ILUSTRE SR. PREGOEIRO DO TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ - TJCE

Ref**.** *Processo n. 8517998-37.2023.8.06.0000*. Pregão Eletrônico n° 023/2023.

SCANSOURCE BRASIL DISTRIBUIDORA DE TECNOLOGIAS LTDA., sociedade empresária limitada, inscrita sob o CNPJ nº 05.607.657/0001-35, com sede na Avenida Rui Barbosa, 2529, CEP: 83.055-320, Bairro Ipê, São José dos Pinhais/PR (doravante “**SCANSOURCE**” ou “**RECORRIDA**”), neste ato representada na forma de seu contrato social, vem, respeitosamente, com fundamento no Item 9.1[1] do Edital do Pregão Eletrônico n° 023/2023 apresentar

CONTRARRAZÕES AO RECURSO ADMINISTRATIVO

interposto por **CLM SOFTWARE COMÉRCIO IMPORTAÇÃO E EXPORTAÇÃO LTDA.** (“**CLM**” ou “**RECORRENTE**”"), em face da decisão que declarou a ora Recorrida habilitada e vencedora no bojo dos autos da licitação em epígrafe, o que faz com base nas razões de fato e de direito a seguir expostas.

[1] *“ 9.1. Do ato que encerra o julgamento das propostas ou do ato de habilitação ou inabilitação de licitante, o proponente que desejar recorrer contra decisões do(a) Pregoeiro(a), poderá fazê-lo de imediato e motivadamente, até 2 (duas) horas do mencionado ato, manifestando sua intenção com o registro da síntese das suas razões, exclusivamente no âmbito do sistema eletrônico, sendo-lhe concedido prazo de 3 (três) dias para apresentar por escrito as razões do recurso, conforme o art. 165 da Lei nº 14.133, de 2021, devidamente protocolizadas no Tribunal de Justiça do Estado do Ceará, no endereço eletrônico constante no preâmbulo deste edital. Os demais licitantes ficam, desde logo, convidados a apresentar contrarrazões em igual número de dias, que começarão a correr da data da intimação pessoal ou da divulgação da interposição do recurso”.*

I. DA TEMPESTIVIDADE

1. O recurso administrativo foi interposto pela RECORRENTE em 21/02/2024 (quarta-feira), razão pela qual o termo final do prazo de 3 (três) dias úteis para protocolo das presentes contrarrazões, *vide* item 9 do edital, encerra-se em 26/02/2024 (segunda-feira).

2. Com o protocolo na presente data, torna-se inequívoca a **tempestividade** das contrarrazões recursais ora apresentadas.

II. DA SÍNTESE FÁTICA E DO RECURSO APRESENTADO

3. O Pregão Eletrônico n° 023/2024 tem como objeto a contratação de empresa especializada no *"fornecimento de licenças de software de cópias de proteção, armazenamento de dados para backup em equipamentos e nuvem e serviços de instalação, configuração e treinamento"*, a fim de atender as necessidades do Tribunal de Justiça do Estado do Ceará - TJCE, conforme condições estipuladas no edital e em seus anexos.

4. A SCANSOURCE, após cautelosa análise de sua equipe técnica junto ao parceiro, encaminhou sua proposta contendo a solução da *Commvault*, tendo em vista que cumpre com todas as exigências técnicas exigidas no certame. Ao ensejo, a empresa é referência do segmento tecnológico a nível global, **e nos últimos anos tem ganhado cada vez maior destaque**, **o que é comprovado com uma série de prêmios recebidos em matéria de inovação e qualidade**[2].

5. Em 16.02.2024, em cumprimento às disposições estabelecidas do instrumento convocatório, foi realizada a sessão pública em que as licitantes puderam fazer seus respectivos lances, os quais foram julgados sob o critério de Menor Preço.

5. Na oportunidade, verificou-se que a proposta da SCANSOURCE apresentou as melhores condições e os menores valores dentre as demais, razão pela qual o órgão procedeu com a análise do objeto ofertado e solicitou o envio dos documentos de habilitação e da Proposta Comercial atualizada, *vide* termos do item 4.51 do edital.

[2] Conforme verifica-se no seguinte link: *https://www.commvault.com/awards*. Acesso em 26/02/2014.

6. Contudo, incomodada com o resultado, a CLM interpôs recurso administrativo visando a reforma da decisão, sob a alegação de que a SCANSOURCE deveria ser desclassificada, tendo em vista que sua Proposta Comercial supostamente não teria cumprido com as especificações técnicas dispostas no Termo de Referência.

7. Em seu recurso genérico e desprovido de fundamentos, a RECORRENTE se limita a afirmar que o *"HPE Proliant DL380"* não apresentaria *"as métricas de desempenho de taxa de transferência"* demandados, pois *"não possui evidências de seu desempenho expresso em TB/hora/"*, e que referido equipamento não possibilitaria o *backup* de *Oracle, MSSQL* e *database dump* de modo direto e *"sem consumo de licenças do software de backup"*, em suposta violação às exigências do instrumento convocatório.

8. Com a devida vênia, trata-se de mero inconformismo pelo fato de a SCANSOURCE apresentou a proposta mais vantajosa ao Poder Público, eis que o corpo técnico do órgão licitante já comprovou o atendimento de todos os requisitos demandados no certame.

9. Nada obstante, em prestígio à cooperação, a RECORRIDA confirma, nos tópicos adiante, que a solução ofertada preenche as exigências do instrumento convocatório e, consequentemente, a total improcedência dos pontos suscitados pela RECORRENTE.

III. CONTRARRAZÕES RECURSAIS

III.1 DO INEQUÍVOCO CUMPRIMENTO DOS REQUISITOS DO EDITAL

10. A RECORRENTE discorre que a solução apresentada não atenderia às exigências da licitação, tendo em vista que equipamento HPE Proliant DL380 e seus componentes *(i)* não apresentariam as métricas de desempenho de taxa de transferência em TB/hora; *(ii)* não possibilitaria o *backup* de *Oracle, MSSQL* e *data base dump*, de modo direto, ao equipamento ofertado e dependeria do consumo de licenças; *(iii)* e não permitiria a separação de volumes de dados através da funcionalidade de air-gap físico ou virtual. Por isso, a solução não observaria o que consta nos itens 3.7, 3.18, 3.19, 3.36 e 3.48.3 do edital da licitação.

Ba sb
BA sb

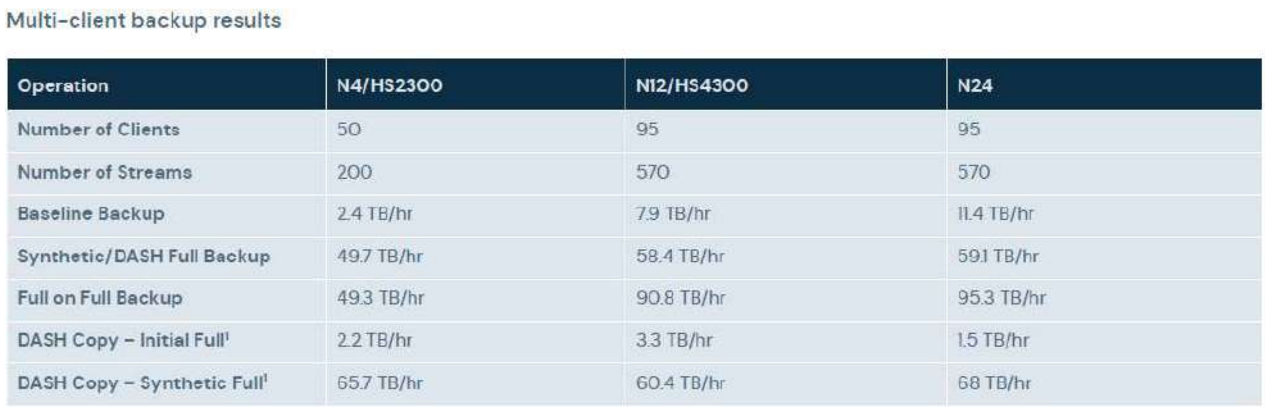
11. Ocorre que, ao contrário do que pretende induzir a CLM, o objeto licitado corresponde a solução composta por *software* e *hardware*, a qual, por consequência lógica, deve ser analisada em todo o seu conjunto, eis que, na prática, deve garantir o atendimento às necessidades institucionais do órgão licitante.

12. Em evidente observância às descrições do edital, a SCANSOURCE apresentou em sua Proposta Comercial a solução denominada *"Hyperscale-X"*, a qual é composta pelos servidores *"HPE DL380"* – o hardware da solução – e por *storage* definido pelo *software* da *Commvault*.

13. No entanto, ao pretender induzir esta Comissão Permanente de Licitação a erro, a CLM, promoveu com a análise de apenas ***um*** dos componentes da solução ofertada e não do conjunto de elementos inerentes à solução – que, como informado, compõe-se de *hardware* e *software*. Somente descrições relativas ao *hardware* de um único servidor foram mencionadas, ignorando os descritivos de outros itens constantes do *"Hyperscale-X"*.

14. Não há dúvidas de que a solução atende integralmente às métricas exigidas pelo instrumento convocatório, relativas à medição por TB/h, fator que consta pormenorizadamente especificado no descritivo de performance da solução, o *"Commvault® HyperScale X™ Performance"*, **documento oficial** emitido pela própria *Commvault* e ora anexo às presentes Contrarrazões.

15. Referido arquivo demonstra, em tópico denominado *"Performance Tests"* tais apontamentos e, após ilustrar que os testes de desempenho da solução são utilizados com base em uma variedade de diferentes operações, no subtópico *"Multi-client backup results"*, consta a seguinte tabela:



Multi-client backup results

Operation	N4/HS2300	N12/HS4300	N24
Number of Clients	50	95	95
Number of Streams	200	570	570
Baseline Backup	2.4 TB/hr	7.9 TB/hr	11.4 TB/hr
Synthetic/DASH Full Backup	49.7 TB/hr	58.4 TB/hr	59.1 TB/hr
Full on Full Backup	49.3 TB/hr	90.8 TB/hr	95.3 TB/hr
DASH Copy – Initial Full[1]	2.2 TB/hr	3.3 TB/hr	1.5 TB/hr
DASH Copy – Synthetic Full[1]	65.7 TB/hr	60.4 TB/hr	68 TB/hr

Ba BA sb sb

16. Com isso, confirma-se que o *"Synthetic/DASH Full Backup"* possui as mesmas métricas suscitadas nos itens referenciados pela CLM em suas razões recursais. E as mesmas taxas de transferência para operações de *backup* são possíveis em *terabytes* por hora.

17. A propósito, cumpre ressaltar que a solução proposta pela SCANSOURCE traz flexibilidade de liberdade para que o cliente escolha o *hardware* de menor custo e que melhor atenda às suas necessidades. Também se observa que em futuras expansões a solução agregará volume, performance e maior resiliência – ao contrário das demais ofertadas, as quais só entregam volume.

18. O mesmo se confirma em relação ao consumo de licenças, as quais se encontram devidamente contempladas na solução: há total suporte a CIFS e NFS. É o que se constata na página oficial da *Commvault*, em documento denominado *"Hybrid File Store Data Protection Overview"*. Senão, vejamos o que afirma o arquivo:

> *"Os usuários* ***não precisam realizar nenhuma operação adicional*** *para proteger os dados armazenados no compartilhamento do Hybrid File Store.*
>
> *Quando os usuários gravam dados no Hybrid File Store usando o protocolo NFS ou SMB, o software Commvault envia automaticamente os dados para o Commvault Content Store. Os dados seguem as regras de retenção definidas para a política de subcliente associada ao Armazenamento de Arquivos Híbridos.*
>
> *Quando os usuários leem dados do Hybrid File Store, o software Commvault recupera automaticamente os dados do Commvault Content Store e os apresenta aos usuários.*
>
> *Se um usuário precisar de acesso aos dados por um horário específico, o administrador criará uma visualização pontual somente leitura do Armazenamento de Arquivos Híbridos especificado que reflete os dados antes do horário especificado. Os usuários podem montar a visualização pontual e, em seguida, recuperar os dados"*[3].

19. Por isso tudo, não prospera a alegação de que referidas licenças se encontram plenamente disponibilizadas por meio da solução apresentada.

20. Não bastasse, a CLM afirma que a solução não permite a separação de volumes de dados através da funcionalidade de air-gap físico ou virtual, eis que *"não indica qual metodologia será usada e nem fornece os componentes do ambiente isolado"*.

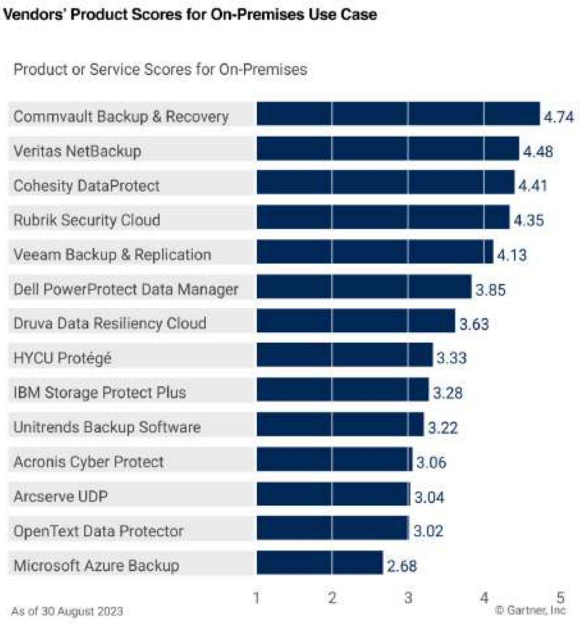
[3] Conforme texto disponível na página oficial da *Commvault*, cujo teor, em sua íntegra, pode ser conferido no seguinte link: *https://documentation.commvault.com/2023e/essential/hybrid_file_store_data_protection_overview.html.* Acesso em 26/02/2024.

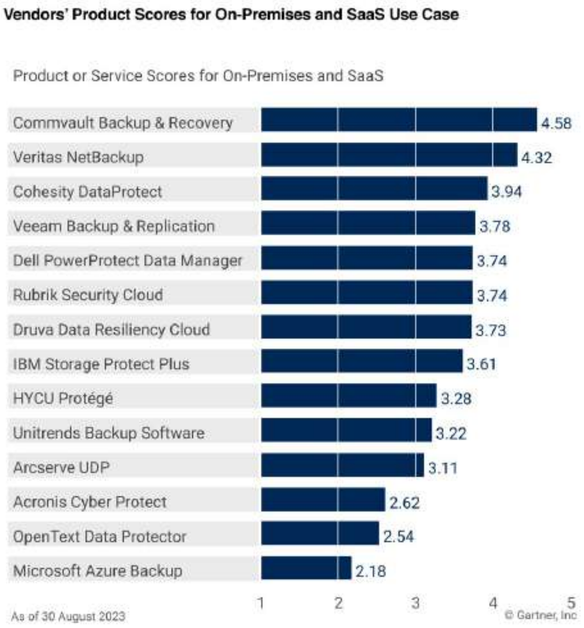
Ba
BA

sb
sb

21. No ponto, ao contrário do que pretende ilustrar a licitante, a real preocupação do órgão licitante é com a efetiva segurança dos dados a serem disponibilizados e manejados por meio da solução, o que é integralmente cumprido com o *Hyperscale-X*.

22. Ao ensejo, essencial destacar que a ***Commvault* é um dos líderes do Gartner em Segurança e Proteção de Dados**. No ano de 2023, a empresa obteve a pontuação mais alta em 6 (seis) dos 7 (sete) casos de uso descritos no *Relatório de Capacidades Críticas*[4], conforme relação a seguir:

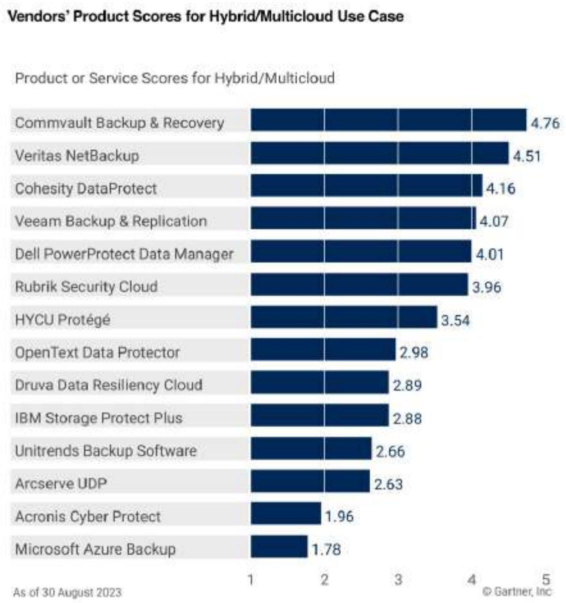


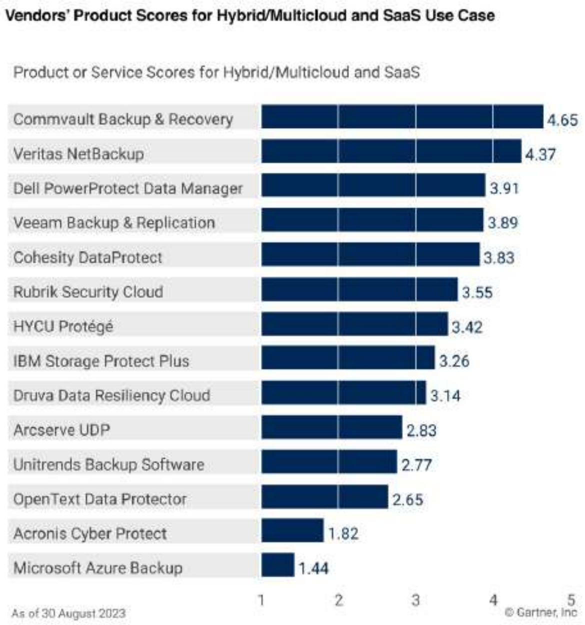


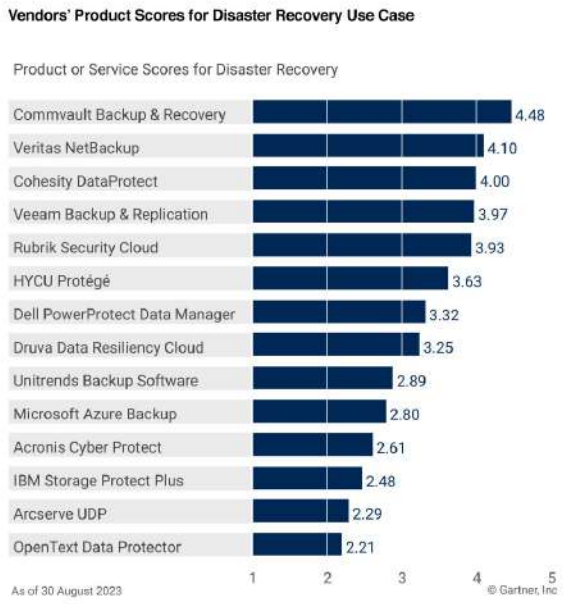
[4] A respeito, conferir: *https://www.commvault.com/blogs/recognized-again-in-gartner-critical-capabilities.* Acesso em 26/02/2024.

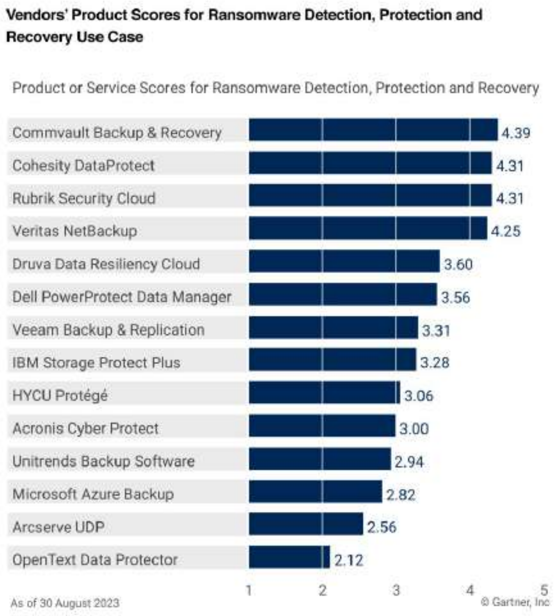
Ba
BA

sb
sb


Vendors' Product Scores for Hybrid/Multicloud Use Case


Vendors' Product Scores for Hybrid/Multicloud and SaaS Use Case


Vendors' Product Scores for Disaster Recovery Use Case


Vendors' Product Scores for Ransomware Detection, Protection and Recovery Use Case

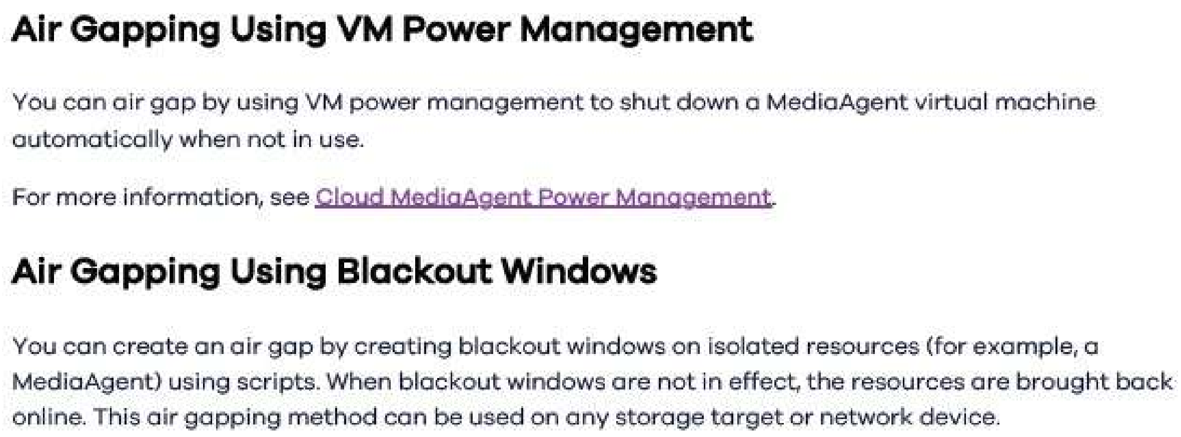
23. Tais fatores comprovam que a qualidade dos atributos contemplados na solução proposta pela SCANSOURCE, conforme parâmetros estabelecidos pelo Gartner, cujos estudos são largamente utilizados a fim de subsidiar a tomada de decisões em contratos de tecnologias.

24. Além do mais, conforme se comprova pela documentação anexa, o volume de armazenamento do *Hyperscale-X* é imutável, sem perda de performance e resiliência, ao contrário de outras soluções que consomem maiores recursos. Além de *feature* de imutabilidade, a *Commvault*

Ba sb
BA sb

permite a utilização de *WORM* sem custos ou *hardwares* adicionais, e como se observa, pairam opções em que entregas podem ser realizadas via *software* e sem a necessidade de soluções adicionais.

25. A respeito disso, vejamos o que consta no documento *"Data Isolation and Air Gapping"*, o qual contextualiza o *AirGap* em sua fl. 06:



Air Gapping Using VM Power Management

You can air gap by using VM power management to shut down a MediaAgent virtual machine automatically when not in use.

For more information, see Cloud MediaAgent Power Management.

Air Gapping Using Blackout Windows

You can create an air gap by creating blackout windows on isolated resources (for example, a MediaAgent) using scripts. When blackout windows are not in effect, the resources are brought back online. This air gapping method can be used on any storage target or network device.

26. Diante de tais razões, resta plenamente demonstrado e comprovado que a solução ofertada pela SCANSOURCE atende, de modo integral, as especificações técnicas constantes no instrumento convocatório.

III.2. NECESSIDADE DE MANUTENÇÃO DO RESULTADO FINAL. PRINCÍPIOS DO JULGAMENTO OBJETIVO E BUSCA PELA PROPOSTA MAIS VANTAJOSA.

27. O julgamento objetivo determina que o Poder Público se paute em critérios previamente estabelecidos no edital da licitação ao analisar as propostas. Referido princípio deve ser o norte de toda atuação administrativa.

28. No caso, o instrumento convocatório é expresso ao dispor que a licitação possui como critério de julgamento o Menor Preço Global, motivo pelo qual, verificado o cumprimento dos parâmetros técnicos exigidos, a proposta com o menor valor será a mais vantajosa e, por consequência, declarada a vencedora.

Ba sb
BA sb

29. Nesse mesmo sentido discorre o art. 34 da Lei nº 14.133/2021, segundo o qual: *"O julgamento por **menor preço** ou maior desconto e, quando couber, por técnica **e preço considerará o menor dispêndio para a Administração, atendidos os parâmetros mínimos de qualidade definidos no edital de licitação**".*

30. Com isso, demonstrado o integral atendimento às especificações técnicas constantes no Termo de Referência, conforme demonstrado por meio dos *links* e da documentação oficial anexa, não pairam razões para que o resultado do julgamento da licitação se mantenha.

31. Como é de conhecimento do órgão, a proposta ofertada pela SCANSOURCE corresponde ao montante de R$ 7.209.000,00 (sete milhões e duzentos e nove mil reais), razão pela qual **representa menos da metade do valor inicialmente estimado para a presente contratação**[5] e, **comparada às demais ofertas**, **representa a maior economia para os cofres públicos**.

32. **Especificamente em relação à CLM, a Proposta Comercial da SCANSOURCE corresponde a mais de R$ 400.000,00 (quatrocentos mil reais) de economia ao Tribunal de Justiça do Estado do Ceará**.

33. Logo, ao se depreender com análise dos propósitos norteadores da licitação, o julgamento objetivo das propostas apenas restaria cumprido com a devida declaração da SCANSOURCE como vencedora do processo licitatório. **Eis que**, **caso contrário**, **o órgão não contratará com a proposta mais vantajosa, de acordo com os preceitos editalícios e legais**.

34. Segundo a Nova Lei de Licitações, um dos principais objetivos do processo licitatório é **assegurar a seleção da proposta apta a gerar o resultado de contratação mais vantajoso** para a Administração Pública.

35. A respeito disso, o Tribunal de Contas da União (TCU) tem jurisprudência consolidada no sentido de que o julgamento objetivo deve ser observado na seleção da proposta mais vantajosa.

> *"[...] A ausência de critérios pré-definidos para seleção da proposta mais vantajosa viola mandamentos básicos da impessoalidade, da isonomia e do julgamento objetivo,*

[5] O valor estimado para a contratação era o de R$ 16.972.214,00 (dezesseis milhões, novecentos e setenta e dois mil, duzentos e quatorze reais),

Ba sb
BA sb

> *[...], podendo, inclusive, dar margem a direcionamentos indevidos nos procedimentos licitatórios.*
>
> *(Acórdão 549/2006 - Plenário. Ministro Relator: Walton Alencar)*
>
> *"[...] A violação de princípios básicos da razoabilidade, da economicidade, da legalidade e da moralidade administrativa, e a desobediência às diretrizes fundamentais da licitação pública, no caso, a isonomia entre licitantes, o julgamento objetivo, a vinculação ao instrumento convocatório, bem como o caráter competitivo do certame constituem vícios insanáveis que ensejam a fixação de prazo para exato cumprimento da lei, no sentido de declarar a nulidade do certame".*
>
> *(Acórdão 6198/2009 - Primeira Câmara. Ministro Relator: Walton Alencar)*
>
> *"[...] A licitação não deve perder seu objetivo principal, que é obter a proposta mais vantajosa à Administração, mediante ampla competitividade".*
>
> *(Acórdão 1734/2009 – Plenário. Ministro Relator: Raimundo Carreiro).*

36. Em complemento a tais disposições, Marçal Justen Filho dispõe que *"[...] a licitação é um instrumento para atingir um resultado, consistente na seleção da melhor proposta possível [...]. Ou seja, realizar uma licitação somente merece aplausos quando atingido o resultado pretendido"*[6].

37. Por fim, comprovado que a proposta apresentada cumpriu, integralmente, com todos os requisitos técnicos do edital e do Termo de Referência - conforme documentação, links e declaração emitida pelo próprio fabricante da solução -, e sendo o critério de julgamento da licitação o Menor Preço Global, não há dúvidas quanto à necessidade de que o resultado da licitação seja efetivamente mantido.

IV. DO PEDIDO

38. Ante ao exposto, a SCANSOURCE requer sejam as presentes contrarrazões conhecidas e providas, a fim de que o recurso apresentado pela CLM não prospere, conforme os fundamentos e esclarecimentos expostos acima.

[6] JUSTEN FILHO, Marçal. *Comentários à Lei de Licitações e Contratações Administrativas*, 2ª ed. São Paulo: Thomson Reuters Brasil, 2023, p. 259.

Nestes termos, pede deferimento.

São Paulo, 26 de fevereiro de 2024.

sandra r b m borba

sandra r b m borba (26 de fevereiro de 2024 18:38 GMT-3)

Bernardo Atamian (26 de fevereiro de 2024 18:33 GMT-3)

SCANSOURCE BRASIL DISTRIBUIDORA DE TECNOLOGIAS LTDA.

Contrarrazões - TJCE - ScanSource x CLM pdf

Relatório de auditoria final 2024-02-26

Criado em:	2024-02-26
Por:	Thamires Monteiro (thamires.monteiro@scansource.com)
Status:	Assinado
ID da transação:	CBJCHBCAABAAPU0g_tr7Hb0CRLj0yhc7GeUxuGpqXtFw

Histórico de "Contrarrazões - TJCE - ScanSource x CLM pdf"

Documento criado por Thamires Monteiro (thamires.monteiro@scansource.com)

2024-02-26 - 21:13:54 GMT

Documento enviado por email para bernardo.atamian@scansource.com para assinatura

2024-02-26 - 21:14:42 GMT

Email visualizado por bernardo.atamian@scansource.com

2024-02-26 - 21:31:09 GMT

O signatário bernardo.atamian@scansource.com inseriu o nome Bernardo Atamian ao assinar

2024-02-26 - 21:33:36 GMT

Documento assinado eletronicamente por Bernardo Atamian (bernardo.atamian@scansource.com)

Data da assinatura: 2024-02-26 - 21:33:38 GMT - Fonte da hora: servidor

Documento enviado por email para sandra.borba@scansource.com para assinatura

2024-02-26 - 21:33:40 GMT

Email visualizado por sandra.borba@scansource.com

2024-02-26 - 21:37:31 GMT

O signatário sandra.borba@scansource.com inseriu o nome sandra r b m borba ao assinar

2024-02-26 - 21:38:50 GMT

Documento assinado eletronicamente por sandra r b m borba (sandra.borba@scansource.com)

Data da assinatura: 2024-02-26 - 21:38:52 GMT - Fonte da hora: servidor

✓ Contrato finalizado.

2024-02-26 - 21:38:52 GMT

Commvault®

Documentation PDF

Protect. Access. Comply. Share.

Data Isolation and Air Gapping

Updated Wednesday, November 29, 2023

Two proven techniques for reducing the attack surface on your backup data are data isolation and air gapping.

Data isolation is a technique that uses secondary and/or tertiary copies of backup storage targets that are segmented and unreachable from the public portions of the environment using virtual LAN (VLAN) switching, next generation firewalls, or zero trust technologies. If your organization is infiltrated by ransomware, or a malicious attacker, the cyber threat will have a limited attack surface. The public portions of the environment may get infected, but the isolated data will not because it cannot be accessed. To be most effective, isolated environments should not be accessible to public networks of the organization as well as the internet. Physical access to isolated resources should be secured and heavily controlled. All inbound network communication is blocked, and only restricted outbound access is allowed. Commvault will then securely tunnel from the isolated storage targets to the Commvault resources and source storage targets for data replication.

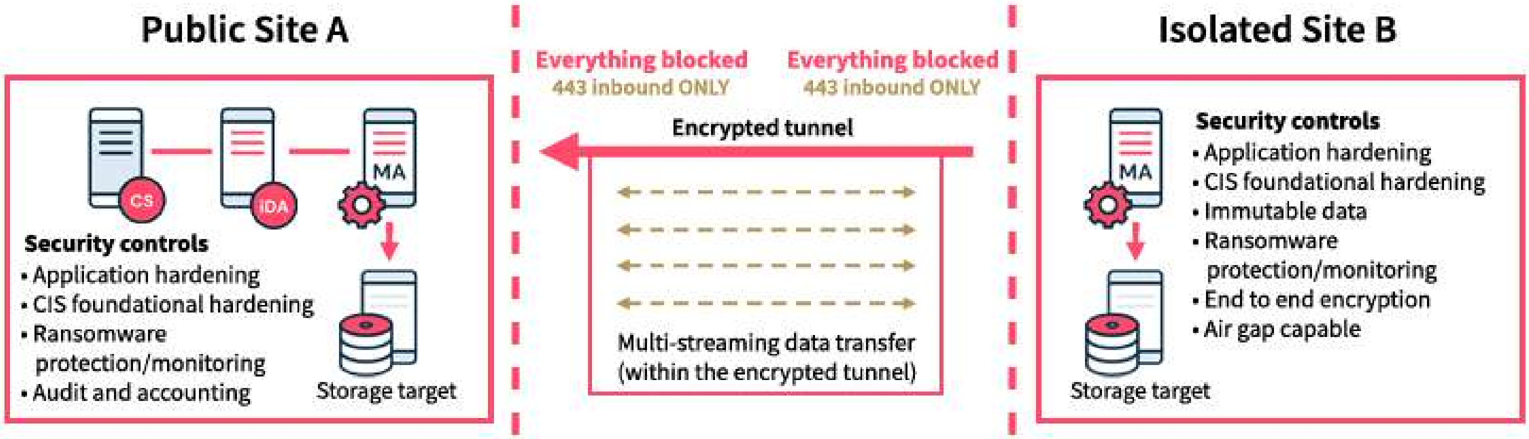
Air gapping is another technique that complements data isolation. Traditionally, air gapped networks have absolutely no connectivity to public networks. Tape is a traditional medium for air gapped backups because tape can be removed from the tape library and stored offsite. To air gap secondary backup targets on disk, or cloud, some access is needed, but when it is not needed, communication is severed. Commvault provides secure replication of data to an isolated environment with air gap capabilities. The isolated environment is completely blocked from all incoming connections. Outgoing connections are restricted, which greatly reduces the attack surface of cyber threats. Once data is fully replicated, the connection can be severed, and the secondary data becomes air gapped until data needs to replicate again or recovered.

How They Work

Commvault’s network topology and workflow engine provide the basis for configuring data isolation and air gap solutions.

Data Isolation Using a Direct Connection

The figure below represents the overall high-level functionality of Commvault data isolation using a direct connection.



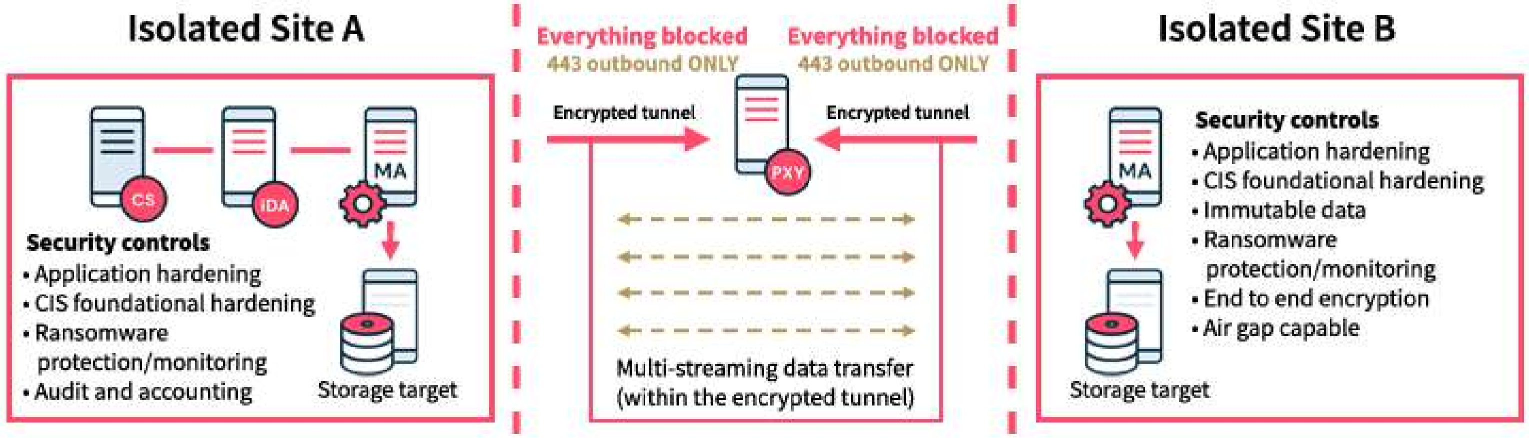
Site A represents the public portion of the production backup environment. Site B is a segmented portion of the environment, isolated logically and physically. Site B communicates through the firewall over a single outbound port, and everything else is blocked. The tunnel supports HTTPS encapsulation using the TLS 1.3 protocol, and will connect only when certificate authentication is successful. This protects against man-in-the-middle and spoofing attacks.

Data transfer is multi-streamed through the tunnel to ensure the fastest backup possible. Data residing on the storage target on Site B is protected from ransomware and accidental deletion by utilizing Commvault's security controls, encryption, WORM and native ransomware locks for immutable storage. Data replication is deduplicated to further optimize bandwidth and storage considerations.

Once data transfer is complete, connectivity can be severed by turning off routing, enabling firewall rules, or shutting systems down. Severing the connection can be scheduled around VM power management, or blackout windows.

Data Isolation Using a Proxy-Based Connection

A proxy-based configuration, as shown in the figure below, has the same ransomware and encryption benefits as a direct connection. However, in a proxy-based configuration, both sites communicate between each other using a proxy located between the isolated and public networks. All inbound connectivity is blocked between the sites, providing isolation capabilities on both sites. Proxy-based configurations are very common, especially when data is moving between remote geographic locations across the internet.



Air Gapping

The simplest method of air gapping is to use VM power management, a Commvault capability that automatically shuts down a MediaAgent virtual machine when not in use. The VM only starts up when needed. This method requires a hypervisor in the isolated environment and does not need additional scripts.

Another method of air gapping is to create blackout windows using scripts and workflows. Blackout windows are defined time frames when backup and administrative tasks are not allowed to run on isolated resources. When blackout windows are not in effect, the resources are brought online using scheduled scripts included on the air gapped resource (such as the MediaAgent). This air gapping method can be used on any storage target or network device.

The downside to air gapping is planning around recovery point objectives (RPOs), because when resources are turned off, data replication will not run. Depending on the environment, resources, and service level requirements, data replication will queue when destination targets are offline. To help reduce the effects of this downside, Commvault incorporates multi-streaming within the one-way encrypted tunnel to maximize backup performance.

Data Isolation

Updated Tuesday, November 14, 2023

You can isolate data by using direct connections or proxy-based connections to/from isolated storage targets and Commvault resources.

Direct Connections

You can use predefined network topology types when setting up network connections between client groups.

The client groups use a network topology instance to establish connections between each other, either in one direction, or in both directions. The clients in the client groups can be the CommServe computer, MediaAgents, or client computers.

For more information, see Direct Connections Using Predefined Network Topologies.

Proxy-Based Connections

You can establish port forwarding at the gateway to forward connections received by specific gateway ports to clients on the internal network. You can then configure the clients to open a direct connection to the port-forwarder’s IP address on a specific port to reach a particular internal server. This creates a custom route from the client towards the internal servers.

A port-forwarding gateway sends incoming connections to specific machines on the internal network based on the incoming connection’s destination port number.

For more information, see Port-Forwarding Gateway.

Air Gapping

Updated Wednesday, November 29, 2023

You can air gap isolated data by severing communication with the machine that contains or manages the data.

Air gapping can be achieved by using one of the following methods:

- Use VM power management to automatically shut down a MediaAgent virtual machine when not in use.
- Create blackout windows on storage targets or network devices using scripts and workflows.

Air Gapping Using VM Power Management

You can air gap by using VM power management to shut down a MediaAgent virtual machine automatically when not in use.

For more information, see Cloud MediaAgent Power Management.

Air Gapping Using Blackout Windows

You can create an air gap by creating blackout windows on isolated resources (for example, a MediaAgent) using scripts. When blackout windows are not in effect, the resources are brought back online. This air gapping method can be used on any storage target or network device.

Procedure 1: Starting and Stopping Outbound Connections to a MediaAgent

You can start and stop outbound connections to a MediaAgent using a one-way topology, in order to create an air gap.

1. Create a blackout window to control when you want connections established on the MediaAgent.

   For more information, see Blackout Window.

2. Use commands to turn services on and off, as follows:

   - For Windows, do the following:

     - Create a task schedule that runs the following command to stop services at the beginning of the blackout window:

       <Path to Commvault Base Directory>`\gxadmin -stopsvcgrp “All” -console`

     - Create another task schedule that runs the following command to start services at the end of the blackout window:

<Path to Commvault Base Directory>`\gxadmin -startsvcgrp "All" -console`

- For UNIX, do the following:
  - Create a cron job that runs the following command to stop services at the beginning of the blackout window:

    ```
    commvault -all stop
    ```

  - Create another cron job that runs the following command to start services at the end of the blackout window:

    ```
    commvault -all start
    ```

Procedure 2: Starting and Stopping a Network Gateway to Create an Air Gap

You can use the **Airgap** workflow to start or stop network gateway proxies to create an air gap. This workflow can be scheduled to run at the beginning of the auxiliary copy blackout window to stop the gateway machines and at the end of the blackout window to start the gateway machines.

For more information, see Starting or Stopping a Network Gateway to Create an Air Gap.

Virtual Air Gap Using Metallic Recovery Reserve

You can create a virtual air gap by using Metallic Recovery Reserve.

Since connections to Metallic Recovery Reserve rely on authenticated APIs once data is written to the them, there are no persistent connections to the storage, thus reducing the chance of infection by a potential threat.

Using Metallic Recovery Reserve as a virtual air gap has a further advantage, since credentials are not provided and there is no direct access to the storage accounts.

Data Isolation

Updated Tuesday, November 14, 2023

You can isolate data by using direct connections or proxy-based connections to/from isolated storage targets and Commvault resources.

Direct Connections

You can use predefined network topology types when setting up network connections between client groups.

The client groups use a network topology instance to establish connections between each other, either in one direction, or in both directions. The clients in the client groups can be the CommServe computer, MediaAgents, or client computers.

For more information, see Direct Connections Using Predefined Network Topologies.

Proxy-Based Connections

You can establish port forwarding at the gateway to forward connections received by specific gateway ports to clients on the internal network. You can then configure the clients to open a direct connection to the port-forwarder's IP address on a specific port to reach a particular internal server. This creates a custom route from the client towards the internal servers.

A port-forwarding gateway sends incoming connections to specific machines on the internal network based on the incoming connection's destination port number.

For more information, see Port-Forwarding Gateway.

Air Gapping

Updated Wednesday, November 29, 2023

You can air gap isolated data by severing communication with the machine that contains or manages the data.

Air gapping can be achieved by using one of the following methods:

- Use VM power management to automatically shut down a MediaAgent virtual machine when not in use.
- Create blackout windows on storage targets or network devices using scripts and workflows.

Air Gapping Using VM Power Management

You can air gap by using VM power management to shut down a MediaAgent virtual machine automatically when not in use.

For more information, see Cloud MediaAgent Power Management.

Air Gapping Using Blackout Windows

You can create an air gap by creating blackout windows on isolated resources (for example, a MediaAgent) using scripts. When blackout windows are not in effect, the resources are brought back online. This air gapping method can be used on any storage target or network device.

Procedure 1: Starting and Stopping Outbound Connections to a MediaAgent

You can start and stop outbound connections to a MediaAgent using a one-way topology, in order to create an air gap.

1. Create a blackout window to control when you want connections established on the MediaAgent.

   For more information, see Blackout Window.

2. Use commands to turn services on and off, as follows:

   - For Windows, do the following:

     - Create a task schedule that runs the following command to stop services at the beginning of the blackout window:

       <Path to Commvault Base Directory>`\gxadmin -stopsvcgrp “All” -console`

     - Create another task schedule that runs the following command to start services at the end of the blackout window:

<Path to Commvault Base Directory> `\gxadmin -startsvcgrp "All" -console`

- For UNIX, do the following:
    - Create a cron job that runs the following command to stop services at the beginning of the blackout window:

      ```
      commvault -all stop
      ```

    - Create another cron job that runs the following command to start services at the end of the blackout window:

      ```
      commvault -all start
      ```

Procedure 2: Starting and Stopping a Network Gateway to Create an Air Gap

You can use the **Airgap** workflow to start or stop network gateway proxies to create an air gap. This workflow can be scheduled to run at the beginning of the auxiliary copy blackout window to stop the gateway machines and at the end of the blackout window to start the gateway machines.

For more information, see Starting or Stopping a Network Gateway to Create an Air Gap.

Virtual Air Gap Using Metallic Recovery Reserve

You can create a virtual air gap by using Metallic Recovery Reserve.

Since connections to Metallic Recovery Reserve rely on authenticated APIs once data is written to the them, there are no persistent connections to the storage, thus reducing the chance of infection by a potential threat.

Using Metallic Recovery Reserve as a virtual air gap has a further advantage, since credentials are not provided and there is no direct access to the storage accounts.

Commvault®

For more information about Commvault® softwaremodules and solutions,
and for up-to-date system requirements, please contact us:
www.commvault.com | 888.746.3849 | get-info@commvault.com

CommvaultWorldwide Headquarters
1 Commvault Way | Tinton Falls, NJ07724 | Phone: 888.746.3849 | Fax: 732.870.4525

Commvault Regional Offices
United States | Europe | Middle East & Africa | Asia-Pacific | Latin America & Caribbean | Canada | India | Oceania

GARTNER

Recognized Again! Commvault Ranked Highest in Six out of Seven Use Cases in the 2023 Gartner® Critical Capabilities for Enterprise Backup and Recovery Software Solutions

Commvault Backup & Recovery has scored the highest in six of the seven Use Cases in the 2023 Gartner® Critical Capabilities report.

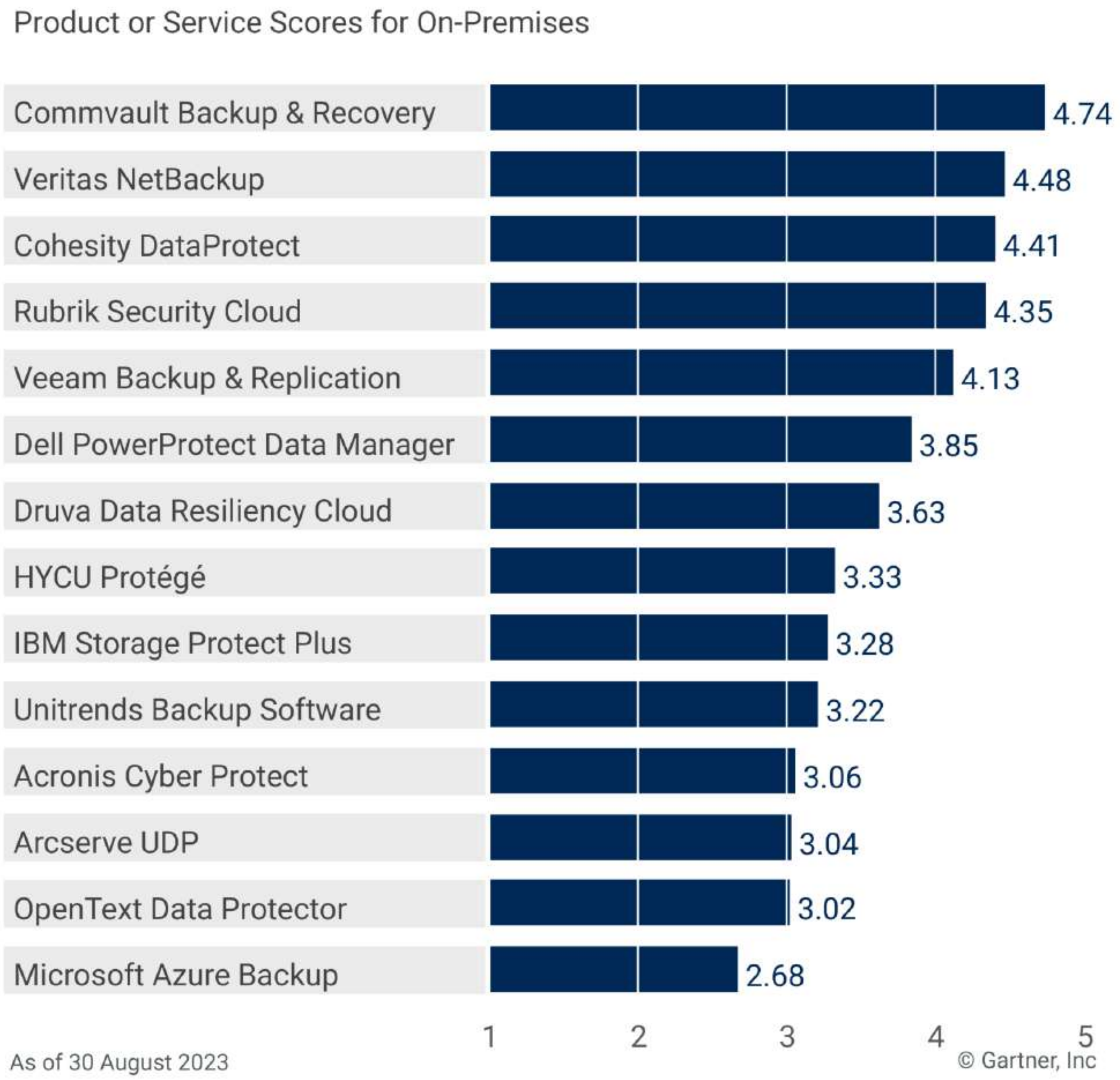
BY PARAM KUMARASAMY | SEPTEMBER 21, 2023

In today's hybrid multi-cloud world, enterprises are running applications and supporting workloads in on-premises, Edge, Cloud or SaaS. As new applications and locations emerge, ensuring consistent strategy around data protection and recoverability wherever data lives is critical – especially in the face of rapidly proliferating, and increasingly autonomous threats.

Gartner Critical Capabilities report, which is released as an essential companion to the Gartner Magic Quadrant, assesses vendors based on 15 key capabilities including Data Center Integration, Platform Security, Ransomware, and Management and more, across seven Use Cases.

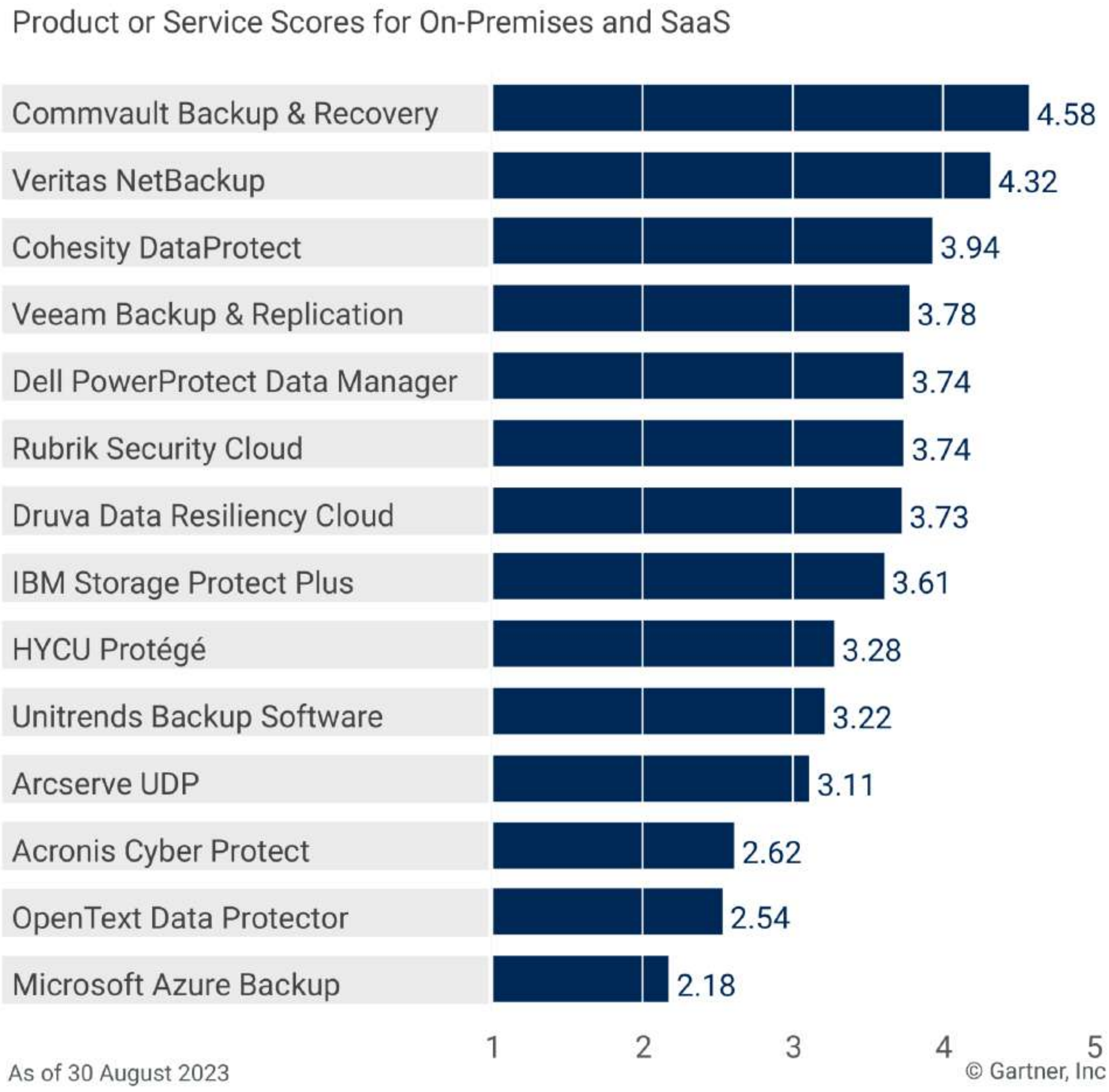
We are thrilled and honored that Commvault Backup & Recovery has scored the highest in six of the seven Use Cases in the Gartner Critical Capabilities for Enterprise Backup and Recovery Software Solutions: On-premises (4.74/5), On-premises and SaaS (4.58/5), Hybrid/Multicloud (4.76/5), Hybrid/Multicloud and SaaS (4.65/5), Disaster Recovery (4.48/5), and Ransomware Detection, Protection and Recovery (4.39/5)! Commvault ranked second highest (4.36/5) for the Data Services Use Case.[1]

®



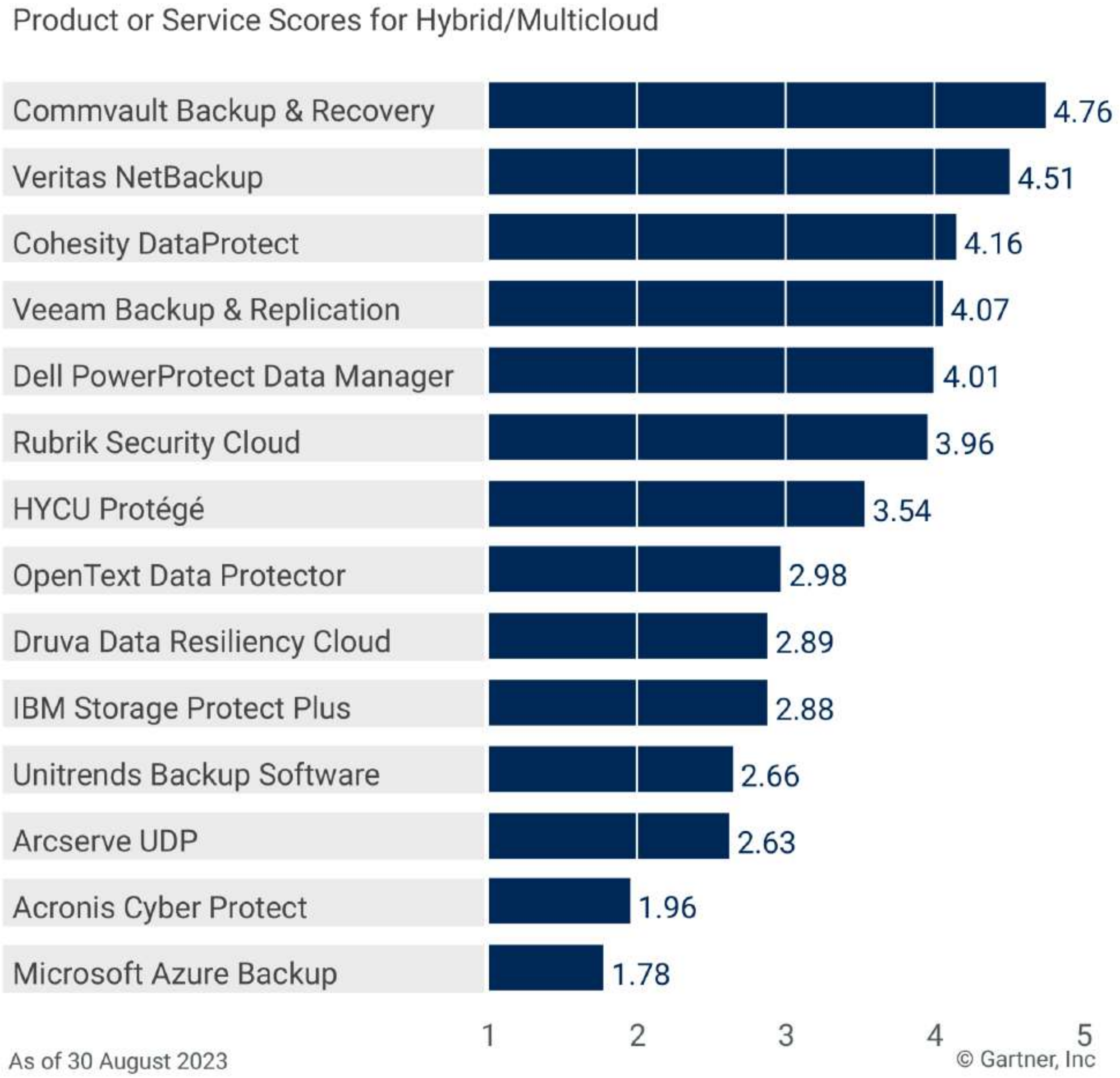
On-premises (4.74/5)

®



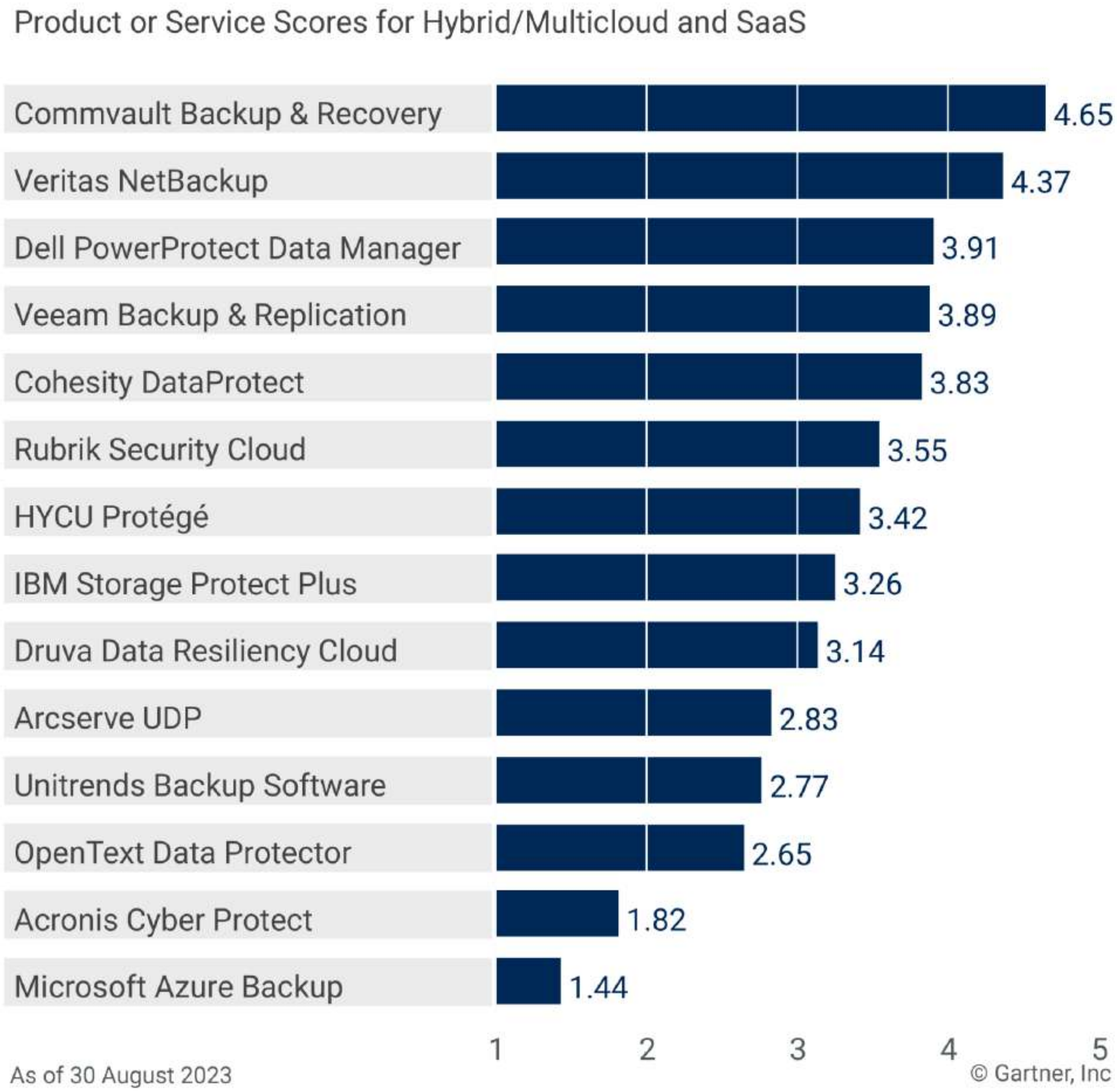
On-premises and SaaS (4.58/5)

®



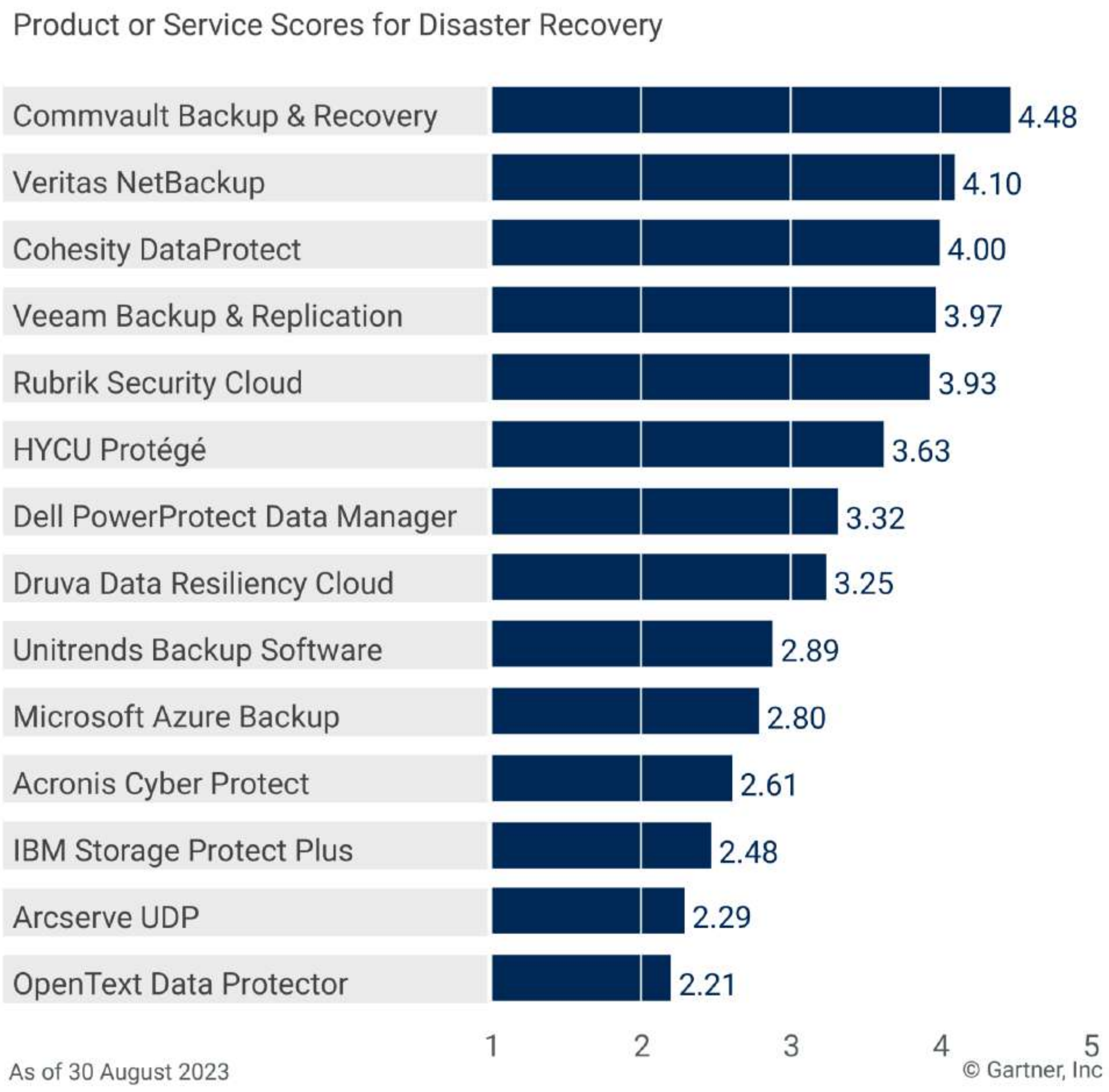
Hybrid/Multicloud (4.76/5)

®



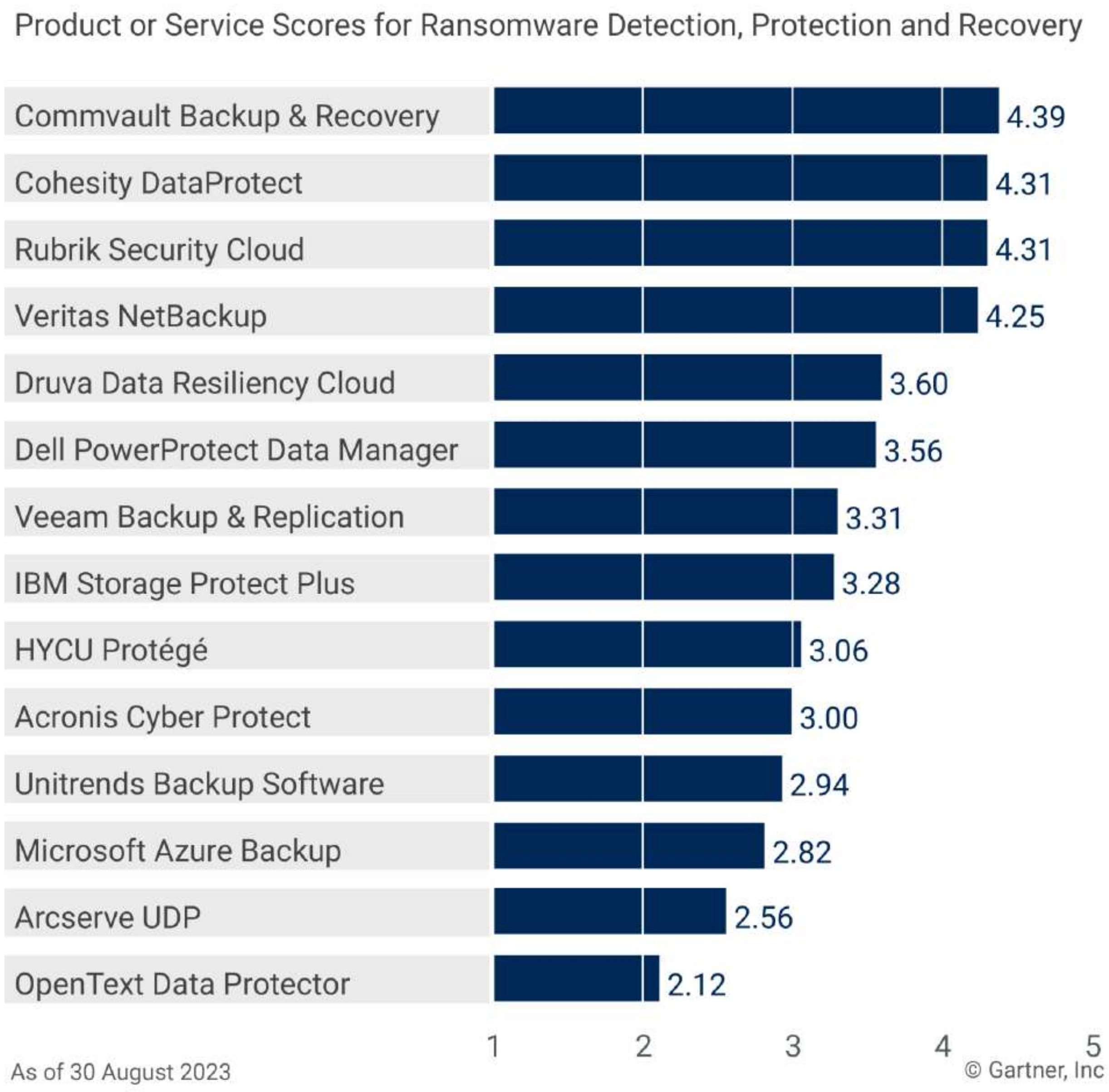
Hybrid/Multicloud and SaaS (4.65/5)

®



Disaster Recovery (4.48/5)

®



Ransomware Detection, Protection and Recovery (4.39/5)

We believe/think/feel that the release of this year's report is indicative of the industry as a whole; data continues to require stronger protection, cyber threat detection and recovery across more

®

Gartner, Magic Quadrant for Enterprise Backup and Recovery Software Solutions, Michael Hoeck, Nik Simpson, Jerry Rozeman, Jason Donham, 7 August 2023. This Magic Quadrant report was previously published as Magic Quadrant for Data Center Backup and Recovery Solutions (2016-2017; 2019-2020); Magic Quadrant for Enterprise Backup Software and Integrated Appliances (2014-2015); Magic Quadrant for Enterprise Backup/Recovery Software (2012-2013); and Magic Quadrant for Enterprise Disk-Based Backup/Recovery (2011).

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved.

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Commvault.

1. Gartner, "2023 Gartner® Critical Capabilities for Enterprise Backup and Recovery Software Solutions," Jason Donham, Jerry Rozeman, Michael Hoeck, Nik Simpson, 18 September 2023.

Gartner disclaimer

Gartner does not endorse any vendor, product or service depicted in our research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

More related posts

No posts founds

Commvault®

Legal

Privacy Policy

Trust Center

Cookie Preferences

WHITE PAPER

Strengthen ransomware resilience with data isolation and air-gap technologies

Securing and defending your data is essential to the rapid recovery of clean backups. You must be vigilant and take a proactive, multilayered approach. That means actively defending your data and its recoverability across a broad range of production and backup workloads and environments. Commvault Cloud Autonomous Recovery and Commvault Cloud Backup & Recovery deliver proven, cyber-resilient data protection for unrivaled business continuity. Commvault® Cloud, powered by Metallic® AI is focused on enabling cyber resilience—the industry's first platform for true cloud data security that empowers businesses to secure data, predict risks, minimize damage, and rapidly recover.

DATA ISOLATION

Best cyber resilience practices revolve around separating backup copies from source environments to minimize the threat of data loss or cyber breach. Commvault isolates your backup data to maintain secondary/tertiary copies in a separate network and security domain. LAN/VLAN switching, firewalls, least-privilege protocols, and foundational security that includes zero-trust principles to secure your data and reduce the attack surface to contain cyberthreats. Data stored within Commvault is not only isolated, but also immutable. This means that it cannot be alerted, deleted, or changed, while restricting inbound communication and enabling outbound connections to reduce your attack surface. Commvault also tunnels securely between isolated targets and sources for data security and replication.

AIR GAPPING

Air gapping is a data security technique that isolates data from corporate networks. It works like surrounding a castle with a moat; access is controlled via a drawbridge that can be deployed as needed. When data does not need to be accessed, communication is blocked by disabling ports, VLANs, and firewalls. Commvault provides secure replication of backup data to an isolated environment, coordinating when connections can be opened and closed. Outgoing connections are restricted, reducing the attack surface and allowing data to remain air-gapped until recovery or replication is needed.

KEY FOUNDATIONAL ADVANTAGES

Commvault's cyber resilience platform delivers key architectural components and tools, offering businesses of every size a durable, resilient, and proven backup framework:

Outbound communication only: All inbound access to the isolated data is blocked. Only restricted outbound connections are allowed from the isolated data to the source data for replication.

Air gap–ready: On-premises and hybrid configurations can be set up easily to create functionally secure air gaps within your environment Commvault Cloud Air Gap Protect provides a turnkey cloud air-gap solution that can be up and running in minutes and/or use Commvault Cloud HyperScale™ X for a secondary storage target on premises.

Hardware agnostic: When using Commvault as an air-gap solution, any supported storage can be used, including the Commvault HyperScale™ Appliance. Commvault also supports write once, read many (WORM) storage policies and immutable locks used with third-party storage devices.

Data integrity verification: Commvault validates data integrity during backup, when data is at rest, and during data-copy operations.

- Verification operations run automatically, using the data signatures to validate the backup data at rest. When copying the data, the signatures are used again to validate the data blocks during the copy operation.

Industry-leading security controls: Commvault's AAA Security Framework (authentication, authorization, and accounting) provides a suite of security and access controls to harden the Commvault platform itself–reducing risks from malicious actors and inside threats via a least-privilege approach to authorization. Advanced controls include:

- Strong multifactor authentication and multiperson authentication controls, retention locks, and command authorization to protect data from accidents as well as limit potentially destructive actions.
- Integration with privileged access management (PAM) and enhanced identity and access management (IAM) tools such as CyberArk, YubiKey, and biometrics for added user authentication and assurance (AAL3).
- End-to-end data encryption (while allowing external key-management platforms to manage and control keys), and certificate authentication–protecting against malicious data access.

Foundational hardening: The Commvault platform foundation is hardened using industry-leading CIS Level 1 benchmarks to reduce your attack surface.

Immutable backups: Commvault's hardware-agnostic approach offers ransomware-protection locks for just about any storage. Prevent unauthorized activity within the I/O stack (attempts to delete, change, or modify backup data) while preserving the integrity of backups:

- Ensure a fully immutable storage target with HyperScale X, leveraging scalable software-defined storage.
- Native OS and file-system controls embedded within the HyperScale X platform protect data from unauthorized or random modifications.
- Commvault Cloud Air Gap Protect easily provides immutability to house data in a secure, air-gapped cloud storage target.

Ransomware detection: Going beyond data validation, Commvault provides insights into suspicious and changed files with layered anomaly detection, honeypots, threat analysis, and file data analysis.

- Anomaly detection looks for suspicious behavior and activity within the backup data.
- Commvault® Cloud Threat Scan* detects malicious content. It performs a deep scan of the backup content, leveraging available scanning/antivirus tools to identify malware and files that have been encrypted, corrupted, or significantly changed so you can recover clean data and avoid file reinfection.
- Threat Scan Predict finds AI-driven ransomware to predict threats before they infect backups.
- Honeypots and file anomaly detection to actively detect threats in the live environment.
- Commvault Cloud Threatwise™ provides industry-unique early-warning threat detection technology to surface advanced cyber threats in production environments.

Rapid incident remediation and recovery:

- Curated data restores ensure that the last-known good copy of the backup is automatically selected when restoring data.
- Malware files are surgically and automatically purged from the Commvault index.
- Powerful cross-platform and cross-cloud restore capabilities to rapidly recover data, meet SLA compliance, and fulfill forensic analysis.
- Commvault provides instant recovery options to provide rapid access to critical data and systems.
- With Cleanroom as a Service gain capabilities to identify and ensure clean recovery, plus the ability to guarantee safe recovery to a cleanroom in the cloud.
- Cloudburst Recovery combines infrastructure-as-code and cloud scaling to ensure fast, predictable, and reliable cyber recovery at scale.

*Available with Commvault software only.

HOW DATA ISOLATION AND AIR GAPPING WORK

On-premises air-gap solutions require a mix of network architecture and software configurations. From an architectural perspective, storage must first be isolated and segmented on the network–without allowing inbound connections to that storage. Leveraging the components above, the Commvault software layer, network topologies, and workflows provide the basis for controlling data-pipe tunnels and orchestrating air-gap controls. In addition, Commvault's flexibility allows seamless integration with the topology or security profiles that organizations commonly deploy.

Direct connection for data isolation

Figure 1 depicts the high-level functionality of Commvault data isolation using direct connections. Site A represents the public portion of the production backup environment. Site B is a segmented portion of the environment, which has been isolated both logically and physically. Site B communicates through the firewall over a single outbound port. Everything else is blocked. The tunnel between the two sites supports HTTPS encapsulation using the TLS 1.3 protocol. The tunnel will connect only once certificate authentication is successful. This protects against man-in-the-middle and spoofing attacks.

Data transfer is multistreamed through the tunnel to ensure the fastest backup possible. Commvault's security controls, encryption, WORM, threat analysis, data analysis, and native ransomware locks for immutable storage protect data residing on the storage target on Site B from ransomware and accidental deletion. Data replication is deduplicated to further optimize bandwidth and storage considerations.

Once data transfer is complete, connectivity can be severed by turning off routing, enabling firewall rules, or shutting down systems. Connection severance can be scheduled around virtual machine (VM) power management or blackout windows.

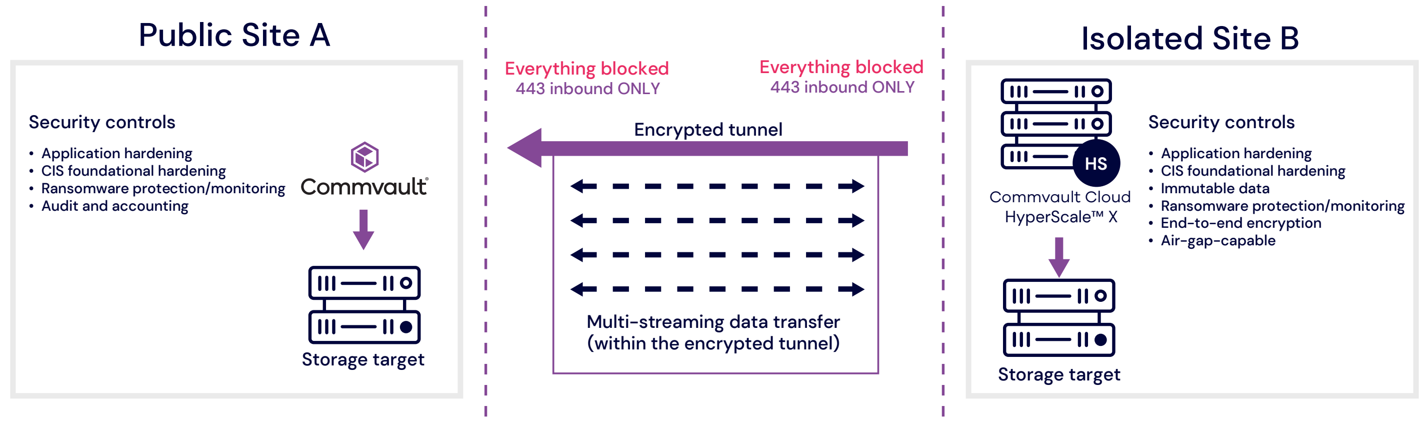


Figure 1 - Data isolation using direct connections

PROXY/NETWORK GATEWAY CONNECTION

A proxy-based configuration (Figure 2) has the same ransomware and encryption benefits as a direct connection. However, proxy-based isolation differs in that both sites communicate using a proxy located between the isolated and public networks (possibly a DMZ). All inbound connectivity is blocked between the sites, providing isolation capabilities on both sites. Proxy-based configurations are prevalent, especially when data moves between remote geographic locations across the internet.

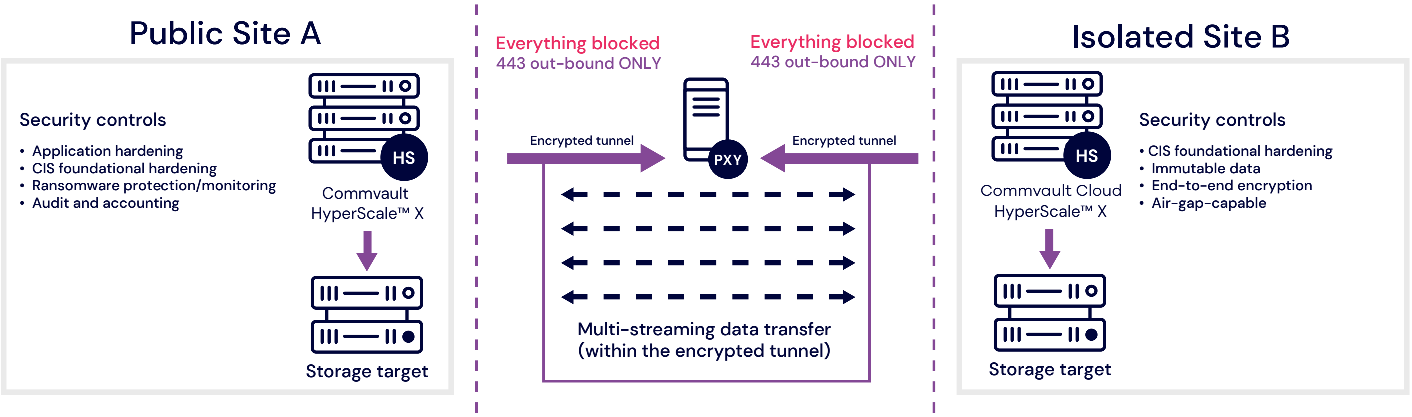


Figure 2 - Data isolation using a proxy-based network gateway connection

USING OBJECT STORAGE AND THE CLOUD

Object storage targets enable secure backup data isolation with WORM and immutable locks. Commvault integrates these storage targets for retention, encryption, and security. API calls over HTTPS provide more on-demand access and help reduce the ransomware attack surface. Object storage is ideal for secondary and tertiary copies, providing a secure, isolated target.

USING CLOUD STORAGE: COMMVAULT CLOUD AIR GAP PROTECT

Cloud storage targets (such as Azure and AWS) offer benefits similar to those of object storage solutions. The key difference is that cloud solutions are inherently isolated because they don't reside on premises with the rest of the organization's environment. This makes cloud storage a very economical solution because the copy is stored offsite and resources are readily available, elastic, and multitiered.

Commvault Cloud Air Gap Protect makes it easy to achieve secure and scalable cloud storage in just minutes, allowing you to meet the needs of your organization's hybrid cloud strategy while providing an additional layer of ransomware protection. With Commvault Cloud Air Gap Protect you can seamlessly adopt air-gapped cloud storage and gain predictable costs and reduced overhead. It can also be the foundation for improving your cyber recovery strategy by leveraging a fully integrated, secondary cloud storage target for Commvault Cloud HyperScale™ X.

THE COMMVAULT CLOUD PLATFORM

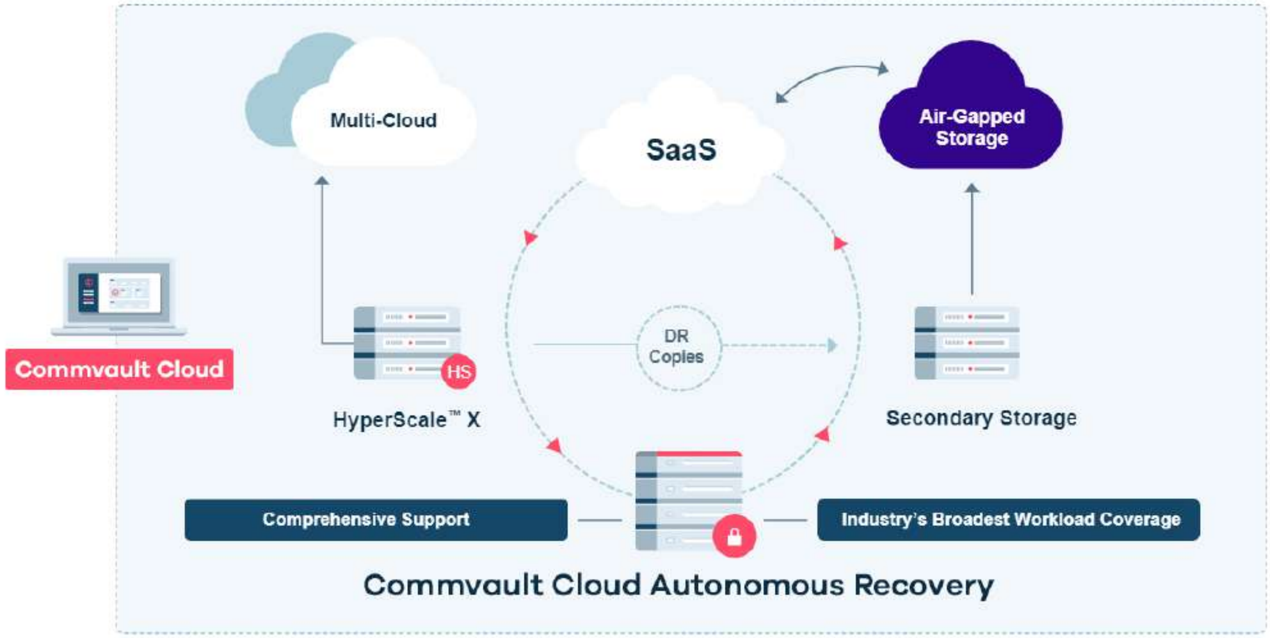


Figure 3 – Commvault provides the broadest workload protection, from on premises to the cloud, multi-cloud, edge, SaaS, and native cloud integration. Using the immutability locks offered by cloud providers in tandem with role-based security can secure backup data while supplying a remote, isolated, offsite data copy.

SEVERING THE CONNECTION AND AIR GAPPING

Combining a properly isolated and segmented data center with Commvault Cloud security controls can substantially reduce risks. Air gapping further limits the ability to access backup data when it's not in use. During air gapping, resources are turned off and data replication doesn't run, which may affect planning around recovery point objectives (RPOs). Depending on the environment, resources, and service level requirements, data replication is likely to queue when destination targets are offline. To help reduce this effect, Commvault incorporates multi-streaming within the one-way encrypted tunnel to maximize backup performance.

The simplest method of air gapping is to use VM power management, a capability within Commvault for automatically shutting down media agent virtual machines (data mover virtual machines) when not in use. The VMs will then start up when needed. This method requires a hypervisor in the isolated environment but does not need additional scripts.

Another method of air gapping is to use blackout windows, scripts, and workflows. Blackout windows define the time frames during which backups and administrative tasks are not allowed to run. During blackout windows, the isolated resources are set offline and made inaccessible using scripts or Commvault workflows. When blackout windows are not in effect, the resources are brought online again using scheduled scripts included on the air-gapped resource, such as the media agent. This method does not require a hypervisor for the VM power management air-gap method, because any storage target or network device can be shut down to air-gap the isolated site.

Here are some examples of using scripts to orchestrate air gapping:

- Stopping and starting Commvault services on the isolated media agents/storage targets
- Disabling/enabling network interfaces on media agents around blackout windows
- Disabling/enabling VLAN routing policies around blackout windows
- Disabling/enabling firewall policies around windows, using scripts

CONCLUSION

Like a castle, your backup data requires multiple layers of protection to defend against internal and external threats. Using Commvault Cloud security controls and immutable locks (ransomware protection, WORM, and encryption), Commvault Cloud Threat Scan, Commvault Cloud Autonomous Recovery, and more–in combination with proven data isolation and air-gapping techniques–provide a well-protected, multilayered strategic solution that ensures you are cyber recovery-ready.

Commvault cyber resilience delivers a proactive, multilayered approach for securing, defending, and recovering your data. **Learn more**

Commvault® | commvault.com | 888.746.3849

Enable Retention Lock Workflow

Updated Monday, November 13, 2023

The **Enable Retention Lock** workflow enables software WORM on all the dependent copies of a selected storage pool.

After you run this workflow to enable the retention lock, for entities that have valid jobs, you cannot decrease the retention or delete the entities.

Procedure

1. Download the **Enable Retention Lock** workflow from the Commvault Store using the instructions in Download Workflows from Commvault Store.

2. From the **CommCell Browser**, go to **Workflows**.

3. Right-click **Enable Retention Lock**, and then click **All Tasks > Deploy**.

4. Right-click **Enable Retention Lock** again, and then click **All Tasks > Execute**.

   The **Enable Retention Lock Options** dialog box appears.

5. Click **OK**.

   The **Select Storage Pool** dialog box appears.

6. From the **Storage Pool** list, select the storage pool that you want to configure the retention lock storage mode on, and then click **OK**.

   A warning message appears stating that, once you enable the retention lock, for entities that have valid jobs, you cannot decrease the retention or delete the entities.

7. Click **Yes** to run the workflow.

   The **Enable Retention Lock** workflow starts, and you can monitor the progress from the Job Controller window.

Results

After the workflow completes, the user who ran the workflow receives an email as follows:

- If the workflow completes successfully, the alert includes details of the actions completed by the workflow.

- If the workflow fails, then the alert contains the reason for the failure, and solutions to troubleshoot the issue.

Related Topics

- Configuring WORM Storage Mode on Cloud Storage
- Configuring WORM Storage Mode on Disk Libraries

COMMVAULT®

WHITE PAPER

Commvault® HyperScale X™ Performance

Purpose/Objectives

The purpose of this paper is to demonstrate the performance of Commvault HyperScale X within a set environment to show what results are achievable within similar environments. Due to the variations in all environments, results will be varied compared to the results achieved within this paper. While some environments can and will achieve better performance, other environments may not match the performance metrics captured in this paper.

This paper is not meant to show the maximum or minimum performance of the solution, but a snapshot of performance based on conditions used in this testing. This paper, including any results or statements herein, does not guarantee or warrant performance. This paper will also be limited to testing on the File System, Virtual Server and Oracle agents and cannot be used to extrapolate performance for other agent types.

Introduction to the Commvault HyperScale X™

Commvault HyperScale X accelerates hybrid cloud adoption with an integrated solution that delivers comprehensive data management for all workloads, including containers, virtual, and databases, from a single, extensible platform.

With Commvault HyperScale X, you can leverage the entire Commvault software portfolio giving you access to all the features, functions, and industry leading integration with applications, databases, public cloud environments, hypervisors, operating systems, NAS systems, and primary storage arrays. Wherever your data resides, you have ability to view it, use it, and confidently protect it.

Commvault HyperScale X provides two approaches to leverage the hybrid cloud:

Start on-prem, extend to cloud. This is for customers who want to protect on-premises data center workloads using HyperScale X, manage their own infrastructure, and extend to the cloud – including Metallic® Cloud Storage Service – for secondary and/or air-gapped copies of data.

Start with SaaS, use HyperScale X as edge storage. This approach is for customers who want the simplicity of SaaS data protection (e.g., Metallic® Backup as a service), but want to deploy HyperScale X at the edge, providing local air-gapped copies for faster recovery and lower costs.

Commvault HyperScale X options

Commvault HyperScale X is available in two options giving you the flexibility to choose an implementation based on your specific needs and preferences, delivered as a turn-key appliance or validated reference architecture (RA). Individual or multiple nodes can be added to either option to increase the storage pool usable capacity. Expansion nodes must match the same disk count and capacity as the starting three node cluster.

Appliances are available in two models, HS2300 and HS4300. Regardless of deployment model, Commvault Distributed Storage is our underlying solution for optimized scalability and performance to easily grow as needed.

There are two appliance configurations:

- HS2300 – 4 x LFF HDD servers
- HS4300 – 12 x LFF HDD servers

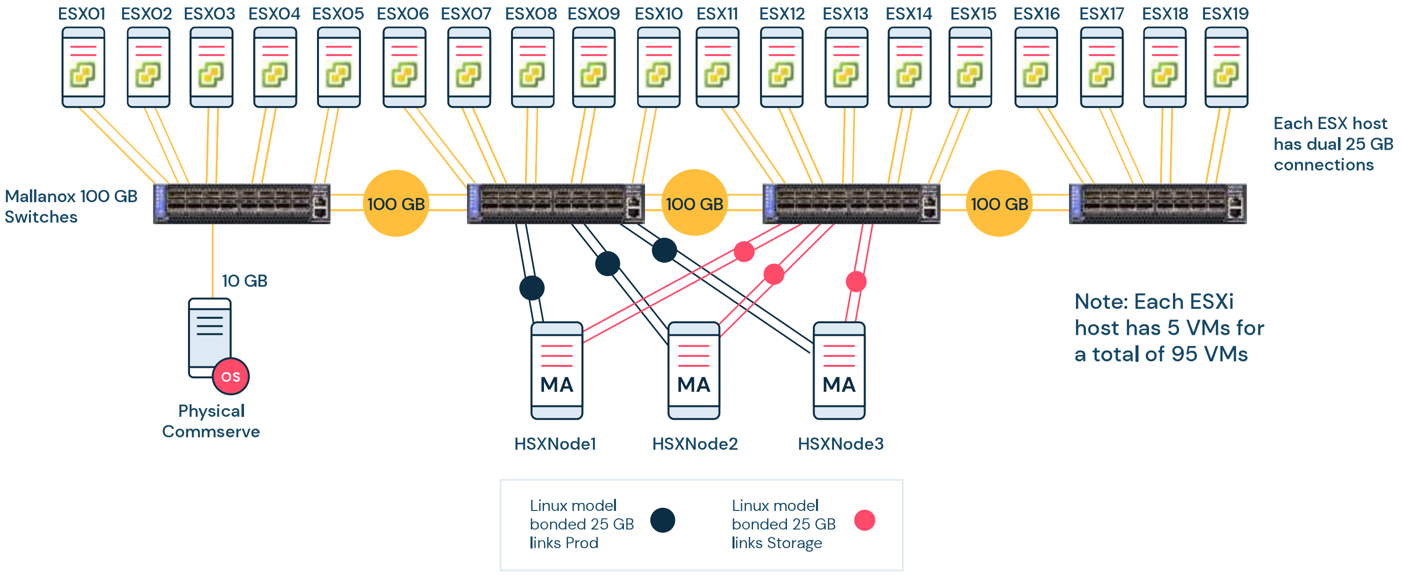
The three Commvault HyperScale X RA configurations are:

- N4 – 4 x LFF HDD servers
- N12 – 12 x LFF HDD servers
- N24 – 24 x LFF HDD servers

Test environment details

	N4 RA/HS2300	N12 RA/HS4300	N24 RA
Number of clients	50	95	95
Data size	750 GB per client or VM		
Compression factor	50%		
Daily change rate	2% per incremental backup		
Job run	Baseline full; 5x Incremental; Synthetic Full; 5x Incremental; Subsequent Full; Auxcopy; Restore		

Lab diagram:



	Commserve	ESX Hosts	VM Clients	Oracle VM
CPU	Dual 8 Core 4108 CPU	Dual 24 Core 6126 CPU	4 vCPU	12 vCPU
Memory	64 GB	256 GB	16 GB	128 GB
OS	Windows 2019	ESXi 6.7	Rocky Linux 8.5	Oracle Linux 8
Storage	450 GB SSD	4 x 1.7 TB SSD RAIDO for Datastore	OS – 40 GB disk Data – 1 TB disk – Data (on SSD Datastore)	OS – 500 GB Disk Data – 4 x 3 TB disk (on SSD datastore)
Networking	Single 10 GB connection	Dual 25 GB connections	Single NIC	Single NIC

Environment hardware used for testing:

- N4/2300 – Cluster of 3 nodes with 4 x 14 TB LFF HDDs
- N12/4300 – Cluster of 3 nodes with 12 x 14 TB LFF HDDs
- N24 – Cluster of 3 nodes with 24 x 8 TB LFF HDDs

Test objectives

The objective of the test environment is to simulate typical customer workloads in a production environment. Those workloads were applied across standard three-node configurations. While these results are representative and achievable, they are not intended to be performance guarantees. The testing was performed in a closed lab environment using source virtual machines running on SSD storage. These tests were not intended to illustrate peak performance but rather show a snapshot representative of a typical environment with multiple stream count.

Driving optimal performance

The Commvault HyperScale X architecture leverages the hyperconverged compute, networking, and storage resources to drive optimal performance for data management operations.

Parallelized operations

- Backup and restore data distributed across the maximum number of parallel streams
- Maximized parallel streams engage all available storage resources
- Jobs automatically distributed across all nodes

Scalability

- Performance will increase as nodes are added to the cluster, including single node expansion
- As storage pool grows I/O performance grows proportionally

Network performance

- Bonded ports provide both redundancy and increased performance

Incremental forever

- Where supported, reads and processes only changed data sets and blocks
- Commvault intelligent indexing performs single pass restore even with many incremental backups
- Provides low RPO/RTO for extremely large workloads

Performance tests

The performance tests were run using a variety of different operations. Below are a list of the different operations and relevant details.

Baseline Backup: The initial full backup of a client/VM or a group of clients/VMs. Typically, from this operation, storage optimization is mainly due to the 50% data compression with no to little deduplication.

Synthetic DASH Full: This consolidates the data from the latest true or synthetic full backup together with any subsequent incremental backups, instead of reading and backing up data directly from the source client. Since synthetic full backups do not back up data directly from the source client, this operation imposes no load on the source. Only the deduplication and index records are updated without the need to read each block and generate a signature, therefore this operation is significantly faster than a baseline operation.

Full on Full Backup: This is a secondary full backup of data from the client/VM, with only the changed blocks written to disk. Significant performance is gained due to deduplication eliminating up to 90%+ of the writes.

DASH Copy – Initial Full: Uses deduplication to reduce the amount of data traversing the network by sending only the unique blocks, files, or chunks. The initial full DASH copy will need to copy the entire data set from one copy to another.

DASH Copy – Secondary Full: Like above, however only the unique data between the first and subsequent copies will be transmitted over the network which greatly improves performance.

Restore – Restore of the full dataset back to the source client(s) or VM(s).

File system tests:

The Linux file system agent was used for all file system tests.

Single client backup results

Operation	N4/HS2300	N12/HS4300	N24
Number of Streams	4	10	10
Baseline Backup	1.6 TB/hr	4.1 TB/hr	4.1 TB/hr
Synthetic DASH Full Backup	11 TB/hr	11.5 TB/hr	11.5 TB/hr
Full on Full Backup	4.4 TB/hr	4.9 TB/hr	4.7 TB/hr
DASH Copy Initial Full[1]	2.0 TB/hr	5.1 TB/hr	5.33 TB/hr
DASH Copy Synthetic Full[1]	16.0 TB/hr	17.3 TB/hr	16.31 TB/hr

Multi-client backup results

Operation	N4/HS2300	N12/HS4300	N24
Number of Clients	50	95	95
Number of Streams	200	570	570
Baseline Backup	2.4 TB/hr	7.9 TB/hr	11.4 TB/hr
Synthetic/DASH Full Backup	49.7 TB/hr	58.4 TB/hr	59.1 TB/hr
Full on Full Backup	49.3 TB/hr	90.8 TB/hr	95.3 TB/hr
DASH Copy – Initial Full[1]	2.2 TB/hr	3.3 TB/hr	1.5 TB/hr
DASH Copy – Synthetic Full[1]	65.7 TB/hr	60.4 TB/hr	68 TB/hr

Restores results

Operation	Total # of streams	N4/HS2300	N12/HS4300	N24
Single Client Restore	4	2.0 TB/hr	2.2 TB/hr	2.2 .TB/hr
5 Client Restore	20	2.1 TB/hr	4.6 TB/hr	4.2 TB/hr
25 Client Restore	100	2.1 TB/hr	3.9 TB/hr	3.7 TB/hr
50 Client Restore	200		3.8 TB/hr	3.8 TB/hr

Virtual Server Agent (VSA) tests:

The VSA agent on each of the Commvault HyperScale X nodes were used for protecting the VMs using NBD mode, and App Aware was not used for this testing.

Single VM Backup results

Operation	N4/HS2300	N12/HS4300	N24
Number of Streams	2	2	2
Baseline Backup	573.8 GB/hr	1 TB/hr	1.1 TB/hr
Synthetic DASH Full Backup	10.1 TB/hr	11.8 TB/hr	11.7 TB/hr
Full on Full Backup	881 GB/hr	1.2 TB/hr	1.3 TB/hr
DASH Copy Initial Full[1]	1.2 TB/hr	1.7 TB/hr	554 GB/hr
DASH Copy Synthetic Full[1]	16 TB/hr	17.3 TB/hr	18 TB/hr

Multi-VM Backup results

Operation	N4/HS2300	N12/HS4300	N24
Number of Clients	50	95	95
Number of Streams	100	190	190
Baseline Backup	2.5 TB/hr.	7.5 TB/hr	8.3 TB/hr
Synthetic/DASH Full Backup	39 TB/hr	52.5 TB/hr	64.3 TB/hr
Full on Full Backup	7.3 TB/hr	18.9 TB/hr	25.6 TB/hr
DASH Copy – Initial Ful[l1]	2.2 TB/hr	3.5 TB/hr	1.5 TB/hr
DASH Copy – Synthetic Ful[l]	53.5 TB/hr	60.1 TB/hr	54 TB/hr

Restores results

Operation	Total # of streams	N4/HS2300	N12/HS4300	N24
Single VM Restore	1	461 GB/hr	413 GB/hr	433 GB/hr
5 VM Restore	5	2 TB/hr	1.6 TB/hr	1.9 TB/hr
25 VM Restore	25	2.2 TB/hr	2.6 TB/hr	2.8 TB/hr
50 VM Restore	50	2.2 TB/hr	1.6 TB/hr	3.7 TB/hr

Oracle Agent tests

The Oracle agent was installed on a VM for this test. This is for a single Oracle DB on a single VM.

Operation	N4/HS2300	N12/HS4300	N24
Number of Streams	10	16	20
Baseline Backup	1.2 TB/hr	3.2 TB/hr	3.7 TB/hr
Full on Full Backup	5.1 TB/hr	5.8 TB/hr	6.0 TB/hr

Restore results

Operation	N4/HS2300	N12/HS4300	N24
Number of Streams	10	16	24
Single DB Restore	1.1 TB/hr	1.5 TB/hr	1.6 TB/hr

Performance – Interpreting the numbers

Backup performance

As can be seen from the results, by increasing concurrent streams and the number of clients/VMs, backup performance can be improved, however, at some point a saturation within the environment will be hit and if increased too far, it will have a negative impact on performance. Since each environment is different, the saturation points within a given environment will also be different.

For each test (except Oracle), there are results for single client vs multiclient backups. This is to show that to get the best performance possible, it is highly dependent on maximizing both the number of streams and clients/VMs. A single client or a single VM will not achieve the same results as backing up multiple clients/VMs in parallel.

Restore performance

As can be seen by the restore numbers, and like backup performance, better results can be achieved by increasing the concurrent streams and the number of clients/VM. However, also as the backup performance has shown, at some point a saturation within the environment will be hit where increasing clients and streams will have a negative effect, and this point will be different within different environments.

Each restore test was done using single and multiple clients/VMs to show that to get the best performance, it is highly dependent on maximizing both the number of streams and clients/VMs. A single client or a single VM will not achieve the same results as restoring multiple clients/VMs in parallel.

Other factors which can affect performance

Unfortunately, performance can also be negatively impacted by several things within an environment, and some are listed here as possible areas to explore when analyzing slow performance:

- Network latency, which refers to the time needed to send data from the source to the destination, this can be caused by the number of networks hops the data needs to take between the source and destination
- Network bandwidth
- Network congestion which is the saturation of a path that the data flows between the source and the destination
- Network prioritization, some traffic/applications may have a lower priority set than others

- Routing and/or load balancing
- Anti-virus software
- Encryption
- Source clients with limited or highly utilized resources
- Other operations running at the same time[2]

While the above is not a complete list, it is used to show that there are many things that need to be taken into consideration when looking at performance.

Conclusion

As can be seen from the results, performance varies based on cluster size, stream counts and number of clients being backed up or restored at any one time. There is also a large difference when using different agent types, which shows that the performance based on one agent type cannot be used to predict the performance of another agent.

We also need to look at single client/job vs multi-client results. A single client/job will never be as performant as the aggregate sum of multiple clients/jobs. Even when adding one or more nodes, this will not increase the performance of a single client/job. The same can be said for multi-client backups or restores, if the number of clients and streams remains the same and the only change is adding one or more nodes, there may be a slight increase in performance, but not a significant increase as the job/streams has remained the same. To increase performance when adding nodes, more clients/streams will need to be added to improve the overall aggregate throughput of all jobs.

Notes

[1] For each test above, specifically for all DASH copy jobs, the N4 system copied to a N12 system, the N12 system copied to a N24 system, and the N24 system copied to the N12 system. The result of this is that both N4 and N12 systems will have higher than normal results are they are both copying to larger systems (which in a larger environment smaller cluster may copy to a larger DR cluster) as opposed to copying to a system of the same size. Since the N24 is copying to a smaller system, it has lower than normal results.

[2] For all tests performed, each job ran when no other processes were running in the environment or on the source clients to ensure full resources were available. Except for Oracle, where the Oracle DB was running.