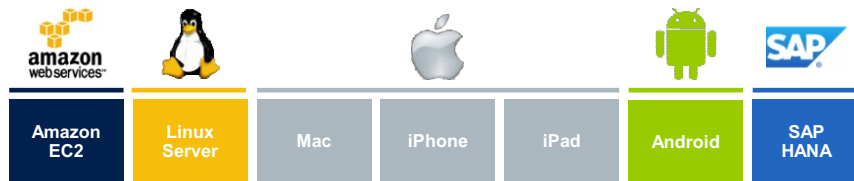
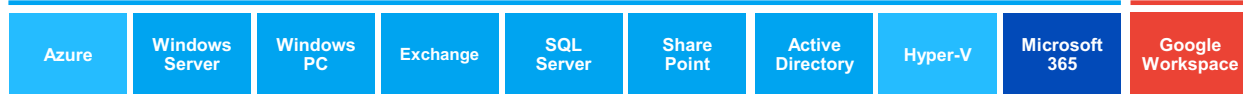
Seguro, econômico e expansível de acordo com as suas necessidades!

- *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.

Create protection plan

New protection plan (1) Cancel Create

Backup Entire machine to C://backups, Monday to Friday at 11:00 PM On

What to back up Entire machine

Continuous data protection (CDP) Off

Where to back up C://backups

Schedule Monday to Friday at 11:00 PM

How long to keep Monthly: 6 months
Weekly: 4 weeks
Daily: 7 days

Encryption Off

Convert to VM Disabled

Application backup Disabled

+ Add location

Backup options Change

Opções de armazenamento flexíveis

Armazenamento nuvem



Google Cloud Platform



Acronis Cyber
Cloud Storage



aws



IBM Cloud



Alibaba Cloud



Três opções de
armazenamento
em nuvem

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

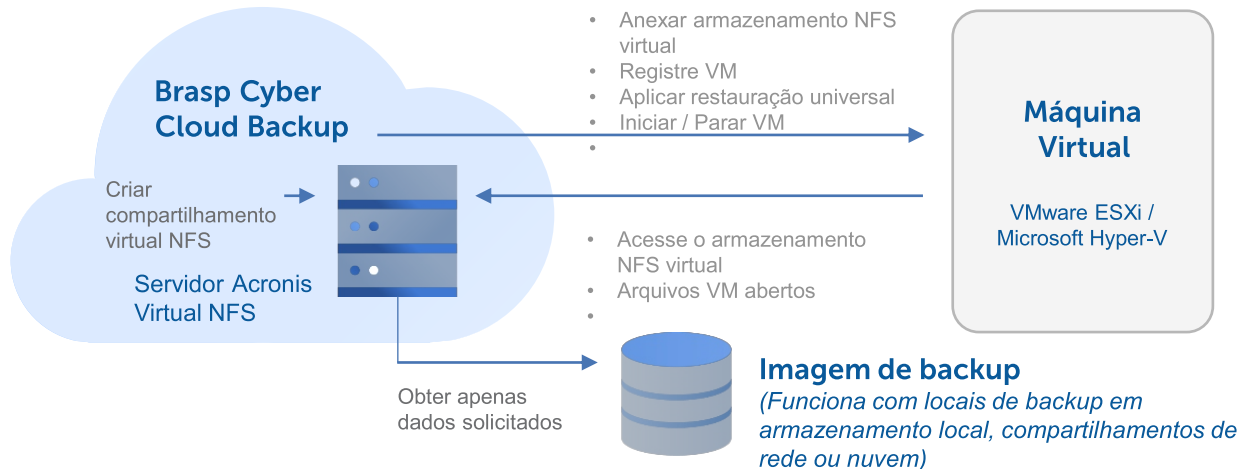
Forte presença na Ásia - Pacífico:
Cingapura, Japão, Austrália



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:

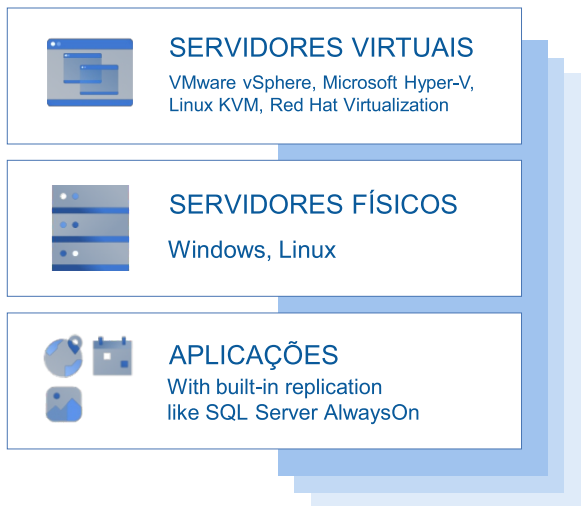


Benefícios

- **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

Seu Site

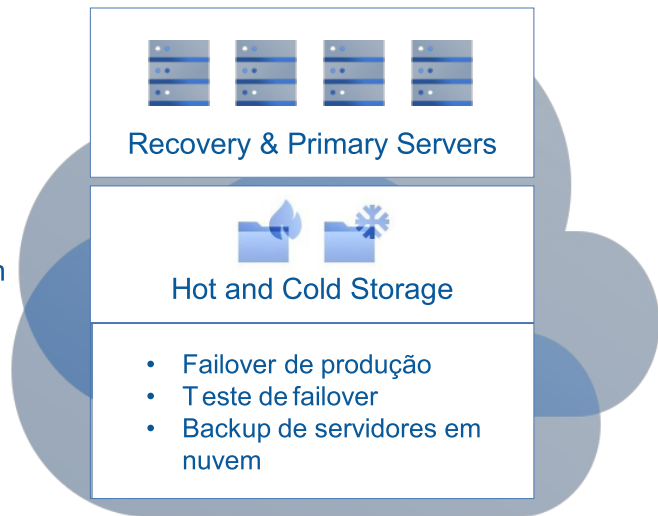


← VPN segura →

→ Backup completo da imagem
Replicação de aplicativos

← Failback

Cyber Cloud Recovery Site

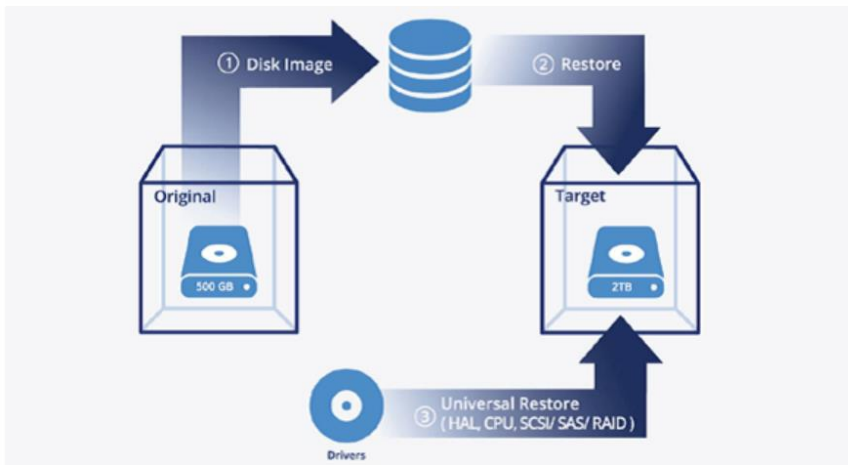


Universal Restore

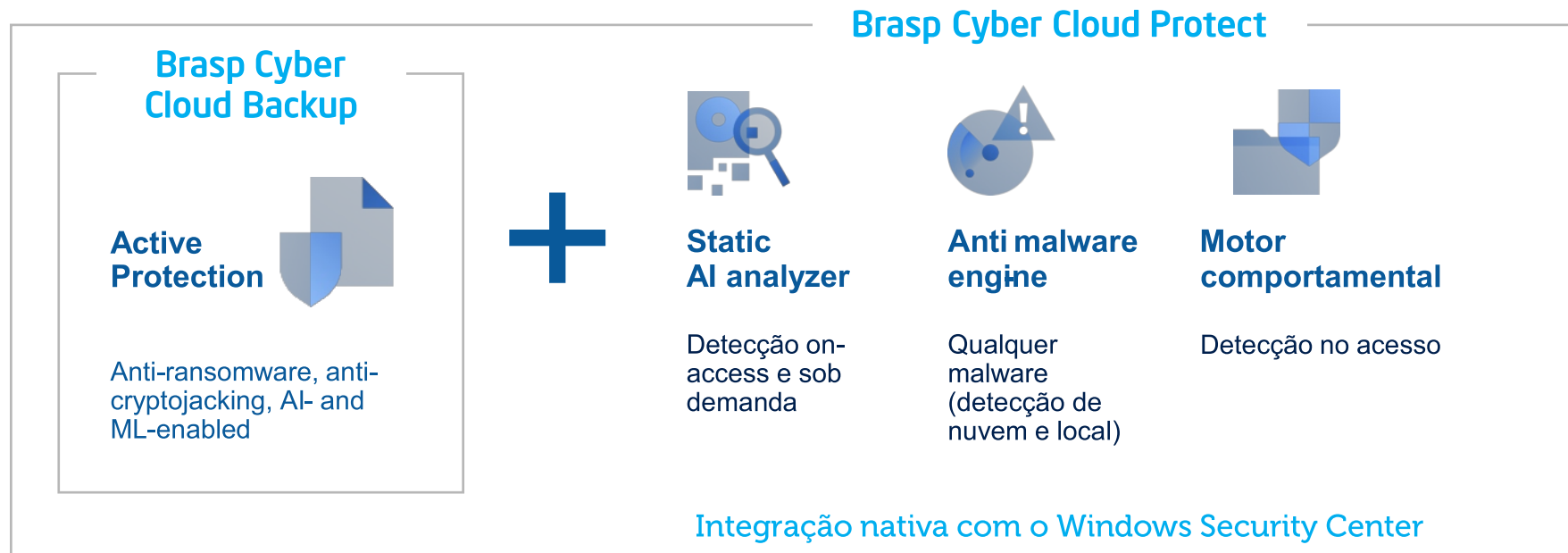
- Restaurar sistemas Windows e Linux para hardware diferente.
- Recuperação rápida e fácil do sistema para hardware diferente, incluindo ambientes físicos, virtuais ou em nuvem – Bare Metal.
- Depois de recuperar uma imagem de disco como está, o Universal Restore analisa a nova plataforma de hardware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



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.

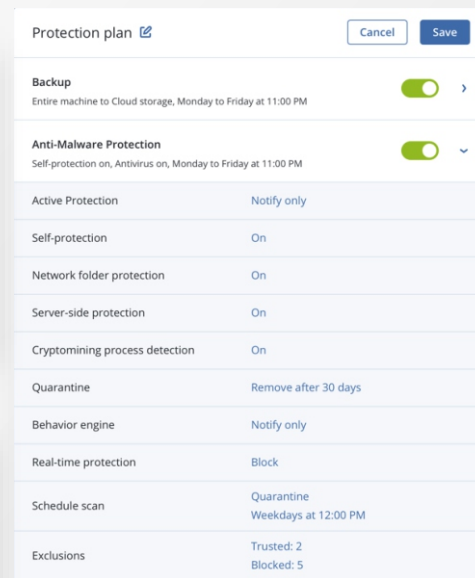
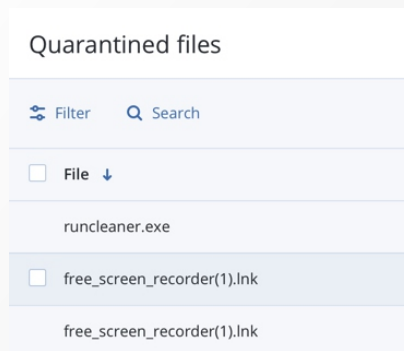
Autoproteção: Proteger os componentes do Acronis (por exemplo, registro, parada de serviço, proteção de arquivos Acronis).

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.

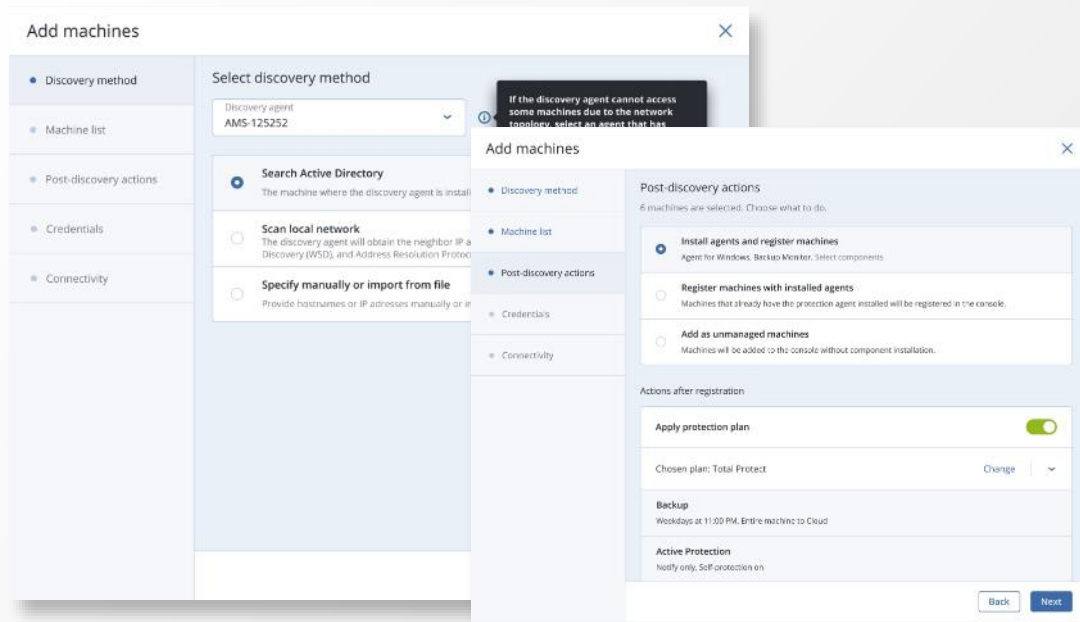
Gerenciamento de exclusões: Especifique processos que não serão considerados malware; excluir pastas onde as alterações de arquivo não serão monitoradas; selecionar arquivos e pastas onde a digitalização programada não será executada.



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 e aplicativos de servidor
 - e) Adobe, Oracle Java
- Navegadores e outros softwares.

BRASP Cyber Cloud

Vulnerabilities

Install patches. 4 items selected

Name	Affected products	Machines	Severity	Patches
<input checked="" type="checkbox"/> CVE-2018-209654	Chrome, Firefox	12	CRITICAL	—
<input checked="" type="checkbox"/> CVE-2018-1000016	Office 2010	3	HIGH	2
<input type="checkbox"/> CVE-2018-1003	Acrobat Reader	3	HIGH	2
<input type="checkbox"/> CVE-2018-100047	Flash Player for Chrome, Flash PL...	7	MEDIUM	—
<input checked="" type="checkbox"/> CVE-2018-3223	Windows Server 2016	14	LOW	1
<input type="checkbox"/> CVE-2018-0900	Office 365 Client	9	NONE	3
<input checked="" type="checkbox"/> CVE-2018-337864	Firefox	3	NONE	1

Reset to default Cancel Done

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

BRASP Cyber Cloud

Patches

Name	Severity	Affected products
Flash Player Plugin	CRITICAL	Chrome
Flash Player Plugin	HIGH	Office 2010
Optional update for Reader	HIGH	Acrobat Reader
Security Update for Microsoft...	MEDIUM	Flash Player for
Definition update for Window...	LOW	Windows Server
Definition update for Window...	NONE	Office 365 Client
Java Runtime Environment 7J...	NONE	Firefox

Products to update

Products	Category	Severity	Approval status
Windows 10	Custom	Custom	Custom
Windows Server 2008R2	9 items selected	Critical	All
Windows Server 2012	All		
Windows Server 2012R2	Critical updates	Critical	All
Windows Server 2016	Drivers		
Office 2010	Feature packs	All	Approved
Office 2013	Security packs	All	Not defined
Office 2015	Service packs		
Office 365 Client	Tools		

Schedule

Schedule this task manually, then following events:
Schedule by time

Schedule type: Daily
Days: Mon, Tue, Wed, Thu, Fri, Sat, Sun
Start at: 02:00 PM

Run within a date range

Start conditions

Reboot after update: If required

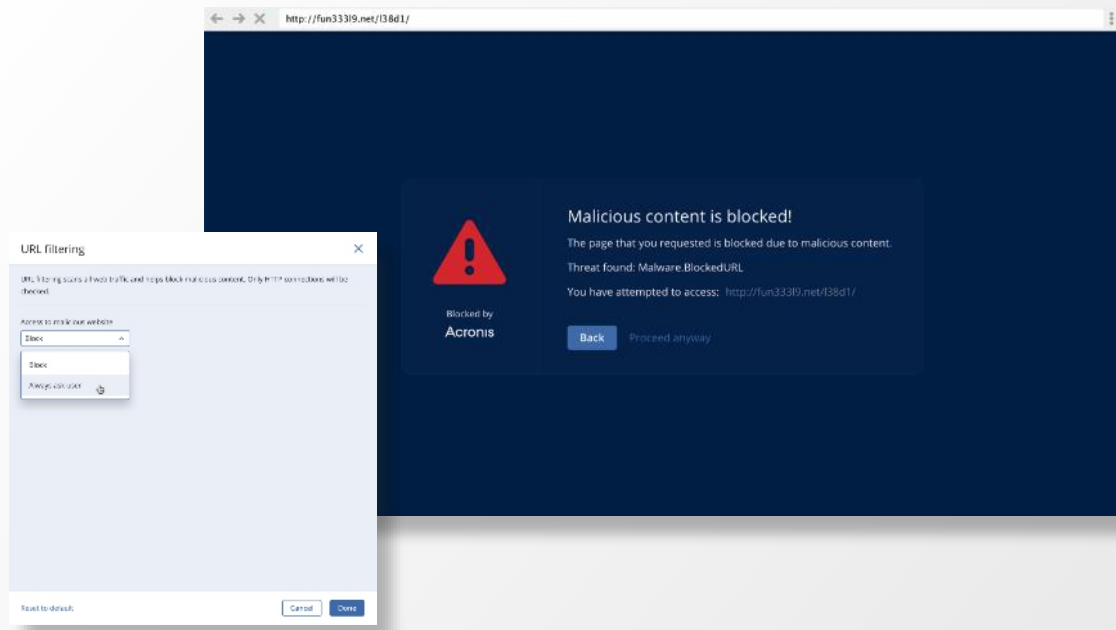
If required: Never, Always

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

The screenshot displays the BRASP Cyber Cloud interface. On the left is a dark navigation sidebar with menu items: DASHBOARD, DEVICES, PLANS, DISASTER RECOVERY, ANTI-MALWARE PROTECTION, SOFTWARE MANAGEMENT, BACKUP STORAGE, REPORTS, and SETTINGS. The main content area is titled 'All devices' and contains a search bar and a table of devices. The table has columns for 'Type' and 'Name'. The device 'DESKTOP-GLN477D' is selected and highlighted. To the right, a detailed view for 'DESKTOP-GLN477D' is shown, featuring tabs for OVERVIEW, PLANS, DETAILS, SOFTWARE, HARDWARE, and ACTIVITIES. The 'HARDWARE' tab is active, displaying a 'Last hardware scan' of 'Mar 31, 13:00' and a 'Scan now' button. Below this, two hardware components are listed: 'Motherboard' and 'Processors'. The Motherboard section shows details: Name (Z170X), Manufacturer (Gigabyte Technology Co. Ltd.), Model (Z170X Gaming), and Serial number (132-LF-E657). The Processors section shows details for an Intel(R) Core(TM) i5-9600K CPU: Manufacturer (Intel Corporation), Model (9600K), Max clock speed (3.7 GHz), and Number of cores (4 Cores, 8 Logical Processors).

Type	Name
VM	qa-gw3t68hh
VM	MF_2012_R2
VM	10.250.194.111
VM	Oracle 11 Linux
	APanin CentOS7
	vm-sql_2012
VM	DESKTOP-GLN477D
VM	qa-gw3t68hh
	dc_w2k12_r2
	τ
	10.250.210.89
	HyperV_for12A

Motherboard	
Name	Z170X
Manufacturer	Gigabyte Technology Co. Ltd.
Model	Z170X Gaming
Serial number	132-LF-E657

Processors	
Intel(R) Core(TM) i5-9600K CPU	
Manufacturer	Intel Corporation
Model	9600K
Max clock speed	3.7 GHz
Number of cores	4 Cores, 8 Logical Processors

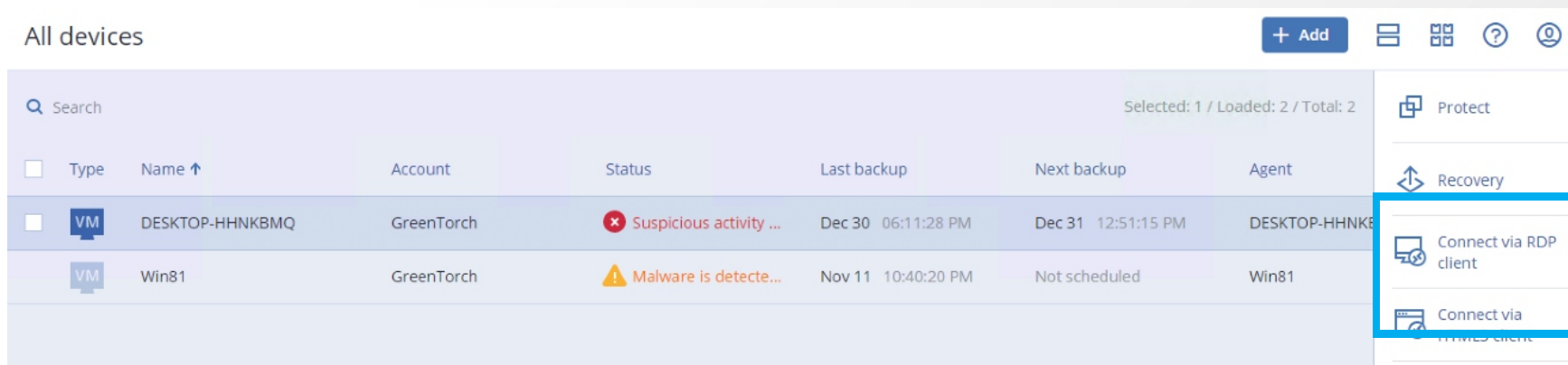
Porque? Economize tempo e esforço com informações atualizadas de inventário de hardware.

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.



The screenshot shows a web interface for managing devices. At the top, it says "All devices" with a "+ Add" button and several utility icons. Below is a search bar and a table of devices. The table has columns for checkboxes, Type, Name, Account, Status, Last backup, Next backup, and Agent. Two devices are listed: "DESKTOP-HHNKBMQ" and "Win81". The first device has a red status icon and text "Suspicious activity ...". The second device has a yellow status icon and text "Malware is detecte...". To the right of the table is a context menu with options: "Protect", "Recovery", "Connect via RDP client", and "Connect via". The "Connect via RDP client" option is highlighted with a blue box.

<input type="checkbox"/>	Type	Name ↑	Account	Status	Last backup	Next backup	Agent
<input type="checkbox"/>	VM	DESKTOP-HHNKBMQ	GreenTorch	⊗ Suspicious activity ...	Dec 30 06:11:28 PM	Dec 31 12:51:15 PM	DESKTOP-HHNK...
<input type="checkbox"/>	VM	Win81	GreenTorch	⚠ Malware is detecte...	Nov 11 10:40:20 PM	Not scheduled	Win81

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

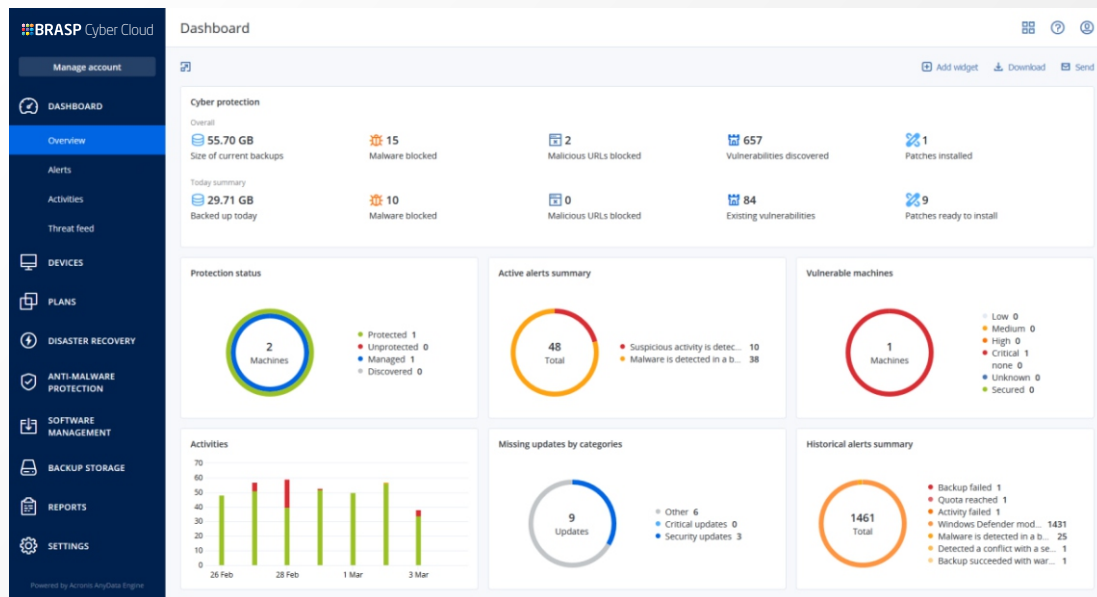
The screenshot shows the 'Cyber Protection Plan' configuration window. At the top right, there are 'Cancel' and 'Save' buttons. The main area lists several protection features, each with a toggle switch and a right-pointing arrow:

- Backup**: Disks/volumes to Cloud storage, Monday to Friday at 10:30 AM + CDP. Toggle is ON.
- Anti-malware Protection**: Self-protection on, Real-time protection on, at 02:20 PM, Sunday through Saturday. Toggle is ON.
- URL filtering**: Always ask user. Toggle is ON.
- Windows Defender Antivirus**: Full scan, Real-time protection on, at 12:00 PM, only on Friday. Toggle is OFF.
- Microsoft Security Essentials**: Full scan, at 12:00 PM, only on Friday. Toggle is OFF.
- Vulnerability assessment**: Microsoft products, Windows third-party products, at 01:40 PM, only on Monday. Toggle is ON.
- Patch management**: Microsoft and other third-party products, at 02:35 PM, only on Monday. Toggle is ON.
- Data protection map**: 66 extensions, at 04:00 PM, Monday through Friday. Toggle is ON.

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

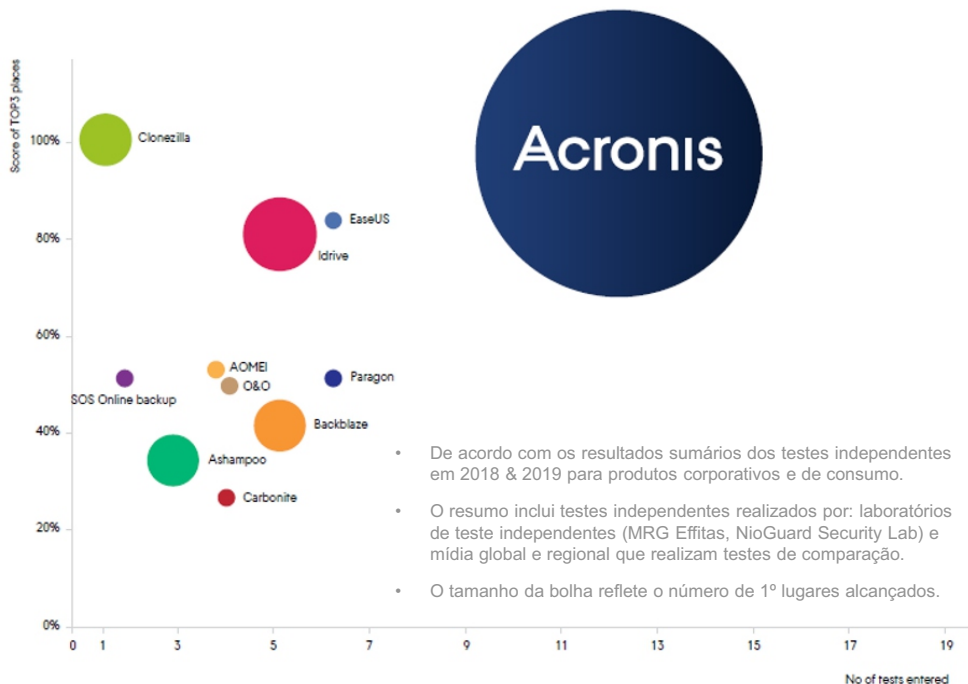
Advanced Security:

- ✓ 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 endpoints 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



- 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.





 **BRASP** Cyber Cloud

Acronis