Crosscode Panoptics – Security & Compliance

Introduction

This white paper describes Crosscode's overall architecture regarding its application, firewalls, data privacy, disaster recovery, security, processes, and data center facilities.

Compliance

Crosscode stores its data in top-tier data center facilities hosted by Amazon Web Services. The IT infrastructure that AWS provides to its customers is designed and managed in alignment with security best practices and a variety of IT security standards, including SOC 2, ISO 27001, PCI DSS Level1 and more. Crosscode itself is undergoing SOC2 certification at this time.

Physical and Operational Security

Data Centers

Crosscode's data centers reside in enterprise-class data center facilities provided by Amazon Web Services in Oregon and Ohio. These data centers offer the full range of hosting facility features such as fully redundant power and environmental as well as the highest levels of security.

Premises - AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing state-of-the-art electronic surveillance and multi-factor access control systems, intrusion detection systems, and other electronic means. Data centers are staffed 24x7 by trained security guards, and access is authorized strictly on a least privileged basis.

All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. All physical access to data centers by AWS employees is logged and audited routinely.

Power - The IT infrastructure that AWS provides to its customers have power failover. The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide backup power for the entire facility.

Environment – Heating, ventilation and air conditioning (HVAC) systems provide appropriate and consistent airflow, temperature and humidity levels. Every data center's HVAC system is

N+1 redundant. This ensures that redundant systems immediately and automatically come online should there be an HVAC system failure. Advanced fire suppression systems are designed to stop fires from spreading in the unlikely event one should occur.

Business

Crosscode employees and contractors are required to sign a Proprietary Information Agreement. Crosscode maintains a set of information security policies that are approved by the executive team and enforced by Crosscode's security team. The policies cover areas such as access control, change management, acceptable use, anti-virus, asset management, audit logging, business continuity and disaster recovery, clear desk screen, data backups, data classification, email usage, encryption (at rest and in transit), hiring, incident response, information media handling, roles and responsibilities, mobile device and laptop security, network scanning, password policy, patch management, physical access, remote access, risk assessment and management, telecommuting, user access, vendor management and wireless networking.

Application Architecture

Software Development Process

Crosscode's software development process follows the industry best practices. Our software development cycle includes stringent code reviews, integration and regression testing, and full internal and external security testing to check for vulnerabilities. Crosscode's operations team reviews the releases or patches and then creates a rollout plan consisting of planning, deployment, and testing.

Crosscode conducts internal audits on our software components and checks the implementation against well-known vulnerabilities, including the OWASP top 10. Any critical findings are taken as a “hotfix” in an immediate release.

Software Architecture

The servers behind the Crosscode platform service are locked down and behind a firewall. Only the essential ports are open to the public. Data in and out of the firewall are always encrypted in transit using TLS1.2 for application access or SSH and TLS (over IPSec) for administration.

The application supports role-based access control (RBAC), where client users have a unique account and a designated role that determines the type and scope of data access. A role maps to a job function or duty (e.g., "Administrator"), and the permissions to perform certain operations are assigned to specific roles. The role serves as a level of indirection between the users and their access to resources. Every incoming request to our platform service requires proper authentication and authorization via RBAC.

Administration of the servers must be performed over a VPN connection with two-factor authentication. All servers send full audit logs to a central encrypted log repository. Every authorized technical operation staff member has a unique account, and administration is done via a limited set of setuid commands, reducing the exposure of production server credentials.

All server data such as audit trails, databases, backups, executables and elastic disk volumes are encrypted at rest with industry strength cipher AES-256.

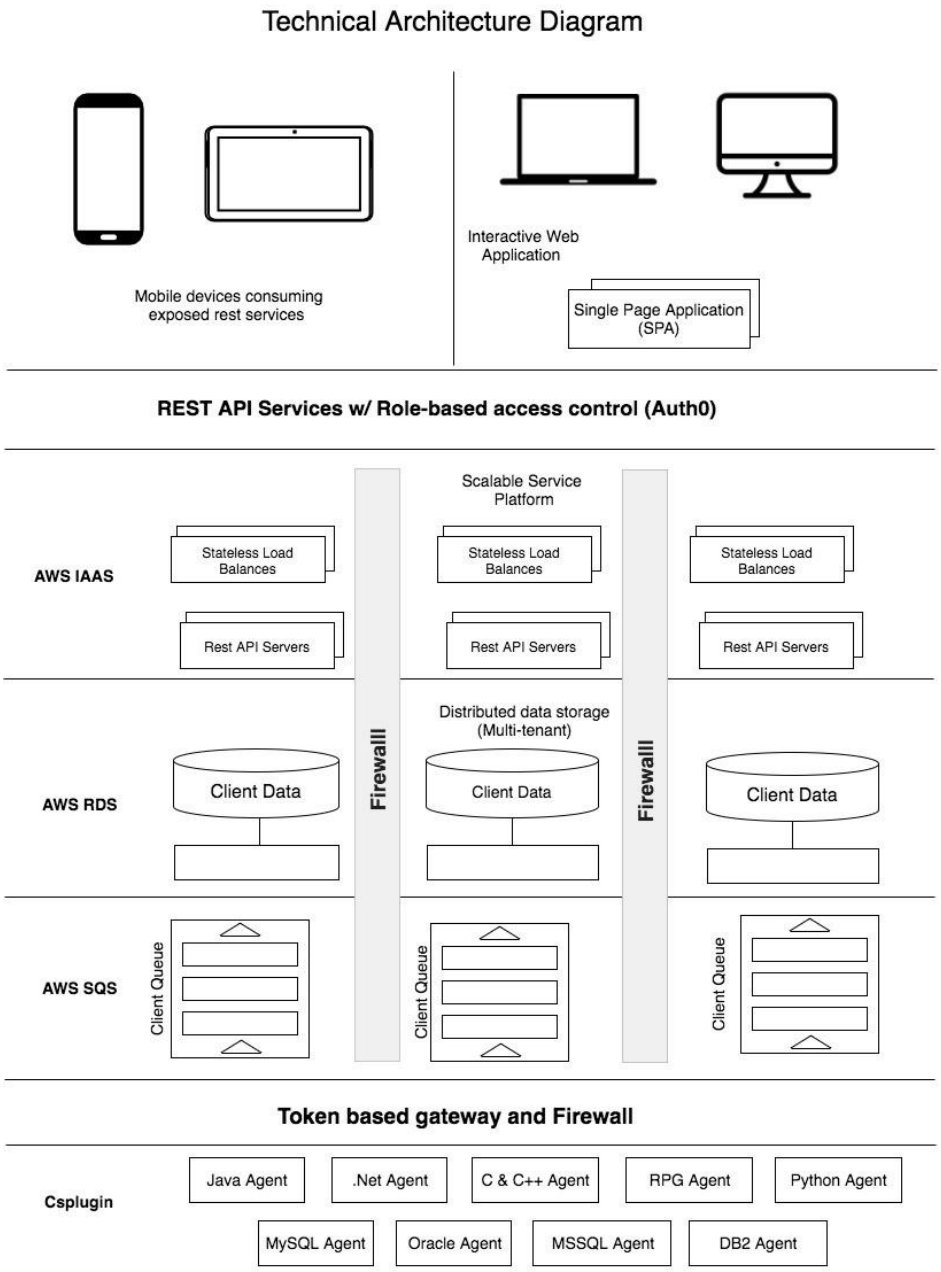
The diagram below illustrates the technical architecture of Crosscode.

The distributed data store layer consists of a collection of partitioned relational databases, each of which has a synchronously replicated hot standby. Each customer has it's own database encrypted with a unique key in it's own Virtual Private Cloud (VPC). The data store sits behind the firewall and is inaccessible to the public. Ingestion of the client data is done via the client-facing web application or our csplugin agent running on customer servers.

The service platform uses a service-oriented architecture, which consists of a collection of functional components, each of which runs on its own cluster of servers. Each server cluster is partitioned and/or replicated to maximize scalability and availability. The REST API servers are accessible to the web application layer and csplugin. The other servers are inaccessible to the public.

The application service layer consists of a collection of load balanced web application servers that call upon the service platform to collect and present the data to the browser, which runs a single page (AJAX) application. The application servers are stateless, and incoming requests to a downstream server can easily fail over to a different server.

Every request between the web application layer/mobile app and the REST API servers is authenticated and validated with RBAC.



Authentication and Access Controls

Crosscode's application is accessible via a browser. All user activity is tracked in audit logs. Session timeouts automatically log an idle user out of the applications. The application supports role-based access control, where client users have a unique account and a designated role that determines the type and scope of data access.

The user session automatically times out after 30 minutes of inactivity. Every incoming request to our platform service requires proper authentication and authorization.

Network Security

Crosscode implements industry best practices in the design and configuration of its network, utilizing AWS' enterprise architecture to provide a secure and reliable platform. Only essential ports (HTTPS) are accessible to the public.

Data Communication

Crosscode employs data communication practices that provide the maximum scalability, security, and reliability. AWS employs a redundant connection to more than one communication service at each Internet-facing edge of the AWS network. These connections each have dedicated Network devices. All data in transit (network connections to Crosscode) are through HTTPS, and all data is encrypted and presented over a TLS connection.

Network Architecture

Network access to and from Crosscode's application is controlled by dedicated firewall devices, Intrusion Detection Systems (IDS), access control lists, and load balancing. Crosscode has firewalls and load balancers at every tier of the application. Crosscode employs separate AWS Security groups based on the server function. Firewall rules apply between servers of different Security groups. We require MFA for production account access (Amazon Web Services). The internal admin web application requires an individual login, and the server is locked down by IP. Access is closely monitored.

Crosscode's servers are monitored and secured through regular penetration tests and vulnerability scans against the production system to ensure that only essential ports are open on public access points (HTTPS port for the app servers). Crosscode uses a host-based intrusion detection system that analyzes server logs to flag possible intrusion attempts. Such alerts a re enabled at all public access points. Crosscode also uses AWS CloudWatch for external site availability and error reporting services to actively monitor the health of its system.

Data Security

Crosscode's data security and protection protocols focus on employee access to systems that house customer data, regulatory compliance, data encryption, user roles, and data retention/destruction.

Administrative Controls

Data access

Access to customer data is restricted to authorized Customer Support and Operations teams. Access to SaaS servers is limited, log tracked, and regularly checked.

Data security policies

These address areas of access control, change management, acceptable use, anti-virus, asset management, audit logging, business continuity and disaster recovery, clear desk screen, data backups, data classification, email usage, encryption (at rest and in transit), hiring, incident response, information media handling, roles and responsibilities, mobile device and laptop security, network scanning, password policy, patch management, physical access, remote access, risk assessment and management, telecommuting, user access, vendor management and wireless networking. All employees are required to agree to the terms of these policies. Any employees that have access to customer data or production systems must undergo security and data privacy training to ensure compliance with corporate security policies and practices.

Technical controls

Data Encryption, Protection, and Destruction

Access to Crosscode application by users is through HTTPS (TLS1.2) and all data is encrypted and presented over a TLS connection, At-rest data is encrypted using industry strength cipher AES-256.

Crosscode continuously performs backup snapshots of the database throughout the day and has daily full backups with a 30-day backup retention period. After the retention period, the data is purged. Upon a client’s termination of a contract, data would be removed with full secure erasures.

Application Security Features

Role-based access

Customer logins have different access permissions based on assigned user roles. These roles limit both the data and the application functionality according to the user's roles and capabilities.

Single Sign On (SSO)

SSO is supported using SAML v2.0 via Auth0.

Login information protection

Users who failed an excessive number of login attempts in a short period are automatically locked out of Crosscode’s system for a period of time.

Business Continuity and Disaster Recovery

Crosscode's data protection, high availability, and enterprise architecture are designed to ensure application availability and protect information from accidental loss or destruction.

Backup and Recovery

Our primary data backup strategy leverages snapshot and data mirroring strategies. Crosscode continuously performs backup snapshots of the database throughout the day and has nightly full backups generated. The databases and server logs are transmitted to multiple AWS data centers in the same availability zone with Amazon's own network infrastructure, the databases are synchronously replicated to a hot standby in a different data center. In addition, snapshots are backed up in the Ohio data center. Because of this, the RPO will be the backup data generated which will be close to current. The RTO is 48 hours.

Network and Storage Redundancy

Every component in the SaaS infrastructure is redundant. There are at least two of each hardware component that process the flow and storage of data. All network devices, including firewalls, load balancers (AWS ELB), and switches are fully redundant and highly-available. High availability for Internet connectivity is ensured by multiple connections in each of AWS' data center to different ISPs. Crosscode's data is stored in redundant storage hosted by Amazon Web Services (e.g., S3 and RDS with synchronization replication).

Load Balancing and Server Clustering

Crosscode load-balances at every tier in the infrastructure, from the network to the database servers. Application server clusters are enabled to ensure that servers can fail without interrupting the user experience. Database servers are clustered for failover.

Disaster Recovery (DR) Plan

Our Disaster Recovery plan incorporates geographic failover between US data-centers in Ohio and California. Service restoration is within commercially reasonable best efforts and is

performed in conjunction with data-center provider's ability to provide adequate infrastructure at the prevailing failover location. We simulate such scenarios at least once every six months in the QA environment.

Business Continuity

Crosscode has a business continuity policy and disaster recovery plan for all critical business functions.

Monitoring Services and Security Audits

Monitoring and Incident Reporting

Crosscode uses a variety of methods to monitor and enhance application and data security.

Application access logging – all successful and unsuccessful access activities are recorded in the system and in application logs, including username, action, and timestamp of access. The server logs (e.g., authentication and access logs) on all public access points are backed up weekly. System credentials are backed up monthly and on change.

Software coding methodology – Software development at Crosscode includes thorough documentation and disciplined use of version control process. Agile methodologies are used throughout Crosscode's software development. Crosscode uses Git as its centralized source code control system. Every release starts with a detailed design process involving Engineering, Product Management, and User Experience. Once release plans and dates are finalized, Crosscode follows an iterative, agile planning/design/development process with regular demos and feature completion check-off. QA performs rigorous regression and stage testing. In addition to Crosscode's development methodology, Crosscode has a formal process for software escalation issues and weekly triages for bug fixes and patches in priority releases called "hotfixes".

Intrusion detection - To prevent data breaches, Crosscode uses OSSEC, a host-based intrusion detection system that analyzes our server logs to flag possible intrusion attempts. OSSEC alerts are enabled on all servers. Crosscode also makes use of CloudWatch which monitors the external site availability and performs error reporting services to actively monitor the health of Crosscode's system.

Security Audits

Vulnerability Testing – We perform regular vulnerability scans on our servers both from outside the perimeter as well as inside.

Penetration Testing – We perform regular internal application penetration tests using tools like OWASP ZAP. Once a year Crosscode engages an independent third party to perform pen-test of our applications.

Internal Audits

In addition to security audits, Crosscode conducts internal audits on

- Access to sensitive areas of the office
- Application and data access by users
- Annual financial audit

System audit logs are retained for at least a year and are stored encrypted in Amazon S3.

Summary

At Crosscode, security, integrity, and the availability of our customers' data is a top priority. We believe this is vital to their business operations and to our own success. Therefore, we use a multi-layered security approach, involving data privacy, application security, physical and environmental security, network access controls, monitoring and incident reporting, administrative and service availability controls, and regulatory compliance.