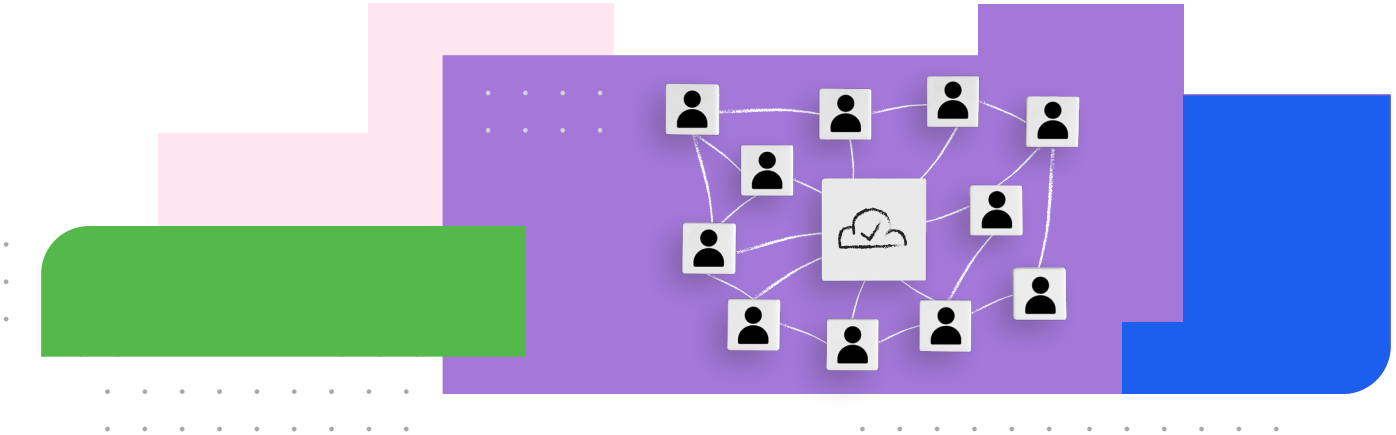
caseware

Cloud Security: Iron-clad Protection for Modern Accounting Firms

www.caseware.com

Contents



Introduction

Ask most business leaders for a single reason why they may be reluctant or entirely opposed to moving their company's data and applications to the cloud and you'll likely hear a common refrain — we don't trust that the cloud is a secure place to do business.

They'll reason that if data doesn't reside within the physical confines of an organization's brick-and-mortar facilities then it can't possibly be safe. Or that the internet can't be made secure and data transmitted and received across a public network will be intercepted, corrupted or stolen. Then there's the belief that third-party management of information won't ensure confidentiality and the computing resources of a cloud provider are not as reliable as an organization's internally owned and managed resources.

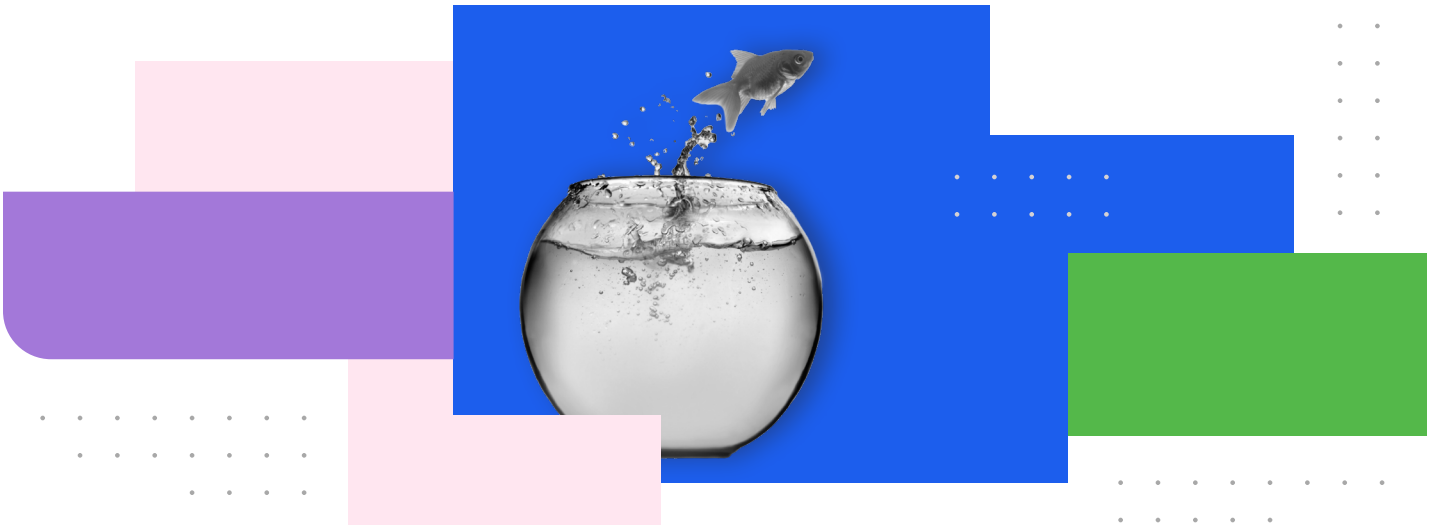
But these perceptions of cloud-based computing are simply not in line with the reality of what the cloud truly is today. In fact, for most businesses, including accounting firms, the cloud is the most secure environment for storing data and the most reliable and easiest way to access business applications.

Today's major cloud service providers apply the most comprehensive and advanced cybersecurity tools and solutions, their facilities are among the most secure anywhere, and they employ many of the world's best data security experts.

The business world has made the move to the cloud and the accounting industry is likewise pivoting and realizing newfound savings, efficiencies and application customization capabilities.

Cloud-based accounting software gives accountants greater flexibility in how they work and simplifies the way their tasks are performed. The cloud delivers dynamic collaboration capabilities and enriches workflows by optimizing and extending accounting processes. Caseware's *2022 State of Accounting Firms Trends Report* surveyed 3,000 respondents and observed that "nearly two-thirds of accountants plan to adopt some form of cloud computing technology over the next two years...and a third are expecting to do so within the next 12 months."

This report will show how the cloud has evolved to become a safer and much more reliable computing environment than most accounting firms and organizations can recreate "in house." It will outline the key cybersecurity features and functions used by most cloud service providers that make the cloud a reliable and secure platform for accounting software. And we will see the types of cloud services available today, explain why businesses of all types have moved en masse to the cloud, and detail the security frameworks, standards and protocols accounting and audit leaders should look for when considering a cloud service.



Why is there reluctance to move to the cloud?

As mentioned previously, unease around the security and privacy of data is among the sources of reluctance and hesitancy to move operations to the cloud. There's fear of losing control of data, having to trust a third party with confidential and important information, concerns about what constitutes strong security on public networks, and worries regarding whether cloud service providers can adhere to necessary compliance mandates that govern accounting and the financial industry.

Let's address these concerns separately:

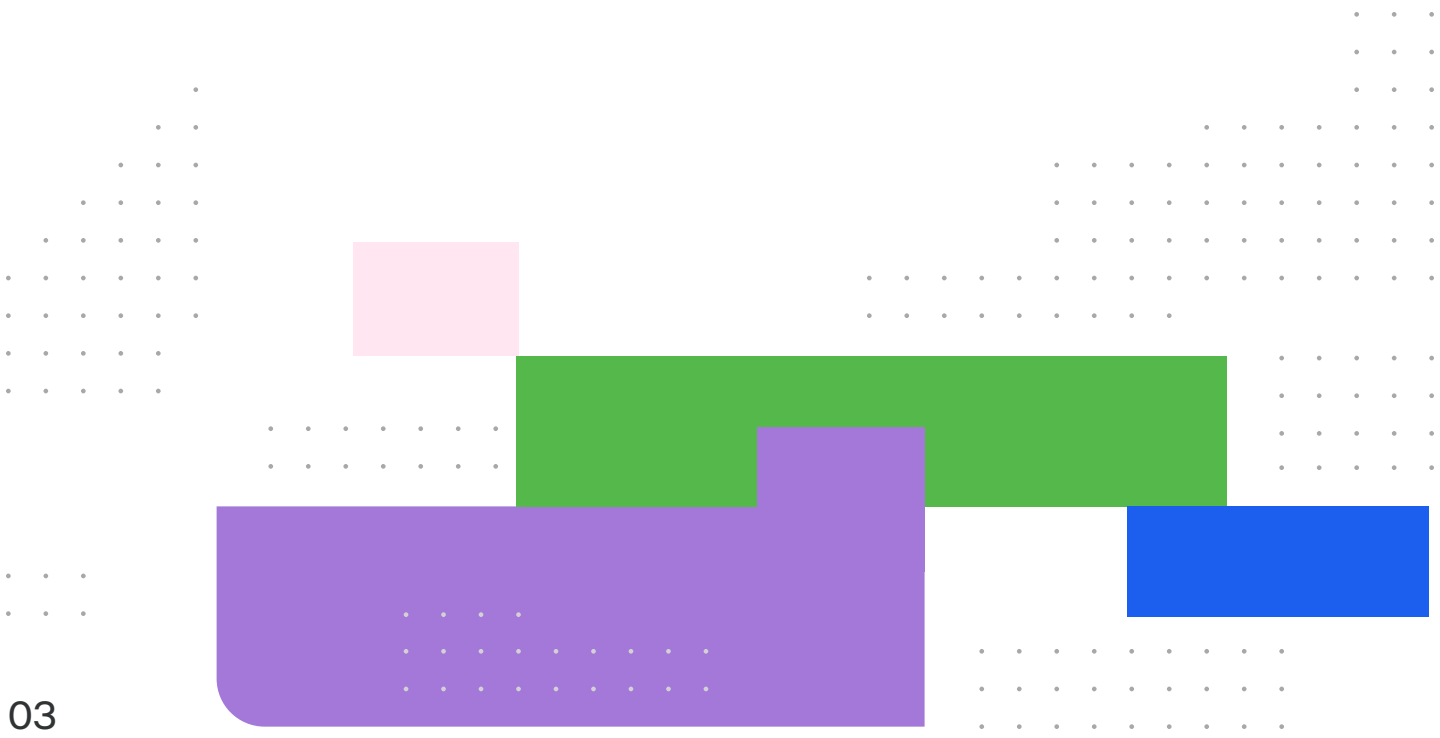
1. **Losing control of data:** There may be a leap of faith to be made when letting go and moving data and information to a third party — beyond the walls of a business's corporate offices and out from under the management of an in-house IT department. But cloud service providers have proven their reliability. Today, 60 percent of all corporate data is stored in the cloud and the percentage continues to rise every year. In 2021, cloud data centers processed 94 percent of all workloads, with 75 percent of those workloads tied to software-as-a-service (SaaS). Cloud service providers have been in business for many years and have proven they can be trusted to protect data and apply necessary due diligence to secure applications, operating systems, networks and physical data centers. Through data loss prevention (DLP) policies and trusted third party (TTP) agreements, cloud service providers offer contractual assurances of trust and their obligation to keep data safe. In fact, it may be a fallacy to believe that keeping data onsite is the most secure option for many businesses. A single location for data storage has its own set of physical and cyber risks, and cloud-based accounting services companies offer security expertise, always current software and equipment plus fortified and secure facilities that most businesses simply can't match or duplicate.

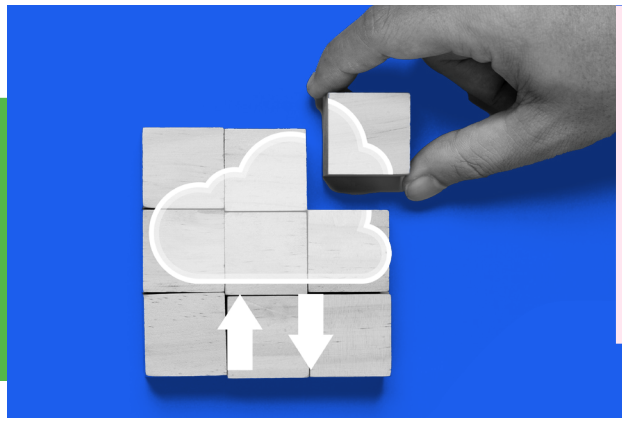
> **Cloud-based accounting services companies offer security expertise, always current software and equipment plus fortified and secure facilities.**

2. **Trusting a third party:** It's an obvious concern for accountants who deal with highly confidential and critical client information. Agreements between cloud providers and customers — covering service levels, confidentiality, security and privacy plus acceptable-use policies — describe the security technologies and measures used and the actions a provider takes to mitigate risk in the event of any security breach. Cloud service providers demonstrate their accountability through monitoring and measuring the relevant metrics of their customer agreements.

3. **Security on public networks:** Through the applications of today's security standards, cybersecurity tools and solutions, the internet is now a secure place to do business. Many layers of security protections are applied by cloud service providers; a section further down in this report details the features and functions of key security best practices, protocols and security standards used by cloud providers.

4. **Compliance mandates:** These are critical and essential elements in the accounting world, which some believe can only be applied and ensured through on-premises efforts. But cloud service providers do it every day and often specialize in serving specific industry types. Many are highly experienced in their proven ability to comply with the standards demanded by most industries.





The cloud's components

The cloud is an information technology infrastructure of computing servers that are interconnected and accessed through the internet. Cloud services provide software and applications, data storage and compute power, all accessed and secured remotely through the internet.

By utilizing cloud services, an organization does not own or maintain computing hardware and software. No equipment or IT department is required. A cloud service provider manages and maintains the servers, databases, software, computer processing and data storage, which all reside in the provider's secure facilities. A customer pays a recurring fee to license, remotely access and use these offerings.

Cloud computing makes it possible to work with software applications from any location through a web browser. Cloud service providers offer the facilities to store as much data as is required, and to retrieve and work with that data from anywhere and at any time. For accountants, cloud technology brings much greater working and application flexibility, eliminates outdated manual and paper-based procedures while enhancing controls, bringing greater visibility to processes and information, and offering a better customer experience.

Cloud computing makes it possible to work with software applications from any location through a web browser.

A brief cloud history

The history of the cloud computing approach traces as far back as the 1950s. It began with large and extremely expensive enterprise business **mainframe computer systems** that were used for shared and centralized data storage and access, plus computing capability delivered through "hard-wired" networks to connected "dumb" terminals.

The advent of client/server computing during the 1980s and 1990s brought a "lighter" form to the business masses. In this distributed computing model, much less expensive servers substituted for mainframes and were connected by **local area networks** (LANs) constructed within private business environments. These LANs linked personal desktop computers together for file-sharing, storage and printing. Different branch office LANs could be interconnected through a **wide-area network service** from a telecommunications provider.

One of the earliest iterations of cloud computing came in the form of application **service providers (ASPs)** that appeared around the turn of the century. ASPs offered fairly generic applications that were accessed through the internet, with little or no customization available or integration with other business software. However, the ASP model during this early period stalled due to poor system and network management capabilities coupled with public network unreliability and low-speed connectivity.

Many experts say the current form of cloud computing we see today took hold around 2006 as companies such as Amazon, Google and Microsoft began building large data centers to support growing interest in ecommerce and remotely delivered software. SaaS emerged around 2007 with the Google Apps suite, which was later followed by online document sharing and editing solutions from Apple and Microsoft in 2011.

Consumers were among the first to embrace the cloud through various file-storage products such as Dropbox and Google Drive. Other low-cost data storage services have since targeted enterprise data centers, and many organizations today use less-expensive remote cloud-based disaster recovery environments instead of owning and operating dedicated secondary facilities.

The business world has moved to the cloud

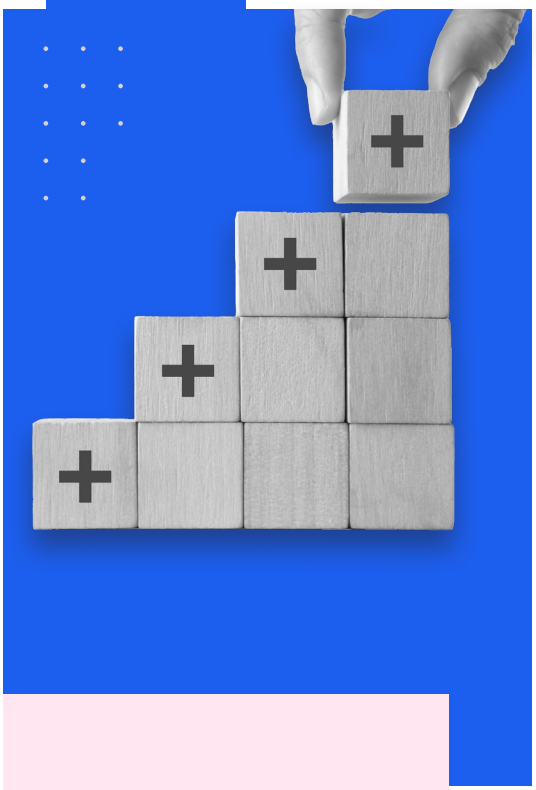
Researchers at Gartner predict "almost two-thirds (65.9 percent) of spending on application software will be directed toward cloud technologies in 2025, up from 57.7 percent in 2022." Other research from 2022 shows 70 percent of companies using the cloud say they plan to increase their budgets in the future and that 57 percent of businesses will have migrated their workloads to the cloud in 2022. It's also reported that 94 percent of enterprises use cloud services and that half of organizations store their confidential data on cloud technologies.

The COVID-19 pandemic further accelerated the move to the cloud as organizations needed to digitize their businesses and quickly shift employees to remote working. In 2020 alone, 61 percent of businesses moved workloads to the cloud.

Caseware's *2023 State of Accounting Firms Trends Report* reveals cloud adoption continues to grow as accounting firms realize the benefits of both hybrid and pure cloud working environments.

Caseware's research shows nearly 60 percent of those surveyed say they use cloud platforms in their practices, with slightly more than half of respondents indicating they use a blended approach of both cloud and traditional desktop solutions. The report also noted:

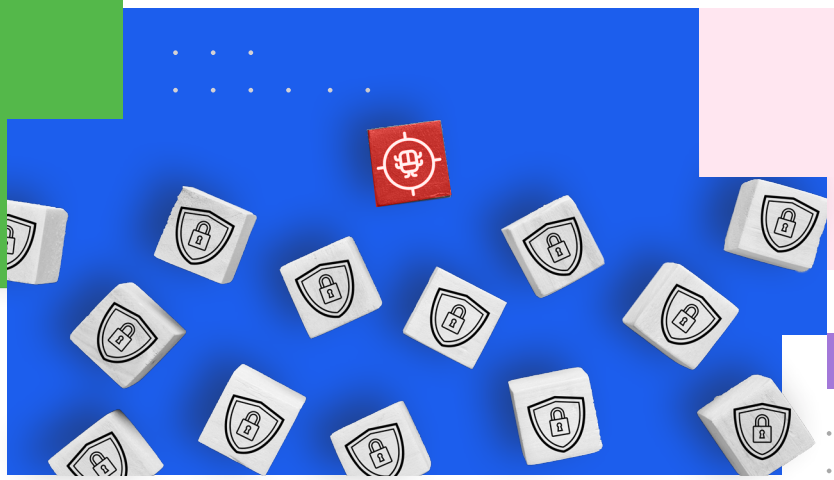
"The move to the cloud is only going to increase. We see an interesting shift in firms' plans for adopting cloud in the future: While nearly one-quarter of respondents to last year's (2022) survey said they had all the cloud tech they needed, this year, that figure has dropped to just slightly more than 18 percent. It appears some organizations have, in the course of the past 12 months, seen additional benefits that cloud offers that perhaps they had not realized existed."



Advantages of cloud

Cloud computing offers convenience, portability, reliability, security and greater efficiency through what's typically described as an "on-demand" approach to utilizing IT resources. The general advantages of cloud computing include:

- **Low/no maintenance:** Cloud providers own and manage computing resources
- **Cost-effective:** There's no capital investment required and no need to continually invest in expansion and upgrading to the latest and greatest technologies and new versions
- **Extensible:** Cloud makes it quick and easy to add and expand computing resources as a company grows
- **Portability:** Cloud resources are accessible through any web browser and allow anytime and anywhere access to applications, storage and other computing resources
- **Collaboration:** Cloud allows groups and individuals to easily share files and other resources, and to easily work on the same projects together in real time
- **Security:** Cloud offers advanced security features and functions to ensure the safe handling and storage of data



Cloud security considerations for accounting firms

Security threats are on the rise and Caseware's *2022 State of Internal Audit Trends Report* reveals more than 70 percent of respondents say the global pandemic has caused an increase in fraud threats in their organization.

Many cloud environments provide greater levels of security than most organizations can deliver through their in-house efforts. Cloud accounting software providers take steps to address security by utilizing comprehensive cybersecurity and systems management to ensure their products and services are protected and are in compliance with industry standards.

Two of the most important industry standards (discussed later in this report) that provide assurance are ISO/IEC 27001.2013 and SOC 2.

When considering a cloud service, cloud vendors need to provide their certifications and produce reports to verify they are in compliance with these industry regulatory standards.

A shared responsibility

It's important to recognize that moving to the cloud does not completely absolve cloud customers from their specific security responsibilities. However, the move does significantly lessen these responsibilities. Cloud service providers assume what's often described as the security elements "of the cloud" that include IT components such as hardware, software and networks as well as the physical security of the facility in which services operate and reside. Cloud customers are responsible for user and data access management.

Cloud security features

Is the cloud a truly safe and secure place to conduct business? The unequivocal answer from most experts is a resounding "Yes." Cloud providers heavily invest in the safety of their facilities and the reliability of their services by acquiring cybersecurity tools, applications and expertise to offer a much more comprehensive and secure computing alternative.

Former IDC vice-president and specialist in cybersecurity research David Senf says it's difficult for most businesses to hire the skilled IT staff needed to effectively and securely manage servers and applications. Cloud providers achieve an economy of scale by serving many customers and they have the capacity to add and manage increasing workloads. Cloud providers offer various layers to their security stack — well beyond what most organizations can deliver.

"Understanding what the risks really are is a capability many organizations don't have," Senf says. "Organizations are moving towards software-as-a-service, and cloud providers take care of security and the hardware that run applications. The security teams of cloud providers are typically much larger and more highly skilled than most businesses."

Among the many different layers to the security stack are the network itself, data, cybersecurity, applications, user identity and access management, data security and physical security.

Cloud providers deliver 24/7 ongoing monitoring of their networks and computing resources and utilize automated responses and actions to detect, block and isolate perceived threats. Cloud service provider security extends deep into computer hardware to include microprocessors, server bios and operating systems, capabilities that the average organization would find outside of their expertise, Senf says.

Cloud providers use software programs called playbooks to proactively anticipate certain types of cyberattacks and threats based on knowledge of what attackers typically may have previously done to try and expose vulnerabilities. These playbooks take the form of threat-hunting automated responses within their security software that execute reactions and responses to these situations.

"The security teams of cloud providers are typically much larger and more highly skilled than most businesses."
— David Senf, Cybersecurity Specialist

Cloud services companies follow best practices to enforce access management policies, only allowing those that a company authorizes to view and use data. Senf says customers are responsible for data privacy and need to determine how long data should be kept or deleted. Cloud providers offer encryption around that data, whether it is static or in transit.

Customers also need to manage user behavior: Attackers often gain user credentials through easy-to-crack passwords or passwords that are not secured. Human error accounts for the vast majority of cloud data breaches, as research shows it was to blame for 88 percent of cloud data breach incidents.

Research also reveals 83 percent of organizations that have suffered a security breach believe it resulted from a compromised password or identity compromise. Cloud customers must provide employee training and security guidelines around multi-factor security practices, password managers, and policies on user and data access.

"For example, you want to make sure that if a contract worker is only given temporary access to data that their permissions are rescinded

or turned off when they leave," Senf says. "And only give limited permissions or the least amount of privileges required. A zero trust (security framework) is all about providing the least set of permissions needed. Administrator access privileges also need to be managed properly and only limited access (to data) should be given and only for a certain time frame. The larger the company and end-user base, the more important it is to be diligent with access and privileges."

Key cloud security elements

Security features that cloud services providers typically offer include:

Encryption of data in transit: This is a vital security feature when connecting to a cloud portal through a public network such as the internet, since it is possible to intercept data while it is in transit across a communication network. Cloud providers offer natively encrypted connections that make data in transmission unreadable and ensure its confidentiality.

Encryption of data at rest: Even when data is statically stored on a server and within a database, it needs to be encrypted to ensure it cannot be viewed if it is accessed by someone who is unauthorized. Data encryption at rest is also a capability provided natively by most cloud providers and can be easily scaled to accommodate larger data volumes.

Disaster recovery: Cloud providers often offer contingencies for complete IT recovery to ensure business continuity in the event of major cybersecurity intrusions, power supply failures or a natural catastrophe. Disaster recovery includes mirrored equipment, power redundancy, failover, backup and restoration of data and applications, and ongoing data protection in a cloud environment. Proactive systems management, mitigation to reduce the potential impact of failures and disasters if they happen, and protection against cyberthreats that might take down systems are other aspects of disaster recovery.

Regulatory compliances: Many businesses are governed by industry regulations that dictate what must be done to ensure the safety and integrity of digital assets and data. Regulations govern how data can be used, how it needs to be protected, and even where it must be stored geographically. To address the latter consideration, many cloud providers have facilities in different countries and regions and use these to store client data. They work with clients to ensure compliance with regulations that govern their industries.

Centralized security posture management: This provides a single view and management dashboard for cloud services. Data and the computing infrastructure itself are monitored for performance, integrity, threat detection and identification. In the event of detected threats, breaches or perceived risks, immediate action through automated response can be taken. Centralized security posture management includes: intrusion detection, incident response, data loss prevention and data confidentiality.

User management: It's essential to ensure only authorized users have access to corporate data and only to what they need. User management is a fundamental security activity where IT administrators provide permissions and monitor data-access activity throughout systems, applications, files and networks.

Cloud providers often offer contingencies for complete IT recovery to ensure business continuity.

Security frameworks, standards and protocols to look for

Among the cloud security protocols, frameworks and standards that a customer should be aware of and look for when selecting a cloud provider are:

- **HTTPS** or Hypertext Transfer Protocol Secure that adds two-way data encryption to standard HTTP to and from origin servers and uses cryptography to ensure secure communication over a public computer network. HTTPS is widely used across the internet — between web browsers and websites — to prevent possible decryption and interception of data transfers or other communication in transit. HTTPS was developed by Netscape Communications in 1994 for its Netscape Navigator web browser.

- **PKI** or Public Key Infrastructure (PKI) is a highly secure connection infrastructure. PKIs apply a defined set of cybersecurity roles and policies to hardware, software and procedures for creating, managing, distributing, using, storing and revoking digital certificates (see below). PKIs ensure that electronic information transferred during e-commerce transactions, internet banking and confidential emails remains secure. PKI was developed in the early 1970s as a secure communications technology by the Government Communications Headquarters (GCHQ), a British intelligence and security agency. It was made public in the mid-1990s.

- **Digital certificates**, or public key certificates, apply cryptography to the electronic transfer of files. Digital certificates are unique pairing credentials (password identifiers) that validate people, devices and applications. Digital certificates are a way to validate and ensure secure delivery of electronic files to intended recipients by matching unique digital passwords or "keys" from a sending source to a receiving destination.

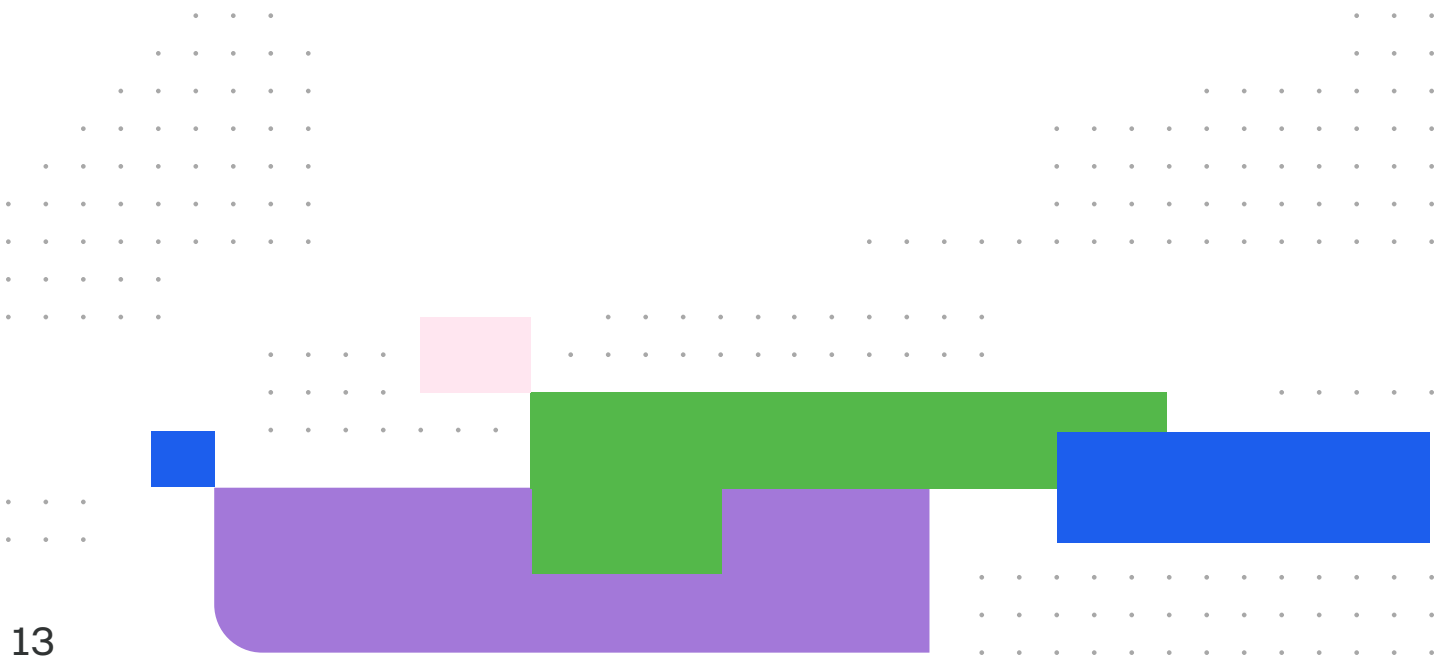
- **SOC 2**, or System and Organization Controls, were developed by the American Institute of Certified Public Accountants and are considered a minimal requirement for choosing a cloud software service provider. SOC 2 offers a set of standard guidelines for preventing unauthorized data use and defines how cloud providers should manage data through a set of auditing procedures for securing that data and protecting an organization's interests and client privacy. SOC 2 provides internal controls for data security, confidentiality, processing integrity, privacy and availability.

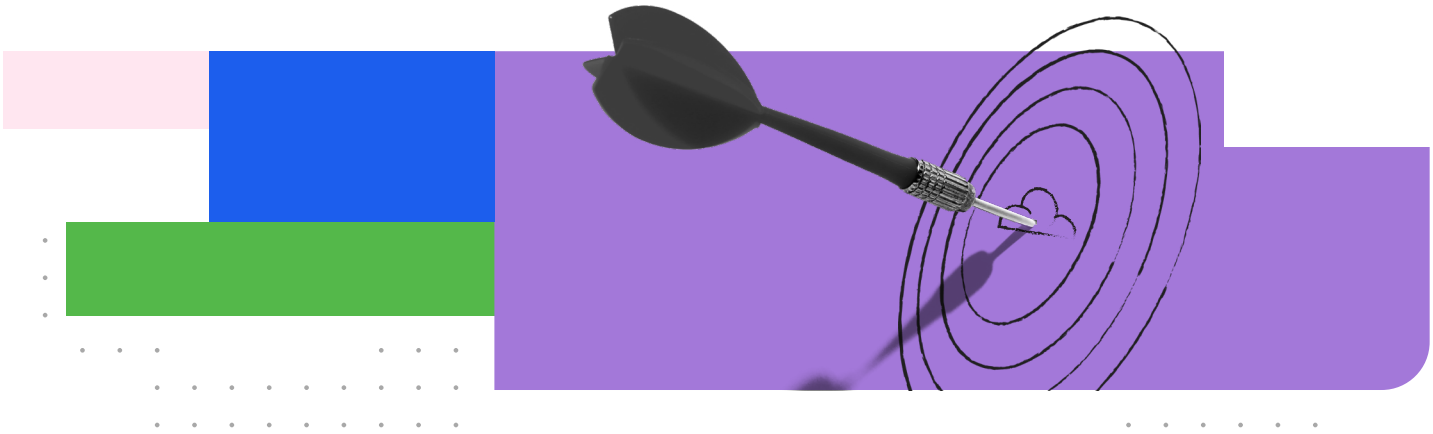
- **FedRAMP**, or the Federal Risk and Authorization Management Program, provides a standardized approach for evaluating the security of cloud services offerings. FedRAMP is intended to promote the adoption of secure cloud services by the U.S. government through a standardized and common framework of security guidelines for a cloud service. FedRAMP applies National Institute of Standards and Technology (NIST) guidelines for cloud services security including: a conformity assessment program; standardized authorization packages and contract language; and a repository for authorization packages.

- **CSA CCM**, or the Cloud Security Alliance's Cloud Capability Model, is a cybersecurity control framework for assessing cloud computing vendors. It defines a comprehensive set of control requirements for securing business information. CCM maps to a wide range of industry-accepted security standards, regulations and frameworks that a cloud provider must comply with. It is a generally agreed-upon framework demanded by financial services companies in the U.S. and outlines the secure use of the cloud.

- **ISO 27001** is an international standard for information security management systems. ISO 27001 is used by cloud providers to manage financial information, intellectual property, employee data and information entrusted to third parties.

- **PCI** is the Payment Card Industry (PCI) data security standard used to safeguard account security during financial transaction processing. PCI has been adopted by credit card companies to provide a secure environment for processing, storing and transmitting credit card information.





The Caseware Cloud platform

Caseware Cloud is a web-based platform for managing your accounting organization and workflows. Its features and apps combine to provide a convenient and centralized solution for the management of both your organization and your engagements. Caseware Cloud is a secure portal that allows you to continually take the pulse of all your projects and engagements anytime, anywhere and with peace of mind.

Caseware Cloud is hosted on Amazon's AWS web servers located around the world. Customers can request a specific region for their cloud environment. AWS is PCI Level 1 and Level 2 certified, ISO 27001 certified, and compliant with all major security control frameworks. These security certifications are issued by authoritative international standards bodies.

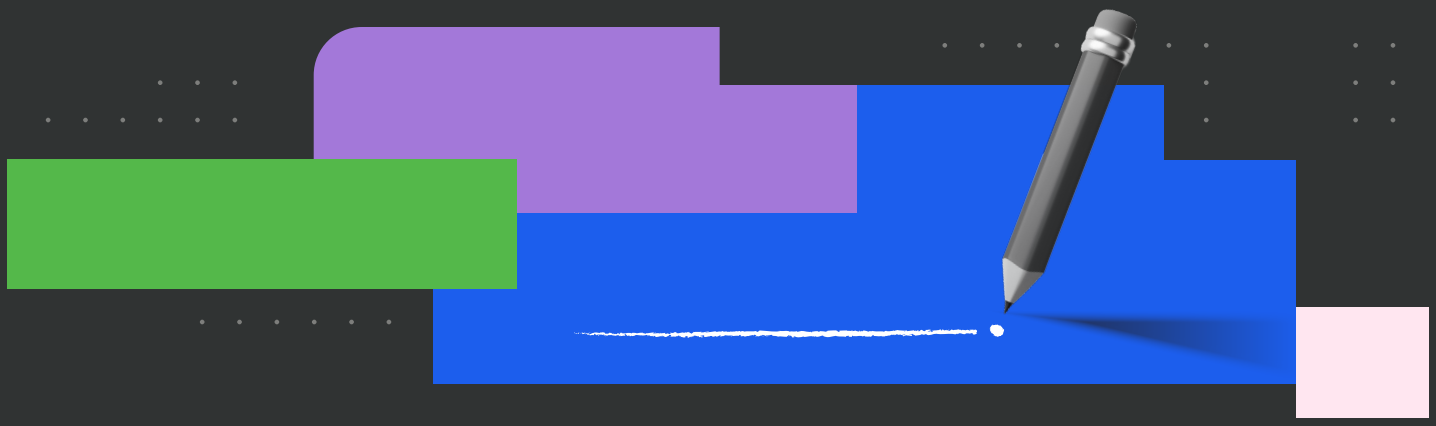
Caseware Cloud is built with security in mind every step of the way. Caseware engineers constantly perform tests to ensure only quality and secure code reaches its production environments. A wide array of vulnerabilities are tested for, including SQL injection, cross-site scripting, tampering and session and authentication vulnerabilities, among many others.

The cloud platform also enables advanced services that allow firms to work in ways never before possible. Applications such as Caseware Sherlock, for instance, allow practice leaders to apply powerful data analytics to their large stores of engagement data and help them identify previously unseen trends and patterns that ultimately lead to more effective decision-making.

Caseware Cloud offers granular access control at various levels that provides best-in-class security. In desktop environments, security is managed at the engagement level — creating a folder where data is stored on a desktop. Large accounting firms often work on thousands of engagements, which makes it extremely challenging to manage and update security for each one individually.

Take, for example, the case of an accountant who might leave a company. When that happens, it could be necessary to search through and individually update thousands of client engagements to remove access for that departed employee. It's an expensive process to perform and often takes many hours to complete.

In a cloud environment, individual engagement lockout can be performed, but user access defaults to the client rather than the engagement. That means account security restriction is simply a matter of removing that same person at a client level, which would automatically lock out access to any number of engagements associated with that client. It's a much faster, simpler and more efficient approach to file permission management.



Conclusion

Adoption of cloud services has definitely turned a corner, according to Senf, who adds that COVID-19 showed that remote work, meeting services and applications that are accessed through the internet can be trusted. Today's cloud services are mature and the tipping point for broad adoption may have happened during the 2010s. That's when many businesses shifted to cloud-based email server services, rather than using inhouse email services that were often unreliable.

"People are generally trusting of cloud services, using many of these in their personal lives for email, social media, banking and shopping," Senf explains. "Perception has decidedly changed around the security of cloud vs. on-premises. Many perceive cloud as a much safer environment than on-premise options. Cloud data centers feature state-of-the-art security technology and are staffed 24/7. They maintain the latest security features and updates."

Caseware's *2023 State of Account Firms Trends Report* revealed that "accountants continue crossing over to the cloud: More firms are recognizing the benefits of moving their operations to the cloud, whether in a pure cloud environment or in conjunction with their traditional desktop tools. They are also looking to do this quickly, suggesting an urgency to make the move is more acute than ever. With benefits like easier file management, reduction of IT overhead and maintenance, and stronger security, this trend does not come as a surprise."

According to Senf, the future of the cloud and the security around it will include even better detection and response to react more quickly to threats or intrusions. There will be more integration of security technologies and these will converge to work better together and create fewer intrusion gaps through a security services mesh, as opposed to separate and independently working tools.

"It's a move away from point security solutions that organizations would typically deploy themselves," Senf says, "to engineered systems that cloud providers create to dramatically improve the ability to respond to events and incidents."

About the author

Dan McLean has been a journalist, market researcher, executive communications specialist and content marketer over his 30-plus-year career in information technology.

Caseware International Inc.

351 King St E Suite 1100,
Toronto, ON M5A 2W4,
Canada

T +1 416 867 9504
F +1 416 867 1906
E info@caseware.com

www.caseware.com

caseware™