arcserve®

Solution Brief

Remote Office, Branch Office

Protecting your distributed data and systems for robust business continuity

How an all-in-one disaster recovery solution for your remote or branch offices, keep you running around the clock.

Remote Office, Branch Office

Contents

Introduction

Remote office and branch office (RoBo), like retail stores, hotel chains, construction sites, transport and logistic depots, manufacturing plants, highstreet banking and many more industries, have to deal with unique challenges. One of them, as they are geographically spread, is that they do not have many or any IT staff based on site.

Like any type of organisation, RoBo architectures have to make sure that data is backed up and secured all the time, so it can be recovered, in the event of a disaster.

Many businesses lack processes to deal with managing backups, while others do not have the right technology to achieve complete business continuity.

Any type of disruption, from a transport strike to a power outage or cyber-attack, can put operations at risk, so it is important to close this gap before it is too late.

This brief shows how to keep your RoBo data safe, and the business running in a consistent and easy way.

[1] Cybersecurity Ventures: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

The remote and branch office data protection challenge

Many organisations have some form of RoBo architecture and distributed networks; small businesses with only one office, including home-based employees, can also be exposed to data loss in the event of a problem and should be backed up properly.

This increasingly distributed working environment poses challenges for data protection. Traditional enterprise backup and disaster recovery products and services are often too expensive, complex to deploy and manage at a branch office. This leaves IT and other staff to “make do” with whatever technology they have access to.

Even with local backups taking place on a regular basis, a remote office can experience data loss if there is no offsite protection. This is why branch offices need a combination of on-premises data backup and off-site replication and failover.

Start by taking a few steps to assess your branch office data protection:

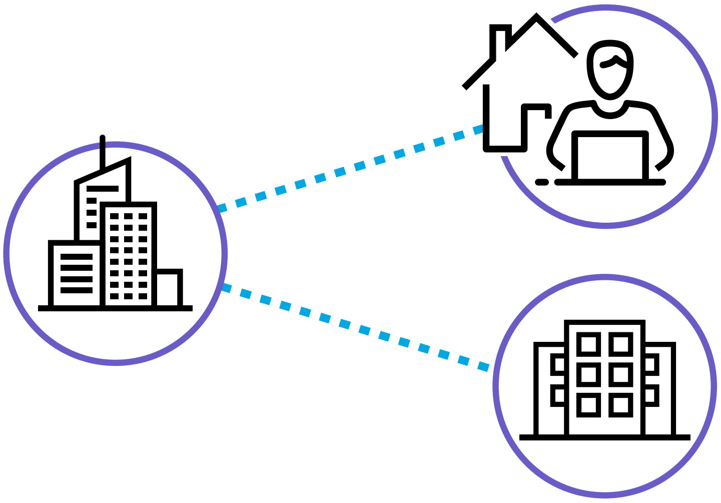
- How much of your data is being generated and consumed in remote offices?
- Are your remote and branch offices being protected?
- How exposed are the remote sites in the event of a problem?
- Are you meeting all your regulatory or compliance requirements?
- What tools and services are in use? Are these doing the job?
- Are you able to protect the data off-premises when a site access is not available?
- Can you recover your RoBo data and how quickly?

Data recovery is just as important as data protection, if not more.

If an office server failed, how would you get the data back and the system working again? Recovery is just as important as data protection, but is also too often overlooked and not tested.

Organisations must include data recovery as part of their remote office data protection strategy and avoid falling into the trap of thinking - just because data is backed up it will be available when you need it.

A solid RoBo data protection strategy should deal with the daily reality of distributed networks and include backup and recovery in the same policy.



Locked out?

Site access is not required with Arcserve

Is your IT staff or service provider locked out of the office? Arcserves technology does not require personnel to be on site to protect and recover data.

In a total lock-down scenario, no one might be allowed to go to the office. Also, if you cannot access the on-premises applications, due to the servers being down, or the NAS with the backups not being accessible, you will be facing a huge problem. With Arcserve's Disaster Recovery as a Service (DRaaS), the on-premises servers can be virtualised in Arcserve's data center and can be made accessible from any location, keeping staff productive.

The importance of centralised and remote management

In recent years the workplace has become significantly more distributed. Thanks to better broadband coverage and availability, it has become much easier to set RoBo, allowing more employees to work remotely.

This distribution of the workplace has reduced many single points of failure, but it also calls for a new approach to data protection and management.

In a central office, data management can happen locally and systems can be configured to use on-premises storage infrastructure.

In a remote office environment, IT staff do not have the luxury of having everything in one place. This is why centralised remote management is so important. Data protection and recovery is needed at multiple locations; however backup management should be central to optimise resources and reduce risk.

Without centralised management, organisations can waste too much time configuring remote offices on-site.

Centralised management is also very important for disaster recovery. For example, if a remote site was closed due to a flooding incident, having centralised management will allow that branch office data to be recovered without the need to forensically recover the data at the original site.

Unified management allows IT staff to be more effective across the business as they do not need to be on site for everyday tasks.

The many faces of a disaster

In 2020, the COVID-19 disaster shocked the world with a rare, one-in-100-year pandemic. However, most businesses face more common disasters including:

- **Malware:** Malware, including ransomware, is a persistent threat that can capture critical information from any location
- **Weather:** Extreme weather, such as a flood, can ruin offices and computer systems
- **Fire:** A fire can destroy part or all of an office
- **Transport:** A disruption in transport links can stop people from getting to a branch office
- **Power:** A power outage can disrupt operations and take days to restore
- **Insider threats:** A rogue employee could use their access privileges to maliciously destroy data
- **System failure:** A client or server computer can fail at any time. This could be due to a disk failure or another component
- **Network outage:** Both fixed and mobile network outages can stop applications in their tracks

A proper disaster recovery capability will protect the business from any type of disruption.

INTRODUCING...

OneXafe® Solo

Plug-and-Protect

Direct-to-Cloud Data Protection

A better way to protect RoBo data

A recent addition to the Arcserve portfolio is OneXafe Solo, a true plug-and-protect data backup solution.

The neat data protection appliance enables anywhere, anytime protection. By being bundled with Arcserve's next-generation data protection software, ShadowXafe, customers simply connect the OneXafe Solo to the Internet and start protecting immediately.

Having disparate hardware and software to protect small and remote offices' data adds complexity, and risk of failure, during an incident. A single, integrated solution is more streamlined and much less of a burden on the business, which is imperative when it comes to remote offices.

Organisations now have the option to consolidate remote office server, desktop, and laptop backup data into Arcserve's secure cloud with OneXafe Solo. Benefit from world-leading data protection and cloud technologies in an easy to use appliance.

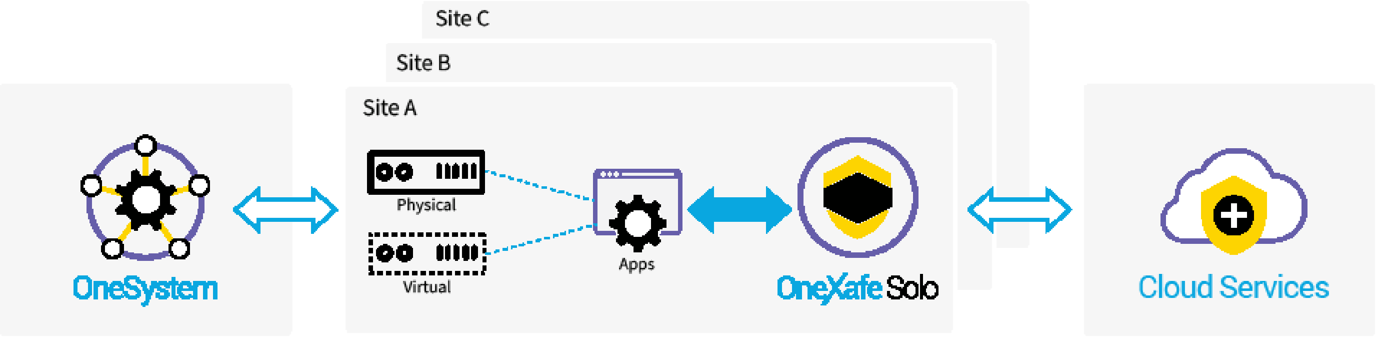
- ✓ **Easy to deploy:** plug it in and start protecting data in minutes
- ✓ **Enterprise grade:** ShadowXafe data protection technology in a compact appliance
- ✓ **Off-site protection:** Integrated with Arcserve Cloud Services (Premium)
- ✓ **Native disaster recovery:** DRaaS with one-click failover to recover and entire site
- ✓ **Economical:** Suitable for environments with limited infrastructure or local storage
- ✓ **Fast recovery:** Recover files and folders in seconds, and entire systems in minutes
- ✓ **Integrated management:** Set-and-forget remote management (including SLAs) without dedicated staff or capital resources
- ✓ **Expandable storage:** Add internal, NAS, flash drive, Arcserve Cloud or third-party cloud storage options.

In the event of a disaster, OneXafe Solo quickly boots backup images as virtual machines using Arcserve's VirtualBoot technology. And since data protection is both host-based and agent-based, total physical and virtual system recovery will get you back in business quickly.

Organisations with distributed networks can now say goodbye to the days of remote office uncertainty thanks to the integrated software, appliance and cloud solution for data protection.

OneXafe Solo functions as a Service Leader and Service Node with native hypervisor API-based backup and restore capability. This is embedded in OneXafe Solo appliance, which will scale from one to many, depending on the number of servers at the remote office.

To simplify the registration, deployment and management process, the OneXafe Solo Service Leader includes the ability to call home for automatic appliance claiming. This makes life easy for IT staff as non-IT personnel can power up and connect the device to the Internet. Once this is done, everything else is managed remotely by IT.



OneXafe® Solo

The ideal solution for RoBo backups, offsite data protection, disaster recovery and business continuity.

OneXafe Solo provides ultimate flexibility with a range of deployment options independent of the IT environment. It can be deployed in places with no or little local storage or virtual environments, ensuring secure data protection. With its set-and-forget capability, OneXafe Solo enables efficient management of data protection without requiring dedicated resources, whether staffing or capital.

In the event of a problem, OneXafe Solo can recover a virtual machine in milliseconds with patented VirtualBoot technology; files or folders in seconds; and entire systems in minutes. By offering recovery to anywhere, from anywhere, it is integrated with Arcserve purpose-built, self-service disaster recovery cloud.

Benefit from easy DRaaS with Arcserve Cloud Services

Protecting RoBo data is critical for every distributed organisation. To ensure total business continuity, local data must be transferred to a remote location to eliminate the risk of data loss. Arcserve Cloud Services meets this requirement in an automated way.

A site-wide disaster, such as a fire, can destroy local backups, which would result in significant downtime and data loss for a business. By replicating OneXafe Solo backup images directly to Arcserve's disaster-recovery cloud, organisations get the tools they need to keep business running no matter what happens.

Arcserve Cloud Services delivers a fully automated and orchestrated cloud-based DRaaS to protect RoBo systems and data for total business continuity. This includes:

- ✓ **Accessible:** Access cloud data anywhere, anytime
- ✓ **Predictable**: Set monthly pricing. Choose the service level based on your needs
- ✓ **Resilience:** Highly distributed and fault-tolerant DR cloud with 99.999+ percent uptime
- ✓ **Testable:** Pre-stage a site-wide failover processes for one-click testing or execution of a failover
- ✓ **Granular:** Everything from file and folder recovery and machine virtualization to instant failover of an entire site and network
- ✓ **Management:** Centrally manage your cloud backup and recovery with an easy-to-use, self-service online portal
- ✓ **Security:** Only you can access stored backup images
- ✓ **Seamless:** Complete control over networking allows for seamless failover during a disaster

OneXafe Solo uses Arcserve OneSystem for cloud-based management from anywhere, anytime through any web browser.

This eliminates the need for onsite dedicated servers and time-consuming software upgrades to manage data protection. OneSystem manages OneXafe Solo's data protection workflow with a true SLA-based protection framework. Policy creation is intuitive with all the ingredients that make up the SLA— backup frequency, retention policy, target location, and replication for cloud disaster recovery.

OneSystem allows IT professionals to centrally manage multiple OneXafe Solo deployments across multiple RoBo locations very easily.

It is not a case of if disaster happens, but when disaster will happen

Businesses cannot be without their critical data for long. Yet, a large-scale disaster can readily disrupt systems and make doing business impossible.

Building out your own data center for disaster recovery is costly. But Arcserve Cloud Services™ lets you control costs by letting you customise services to fit business needs and budget. Plus you will never be surprised with extra fees at the time of recovery. When the worst happens, know that data is safe, recoverable, and available.

99.999+ uptime

Conclusion

Protecting RoBo data is more important than ever. With more people working from home and remote locations, data has the potential to be more disparate and less controlled.

IT professionals now have the option of an integrated software, appliance and cloud services to vastly improve how data generated in remote locations is protected and restored in the event of a problem.

Disaster recovery should not be an afterthought. Modern DRaaS solutions enable effective, affordable off-site data protection and a better ability to get back in business when an incident occurs.

Take the Next Step

**Find out more at arcserve.com
or contact us at info@arcserve.com
or view all our contact details here.**

About Arcserve

Arcserve, a global top 5 data protection vendor, provides the broadest set of best-in-class solutions to manage, protect and recover all data workloads, from SMB to enterprise and regardless of location or complexity. Arcserve solutions eliminate complexity while bringing best-in-class, cost-effective, agile, and massively scalable data protection and certainty across all data environments. This includes on-premises, cloud (including DRaaS, BaaS, and Cloud-to-Cloud), hyperconverged, and edge infrastructures. The company's nearly three decades of award-winning IP, plus a continuous focus on innovation, means that partners and customers, including MSPs, VARs, LARs, and end-users are assured of the fastest route to next-generation data workloads and infrastructures. A 100% channel-centric organization, Arcserve has a presence in over 150 countries, with 19,000 channel partners helping to protect 235,000 customers' critical data assets. Explore more at arcserve.com and follow @Arcserve on Twitter.