Digital Asset

Digital Asset Security Posture

Secure Products, Secure Data

Digital Asset

March 2026

Executive Summary

Digital Asset understands and appreciates the importance of security to our clients, which is reflected in how we architect, design, develop, build and distribute our products, and in how we protect our staff, our locations, our and client's confidential data, our services, and our infrastructure. This position paper describes how we view security and the implementation of controls to ensure this is enforced.

Table of Contents

1 Digital Asset Security Initiatives and Programs

1.1 The Digital Asset Information Security Program

The goals of the Digital Asset Security Program include:

- Protect the information and privacy of our clients and partners.
- Protect Digital Asset staff, locations, data, services, and infrastructure from compromise or misuse.
- Ensure the appropriate security (Confidentiality, Integrity, and Availability) and privacy capabilities are built into Digital Asset products & services.
- Implement a secure Software Development Life Cycle (SDLC) process (plan, design, develop, package, distribute) to produce hardened, well-tested, high-quality products commensurate with their expected applications.
- Ensure Digital Asset clients, partners, and operations teams can deploy and run the product securely.

1.2 Security Program and Governance

The Digital Asset Information Security Program covers four primary views of information security:

- Corporate Security: the security of Digital Asset people, locations, data, systems, and services
- Secure SDLC: how we develop, test, and deliver our products
- Product & Service Security: the security of Digital Asset products and services
- Customer Security: enabling our customers to use our products and services in a secure manner

The Digital Asset Information Security Framework is diagrammed in Figure 1.

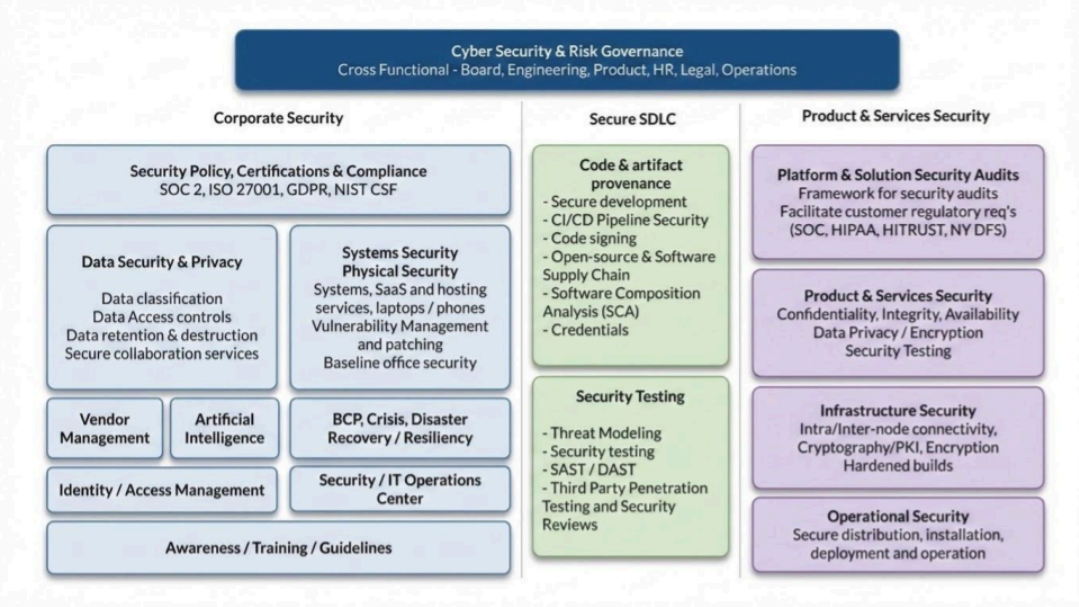

Figure 1: Digital Asset Information Security Framework

1.3 Digital Asset Security Team

The Security Team consists of staff who have made careers working for the largest financial services organizations. The team members hold many industry security certifications and have a breadth of experience across a wide variety of technology platforms and services.

1.4 Digital Asset Security Attestations and Certifications

Digital Asset monitors a variety of initiatives and regulations to ensure that it meets all regulatory, contractual, and compliance requirements. Our attestations and certifications provide confidence and external validation that Digital Asset's software and services are properly secured and protected against unauthorized modification or disclosure.

1.4.1 ISO 27001

Digital Asset is certified to ISO 27001:2022. The certificate is available on our Trust Center (https://digitalasset.com/trust-center).

1.4.2 SOC 2

Since 2019, Digital Asset has successfully completed the SOC 2 Type 2 independent audit with an unqualified opinion from our auditor. The scope of the assessment is our products and services with respect to the Common Controls and Security Trust Principle.

As the scope and range of services changes, we will also consider assessment against a broader scope of services and other SOC2 Trust Principles.

1.4.3 Privacy, GDPR and UK PECR

Digital Asset is compliant with the European Union General Data Protection Regulation (GDPR) and the UK GDPR and PECR regulations. Digital Asset monitors international, national and local privacy regulations to ensure we meet any requirements. We take the security and privacy of personal data seriously. Our privacy policy is published on our public website:

https://digitalasset.com/privacy

Questions relating to GDPR or our Data Privacy Policies can be directed to privacy@digitalasset.com

1.4.4 Cloud Security Alliance | Star Registry Participant

Digital Asset has completed and registered responses to the CSA CAIQ in the Cloud Security Alliance STAR registry. A version of that same response including all detailed comments is available under NDA from Digital Asset directly.

https://cloudsecurityalliance.org/star/registry/digital-asset-holdings-llc/services/digital-asset-holdings-llc

1.4.5 Other Third Party Vendor Risk Management

Digital Asset also participates in a number of Third Party Risk Management (TPRM) and external perimeter tracking services, including:

- Helios FSQS
- Prevalent
- Risk Recon
- Trusight
- Whistic
- UpGuard
- Process Unity
- KY3P
- Bitsight
- Security Scorecard
- Insurance Cyber Trackers - Corvus, Coalition

We have responded to Due Diligence questions from the major global financial services organizations.

1.4.6 Responsible Disclosure of Security Vulnerabilities

Digital Asset maintains a Responsible Disclosure policy for reporting security vulnerabilities and concerns. We do not currently operate a bug bounty program. The policy is detailed on our public website:

https://www.digitalasset.com/responsible-disclosure

The Digital Asset Security Team can be contacted at security@digitalasset.com

2 Security of the Company

2.1 Risk Management and Governance

Governance of the Risk Management program is executed through the Risk Management Committee, with a membership consisting of the COO, CFO, CISO, CTO, CPO, Head of Marketing and our General Counsel. The committee meets regularly to review identified risks and prioritize mitigation efforts. The committee reports to the CEO and, ultimately, to the Board on the critical concerns of the firm.

Digital Asset employs an established global risk management process consisting of three primary streams:

- Annual Risk Assessment: A comprehensive review of information security threats, critical assets, and the effectiveness of current controls.
- Risk Register: A centralized repository where identified risks are tracked, prioritized, and reviewed on a regular basis.
- Vendor Risk Assessments: Rigorous security and privacy reviews performed for third-party vendors and services.

2.1.1 Risk Management Policies and Procedures

Digital Asset maintains a set of industry standard policy and procedures, including:

- Information Security and Privacy Program & Policy Framework
- Authentication, Identity, and Access Management Policy
- Data Classification, Protection, Retention and Disposal
- Cloud and Network Security Policies
- Cryptography Policy
- Change & Incident Management
- DR, BCP and Crisis Management
- Vulnerability and Patch Management
- Vendor and Supply Chain Risk Management and AI Acceptable Use
- Open-Source Software Policy
- Fraud Detection and Prevention Policy
- Disciplinary Action Process

These are reviewed annually, and staff are required to acknowledge them annually.

2.2 Data Governance and Oversight

All Digital Asset staff are required to review and acknowledge all information security policies, including the Digital Asset Secure Information Lifecycle Policy, Data Privacy and AI. This defines data classification tiers for all data and defines the appropriate handling, backup, retention, and destruction requirements.

Digital Asset requires appropriate risk assessment of all data services used for storage and processing of Digital Asset data, including data shared from partners and clients. Reviews are particularly focused on confidential information (including customer data if applicable), Personally Identifiable Information (PII), internal security requirements and broader compliance requirements for GDPR and related data privacy regulations.

2.3 Supply Chain Risks and Vendor Management

As a supplier to many financial services and financial market infrastructure providers, Digital Asset is aware of its position in the overall supply chain. The company works to ensure that our customers can trust us with their data, trust our products in their environments, and trust applications and services built on our technology.

Digital Asset Vendor Risk Reviews are performed for all vendors/business associates. The use case, scope, and data classification drive the risk assessment process. Overall risk rating and general risk maturity are created specific to the vendor and the data class being handled. Critical vendors are reassessed annually or on major changes of use.

2.4 Email & Web Security

Digital Asset has implemented mail gateway services for inbound and outbound email security. This filters and protects emails to staff, including spam, malicious emails, attachment and URL security, and malware protection. Phishing awareness training is provided to all staff, and continual simulated phish campaigns are performed to drive further awareness and measure employee susceptibility to phishing attacks.

Digital Asset has implemented local endpoint agents and browser extensions to protect against website-based attacks and other forms of spam and phishing attacks.

Digital Asset has implemented email security controls (DMARC, DKIM, and SPF) to reduce the opportunity to impersonate the firm or staff.

2.5 Endpoint Security

All users are required to use Digital Asset managed endpoints for work-related activities. All endpoints are managed centrally by MDM solutions. Native capabilities of the device and MDM services are leveraged for full disk encryption, firewall, configuration compliance, security agent enforcement, screensaver locks, and other security requirements.

Digital Asset leverages a suite of host-based agents to ensure comprehensive protection, including real-time next-gen malware detection and endpoint detection and response (EDR), insider risk and data leakage prevention (DLP), USB blocking agent and a vulnerability scanning agent is deployed to all endpoints to provide continuous vulnerability scanning and audit oversight.

2.6 Network Infrastructure

Digital Asset corporate network is in place between Digital Asset offices and cloud provider private networks. Network segmentation is used to segregate networks from each other within each cloud environment. Firewalls are used at all office locations to block malicious traffic. Security Groups and firewall rules are used in Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure to block malicious traffic. For production GKE clusters, Google Cloud Armor is implemented to provide threat protection against common attack vectors such as those listed in the OWASP Top 10.

The network infrastructure is patched in a timely fashion, with monthly configuration samples taken as part of our audit-control process. Network traffic is sampled and reviewed, and flow traffic is sent to our SIEM for malicious traffic analysis.

Secured, full tunnel VPN is installed and available on all Digital Asset endpoints through a connection icon in the menu bar of each endpoint, should the Digital Asset employee find themselves working on an untrusted network.

2.7 SaaS, Cloud Services and Infrastructure

Digital Asset leverages many SaaS cloud-based services and also uses public cloud (AWS, GCP, and Azure) to host and run our corporate infrastructure.

A mixture of public and private network segments, with firewall rules and access control lists in each cloud provider, are used to ensure that only trusted entities are allowed access to resources within these cloud environments.

IAM roles and policies are in place to control user and administrative access to the cloud environments and administrative consoles. The principle of Most Reasonable Privileged Access is followed when provisioning user and service account access to the cloud resources. A privileged access management (PAM) process is in place to control, authorize and document privileged access right escalations.

All rights and account access are regularly reviewed and inventoried as part of the Digital Asset audit process.

For data held in SaaS services, Digital Asset leverages DoControl to provide automated guardrails and security oversight. This solution enforces automated permissions revocation for cloud SaaS, specifically monitoring and automatically removing Google Drive permissions for files shared with external parties after 30 days. To secure the interconnected application environment, Astrix Security is utilized for oversight of service-to-service integrations and non-human accounts. The security team uses this platform to review for non-human accounts, third-party extensions/add-ons for risky integrations and to monitor related logs for anomalous behavior across the company.

Security events from syslogs, network flow logs, and cloud audit logs are forwarded to our SIEM tool for centralized logging, alerting, threat detection, and ticketing for remediation. The security team monitors the logs to identify potential threats and unauthorized activity and follows appropriate steps for remediation.

The Orca Security vulnerability assessment platform and other Cloud Security Posture Management (CSPM) solutions are used to identify and remediate vulnerabilities and misconfigurations in all environments. Additional open-source security tools and in-house developed solutions are also used to audit and validate security configuration and access.

2.8 Personnel Security

2.8.1 Staff Background Checks

All Digital Asset staff are required to pass background and screening checks. This includes ten-year criminal background checks. These checks are performed at a local level and include checks against the legal systems in the country of residence.

2.8.2 Staff Onboarding and Offboarding

Digital Asset employs comprehensive onboarding and offboarding processes that include the provisioning and deprovisioning of physical resources, as well as user logon accounts, logical access rights, and data access permissions. User access is revoked on the last day of employment. Staff access rights are periodically reviewed for alignment to role or function.

2.8.3 Security Awareness Training

Security is considered a key responsibility of each and every member of staff. The company provides onboarding and ongoing awareness training. Training includes:

- Onboarding security training for all new hires
- Annual Security Awareness training and acknowledgement
- Continual Phishing testing and awareness
- Use-case- or SME-related training, as required
- Annual Policy review and acknowledgement

Employees are provided training for emergency situations with CPR, fire drills, and table-top exercises as available.

2.9 Physical Security

Digital Asset requires physical security controls for all office locations. These may be maintained by Digital Asset directly or utilize building management or office services. Each staff member is required to have an individual access badge to access the office spaces. Security cameras or CCTV are required, as appropriate based on risk, only ingress/egress points and for internal secure technology or IT closet. Ingress lists are produced on a monthly basis and reviewed against current employee lists.

Digital Asset does not maintain its own data centers, but utilizes premier-tier cloud services providers, including Amazon AWS, Google GCP, and Microsoft Azure. The security of physical access to such services is delegated to the service providers, who can provide the appropriate security certifications and assessments on request.

2.10 Artificial Intelligence

Digital Asset has established guidelines for the secure, ethical and responsible use of all Artificial Intelligence (AI) tools.

Digital Asset follows a human-in-the-loop requirement where all generative AI outputs must be reviewed for accuracy, bias, and appropriateness. Employees are prohibited from utilizing confidential data with publicly available AI tools. Confidential data is only permitted with officially sanctioned tools with appropriate corporate data protection terms, such as Google Gemini, Slack AI, and Github CoPilot Business with authorized LLM models. New AI tools undergo security and legal reviews via our Vendor Risk Management Process where security, model training, and data protection terms are considered.

3 Secure SDLC

Digital Asset runs full CI/CD pipelines for the development, build, packaging, distribution, and deployment of our technologies. The firm has implemented a variety of controls to ensure the security, quality, and provenance of our products and services. The Digital Asset Security Team continually assesses these controls in light of changes in industry best practices, our product features, services, and choice of technology.

3.1 Goals of Secure SDLC

- Security considerations are brought as early in the process as practical.
- All code is tested, reviewed, and approved prior to submission.
- All commercial and open-source dependencies are understood and tracked.
- Licensing of dependencies is understood and approved.
- Vulnerabilities are identified and mitigated during development and during the lifetime of artifacts.
- Opportunities for introduction of Harmful Code accidentally or intentionally are removed.
- Enhancing our practices to align with industry best practices as these evolve.

3.2 High-Level CI/CD Pipeline

Digital Asset follows industry best practices in the setup and management of its CI/CD pipeline (Figure 2). Digital Asset has implemented and continues to evolve a set of controls at various gates of the pipeline.

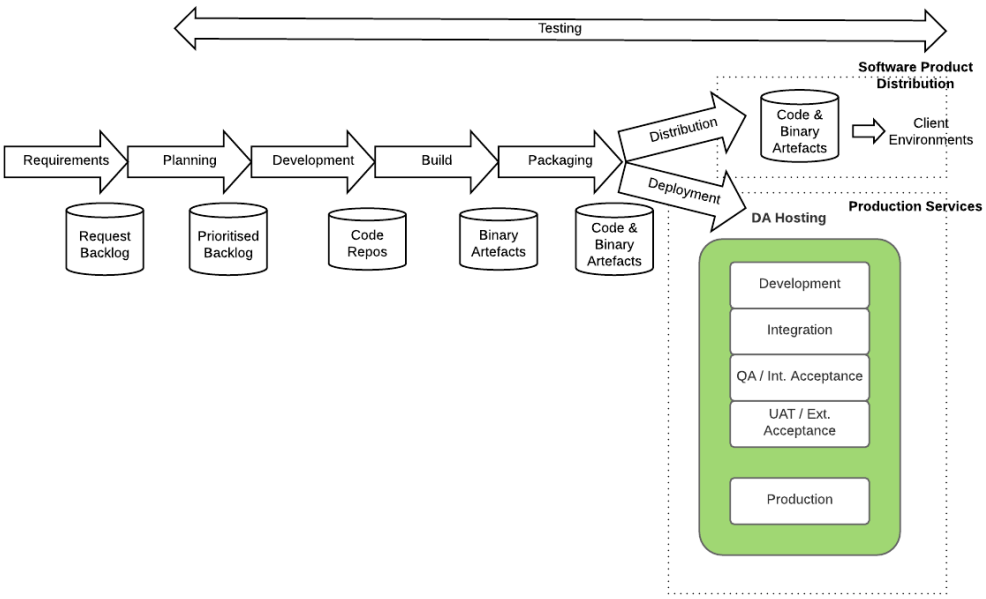

Figure 2: Diagram of SDLC Pipeline

3.3 Pipeline Security

3.3.1 Infrastructure

CI/CD pipelines are used to build Digital Asset products. Administrative access to these systems (build pipelines, configuration, and infrastructure) is restricted to an approved set of Security and DevOps engineers. Access logs are sent to our SIEM for review.

Sensitive credentials for the build pipeline are managed and secured through the pipeline KMS services and are not stored in source code or configuration files. Access to the build infrastructure is also restricted to a core set of staff.

3.3.2 Build Pipeline Compliance and Security

Digital Asset has implemented Pipeline Security Compliance checks. This includes:

- CI/CD and SCM posture checks
- Credential scanning and reviews, including access or API tokens, SSH keys, webhooks
- Third-party extensions and add-ins, and their access permissions
- SCA checks for vulnerability and licensing
- Pipeline access permissions review and behavior monitoring
- Artifact integrity checks
- Artifact repo deploy permissions

3.4 Source Code Management (SCM)

Digital Asset uses GitHub as its source code management system for its proprietary and open source projects. Branch protection rules are enforced for code reviews (see below) and build & test check completion prior to code merge.

For open source projects, CLA (Contributor License Agreements) are enforced for external contributions with mandatory Digital Asset staff reviews of contributions.

3.4.1 Code Reviews

All GitHub Pull Requests (PRs) are reviewed prior to being committed to the “main” branch. GitHub branch protections are used to enforce that all PRs must successfully pass all automated tests (unit, integration, functional, non-functional, CLA, etc.) before they can be merged. Additional tests and jobs are scheduled daily and weekly to perform other security scanning activities.

In the case of submissions to our open source projects, Digital Asset staff are required to review all external contributions prior to merging to the main branch. No external staff are authorized to approve such code submissions.

Where code submissions may result in production changes (Infrastructure / Application as Code deployments, External Releases), peer review and approval are required as part of our Change Management process.

Digital Asset continues to improve the efficacy and completeness of its code reviews and testing through new tools and through developer security awareness training.

3.4.2 Source Code Analysis

Digital Asset utilizes a variety of tools to review its code (SAST, Veracode, credential scanners and compiler restrictions). Many Digital Asset staff have backgrounds in security and formal analysis. These reviews cover both functional and non-functional aspects. Digital Asset continues to evaluate new tools in this space to improve the effectiveness and completeness of coverage.

3.5 Vulnerability Management, Software Composition, and Supply Chain Risk

Digital Asset has open sourced significant portions of the Daml and Canton code bases and is also a heavy user of open source components and libraries. Digital Asset uses commercial and open source tools to discover (Software Composition Analysis, SCA) and validate the set of all open source dependencies. These tools allow Digital Asset to identify improper licensing or vulnerabilities in upstream dependencies that are used in Digital Asset products.

Synopsys BlackDuck is used to identify dependencies in Digital Asset products and to scan for software license issues (toxic and copyleft license types) and vulnerable dependencies. All identified issues are ticketed and assigned to relevant product or component owners for assessment and prioritization. Digital Asset provides a Bill of Materials (BOM) detailing all components in a release and their associated licenses.

Digital Asset also leverages other tools, such as Ox Security, GitHub Repository Vulnerability Analysis and Google Container Registry Analysis to identify dependencies and their associated vulnerabilities in source code and Docker containers.

As this is a rapidly evolving area in the security space, the firm continues to evaluate additional tools and works to understand best practices in this area.

3.5.1 Containers and Docker Security

Digital Asset uses Docker technology during the development, testing, and distribution of our products. We use Blackduck SCA Analysis to scan for vulnerabilities in published images. We continue to evaluate additional tools to enhance our capabilities of vulnerability analysis and runtime access control and protection.

In line with other open source projects, Digital Asset updates the base images of Docker containers as new ones are released, keeping the same minor & patch release version. Changes to functionality or updates to dependencies to the components layer on top of base layers

result in a new patch release version. Companies that use Docker caching repos may need to ensure that updated images are pulled for base layer changes.

Due to the wide variety and quality of such tools, we work with our customers to evaluate any differences they detect through their chosen tools.

3.6 Release Management & Artifact Signing

Digital Asset software releases are taken from the source repo main branch and built through the automated CI/CD tools. The main branch reflects the latest set of peer-reviewed and tested code.

All releases are tested through automated and manual tests prior to publishing and distribution.

Code signing is done when pushing to a variety of external artifact repos, and access to the signing keys is controlled within the CI/CD toolset. Only a very small set of engineers have access to the signing keys.

Details of our public signing key can be found here :

https://docs.daml.com/getting-started/manual-download.html