Kenna Platform Security

A technical overview of the comprehensive security measures Kenna uses to protect your data

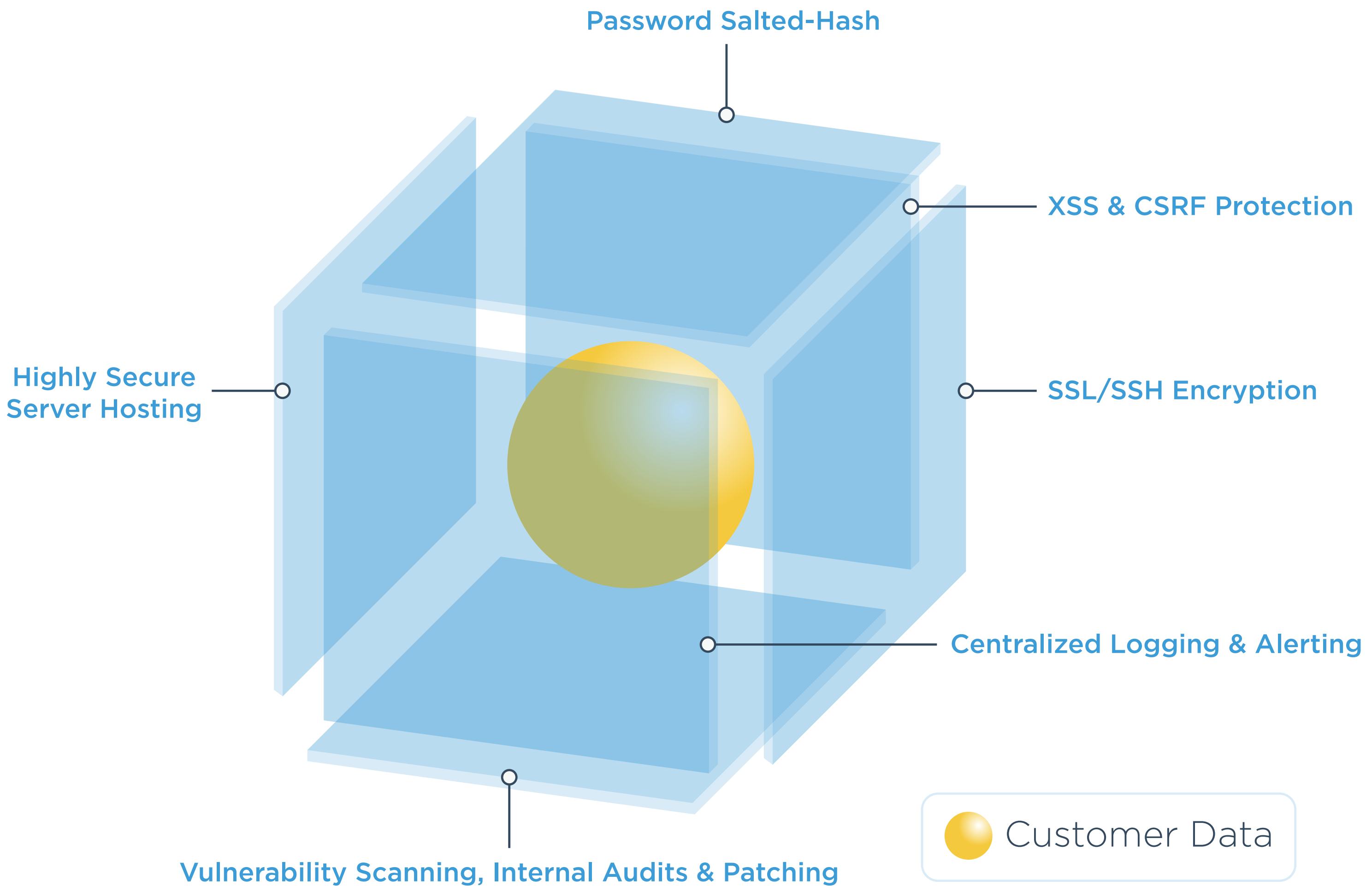
V3.0, MAY 2017

Overview

Thank you for your interest in Kenna Security. In this document, you'll find a technical overview of the comprehensive security measures Kenna uses to protect your data while using the platform. These processes are important to achieving our goal of safeguarding user data while maintaining a positive and effective user experience.

At Kenna we take the security and privacy of your data very seriously. We make every effort to help ensure that your data stays protected whenever you use our platform. Our software and systems architecture was built with maximum security in mind.

Multiple Layers of Protection

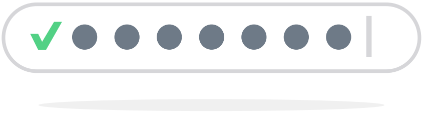

Password Salted-Hash
XSS & CSRF Protection
Highly Secure Server Hosting
SSL/SSH Encryption
Centralized Logging & Alerting
Vulnerability Scanning, Internal Audits & Patching
Customer Data

Key Security Feature List

The summarized list shown below are some of the key ways that our Kenna service has been designed and developed to better protect your data:

- AES-256 (data at rest) and SSL/TLS (data in transit) to encrypt and protect stored information.
- Network traffic encrypted using SSL/SSH.
- Password data stored in a one-way salted hash.
- FIPS-approved encryption algorithms and implementations.
- Servers hosted in a highly secure data center facility with multiple third-party certifications.
- Annual internal audits using SSAE16 and regularly scheduled penetration testing.
- Regularly scheduled vulnerability scanning using proprietary, commercial and open-sourced tools. Full vulnerability management and remediation using Kenna.
- Security patches deployed within 24 hours, and minor patches within 48 hours of public release and verification testing.
- Built-in platform protection and implementation controls to reduce risk from common web-based threats, such as cross-site scripting attacks (XSS) and cross-site request forgery (CSRF).
- Centralized logging and alerting.
- Strong authentication mechanisms for remote access through two-factor authentication.
- Automatic session expiration after a certain period of inactivity.
- Role-Based Access Control.

Security Architecture Design



User Sign Up

During the sign-up process, the user generates their own password. User passwords are stored in a one-way salted hash.

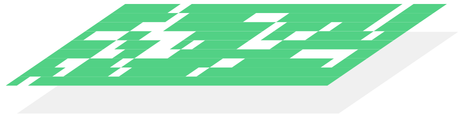
By design, it is impossible for any Kenna employee to access user passwords.

User Sign In

Users are authenticated when they sign in to Kenna using their password. The password is used to send an authentication hash via SSL to the Kenna server for authentication. Sessions expire after a 15-minute session timeout.

The application supports single sign-on using oAuth Login standards.

Two-factor authentication can also be setup on the client-level by sending a one-time password to supporting applications.



Data in Transit

All application traffic occurs over SSL/TLS, and all network traffic is encrypted via SSL/SSH. All communication between the user's device and Kenna is further encrypted at all times using SSL/TLS as an automated layer of data protection.

HTTPS Transport Security

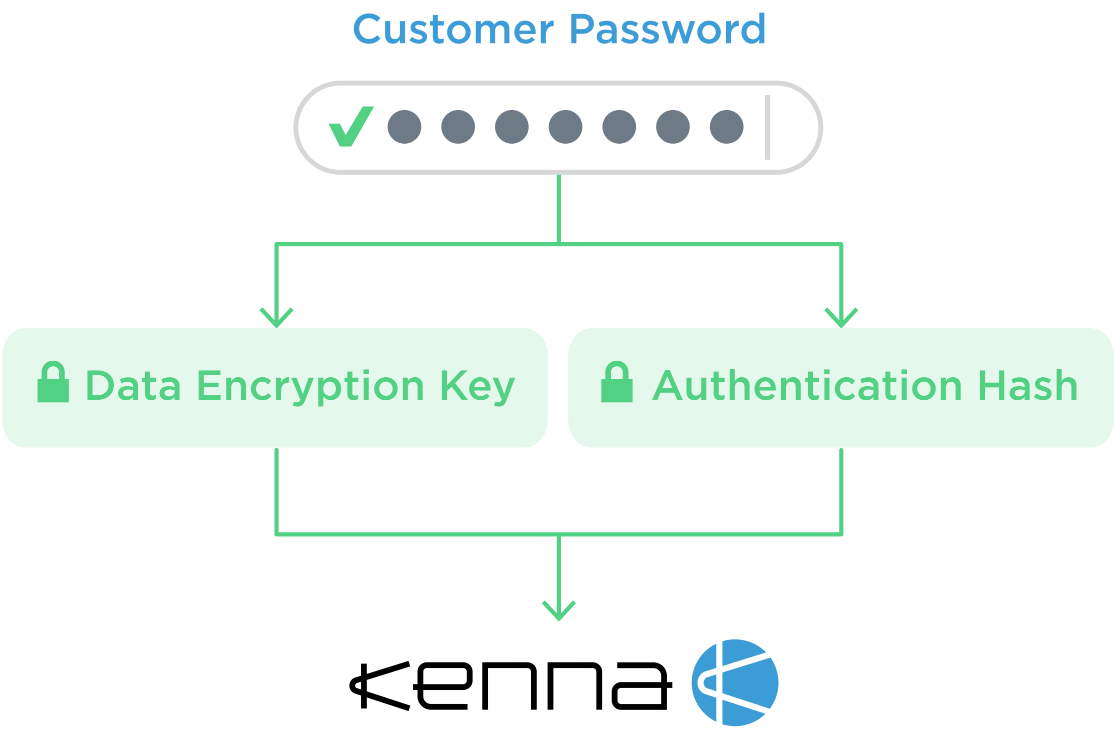
The Kenna platform runs exclusively over HTTPS, such that if someone manually edited the URL to start with http://, they would be redirected to an https:// URL. This prevents SSL-stripping attacks in the event that a user connects to Kenna from an untrusted network.

Cookie Attributes

All authentication cookies use the "secure" flag as well as the http-only flag. This ensures that cookies are only sent over secured connections and that the cookies cannot be accessed over non-HTTP(S) methods.

Kenna Security – Architecture & Benefits

The rapid growth of cloud-based services, coupled with the discovery of significant security weaknesses, has demanded heightened awareness and the use of high-level security measures and encryption protocols. We have carefully designed every aspect of Kenna to maximize the security of our users. In this section, we'll highlight some of the benefits of this approach.



- All data is encrypted using a salted hash before being transferred to Kenna. Both the data encryption key and the authentication hash are derived on the user's computer from the user's password. This architecture is much more resilient to attack.

- **Kenna & Bcrypt**
  Even in the unlikely event that an attack were to occur, the attacker would face the difficult task of a brute force attack attempt on each user's AES user data files separately. And as Kenna employs the bcrypt algorithm, with more than 10,000 iterations, the encryption keys used to protect users' data have high complexity. This makes an attack impractical.

Operational Security

We apply high security standards not only to our product software, but also to our infrastructure and operational model. This ensures that we are protecting the confidentiality and integrity of our customers and our data.

Kenna Corporate Security Policy

Kenna has clearly defined corporate security requirements with which every employee must comply, and technical standards for secure software development.

Kenna has a process set in place to ensure that access to data is granted solely on a "need-to-know" basis. There is also an active process to revoke access by employees, contractors, or others that have left our company and no longer require access (this includes physical access, logical access, and access to any SaaS or external applications that our company uses).

Third parties (such as outsourcing partners, vendors and subcontractors) do not have access to unencrypted company data.

We have a documented incident response process, with personnel available on a 24x7 basis to respond to information protection incidents. We will notify company of an information protection incident affecting their data within twenty-four hours of becoming aware of the incident. If a security incident were to occur, we'd be willing to share audit logs with the affected company for review.

We provide adequate security and privacy training internally. We provide secure software development training to our engineers, teaching them about common threats and countermeasures related to the software they are writing. Within the code itself our development team leverages as many of the security functions that are made available by the Rails framework. All of our developers utilize the OWASP secure coding guide, cheat sheets and relevant technology specific guidelines such as the OWASP Rails Security Guide.

Kenna regularly conducts vulnerability scanning using proprietary, commercial and open-source tools, and using our own platform for vulnerability management and remediation.

PCI Compliant Data Center

Although the Kenna platform does not store credit card information, our data center complies with the Payment Card Industry Data Security Standard (PCI-DSS).

Server Hosting

All Kenna servers, including all of our production computing equipment that handles and processes company information, are located in a physically secure data-center.

This data center has received the following certifications:

- SSAE 16 Type II certification detailing physical and environmental controls (available upon request).

- Control program certified based on ISO/IEC 27001:2005 standard for Information Security Management Systems.

- Validated as a Level 1 Service Provider under PCI-DSS.

- Certified for HIPAA compliance.

Kenna has the ability to delete data on demand in response to a request to delete data. Conversely, we have established anti-recovery techniques to help prevent malicious recovery of deleted-data.

Third Party Security Testing

Kenna conducts annual security audits that use SSAE16 by an independent auditor, as well as regularly scheduled self-penetration testing. We also perform software code reviews before every release using expert manual techniques and automated code analysis tools.

This method specifically addresses security issues in the code and ensures high code quality and regression testing. These code reviews are performed by both peers within our organization and by an independent company.

Network Architecture - Application Database Server Isolation

The design of our network is based on three-tiered Model View Controller architecture that has been compartmentalized and firewalled, and we carefully segment each of these technology layers via network and access controls. Kenna has implemented documented security configuration baselines that harden and secure our systems.

Secure Admin Access

Kenna implements levels of access privileges or roles called Role-Based Access Control, so that users can be assigned only the permissions they need to perform their respective functions. By default, no access to front and back-end services is granted to any employee and access is granted based only on operational need and at the Least Privilege necessary to perform the duty. All access to the Kenna infrastructure requires VPN access with two-factor authentication to enhance security and accountability.

Log Management

A centralized log management and monitoring solution is in place to detect, prevent and alert on unauthorized access to Kenna systems. This also allows our team to reconstruct the actions that any given user took within the application.

Server Hardening

Web servers and databases have been hardened and secured using documented security configuration baselines from NIST's Guide to General Server Security.

Change Management

Our code is tested via static analysis and dynamic scanning prior to being deployed to our production environment. All code is deployed using Reduced Attack Surface deployment, and we use generic exception handling to help prevent information disclosure attacks. Source code is also kept in a code repository with versioning controls.

Patch Management

All servers and applications are kept up to date with the latest tested patches in the production environment through daily forced patches. Specifically, security patches are deployed within 24 hours, and minor patches within 48 hours of public release and verification testing. We also have an emergency process in place to install patches outside the regular patching schedule for security updates that address high-risk vulnerabilities. All configuration is managed centrally via Chef.

Web Application Platform Protections

Kenna protects all state-changing actions across cross-site request forgery (CSRF) using built-in platform protection and implementation controls to prevent cross-site scripting attacks (XSS) as well as additional code side filtering. These methods are also used to protect cross-site scripting as well as SQL Injection and any significant security vulnerabilities from web traffic.

Firewalls restrict network access to only the necessary ports, and are configured based on the principle of least privilege according to NIST's Guide to General Server Security.

Ensuring User Data is Safe and Secure

While designing and developing the platform, we have made it our mission to deliver a product that provides users with an effective vulnerability threat prioritization platform that also delivers strong data security. As this document explains, Kenna performs many complex security functions in the background to protect confidential data, but by design the user need not be aware of these processes. Regardless of technical knowledge, all user types can benefit from the high level of security that Kenna offers in their platform.

At Kenna, we are both a user as well as the developers of our platform. Just as our users use a variety of tools, processes and technologies to help secure and control their environment, we're doing much of the same here. Of course at the center of our vulnerability intelligence is our own instance of Kenna, which is a reliable part of our daily workflow. Not only do we use Kenna to manage and remediate our vulnerabilities internally, we also offer our clients read-only access to our account, upon request. We understand the trust our customers place in our services and are committed to transparency in our controls.

kenna