arcserve®

SaaS Platform Data Security with Arcserve SaaS Backup

Backup and Recovery for Critical SaaS Data

A Security White Paper

Executive Summary

Information security has never been more important—or challenging—than it is today. There are growing threats from external actors and insiders, new systems and software are being deployed faster and more frequently than ever before, the zero-trust model is leading to widespread changes in visibility and access control, and economic pressures demand that costs be reduced or avoided altogether.

At the same time, IT leaders also need to ensure appropriate data privacy and protection throughout the company's entire tech stack.

These evolving demands exist at a time when a range of workloads—from customer-facing applications to business-critical operational systems—have migrated from on-premises appliances and servers to third-party cloud environments.

The cloud-based software platforms bring the agility and availability organizations require, but they also introduce new challenges. One of the least-recognized issues is a shared data responsibility model for ownership of data backup and recovery. Significant to business continuity planning and disaster recovery practices, many organizations overlook the challenge in restoring data from SaaS business platforms.

Backing up cloud SaaS platform data is the responsibility of the SaaS customer, not the vendor. However, this reality is not yet well understood within the IT circle, and with that lack of understanding comes significant risk:

More than 60% of organizations experienced security incidents related to public cloud usage*

*DatapaceLift.io, 100+ Cloud Security Statistics for 2025

When IT teams store SaaS data backups in the same cloud as their regular organizational data backups, a risk is presented. Many organizations have not yet recognized that backing up SaaS data within the same public cloud infrastructure that hosts their primary data fails to provide complete recovery assurances. An event impacting that public cloud could render both the primary and backup data inaccessible, even with geographic distribution.

Many organizations choose to backup SaaS platform data in an infrastructure completely independent from public cloud environments. Leaders are choosing Arcserve SaaS Backup—a vendor-neutral and dedicated SaaS data backup solution that is resilient, secure, and exceptionally easy to use. This solution stores data in a separate private cloud, lowering business continuity risks.

Arcserve SaaS Backup has a security-first design, with required features that meet the needs of even the most demanding enterprises. The same care is extended to its physical and operational security. As an added benefit, constructing and managing the infrastructure in-house allows to offer the backup service with a predictable, inclusive pricing structure.

The State of SaaS Data

As software-as-a-service (SaaS) applications enable modern businesses, critical services are migrating from on-premises computing facilities to cloud providers, far away from traditional backup solutions. As organizations generate significant business data in SaaS applications, this creates a significant amount of data that's stored outside of the usual IT-managed data environment.

This shift introduces a shared responsibility model in which the SaaS provider and the SaaS customer-you- each assume ownership of particular responsibilities with respect to data security (Figure 1).

Unfortunately, many organizations will learn the hard way that relying on their SaaS provider to keep their data safe is a risky proposition: more than 60% of organizations experienced security incidents related to public cloud usage in 2024.

*DatapaceLift.io, 100+ Cloud Security Statistics for 2025

arcserve®

While adoption of cloud-based SaaS services has soared, some organizations are only now beginning to understand the implications of shared data responsibility.

To help organizations avoid disruption due to lost SaaS data, Arcserve offers a dedicated, vendor-neutral SaaS data backup solution that is resilient, secure, and easy to use—and that's provided with a predictable, inclusive pricing structure.

In this guide, learn how this dedicated cloud backup environment helps you provide secure data resilience for SaaS data. Understand how specific SaaS backup security standards, practices, and features protect your data.

First, why is a dedicated data protection cloud needed?

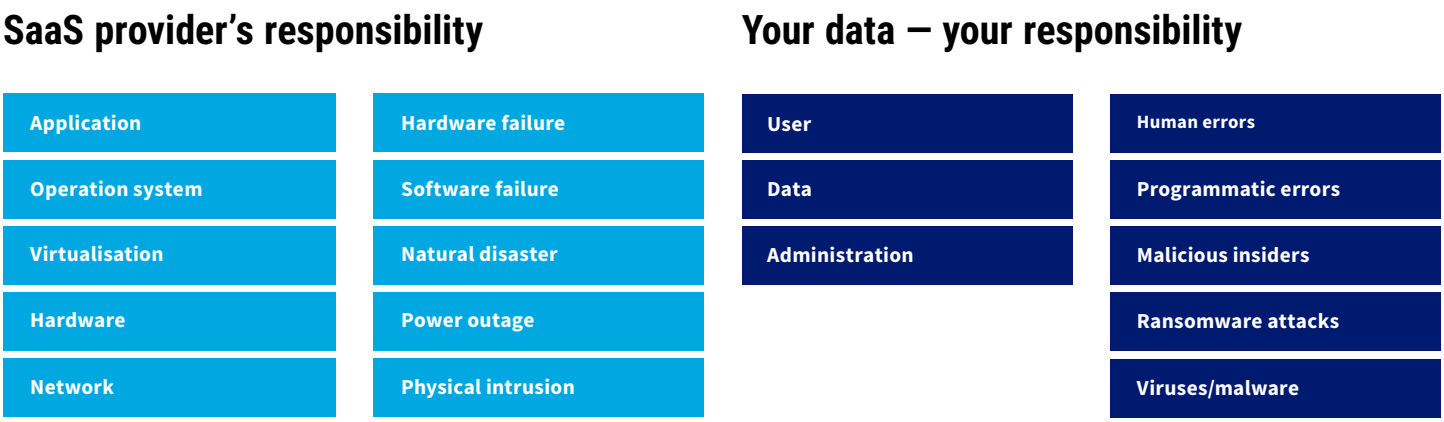


Figure 1—Division of responsibilities between the SaaS provider (left) and the SaaS customer (right)

Why Arcserve SaaS Backup uses a dedicated cloud

Key Takeaways:

- Storing all business data in one cloud has risks. Public cloud comes with significant security compromises (and introduces hidden risks); Arcserve SaaS Backup operates independent cloud data center regions, running on independent hardware, managed by a separate group of people.
- Once a customer chooses an Arcserve SaaS Backup region for backup, their data never leaves that region.
- An independent cloud allows Arcserve to manage supply chain risks and provides tremendous control over costs, which enables you to have simple and predictable "all-in" pricing.

The 3-2-1 principle of backup (Figure 2) mandates that you must have one copy of your data off site. In the days of tape backup, where fire and theft were the only credible threats to your backup data, the off-site copy effectively ensured that your backup data would survive any calamity that could befall your primary data and your primary site.

Figure 2—The time-tested 3-2-1 principle of data backup

In the cloud age, however, backups have become much more complicated: geographic dispersal is insufficient to ensure your data is secure, and hidden risks are introduced by relying on clouds that may be taken offline to protect the providers' primary business interests.

arcserve®

True data backup requires a separate logical infrastructure

While the requirement for separate backup infrastructure may seem self-evident to many IT and security professionals, most alternative cloud backup solutions will readily store your backup directly on the same cloud infrastructure that hosts your primary data—introducing unnecessary risk and really stretching the meaning of "backup."

You can choose to store your backup data in the public cloud, and you can even specify a data center location that is separate from your primary data—but in no way does this approach provide the assurances that you need, because your data (now including your only SaaS data backups!) is now managed under the same administrative infrastructure.

Consequently, if that infrastructure is compromised, then both your primary data and your backups are at risk, no matter if they reside on servers in different parts of the country or even on different continents.

For many IT leaders, "true backup data protection" means planning backup data storage locations that do not reside on the same logical infrastructure as their primary data, regardless of which combination of primary workloads are being protected.

"True backup requires a logical infrastructure separate from the primary data"

To ensure that your backups are not stored on the same cloud infrastructure that hosts your primary data (e.g., Amazon Web Services, Microsoft Azure, etc.), Arcserve SaaS Backup does not run on public cloud infrastructure. Instead, dedicated cloud infrastructure is used:

- runs in its own data center regions
- operates on its own hardware
- is managed by its own staff

To ensure data sovereignty, once a customer chooses an Arcserve SaaS Backup region for backup, their data never leaves that region.

Not only does Arcserve guarantee that backup data will always go to that region, but no processes exist that even could transfer backup data out of that region (aside from customer initiated restores and downloads, of course).

Americas

USA, Washington, D.C.

Toronto, Canada

EU

Copenhagen, Denmark
Frankfurt, Germany

EMEA

London, UK
Zurich, Switzerland

APAC

Sydney, Australia

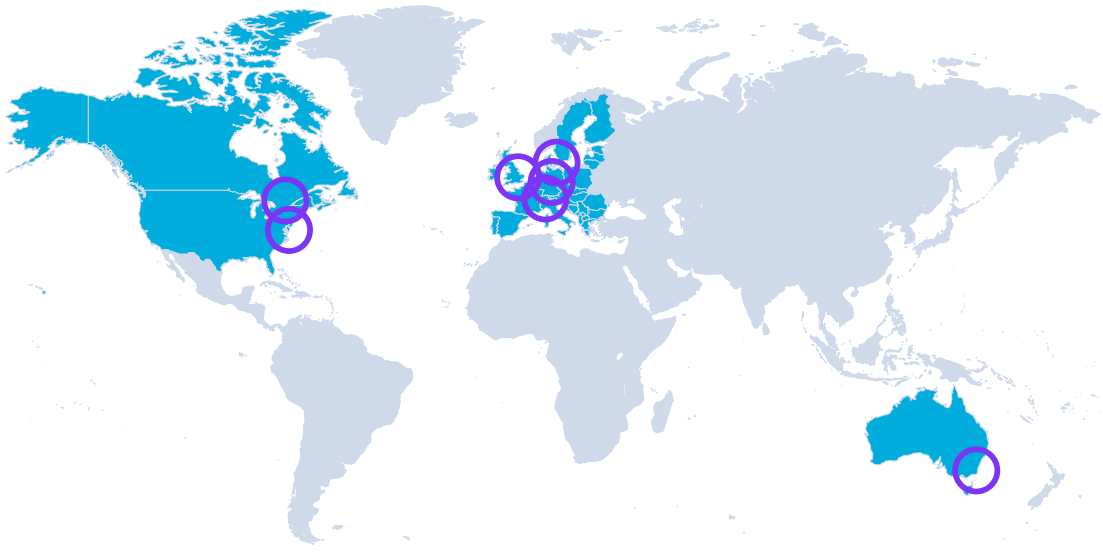


Figure 3: The dedicated cloud spans the globe with seven locations, each of which has two data centers

arcserve®

Gaining control and managing hidden risks

Aside from the fact that a dedicated private cloud is a fundamental requirement of any legitimate backup solution, a separate cloud gives Arcserve SaaS Backup a higher degree of control over both the supply chain and costs, with considerable benefits for customers.

This dedicated private cloud strategy was especially valuable when the COVID-19 pandemic struck. To protect their own primary businesses, many public cloud vendors shut down customer workloads, forcing thousands of those customers offline. Even through turmoil, normal operations continued at the dedicated private cloud used by Arcserve SaaS Backup.

Passing along the benefits

Why Arcserve SaaS Backup customers don't worry about deduplication, compression, and storage

Arcserve SaaS Backup is designed to make SaaS platform data backup and recovery clear and easy for your team.

- Simple licensing model: There are no complicated API transaction fees, network egress or ingress fees, or even storage consumption fees. That's right; storage is included— Arcserve SaaS Backup customers don't need to worry about deduplication capabilities or compression ratios!
- Predictable pricing: Even as the storage technology behind the scenes evolves with technology standards.

Customers and partners are not impacted by the cost structures around the underlying storage. System improvements can continue regardless of how this will affect byte-for-byte consumption.

Single payment for backup and storage functionality: In BYOS (Bring Your Own Storage) business models, the customer effectively pays twice: once for the backup service and once more for the public cloud storage onto which the backup data is subsequently copied.

With Arcserve SaaS Backup, the price you pay encompasses both the backup technology and the storage capacity.

Raising the bar for secure SaaS backups

Key Takeaways:

- Resilience and data immutability are achieved through immediate encryption of backup data, 30-day delete retention, data region sovereignty and dual data center redundancy, and a unique, tamper-proof infrastructure.
- A blockchain-like Merkle tree architecture and innovative "incremental forever" data transfer ensure secure, reliable, and change-based long-term data storage.
- Restoring from a backup is quick and easy: simply browse and search through time and space, then click to restore once you find what you lost with our multiple restore options.

Arcserve SaaS Backup provides a number of important fundamental features and characteristics, including:

- Vendor-neutrality
- Resilience and data immutability
- Secure, reliable, and change-based long-term data storage
- Easy and fast data recovery unparalleled in the industry

The following subsections describe these in detail.

Vendor-neutrality

Today's organizations rely on a growing list of SaaS applications and providers, headlined by Microsoft Office 365 and Dynamics 365, Google Workspace (formerly GSuite), Salesforce, and Zendesk. It is imperative that any practical SaaS data backup solution supports these services, otherwise clients will be burdened with the extra overhead, complexity, and potential risk that comes with maintaining multiple backup systems.

Moreover, the SaaS vendor ecosystem is always expanding. Accordingly, Arcserve SaaS Backup is completely vendor agnostic, meaning there is no technical reason why support for a particular SaaS application provider cannot be introduced in addition to the major vendors already integrated into the platform (Figure 4).

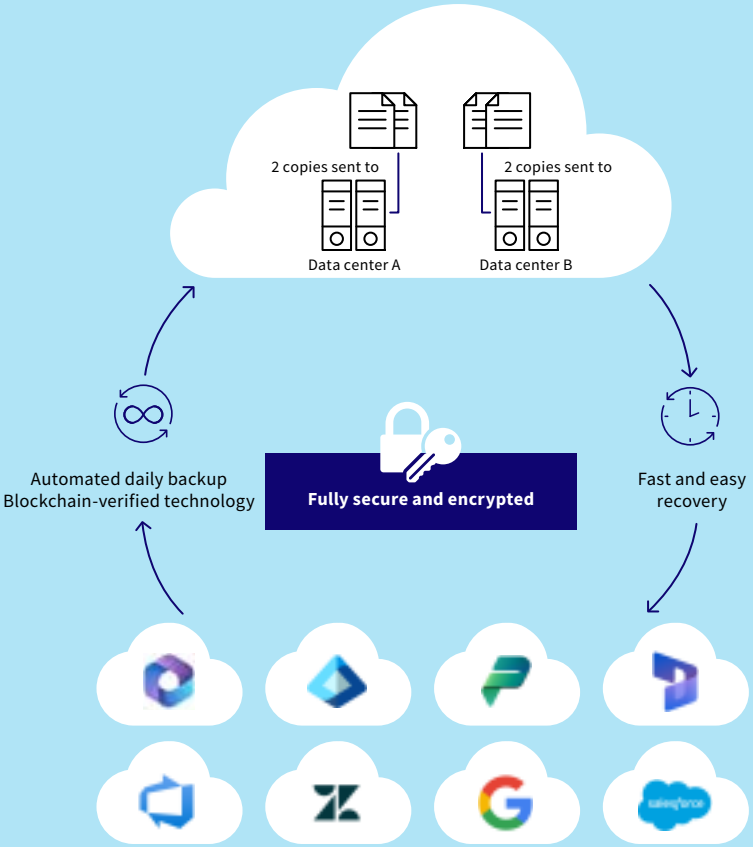


Figure 4— Arcserve SaaS Backup is completely vendor agnostic

arcserve®

Resilience and data immutability

To ensure security while maintaining convenience, Arcserve SaaS Backup combines several protective measures (Table 1).

Protective Measure	Benefits
Immediate encryption	Upon ingestion by the Arcserve SaaS Backup solution, backup data is immediately encrypted before it is written to storage media. This process employs industry best practice algorithms believed to offer unbreakable security for at least the next 30 years.
30-day delete lock	There is no simple way to immediately delete your data in Arcserve SaaS Backup. You, or the attacker who has successfully taken over your identity, will have to wait 30 days for datasets to be deleted or for accounts to be closed. This deliberate delay is the first line of defense against user error, insider threats, and ransomware attacks that target backups.
Data region sovereignty and dual data center redundancy	To comply with data sovereignty requirements and desires for geographical dispersal of information assets, Arcserve SaaS Backup offers multiple data storage regions around the world. Once your data enters a given region, your data stays in that region - forever. To provide protection from the most common disasters such as fire, power, or cooling system outages—or other events that can render a building or complex of buildings unusable—all data is copied into two separate data center facilities within the chosen region.
Unique, tamper-proof infrastructure	The Arcserve SaaS Backup infrastructure runs on software that was designed and built from the ground up. This proprietary storage infrastructure allows for fast and reliable backup at a reasonable cost. Additionally, this structure supports data immutability - the disk-based storage systems do not offer a mechanism for modifying backup data. This core characteristic means that even in a nightmare scenario—e.g., administrative accounts are compromised, primary data is corrupted or encrypted, attackers gain access to your backups—there is no way for the system to comply with an attacker's efforts to tamper with your backup.

Table 1—These protective measures ensure security without limiting convenience

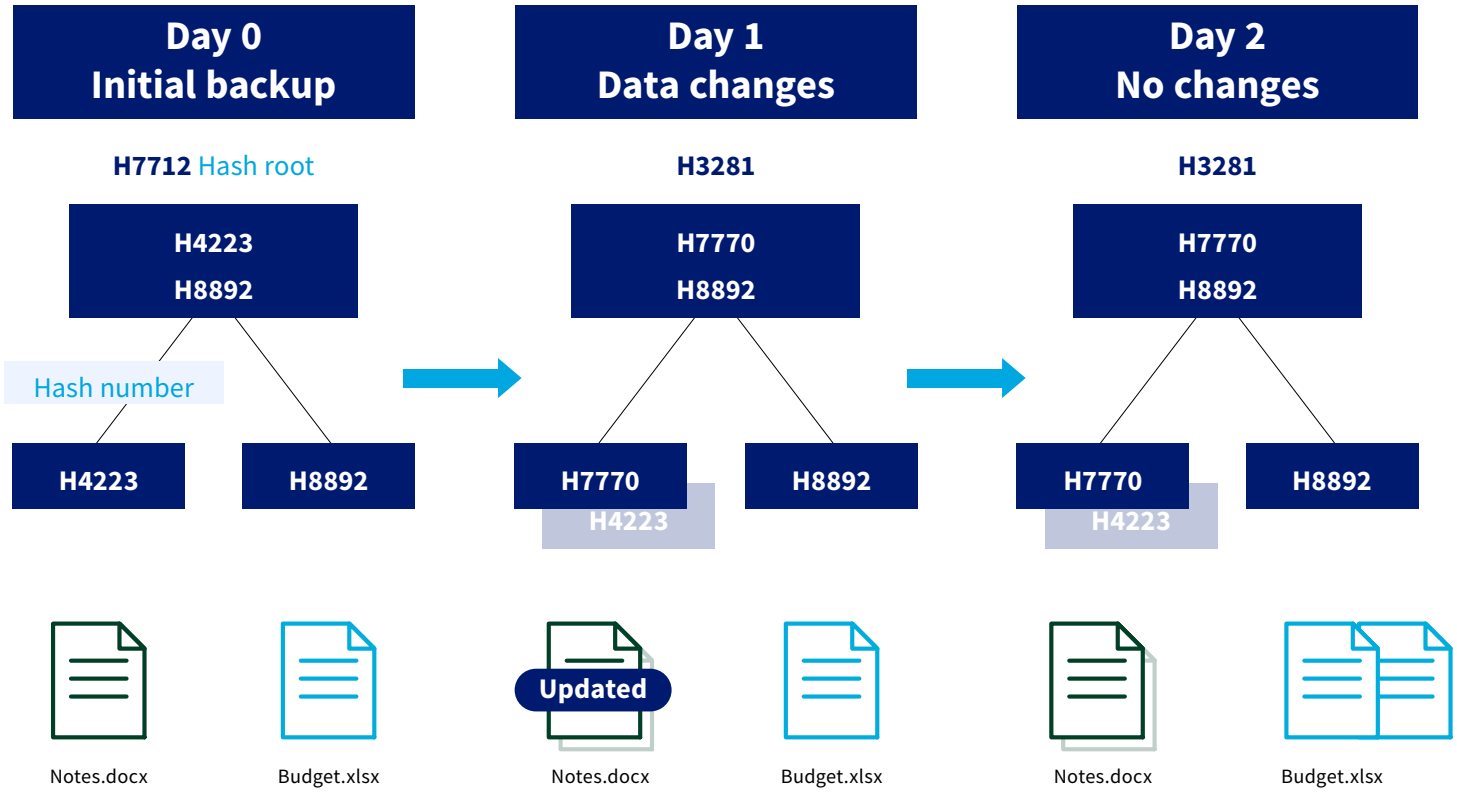
arcserve®

Secure, reliable, and change-based long-term data storage

Arcserve SaaS Backup was designed for the specific purpose of providing secure and reliable long-term storage for SaaS backup data. In pursuit of this objective, a uniquely powerful information architecture was created (Table 2). It employs a Merkle tree structure and an innovative “incremental forever” approach to deliver performance and cost benefits that would simply not be possible on general-purpose storage services.

Architectural Element	Benefits
Merkle Tree architecture	The Arcserve SaaS Backup information architecture is inspired by the Merkle tree structure that gained renown from blockchain systems such as Bitcoin and the ‘git’ version control system. In addition to providing benefits including strong consistency checks, this design also provides the opportunity to represent and access backup sets over time—completely removing the antiquated model of ‘full’ and ‘incremental’ backups, along with all the overhead associated with that legacy approach.
“Incremental forever” data transfer	In the Arcserve SaaS Backup data model, when a backup executes, the system only transfers the differences in your dataset. When you view your data in Arcserve SaaS Backup, all access is instant across time and space, and every single backup—no matter how old—appears as if it was a standalone full copy of your dataset at the time it was taken. Data is additionally protected with one more step. With an object storage architecture designed from scratch, backup data is stored very efficiently on simple high-density hard drive-based storage systems, which simplifies the supply chain and lowers both the risk and the price point for customers.

Table 2—By rethinking information architecture, Arcserve SaaS Backup provides secure and reliable long-term backup with unmatched performance



- We make the initial backup, including the files, notes, and budget.
- The files get structured in a Merkle tree, including hashes.
- A hash is a unique identifier for a particular subset of data.

- Notes is updated and is given a new hash.
- The hash root has also changed.
- The budget remains the same, as it has not been modified.

- No data changes - hash root remains the same.

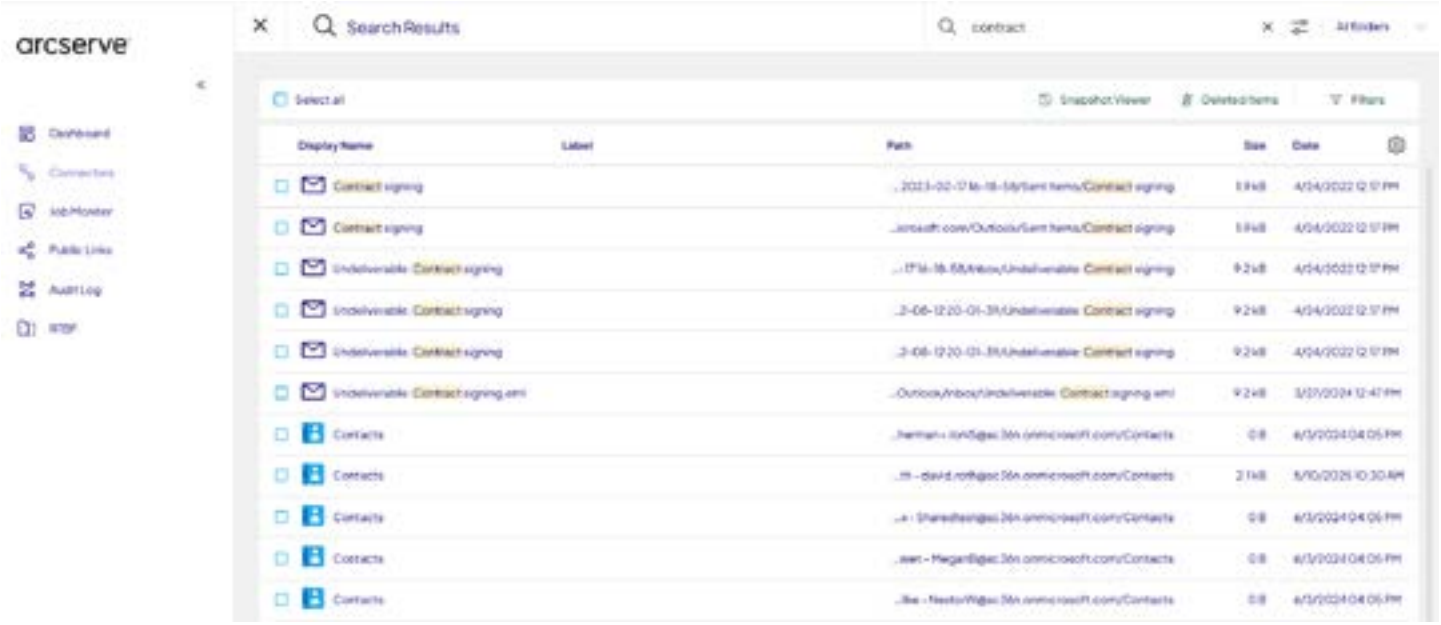
Figure 5—The Merkle Tree architecture

Unparalleled easy and fast data recovery

What good is reliable backup if you can't find what you're looking for, or if it takes days or weeks to recover your data?

With Arcserve SaaS Backup, all data is instantly accessible. To restore from a backup, simply search for or browse to the data you need and click "Restore." All your data with all your history is readily available for you in a modern web-based user interface that offers not only live browsing but also provides previews, downloads, and restores of your data elements.

And that's it—there are no extra steps. You browse and search through time and space, and you click the button once you find what you've lost. The efficiency of the restore process is unparalleled in the market.



Security standards, practices, and features

Key takeaways:

- Technical and organizational measures are in place to ensure operational security. Arcserve SaaS Backup infrastructure demonstrates its ability to deliver best-in-class security technology to its customers by holding the ISO/IEC 27001:2013 certification and the ISAE 3402-II certification.
- Mature software development lifecycle processes ensure that security is incorporated from the inception of a new project and continued throughout the entire life of the system.
- To enhance protection of customer data, Arcserve SaaS Backup incorporates TLS transport security and secure, logged access controls; the recommended best practice for deployment uses the customer's existing authentication infrastructure by means of SAML integration.

Providing secure backup demands more than just a secure platform design. Security extends to the physical and operational aspects of the platform and must be ingrained in the software development lifecycle.

Physical security

As noted in Table 1, once backup data reaches Arcserve SaaS Backup, it is immediately copied into systems in two separate data centers within the designated region.

This practice provides resilience in case a facility is permanently lost (e.g., to fire or a natural disaster) and also ensures continuous availability of data in case of a more benign facility problem (e.g., temporary failure of power or cooling systems).

In every region, Arcserve SaaS Backup operates in active-active mode between the two data centers. This model:

- Allows Arcserve SaaS Backup to continue virtually uninterrupted in the unlikely scenario that a full building is incapacitated
- Provides system-level redundancy, allowing Arcserve SaaS Backup to continue servicing customers in case any single system is lost or needs to be taken offline for service, upgrades, maintenance, or repairs

This system-level redundancy is complemented by significant component-level redundancy on the individual servers that host Arcserve SaaS Backup.

Components that most commonly fail on modern servers (e.g., cooling fans, power supplies and spinning disks) can typically be hot swapped without even powering down the system holding the failed component.

Figure 7—Each region has dual data centers which typically hold the above certifications.

While there are some local differences between the regions[2], all data center facilities employed by Arcserve SaaS Backup must conform to a physical security baseline that:

- Ensures high availability
- Restricts access to the physical systems that constitute Arcserve SaaS Backup

Physical security at a facility can feature a combination of multi-factor authentication including biometric identification for facility access, controlled access with man traps, CCTV monitoring of the facility and facility perimeter, plus onsite security staff.

Typically, the processing facilities will hold an ISO 27001 certification and several complementary certifications such as SOC-2, ISAE 3402, PCI/DSS, HIPAA, etc.

When providing large-scale storage, failure of storage media is a regular and undramatic event. Failed storage media is never sent back to the media vendor for analysis; instead, it is kept onsite for physical disintegration (mechanical shredding) before being disposed of, upholding the commitment that customer data never leaves its designated region.

Additionally, and as noted previously, customer backup data is encrypted before it is written to storage media. Therefore, even in the most unlikely event that a storage device is stolen from a processing facility, any data on the media remains inaccessible.

Operational security

When it comes to backup and recovery, businesses seeking solutions need to be incredibly thorough in their due diligence processes. Arcserve SaaS Backup service is ISO 27001:2013, ISAE 3402-II, and SOC 2 Type 1 compliant.

End-to-end ISO/IEC 27001:2013 compliance

The ISO/IEC 27001:2013 compliance demonstrates the dedication and ability to deliver best-in-class security technology to customers.

Rest assured that all involved processes live up to the highest international security standards.

[2] Please consult your Arcserve sales representative for details.

arcserve®

Benefits of ISO/IEC 27001:2013 compliance

- A systematic, verified approach to information security that results in superior customer data protection
- Ongoing performance evaluations and audits that ensure continued adherence to the requirements of the ISO/IEC 27001 standard
- Continued improvement of business continuity management and disaster recovery plans
- Risk, vulnerability, and security incident management practices that enhance overall information technology (IT) operations security
- Compliance with current and future legal and regulatory requirements

ISAE 3402-II compliance

Arcserve SaaS Backup infrastructure holds the ISAE 3402-II certification.

On top of the conditions required by ISAE 3402-II certification, there's a number of additional operational security measures in place (Table 3).

Operational security measure	Explanation
Automation	The Arcserve SaaS Backup service is fully automated, operating based on the instructions (i.e., the configuration) provided by the customer. Therefore, no human operators outside of the customer's own organization are involved in accessing, reviewing, or otherwise processing actual customer data.
Restricted access	Arcserve SaaS Backup itself is regularly updated as part of the ongoing maintenance and evolution of the service. However, there are no recurring or routine tasks that require human operators to access customer data. Furthermore, there are technical measures in place to ensure that no such access is required and that it is not easily or accidentally invoked. Additionally, there are organizational measures in place to educate and train staff on information security practices and policies.

Operational security measure	Explanation
Regional support	If a customer needs assistance—and in the rare event that this assistance involves access to actual customer backup data— Arcserve SaaS Backup support organization will work with the customer. Requests are served by support staff in an appropriate region, considering data sovereignty requirements, support availability, and time constraints.
Third-party security assessments	External auditors are employed for security assessments. The solution is also subject to regular penetration testing conducted by third-party security and risk management specialists. This process replicates the tactics threat actors employ to gain Initial Access[3], and extends beyond simple automated security scanners (which we also employ, of course).

Table 3—Arcserve SaaS Backup employs a number of operational security measures

SOC 2 Type 1 compliance:

Arcserve SaaS Backup SOC 2 Type 1 compliance underscores its commitment to safeguarding customer data with industry-leading security and operational rigor. This compliance means that Arcserve SaaS Backup delivers stringent trust service criteria, including security, availability, and confidentiality, providing customers with the assurance that their critical information is stored and managed in accordance with the highest standards.

Operational insights

To ensure reliable around-the-clock operation, production systems' physical operational health and software stack health are closely monitored (Table 4).

[2] Please consult your Arcserve sales representative for details.

Operational concern	
Physical operational health	Tens of thousands of datapoints are measured every minute, They're then aggregated and made instantly available to the operational staff, ensuring efficient investigation and mitigation to meet the high uptime guarantees. System and data center performance is continuously compared to baseline thresholds, while the health monitoring system monitors the physical equipment (e.g., environmental, network, hardware, operating systems and services) with 30-second granularity, alerting on a range of unwanted situations (e.g., high temperatures in data centers, failing disks in storage systems, congested network connections that threaten to impede ingress and egress, etc.)
Software stack health	A Real-Time High-Frequency Event Monitoring (RTHFEM) system provides specific deep stack insights on software components and their operational health. The operations team has different dashboards and areas of interest they follow and monitor, and live metrics can even be shared across organizational groups to provide developers with real-world insights into how their code performs in production. The RTHFEM system provides insights into data ingress rates from different SaaS vendors and quickly identifies problems, should they arise within the software stack. Backend engineers also use this system to troubleshoot specific customer-related situations based on anonymized views of the interoperability of each customer's connectors, data estate, and index. Additionally, detailed insights into software processes can assist with determining if an SLA is at risk or if an anomaly might be an indicator of malicious activity.

Table 4—Operational insights provide timely feedback, visibility, and alerts

Software development lifecycle

Arcserve is dedicated to providing best-in-class solutions for cloud-to-cloud backup and data management. Involved software development lifecycle processes (Figure 8) ensure that security is incorporated from the inception of a new project and continued throughout the entire life of the system. These mature processes have been refined over the years but are being continually evolved.

Strong processes are a necessity for the secure development of new functionality for Arcserve SaaS Backup. While information sharing is vital in any growing organization, segregation of duties is also an essential part of the actual execution of development, qualification, and—ultimately—deployment of software.

There's a number of technical and organizational measures in place to ensure that only the software approved by the Quality Assurance team goes into production. By enforcing significant workflow around "simple things" like software deployment, a high degree of confidence is achieved in any and all software that is deployed to production and, in case a problem is discovered, that it can be rolled back or hot fixes can be applied efficiently (once qualified).

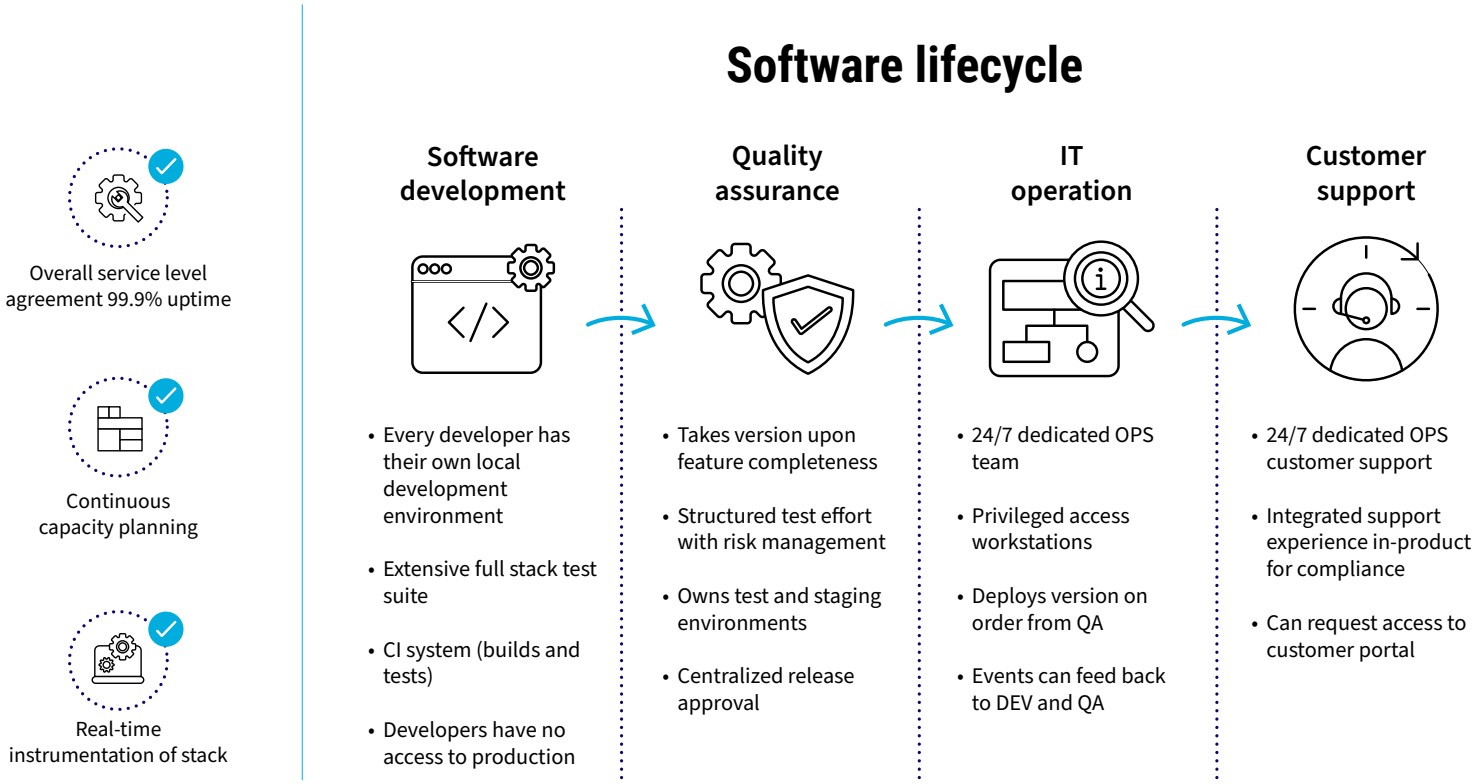


Figure 8—A mature and agile security-oriented software delivery methodology for Arcserve SaaS Backup

Security features

In addition to the measures already presented (e.g., regional lock-in, dual data center redundancy), Arcserve SaaS Backup also incorporates a number of additional security features to enhance protection of customer data. Two of the most important things to govern are transport security and access control (Table 5).

Security feature	Explanation
TLS transport security	**TLS transport security** All primary workloads supported by Arcserve SaaS Backup employ modern Transport Layer Security (TLS) encryption on the endpoints used by Arcserve SaaS Backup and customers to access data. Both the Web UI and mobile app require the use of TLS. These communication protocols are designed to provide safe transport of data over insecure networks such as open Wi-Fi or broadband internet connections. **Network security** Additionally, to ensure a short path and the fastest possible data exchange with the primary customer data clouds for backup and restoration, Arcserve SaaS Backup connects directly to major internet exchanges.
Secure and logged access controls	**Single sign-on** Arcserve SaaS Backup recommended best practice for deployment uses the customer's existing authentication infrastructure (such as AD/ ADFS, Okta, etc.) by means of SAML integration. This approach allows customers to leverage the identity security measures they already have in place (e.g., multi-factor authentication). **Fine-grained role-based access control** Inside Arcserve SaaS Backup, an elaborate access control list (ACL) and role-based access control (RBAC) system allow fine-grained control over which identities can perform which operations on the customer tenant. For example, pre-defined policies permit an administrative role to manage the backup and a support role that can only restore data in place (as part of an internal IT support role) and cannot download or otherwise exfiltrate data from the platform. Additionally, separate groups of administrators can manage separate backup configurations; for example, one group can manage the Salesforce or Dynamics 365 backup while another manages the Microsoft Office 365 or Google Workspace backup. **Immutable system audit log** Finally, an audit trail is maintained for the duration of the customer engagement. The audit log can be viewed directly in the web application by authorized administrators, and it can be accessed via the API for integration into third-party log analysis solutions. Data can also be pushed to Splunk, Sentinel or other third-party SIEM systems.

Table 5—Security features provide additional protection for data in transit and at rest

arcserve
SaaS Backup

Conclusions

With increasing numbers of business-critical SaaS applications migrating to the cloud, and in a world in which new threats arise daily, continuity planning demands a secure SaaS data backup solution—and the SaaS vendors are clear that backups are your responsibility, not theirs.

The question then becomes: where to back up this critical data?

> **"SaaS vendors are clear that data backups are your responsibility, not theirs."**

Best practices outline a separate logical infrastructure from the cloud in which the primary data is hosted. The most practical solution, then, is a dedicated cloud platform.

But simply having a dedicated platform is not enough: the platform must be secure.

However, security is not something that can be bolted on as an afterthought—it needs to be designed into the very essence of a system. This secure-by-design philosophy guided the creation of the Arcserve SaaS Backup solution, architected from the ground up by information security and hosting experts to provide secure backup of SaaS data:

- Resilience and data immutability are achieved through immediate encryption of backup data, 30-day delete retention, data region sovereignty and dual data center redundancy, and a unique, tamper-proof infrastructure with immutability by default
- A blockchain-like Merkle tree architecture and innovative "incremental forever" data transfer ensure secure, reliable, and change-based long-term data storage
- All data center facilities employed by Arcserve SaaS Backup conform to a high physical security baseline and hold ISO 27001 certification plus complementary certifications (e.g., SOC-2, ISAE 3402, PCI/DSS, HIPAA)
- Technical and organizational measures are in place to ensure operational security, including a high degree of automation, comprehensive staff training, third-party security audits, proactive penetration testing, and detailed operational monitoring of the health of physical infrastructure and the software stack
- Mature software development lifecycle processes ensure that security is incorporated from the inception of a new project and continued throughout the entire life of the system
- To enhance protection of customer data, Arcserve SaaS Backup incorporates TLS transport security and secure, logged access controls

These characteristics and others combine to form a SaaS data backup solution that is fundamentally different from other products in the market. It provides you with the benefits of offsite storage and the comforting knowledge that if your primary cloud is compromised, your backup is safe and secure elsewhere.

To learn more about Arcserve SaaS Backup, please visit arcserve.com/saas or request a demo.