Osterman Research
WHITE PAPER

White Paper by Osterman Research
Published **June 2024**
Commissioned by **OpenText**

Backing Up Cloud Workloads to Achieve Security and Compliance Mandates

Executive summary

Many organizations continue to believe that cloud providers are responsible for protecting their data in SaaS apps from all types of data loss, even when cloud providers explicitly opt out of assuring data integrity under the shared responsibility model. When the inevitable happens and data is lost via a cyberattack or deletion action in the normal course of business operations, organizations are faced with the startling realization that their data is actually gone—and the cloud provider can do nothing about it. The data is lost. Irretrievably so.

But there is an alternative, albeit one that requires a decision upfront to assure recovery whatever happens to the cloud provider, whether during a ransomware attack, a malicious insider rampage, or deletion that happens in the normal course of business operations. The alternative is an approach that diligent IT organizations always used to practice—with relentless discipline—in the age of on-premises IT infrastructure. As an increasing proportion of organizations embrace an ever-growing set of SaaS applications, reinstituting solid data backup processes for data in SaaS applications enables organizations to achieve security standards and compliance mandates.

> ***Cloud providers explicitly opt out of data integrity responsibilities, which requires organizations to act proactively to protect against data loss events.***

KEY TAKEAWAYS

The key takeaways from this research are:

- **Widespread usage of SaaS applications across businesses**
  Organizations are embracing hybrid IT environments, leveraging both on-premises infrastructure and cloud services for delivering applications for use by employees, customers, and partners to drive strategic and tactical benefits.
- **SaaS applications are not invulnerable to data loss**
  Data in SaaS apps is lost through ransomware and other malicious attacks, data wiping malware, human error, and deletion operations carried out in the normal course of business, among others. Most organizations struggle to recover lost data without the availability of third-party backups.
- **Cloud providers explicitly opt out of responsibility for data integrity**
  In the shared responsibility model for cloud services, cloud providers do not take responsibility for the integrity of data created by each organization—and neither should they. Assuring data integrity is a responsibility explicitly held by organizations using the service.
- **Regulations require data in SaaS applications to be backed up**
  A solid data backup approach for all data—even data in SaaS applications—is required for meeting a growing body of data protection and other industry regulations, e.g., GDPR, HIPAA, PCI-DSS, and FINRA.
- **Clear and compelling reasons for embracing a third-party backup service**
  While some SaaS vendors offer native backup for their apps, using a third-party backup service that works in a unified, coherent, and consistent approach across multiple SaaS services has clear and compelling benefits.

ABOUT THIS WHITE PAPER

This white paper was commissioned by OpenText. Information about OpenText is provided at the end of the paper.

The move to SaaS applications

Organizations are embracing hybrid IT environments, leveraging both on-premises infrastructure and cloud services to deliver applications for use by employees, customers, and partners. Cloud applications, or SaaS (software as a service), are attractive for many reasons:

- **Costs are met out of operating budgets, not capital ones**
  Expensive deployments of networking equipment, servers, and disaster recovery arrangements are increasingly a legacy approach to offering business applications. These large-scale projects were met out of capital budgets and took many months to plan and even more to deploy and stabilize. Now business applications are licensed from cloud providers with monthly or annual recurring costs paid out of operating budgets—thereby negating the need for capitalization complexities and eliminating elongated planning and deployment timelines.

- **Time to value is significantly reduced**
  After an organization decides to use a SaaS application to drive a customer-facing, employee-enabling, or partner-equipping process, the timeframe from decision to initial usage is measured in minutes and hours. By comparison, when on-premises infrastructure must be deployed and managed, timeframes are measured in months to years depending on the complexity of the setup. This shrinking of time to initial use flows through to a significant reduction in time to value.

- **IT modernization and increased security posture**
  Embracing SaaS applications provides organizations with a rapid way of modernizing their IT ecosystem. In addition, due to the nature of modern cyberthreats against cloud platforms, many SaaS providers have stronger security controls that organizations themselves have not put in place. Security and data protection with SaaS applications is clearly subject to a shared responsibility model versus the full and complete responsibility model incurred with on-premises deployments.

SaaS apps are widely used for strategic business benefits as well as for tactical reasons.

There are several tactical reasons why organizations find themselves with a set of SaaS applications in addition to the strategic reasons above. These include:

- **Adoption by business units to circumvent glacial IT procurement processes**
  If official IT procurement processes for new business applications take too long, business units incentivized on delivering outcomes that depend on those new applications will often make their own arrangements. This leads to under-the-radar adoption of unsanctioned SaaS applications, which over time become entrenched as the way work is done within the business unit. Dislodging these applications becomes increasingly difficult.

- **Consequential adoption due to business partner usage**
  Processes that feature engagement with business partners highlight new ways of working as employees are exposed to the applications that business partners make use of. This means that organizational data is stored in SaaS applications controlled by external parties. There is a second implication as well. Exposure to new SaaS applications during a productive work process creates an increasing likelihood that employees will create their own instance of the SaaS application for their own internal processes.

How data is lost in SaaS applications

SaaS applications are not invulnerable to data loss. Some types of "data loss" occur in the normal course of operating any application (e.g., deleting redundant information or records), while other types are malicious in nature. In this section, we look at various types of data loss in SaaS applications.

LOSS OF DATA BY DELIBERATE MALICIOUS INTENT

Malware attacks, ransomware attacks, and credential compromise attacks can result in data being deleted or corrupted in SaaS applications. One study documented the use of multiple attack vectors in ransomware attacks against SaaS applications, with stolen user credentials (67%), malicious or vulnerable third-party applications (58%), and attacks on the SaaS provider infrastructure (38%) seen most frequently.[1]

Examples of loss by malicious intent include:

- **Phishing for credentials**
  Phishing is a very common attack vector for credentials and sensitive data, with Symantec at one point tracking an average of 135 million attempted phishing attacks per day.[2] Business email compromise (BEC) attacks, a financially oriented type of phishing attack, are also very common, with Microsoft detecting an average of 156,000 attempts per day for the year to April 2023.[3] While many attempts are detected, many others get through to the inbox—and most organizations suffer the consequences of multiple phishing and BEC attacks each year that result in lost credentials that could be used for deleting business data in SaaS applications (most often Microsoft 365).

- **Hyperscale SaaS providers under relentless attack**
  Hyperscale SaaS providers that have attracted hundreds of millions or billions of users are under relentless attack by cyberthreat actors. Almost all organizations rely on cloud services from Microsoft or Google (or both), two services with very high attack rates. Microsoft and Google both regularly appear in lists of the world's most impersonated brands—which cyberthreat actors find useful for tricking unsuspecting and unprepared victims.[4]

- **Microsoft compromised by state-sponsored and state-supported hackers**
  Microsoft—the enterprise and cloud software provider that so many government agencies and commercial organizations rely on for providing high-security offerings—has itself suffered several embarrassing security incidents in recent years. An attack by China-based hackers compromised email accounts at U.S. government agencies after stealing a master key for creating authentication tokens.[5] Another attack, this time by state-sponsored Russian hackers, resulted in Microsoft's own corporate tenant on Microsoft 365 being compromised, resulting in data theft from senior Microsoft executives and wider snooping over several months. Some of Microsoft's customers were also impacted because of the breach.[6] The attack could easily have been focused on deleting data.

- **Mobile carrier employees targeted to join criminal activities**
  Cyberthreat actors recently targeted employees at mobile carriers in the United States offering payment for issuing replacement SIM cards. The threat actors were hoping that the enticement of a payment per SIM swap would turn

> ***Stolen user credentials, malicious third-party apps, and attacks on the SaaS provider are commonly seen attack vectors that threaten data.***

employees into internal criminal collaborators.[7] Access to a customer's mobile phone number—through the replacement SIM—would allow threat actors to gain access to multi-factor authentication codes used for accessing SaaS applications, which could then be used for high-reputation phishing attacks, data theft, and data destruction.

DATA WIPING MALWARE

Ransomware threat actors encrypt and/or exfiltrate data for ransom and extortion, but have generally tried to undo their malicious actions once a ransom payment is made (although the efficacy of decryption has often been lacking, resulting in data loss for victims nonetheless). Other threat actors are not interested in financial gain from malicious activities. Their modus operandi is to inflict unrecoverable damage to make a statement, for reasons including terror, politics, hacktivism, or revenge. Cybersecurity threat reports have noted an increase in the use of wiper malware against organizations in recent years.[8]

LOSS OF DATA BY HUMAN ERROR

Users and administrators with valid authorization to access and perform actions within the SaaS application can delete data by mistake, believing they are doing one thing but actually doing another. If there is no undo option, the data is gone. Or, if the mistake is only recognized sometime later, it is no longer possible to use any available undo function.

Such a mistake happened at a large professional services firm. The firm had a retention policy for chats in Microsoft Teams. The authorized IT administrator edited the policy to remove one user's account from the policy, but the requested change went wrong and was applied to 145,000 people. Consequently, the personal chat histories in Microsoft Teams for all users were lost—and Microsoft had no way of recovering them.[9] The firm worked with Microsoft to make Teams "less dangerous to data."

> ***Creating an enduring backup posture for SaaS application data enables data recovery at any point in the future for any point in the past.***

LOSS OF DATA THROUGH NORMAL OPERATIONS—THAT ONLY LATER BECOMES A PROBLEM

Tidying up, cleaning up, and rearranging data in business applications are normal parts of maintaining a performant application and driving maturity in use. When normal operations include deletion of records, data can be irretrievably lost. What the employee believes to be an appropriate action in the moment can become a problem downstream—perhaps weeks, months, or years later when that data is urgently needed.

Under general provisions for a shared responsibility model by cloud providers, most data loss situations are the organization's responsibility. Creating an enduring backup posture for SaaS application data enables data recovery at any point in the future for any point in the past.

LOSS OF DATA BY UNFORESEEN PROGRAMMATIC ERRORS OR UPDATES

Software errors, updates gone wrong, and other unforeseen situations caused by the cloud provider can result in data loss. While cloud providers will do their best to reverse the effects of any issues they have caused, this is not guaranteed. Even never-seen-before problems only mean they have not been seen, not that they will not happen in the future.

UniSuper, a large retirement fund provider in Australia, experienced such an incident in May 2024. The firm experienced a never-seen-before disruption to its Google Cloud services that resulted in its account being deleted. It was described by UniSuper and Google Cloud as "*… an isolated, 'one-of-a-kind occurrence' that has never before occurred with any of Google Cloud's clients globally. This should not have happened. Google Cloud has identified the events that led to this disruption and taken measures to ensure this does not happen again*." Recovery at UniSuper hinged on the use of backups with a third-party service provider.[10]

LOSS OF DATA BY MALICIOUS INSIDERS

Employees have legitimate access to data stored in SaaS applications, which can be weaponized against the organization by malicious insiders in situations of disgruntlement, revenge, and collusion with external threat actors. These types of insider threats have often been difficult to identify since the access is legitimate and the actions taken are within the normally exercised rights of the individual. It has often been discovered too late that data has been stolen, corrupted, or deleted.

> ***Recovering data after a data loss incident affecting a SaaS application has not been straightforward or easy for most organizations.***

RESEARCH ON RECOVERY AFTER DATA LOSS

Recovering data after a data loss incident affecting a SaaS application has not been straightforward or easy for most organizations. The research data says:

- **It does not happen quickly**
  79% of respondents to one study said data recovery took days, weeks, or months; only 21% were able to recover within a day.[11] A different study found that only 31% were able to complete all remediation and recovery processes within a week.[12] A third study said the average recovery time was 24 days.[13]

- **It may not happen completely**
  Only half of organizations responding to one study were able to recover all their data after a ransomware attack that affected a SaaS application.[14] Another study found that only 65% of data on average was restored after organizations paid the ransom for swift recovery after a ransomware attack.[15] A third study found that among companies that lost data from Microsoft 365, only 15% were able to recover 100% of their data—and this proportion declined from the previous research study commissioned two years earlier.[16]

- **It doesn't happen without costly downtime**
  When SaaS applications are unavailable due to a malicious attack, business processes are compromised. Downtime costs are often estimated from the low thousands per minute[17] to more than four times that amount.[18] In other situations, the inability to produce required documentation that has been deleted maliciously or by accident can result in the loss of a customer order, a customer entirely, a lawsuit, or a regulatory audit with costly downstream consequences.

The argument for backing up SaaS applications

With the multidimensional threat of data loss in SaaS applications, organizations need to ensure they have the right capabilities in play to achieve security standards and meet compliance obligations. In this section, we look at what is required.

BACKING UP YOUR DATA IS YOUR RESPONSIBILITY

The use of cloud services has immediate productivity and efficiency benefits that are visible across an organization, but there are background responsibilities to meet for locking in long-term value. Cloud providers become partners in delivering long-term value, and hence there is a shared responsibility model that exists between providers and organizations. This model outlines who is responsible for what in the operation and use of cloud services. It is merely standard business practice.

In a shared responsibility model, cloud providers naturally take responsibility for managing the cloud infrastructure, maintaining or upgrading computer and storage capabilities, offering a performant and highly available service, and being ready to restore service operations in the event of a significant cyberattack or any other type of disaster (e.g., fire, earthquake, hurricane). It would be weird if organizations were responsible for any of these tasks.

What cloud providers do not take responsibility for—and neither should they—is the integrity of data created by each organization. If an employee deletes a file stored in a SaaS application, the cloud provider should not have to call the organization's CEO to ask if this is a correct action. If data is moved from one site to another, updated based on changing information, or deleted entirely when an employee leaves, these are organizational responsibilities—not cloud provider ones. The cloud provider must establish the right guardrails in their SaaS application so these actions happen within the context of appropriate authorization. But the interference of a cloud provider in all data creation, modification, and deletion events would be an untenable proposition.

> ***Cloud providers explicitly state that they are not responsible for backing up customer data.***

To make clear the responsibilities held by organizations for safeguarding the integrity of their data, some cloud providers explicitly state that they are not responsible for data backup:

- Microsoft: *We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services.* (Microsoft Services Agreement, Section 6b).[19]

- Salesforce: *It is important for Salesforce customers to develop a routine data backup strategy as part of their overall data management and security model.*[20]

Google's approach is less explicit, starting with a statement about enabling customers to delete data: *[Section 6.1 Deletion by Customer] Google will enable Customer to delete Customer Data during the Term in a manner consistent with the functionality of the Services. If Customer uses the Services to delete any Customer Data during the Term and that Customer Data cannot be recovered by Customer, this use will constitute an Instruction to Google to delete the relevant Customer Data from Google's systems in accordance with applicable law.*[21]

In other words, if data is deleted by the customer and Google can't get it back, it's not Google's problem.

The first argument for backing up SaaS applications, therefore, is that it is not a responsibility of the cloud provider and is a responsibility of each organization using cloud services.

BACKING UP DATA TO ENABLE RECOVERY AFTER A DISASTER

Disaster recovery planning processes historically focused on infrequent but catastrophic natural events such as earthquakes, floods, fires, and the like. With the investments made by cloud providers in multiple data centers, replication, and high availability, such disasters are now much less likely to inflict the costs they previously did on individual organizations operating with a much smaller technology footprint.

The disasters to mitigate are now of a different nature. It is much more likely that organizations will have to enact disaster recovery processes following a cyberattack that exploits a vulnerability, exposure, or misconfiguration; the use of ransomware or malware against the organization; or mistaken deletion that is processed by the cloud provider resulting in all copies of the data being lost. Every organization is a potential target for these types of cyberattacks and deletion processes, and without a data backup strategy that encompasses SaaS applications, organisations are at risk of catastrophic data loss events.

BACKING UP DATA TO MEET COMPLIANCE MANDATES

Organizations subject to the growing body of data protection regulations and those in highly regulated industries must ensure they have a solid data backup approach for all data, even data in SaaS applications. SaaS is an IT infrastructure, not an IT excuse.

A data backup approach needs to cover the full extent of data stored and processed in SaaS applications, including metadata for chain of custody, sharing settings, access rights, and other tags or labels used within the service to present the data to appropriate personnel, enforce security settings, and enable the data to work within the context of the information system.

> ***Organizations subject to the growing body of data protection regulations and those in highly regulated industries must ensure they have a solid data backup approach for all data, even data in SaaS applications.***

Applicable compliance mandates include:

- **GDPR, Article 32 on availability and access to personal data**
  Article 32 is the "security of processing" provision in the General Data Protection Regulation. It states that controllers (under GDPR, organizations using SaaS services) and processors (the SaaS cloud providers themselves) "implement appropriate technical and organizational measures" to ensure ongoing availability and resilience of systems; be able to restore availability and access to personal data; and have a process for regularly testing the efficacy of these (and other) technical and organizational measures. Since cloud providers—or processors in GDPR terminology—explicitly exclude backup of customer data stored in SaaS applications as a condition of service delivery, organizations must do it themselves.

  Additionally, encryption of personal data is a core control recommended by GDPR. Backups require this too.

- **HIPAA Security Rule for data backup**
  Organizations handling personal health information (PHI) in the United States are required to meet data backup requirements per the HIPAA Security Rule. Backups must support the 3-2-1 approach at minimum (three copies of data, stored on two forms of media, with one stored offsite); strong data encryption; the ability to restore and recover data; and daily, weekly, monthly, and annual backup schedules. Backups must be created, tested, and assessed for efficacy, and the overall process strengthened as required. Any organization subject to HIPAA that is using SaaS applications for PHI must ensure they meet these backup requirements. With the frequency with which healthcare organizations are under cyberattack—and succumb to those attacks—being on the right side of the HIPAA Security Rule is essential.

- **PCI DSS requirements for data backup**
  The PCI DSS (Payment Card Industry Data Security Standard) sets out mandatory data security requirements for organizations accepting payments by credit and debit cards. One requirement is that access to cardholder data is restricted, and that backups are stored in a separate and remote location to the primary storage location. When SaaS apps are used to store cardholder details, backing up those SaaS apps using a third-party backup service contributes to achieving and maintaining PCI DSS compliance.

- **FINRA 4511**
  FINRA (Financial Industry Regulatory Authority) sets rules for brokers and broker-dealers in the United States. Rule 4511 covers the protection of records across multiple content channels, requiring record retention for at least six years with no ability to surreptitiously change the records, and with a dictate to store a second copy of all records at an offsite location for purposes of disaster recovery and resilience.[22] With the increased use of SaaS applications for internal and external communication, broker and broker-dealer firms must ensure they are abiding by these requirements. By backing up covered data in SaaS applications, broker and broker-dealer firms can ensure they will not lose any data due to human error, cyberattack, or platform malfunction. By using a backup solution that offers immutable storage options, organizations covered by FINRA 4511 can safeguard their data and meet their compliance obligations.

Organizations subject to HIPAA must meet the data backup requirements in the HIPAA Security Rule.

Finally, for any organization subject to data sovereignty mandates—either externally imposed or in line with corporate regulations—being able to control where data in SaaS applications is backed up to is essential.

THIRD-PARTY VERSUS NATIVE BACKUP FOR SaaS APPLICATIONS

Organizations embracing a backup strategy for SaaS applications need to decide whether they use the native backup options available from their cloud provider or use a third-party backup service. We can compare and contrast each approach (see Figure 1).

Figure 1
Comparing third-party and native backup services for cloud services

Attribute	Third-party backup service for multiple SaaS services	Native backup options offered by each SaaS service
Scope of service	Backup that works with multiple SaaS services	Backup that works with one SaaS service
Nature of approach	Unified, coherent and consistent approach across all services	Nuanced approaches for each SaaS provider
Support for restructuring of content	More likely to offer non-destructive restoration and re-allocation of content as needed	Restoration more likely to be destructive to current data, e.g., overwrites current data
Option to export data for local download	Yes, with the scope dependent on the access rights of the accessing individual	Yes, with the scope dependent on the access rights of the accessing individual
Importance of the approach to the vendor	Primary service offering with emphasis on world-class design and performance	Backup service capabilities of much lower priority than the primary SaaS offering; more likely to deprecate service offerings
Optimization of the service offering	Features offered to minimize setup and ongoing administrative overhead	Optimization less likely to be a high focus since engineering effort detracts from improving the primary SaaS offering
Process of restoration	Streamlined and designed for repeated usage	Tedious and designed for one-off or infrequent usage
Who can use the service	Administrators (with account-level privileges) and individual users (with self-service privileges covering their own data)	Administrators only

Source: Osterman Research (2024)

A third-party backup service that works across multiple SaaS services offers a unified, coherent and consistent approach to backing up all SaaS services.

Salesforce, for example, specifically paints this difference between their native backup offering and third-party backup offerings: *There are a number of data backup solutions offered by our partners on our AppExchange. Some of these are more comprehensive in that they allow you to automate backups of both your data AND your metadata and provide a mechanism by which to restore that data easily.*[23]

Reasons for not backing up SaaS applications

While a strong case can be made for backing up data in SaaS applications—as we have done in this white paper—we lay out the inverse in this section. If an organization decides that they will not back up their data in the SaaS applications they use, what is the rationale? Here are five possibilities:

- **The risk of data loss is not worth the cost of a backup service**
  After running the numbers on the likelihood of a data loss event affecting your organization—including malicious deletion, programming errors, accidental mistakes, and the like—the nested if-then statements result in such a low likelihood of loss that the cost of a backup service is out-of-balance by comparison. You are sufficiently confident that your cyber defenses are world-class and will keep malicious actors out of your SaaS applications, that your SaaS providers have bulletproof change processes, and that all your employees have all the right training and cautions so mistakes won't happen.

- **The data stored in SaaS applications is not important enough to warrant the use of a backup service**
  While your organization does use SaaS applications and while you do have data in SaaS application that you see as your responsibility, the data itself is not of much consequence. Its value is low and is not worth protecting against loss. The data is not needed for any ongoing business operations—you could operate just as well without it. And it is not subject to any regulatory oversight—no regulatory body would express any concern about the loss of data.

- **Hyperscale cloud providers are unlikely to suffer a significant data loss event**
  With the advantages available to SaaS cloud providers—massive capital budgets, the ability to attract top-flight cybersecurity and IT talent, and the defense in depth security infrastructure they put in place—the likelihood of something going wrong is perceived as being small. Put another way, you hope your cloud provider will never suffer a security incident or outage that negatively affects your business and its data. It was good that UniSuper, the large retirement fund provider in Australia, went beyond hope. After experiencing a never-seen-before disruption to its Google Cloud services that resulted in its account being deleted, recovery hinged on the use of backups with a third-party service provider.[24]

- **Prefer to believe cloud providers are responsible for your data, even though they explicitly state they are not**
  While the shared responsibility model for cloud services explicitly states that organizations are responsible for the data they store and process in cloud services, some proportion of organizations refuse to accept this could be the case. One study found that 25% of organizations were in this group[25]—and your organization is one of them. If the worst happens and your data is lost, you will take the cloud provider to court or join a class action suit to contest your losses.

- **Your employees always do everything perfectly and no one makes mistakes**
  Human error, one of the causes of data loss in SaaS applications, is something that never happens at your organization. It always happens to the other guy. Therefore, since you can rely completely on your employees and executives to always do the right thing, backups to counteract human error are not necessary. No one ever makes mistakes at your organization.

While the shared responsibility model for cloud services explicitly states that organizations are responsible for the data they store and process in cloud services, some proportion of organizations refuse to accept this could be the case.

Conclusion

Unless organizations take initiative to assure recovery of data in SaaS applications, a cyberattack, malicious insider, or deletion action by an authorized individual will inevitably result in unrecoverable data. For the growing roster of organizations subject to compliance mandates, such as GDPR, HIPAA, and FINRA, data backup is a required capability to assure the integrity of covered data types irrespective of where it is stored. Using SaaS apps for business purposes does not give organizations a free pass to these security and compliance mandates; if anything, it elevates the intensity of assuring data integrity because cloud providers explicitly state they are not responsible for data loss.

> ***Using SaaS apps for business purposes does not give organizations a free pass to security and compliance mandates.***

About OpenText

OpenText™ is The Information Company™. We are the No. 1 information management software and services company in the world. We power and protect information to elevate every person and every organization to gain the information advantage and be their best. OpenText offers a comprehensive portfolio of solutions for content, business network, digital experience, security, analytics and AI, DevOps, IT operations management, and developer APIs.

For more information about OpenText, visit www.opentext.com

www.opentext.com

@OpenText

+1 800 499 6544

OPENTEXT DATA PROTECTOR

OpenText Data Protector is an enterprise-grade data backup and recovery software solution designed to help organizations protect their critical data across physical, virtual, and cloud workload environments. It provides centralized management of backup and recovery operations, enabling IT administrators to efficiently protect and recover their data across a wide range of platforms and applications. With Data Protector, organizations automate backup and recovery tasks, reduce the risk of data loss, and improve reliability and efficiency of their IT operations. Data Protector delivers secure, compliant backups of all your company data from a single management point. Fast restoration ensures operations quickly return to normal, minimizing revenue loss and maintaining reputation.

Visit www.opentext.com/products/data-protector

DATA PROTECTOR FOR CLOUD WORKLOADS

Data Protector for Cloud Workloads is an agentless backup software solution for modern workloads. Providing enterprise class protection for Microsoft 365 workloads as well as an extensive range of hypervisors, containers, and cloud storage targets.

Visit www.opentext.com/products/data-protector-for-cloud-workloads

CLOUDALLY

CloudAlly provides ISO 27001-certified and GDPR/HIPAA-compliant SaaS backup and recovery solutions. CloudAlly comprehensively protects Microsoft 365, Google Workspace, Salesforce, Dropbox, and Box SaaS data with secure automated cloud-to-cloud backup and easy recovery from any point in time with unlimited data retention. Additionally, CloudAlly offers unlimited storage and tier-one customer service.

Visit www.cloudally.com

Osterman Research does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

[1] Odaseva, The State of SaaS Ransomware Attack Preparedness, August 2022, at https://go.odaseva.com/web-2022-q3-resource-saas-ransomware-report-lp

[2] Robert Grimmick, Phishing Attacks: Types, Prevention and Examples, July 2023, at https://www.varonis.com/blog/phishing-attacks

[3] Microsoft, Microsoft Cyber Signals report highlights spike in cybercriminal activity around business email compromise, May 2023, at https://news.microsoft.com/apac/2023/05/22/microsoft-cyber-signals-report-highlights-spike-in-cybercriminal-activity-around-business-email-compromise/

[4] James Coker, Microsoft Most Impersonated Brand in Phishing Scams, April 2024, at https://www.infosecurity-magazine.com/news/microsoft-impersonated-brand/

[5] D. Howard Kass, Chinese Hackers Breached State, Commerce Dept.'s Email Accounts, Microsoft and U.S. Say, July 2023, at https://www.msspalert.com/cybersecurity-news/chinese-hackers-breached-state-commerce-dept-s-email-accounts-microsoft-and-u-s-say/

[6] Microsoft Security Response Center, Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard, March 2024, at https://msrc.microsoft.com/blog/2024/03/update-on-microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

[7] Richi Jennings, SIM Swappers Try Bribing T-Mobile and Verizon Staff $300, April 2024, at https://securityboulevard.com/2024/04/sim-swap-bribe-t-mobile-300-richixbw/

[8] Derek Manky, Key Findings from the 2H 2022 FortiGuard Labs Threat Report, February 2023, at https://www.fortinet.com/blog/threat-research/fortiguard-labs-threat-report-key-findings-2h-2022

[9] Thomas Claburn, IT Blunder Permanently Erases 145,000 Users' Personal Chats in KPMG's Microsoft Teams Deployment - Memo, August 2020, at https://www.theregister.com/2020/08/24/kpmg_microsoft_teams/

[10] UniSuper, A joint statement from UniSuper CEO Peter Chun, and Google Cloud CEO, Thomas Kurian, May 2024, at https://www.unisuper.com.au/about-us/media-centre/2024/a-joint-statement-from-unisuper-and-google-cloud

[11] Odaseva, The State of SaaS Ransomware Attack Preparedness, August 2022, at https://go.odaseva.com/web-2022-q3-resource-saas-ransomware-report-lp

[12] Veeam, 2022 Ransomware Trends Report, June 2022, at https://go.veeam.com/wp-ransomware-trends-report-2022

[13] Pure Storage, Life Cycle of a Ransomware Attack, at https://www.purestorage.com/knowledge/life-cycle-of-a-ransomware-attack.html. Accessed May 2024.

[14] Odaseva, The State of SaaS Ransomware Attack Preparedness, August 2022, at https://go.odaseva.com/web-2022-q3-resource-saas-ransomware-report-lp

[15] Sophos, The State of Ransomware in Government 2021, June 2021, at https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-state-of-ransomware-in-government-2021-wp.pdf

[16] Enterprise Strategy Group, The Evolution of Data Protection Cloud Strategies, April 2021, at https://www.techtarget.com/esg-global/research-report/research-report-the-evolution-of-data-protection-cloud-strategies

[17] Chris Hoff, Ransomware: Secure Backup Is Your Last Line of Defense, April 2022, at https://www.veeam.com/blog/secure-backup-ransomware-defense.html

[18] Osterman Research, Application Security in a Multi-Cloud World 2023, November 2023, at https://ostermanresearch.com/2023/11/17/radware-multi-cloud-2023/

[19] Microsoft, Microsoft Services Agreement (United States), September 2023, at https://www.microsoft.com/en-us/servicesagreement

[20] Salesforce, Best practices to back up Salesforce data, May 2024, at https://help.salesforce.com/s/articleView?id=000386692&type=1

[21] Google, Cloud Data Processing Addendum (Customers), April 2024, at https://cloud.google.com/terms/data-processing-addendum/

[22] FINRA, 4511. General Requirements, December 2011, at https://www.finra.org/rules-guidance/rulebooks/finra-rules/4511

[23] Salesforce, Best practices to back up Salesforce data, May 2024, at https://help.salesforce.com/s/articleView?id=000386692&type=1

[24] UniSuper, A joint statement from UniSuper CEO Peter Chun, and Google Cloud CEO, Thomas Kurian, May 2024, at https://www.unisuper.com.au/about-us/media-centre/2024/a-joint-statement-from-unisuper-and-google-cloud

[25] Odaseva, The State of SaaS Ransomware Attack Preparedness, August 2022, at https://go.odaseva.com/web-2022-q3-resource-saas-ransomware-report-lp

248-000040-001