CLARIZEN
SECURITY
WHITE PAPER

2016

Clarizen Security White Paper

Standards and Practices

clarizen

UNITED STATES
1.866.502.9813

UNITED KINGDOM
+44 (0)20 3411 4044

ISRAEL
+972.9.794.4300

FRANCE
+33 (0) 9 50 11 55 22

Table of Contents

clarizen

Introduction

Enterprises increasingly rely upon third-party software and services to handle business-critical processes and operations. Whether on-premises or in the cloud, these solutions must provide a level of security that protects critical company data and minimizes risk.

Clarizen's security standards and practices are backed by a multi-layered approach that incorporates best practices for preventing security breaches, as well as ensuring data integrity, availability and confidentiality

The Clarizen security model encompasses the following components:

- Application Security
- Network and Infrastructure Security
- Physical and Environmental Security
- Organizational Security
- Cloud Operational Security
- Service Compliance and Certification

Application Security

Password Policy

STRONG PASSWORD POLICY

Clarizen's strong password policy requirements govern the creation, protection and frequency of password changes. These requirements serve as a baseline or minimum recommended password requirement; more stringent password policies can be established as needed. Passwords are transferred via a hypertext transfer protocol secured (HTTPS) connection, a protocol that encrypts communication between the web server and browser and secures the identification of the web server.

Every Clarizen user must have a unique account ID in order to access the platform. This account ID is used to track user activity, as well as assign and enforce the correct permissions level.

ACCOUNT LOCKOUT POLICY

To protect against dictionary-based, brute-force attacks, Clarizen uses an account lock-out policy, where user accounts are locked after three failed login attempts.

See the Encryption section (page 5) for information on password encryption.

Application Security (cont.)

Logical Security

MULTI-TENANCY ACCESS CONTROL

Clarizen uses a proprietary data-access layer that requires a valid organization identifier in order to access the database. The identifier resides in a secured session variable and is passed between all layers to the data access layer, thereby restricting user access within each session.

Given the importance of access control mechanisms, Clarizen continuously tests its security system and processes, and constantly monitors them to ensure they are functioning properly.

Penetration Testing

EXTERNAL SECURITY AUDITS

Clarizen regularly engages external security testers and professional application auditors as part of its software development lifecycle. These experts perform penetration tests using the open web application security project (OWASP) methodology for multiple attack scenarios, as well as several proprietary attack scenarios developed by Clarizen.

PENETRATION TEST SUMMARY REPORT

Clarizen shares penetration test report executive summaries with its customers. These summaries include test findings, along with all actions taken to remediate any issues that may have been found.

AUTOMATED SECURITY SCANS

Clarizen's internal security team performs regular, automated security scans on the production network to validate that both the network and infrastructure are free of vulnerabilities.

Application Content Filtering

WEB TRAFFIC INSPECTION AND SANITATION

To prevent all forms of cross-site scripting (XSS), SQL injection and other such activities, Clarizen has fully integrated a proprietary sanitation engine into the platform, which inspects all traffic prior to processing.

Application Security (cont.)

IP Restriction

RESTRICTING LOGIN IP ADDRESS

Clarizen users can restrict access to their projects and data by monitoring and filtering account access by IP address. Only the IP addresses on the customizable list will be granted account access—all other IP addresses are automatically blocked.

Encryption

DATA AT REST ENCRYPTION

Clarizen deploys industry-leading encryption algorithms to secure customer data, files and media that reside in Clarizen storage systems. All data is encrypted with advanced encryption standard (AES) with a 256-bits block size – the same level of data security required by the Sarbanes-Oxley Act, the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act (HIPAA).

KEY MANAGEMENT POLICY

Clarizen pays special attention to the key lifecycle, as well as the allocation of roles within the key management infrastructure. Clarizen's key management policy employs a set of rules designed to secure the key lifecycle, using a combination of security mechanisms that include strong password, routine revocation of keying, key backup and recovery.

PASSWORD: HASH, SALT AND STORE

Clarizen takes a multi-level approach to storing all sign-in credentials. Protection begins with "hashing" passwords, a common approach for taking passwords of varied lengths and turning them into cryptic, fixed-length passwords for storage. Clarizen also "salts" customer passwords, or adds extra data that is unique to every user to employ an additional level of password protection.

DATA IN TRANSIT ENCRYPTION

Upon sending any data between the user browser and the Clarizen cloud, Clarizen establishes an HTTPS connection, which encrypts all communication between the web server and client browser. It also secures the identification of the web server via an industry-leading certificate authority.

Application Security (cont.)

Cloud Authentication

FORM AUTHENTICATION

Clarizen authenticates all users with a unique ID and password. Prior to submitting the authentication form, Clarizen creates a secured communication tunnel so that user credentials are submitted over encrypted sessions. The authentication process requires an HTTPS/443 port in order to communicate with the Clarizen cloud. Users do not need to download or install software to access their projects or data.

SAML AUTHENTICATION

As an additional security mechanism, Clarizen supports security assertion markup language (SAML) authentication, which is a protocol used to securely exchange authentication and authorization data between customer systems and Clarizen.

SAML gives Clarizen customers the ability to control password policy, user management and authentication. During the login process, a SAML token is transmitted to the Clarizen platform over a secured tunnel and a session is created. To enhance security, the tokens do not contain user passwords.

SINGLE SIGN-ON (SSO) AND TWO-FACTOR AUTHENTICATION

The Clarizen platform integrates with OneLogin to provide users with a single sign-on (SSO) solution. When using the SSO integration, organizations can require their employees to use a strong authentication factor, in addition to their password, when they sign in. Two-factor authentication is a more secure method of verifying or validating identity. OneLogin offers a range of strong authentication options and supports pre-integrated solutions from Duo Security, RSA, Symantec, VASCO and Yubico.

APPLICATION SESSION TIME-OUT

Clarizen helps to secure user accounts with an application session time-out. Once an inactive or idle sessions session is timed out, users must re-authenticate to access their account. In the event of a session time-out, no data or work is lost—since Clarizen automatically saves all data every few seconds.

Infrastructure Security

Network Architecture

FIREWALLS

Clarizen's ICSA Labs-certified firewall provides next-generation protection, including deep-packet inspections while maintaining high bandwidth and low latency.

Clarizen application-layer firewalls protect against the OWASP top- ten attacks. The firewalls are fully integrated with Clarizen application scanners and can provide virtual patching capabilities. Assessment results are imported from the security scanner and custom policies can be created in real time to remediate any vulnerabilities.

A reputation engine also detects and filters against known malicious IP addresses, anonymizing services, phishing URLs and IP geo-location data. This serves as an additional defense against automated attacks.

ANTI-VIRUS PROTECTION

Today's viruses and malware are persistent, difficult to detect and require a multi-layered approach to combat. The Clarizen network topology gives Clarizen security teams visibility into system health via multiple points across the network—along with the ability to inspect suspicious behavior, botnet connections and viruses.

MULTI ENGINE ARCHITECTURE

Clarizen anti-virus engines protect against viruses, Trojans, malware and other malicious code. Additionally, all scan engines are connected to a management server. The management server also validates that all updates are deployed and functioning properly, and looks for anomalies that may indicate an update has failed. If an update fails, the management server alerts the Clarizen security team in real time.

ACCESS CONTROL

A centralized group and role management system is used to define and control Clarizen engineers' access to data centers.

The following practices are followed to prevent unauthorized access to Clarizen data centers:

- Maintain strict access control approval process
- Block administrator (root user) logins
- Grant least privilege access (access given on an as-needed basis)
- Record successful and failed login audit logs
- Conduct content filtering, intrusion prevention and application validation

Infrastructure Security (cont.)

Vulnerability Management

All cloud assets are classified so that potential threats are prioritized and assigned an appropriate remediation process according to the type of issue and its severity and exposure. Clarizen uses a combination of automated and manual tools to continuously scan for security threats and prioritize, investigate and re-mediate any incidents or vulnerabilities.

PATCH MANAGEMENT LIFECYCLE

Remediation often results in a "patch" to some component of the Clarizen platform. Clarizen thoroughly checks and tests that any remediation is working properly throughout the platform. Moreover, Clarizen scans all network segments in real time to detect vulnerabilities or missing patches. The system agent reports any vulnerability to the management server so that remediation can begin. Remediation patches are deployed to the production network after passing a required quality assurance test and a strict policy approval.

All emergency security patches that re-mediate vulnerabilities are installed immediately. System snapshots are also created to provide rollback capabilities, if required.

Infrastructure Security (cont.)

Data Centers

Clarizen cloud applications are hosted in highly available data centers in the US and Europe, with a global uptime average of >99.999%. Clarizen's primary US data center is located at Equinix, in California; the disaster recovery site is located at Telx in New Jersey. The European data centers are both Equinix locations; the primary is in Amsterdam and the disaster recovery site is in London.

DATA CENTER CERTIFICATION

Clarizen data centers operate with the following data center certificates:

SSAE16 COMPLIANCE — The SSAE16 audit minimizes the need for multiple sets of auditors to separately examine the same set of controls that govern a third party's services. "SAS" statement on auditing standards, are a set of standards issued by the American Institute of Certified Public Accountants.

ISO 27001 Certification — This certification indicates the standard of protection supported at a data center related to the level of information security, physical security and business continuity maintained. It ensures that:

- Risks and threats to the business are assessed and managed
- Physical security processes such as restricted/named access are enforced consistently
- Audits are conducted regularly at each site that include tests of security and CCTV planning and monitoring

LEED Certification – LEED, or Leadership in Energy and Environmental Design, is an internationally recognized green building certification system. Developed by the U.S. Green Building Council (USGBC) in March 2000, LEED provides building owners and operators with a framework for identifying and implementing practical and measurable green building design, construction, operations and maintenance solutions.

DISASTER RECOVERY

Clarizen maintains a robust disaster recovery program at all data centers, which are distributed across the United States and Europe. A high-speed encrypted VPN tunnel connects the data centers and supports traffic shifting or traffic failover. To prevent data loss, Clarizen performs ongoing data replication and backup within each data center to a local disaster recovery site, and to the hot standby data center.

BUSINESS CONTINUITY TESTING

Clarizen has both a disaster recovery plan and a business continuity plan in place, and regularly tests them to ensure they are working properly.
The disaster recovery plan includes a comprehensive and established series of actions to take before, during and after a disruptive event. It includes an alternative processing site and an approach to return to the primary processing site as quickly as possible. The business continuity plan includes a comprehensive approach to quickly restore computer systems upon the event of any service interruption.

Infrastructure Security (cont.)

Cloud Operation Security

CHANGE MANAGEMENT

Production changes are executed strictly within scheduled maintenance windows, which are communicated to customers via the Clarizen Trust Site and RSS feeds. Clarizen change management processes include separation of duties, authorization chain, change auditing and change summary management reporting.

CONTINUOUS SERVICE MONITORING

The Clarizen platform is monitored on a 24/7 basis, using external and internal probes to monitor service availability and security issues. These probes are configured to send alerts on a wide variety of criteria, including security, availability and performance degradation.

LOG ANALYSIS

Clarizen conducts log analysis to identify any events that are relevant to the security and availability of Clarizen systems. Servers and network equipment logs are delivered to the centralized log analysis server. This server is configured to send alerts any time a threshold has been passed or a correlation rule has been triggered. If the system discovers that thresholds have been reached across multiple infrastructure components the incidents are flagged as a network anomaly and are escalated and investigated.

CLARIZEN TRUST SITE

The Clarizen security team communicates all service status changes to customers via the Clarizen Trust Site, trust.clarizen.com. There, customers can subscribe to receive real-time updates.

Infrastructure Security (cont.)

Data Privacy and Certificates

PRIVACY POLICY

Clarizen's Privacy Policy fully discloses the type of information we may gather from Clarizen website visitors, as well as how we may use this information. We do not collect any personally identifiable information (PII), except when such information is voluntarily submitted by the visitor. Clarizen operates data centers in the US and Europe to adhere to the latest regulations regarding regional data storage and privacy.

PERSONAL INFORMATION OF CUSTOMERS AND PROSPECTS

Contact information represents any PII data that can be used to uniquely identify a visitor. Contact information is required for visitors to access Clarizen services and software, as well as for receiving newsletters or any commercial offers. All contact information, including, but not limited to, name, address, telephone number and email address, is held in strict confidence. This information is collected so that Clarizen can deliver the services customers and prospects request, and may also be used to deliver customer information and updates along with newsletters or commercial offers. Clarizen does not sell or share contact information with any third party.

ISO/IEC 27001:2013

Clarizen has received the prestigious ISO/IEC 27001:2013 Security Certification (ISO 27001). ISO 27001 is the internationally recognized standard for certifying that our Information Security programs and processes protect our internal assets and that of our customers.

As one of the most recognized and internationally accepted security standards, achieving ISO 27001 certification demonstrates and ensures Clarizen's ongoing dedication to security best practices. ISO 27001 certification validates and supports our systematically managed approach to business information protection; including risk, governance and compliance, on par with the largest of cloud service providers.

SOC 2 TYPE II

Clarizen is in full compliance with service organization control (SOC) 2 Type II, an audit that ensures an effective control system is in place to mitigate operational and compliance risks, and can demonstrate Clarizen's commitment to security. Clarizen has completed the SOC 2 Type II audit of its hosted services and applications and is fully compliant with the SOC 2 trust service principles of security, availability, processing integrity, confidentiality and privacy of its systems.

Physical Security

Environmental Security

Clarizen's data centers are geographically distributed and employ a variety of strict physical security controls, which include:

- Closed-circuit TV cameras
- Security zone separation and authorization
- Security authentication and Access Logs
- HVAC - Heating, ventilation and air conditioning
- Fire prevention detection and suppression

Organizational Security

PERSONNEL SECURITY

Clarizen makes every effort to screen all employees and contractors. All candidates are pre-screened, and when allowable by law, subject to background checks. In addition, all employees and contractors are bound by the Clarizen code of ethics, information security policy and application and security training.

ACCEPTABLE USE POLICY

Clarizen maintains a comprehensive and clear acceptable use policy (AUP), which is communicated to all Clarizen employees and contractors. The AUP outlines the acceptable use of all equipment, information, electronic mail, computing devices and network resources. Clarizen ensures that its employees understand and comply with information security policies to minimize the risk of virus attacks, legal issues and compromised systems or services.

INFORMATION SECURITY

The Clarizen security team Is responsible for maintaining Clarizen's defense systems, developing security review processes, conducting security design and implementation reviews and building a customized security infrastructure. The team is also responsible for the development, documentation and implementation of security policies and standards.

CONTACT US

Contact Us

UNITED STATES

2755 Campus Drive. Suite 300,
San Mateo, CA 94403
T: 1 (866) 502-9813
F: 1 (650) 227-0308

UNITED KINGDOM

48 Warwick St.,
London,
W1B 5AW
T: 0044 203 411 40 44

FRANCE

T: +33 (0) 9 50 11 55 22

RUSSIA

T: +7 499-9187358

ISRAEL

4 Hacharash St, 10th Floor,
Building C
PO Box 7330
Hod Hasharon, 45241
T: 972 (9) 794-4300
F: 972 (9) 794-4333

JAPAN

Japan
Okubo Fuji Building 806,
2-7-1 Okubo Shinjuku-ku,
Tokyo Japan 169-0072
T: 81-3-6233-8164
F : 81-3-6233-7064

SOUTH AFRICA

T: +27 (11) 87-5502486

NEW ZEALAND

T: +64 9 887 0501

AUSTRALIA

Level 31, 120 Collins Street,
Melbourne Victoria
T: +61 3 9013 8621

TAIWAN

413, Mingshui Rd.,
Zhongshan Dist.,
Taipei City 104,
Taiwan (R.O.C.)
T:+886 (2) 8509-6680

CLARIZEN SALES

If you'd like to receive more information about purchasing Clarizen project management software subscription licenses, contact us at **sales@clarizen.com**

BUSINESS DEVELOPMENT

Companies seeking to forge mutually beneficial partnerships can send an email to **busdev@clarizen.com**

GENERAL INFORMATION

For general information and queries, please send an email to **info@clarizen.com**

About Clarizen

Clarizen is a global leader in collaborative work management software, bringing together cross-company project management, configurable work flow automation, in-context collaboration and a tailored, role-based experience, all built on a secure, scalable enterprise platform. **Visit us today at www.clarizen.com**

clarizen