GoodData Corporation

Security White Paper

Apr 2017

Executive Overview

The GoodData Enterprise Insights Platform is designed to help Enterprises and Independent Software Vendors (ISVs) securely transform their data into actionable insights and deliver them to business users, customers, and partners at their point-of-work to drive better business outcomes. GoodData realizes that helping to protect our customer's data, ensure proper security regulations, and mitigate any potential risk is essential to building trust and delivering a high-level of service. GoodData takes a risk based approach to security and this paper will detail the many different measures and technologies in place to protect our customers.

Our security implementation allows us to adhere to the following best practices, demonstrating our commitment to customer security and privacy:

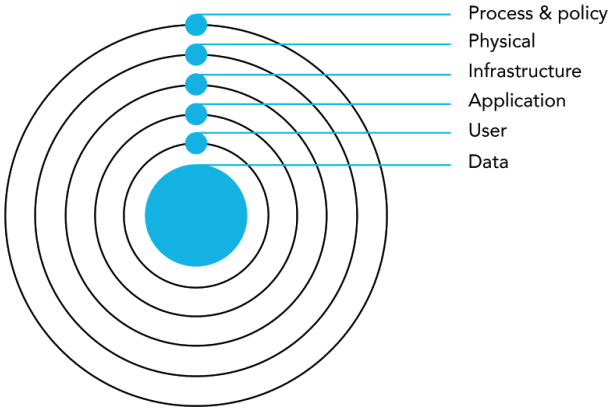
- Service Organization Control (SOC) 2 Report
- A licensee of the TRUSTe® Privacy Program
- HIPAA Compliance
- Abides by the EU Data Directive by entering into Model Clauses with applicable customers, partners, and suppliers
- Registered participant in the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks

Defense in Depth

As you'll see from any best-in-class SaaS provider, there is no single layer that protects customer data, but rather a well-architected solution that considers every layer from the physical security measures at the data center, all the way through the access privileges that determine what data an individual user can access. GoodData, as a best-in-class analytics provider, uses this approach to protect customer data.

"Defense in depth is the coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise. The strategy is based on the military principle that it is more difficult for an enemy to defeat a complex and multi-layered defense system than to penetrate a single barrier."

TechTarget.com



GoodData Confidential. 2017 GoodData Corporation. All rights reserved.

Process & Policy

The first layer of defense is having a well-defined and comprehensive set of security processes and policies to ensure the security of our customers' data and users. GoodData's ISMS employs a number of process and policy measures that instill security as a key priority at our most core layer…. our people.

SOC 2 Type II Audit

GoodData undergoes yearly examination by external auditors against the SOC 2 Security and Availability Trust Criteria.

TRUSTe Review

GoodData's Privacy Policy, platform, website, and support portal has been reviewed by TRUSTe for compliance with TRUSTe's program requirements and the TRUSTe Cloud Program Requirements including transparency and accountability.

Change Control

A formal change control process minimizes the risk associated with system changes. The process enables tracking of changes made to the systems and verifies that risks have been assessed, inter-dependencies are explored and necessary policies and procedures have been considered and applied before any change is authorized.

Training

GoodData employees authorized to access the GoodData platform undergo periodic training to focus employee attention to compliance with corporate security policies. For example, GoodData DevOps and Professional Services personnel who may handle sensitive customer data and information will regularly undergo security, auditing, access, and compliance training (e.g. for HIPAA)

Authorized Access

In addition to restricted personnel entering the production area, operational access is limited to only a restricted set of GoodData operations employees. Access is controlled via a physically separate network that is isolated from the GoodData corporate network that serves its general employee population ensuring that only personnel authorized to access the data center may do so. All GoodData personnel with physical or operational access to production environments are subject to training, deep background checks, and all activities are logged for auditability.

GoodData Confidential. 2017 GoodData Corporation. All rights reserved.

Physical

All GoodData data centers are certified to major InfoSec standards, including ISO 27001 and SOC 2 Type II. These data centers also feature N+1 redundant HVAC and UPS. The physical security adheres to the best practices in the industry and include:

- Keycard protocols, biometric scanning protocols, and around-the-clock interior and exterior surveillance
- Access limited to authorized datacenter personnel—no one can enter the production area without prior clearance and appropriate escort
- Every data center employee undergoes thorough background security checks

Infrastructure

Between the physical datacenter layer and the GoodData Enterprise Insights Platform application layer is the infrastructure that supports our solution. Throughout the infrastructure, security is implemented in a comprehensive and coordinated fashion to enhance the safety and security of customer data.

Firewalls

All network access to the virtual hosts is protected by a multi-layered firewall operating in a deny-all mode. Internet access is only permitted on explicitly opened ports for only a subset of specified virtual hosts. For an additional layer of security, all database servers reside behind an additional firewall.

Networking

GoodData platform servers are allocated to the respective security groups, characterized by specific security settings (TCP/IP level), supplemented by individual instance level stateful firewalls. Separate VLANs are used to split production, testing and development environments as well as to segregate end-user and administrative traffic.

GoodData employs a three-tier security model:

- Web servers at the frontline
- Application servers in the demilitarized zone
- Database servers behind an additional firewall

GoodData Confidential. 2017 GoodData Corporation. All rights reserved.

Systems Hardening

Just like any SaaS offering, the GoodData Enterprise Insights Platform utilizes many well coordinated technologies to deliver our service, yet there may be many capabilities that are not required. Consistent with industry best practices, GoodData DevOps closely inspects the entire solution to identify unnecessary services and remove and/or disable these capabilities to reduce vulnerabilities to security threats.

No Root Access

All customer access to the GoodData Enterprise Insights Platform is controlled through user interfaces (UI), APIs, and/or dedicated tools. Use of any of these methods of access require a username and password with privileges appropriate for the requested access.

Customers do not have root or administrative access to any portion of the Enterprise Insights Platform technology stack and access is permitted only via the Enterprise Insights Platform application layer (UI or API).

Shutdown All Unnecessary Ports

As previously mentioned in the Firewalls section, any ports on any server and/or virtual host not required for the operation of the GoodData Enterprise Insights Platform is disabled eliminating additional opportunities for external intrusion.

Security Patches

GoodData has rigorous policies and procedures in place to update all components of the GoodData Enterprise Insights platform, including operating systems, VM hypervisors, middleware, databases, etc. with their vendors' security patches. These security patch activities are subject to SOC2 auditing and are subject to rigorous standards.

Application

The GoodData application doesn't just provide the end users with the ability to access reports, dashboards, and data, but it also delivers the integration end-points to connect the Enterprise Insights Platform to data sources and integrate it with other software to provide a seamless experience for the end user. The GoodData application employs many security measures to enable the secure flow of data from when it is loaded into the Enterprise Insights Platform through the delivery to the workspaces for end-user consumption.

Encryption-in-Transit

All traffic into and out-of the GoodData Analytics Distribution Platform is encrypted using TLS/SSL protocol that leverages either SHA-2 or AES algorithms.

GoodData Confidential. 2017 GoodData Corporation. All rights reserved.

Encryption-at-Rest

Encryption-at-Rest is available in the Enterprise subscription to the GoodData Enterprise Insights Platform and in connection with the Compliance Package offering.

Application Access

Whether an end-user is accessing dashboards or reports in the Enterprise Insights Platform user interface or an administrator configuring an environment using the configuration tools, all access to the UI is encrypted via HTTPS/SSL.

Integration

Any integration with the GoodData application programmatic interface (API) leverages HTTPS/SSL encryption. The user security model is enforced at the API level providing that data retrieved with the API is still subject to user authentication and access privileges (see User below).

Data Marts

For a customer that subscribes to the Enterprise version of the GoodData Enterprise Insights Platform, data stored in the data mart databases supporting the workspace are encrypted while at rest, implemented with AES256 strong encryption. The encryption is performed at the whole disk level resulting in greater levels of security.

Shared Storage

As data flows through the GoodData Enterprise Insights Platform, data may temporarily be transferred to a shared storage service that is used to move data between virtual hosts. Any data transferred to the shared storage service is encrypted in-transit (see above) and is encrypted-at-rest using a hardware encryption appliance providing AES256 strong encryption.

When the data has reached its destination, it is removed from the shared storage service, but at no time is the data unencrypted.

Backup Storage

To maintain a robust disaster recovery strategy, backups are retained at a separate GoodData data center at a geographically different location within the same region as the primary data center, with the same level of physical and infrastructure security described above, to maintain a robust disaster recovery strategy. All backups are encrypted-in-transit to the separate data center and are encrypted-at-rest while stored at that location.

GoodData Confidential. 2017 GoodData Corporation. All rights reserved.

Application Access

Customer data may only be accessed through the application layer. Whether this access is through the user interfaces or through the publicly available API, it enforces user access controls to regulate access to the customer data only to authorized users and personnel. As such, GoodData does not provide direct access to any database. This approach prevents unauthorized services or systems from accidentally or maliciously retrieving or modifying customer data.

User

User security is enforced via a variety of security measures allowing only authorized users to view a strictly defined set of objects and data, enabling the user to have access to the analytics they need to perform their job.

Authentication

GoodData's architecture relies on a centralized authentication and authorization security framework to control access to services. The security framework enables the enforcement of security policy by requiring password strength, algorithms to set minimum password length and complexity, and CAPTCHA filters that use human readable images to reduce the risk of automated attacks against customer data. Customers may also choose to implement Single-Sign-On (SSO) with their own access policies (e.g. whitelisting, multi factor, etc.) to integrate user authentication with their own policy store (e.g. Active Directory or other LDAP provider).

Role Based Access Control (RBAC)

The GoodData Enterprise Insights Platform supports enterprise and ISVs to define user roles that control which objects and capabilities within the Enterprise Insights Platform a user will have access to. For example, if a customer has implemented a Loan Insights solution, an Account Manager may be granted a role that allows access to a Client Health dashboard while a Regional Sales VP may be granted a role that allows access to both the Client Health dashboard and a Loan Pipeline Dashboard.

IP Whitelisting

IP Whitelisting is an additional security measure. This feature should be used to limit and control access based on a list of defined IP addresses or address ranges from which users can access your GoodData domains. IP Whitelisting can be set on a domain or user level. We recommend you to configure IP Whitelisting for HIPAA compliant solutions in accordance with industry best practices.

GoodData Confidential. 2017 GoodData Corporation. All rights reserved.

Some scenarios under which customers might benefit from IP Whitelisting include:

- Ensuring Administrative access is restricted only to a trusted company network
- Enforcing change control process to all changes to ETLs by allowing deployment of ETLs only to a trusted deployment system
- Implementing any custom policy that prevents end users accessing the data from non-trusted networks

User Session Expiration

User session expiration (or user session timeout) allows you to specify a period of inactivity after which user sessions are terminated and users are automatically logged out of the GoodData platform. In accordance with industry best practices, we recommend to configure user session expiration for HIPAA compliance or other security sensitive solutions.

Explicit User Access

Users added to the GoodData Enterprise Insights Platform are not given broad access to the network, but to an explicit workspace that is assigned to a “consumer” site (see diagram below), facilitating access for users to only have access to the workspaces appropriate for them.

Data

Data security is that final layer of security that limits access to users on the GoodData Enterprise Insights Platform based on permissions that each user has. GoodData employs several redundant layers of data security for the safety of our customer’s data.

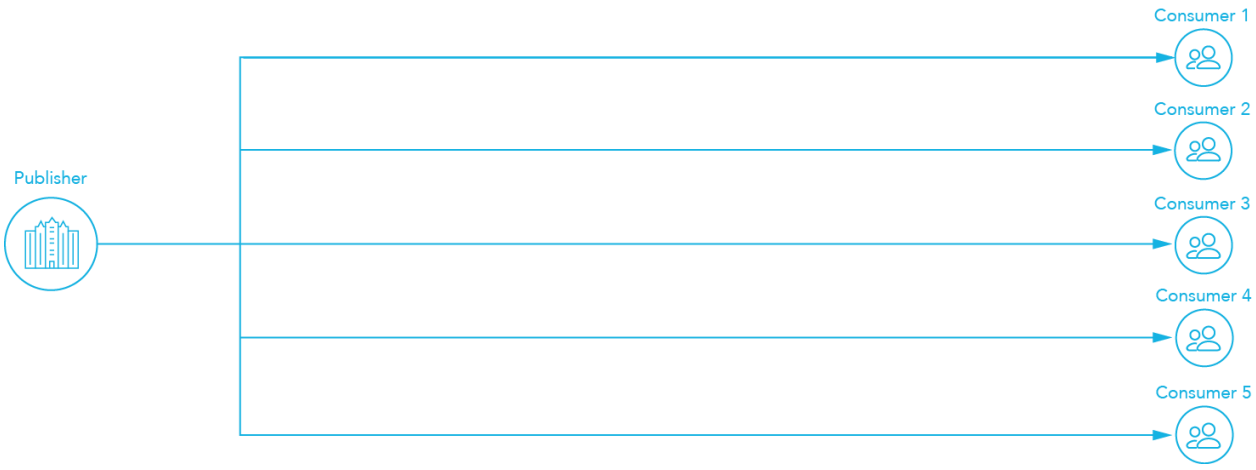
Data Based Access Control (DBAC)

The GoodData Enterprise Insights Platform supports enterprise and ISVs restricting query results based on a user's pre-defined permissions. For example, a customer may implement Data Based Access Controls on a Sales Insights solution for individual sales reps and sales managers. On a Quarterly Sales recommendations view, sales managers’ queries will be unrestricted and they can assess quarterly sales across their business, but the same dashboard for individual sales reps will only query data rows specific to their personal sales results.

Segmented/Isolated Data Mart

The GoodData Enterprise Insights Platform, as the name suggests, is intended to securely deliver insights from a Publisher to one or more enterprise sites, each site having one or more users.

GoodData Confidential. 2017 GoodData Corporation. All rights reserved.



To organize each site and its users so that each has access to only data intended for that subset, the data is distributed to a dedicated and isolated data mart to support the workspace for that consumer site. This physical security measure is in addition to the logical RBAC and DBAC security measures.

Regional Deployments

Data sovereignty is a complex issue that ranges from the technical to the regulatory and sometimes even the political arena. Understanding the complexities of this issue, GoodData operates data centers in the United States to serve the US and most other North American companies and also in the United Kingdom to support customers in the European Union.

Additional Compliance Safeguards

In addition to the many layers of security measures previously described in this document, GoodData implements a number of additional security and compliance measures to support the needs of our customers.

Quarterly Audit Health Checks

In coordination with our external SOC 2 auditors, quarterly control tests are performed.

Periodic Vulnerability Scans

GoodData has third-party bi-annual vulnerability and penetration testing which covers OWASP Top 10 Application Security Flaws.

Periodic Penetration Tests

Quarterly OWASP compliant penetration testing

GoodData Confidential. 2017 GoodData Corporation. All rights reserved.

HIPAA compliant environment option

GoodData leverages the existing SOC 2 security controls and adds additional Technical, Organizational, and Legal measures to create a HIPAA compliant environment. This option manages analytics involving PHI in accordance with the HIPAA Security and Privacy Rule.

Conclusion

Here at GoodData, we pride ourselves on the vigilance we employ to protect our customers' data assets and we continually stress that a mature security organization requires coordinated dedication across technology, policy, procedures, and people. This dedication is underscored by the risk-based approach laid out in this document to demonstrate strength at every layer of security, minimizing any potential vulnerability or weakness.

We want our customers to know their data is sufficiently protected by this approach and welcome the opportunity to discuss these practices and approaches further.

GoodData Corporation reserves the right to amend, modify, delete or remove this Security White Paper, at its sole and exclusive discretion, at any time. All information contained herein is provided "as-is", and GoodData disclaims all liability for itself and its affiliates, licensors and suppliers, with respect to the descriptions, statements and contents of this Security White Paper.