About Kanda

Kanda Software is a fully integrated service provider specializing in assisting the delivery of custom software solutions to established companies like Nuance and Lionbridge and exciting startups like Intervention Insights, RallyPoint, and Worthworm. Since 1993 Kanda successfully delivered over a hundred solutions to clients ranging from small dynamic companies to Fortune 500. Our exceptional team of senior developers has years of experience working across multiple platforms, servers and languages allowing Kanda to quickly deliver reliable and scalable solutions that are integrated with company's infrastructure.

CLIENT

Worthworm, web-based pre-money valuation (PMV) system for early stage ventures seeking investment and angel investors

CLIENT NEED

Security and encryption of sensitive user information including business ideas, company specifics, personal data and the network.

SOLUTION

Implementation of the Regulatory Compliant Cloud Computing (RC3) web-application architecture using the StrongAuth KeyApplianceTM to achieve state-of-the-art security of sensitive data in a public cloud

CASE STUDY

kanda SOFTWARE

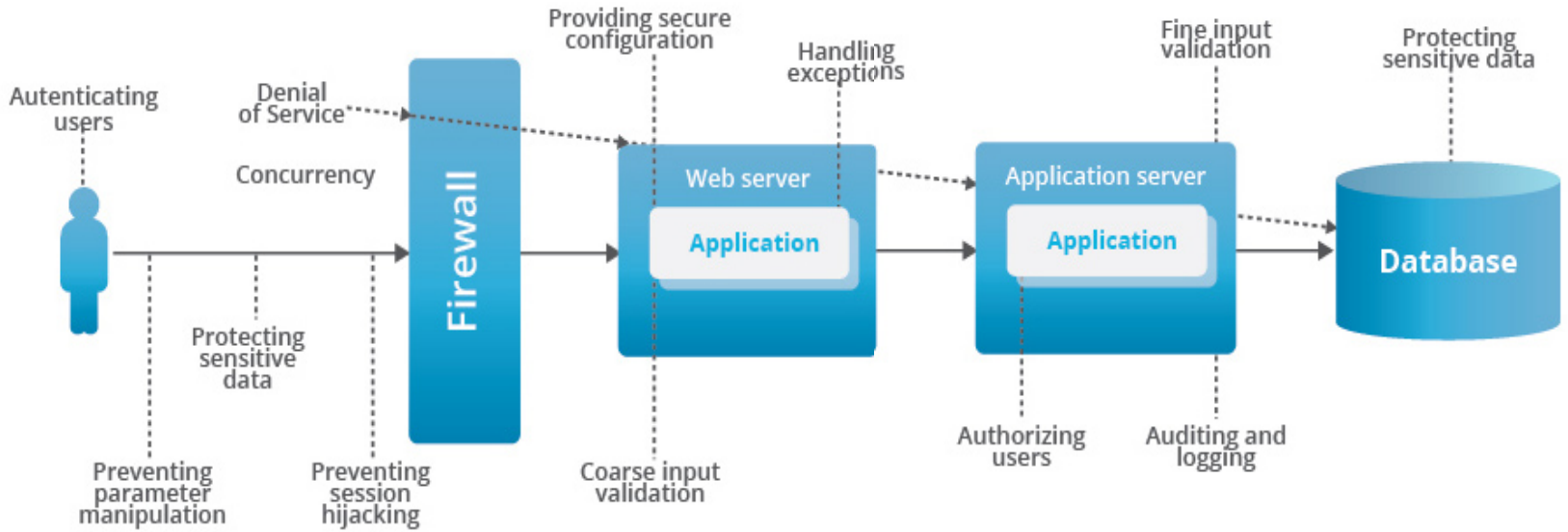
CHALLENGE

Worthworm's questionnaire is the basis for the valuation calculation. Clients have to answer questions about product differentiation, competitive advantage, current sales figures, management team, prior funding and risk factors.

Thus, protection and security of proprietary business ideas, company data and personal information is of extreme importance to Worthworm, and can potentially define the success of the application on the market.

Sensitive information provided by the customer required sophisticated security measures and data encryption comparable to those provided by the financial institutions.

Kanda Software faced the challenge of finding a cost-effective, scalable solution for data encryption and key-management.

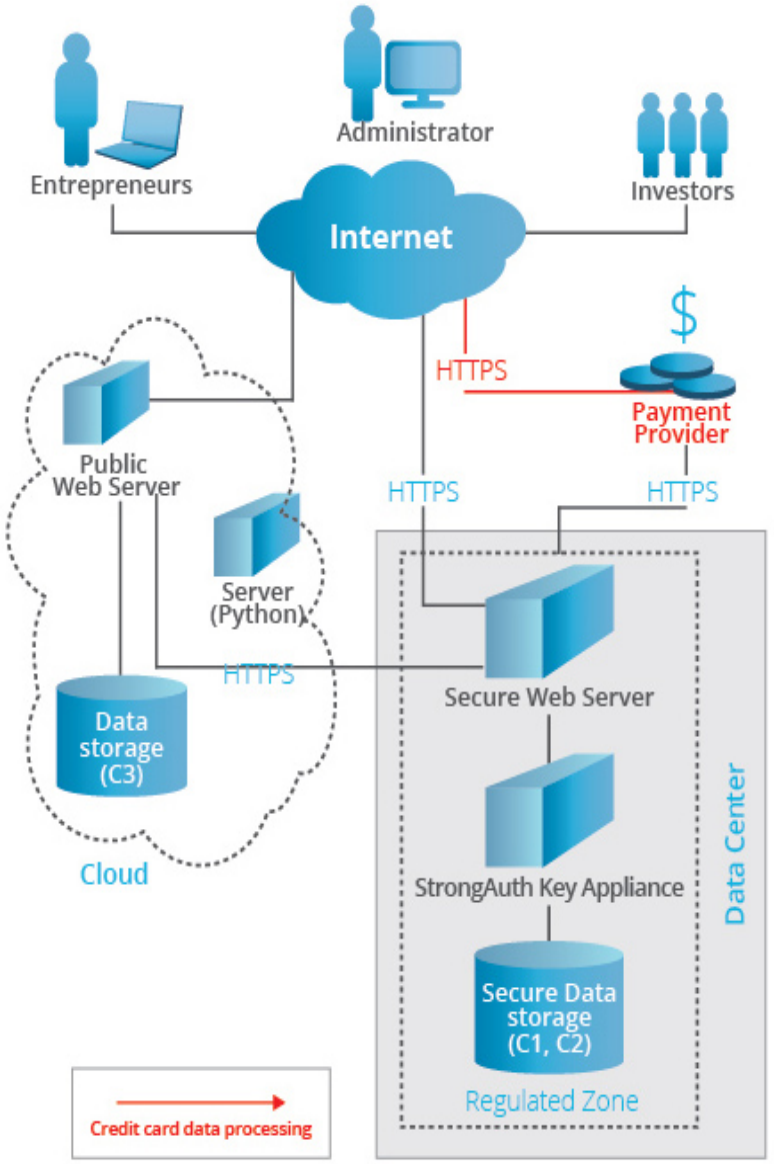


SOLUTION

The StrongAuth KeyAppliance

is an integrated hardware and software solution – with a built-in cryptographic hardware module - designed to protect sensitive data in ompliance to data-security regulations such as PCI-DSS, 201 CMR 17.00, HIPAA/HITECH, FISMA, the EU Directive, etc.

After evaluating all available solutions on the market, the Worthworm and Kanda teams chosen StrongAuth's KeyAppliance to provide encryption, tokenization and key-management services to the application – which would be implemented using the RC3 web-application architecture (documented at http://ibm.co/rc3dw and http://bit.ly/rc3infoq) to provide data-security in the cloud.



06

The RC3 web-application architecture allowed Kanda to protect sensitive data secure, regulated zones, while leveraging public clouds for its business benefits.

Following RC3 Worthworm data was classified into 3 categories. The data-modeling section of RC3 simplified communication between business units and IT because there was no confusion about the security/regulatory requirements for any given data-element – this effectively provided one of the most secure data-architectures from the ground-up.

CLASS	CLASSIFICATION	DESCRIPTION
1	Sensitive and regulated data	Data whose disclosure to the public would result in fines, potential law suits, and loss of goodwill to the breached entity.
2	Sensitive but non-regulated data	Worthworm data examples: Credit Card data, payment and purchase information Data which is not regulated, but whose disclosure to the public would be detrimental to a company and/or result in some loss of goodwill to the breached entity. Worthworm data examples: User information, including personal details and e-mails, business information that consisted of venture and model names, questionnaire responses and any other business sensitive data.
3	Non-sensitive data	All other data.

07

Solution:

Class 1 and Class 2 data is encrypted, tokenized, processed and stored in regulated zones, within a secure network perimeter - outside the public cloud where the Worthworm application is hosted - in complian with applicable data-security regulations. Since Class 3 data is declared to be non-sensitive, it is processed and stored – unencrypted – in the public cloud.

The StrongAuth KeyAppliance is used for encryption, decryption, search and deletion of sensitive data stored in the system. Key-management automation capability in the appliance allowed Worthworm to eliminate the burden of dealing with cryptographic primitives in the application, while drastically reducing the number of requests to the appliance's web-services while in use.

Data tokens generated by KeyAppliance can be safely stored in the public cloud. The token has no cryptographic relation to encrypted data other than being a unique identifier. Since the RC3 model prohibits the application in the cloud from calling the regulated zone for any reason – all communications are only one way: the regulated zone calls the application in the cloud if it needs anything from the cloud - lin the event of a breach in the public cloud, attackers will be unable to decode or connect this data to user information either in the cloud or the regulated zone.

TheSensitive data is encrypted before it is stored in the database, while its decryption happens when data needs to be sent to the authorized user, through the Worthworm interface in the regulated zone.

StrongAuth KeyAppliance was integrated using Spring Web Services that ensured additional flexibility.

08

SOLUTION BENEFITS

Implementing RC3 мwith the StrongAuth KeyAppliance allowed Kanda Software to leverage cloud technologies and achieve lower implementation costs, faster time to market and scalability along with compliance to data security regulations.

In Addition, Keyappliance Provided such Benefits as:

- Key management automation including key-generation, escrow, recovery and access-control;
- Data security compliance while leveraging public clouds for processing sensitive client information and transaction data.
- Easy scalability
- NIST-approved encryption algorithms
- Integrated cryptographic hardware module with a true random number generator
- Secure and robust messaging services for data and key replication.

About StroungAuth

StrongAuth, Inc. is a Silicon Valley-based company, focused on enterprise key-management solutions since 2001. It has been building key-management infrastructures for large and small companies – and government entities - on six continents where its products are used to protect sensitive data in dozens of mission-critical environments.