# Security & Compliance FAQ

Digital.ai's approach to security is based on ensuring we create products that are as dependable as possible for our customers. Your trust and security are our top priority, so we're making our security program transparent by discussing the most common customer questions related to security and compliance.

**Does Digital.ai have an established information security and risk management program?**

**How does Digital.ai keep customer data secure?**

**How does Digital.ai manage customer data?**

**How does Digital.ai secure its internal environment?**

**How does Digital.ai ensure staff are working securely?**

**How does Digital.ai manage security incidents?**

**How does Digital.ai handle security vulnerabilities?**

**How does Digital.ai ensure security within supply chain partnerships?**

## Does Digital.ai have an established information security and risk management program? Yes.

Security and technology policies. Digital.ai has established an Information Security Program which is based on the ISO 27001 Information Security Management System Standard.

These policies describe the principles for maintaining trust and security for internal and cloud environments. We continually evaluate risks in our operations and improve the security, confidentiality, integrity, and availability of our environment. We regularly review and update security policies, perform application and network security testing of our environment, and monitor compliance with security policies.

Policy management. While programmatically, these policies are updated annually, if  we observe new threats and risks, we will update accordingly.

Risk management. We perform an annual risk assessment in support of our Enterprise Risk Management Program and implement projects to mitigate identified risks. We evaluate the current risks we face and ensure the controls we have in place effectively manage those risks.

Compliance. Our security program is developed in compliance with several industry standards. We understand complying with these well-known industry standards is critical to provide independent assurance to our customers that Digital.ai's security program meets a baseline of security controls.

Certifications. Our current certifications are listed below. Our main data hosting provider, AWS, has a SOC 2 and ISO 27001 certification.

| Product Name | Legacy Product Name | Certification(s) |
|---|---|---|
| SeeTest | Experitest | ISO 27001, SOC2 |
| Digital.ai Value Stream Intelligence | Numerify | SOC2 |
| Digital.ai Application Protection | Arxan for Android, iOS (EnsureIT)<br>Arxan for Web/Hybrid (SecureJS),<br>Arxan for Java Library | ISO 13485 |
| Digital.ai Key and Data Protection | Arxan for Whitebox (TranformIT) | ISO 13485 |
| Digital.ai App Management | Apperian | ISO 13485 |
| Digital.ai App Aware | Threat Analytics | ISO 13485 |
| GovCloud (Digital.ai Agility) | N/A | *FedRAMP in process* |

Internal and external audit. A comprehensive security evaluation as part of our annual compliance audits (e.g., ISO 27001, SOC2, ISO 13485) is performed which also involves an independent assessment by external audit firms. Additionally, we perform internal operational audits in areas that are considered high risk in various security domains. The results of the audit are fed into a continuous improvement cycle and corrective action program.

Privacy. Privacy controls are an important component of the program. Refer to Digital.ai Data Protection FAQ for further information.

## How does Digital.ai keep customer data secure?

Data encryption. Digital.ai utilizes encryption methods which are considered secure according to industry best practices to protect data both at rest and while in transit. All customer data is encrypted in transit over public networks using TLS 1.2+ to protect it from unauthorized disclosure and modification. Data at rest is protected using industry standard AES-256 encryption.

Tenant separation. While our customers share a common cloud-based IT infrastructure when using Digital.ai's products, we have measures in place to ensure they are logically separated so that the actions of one customer cannot compromise the data or service of other customers. Each customer's data is kept logically segregated from other tenants when at rest.

Controlling access. We treat all customer data as equally sensitive and have implemented stringent controls governing this data. All access is restricted to privileged groups unless requested and reviewed, with additional authentication requiring 2FA. Unauthorized or inappropriate access to customer data is treated as a security incident and managed through our incident management process.

## How does Digital.ai manage customer data?

Data availability. Digital.ai's cloud products are designed to leverage highly available data centers in multiple geographically diverse regions to minimize customer impact in the event of any disruptions.

Data backups. Digital.ai products utilize native AWS capabilities to collect snapshots of each instance to ensure availability of our services.Backups are regularly tested and issues are tracked until remediated.

Data resilience. Digital.ai strives to maintain strong Business Continuity and Disaster Recovery capabilities to ensure that the impact on our customers is minimized in the event of a disruption. The key principles include:

- Ongoing improvements
- Scheduled testing
- Dedicated people and teams

Service availability. Digital.ai strives to meet contractually required SLA/SLO criteria to ensure adequate availability of its products.

## How does Digital.ai secure its internal environment?

Network architecture. Digital.ai practices a layered approach to security for our networks. We implement controls at each layer of our cloud environments, dividing our infrastructure by zones, environments, and services. We also have environment separation to limit connectivity between production and non-production environments. Additionally, we have implemented intrusion detection in both our office and production networks to detect potential compromises.

Managing access. Digital.ai secures access to its corporate network, internal applications and cloud environments using active directory and 2FA. Digital.ai has a well-defined process for provisioning (assigning or revoking) user access for all systems and services and use role-based access control based on job duties.

Endpoint security. Digital.ai uses a combination of endpoint management to deploy updates and patches to operating systems and key applications. We have also implemented multiple endpoint protection solutions to protect against threats such as malware. This enables us to make sure all devices connecting to our network meet our minimum-security requirements, covering aspects such as encryption, device locking, anti-malware software and OS versions.

Change management. Our change management approach requires that each change – be it a code change or an infrastructure change – is reviewed by one or more peers to identify any issues the change may potentially cause.

Configuration management. Configuration management tools are utilized in our production environments to manage configurations and changes to servers. Digital.ai has maintained a current baseline configuration of all systems. Baseline is reviewed and update annually or as needed due to upgrades or significant changes. Previous configurations are maintained to support rollback. All changes to the baseline must be made via our standard change management process.

Logging and monitoring. Digital.ai uses centralized logging and monitoring to aggregate logs from various sources, apply monitoring rules and flag any suspicious activity. Our internal incident response process defines how alerts are triaged, investigated, or escalated.

## How does Digital.ai manage security incidents?

Incident Management. Digital.ai has a comprehensive set of security measures in place to ensure we protect customer information and offer the most reliable and secure services. We have a clearly defined approach structured on guidance from on guidance from NIST 800-61 Computer Security Incident Handling Guide for responding to security incidents affecting our services or infrastructure. All incidents are treated as serious. After a complete analysis, a decision is made to define the incident as serious or non-serious. If it is found serious, then the incident is reported to affected customers. All incidents are resolved as necessary.

Logging and monitoring. Our incident response approach includes comprehensive logging and monitoring of our products and infrastructure to ensure we quickly detect potential incidents.

Incident response process. Digital.ai has carefully defined processes that ensure there is clarity in what we need to do at all stages of an incident.

Cybersecurity incident response team. The incident response approach is supported by a team of highly qualified on-call incident managers who have significant experience in coordinating an effective response.

Customer notification. Digital.ai aims to notify any customer without undue delay if their data is involved in a confirmed incident or a breach.

## How does Digital.ai handle security vulnerabilities?

Continuous monitoring. Digital.ai uses vulnerability detection tools that are run across our products and infrastructure to automatically scan for and identify vulnerabilities. This includes application images, internal and third-party application, as well as our infrastructure bon premises and in our cloud. These identify vulnerabilities that exist and include network scans, container image scans, open-source dependency scans, and AWS configuration monitoring.

Internal security review. Our Security & Compliance team runs a security review program including internal auditing and security testing as a regular activity.

External testing. Digital.ai performs penetration test on all products and infrastructure at least once annually or when significant changes occur in the environment. Testing is conducted with an exclusive community of testers delivering real-time insights needed to remediate risk quickly while innovating securely.

Code review. Targeted code reviews, both manual and tools-assisted is being performed to enhance the product team's ability to self-detect and resolve vulnerabilities before the code reaches the customer.

Vulnerability tracking and remediation. Digital.ai's vulnerability management program integrates the processes we use to identify vulnerabilities with a centralized internal ticketing and escalation system. The security team provides oversight of this process and works with product and infrastructure teams to ensure accuracy of vulnerabilities, answer remediation questions, and ensure all vulnerabilities are resolved in compliance with remediation timeframes. Once a fix for a vulnerability is developed, it is tested thoroughly and then, in the case of our cloud products, incorporated into our CI/CD pipeline for deployment.

| Risk Rating | Timeline Vendor Release to Start of Deployment | |
|---|---|---|
| | High Priority Systems | All Other Systems |
| Critical | 5 Calendar Days | 7 Calendar Days |
| High | 14 Calendar Days | 30 Calendar Days |
| Moderate | 60 Calendar Days | 90 Calendar Days |
| Low | 90 Calendar Days | 180 Calendar Days |

Preventing vulnerabilities. Container images are scanned to ensure they do not consist of out-of-date or insecure libraries and components. It is critical that we are aware of what libraries we're using and that they are updated with the latest security bug fixes.

## How does Digital.ai ensure security within supply chain partnerships?

Third-party risk management. Third-party suppliers, including contractors and cloud service providers, are reviewed by legal and procurement teams for any proposed third-party supplier engagements. For any engagements deemed high or critical risk, additional reviews are performed by the Security and Compliance team. Ongoing due diligence also occurs via subsequent reviews either upon contract renewal or annually depending on the risk level of the engagement.

## Questions or Comments

The information in this FAQ was designed to provide you with the resources you need to address your security and compliance questions related to our products. If this information does not satisfy your needs or if you have any questions or comments, please contact us at: compliance@digital.ai.

## About Digital.ai

Digital.ai enables enterprises to focus on outcomes instead of outputs, create greater business value faster, and deliver secure digital experiences their customers trust. The Digital.ai Platform seamlessly integrates all the disparate tools and processes across the various value streams, uses data and AI/ML to create connective tissue between them, and provides the real-time, contextual insights required to drive and sustain successful digital transformation. With Digital.ai, enterprises have the visibility they've been seeking to deliver value, drive growth, increase profitability, reduce security risk, and improve customer experience.

**Learn more at Digital.ai**