CASE STUDY

HIPAA Compliance at GoodData a US-Based Smart Business Application Provider

Safeguard for Privileged Sessions

"SAFEGUARD FOR PRIVILEGED SESSIONS GIVES ME THE ASSURANCE OF A RELIABLE AUDIT TRAIL PERTAINING TO SENSITIVE DATA THAT IS ACCEPTED BY ALL PARTIES..."

– Tomáš Honzák, Director of Security & Compliance, GoodData.

GoodData

GoodData accelerates the digital transformation of enterprises by turning their data into a profit center. It does this by enabling them to quickly create and distribute data products and Smart Business Applications to their B2B networks, including their clients, business units, suppliers, or partners.

Their clients include enterprises like information services firm Penton that need to deliver revenue-generating data products to their clients and software companies like Zendesk that market their own Smart Business Applications using GoodData.

GoodData is headquartered in San Francisco and is backed by venture capital firms Andreessen Horowitz, General Catalyst Partners, Intel Capital, TOTVS

Learn more

- Safeguard homepage
- Request callback

The Challenge

To support the regulatory needs of US customers and enable them to build data products using the GoodData platform, GoodData needed to comply with HIPAA (Health Insurance Portability and Accountability Act). As part of the HIPAA compliance, GoodData needed a solution that could provide complete audit trails of all access to sensitive data to be able to prove to customers, end users and regulators that they haven't violated the privacy policies.

During their customer project implementations, GoodData's solution engineers have to do a lot of data discovery activities to build the right data models, BI reports and visualizations for their customers. Their engineers directly access client data warehouses containing sensitive production data and they need to not just log the actual SQL queries, but to see them in context. In addition, they continuously want to prove that they don't offload data from the production environment. In other words, GoodData needed to provide complete and undisputable evidence of actions performed in their heterogeneous desktop environment without compromising usability.

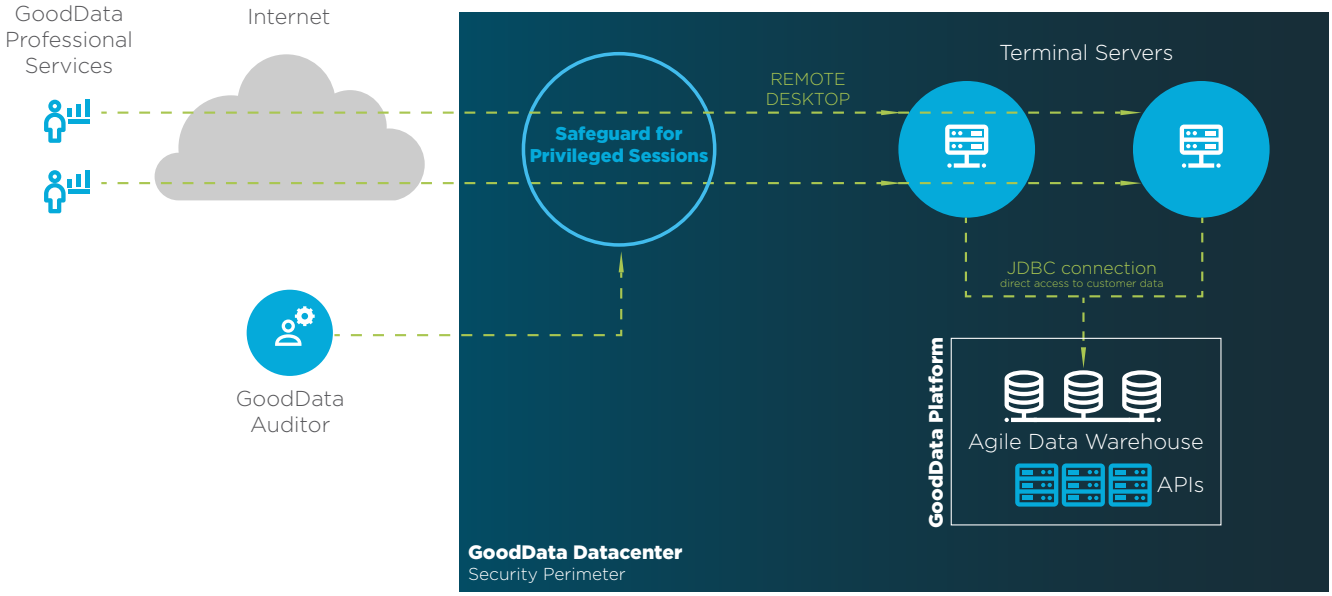
The Solution

During selection process GoodData considered building its own solution and contacted several companies that offered fully audited terminal server as a service (SaaS). Finally, they chose One Identity's privileged session monitoring solution, Safeguard for Privileged Sessions.

"Our security architect recommended Safeguard for Privileged Sessions for us. We chose Safeguard for Privileged Sessions based on its lower cost, its rapid deployment and the possibility to host it in our datacenter. We also ascertained that this solution is used by major companies in regulated industries such as banking to deliver ISO 27001 and PCI-DSS compliance." – adds Tomáš Honzák, Director of Security & Compliance at GoodData.

GoodData has deployed Safeguard for Privileged Sessions into their datacenter hosted at a Rackspace facility in Chicago. As an audit node Safeguard for Privileged Sessions is connected to two virtual Linux-based terminal servers. During their implementation projects, these servers are used to access sensitive customer data in the data warehouse managed by GoodData's solution- and support engineers on behalf of the clients. The terminal servers as well as the production nodes run on Scientific Linux.

The full implementation took 6 weeks. Today Safeguard for Privileged Sessions system is in full operation, monitoring the work of 50 GoodData employees: it records and indexes all sessions initiated by the Services team members on the terminal servers and provides tamper proof audit trails.



"The heavily controlled IT environment and the presence of recording make our employees more focused and helps prevent mistakes."

says Honzá

Benefits

For GoodData, the primary benefit of Safeguard for Privileged Sessions is the assurance of compliance. Every session - where access to raw data containing sensitive personal information (ePHI) is required - is recorded into secure audit trails. GoodData also uses Safeguard for Privileged Sessions to conduct quarterly audits of user sessions. Usually, they audit a percentage of all sessions and have not found any case of non-compliance.

"As a HIPAA security and privacy officer, Safeguard for Privileged Sessions gives me the assurance that in case of any dispute related to the access to sensitive health data by GoodData employees, I have a complete and reliable audit trail that is accepted by all involved parties, including the regulatory bodies, as well." – concludes Tomáš Honzák.

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats. Learn more at OneIdentity.com