sage Intacct

WHITEPAPER

Security: Protecting Data Value

Practices and policies required for strong security

Contents

Introduction

With financial management often being a core system of record for businesses, ensuring the security of financial data is essential due diligence for any organization. As a protector of the company's funds, finance needs to weigh the rigor taken to protect this data. In this paper, we will consider questions regarding the practices and policies required for strong security and along the way, point out what Sage Intacct has put into place to protect the financial and operational data our customers have placed in our care.

Born on the internet

As an early and consistent visionary in online financial management, Sage Intacct has kept a close eye on web security and how it's progressed over the past two decades. One of the concerns early prospects expressed was the safety of their data. They had become used to on-premises computers and servers for storing and accessing their data. The thought, in those early days, of using the internet to do their accounting felt like they were giving up control of a vital asset entrusted to their stewardship. Their fears of losing data or losing access to data were natural.

The truth was that even from the first release of Sage Intacct over 20 years ago, customer data has been safer in our hands than on the on-premises systems they had been using. As you'll see in this paper, top-tier SaaS security measures, though constantly advancing, far outweigh the measures that most of our customers could individually afford to take. You'll see how Sage Intacct customers enjoy financial data security and access that used to only be available to the largest enterprises.

Is my data safe?

The first question I'll address is the question we used to hear from those very first customers: "Is my data safe?" Beyond answering that question, I'll answer the common follow-up question: "How safe?" Answers to these questions, in concrete terms, support the trust that thousands of companies, including public companies, have placed in Sage Intacct and other SaaS providers.

Saying you can trust us is one thing, and proving it is another. You don't have to take our word for it. I'll explain exactly who is keeping tabs on security compliance and what they are tracking.

Is my data private and accessible to me?

Once you know your data is safe, you'll naturally want to know how easy it is to access. After all, data you can't access doesn't have nearly as much value as data at your fingertips. The second part of this paper answers key questions like, "Who owns my data?" And that is followed up with, "How can I access it and control access to it?" These questions should be part of every due diligence process, and as the service provider, Sage Intacct has an obligation to answer them.

Is my data safe?

Modern SaaS security needs to be covered from multiple angles: physical, network, application, and data. External audits and other third-party certifications ensure that a provider is making every possible effort to protect vital information in a highly secure environment.

A provider should be able to show relevant security-related policies and procedures, as well as updates to policies and procedures performed on at least a yearly basis. A list of Sage Intacct policies can be found online: sageintacct.com/information-security-management-program.

A security culture

Trained and certified people are a big part of the security equation. Requiring that all employees take periodic security training keeps a SaaS company's entire staff aware of new threats and how to combat them. At Sage Intacct, we strive to promote a culture of security. This starts during orientation and continues throughout an employee's tenure with email reminders, displays on posters and monitors, and mandatory ongoing training. This training includes:

- Acceptable use
- Social engineering
- Personnel security
- Data protection
- PCI

- HIPAA
- GDPR
- Incident response

Application developers and engineers are required to take additional application development related security training to include the top 10 security risks outlined by the Open Web Application Security Project (OWASP Top 10).

Sage Intacct also employs dedicated, seasoned, and certified information security professionals (CISSP) who develop and drive its security program. The program encompasses both the physical and cyber security of Sage Intacct applications and infrastructure, as well as internal IT systems.

System monitoring, testing, and response

A secure SaaS vendor monitors system activity within both its production and corporate systems. At Sage Intacct, monitoring utilities track server and user activity including:

- Security settings
- Systems monitoring
- Remote access activity
- Server capacity
- Server event activities

Applications and systems associated with the access, processing, storage, communication, or data transmission require audit logs detailing use, access, disclosure, theft, manipulation, and reproduction. Security-related audit logs need to be generated and reviewed regularly for any indication of compromise or other relevant suspicious activity. Sage Intacct maintains such logs for at least a year. When a review of the audit logs reveals reasonable evidence of a security incident, appropriate action is taken in accordance with the security incident response plan.

In an ever-changing world of technology, SaaS providers need to continually test the reliability of their own security measures. For example, Sage Intacct conducts regular internal and external third-party risk assessments and penetration tests on data applications, systems, and infrastructure associated with accessing, processing, storing, communicating, or transmitting customer or other sensitive data. An independent summary report is available under NDA to relevant parties (including customers and prospective customers) upon request.

Because no system is perfect, every data-centric service needs to maintain a security incident response plan, which details procedures to be followed in the event of an actual or reasonably suspected unauthorized access to or use of data. This includes disclosure, theft or manipulation of data that has the potential to cause harm to the system, stored data, or an organization's brand name. We test our incident response process at least annually and addresses requirements related to PCI, HIPAA, and GDPR.

Regulatory compliance

Several standards are in place for services that deal with sensitive data. Compliance with these standards depends on the kind of data a provider handles. Each standard also has a regulatory body that ensures compliance. Providers perform various types of internal and third-party audits to validate compliance with applicable requirements. Upon completion of each audit, a provider receives a written report of the findings and recommendations that it maintains in a secure repository. At Sage Intacct, when a non-compliance, deficiency, or other finding is discovered, we promptly assess and mitigate with appropriate compensating controls. In the area of SaaS finance, a number of standards come into play.

- **SSAE 18 SOC 1 Type II**—Sage Intacct maintains an SSAE 18 SOC 1Type II opinion from a reputable, independent third-party audit firm. We conduct this activity twice per year to address timeliness of customer reporting requirements. The controlled report is available under NDA to relevant parties (including customers and prospective customers) upon request.
- **SOC 2 Type II**—Sage Intacct maintains an SOC 2 Type II opinion from a reputable, independent third-party audit firm. We conduct this activity once per year. The controlled report is available under NDA to relevant parties (including customers and prospective customers) upon request.
- **ISAE 3402 and ISAE 3000**—The International Standard on Assurance Engagements (ISAE) 3402 and 3000 are international assurance standards, which maps to SSAE 18 and SOC 2 respectively. Sage Intacct maintains an ISAE 3402 and ISAE 3000 opinion from a reputable, independent third-party audit firm. The controlled reports are available under NDA to relevant parties (including customers and prospective customers) upon request.
- **PCI-DCC Level 1**—Sage Intacct maintains a Level 1 PCI status, which includes a full audit by a qualified security assessor (QSA), who issues a Report on Compliance (RoC) and two attestations as both a merchant and service

provider. Our Attestations of Compliance (AoC) are available under NDA to relevant parties (including customers and prospective customers) upon request.

- **HIPAA**—Sage Intacct's product is certified to meet the requirements of the U.S. Health Insurance Portability and Accountability Act.
- **Privacy Shield/GDPR**—Sage Intacct partners with TrustArc, which has verified Sage Intacct privacy practices against the Privacy Shield's Privacy Standards using a combination of technical and manual methodologies. Sage Intacct is Privacy Shield certified, and the Sage Intacct product meets the requirements of the General Data Protection Regulation.

Physical Security

Physically securing data media or data access points is just as important as cyber security. Physical security measures control physical access to office facilities, paper records, and corporate IT systems, as well as data centers that store or process customer data. Sage Intacct data centers are SOC 2 compliant and include the following controls:

- Badge Access
- Biometrics
- Man-Traps
- CCTV
- 24x7 Security
- Strong environmental controls

Vendor management

Since no system is an island these days, SaaS providers need to have processes and policies in place for working with other connected technologies. They need to be able to vet vendors to ensure that vendors treat customer data with the same rigor as the primary provider. Providers should evaluate third-party vendors and partners prior to engaging in a business relationship and regularly thereafter. Sage Intacct takes a risk-based approach to evaluate vendor security maturity, compliance, and security features and functionality available to Sage Intacct and its customers.

Data loss prevention and recovery

SaaS providers should be able to demonstrate their ability to secure data so that data loss is rare and their ability to recover data in the event that it is lost from primary systems. At Sage Intacct, a variety of processes and technologies identify and manage data loss events. In the event of data loss on primary systems, data recovery systems access backups to mitigate the loss.

Sage Intacct adheres to and maintains measures to secure data being transported offsite for usage, hosting, backup purposes, or storage. These include:

- Storing media back-ups in a secure off-site facility, which may be either an alternate third-party or a commercial storage facility
- Maintaining strict control over the internal or external distribution of any media back-ups that contain Sage Intacct customer data
- Transmission of data via secure protocols
- Every provider should maintain a data recovery process, covering back-up and restore procedures for customer data. At Sage Intacct, our SLAs include both a restore point objective (RPO) of no more than 4 hours and restore time objective (RTO) of no more than 24 hours.

Network and host security details

Network and host security rely on a provider's use of reasonable and efficient network intrusion detection capabilities, firewalls, and commercial grade anti-virus protection. Providers need to patch operating systems and applications associated with customer data and the provider's own sensitive data within a commercially reasonable time after learning about security vulnerabilities or vendor patch releases. Sage Intacct takes precautions designed to safeguard the software, systems, or networks that may interact with customer data so they do not become infected by viruses, malware, unauthorized programs, or other harmful components. Methods for securing networks include:

- **Intrusion detection**—an intrusion detection program comprised of network intrusion detection, log analysis, and data integrity monitoring, to monitor all network traffic associated with accessing, processing, storing, communicating, or transmitting customer data. The program alerts security personnel who analyze and, if necessary, take action.
- **Firewalls**—stateful inspection firewalls at various locations within the infrastructure. Sage Intacct has established firewall configuration standards which include:
    - A default to deny policy, requiring only authorized ports and protocols
    - A formal process for approving and testing all external network connections and changes to the firewall configuration
    - Regular audits of our firewall configurations
- **Patch and vulnerability management**—system processes to:
    - Update all system components and software with the latest vendor-supplied security patches
    - Identify newly discovered security vulnerabilities (through subscription to alert services)
    - Update standards to address newly discovered vulnerabilities.
- **Antivirus**—commercial-grade antivirus software to protect from viruses, worms, and other malicious code. We install and maintain virus-screening software (when available) on all systems, to include those that access, store, or process customer data or other identified sensitive information. Once installed, we do not disable antivirus software. We regularly update antivirus software with virus signatures to locate or protect against new viruses or malicious code.
- **System hardening**—industry practices with respect to system hardening on systems hosting customer data, including:
    - Removing unnecessary system functionality including scripts, drivers, features, subsystems, and file systems
    - Disabling unnecessary and non-secure services and protocols
    - Configuring system security parameters in accordance with industry best practices (i.e. CIS/NIST) to prevent misuse
    - Changing vendor-supplied defaults before the system is live on the network.

  For wireless environments with potential access to sensitive information, Sage Intacct changes wireless vendor defaults, including WEP keys, default SSID, passwords, and SNMP community strings. We disable SSID broadcasts and enable Wi-Fi Protected Access (WPA) technology for encryption and authentication when WPA-capable.
- **Routers and network infrastructure**—securing network infrastructure includes:
    - Installing the latest vendor-supplied security patches on all network infrastructure devices (hardware and software)
    - Establishing a process to identify newly discovered security vulnerabilities
    - Periodically auditing devices

Is my data accessible and my privacy protected?

Much of your data is only as valuable as your ability to access and analyze it. Accessing data safely includes steps and policies that allow the right people to see the right data, while preventing unauthorized access. When it comes to controlling access, the provider and the customer work together to meet the customer's needs. The provider assembles the tools and the customer configures them.

Unlike other companies you may have dealt with, at Sage Intacct we work under the core tenet that the data you enter and generate within your subscription companies is your data. We make it available to you in a number of ways including through the graphical user interface, exported reports and lists, web services APIs, and our data delivery service.

Availability

A high availability percentage or uptime is essential for any SaaS provider. It means that customers can rely on getting to their data and getting their work done whenever they need to. Every SaaS system should provide visibility into their availability percentage. At Sage Intacct our availability is monitored and posted to our corporate site. A recent look at our up time showed (as of April 17, 2020):

12 Month Availability Average: 99.974%

For real-time information on system performance, reliability, and security see our dedicated webpage: sageintacct.com/system-status.

The status page includes:

- Live data on system availability from around the world
- Current and historical information on system performance
- Information about Sage Intacct security, reliability, and availability technologies
- Real-time status reported from worldwide monitoring locations.

Buy with Confidence℠

Sage Intacct backs availability efforts with a Buy with Confidence℠ guarantee, which outlines the level of service you can expect. It covers uptime, data ownership, disaster recovery, and professional services quality. It includes customer credits for downtime, should Sage Intacct fail to meet the guarantee. You can see all the details of this guarantee online: sageintacct.com/trust/buy-with-confidence.

Customer processes and policies to ensure data integrity

Part of the responsibility for security resides with the customer. The customer decides who gets access to the data and how much of the data they can access. Like other SaaS systems, Sage Intacct includes a variety of security controls and functionality. Security controls include:

- **Inactivity timeouts**—automatic log out for inactivity (empty chair scenario) set by the administrator
- **Session timeouts**—automatic log out for session time set by the administrator
- **Password complexity, change frequency, and history rules**—protection from brute force attacks configured by the administrator
- **Sign-in lockout**—repeated unsuccessful attempts lock out the account, requiring administrator reset
- **IP Address filtering**—option to restrict access to a specific IP address or range of IP addresses on an account-by-account basis—for example your office IP and an administrator's home IP
- **Two-step verification** (multifactor authentication or MFA)—periodic use of a second devise—usually the user's cell phone—for authentication so that the mere knowledge of a password is not sufficient to access the application
- **Role-based permissions**—fine tune what each user (including API users) can see, create, change, or delete.

Privacy and data disposal

Data protection laws that apply to SaaS providers continue to expand and become part of the compliance landscape. Like so many other services, Sage Intacct has implemented numerous technical and administrative measures for the protection and security of data, and we are transparent regarding how we handle customer and user data. Our product privacy policy can be viewed online: sageintacct.com/privacy_policy.

What about the data you want to get rid of? A provider should have processes to ensure that your old data isn't left floating around the cloud. Sage Intacct sanitizes any out-of-use media containing Sage Intacct or customer data. We dispose of data by one or more of the following methods:

- **Overwriting**—replacing the data previously stored on the magnetic storage media with a predetermined set of meaningless data, rendering the data unrecoverable
- **Degaussing**—exposing the media to strong magnetic fields to destroy its contents to eliminate any data still on the media
- **Physical destruction**—shredding or otherwise physically destroying media, including by physical force and temperature, to preclude further use

Conclusion

This has just been a glimpse into the technologies and policies that protect your data and your ability to safely access and use that data. Hopefully it can serve as a guide to help you make the big decision of choosing a financial software to meet your organizations needs. See additional information online: sageintacct.com/trust-sageintacct.

Some final points to consider are whether the SaaS service you are considering was born on the internet with security at its core, whether the service has documented the steps it takes to keep your data safe, and whether it takes demonstrable steps to help you safely access your data to get the most value from it.

Find out more