Workiva

SECURITY BRIEF

Information Security

Introduction

Workiva created Wdesk, a cloud productivity platform for enterprises to collect, link, report, and analyze business data with control and accountability. Thousands of organizations, including over 75 percent of the 500 largest U.S. corporations by total revenue, use Wdesk to mitigate risk, improve productivity, and give users confidence in data-driven decisions.

Workiva is responsible for the security of critical business information for companies. We take this responsibility very seriously and have gone to great lengths to earn the trust of our customers. Secure products are instrumental to maintaining this trust. We strive to create innovative products that serve our customers' needs and operate in their best interests.

Workiva focuses on several aspects of security that are critical to business customers:

- Application and security architecture – Our applications are designed and developed with careful consideration given to customer data security, reliability, and integrity
- Data security – Customer data is stored in secure facilities, on secure servers, and within secure applications
- Data privacy – Confidential information is kept private
- Organizational and operational security – Policies and procedures ensure security at every phase of design, deployment, and ongoing operations

This paper describes our security implementation; that of our Platform as a Service (PaaS) and hosting partner, Google; and our Infrastructure as a Service (IaaS) hosting partner, Amazon. Together, we utilize numerous physical, logical, and operational security measures to ensure the utmost in data security and privacy.

Product overview

Workiva powers solutions for:

- Compliance
- Reporting
- Enterprise

We are committed to our customers' success and designed our platform to deliver these benefits:

- Time-savings
  - Real-time collaboration – Your entire team can review and edit reports simultaneously
  - Easier content creation – Optimized for reporting formats but lets you leverage existing office documents
  - Multiplatform review – Edit or review on any device
- Improved accuracy
  - Data linking – Eliminates the clerical work of manually updating changes
  - Single document data model – Data lives in one place, so it is accurate everywhere

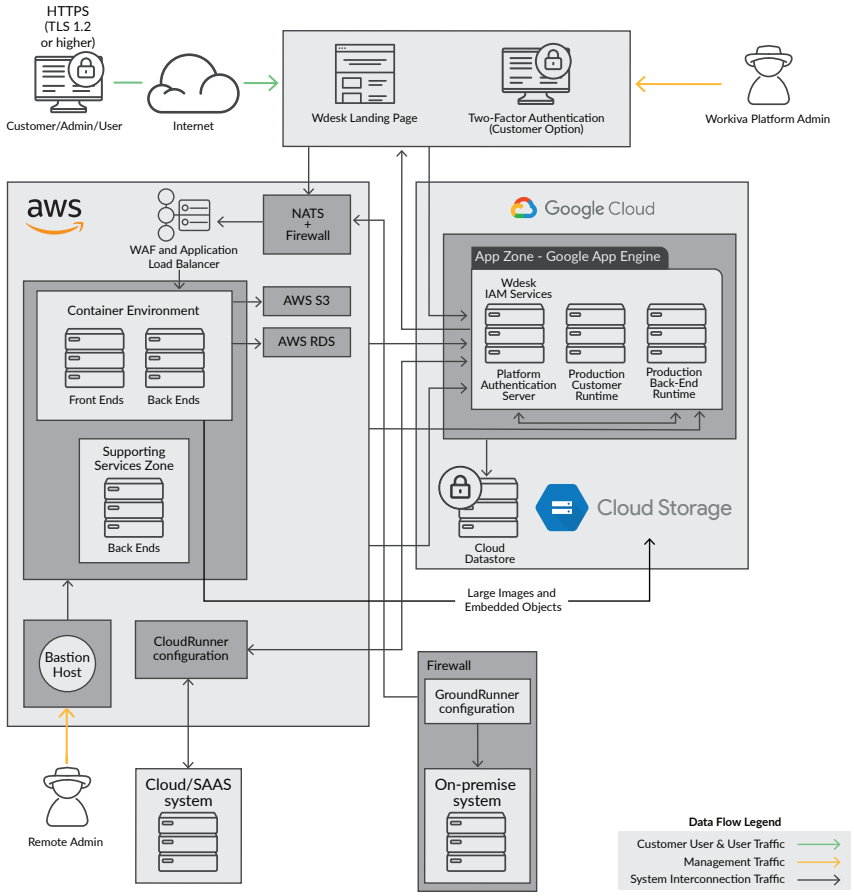
Application and security architecture

The Workiva platform is based upon a four-tier, service oriented architecture as shown in Figure 1.

Access control

Application and web service access is controlled through our authentication system. The system allows our customers to set custom password requirements as an administrative function. Customers may choose password strength criteria including minimum number of characters and inclusion of a case change, a number, and a special character. Customers

FIGURE 1: Wdesk Platform Architecture



may set password expiry rules and force individual users or all users to reset their passwords. This authentication system also supports SSO (Single Sign-On) with SAML (Security Assertion Markup Language) and two-factor authentication. Customers may choose to lock out individual users or deny access to all accounts instantly.

Data security

Protecting our customers' data is at the core of what Workiva does. Wdesk encrypts data both in transit and at rest using at minimum 128-bit encryption methods. Wdesk runs in a restricted sandbox environment on Google appspot. In this environment, the application can execute code, store and query data in the Google App Engine (GAE) datastore, use the GAE mail, URL fetch and user services, and examine the user's web request and prepare the response.

Reliability and data integrity

Google App Engine (GAE) is built on the same infrastructure as Google's search engine and designed for maximum performance and reliability. Google's grid-based computing platform assumes ongoing hardware failure. Google's robust software failover system is designed specifically to withstand this disruption. In addition, GAE scales rapidly to handle heavy loading conditions. GAE replicates both our software and data among thousands of servers and data centers as needed in response to increased loading conditions.

In addition, GAE detects loading conditions that are geographically biased and replicates software and data to be physically close to the load source. This provides the best possible experience for Wdesk users no matter their location. Finally, Google's infrastructure ensures that any additional software and data instances are synchronized in real time, so end users never see stale or orphaned data.

Data privacy

Workiva is exceptionally sensitive to company and user privacy. We realize that the data stored in our product is confidential and highly sensitive. Workiva ensures that the information our customers trust us with is never compromised. Our legally binding privacy policy that protects all services can be found by visiting workiva.com/legal/privacy-policy. At no time will Workiva employees access confidential user and customer data without prior consent. This policy will not be altered in any potentially damaging way without express written consent from the customer. Workiva data center storage is determined by the client. Clients determine if they want data stored within the United States or Europe.

Organizational and operational security

Workiva business information security starts with people and processes. Security must be built into products, infrastructure, and corporate culture from the very beginning. The Workiva Information Security Team is responsible for information security throughout the business and works with all areas of the company. This team meets regularly to review policy, process, and practices, and makes decisions and recommendations to Executive Management.

Compliance

Workiva successfully completes the rigorous SOC 1 Type II and SOC 2 audit processes. The company engages a leading independent audit firm to perform these extensive reviews. SOC audits establish that Workiva employs uniform and reliable operational controls and safeguards as a host and processor of data belonging to their customers. In addition, Workiva adheres to all rules and best practices for HIPAA & GDPR compliance.

Workiva is also FedRAMP-authorized at the moderate security impact level. Workiva has met exacting FedRAMP standards in order to ensure government agencies and departments can trust their data with Wdesk.

System development

Workiva uses a defined Software Development Life Cycle standard with an emphasis on functionality, quality, responsiveness, and security. This systematic approach includes a process to manage change in such a way to ensure that any customer facing services are thoroughly reviewed, tested, approved, and well-communicated.

Business continuity

Business continuity, high availability, and disaster recovery are all included with Wdesk. The cloud basis for Wdesk provides for high availability. With the robust infrastructure of both Google and Amazon, business continuity plans can provide for substantial impacts.

From an enterprise perspective, Workiva recognizes the fact that our mission-critical service delivery relies heavily upon centralized customer success operations, in addition to information technology systems and services at third-party providers. As such, Workiva has a written plan of action to rapidly respond to key enterprise resource needs in the event of an unplanned event (e.g., facilities emergency, natural disaster, or adverse conditions).

Customer confidentiality and securities trading policy

During the course of business, Workiva employees and consultants may become aware of material nonpublic information for a publicly traded company. Federal securities laws prohibit any person from buying and selling securities while in possession of such information. For this reason, we have implemented a strict Customer Confidentiality and Securities Trading Policy along with internal processes and education programs that support enforcement and awareness.

Publicly traded companies, whether a direct customer or not, are placed on a no-trade list the moment relevant business activity warrants this designation. No-trade companies are tracked in our enterprise sales and support database. This list of no-trade companies is updated daily and made available to all employees and consultants of Workiva.

Furthermore, employees are required to disclose their personal holdings and notify the Workiva compliance officer of intent to buy or sell securities whether the securities are on the no-trade list or not. Employees or consultants who violate the Workiva Customer Confidentiality and Securities Trading Policy are subject to immediate disciplinary action up to and including dismissal.

Conclusion

Workiva provides secure and reliable management of your business reporting information. We bring you the latest technologies and best practices for software design and data integrity. When you entrust your company's information with us, you can do so with confidence, knowing that the full weight of the technology and infrastructure investment of Workiva and Google is brought to bear to ensure the security, privacy, and integrity of your data.

For more information about Workiva, go to workiva.com or email info@workiva.com.

sb20200317-j41772
The information contained herein is proprietary to Workiva and cannot be copied, published, or distributed without express prior written consent. Copyright 2020 Workiva Inc. Workiva and Wdesk are registered trademarks of Workiva Inc. All rights reserved.