

Solución todo en uno de backup y recuperación de desastres confiable, accesible y escalable

Destinatarios

De los clientes nuevos, los mejores son: empresas del mercado medio

- Infraestructuras modernas de TI físicas/virtuales/en la nube
- Ensamble complejo de soluciones de recuperación de desastres (DR) y backup
- Estrategia incompleta de DR por cuestiones de costos
- **Alcance total:** clientes de cualquier tamaño, nivel, ubicación geográfica, y soluciones existentes

Profesional de TI

Gerente de TI; Admin. de TI, DR, Backup, Virtual, Nube

Temas de preocupación:

- Tiempo de administración de tareas de backup+DR
- Problemas para cumplir con los SLA
- Control sobre los sistemas
- Falta de tiempo generalizada y personal muy ocupado

Responsable de las decisiones comerciales de TI

CIO, Director de TI, COO, CISO, CDO

Temas de preocupación:

- Crecientes demandas del negocio
- SLA más exigentes
- Estancamiento en la productividad del equipo de TI
- Limitaciones presupuestarias y altos costos de DR
- Necesidad de asegurar un ROI positivo

Propuesta de valor para los profesionales de TI

Arcserve permite que los profesionales de TI cumplan con los SLA y ahorren hasta un 50% del tiempo con soluciones todo-en-uno de backup y recuperación de desastres de fácil implementación y mantenimiento.

Además, las soluciones ofrecen una interfaz unificada para todas las tareas e informes de SLA automatizados que permiten mantener informados a los accionistas; por eso, los profesionales de TI eligen a Arcserve como el camino más sencillo para proteger la totalidad de sus infraestructuras de TI.

¿Desea conocer más detalles?

Principales mensajes

- Implemente una solución de backup y DR todo-en-uno
- Hardware, software y servicios en la nube con un único proveedor y un único punto de contacto
- Logre la confianza de sus partes interesadas con herramientas avanzadas de informes y análisis
- Reduzca los tiempos de administración de backups en hasta un 50%
- Obtenga tranquilidad con soporte de hardware en solo 4 horas y atención 24/7 por teléfono o correo electrónico

Alto nivel de complejidad y costos de un sistema ensamblado con diversas soluciones individuales de DR o backup

El 74% de las empresas no confían plenamente en su capacidad de recuperación. ¿Por qué? Se requiere mucho esfuerzo, recursos y dinero para implementar una estrategia completa de DR+Backup en el contexto de la TI moderna, con una combinación de cargas de trabajo virtuales, físicas y en la nube.

Cada tipo de entorno de TI puede estar conectado a diferentes soluciones de hardware y software, plataformas de infraestructura y redes, lo que lleva rápidamente a un ensamble inestable de más de una docena de componentes y proveedores.

Solución: Solución todo-en-uno de backup y DR con una interfaz unificada para todos los tipos de infraestructuras de TI, que supera ampliamente el ensamble de soluciones individuales en cuanto a rendimiento, confiabilidad, disponibilidad y rentabilidad.

Una solución integrada de backup y DR en la nube es más fácil de implementar, administrar y mantener, para obtener funciones sólidas y comprobadas de backup y recuperación de desastres locales, remotas y en la nube.

Características principales

Diseñada para la recuperación

- Recuperación Bare Metal, desde y hacia cualquier ubicación, Virtual Standby
- Instant VM, Assured Recovery™ para pruebas de DR, recuperación granular

Funcionalidades en la nube

- DR hacia la nube, backup hacia la nube
- Almacenamiento de copias de seguridad en la nube, implementación de UDP en la nube

Backup comprobado y confiable

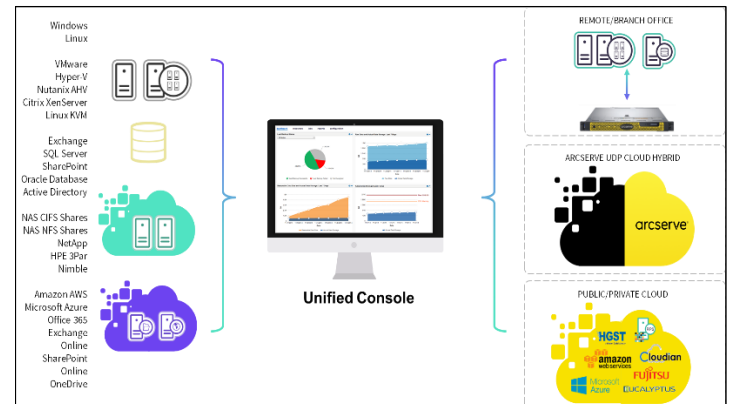
- Entornos físicos de Windows y Linux; Hyper-V, AHV, VMware sin agentes
- Deduplicación global en origen, cifrado AES/SSL, snapshots de HW

Administración intuitiva

- Consola unificada basada en la web; administración basada en políticas
- Administración basada en roles; informes SLA; CLI, API

Principales mensajes para partners

- Ayude a sus clientes a implementar una solución todo-en-uno de backup, DR y alta disponibilidad
- Aumente las ganancias con los mejores márgenes del mercado, respaldados por el Programa Accelerate para Partners de Arcserve
- Reduzca los costos internos y los gastos generales con tecnologías robustas del proveedor de protección de datos más experimentado del mundo
- Disminuya la tasa de abandono de clientes con una solución sólida unificada



Llamadas a la acción

- Activos: Hoja de datos, Novedades, Resumen de la solución
- Acciones: Llamada de preventas, Demo

Solución todo en uno de backup y recuperación de desastres confiable, accesible y escalable

Office 365

Key features:

- Office 365 backup and granular recovery
- Complete support of Exchange Online, SharePoint Online & OneDrive
- Disk storage with deduplication, tape, cloud
- Strong AES encryption
- Companies moving from Exchange to Office 365: One UI, common Reports

Microsoft does not back up Office 365:

| | |
|---|--|
| | Microsoft Office 365 Policy |
| Recycle Bin | Items retained for 93 days |
| Secondary Recycle Bin | Purged after 93 days |
| Deleted Mailbox | Can be restored only within 30 days (14 days is the default) |
| Email Modifications | Items can be modified by users and admins, including the ability to delete attachments. No recovery for this scenario. |
| Offsite backup and point-in-time recovery | “Point in time restoration of mailbox items is out of scope for the Exchange Online service” |

Qualifying and discovery questions:

Metrics/Need – IT Pro: How many Office 365 users/seats do you have? Have you ever lost data in Office 365? How do you back up Office 365? How would you recover if an email or a mailbox is lost? How much time would recovery take? Is that time within expectations of your users? What would you do if Microsoft does not recover some data? Do you have a copy of users emails on-premises?

Champion: Who in your organization manages Office 365? If an email or mailbox in Office 365 would become lost/corrupted, who would be responsible to restore?

| | Arcserve | Veeam | Veritas | Acronis | Baracuda | Rubrik | Commvault | Microsoft |
|-----------------------------------|----------|-------|---------|----------------|----------|--------|-----------|-----------|
| Point-in-time backup and recovery | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| Exchange Online | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | N/A |
| SharePoint Online | ✓ | ✓ | ✓ | ✓ ¹ | ✓ | ✓ | ✓ | N/A |
| OneDrive | ✓ | ✓ | ✓ | ✓ ¹ | ✓ | ✓ | ✓ | N/A |
| Deduplication | ✓ | ✗ | ✗ | ✓ ¹ | ✓ | ✓ | ✓ | N/A |
| Encryption | ✓ | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | N/A |
| Unified interface | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | N/A |
| O365 to on-prem | ✓ | ✓ | ✗ | ✓ ¹ | ✗ | ✗ | ✓ | N/A |
| Flexible licensing | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | N/A |
| Costs | \$ | \$ | \$\$\$ | \$ | \$ | \$\$\$ | \$\$\$ | N/A |

¹ Acronis stores SharePoint and OneDrive backups in the cloud storage. Only Exchange backups by Acronis can be stored on-site with deduplication.

Nutanix AHV

Key features:

- Agentless backup for Windows/Linux AHV VMs
- Any-to-any recovery, including to physical, virtual and AWS/Azure
- Near-zero RTO with Virtual Standby and Instant VM
- DR testing with Assured Recovery
- Granular file and data recovery
- Migration to/from Nutanix AHV
- PRISM integration
- Unified user interface for the entire infrastructure

Qualifying and discovery questions:

Metrics/Need – IT Pro: How many Nutanix AHV systems do you have? How do you back up Nutanix AHV? How and where would you recover if VM is down? What if entire Nutanix is down? How much time would recovery take? Is that time within expectations of your users? How do you protect Nutanix from major disaster, like fire or earthquake? Are you planning to migrate your applications or systems to Nutanix AHV?

Metrics/Need – IT BDM: What will be the consequences for your company and for you if your production systems hosted on Nutanix go down? How long can your business tolerate applications running on Nutanix to be unavailable? What would be the costs of Nutanix downtime to the business? Are you prepared for major disasters?

Champion: Who in your organization manages Nutanix systems? If a workload hosted in Nutanix AHV would malfunction, who would be responsible to recover? Who in your organization would you consult with before selecting any solution for Nutanix? Have you worked with Arcserve and our products before? What was your experience?

| | Arcserve | Veeam | Veritas | Acronis | Baracuda | Rubrik | Commvault | HYCU |
|------------------------|----------|----------------|---------|---------|----------|----------------|-----------|------|
| AHV agentless backup | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✓ |
| Any-to-any recovery | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| Physical Windows/Linux | ✓ | ✓ ¹ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| VMware/Hyper-V | ✓ | ✓ ¹ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| AWS EC2/Azure VMs | ✓ | ✓ ¹ | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ |
| SLA reporting | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| DR testing | ✓ | ✗ | ✓ | ✗ | ✗ | ✓ | ✓ | ✗ |
| Unified interface | ✓ | ✗ | ✓ | ✗ | ✗ | ✓ | ✓ | ✗ |
| Tape storage | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ ² | ✓ | ✗ |
| Flexible licensing | ✓ | ✗ | ✓ | ✗ | ✗ | ✓ | ✓ | ✗ |
| Costs | \$ | \$ | \$\$\$ | \$ | \$ | \$\$\$ | \$\$\$ | \$ |

¹ Veeam has separate UIs for AHV, Physical and Virtual systems, increasing complexity and time to manage

² Rubrik tape support is outsourced to third-party solution by QStar

Reliable, Affordable, Scalable, All-in-one Disaster Recovery & Backup

MEDDIC & BANT qualification

| | |
|--|---|
| Metrics and ROI <i>(Budget)</i> | Describe for me your entire disaster recovery and backup strategy, including on-site and off-site? Tell me, what will be the consequences for your company and for you if your IT systems go down? How much time do you spend every week managing data protection? What would it mean for you if you could spend two hours a month instead of two weeks a month managing DR and backup? What is your approximate downtime cost per hour? How do you measure that? <i>(Hint: If prospect unable to answer, ask about approx. annual revenue and divide by 2000. The result is hourly downtime loss on unrealized revenue.)</i> What is the RTO and RPO you are currently achieving for your mission-critical systems? What is the RTO and RPO your business is asking for? |
| Economic buyer <i>(Authority)</i> | Who, in addition to yourself, would be responsible for final signoff and approval for the solution? |
| Decision criteria <i>(Timeline)</i> | Can you explain how will you evaluate and select a DR and backup solution? How did you select a similar solution last time? |
| Decision process <i>(Timeline)</i> | Who, in addition to yourself, will be involved in the decision process? Are there multiple individuals or committees involved? Can you explain me your review and decisioning process, including the steps required after a vendor is selected? What is your timeline to make a final decision? At what stage of solution selection are you currently? |
| Identify pain <i>(Need)</i> | General qualification: How many sites do you have in your IT infrastructure, including clouds? At what stage are you in your cloud transformation journey? How many servers do you have? What and how many business-critical systems with 1-4 hours RTO you have? What and how many mission-critical systems, that should be available no matter what, do you have? How much total data you are backing up? Do you have requirement to store backups on tape? Do you have non-x86 systems, like Solaris, FreeBSD, UNIX or apps, like Oracle or SAP HANA? |
| | Qualification for Risk of Extended Downtime during Disaster Recovery: Could you please describe your DR strategy for all critical systems, including on-site and off-site? Do you consistently achieve your target RTOs and RPOs? How often do you test your disaster recovery plans? Can you describe the process for me? |
| | Qualification for Risk of High TCO of Multiple Data Protection Tools: Can you clarify what components do you have in your DR and backup infrastructure, including software, platform, hardware and network? What DR and backup solutions do you currently use? How many user interfaces do you use for DR & Backup? How many people in your IT organization manage these DR & Backup tools and solutions? Would you have to reallocate resources to support the growing backup management time requirements? What would it mean if a single appliance would deliver complete DR & Backup strategy? Describe how it would benefit you if you could implement backup and disaster recovery for all cloud, physical, and virtual systems managed from a single interface? If we could reduce the time to manage your data protection solution by 50%, describe how would you use that time? |
| Champion <i>(Authority)</i> | Who in your organization has the most knowledge on data protection solutions and vendors? Who in your organization would you consult with before selecting a solution? Have you worked with Arcserve and our products before? What was your experience? |
| Competition | Are there any other DR & backup solutions you are currently evaluating? What DR & backup solution are you using today? Are you also considering doing nothing? What would happen if you don't select a new DR and/or backup vendor(s)? |

Objection Handling

O: I already have DR & backup in place
H: Do you have DR for all your mission-critical and business-critical systems?
How many components are there in your DR & Backup? When did you last test recovery? How long did the test take? What RTO and RPO did you validate? How will you get help if you face any issues?

O: We manage our multiple solutions just fine

H: How much time do you spend weekly on managing DR & backup? How much would you spend if your IT environment doubles in size? Would you have to reallocate internal resources to support growing existing DR & backup management time requirements? How would you use the time, freed by the backup solution that requires 50% less management effort?

Proof Points

- Downtime costs \$300K+ for 81% of companies (ITIC Study, 2016)
- <25% of companies are highly confident in ability to recover (Arcserve, October 2018)
- 56% businesses use 2+ backup solutions (Kroll OnTrack Survey)
- Backup mgmt. time reduced from 3-4+ hr to 1-2 hr after switching to Arcserve (Arcserve, November 2017)
- >90% businesses experience 1+ IT outage per year (Everbridge survey)
- Company data grows on average 42% per year (IDC Study, DataAge 2025)
- 45% of IT outages caused by hardware failure (DBT study)