minware.

System Description of minware's Software Development Observability Platform

Updated April 30, 2024

Purpose and Scope of Report

This report is intended to provide report users with information about the service organization's system relevant to security to enable such users to assess and address the risks that arise from their relationships with the service organization. This description is intended to focus on the internal control structure of minware that is relevant to only users of its Software Development Observability Platform and does not encompass all aspects of the services provided or procedures followed by minware.

System Description

Company Overview and Services Provided

minware is an all-remote SaaS service company that analyzes data from version control, ticketing systems, and calendars to provide insights about software engineering productivity.

minware's goal is to help client's organization consistently follow best practices used by top-performing teams by providing a step-by-step scorecard and tracking the impact of improvements on productive engineering time. minware tracks best practices across the entire software development lifecycle, from basic ticketing and version control hygiene to predictable sprints, roadmap delivery, and quality.

minware's time model precisely allocates work time to commit activity. It works by dynamically creating a schedule for each author based on their history (so you don't have to manually specify work schedules or time zones), and then allocating active work time between commits to the commit that follows.

Principal Service Commitments and System Requirements

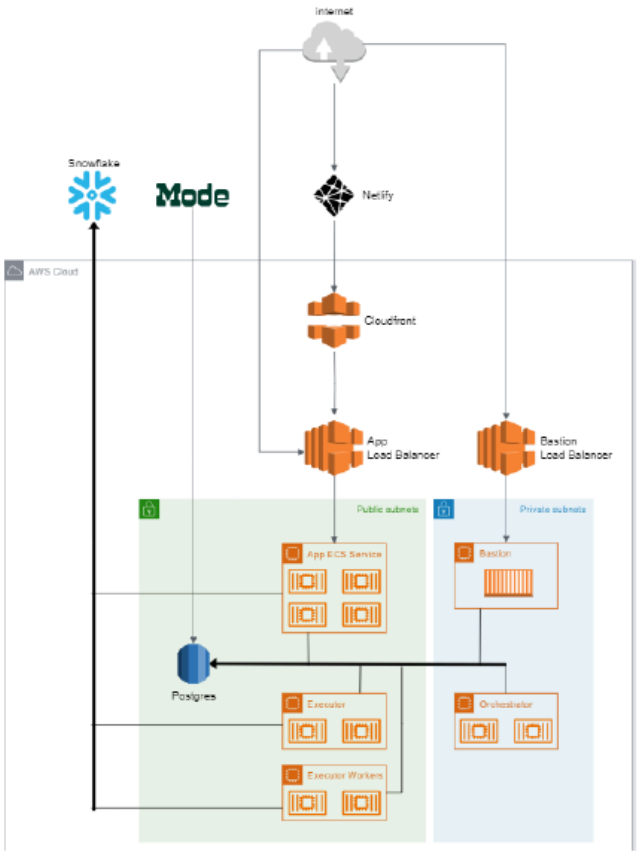
minware designs its processes and procedures related to its Software Development Observability Platform to meet its objectives. Those objectives are based on the service commitments that minware makes to user entities, the laws and regulations that govern service providers, and the financial, operational, and compliance requirements that minware has established for the services.

Security commitments to user entities are documented in customer agreements. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Software Development Observability Platform that are designed to permit system users to access the information they need based on the permission of least privilege provisioning.
- Use of encryption protocols to protect client data at rest and in transit.
- Security of systems services and system components on AWS and Snowflake.
- Monitoring of subservice organizations controls including AWS and Snowflake.

Infrastructure

The minware Software Development Observability Platform's infrastructure is hosted on the AWS cloud platform and uses Snowflake for its data warehousing. Security within the Software Development Observability Platform is addressed by a combination of AWS security groups, MFA, and secure SSH protocol tunneled access through a bastion host on an EC2 instance. Access to the Snowflake database is fortified through the use of SSH protocol tunnels that pass through a dedicated bastion host. The SSH tunnel employs encryption, safeguarding data in transit and providing secure remote access. With the bastion host acting as a single-entry point for SSH connections, it becomes easier to monitor and manage access, allowing system administrators to enforce strict security policies and maintain a high level of data protection within the AWS-hosted Snowflake architecture.



Software

The following provides a summary of the software and related services used in the delivery of the Software Development Observability Platform:

- AWS – cloud infrastructure services.
- Cloudwatch –monitoring and logging of the cloud infrastructure.
- GuardDuty - threat detection service monitoring cloud infrastructure.
- AWS Inspector – vulnerability management service scanning cloud applications settings and configurations.
- AWS ECS – compute services used for scheduled compute.
- AWS Lambda – serverless compute services for on-demand processing jobs.
- AWS S3 – storage services.

- AWS Secrets Manager – manage, retrieve, and rotate secrets and keys.
- Linux – for the bastion host.
- Jira –help desk ticketing, project management, and workflow of alarm configurations to automatically generate a ticket for tracking and resolution.
- GitHub – version control software and CI/CD platform.
- Netlify – composable platform used to build and deploy serverless backend services.
- NEXT.js with React - for the presentation layer of their Web Interface and backend systems.
- Terraform - IAC tool used to automate infrastructure tasks.
- Docker – deployment of applications inside containers.
- NewRelic – application performance monitoring and logging tool.
- OpsGenie - manage and centralize system monitoring alerts.
- Snowflake – data warehousing solution.
- Postgres DB – database management system.
- PopSQL – business intelligence tool.
- Mixpanel – tracking and logging user activities.
- Mode – business intelligence tool.
- Google Workspace – productivity apps (Gmail, Drive, Docs, etc.).
- SendGrid - for email notifications.
- Slack – business communication platform throughout the organization.
- Auth0 –authentication and authorization services to the application.
- BitWarden – password management services.

- Stripe – payment processing platform.
- Dropbox – file storage.

People

People involved in the operation and use of the system are:

- CEO – Responsible for the general oversight of the company and overall business strategy.
- Information Security Steering Committee (ISSC) – Responsible for ensuring the operational effectiveness of the Information Security Policy and all other associated policies and procedures.
- Principal Security Engineer – Responsible for all aspects of the system and application security engineering, conceptualizing and management of projects, and managing technical security risks.
- Employees & Contractors – Responsible for upholding security practices and following company policies and procedures.

Procedures

Executive Management personnel maintain documented automated and manual standard information security policies and procedures involved in operation of Software Development Observability Platform.

Control activities have been placed into operation to help ensure that actions are carried out properly and efficiently. Control procedures serve as mechanisms for managing the achievement of control activities and are a part of the process by which minware strives to achieve its business objectives. minware has applied a risk management approach to the organization in order to select and develop control procedures. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed, and improved when necessary to meet the applicable trust services criteria and the overall objective of the organization.

The minware control procedures, which have been designed to meet the applicable trust services criteria, are included in Section 4 of this report to eliminate the redundancy that would result from listing the procedures in this section as well.

Data

minware ingests data nightly from customer version control, ticketing, and calendar systems to provide insights related to a company's software development practices. Customers' system data is loaded via API integrations and interested into the data warehouse, Snowflake. Once ingested, the data is loaded and transformed by the application, which queries snowflake and displays the following types of reports within the web application:

- Custom Reports and Dashboards - Allow the user to define custom metrics and reporting based on the underlying software development data sources.
- Time Allocation - Provides a high-level view of how people spend their time and whether that time was used productively.
- Sprint Trends - Shows how tasks flow through sprints based on their estimates and illustrates trends in delivery vs. commitments.
- Scorecard - Provides a comprehensive list of how well people follow best practices across all layers of the productivity stack with specific, actionable insights about the most important areas to improve.
- Sprint Insights - Shows a detailed breakdown of all the activity that occurred during a particular sprint, both from a time and ticket/point perspective. This report is designed for teams to use during sprint retrospectives.
- Predictive Roadmap - Helps you plan out future projects and observe historical progress on a per-project basis, with dynamic projections based on configurable team velocity.

Data in transit is protected by employing secure and encrypted communication channels. Specifically, data transfers are safeguarded using the TLS protocol, which ensures that any data moving between the minware and client environments remains encrypted and inaccessible to unauthorized entities. This encryption mechanism is crucial for maintaining the confidentiality and integrity of the data as it traverses potentially vulnerable networks.

System Boundaries

System boundaries, pertaining to collection, use, retention, disclosure, and disposal or anonymization or personalization of data, are governed by contract provisions for particular service engagements. Data is not utilized or disclosed to third parties outside of the scope allowed in such contracts and agreements.

Subservice Organizations

AWS

minware uses AWS for hosting production systems. AWS is responsible for the uptime, management, physical and logical security of the infrastructure that supports the delivery of internet, and environmental conditions that provide power and cooling to their devices. AWS is also responsible for providing physical security controls, administration of their hardware equipment, and reporting any logical or physical security incidents.

The applicable trust services criteria that are intended to be met by controls at AWS, alone or in combination with controls at minware, and the types of controls expected to be implemented at AWS to meet those criteria are described in the section below:

Control Activities Expected to be Implemented by AWS	Applicable Trust Services Criteria
AWS is responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.	CC3.1, CC3.2
AWS is responsible for restricting logical and physical access to their facilities and system components including firewalls, routers, and servers.	CC6.1, CC6.2, CC6.4, CC6.5
AWS is responsible for maintaining segregation of minware's environment(s) from other AWS clients.	CC6.1, CC6.6
AWS is responsible for securely disposing of hosted physical assets once they have reached end-of-life.	CC6.5

Control Activities Expected to be Implemented by AWS	Applicable Trust Services Criteria
AWS is responsible for the management of any third-party vendors with access to customer environments.	CC9.2

Snowflake

Snowflake provides a cloud-based data warehousing solution that manages the storage, retrieval, and analysis of data. It is responsible for maintaining the integrity and security of the data, facilitating scalable and elastic data operations that can adapt to changing workloads. Additionally, Snowflake is tasked with compliance management, adhering to industry standards and regulations to ensure that data handling meets the required security and privacy benchmarks. It supports the SaaS company's analytics and data-driven decision-making by offering a reliable and efficient data warehousing service.

The applicable trust services criteria that are intended to be met by controls at Snowflake, alone or in combination with controls at minware, and the types of controls expected to be implemented at Snowflake to meet those criteria are described in the section below:

Control Activities Expected to be Implemented by Snowflake	Applicable Trust Services Criteria
Snowflake is responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.	CC3.1, CC3.2
Snowflake is responsible for maintaining segregation of minware and minware client environments from other Snowflake clients.	CC6.1, CC6.6
Snowflake is responsible for the management of any third-party vendors with access to customer environments.	CC9.2
Snowflake is responsible for limiting access to information systems and data through user authentication and authorization.	CC6.1, CC6.2
Snowflake is responsible for utilizing firewalls, intrusion detection systems, and other measures to prevent unauthorized access.	CC6.1, CC6.2, CC6.3, CC6.6

Control Activities Expected to be Implemented by Snowflake	Applicable Trust Services Criteria
Snowflake is responsible for maintaining comprehensive information security policies that are communicated to and acknowledged by employees.	CC2.2
Snowflake is responsible for implementing formal processes to manage changes to system software and configurations.	CC8.1
Snowflake is responsible for securing facilities with controls such as badge access, surveillance cameras, and environmental protections.	CC6.4

On an annual basis, minware obtains a third-party SOC 2 Type II report from subservice organizations and reviews the report and testing results to determine if there were appropriate controls in place, and that they were operating effectively. In the event that there are exceptions or controls not operating effectively at the subservice organization, this risk is incorporated into a risk assessment and appropriate actions are taken to mitigate future risks.

Control Environment

Control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Below are the key areas and the description of controls that support the minware control environment.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of the control environment affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the products of the entity's ethical and behavioral standards, how those standards are communicated, and how they are reinforced in practice. Behavioral standards could include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts and the communication of entity values and behavioral standards to personnel through policy statements, codes of conduct, and leadership's example.

minware has implemented, maintains, and regularly communicates a code of conduct and other policies regarding acceptable business practices, guidance on conflicts of interest, and expected standards of ethical and moral behavior. minware's management conducts business dealings with employees, suppliers, customers, and auditors on a high ethical plane and insists others have similar business practices.

Commitment to Competence

Competence is the knowledge and skills necessary to accomplish tasks that define the individual's job. Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge.

minware assigns job responsibilities to personnel based on knowledge and skills needed to adequately perform each job. minware reinforces these responsibilities by providing hands-on training during the initial period of employment, and continual hands-on training for new business processes or job responsibilities.

Management's Philosophy and Operating Style

Management's philosophy and operating style encompass a broad range of characteristics. Such characteristics may include the following: management's approach to taking and monitoring business risk; management's attitude and actions for the security of information. minware's management takes a relatively conservative approach to information processing and risk associated with new business ventures.

Organizational Structure

An entity's organizational structure provides the framework for how company-wide objectives are planned, executed, controlled, and monitored. A relevant organizational structure includes considering key areas of authority and responsibility, as well as appropriate lines of reporting. An entity develops an organizational structure contingent, in part, on its size and nature of activities.

The responsibilities of key positions within minware are clearly defined and communicated. Individuals that hold key positions are knowledgeable and experienced within the industry. minware's organizational structure supports communication of information both up to leadership as well as down to support staff, ensuring clear and effective communication channels. minware's organizational structure consists of five primary business units that work together to deliver the Software Development Observability Platform.

The five business units consist of:

- Executive Management - Responsible for providing execution of business objectives and strategic direction.
- Finance and Human Resources Team – Responsible for managing financial operations and ensuring compliance with regulations.
- Sales Team – Responsible for identifying and pursuing sales opportunities to achieve revenue goals.
- Marketing Team – Responsible for developing and implementing marketing strategies to generate leads and support sales.
- Customer Support and Success Team – Responsible for providing technical support and building customer relationships to improve product success.

- Product and Development Team – Responsible for designing, developing, and implementing software products to ensure their success.

Assignment of Authority and Responsibility

Assignment of authority and responsibility includes delegation of authority to deal with organizational goals and objectives, operating functions, and regulatory requirements, including responsibility for information systems and authorizations for changes. Policies are established relating to business practices, knowledge, and experience required of key personnel and the appropriate number of people to carry out duties. In addition, management's policies and communications are directed at ensuring that personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

As mentioned above, minware has defined job responsibilities and clear communication channels to disseminate information within the organization; this enables minware to react to market and regulation changes and to meet its goals and objectives. minware is appropriately staffed to support its operations, particularly with respect to critical areas such as software development, implementation, customer support, and IT system support.

HR Policies and Practices

HR policies and practices relate to hiring, orientation, training, evaluating, counseling, and remedial action. Standards for hiring the most qualified individuals with emphasis on educational background, prior work experience, past accomplishments and evidence of integrity and ethical behavior demonstrate minware's commitment to hiring and retaining only highly competent and trustworthy people. Personnel career growth and reward of meeting expectations are driven by periodic performance feedback and demonstrate minware's commitment to advance qualified personnel to higher levels of responsibility. Personnel who work for minware are required to read and acknowledge the company's internal policies and confidentiality requirements as well as the confidentiality of customer-managed information.

Risk Assessment

minware management performs an annual risk assessment, which requires management to identify risks in its areas of responsibility and to implement appropriate

measures to address those risks. minware's management reevaluates the risk assessment annually or when otherwise necessary to both update the previous results and to identify new areas of concern.

The risk assessment process consists of the following phases:

- Identifying: The identification phase includes listing out risks (including threats and vulnerabilities) that exist in the environment. This phase provides a basis for all other risk management activities.
- Assessing: The assessment phase considers the potential impact(s) of identified risks to the business and its likelihood of occurrence.
- Mitigating: The mitigation phase includes putting controls, processes, and other physical and virtual safeguards in place to prevent and detect identified and assessed risks.
- Reporting: The reporting phase results in risk reports provided to managers with the necessary data to make effective business decisions and to comply with internal policies and applicable regulations.
- Monitoring: The monitoring phase includes minware management performing monitoring activities to evaluate whether processes, initiatives, functions and/or activities are mitigating the risk as designed.

Consideration of Fraud

Risks of fraudulent activities being carried out are addressed in the risk assessment and the treatment process described above by the risk management team. This process is aimed to identify and address the company's vulnerabilities to internal and external fraud.

In-Scope Trust Service Categories

The table below provides the TSC within the scope of this report. The controls designed and implemented to meet the applicable TSC criteria have been included in Section 4.

Trust Services Category	Definition
Security	Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the security of information or systems and affect the entity's ability to meet its objectives.

Security

Security refers to the protection of

- Information during its collection or creation, use, processing, transmission, and storage.
- Systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Trust Service Categories and Related Control Activities

Integration with Risk Assessment

Along with assessing risks, minware has identified, and put into place, the necessary actions to address those risks and help ensure competent and efficient operations. Control activities serve as mechanisms for managing the achievement of the security principle and applicable criteria.

Selection and Development of Control Activities

The applicable TSC and related control activities are included in the control matrices, within Section 4 of this report, to eliminate the redundancy that would result from listing the items in this section as well. Although the control activities are included in the testing matrices set forth below in Section 4, they are, nevertheless, an integral part of minware's description of its Software Development Observability Platform. Any applicable TSC that are not addressed by control activities at minware are also described within the control matrices.

Information and Communication

Information

Information is necessary for minware to carry out internal control responsibilities to support the achievement of its objective related to its Software Development Observability Platform. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of internal control.

The following provides a summary of internal and external sources of information used in the Software Development Observability Platform:

- Third-party vendor attestation reports are obtained and reviewed, and remediation plans are proposed and monitored through resolution.
- Release notes are communicated to internal system users for system changes, maintenance, and upgrades that affect system security and functionality.
- Annual penetration tests are performed, and remediation plans are documented and tracked until resolved.
- System change management activities (e.g. development efforts, testing, peer review, approvals, etc.) are documented within Jira and GitHub.
- Security events are documented, tracked, resolved, and communicated to all affected parties.
- Enterprise monitoring statistics (e.g. performance, availability, utilization, and capacity levels) are monitored using CloudWatch and New Relic.

Communication

Throughout the organization, minware conducts monthly and quarterly meetings to identify and address significant issues affecting its operations. A defined agenda and corporate information system are used as established vehicles for addressing and monitoring activities, accomplishments, and issues. A monthly management meeting provides the vehicle for Executive Management to communicate and respond to operational tasks and issues. The minware BoD meets regularly to discuss internal controls, operations, and business objectives.

Internal Communications

minware has implemented various methods of communication to help provide assurance that employees understand their individual roles and responsibilities and that significant events were communicated. These methods include orientation for new employees and ongoing training for employees. Job descriptions are provided to employees and evaluations are completed against those job descriptions annually.

External Communications

minware has also implemented various methods of communication to help provide assurance that customers understand the roles and responsibilities in communication of significant events. These methods include the use of e-mail messages and a customer contact option on the minware website.

Monitoring

Monitoring is generally performed through active, hands-on management, including regular management and BoD meetings. Management is involved and active in the business. minware utilizes a risk-based approach to monitor business units and other entities throughout the organization, ensuring that enterprise-wide risks are prioritized and addressed in order of significance. Results from the risk evaluation are documented in formal communications to management and other relevant parties.

minware monitors customer communications through the help desk ticketing system. This information is provided to the system administrators, providing the ability to track, monitor and assist in understanding customer complaints or concerns, and to evaluate and resolve special requests in a timely fashion. Management's ability to actively monitor customers' communications is integral to controlling the quality of the services provided.

minware monitors customer communications and engagements through their customer support department. Client communications are received by the customer support department and are then disseminated throughout the minware organization.

Management strives to be proactive in responding to customer complaints and maintaining a high level of inter-departmental communication about these events. Customer complaints and other issues are handled via the customer support department.

User Entity Controls

The control activities performed by minware cover only a portion of the overall internal control structure of minware's user entities. Therefore, each customer's internal control structure must be evaluated in conjunction with minware's control policies and procedures described in this report. minware's controls over its Software Development Observability Platform were designed with the understanding that certain user entity controls were in place and operating effectively.

Complementary User Entity Controls	Related Applicable Trust Criteria
User entities are responsible for immediately notifying minware of any actual or suspected information security breaches, including compromised user accounts.	CC7.3
User entities are responsible for determining whether minware's security infrastructure is appropriate for its needs and for notifying the service organization of any requested modification.	CC6.0
User entities are responsible for notifying minware of any approved contract modifications.	CC6.2
User entities are responsible for ensuring that user IDs and passwords used for accessing minware systems are assigned only to authorized individuals and that the roles assigned to the user account are appropriate.	CC6.2
User entities are responsible for ensuring the confidentiality of any user accounts and passwords assigned to them for use with minware's Software Development Observability Platform.	CC6.2
User entities are responsible for notifying minware of any changes to their confidentiality requirements and obtaining approval in writing.	CC9.2