AUTODESK

Prodsmart Security Whitepaper

October 2022

Prodsmart Security Whitepaper

Contents

1 Introduction

Prodsmart is a cloud-based Manufacturing Execution System that optimizes the shop floor and connects entire organizations with digitized and automated manufacturing processes. Prodsmart helps manufacturing companies to plan, assign, manage, track and analyze fabricating and manufacturing shop floor production with one software solution.

As of 2022, Prodsmart is part of the Autodesk portfolio and adheres to Autodesk's security framework, which is based on industry standards. Autodesk's security framework is embedded in Prodsmart to protect the confidentiality, integrity, and availability of customer information.

Prodsmart is designed for high availability and scalability, providing our customers with a fast and resilient cloud service. Prodsmart's cloud hosting provider is Amazon Web Services (AWS), a leader in cloud infrastructure. Autodesk relies on the AWS hosting provider shared responsibility model, which includes infrastructure composed of the hardware, software, networking, and facilities that run AWS cloud services. For more information, please refer to: https://aws.amazon.com/compliance/shared-responsibility-model/.

1.1 Document Purpose

The purpose of this document is to outline Autodesk's security framework and information security standards and practices with focus on Prodsmart, and to explain Prodsmart's multi-tenant live production environment.

2 Autodesk Security

The Autodesk security framework is based upon industry standards to ensure consistent security practices, enabling us to build secure, run secure, and stay secure.

- Build secure - Embedding security into our products from the ground up is a critical part of securing our customers' investment in Autodesk products and services. Run secure – We build security directly into our infrastructure. Our holistic approach includes deployment of endpoint protection tools, standardized patching and hardening requirements, identity and access management controls, and offensive security activities.
- Stay secure - Security at Autodesk is focused on three core objectives that protect the confidentiality, integrity, and availability (CIA) of information:
    - Confidentiality: Information is accessible only to authorized persons
    - Integrity: Information is complete and accurate
    - Availability: Data is accessible and available to customers

The Chief Security Officer (CSO) is accountable for the development, implementation, and governance of the security strategy and program and ensures that security policies and standards are applied across all Autodesk products and environments. The CSO and security team are supported by Autodesk executives and Board of Directors.

3 Human Resources Security

Autodesk employees are required to follow the company's Code of Conduct, which requires every employee to conduct business lawfully, ethically, with integrity, and with respect for each other and the company's users, partners, and competitors. Per the Acceptable Use Policy, employees must protect the security, confidentiality, integrity, and availability of Autodesk and customer information.

Autodesk security is also supported through an internal information security awareness program, implemented through a variety of training methods (e.g. instructor-led training, e-learning, periodic newsletters). Employees with privileged role(s) and access (e.g. cloud operation teams) are required to take additional role-specific training to ensure protection of customer data through cloud services.

Where permitted by law, background checks are required for employees with access to the computing resources and support systems used by the Autodesk teams.

4 Access Management

Autodesk restricts access to information and systems based upon business and security requirements to prevent unauthorized access. Access is granted using the principles of least-privilege and need-to-know basis. Formal processes are documented for user provisioning, registration, and de-provisioning. Privileged access is restricted and requires additional management approvals.

Access to software source code and production environments is restricted and aligned with business, security, and privacy requirements.

- Asset Management

Asset management and protection begins with maintaining an inventory of assets with correlated roles (e.g. owners, custodians) and responsibilities for all assets. Autodesk assets inventory includes the name of the asset owner in an Autodesk managed Asset Management System. Assets are classified based on several criteria, such as asset value and importance, business criticality, implementation environment, and associated security and privacy requirements. Inventory of assets recognizes the context of systems that process, transmit, or store customer information.

Formal rules are defined for acceptable use of information assets and handling of assets throughout the assets' lifecycle.

5 Cyber Security Risk Management

Autodesk's Cyber Security Risk Management program considers information security risks as operational risks, defined by the occurrence of any threat event that could compromise Autodesk assets (i.e., unauthorized use, loss, damage, disclosure, or modification of assets) for the profit, personal interest, or political interest of individuals, groups, or other entities, or because of accidental wrongdoing. Risk assessment in Autodesk is a continuous process of risk evaluation and subsequent implementation of controls or actions to limit and maintain the risk to an acceptable level. Autodesk's cyber security risk management program consists of the following elements: risk assessment, risk treatment, and risk monitoring and communication.

An overall risk assessment is performed at least annually, or when new risks are introduced or identified. Continuous monitoring and reassessments are performed for high and critical risks identified. Risk assessments are performed by Autodesk's security team, and assessment results are presented quarterly to relevant business stakeholders and

annually to Autodesk's board of directors. Autodesk's Cyber Security Risk Management methodology follows industry standards and frameworks and includes the following steps: prepare for assessment, conduct assessment, communicate assessment results, and maintain and monitor risk.

6 Data Classification, Management, and Protection

Autodesk implements controls to manage and protect the end-to-end information lifecycle, from creation/acquisition to retention and deletion. Autodesk considers highly sensitive information such as customer PII and intellectual property as confidential restricted information. Security requirements for confidential-Restricted information include:

- Strong authentication and access restrictions based on business need-to-know principles to authorized individuals
- Encryption of data in transit and at rest
- Storage on secure drives not directly accessible from the Internet
- Defined backup procedures, retention periods, integrity checks, and destruction procedures

We store your personal data and content on our servers and the servers of our service providers. Because we and our service providers maintain servers in global locations, your personal data may be transferred across national borders and stored on the servers outside of your country or region. We will retain your personal data for as long as necessary to provide you with the offerings that you are using or have requested, for the establishment, exercise or defense of legal claims, and as needed to comply with our legal obligations. Data may persist in copies made for backup and business continuity purposes for additional time.

7 Cryptography

Cryptographic controls are implemented to ensure the protection of confidentiality, integrity, and authenticity of information.

Autodesk key management controls define the requirements for the use, protection, and lifetime of cryptographic keys and keying material. Cryptographic key management activities are performed by authorized Autodesk employees who adhere to relevant policies.

8.1 Prodsmart Cryptographic Practices

Prodsmart implements cryptographic algorithms based on leading best practices and standards. Information is protected with the most efficient cryptographic controls, taking into consideration the state of the information (i.e., in transit or at rest) and the system or a system component which processes, transmits, or stores information.

Prodsmart implements cryptographic mechanisms for inbound and outbound data flows. All customer data is encrypted in transit and at rest:

- Encryption in transit: TLS v1.2 (min.)
- Encryption at rest: AES-256 (Database, Backups, etc.)

8 Secure Software Development and Change Management

Secure design, coding, testing, and maintenance processes are integrated into Autodesk's secure software development lifecycle methodology. During the design stage, Autodesk creates detailed design documents and threat

models, which are reviewed and approved by security architecture experts to assess functionality, scalability, security, and performance. Software engineers and architects perform peer reviews to detect deviations from secure development practices and maximize code quality. An integral part of the secure development process also includes Static Application Security Testing (SAST), and third-party library scanning. Penetration tests are performed at least once a year by an external vendor.

Functional and acceptance testing programs include manual and automated techniques to check that services are developed on predefined and testable criteria.

1 Operations Security, Vulnerability, and Patch Management

Secure operational procedures and responsibilities are implemented to protect the processing and storage of customer information.

Security non-negotiables require the implementation of security controls for each system component (e.g., server, database, network device, service, etc.) taking into consideration the classification of information processed, transmitted, or stored. Systems and services are continuously monitored, scanned, and tested to validate the correct operation of security controls. Standard system hardening requirements are enforced through configuration and vulnerability scanning activities.

Information about technical vulnerabilities is continuously monitored and processed in a timely manner. Vulnerability identification methods include automated vulnerability scanners, penetration testing, bug bounty programs, and gathering of threat intelligence. All production systems and system components are in scope of the vulnerability management process.

Identified vulnerabilities are evaluated and appropriate measures are taken to remediate identified risks. The priority of vulnerability remediation is determined by a combination of the vulnerability severity score corresponding to CVSS (Common Vulnerability Scoring System) v3, exploitability, exposure, and existing compensating controls.

Remediation methods for all in-scope systems and components include patch management, software change, or implementation of compensating controls. Continuous patching is performed.

10.1 Prodsmart Operational Controls

In addition to the above-described controls, Prodsmart has implemented the following operational security controls:

- Hardening: All system and application infrastructure components are hardened
- Web Application Firewall (WAF): WAF is configured and enabled to protect against common web application attacks
- Anti-malware controls: Advanced anti-malware and anti-virus technical controls are implemented across Prodsmart environments and are combined with operational controls such as Security Awareness Training to increase awareness of malware threats across all employees and users
- Intrusion detection and prevention: Alerts from intrusion detection systems are monitored and investigated for any unusual or suspicious behavior; when alert investigation results in a suspect on true positive alert, Autodesk's Incident Response process is triggered
- Threat intelligence: Threat intelligence sources are regularly reviewed and evaluated for applicability in Prodsmart products; applicable threats are prioritized in accordance with the risk level

9 Prodsmart High Availability and Clustering

Prodsmart is designed to achieve a high level of availability by employing redundant systems in its supporting infrastructure and distributing load across auto-scalable instances. Clustering technology keeps Prodsmart highly available by limiting single points of failure and directing service requests away from instances that are highly utilized. All services are monitored for resource usage (e.g., CPU, memory, storage), DB operation performance, and liveness probes. Automated compensating behaviors and alerts are triggered in cases where the threshold is reached, and action is needed.

As patches and upgrades are applied to the production environment, a rolling deployment approach is taken for Prodsmart whenever possible, aiming to limit downtime of the service.

10 Network Security

Network security management processes and controls ensure the protection of information in networks and supporting information processing components. Services and interfaces are grouped taking into consideration their function, sources, and destination of traffic and exposure. Groups are segregated in network segments (e.g., public, DMZ, internal, restricted, etc.) and filtered by appropriate network security devices, permitting only approved network traffic matrices. The deny-all principle is used on all network filtering security devices.

Transfer of information is protected taking into consideration the nature and risks of each channel. Network security is enforced using a combination of physical and logical controls, including encryption, firewalls, and systems-hardening procedures.

11 Backup and recovery

Backup copies of information, software, and system images are taken and tested regularly to protect against the loss of data. Backup policies define the frequency of creating backups, appropriate security controls and retention periods. After the expiry of the backup retention period, information is securely disposed.

Backups are encrypted at rest and access is restricted to privileged users. Recovery testing is periodically conducted to validate the integrity of backup data and to verify the duration of the recovery process.

12 Prodsmart Data Replication

Data is backed up daily and stored for 30 days to an offsite location, after which it is securely disposed.

13 Logging and monitoring

Production systems and applications are configured to log events and activities to support automated event correlation and analysis. Logs are protected against tampering and unauthorized access with special attention to administrator access and operator logs. An audit trail is established for all relevant user-system interactionsThe retention period of logging records is kept according to business and regulatory requirements.

14 Incident Response

Autodesk implements a security incident response process to consistently detect, respond, and report incidents, minimize data loss, mitigate risks, and restore information system functionality and service continuity as soon as possible.

Autodesk has a documented Security Incident Response Process (SIRP) to effectively manage security incidents. Roles, responsibilities, and procedures are established to ensure a timely and efficient response to potential security or privacy-related incidents. All employees and external parties are required to report any observed or suspected security events in systems or services.

The incident response process includes:

- Continuous monitoring of threats and alerts
- Establishment of an information security incident response team
- Establishment of clear procedures for identifying, responding, assessing, analyzing, and follow-up of information security incidents
- Facilitation of clear communication of security incidents with internal and stakeholders
- Continuous improvement from information security incidents to reduce the probability or impact of future incidents

The SIRP is periodically reviewed and evaluated for effectiveness. The incident response process is tested annually to assess the effectiveness of the process and training of security incident response stakeholders.

15 Compliance

Autodesk assesses its compliance against data protection and information security standards on a regular basis. Autodesk implements security policies based on industry best practices and regularly conducts internal and external audits, attestations, and certifications. Management of information security and the implementation of related processes, policies, and procedures are independently reviewed and audited periodically or when significant changes relevant to security and privacy domains occur. Reviews and audits also include technical inspections to assess the effectiveness of controls to ensure compliance with compliance frameworks, regulatory requirements, or contractual requirements.

Autodesk has selected industry standard attestations and certifications for our products. To learn more please visit Autodesk Trust Center Compliance.

16 Privacy

Legal requirements related to privacy and protection of personally identifiable (PII) are continuously monitored and implemented across Autodesk's operations.

Autodesk is transparent about how customers' personal data is collected and used. Read the Autodesk Privacy Statement to learn more.

17 Additional Resources

The following resources provide general information about Autodesk and other topics referenced in the main section of this document.

- To learn more about Autodesk, visit http://www.autodesk.com
- For more information on our comprehensive security program, visit http://trust.autodesk.com