Clarizen Security White Paper

Standards and practices

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 security standards and practices are backed by a multi-tiered approach that incorporates industry recognized and tested best practices for preventing security breaches, as well as ensuring customer data confidentiality, integrity, and availability.

The Clarizen security model encompasses the following components:

- Application Security
- Network and Infrastructure Security
- Physical Security
- 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 transmitted via a hypertext transfer protocol secured (HTTP with TLS) 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.

Password policy (cont.)

ACCOUNT LOCKOUT POLICY

To protect against dictionary-based, brute-force attacks, Clarizen has implemented best practices that allow administrators to set an account security features:

- Lock-out policy - user accounts are locked after a configurable amount of failed login attempts, and for a configurable lock out duration.
- Antibot gateway – Clarizen implements antibot gateway technology to identify and prevent BOT activities.

See the separate encryption document for details on password and encryption practice.

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 monitors and tests its security system and processes, 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.

CONTINUOUS SECURITY MONITORING

Clarizen security has deployed and relies on industry leading security scanning for ongoing continuous monitoring of its infrastructure. Clarizen relies on award-winning cloud security and compliance solution. The Clarizen Solution delivers critical security intelligence on demand and automates the full spectrum of auditing, compliance and protection for Internet perimeter systems, internal networks, and web applications.

Application content filtering

WEB TRAFFIC INSPECTION AND SANITATION

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

IP restriction

RESTRICTING AND IP WHITELISTING ACCESS

To provide an additional level of security Clarizen customers can restrict user access to their SaaS instances and data by monitoring and filtering privileged 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 phrases for storage. Clarizen relies on industry recognized SHA2 algorithms for creating robust hashes. Clarizen also "salts" customer passwords, or adds extra data that is unique, and random, to every HASH 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 a secure TLS connection, a cryptographic protocol that provides communications security over public computer networks, encrypting all communication between the web server and client browser. Additionally, Clarizen secures the identification of the web server via an industry-leading certificate authority.

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.

SAML2.0 AUTHENTICATION

As an additional security mechanism, Clarizen supports security assertion markup language (SAML2.0) authentication, which is a protocol used to securely exchange authentication and authorization data between customer systems and Clarizen.

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

The Clarizen platform integrates with many SAML2.0 compliant services 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. SAML2.0 compliant SSO services offers a range of strong authentication options and supports pre-integrated solutions from Duo Security, RSA, Symantec, VASCO, Yubico, plus others.

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.

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

Infrastructure security

Network architecture

INTRUSION PREVENTION

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

Clarizen Intrusion Prevention System (IPS) protect against the OWASP top- ten attacks. The systems are fully integrated with Clarizen application scanners and can provide virtual patching capabilities.

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 command and control.

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.

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.

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 27001:2013 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 CTV 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.

UK G-CLOUD

Clarizen is UK G-Cloud certified to provide streamlined SaaS services within the United Kingdom to participating government entities.

Cloud First is the United Kingdom government's initiative to achieve cross-government economies of scale in its procurement practices. Using a centralized procurement framework, G-Cloud , public sector agencies can gain access to more than 800 suppliers and more than 7,000 services across all types of cloud service models, including public, private and hybrid from the G-Cloud Digital Marketplace.

It provides public sector organizations a legally compliant framework through which they can buy commodity pay-as-you-go services, as a cheaper alternative to traditionally sourced ICT – simply and transparently.

G-Cloud is easy to use. In fact it's fast – rapid implementation of days and weeks not months or years. Thousands of hours of development and years of expertise at your fingertips. All of this is making buying easier and saving you costs.

Benefits of Certification

- An established procurement framework
- Innovative technologies delivering faster business benefits and reducing costs
- No long term commitments
- Flexibility to choose from a comprehensive set of products including open source technology
- Choice of several services that have been accredited at an official level

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
- 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

United States

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

Israel

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

United Kingdom

85 Tottenham Court Rd.
London, W1T 4TQ
T: +44 207 268 3464

France

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

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

Australia

T: +61 2 8006 9086
T: +61 3 9018 7075

ABOUT CLARIZEN

Clarizen is a collaborative work management solution designed for people who value their time, and for organizations that value cross-company engagement. Built on a secure, scalable platform, Clarizen brings together project management, configurable workflow automation and in-context collaboration to create a meaningful engagement experience that allows everyone to work the way they work best. Everyone involved can track projects, communicate effortlessly and participate on their terms. When employees can connect to a larger and more meaningful purpose, progress is not only clear, it's accelerated. Organizations of all sizes, across 79 countries already rely on Clarizen to help engage their people and move their business forward. The company is privately held with office locations including San Mateo (California), Tel Aviv and London. Visit us today at **www.clarizen.com**