appian

Appian Cloud Whitepaper

Part 1: Security

Table of Contents

Table of Contents

Appian Cloud Whitepaper

Part 1: Security

Introduction: Appian Cloud Security

Appian has been a recognized leader in cloud-based enterprise software platforms since delivering Appian Cloud in 2007. From the outset, we built our software to integrate with and complement the cloud's unique advantages, and to protect it from any vulnerabilities. We did so with a unique design philosophy, employing cloud-native and globally recognized frameworks like NIST for optimal security protection, business continuity, and enhanced support.

To provide greater detail on these key areas we've created a series of white papers as follows:

- **Part 1:** Security - How Appian Cloud's intelligent cloud design enables the highest levels of security protection for your organization.
- **Part 2:** Business Continuity - How Appian Cloud facilitates cloud resilience by leveraging high availability (HA), disaster recovery (DR), and other technologies to keep your enterprise operating at maximum potential.

Each paper will provide detailed background on how our unique design philosophy provides the highest levels of security protection for your organization's end-to-end workflow, including low code development, automation, robotic process automation (RPA), business process management (BPM), artificial intelligence (AI), intelligent document processing (IDP), case management, and more, along with the highest levels of support to ensure that users can take full advantage of all this powerful technology.

Each paper will provide detailed background on how our unique design philosophy provides the highest levels of security protection for your organization.

Key Takeaways

This series of whitepapers provides readers with five key takeaways on our approach to cloud security:

1. Appian Cloud architecture provides layered defense strategies that encompass perimeter protection, applications, and other security zones.
2. Appian invests in data and process security to protect organizations.
3. Maturity and experience delivering enterprise cloud services is critical.
4. Appian secures cloud instances.
5. Appian Advanced and Enterprise support provide the ultimate availability and security as well as enhanced support.

Key takeaway 1: Appian Cloud architecture provides unique advantages.

The journey of the security-driven Appian Cloud is best described by starting from the inside and working out. Our security strategy is based on layered defense practices. Cloud-native architecture not only forms the core of its design but also facilitates securing all components down to their most minute and important levels. The Appian Cloud is also secured via physical and electronic perimeters—including firewalls, tenant architecture and site isolation, and a dedicated VOC option—to ensure that only authorized users have access to your valuable data.

All of these factors work collectively to form one of the most secure cloud platforms in the industry. Let's dive a bit deeper into each of these areas.

Cloud-native architecture.

Cloud-native architecture forms the foundation of the Appian platform and provides many advantages, including enabling high levels of security.

But what does "cloud-native" mean, and how can it help an organization? The Cloud Native Computing Foundation defines it as follows:

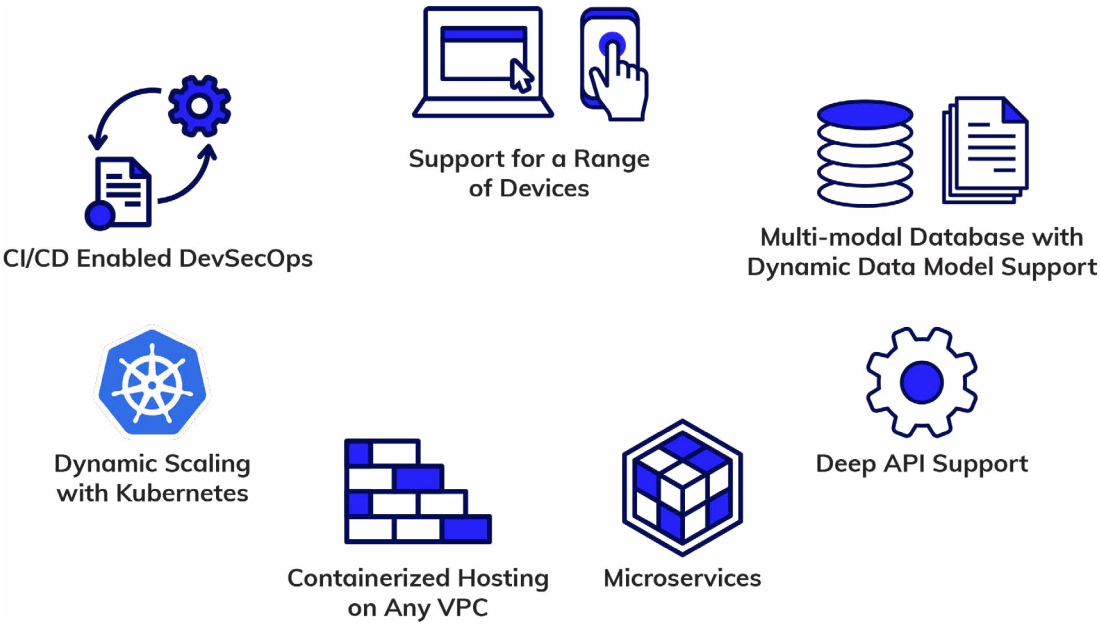
"Cloud native technologies empower organizations to build and run scalable applications in modern, dynamic environments, such as public, private, and hybrid clouds. Containers, service meshes, microservices, immutable infrastructure, and declarative APIs exemplify this approach."

Cloud-native architecture uses a layered approach with three "planes," the data plane, the control plane, and the management plane. Each plane is compartmentalized and segregated from the others. This allows for greater levels of security, as the information at each level does not co-mingle with the others unless it is specifically told to do so.

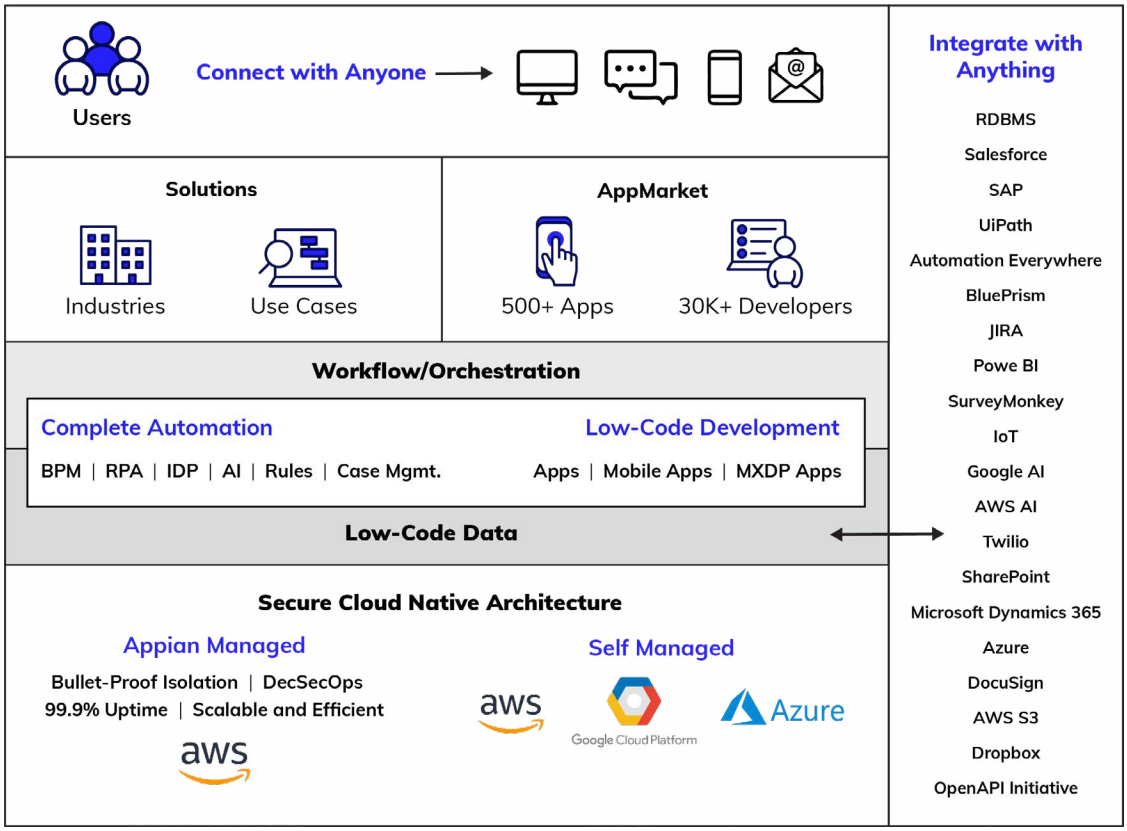
Each plane encapsulates different protocols and behaviors leading to a scalable and resilient system:

Cloud-native vs. cloud-washed architecture.

The Appian Cloud architecture design is much more than just a virtualized version of on-prem applications delivered via the cloud. Our cloud platform's functionality can be packaged in containers orchestrated by Kubernetes and deployed as microservices (collections of loosely coupled, independent services) on elastic cloud infrastructure through agile DevOps processes and continuous delivery workflows.



Modern modular cloud-native architecture for low-code development and secure dynamic scaling.



The Appian Low-Code Platform.

An on-premises application placed in the cloud is known as "cloud-washed" architecture. Cloud-washed architecture still requires all the work of deploying and maintaining traditional software and infrastructure—and has none of the benefits of cloud-native architecture. Because of this, cloud-native is the way to go for security, performance, and maintainability.

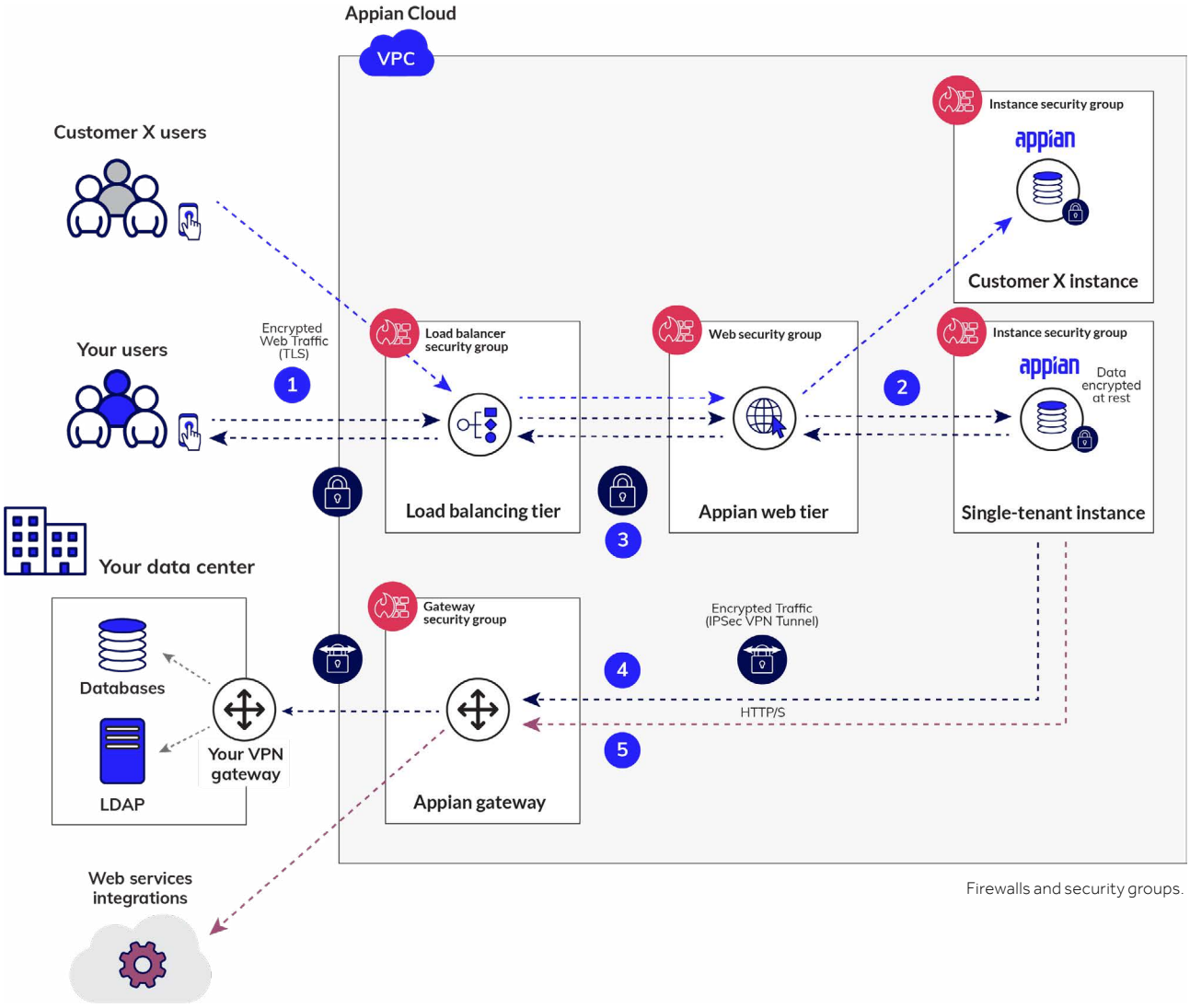
Secure firewalls.

A cloud site is only truly your site when it offers 100% dedicated data processing and storing, separate from the servers and data stores processing and storing somebody else's data. The Appian Cloud architecture supports multiple customers, but more importantly that a "single instance" (i.e., a customer's instance) is completely isolated from those of any other customer.

Such single-instance architecture is correct for a secure cloud application. It does not commingle data or processing. Only this cloud architecture approach can do the following:

- Prevent data from being mistakenly read by another co-resident.
- Ensure that others' flawed processes do not crash your system.
- Limit any potential security issue or vulnerability of one customer's cloud instance to only that instance, so it does not compromise other Appian customers' applications or data.

With the multi-tenant architecture commonly delivered by most cloud vendors, a breach of a single customer's installation is a breach for all customers. These types of architectures will always be prone to multi-hour enterprise-wide outages while breaches are being contained and eradicated. This is why it is often impossible to get a contractual service level agreement (SLA) commitment on recovery time objective (RTO) from many multi-tenant Application Platform as a Service (APaaS) vendors. In contrast, Appian stands by our SLAs, RTO, and recovery point objectives (RPOs) for all our service types.

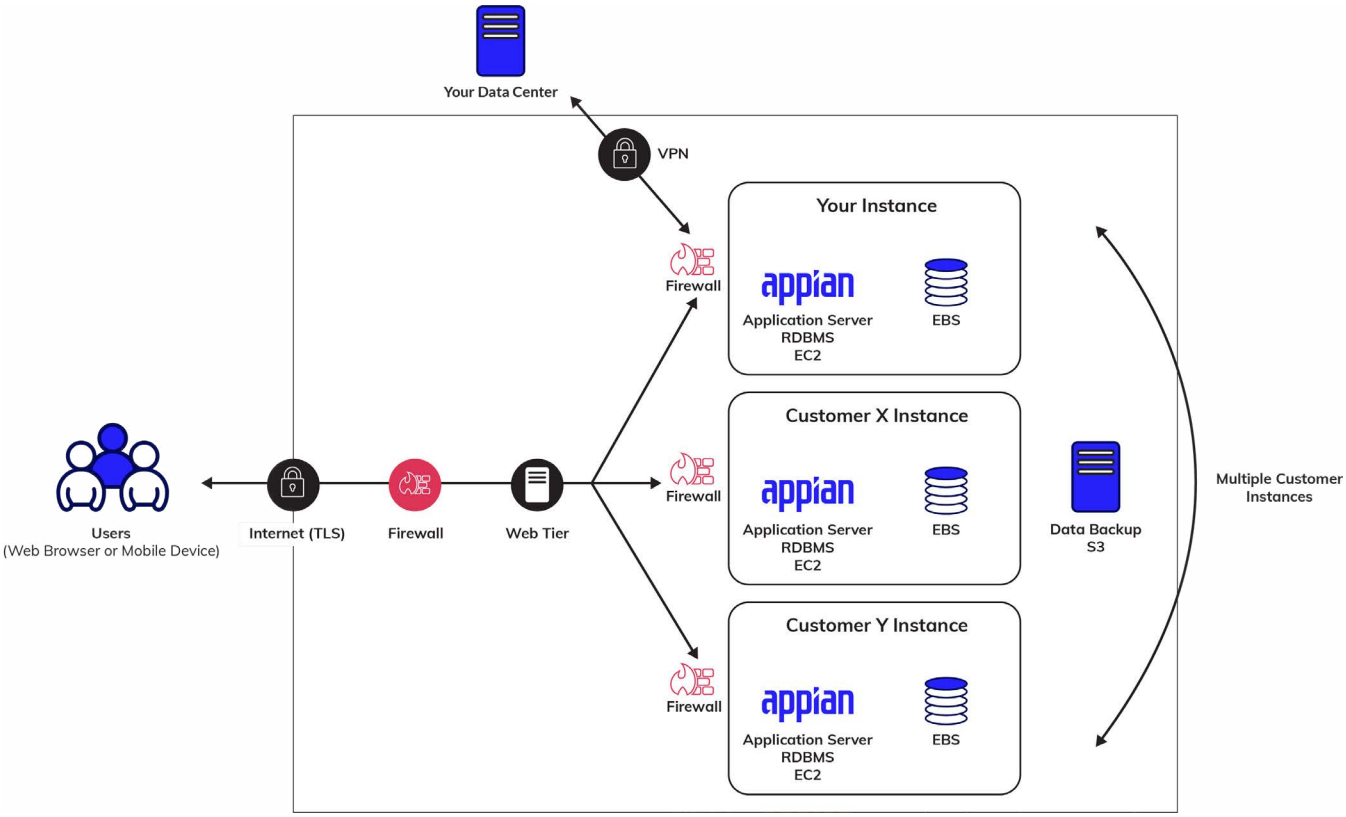


Tenant architecture and site isolation.

Appian Cloud provides each customer with a dedicated, single-tenant virtual machine instance for each cloud site that isolates processing and storage at the operating system (OS), database, and application layers. Resources are never shared with other customers, so pooling or data processing alongside other customer's data is never a concern.

In addition, each customer is provided with separate development, test, and production instances, which are isolated from each other in the same manner. Additional environments can be added as needed for temporary or long-term use. On a quarterly basis, or even more frequently if warranted by potential vulnerabilities, Appian offers to upgrade all instances to the latest software and OS release at an agreed-upon date and time. In addition, the platform components and shared libraries are updated far more frequently than that.

Stateful inspection firewalls, such as Amazon Web Services (AWS) security groups, isolate each site and provide ingress- and egress-level security through individual and group access control. These virtual firewalls enforce segmentation between separate client instances in the virtual private cloud. AWS security groups also give Appian precise control over what servers are allowed to talk to each other and how they are allowed to communicate. Each server in Appian Cloud is assigned to one or more security groups with explicit data



Customer instance isolation.

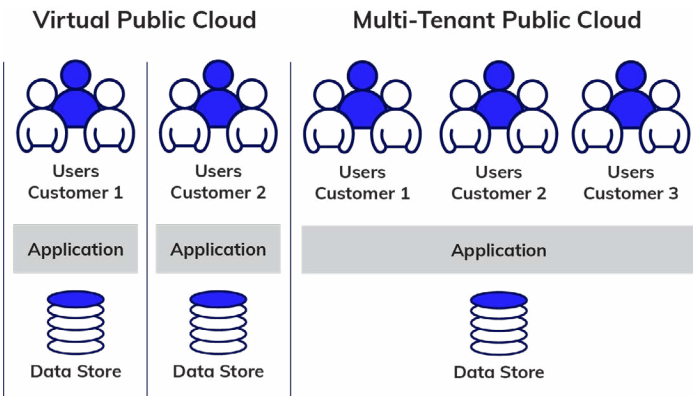
flow rules controlling the traffic (port, protocol, etc.) allowed into that server. Any traffic not explicitly defined is not allowed. Rules also define the necessary ports, protocols, and other security groups, such as servers, allowed into that server. Inbound security group rules ensure site isolation by preventing all inbound traffic from other customer servers. Only traffic originating from specifically defined Appian-managed infrastructure tiers, such as web-tier, is permitted.

To ensure fast response times and high availability, Appian Cloud uses a common load-balanced, auto-scaling web tier that acts as a traffic director when a user accesses an Appian Cloud site.

The above diagram depicts Appian tenant, single-instance architecture.

A dedicated VPC option.

For Appian Enterprise customers, a dedicated Amazon Virtual Private Cloud (VPC) can provide even greater security by creating more separation between their environment and the rest of the Appian Cloud. This gives customers increased control over authorization and audit processes. Appian is able to deliver this feature, created in response to customer requests, because of the multi-tenant, single-instance model we implemented from the very beginning with the original Appian Cloud release in 2007.



VPC provides greater security by creating greater separation between the customer's environment and the rest of the Appian Cloud.

Key takeaway 2: Appian invests in data and process security.

As a high-growth public company, Appian is able to provide a comprehensive, consistent, and complete security posture and invests heavily in planning, architecting, building, and, most importantly, validating each of these security posture elements. We continually roll out advanced features that layer additional security into the platform and validate security posture through tactics including third-party testing by leading independent global security firms and a bug bounty program that encourages hackers to find vulnerabilities in isolated cloud test environments.

All of this is to protect our customers' data. We encrypt at rest and in transit, leveraging keys that the customers can supply, control, and retire.

Appian maintains rigorous security training requirements, a dedicated Engineering Security Operations team, security-focused feature enhancements to our core platform, and multiple security reviews of every proposed cloud and platform enhancement, even if the enhancement is not directly related to security. Every new feature and change request is reviewed in the exploration and design phase by the Information Security team for potential impacts. Every feature is tested for vulnerabilities in the development, integration, and testing process.

Appian embeds security into the engineering software development life cycle, independent continuous third-party vulnerability testing, and advanced features like bring your own key.

End-to-end encryption and advanced key management.

Appian Cloud uses strong encryption algorithms to secure data in transit and at rest. Any connections to Appian Cloud are encrypted using TLS 1.2 or above. Customers may provide their own TLS certificates, including those with extended validation, whitelist IP ranges, or set up inbound VPN tunnels to limit connections to users from trusted sites.

Data at rest—which includes all business, process, and log data as well as all documents and anything in a virtual storage container—is protected at the virtual disk level with best-in-class, industry-standard algorithms, such as AES, using key lengths considered to be strong (e.g., 128-bit, 256-bit, etc.). Data backups on existing AWS services are encrypted using similar algorithms.

Each Appian Cloud site is protected through a unique key encryption key (KEK) for each customer and each customer environment (i.e., development, test, and production). The KEK is used to encrypt the data encryption Key (DEK) that, in turn, encrypts data spaces on disk. Appian creates and manages keys with strong protections in an Appian-managed key store using the AWS Key Management Service. These keys never leave the AWS environment.

Bring your own key.

Appian Advanced and Enterprise support customers receive an additional data security feature: bring your own key (BYOK). With BYOK, each customer provides an encrypted DEK to be used on their behalf; the DEK is decryptable only with a KEK stored in a private AWS instance over which Appian has no control. Appian stores the encrypted DEK, but it can only be used after it is decrypted by the customer's cloud-based hardware security module. The BYOK model gives each customer complete control over how their DEK is used, how long it remains in use, and when it should be made inaccessible in response to a security incident. (Read more at the Appian documentation site page.)

Secure software development life cycle.

Appian Engineering invests heavily in application and cloud security. Our dedicated Engineering Security Operations team leads the initiative, sets the policy, and coordinates the incorporation of secure engineering practices into all engineering teams and release processes. The Application Security and Tools and Infrastructures teams are responsible for implementation, starting with training all new engineers on secure engineering best practices. This includes Open Web Application Security Project (OWASP) secure coding techniques and periodic group training and refreshers on advanced security topics. Efforts are supported with a set of secure build/test/deploy tools, including multi-factor credentials and infrastructure access management.

Appian also invests in security-conscious engineering by building security-specific gates into the Appian software

development life cycle. This includes documented change control, configuration management, build and test processes, and security-specific processes such as feature security reviews. Here the security impact and risk of every feature request is reviewed by both Engineering Security operations and the corporate InfoSec teams. Prior to release to customers, our formal change management program combines manual and automated techniques, including both static and dynamic code analysis, to identify security risks such as OWASP Top 10 defects.These techniques include manual code review, code analysis tools, CVE-detection tools, third-party code review strategies, and penetration testing tools.

Vulnerability management.

As part of the enterprise security monitoring program, Appian regularly performs extensive vulnerability testing. Results are triaged in accordance with our documented remediation process for analyzing, prioritizing, and addressing identified security issues. These issues are addressed in accordance with an assessment of risk for each. Any issue deemed high or critical is addressed promptly.

Appian contracts with some of the most respected independent security testing firms in the world, including NCC Group, to perform biweekly penetration testing and source code review

Appian contracts with some of the most respected independent security testing firms in the world, including NCC Group, to perform biweekly penetration testing and source code review against the Appian Platform and to conduct vulnerability risk assessments and ad hoc design reviews. Appian also works with these security testing firms on certifying each quarterly release before making it available to customers. Testing includes assessing for attacks, such as SQL injection, cross-site scripting, and the forgery of cross-site requests. Appian makes its third-party penetration test report available to customers under non-disclosure agreement. In addition, in accordance with the frameworks listed at the Appian trust site, Appian Cloud undergoes regular penetration testing. Release notes for new releases and hot fixes detail specific issues and corrections.

To test Appian Cloud against expert hackers, Appian implements a bug bounty program through HackerOne. Test Appian applications are hosted on a test cloud instance in an Amazon region not otherwise used by Appian under the same security controls and security monitoring. Appian includes test applications hosted on the platform and hackers are given the same level of credentials as Appian customers and rewarded for any vulnerabilities they find.

Appian also recommends customers perform penetration testing specifically tailored to their applications. Appian requires customers to give notice of planned penetration and vulnerability testing via a support ticket at least three business days in advance of testing. Customers must provide contact information, the start time of the test, its duration, the expected peak bandwidth in gigabits per second, and the source IP addresses generating the test traffic to prevent Appian or its hosting service providers from blacklisting those IP addresses.

Appian does not release any software with known critical or high-severity vulnerabilities and strives to have no medium-severity vulnerabilities either. Vulnerabilities discovered or reported post-release are triaged, assessed for risk, and resolved via hot fixes or future releases based on risk and impact. Customers are notified of hotfixes via the Appian forum.

All servers in Appian Cloud run antivirus software with antivirus definitions updated on a daily basis. Uploads by end users are scanned for viruses in real time as they are uploaded. Additional antivirus scans are performed against all Appian Cloud servers on a daily basis.

Key takeaway 3

Appian has the financial resources, staff resources, and global presence to provide a seamless, reliable, continuously monitored platform, and our resources and staff make us a reliable cloud partner. Yet Appian is also nimble enough to offer each major customer a high-touch experience, with optional controls set specifically to the needs of their mission.

Managing and continuously monitoring a reliable cloud infrastructure requires around-the-clock staffing, expertise available at all hours, a continuous investment of time and resources to keep current with security and compliance requirements, and rigorous process plans that must be thoroughly documented and periodically tested in order to meet customer audit requirements and disaster recovery SLAs. Small companies outsource these functions, giving them little control over events when problems happen. Appian keeps all the Appian-specific steps necessary to recover after an outage in-house, with 24x7x365 monitoring for external threats and internal anomalies.

In our security partnership with our customers, Appian can segregate logs and send log data back to each customer so they can leverage their own security operations as part of overall continuous monitoring of Appian-hosted applications.

Appian invests in numerous industry certifications to give customers confidence that we have met, or can meet, their internal security requirements. We devote additional InfoSec resources to the questionnaires and annual or biannual on-site audits required for each certification and support each customer's annual on-site audit requirement as part of the Enterprise support program—an important part of any enterprise software purchase that is generally hard for small companies to maintain over the long term.

And we support all this with a well-vetted disaster recovery and high availability plan that allows customers to make Appian an extension of their reliability and availability guarantee to their own customers. The time, effort, and financial expense Appian invests in disaster recovery planning enables us to provide a redundant data processing and storage environment.

Appian security partnerships are further enhanced through our position on control of data. Appian Cloud can host customer data, but this is never required. Customers can host any of their business data in their own cloud. And even when data is hosted in the Appian Cloud, customers can easily replicate it back to their own data centers for other use cases with the enhanced data pipeline. Appian aims to be a key part of our customers' data architecture, not an isolated island of disconnected information.

Continuous monitoring.

Appian Cloud instances are monitored 24x7x365 from multiple cities worldwide, with several defense-in-depth security mechanisms and a solution that aggregates and correlates data from many sources for monitoring purposes. This provides reviewers a central point for identifying potential issues or incidents across the Appian Cloud network.

To help prevent and mitigate threats, Appian automatically monitors key operational metrics and alerts appropriate personnel when certain operational thresholds are reached. This monitoring includes, but is not limited to the following:

- Storage space availability
- CPU utilization
- Memory utilization
- Login page availability
- Appian engine status
- Anti-virus alerts

In addition, Appian Information Security reviews common alerts on a daily basis and more frequently when front-line staff identify anomalous patterns. The systems and attributes monitored include the following:

- Security notifications and alerts
- Performance
- Platform response times
- Administrative accesses
- Security vulnerability monitoring
- Uptime/availability
- Compliance auditing

Appian has a dedicated system log server to protect audit logs and preserve them for any forensic investigations or other audit activities. Access is limited to personnel who require such access for their job duties. Appian logs are also available to Appian Cloud customer administrators for reviewing operational and security access of a specific cloud instance.

Log streaming.

Elite Support customers can have Appian stream all collected logs back for their own continuous monitoring efforts for industry certifications and internal audits. Most IPaaS providers cannot provide a service like this because their architecture is not segregated enough to do so. With Appian Cloud, customers can copy log and alert information into their own SIEM environment, correlate it with additional data they collect, and look for anomalous patterns across multiple attack vectors, some which would be invisible to Appian because they exist solely within customer infrastructure.

Appian Trust—compliance and audit programs.

Appian Cloud's comprehensive security compliance program meets an array of industry standards, including Service Organization Control 2 (SOC 2), PCI-Data Security Standard (PCI-DSS), International Standard for Assurance Engagements (ISAE) 3402, GxP, Health Insurance Portability and Accountability Act (HIPAA), ISO 27001, and FedRAMP. Each certification sets rigorous requirements and demands and requires evidence of conformance with those requirements via submission of test results and on-site audits. To protect customer data and continue to meet the certification requirements of each compliance framework, Appian hosts numerous annual third-party audits to validate that controls are operating effectively.

The list below identifies some of the certifications that are most important to Appian customers. A detailed description of each security framework, along with the accrediting organization's background and contact information, can be found in Appendix A of this document. Similar information, which may be more current, may be viewed at http://trust.appian.com. A mapping of controls between the many different compliance frameworks can be found in the submission to the Cloud Security Alliance registry.

Annual customer audits.

Appian customers with Enterprise support are entitled to perform an annual audit of Appian in order to support their own specific audit requirements. This might include a security questionnaire, an onsite visit with a full day of audit review meetings, and a walkthrough of facilities.

All customers under non-disclosure agreement are entitled to receive formal notifications of Appian compliance framework certifications. Please note that some frameworks, especially industry-specific ones, have additional requirements outside the scope of Appian Cloud.

Enhanced data pipeline.

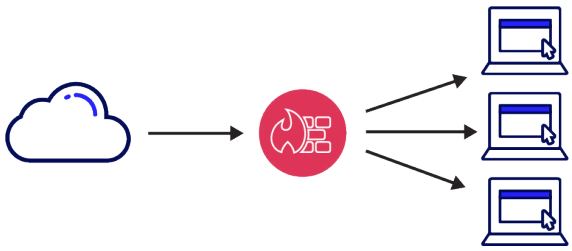
Appian gives customers the ability to make full copies of data exports at any time. Additionally, Appian Elite support customers can use an enhanced data pipeline that allows a native endpoint to connect to the business data source on an Appian Cloud instance, integrating the data source further with the customer's data processing procedures. The enhanced pipeline delivers the following benefits:

- Increased flexibility to access data with external DBMS tools (e.g., MySQL Workbench) and manage and analyze data in a more familiar way.
- Direct integration with data analysis tools, with enterprise reporting tools like Tableau and PowerBI directly connecting to the Appian Cloud business data source for unified analytics.
- Simplified ETL processes for exporting, transforming, and moving data to data marts and data warehouses located on a customer's own infrastructure.

Key takeaway 4: Appian secures the perimeter.

Appian Cloud secures its cloud instance and cloud infrastructure with a defense-in-depth approach: it layers web application firewalls, network firewalls, and multiple types of intrusion detection systems to identify attacks early and prevent them from reaching the servers where business and process data reside. Outbound communication to data centers via mutually authenticated, multichannel VPN tunnels with an optional inbound VPN tunnel supplement the best-in-class protection provided by AWS infrastructure. Appian Cloud's automated and redundant defensive posture never relies exclusively on out-of-the-box AWS controls, except for the physical security of the infrastructure layer.

Defense in depth protection.



Appian Cloud uses multiple layers of security components to apply its defense in depth security strategy across its global infrastructure. These measures guard access to Appian Cloud systems and prevent intrusion attempts. Software and network controls include, but are not limited to the following:

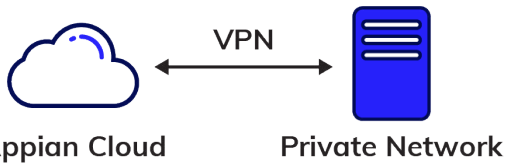
- A network intrusion detection system.
- A host intrusion detection system.
- A web application firewall.
- Network layer firewalls.
- File integrity monitoring.

Appian Cloud uses a tiered architecture segregated by multiple layers of firewalls. Public-facing servers, such as the web tier, reside in a demilitarized zone with customer and other non-public servers in their own segmented networks deeper within the architecture. Appian hardens network infrastructure to allow only the required ports and protocols necessary for the operation of the system. The default for access control is "access denied."

Appian further restricts the threat footprint with security tools from AWS, a third-party inspection solution, and home-grown security utilities.

One important but often overlooked defensive mechanism is the replacement of all virtual servers at each maintenance window. Appian Cloud always rebuilds its virtual servers from its current gold image of that server type, then copies customer artifacts and content to a specific server. The net effect is that any accumulated content not directly identified as customer data or known configuration changes simply disappears when security updates, hot fixes, or new releases are applied. In addition, with this approach, potential vulnerabilities that might lie dormant before activation are regularly removed.

Secure communications.



To enhance the security partnership, Appian Cloud supports additional mechanisms to allow customers to secure communications to and from the Appian Cloud, such as a secure VPN tunnel and access limitations based on trusted IP ranges. VPN connections from Appian Cloud instances can connect to a customer's private network on-premises, in a virtual private cloud (VPC) on AWS, or in a different cloud environment. Various transport protocols are supported, including IP Security (IPSec), and AWS private link offers another option for certain AWS-to-AWS communication channels. Dynamic routing using Border Gateway Protocol (BGP) adds reliability.

Leveraging this secure communication channel, Appian Cloud customers are able to control access to their Appian Cloud instances through their private and secure network with no network access from the public internet. Customers can use this secure concentration of connections to further restrict access, perform auditing, or look at additional threat vectors including insider threats.

Authentication and authorization.

To accommodate customer security requirements, Appian supports multiple authentication models. A native solution is provided with every Appian Cloud site, fully manageable from the site's administration console. Controls such as password requirements, lockout, and concurrent sessions are all modifiable for controlling user access.

Alternatively, if customers already have enterprise authentication solutions or require multi-factor authentication, Appian can be integrated with a Lightweight Directory Access Protocol (LDAP) or Security Assertion Markup Language (SAML) 2.0 authentication system already in use. User authentication configurations are available for configuring the Appian Cloud instance from the Appian Administration Console.

Control over authorization is flexible and can be granted widely or granularly. It can be implemented by groups defined within Appian or leveraged from external identity and access management (IAM) solutions. Access privileges are not shared across environments unless a customer administrator chooses to configure them that way. All access requests are logged and can be routed back to security information and event management (SIEM) solutions managed by the customer.

With the Appian platform, application-level granular control can be built into each customer application and added to entire application suites so that individuals only have access to what they need and granting and revoking access to specific functions and data is easy.

With the Appian platform, application-level granular control can be built into each customer application and added to entire application suites so that individuals only have access to what they need and granting and revoking access to specific functions and data is easy. Controls can be added at the page, data object, grid column, and all the way down to the individual control levels. This granular control, based primarily upon group permissions, allows customers to control visibility and editability. Appian customers are responsible for implementing these features using the principles of least privilege and segregation of duties.

Physical security.

Because Appian Cloud is hosted by AWS, all hardware resides in AWS data centers in the regions specified. AWS has a shared responsibility with its customers, including Appian Cloud. Details on how AWS controls security and specific frameworks can be found at https://aws.amazon.com/compliance. Appian inherently leverages all AWS physical control.

Key takeaway 5: Appian Cloud security controls.

Going beyond the perimeter and other security measures described previously, Appian also implements cloud security controls to maximize protection in the Appian Cloud.

Controls framework.

The security model and related policies and procedures for Appian Cloud are based on the frameworks listed at the Appian trust site, with the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) at the core. Appian follows the high-water mark in most cases across these frameworks, applying the strongest control set to all Appian Cloud sites.

Policies and procedures.

A security program is grounded in the policies and procedures that drive and standardize it. Appian has formal, documented policies and procedures covering a broad range of security topics: access control, personnel management, logging and monitoring, training, disaster recovery, change control, and risk assessments. These documents are updated at least annually as requirements and controls change. Strict control and review processes ensure that only appropriate changes are made.

Risk management.

Appian conducts an annual risk assessment that includes input from key stakeholders across the organization. These stakeholders meet quarterly to maintain and update the results of this assessment throughout the year. In addition, regular audits, control monitoring, vulnerability scanning, and penetration testing are performed to validate controls and ensure that new risks have not materialized and existing risks are being appropriately addressed.

Appian also has a vendor security assurance program to validate controls at least annually for third parties that support Appian Cloud. This process includes, as appropriate, site visits, control reviews, and reviews of security and audit reports. Appian looks for any material issues that would affect Appian, the Appian Cloud offering, or customers of Appian Cloud.

Access control.

Strict controls are in place to access the underlying infrastructure of the Appian offering. Personnel undergo a background check prior to access and periodic rescreening. Appian personnel also complete extensive cloud security training that covers Appian Cloud security and operational practices. Refresher training on Appian Cloud security and biannual reinvestigations are required for all Appian Cloud personnel.

Appian Cloud personnel have segregated responsibilities, with least privileged access to only the functions necessary to perform their role, which are reevaluated annually. Operational roles and security roles are always separate. Additionally, Appian Cloud access is always removed within 24 hours of an employee's termination or change in role.

Appian has implemented layers of security controls to appropriately restrict access to the Appian Cloud infrastructure. Controls include securely managed VPNs, multiple forms of multifactor authentication, jump servers to prevent direct access, Transport Layer Security (TLS) of all communication in transit, central access control systems with no wireless access within the cloud architecture, process management for account control, firewalls, intrusion detection systems, timed access, logging, and monitoring controls. Most importantly, logical removable media restrictions and outbound data flow restrictions are in place to prevent exfiltration of data.

To provide assistance, Appian Cloud and technical support teams have the ability to log in to customer sites. However, prior written authorization from the customer point of contact is required first, usage is tied directly to an individual, and Appian audits its usage to ensure appropriateness. Authorized access requires multi-factor authentication, and all access and administrative actions are logged. Sites conforming to FedRAMP or PCI-DSS requirements have further controls on this access.

Access to system-collected data files, whether database files or uploaded documents, is controlled in a similar way. Access requires multiple factors, all accesses to all cloud resources are logged, and access is further controlled via a jump box. Additional behavior-based controls exist to prevent anomalous activity, and more are added periodically. This is the basis of the data loss prevention regime at the platform level of Appian Cloud.

Incident response.

Appian monitors for security vulnerabilities continuously and encourages security professionals to report new vulnerabilities and security incidents via the Incident Reporting Form. All form submissions are investigated by the Appian Security Incident Response Team. If the reported vulnerability/incident has been confirmed to adversely affect an Appian product or service, Appian responds with fast, appropriate action such as hot fixes, upgrades, or mitigation information.

For any confirmed incidents or major updates that affect security, confidentiality, or availability of customer data, Appian will notify affected customers via the Technical Support application in Appian Forum.

Appian reviews security-related events at the infrastructure level on a daily basis, investigating and escalating unusual or suspicious activity as necessary. To reinforce our security partnership, customers have access to application and application server logs, including security logs that can be reviewed or downloaded via the web interface or via the log streaming option.

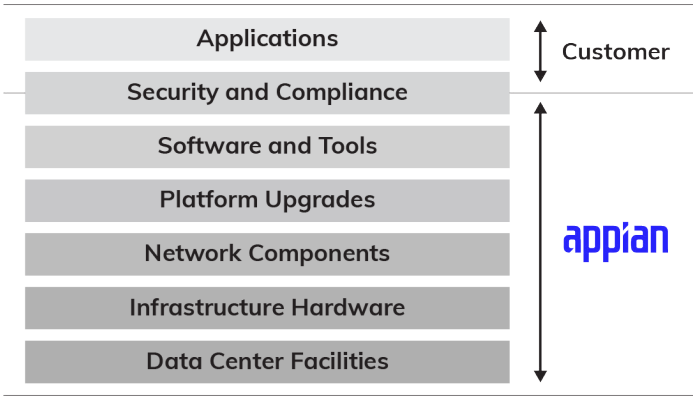
As part of our policy and procedure best practices, Appian has a documented incident handling and response guide that includes detection, analysis, containment, eradication, recovery, and reporting. Appian creates an after-action report for any incident, with lessons learned/corrective actions as appropriate to improve processes and security. Appian trains all cloud personnel on incident handling and response procedures and performs incident response testing at least once annually.

Appian has a documented incident handling and response guide that includes detection, analysis, containment, eradication, recovery, and reporting.

Shared security model.

Appian Cloud operates on a shared security model, breaking down control responsibility as either Appian owned, customer owned, or jointly owned.

Appian and hosting partner AWS are responsible for the security of the physical facilities, hardware, virtual networks and resources, and Appian platform installation and maintenance as well as the data stored within the Appian Cloud boundaries. Each Appian customer is responsible for all use of the platform through the web interface, integrations, and through other methods. Customers are also responsible for controls such as end-user administration, authentication and authorization, application development and security, and ensuring exposed functionality meets internal requirements and the requirements of accrediting organizations.



Data stewardship.

Data in the Appian Cloud belongs to each Appian customer, and the customer is the steward of all data usage. Appian security controls are designed so that Appian Cloud operations personnel do not need to have access to customer data via the application user interface, except in special debugging circumstances and with explicit customer permission. Appian treats all data as confidential and applies protections equally to all customer data. Encryption is also applied equally to all data, as is checking the integrity of host-level files. All other data use controls are considered a customer responsibility under the shared security model. This

includes any data classification and granular data integrity as a part of the application built and put into production, data loss prevention at the application layer including system generated emails, and any required privacy controls at the application tier.

Appian Cloud sites use data-at-rest encryption on all virtual storage devices, which includes the provided database in a cloud instance. In case additional levels of database encryption are needed, like row or column encryption, customers can use their own on-premise or private cloud-hosted database as the business datasource. This enables their own database administrators to set up the database around various industry best practices.

Our extensive history providing cloud solutions for leading enterprises has made Appian Cloud's security architecture among the most mature in the enterprise High-Productivity Application Platform as a Service (HPaPaaS) market.

Summary.

Our extensive history providing cloud solutions for leading enterprises has made Appian Cloud's security architecture among the most mature in the enterprise High-Productivity Application Platform as a Service (HPaPaaS) market. Appian is committed to transparency in our security posture and to helping our customers understand the Appian Cloud security framework.

As large enterprises, regulated organizations, and public sector agencies move to cloud environments, they are rightfully concerned about commingling data, unencrypted data, insufficient access controls, and unmonitored cloud assets. Appian is uniquely positioned to meet these needs through a robust, extensible HPaPaaS platform. Appian Cloud's single-instance architecture, extensive cloud security capabilities (including 24x7x365 operations team monitoring), and multiple security certifications make Appian a secure and reliable platform.

Appendix: Appian compliance frameworks.

To support the government, financial services, healthcare, and insurance organizations that rely on Appian Cloud, Appian participates in numerous reviews and audits to remain compliant with all the frameworks below. To maintain the data security, perimeter defenses, and overall reliability critical to our customers' organizational continuity, Appian provides a comprehensive approach to the security of the Appian Cloud environment. This includes careful review of policies, procedures, personnel, and overall operations of Appian Cloud, with a focus on transparency, third-party auditing, and attestation to independently certify Appian Cloud security operations.

SOC 1 / ISAE 3402.

Service Organization Controls (SOC) reports (formerly SAS 70 reports) are designed to help information systems operators and providers build trust and confidence in their service processes and controls.

Appian publishes a SOC 1 Type II report and an International Standards for Assurance Engagements (ISAE) 3402 report. Performed by an independent Certified Public Accountant, this audit engagement examines over a period of time the internal controls that could impact financial reporting. These reports are often important components of customer evaluations of their internal controls over financial reporting for purposes of supporting customers' financial statement audit and compliance needs.

A Type II engagement provides an opinion on the fairness of the presentation of management's description of the service organization's system and the suitability of the design and operating effectiveness of the controls. The effectiveness of the controls is evaluated based on their ability to achieve the related control objectives included in the description throughout a specified period, rather than just for a point in time.

SOC 2.

SOC 2 reports are intended to help a broad range of users understand internal control at a service organization as it relates to applicable Trust Services Principles and Criteria, including security, availability, processing integrity, confidentiality, privacy, and trust principles.

A Type II reports on the fairness of presentation of management's description of a service organization's system and the suitability of the design and operating effectiveness of controls over a period of time.

The SOC 2 Type II report provides a detailed review, by an independent audit firm, of Appian Cloud's security, availability, and confidentiality controls.

ISO/IEC 27001:2013.

An international standard for information security and risk management, ISO/IEC 27001:2013 protects organizations in all industries and sectors across the globe.

The ISO 27001:2013 standard calls for organizations to implement an appropriate Information Security Management System (ISMS), which ensures management, operational, and technical security controls are operating effectively.

By becoming certified in ISO 27001:2013, Appian Cloud demonstrates it has reached a high level of security maturity. With a goal of providing the most robust security possible, Appian has put controls in place to manage or eliminate security risks, enabling customers to trust that their confidential data is protected.

FedRAMP.

The Federal Risk and Authorization Management Program (FedRAMP) is a United States government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Being FedRAMP compliant means a cloud system has an established and highly secure environment that has withstood comprehensive audit review before federal agencies are authorized to engage the system.

Appian Cloud is FedRAMP compliant and has received an Agency Authorization to Operate (ATO) at the Moderate level.

By achieving FedRAMP compliance, Appian Cloud has been deemed a viable solution to provide significant time and cost savings, improved security risk management, and enhanced program transparency for mission-critical federal operations. This authorization can be reused by other federal agencies to save both time and staff resources.

Access the Appian Cloud FedRAMP compliant package

PCI-DSS.

The Payment Card Industry (PCI) Security Standards Council offers standards to enhance payment card data security. The PCI Data Security Standard (PCI DSS) provides a framework for developing a robust payment card data security process; including prevention, detection, and appropriate handling of security incidents. After agreeing to Appian Cloud PCI-DSS terms, customers can leverage Appian Cloud's PCI-DSS certification to reduce their own PCI compliance complexity.

Appian Cloud has been assessed by an external independent auditor and is compliant with PCI DSS.

Health Information Trust Alliance.

Organizations rely on prescriptive guidance from the Health Information Trust Alliance (HITRUST) Common Security Framework (CSF) for managing HIPAA security requirements.

To protect highly sensitive information, healthcare organizations—including health insurance companies, hospitals, medical practices, and SaaS providers—require HITRUST CSF (Common Security Framework) certified infrastructure.

HITRUST CSF uses nationally and internationally accepted standards including ISO, NIST, PCI, and HIPAA to ensure a comprehensive set of baseline security controls.

HIPAA.

The United States Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulates the security and privacy of Protected Health Information (PHI).

Appian Cloud is compliant with the HIPAA security requirements. With HIPAA compliance, customers can securely process and store PHI in Appian Cloud after executing a Business Associate Agreement.

Learn more about Appian and HIPAA

GxP.

Pharmaceutical and life sciences companies are required by law to meet Validation and Good Practice Standards (GxP) when building systems that touch or implicate predicate records. These include records and processes associated with clinical trials, laboratory work, quality assurance, regulatory information management, manufacturing, and electronic health records.

Appian Cloud has undergone an independent assessment performed by life science industry experts to evaluate Appian Cloud's controls and their alignment to GxP computer system validation requirements and standards.

Customers can leverage this independent assessment report to supplement and support their GxP compliance and diligence efforts.

Cloud Security Alliance.

The Cloud Security Alliance's (CSA) Security, Trust and Assurance Registry (STAR) program provides a comprehensive framework for cloud provider trust and assurance. The CSA STAR program is a publicly accessible registry designed to recognize the varying assurance requirements and maturity levels of providers and consumers and is used by customers, providers, industries, and governments around the world. The STAR program allows cloud providers to assess their controls against the CSA Cloud Controls Matrix.

Appian Cloud is registered in the CSA Security, Trust, and Assurance Registry, having completed the Consensus Assessments Initiative Questionnaire (CAIQ) covering 133 controls across 16 domains.

View Appian Cloud's STAR submission

DISA Level 2 (IL2) – Appian Cloud.

FedRAMP+ is the United States Department of Defense (DoD) adaptation of the FedRAMP process, where they independently approve cloud-based systems for DoD use.

Appian Cloud currently has a DoD Provisional Authorization (PA) rated at Level 2 Impact Level. For additional information on DoD Cloud Security Impact Levels, visit the DoD Cloud Security portal.

DoD customers can leverage Appian Cloud's PA when assessing and authorizing their system to operate on Appian Cloud.

FISMA.

The Federal Information Security Management Act (FISMA), enacted in 2002 and amended in 2014, provides a comprehensive framework for ensuring the effectiveness of information security controls for United States federal government IT systems. Together the Office of Management and Budget (OMB), Department of Homeland Security (DHS), and the National Institute of Standards and Technology (NIST) have put a program in place to set the standards and oversee compliance.

Appian Cloud has a security framework with a robust security control structure in place that enables federal organizations to achieve Authorization to Operate (ATO).

FDA.

The Food and Drug Administration (FDA) introduced 21 CFR Part 11 as a requirement for commercial life science companies that maintain FDA-required records and signatures in electronic format to meet specific standards and comply with good clinical, laboratory, and manufacturing practices. The primary goals of this regulation are to ensure the integrity of data; that changes made to the system are documented, reasoned, and non-repudiated; that computer systems used are trustworthy; and that applications are validated for intended use.

Appian Cloud supports the necessary capabilities and technology to allow customers to build applications that are compliant with 21 CFR Part 11.

UK G-Cloud.

G-Cloud 10 is a digital marketplace that enables the UK public sector to find people and technology for projects across the government. The G-Cloud Framework is made possible by the Crown Commercial Service (CCS), which is focused on providing commercial services to the public sector and saving money for the taxpayer. CCS is able to do this by combining policy, offering advice, pre-vetting quality offerings and allowing organizations to conduct direct buying.

CCS works with both departments and organizations across the whole of the public sector to ensure maximum value is extracted from every commercial relationship and to improve the quality of service delivery.

Appian Cloud is compliant with the G-Cloud Framework. Appian Cloud's G-Cloud certification can be found in the gov.uk Digital Marketplace.

Section 508 / VPAT.

The Rehabilitation Act of 1973, Section 508, requires that federal agencies' electronic and information technology is accessible to people with disabilities.

The Voluntary Product Accessibility Template (VPAT) is a tool used to document a product's conformance with the accessibility standards under Section 508 of the Rehabilitation Act.

Appian has completed the VPAT and the Appian product is compliant with Section 508. Learn more.

EU-US and Swiss-US Privacy Shield Frameworks.

The EU-US and Swiss-US Privacy Shield Frameworks were designed by the US Department of Commerce and the European Commission and US Department of Commerce and the Swiss Administration, respectively, to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce.

The privacy shield frameworks replaced the US-EU Safe Harbor framework in 2016 (EU) and 2017 (Swiss). Additional detail on these frameworks can be found at privacyshield.gov.

Appian is compliant with the EU-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union to the United States. The Appian Privacy Shield certification can be viewed on the Privacy Shield List.

appian

Appian is the unified platform for change. We accelerate customers' businesses by discovering, designing, and automating their most important processes. The Appian Low-Code Platform combines the key capabilities needed to get work done faster, Process Mining + Workflow + Automation, in a unified low-code platform. Appian is open, enterprise-grade, and trusted by industry leaders. For more information, visit **appian.com**.