Security and Privacy at Secure Code Warrior

Whitepaper

Version: 1.0

Date: 12th April 2021
Author: Secure Code Warrior Trust Team

Background and Philosophy

Any time data is moved into the cloud or through cloud-based applications or services, there are legitimate concerns around security, reliability, and privacy. Cloud-based systems are outside the direct control of IT departments, and under the management of a vendor's hosted environment. It is essential to ensure that cloud systems are at least as strongly secured as would be an application in a well-managed private cloud or internal IT environment.

Secure Code Warrior is committed to safeguarding our information assets, and those of our customers, against misuse, abuse or compromise. We adopt and foster a risk-based approach to managing information security, with the goal of consistently implementing appropriate risk management and mitigation measures to address the threat landscape posed to the security of the platform, customer data and information.

As Secure Code Warrior continues to succeed as a major player providing services to our customers, we will continue to build security capabilities as part of our Information Security Program.

In order to meet the changing threat landscape, and needs of our customers, Secure Code Warrior will use a risk-based approach to;

- protect data and information assets against unauthorised access.
- assure the confidentiality of data and information assets.
- maintain the integrity of data and information assets.
- manage information systems in accordance with best practice.
- comply with legal and regulatory requirements.
- maintain availability of Secure Code Warrior's information assets and systems.
- ensure all Secure Code Warrior staff receive Information Security Awareness Training.
- report, investigate and escalate, where appropriate, all information security breaches, whether actual or suspected, internal or external.
- assess and monitor the security of our supply-chain as appropriate.

Secure Code Warrior is committed to providing a highly secure and reliable platform using proven, tested, best-in-class technologies, practices and procedures.

The following sections detail Secure Code Warrior's comprehensive approach to security.

Compliance, Certification, and Testing

Is Secure Code Warrior Compliant with International Privacy Frameworks?

Secure Code Warrior meets all requirements of the General Data Protection Regulation (GDPR). Please refer to our Data Protection Agreement and Privacy Policy for more information.

In addition, to comply with E.U. data protection laws around international data transfer mechanisms, Secure Code Warrior has included (where relevant) Standard Contractual Clauses (SCCs) into data processing agreements with our data processors. For more information please email our Privacy Officer - privacy@securecodewarrior.com

Is Secure Code Warrior Compliant with International Security Frameworks?

Secure Code Warrior has achieved ISO 27001 compliance. This involves a comprehensive examination of security policies and practices.

Secure Code Warrior also uses the Cloud Security Alliance (CAIQ) and Standard Information Gathering (SIG) questionnaires to self assess against industry aligned security controls and frameworks to provide more assurance about our security practices. CAIQ/SIG available on request.

Secure Code Warrior's technical staff are trained in industry standard security practices, including avoidance of the OWASP Top Ten Web application vulnerabilities.

Does Secure Code Warrior undergo regular vulnerability assessments or penetration testing?

Yes. We perform penetration tests twice a year on our platform, conducted by a qualified third party. Results of this assessment are available upon request (after signing an NDA).

In addition, we have deployed tools internally to scan vulnerabilities during software development and across our network and infrastructure.

Our Organisation

Corporate Security Policies

Secure Code Warrior has a security team with defined responsibilities and maintains a comprehensive information security management system (ISMS) to meet ISO 27001 compliance. Our security policies and procedures are reviewed and revised as necessary, at least annually.

Our staff undergo background checks as a condition of employment and accept corporate security policies as a condition of employment.

Employee and contractor devices are required to have secure configurations, including disk encryption, strong passwords, and screen timeout.

All employees receive annual security training which includes review of the corporate security policies, awareness of social attacks including phishing, and employee responsibilities with respect to data confidentiality and privacy.

Employees have unique logins for all business critical systems and two-factor authentication is enforced wherever possible. We use OKTA as our corporate identity management solution with SSO functionality. We conduct regular access audits and operate on the principle of least privilege. Access to production systems containing customer data is limited to a small number of system administrators.

Secure Software Development

Secure Code Warrior's technical staff are trained in industry standard security practices, including avoidance of the OWASP Top Ten Web application vulnerabilities.

Secure Code Warrior has implemented a Secure Development Lifecycle for its software. Our processes are based on an agile methodology. We use a centralized secure version control system. Design reviews integrate security and privacy considerations. Code commit follows a process that includes peer review, secret scanning, static code analysis, open-source vulnerability scanning, container image scanning and unit and integration and functional testing. We use CI/CD pipeline to build and deploy the changes to the production system, deployment to production environments is controlled by approval gates.

How we secure our products

At Secure Code Warrior, we understand that SaaS offerings must be backed by a world-class technology that customers can count on day in and day out. Furthermore, maintaining the security of our products and the security of your data are our primary concerns. That's why our platform cloud infrastructure environment features an architecture that provides industry best practice security, system uptime and built-in redundancy.

In addition, Secure Code Warrior has established a Product Security Framework that ensures our products protect your people and data. Our mission is to establish trust and to ensure a safe and secure user experience with our products.

How do we assess risk?

We use a risk-based approach to information security, following the ISO 27001 standard together with the ISO 31000 risk management framework to continually assess all possible risks to our information. The results are then reviewed by management and a corrective action plan is prepared, if necessary.

Do you assess risk with your third parties (suppliers/vendors)?

We have a supplier due diligence process for managing our critical suppliers in terms of assessing their security/privacy controls. Due diligence reviews are completed as part of onboarding and annually thereafter. In addition, we cover security and privacy requirements within our contracts with all our critical suppliers.

How do we screen and train our employees?

Secure code Warrior staff undergo background checks as a condition of employment. Staff accept corporate policies as a condition of employment, and receive onboard training on security policies and practices.

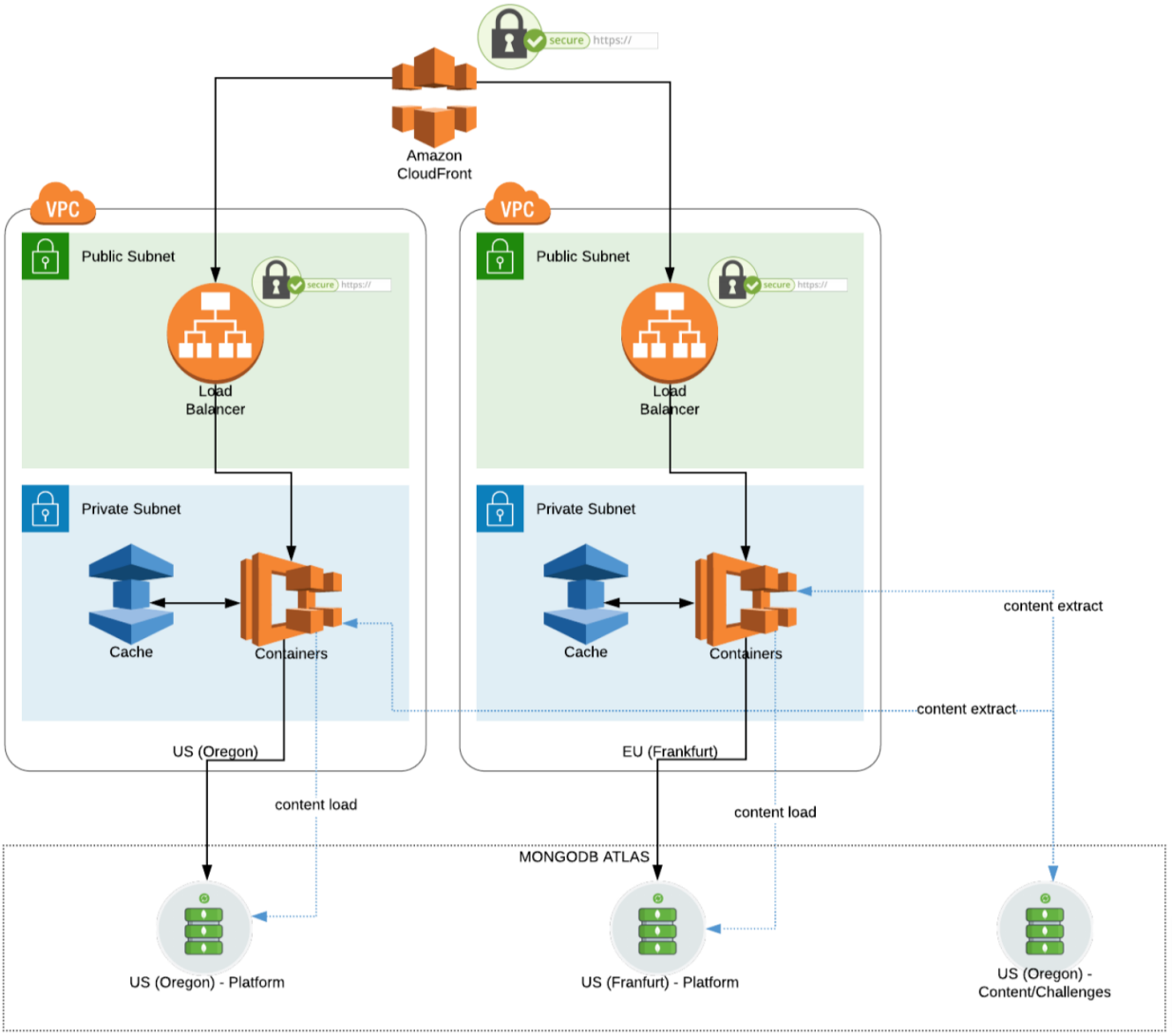
All employees receive annual security training which includes review of the corporate security policies, awareness of social attacks including phishing, and employee responsibilities with respect for data confidentiality and privacy.

Cloud Security

We leverage infrastructure services from AWS (Amazon Web Services) and MongoDB Atlas to provide a virtual private cloud (VPC) environment which meets ISO27001 standards and is SOC 1/SOC 2 compliant.

Inside the VPC all our application servers are on a private network segment that is not directly accessible from the Internet. Traffic to our application servers can only come from AWS application load balancers. Each internal service has its own security group and its own IAM policy. We apply the principle of least privilege and only grant the necessary permissions to our instances. We use an hardened Linux base image which is regularly managed and patched.

Figure 1 (below) is a diagram showing the overall architecture and data flows.



Components

The following table details the major application components:

#	Component	Explanation
1	CloudFrount	• The cloudfront is common to both the regions and is mostly used to serve the front end of the platform. • It additionally also serves the content for the challenges as well. • Caching capability in cloudfront is enabled
2	Load Balancer	• The application has a number of load balancers to distribute the load among various instances. • Different load balancers serve different regions.
3	ECS	• The application in both the regions is served using ECS with the application running on them.
4	Elasticache (Redis)	• Redis is used for caching some of the commonly used data to help in faster data retrieval. • There are different types of caches, like "User Cache", "Session Cache" to name a few.
5	Mongodb Atlas	• The database is hosted on the Mongodb cloud service called Atlas. • Each region has its own Atlas service. • Atlas being a cloud service itself, deals with the scaling, fault tolerance and load balancing of the requests being received from the application.

The infrastructure of the platform is hosted into two regions, Oregon, which serves mostly the US customers while the Frankfurt region serves mostly the EU and APAC customers. The architecture in both the regions is the same but they have been divided into different regions owing to GDPR regulations.

Management access to the infrastructure is limited to authorised support staff. The security architecture has been designed to control appropriate logical access using two-factor authentication when accessing the infrastructure. This authentication technology helps mitigate a number of security risks associated with logging into the infrastructure.

Within the Secure Code Warrior platform, you can configure access requirements based on roles and furthermore we allow the ability for you to integrate your own Identity Management Solution.

In addition, our application uses SSL certificates that support 256-bit SSL encryption, the same level of encryption used by online banks. Data transmitted to, from, and between our infrastructure is encrypted using TLS 1.2. The application also supports SSO and MFA (via SSO).

Hosting and Physical Security

Secure Code Warrior does not maintain any of its own physical datacenters, nor is any production data or customer data stored on local media. Instead, all platform specific data is stored and processed in a virtual private cloud (VPC) hosted by Amazon Web Services (AWS), which is our exclusive compute environment (see below under "Network Security '' for more details). Customer data is hosted and processed by our cloud-based database provider (MongoDB Atlas), who themselves use public cloud infrastructure from AWS to host their environments. You can learn more about AWS's compliance certifications here and refer to this document about MongoDB Atlas security features.

Network Security

All environments are hosted in a Virtual Private Cloud (VPC) in Amazon Web Services, containing separate public and private subnets. No inbound internet traffic is allowed to the private subnets and all application servers only reside in private subnets without public IP addresses. Only Amazon managed and maintained load balancers have ingress access to the application servers. Communication between Secure Code Warrior's AWS environment and MongoDB's AWS environment occur over peered VPC's (private links). Refer to Figure 1, above.

How are data transfers secured?

All internal data is transferred within our private Virtual Private Cloud, and such data never reaches the public internet. All external data transfers, whether between the browser and our platform or between our platform and technical partners such as AWS and Salesforce, are encrypted in transit with TLS. Once external data is transferred to our platform, it continues to be encrypted at rest using AES-256 encryption.

Do you have a process in place for timely updates of security patches?

For infrastructure hosted in AWS, security issues identified from various sources can include but are not limited to scanning tools or reported by a customer/external pentest or our employees are triaged and prioritized using a risk based approach. We use the following timeframe to patch the security issues based on the risk.

- Extreme risk: 2 days (Hotfix)
- High risk: 30 days (Release)

- Medium risk: 90 days
- Low risk: 180 days

For databases that host customer data, our managed services providers apply timely patches - which we verify and review with them.

Data Security and Privacy

General Information

Secure Code Warrior is compliant with European General Data Protection Regulation (GDPR), as are those suppliers which process and handle Personal Data on its behalf.

Secure Code Warrior's standard agreement with suppliers incorporates the Standard Contractual Clauses approved by the European Commission to secure European users' legal privacy rights.

Our Privacy Policy, further details the steps we take to protect customer information.

What types of data does Secure Code Warrior access, collect, store or transmit?

As a user of the Secure Code Warrior platform we will hold the following information about you,

- Identification data such as email address, username and password.
- Professional data such as job title or function, company name and location.
- Technical information used by the platform such as, test results, IP address, browser information. Please refer to Secure Code Warriors Privacy Policy (Appendix B) for more information.

Is data encrypted at rest?

We use MongoDB Atlas as our cloud hosted database management system. Encryption-at-rest is automated using AWS's transparent disk encryption, which uses industry standard AES-256 encryption to secure all volume (disk) data. All keys are fully managed by AWS. For more information refer here.

Is backup media encrypted?

Yes. All managed snapshots and images are automatically encrypted by our cloud based database management system (MongoDB Atlas).

Is access to data controlled and restricted?

Secure Code Warrior is a multi-tenant SaaS application. Multi-tenancy is a key feature that enables multiple customers to share one instance of the application layer, while isolating each customer's company application data. Every user ID is associated with exactly one customer, which is then used to access the platform. Access to the data is controlled within the application layer. For each backend endpoint, whenever it queries company data, it verifies if the userID is associated with the company.

Application Security

Any access to the Secure Code Warrior platform requires authentication, either via SSO (SAML) or by email + password combination. All communications are secure, only occurring over HTTPS (using TLS 1.2).

The software itself is secured by focusing on preventative measures: developers are trained in secure coding (using our own courses) in addition to regular automated scanning, including static application security testing, and scanning for vulnerabilities in dependencies and third-party libraries, containers (static and dynamic testing), and any infrastructure hosting our platform. All findings are triaged, prioritised, and addressed using a risk-based approach which means issues are usually resolved within 2 business days of discovery.

Our production and development environments are separated with strict rules preventing sensitive data from leaving our secure production database. Access to production data is controlled with strict access control rules and ephemeral credentials. All secrets are managed using secure vaults designed to ensure that secrets remain, well... secret.

To protect the integrity and privacy of the code itself, it is all developed on secured laptops which are fully managed by Secure Code Warrior: administrative privileges are restricted to staff in operational/support roles and all administrator activities are logged. The devices are encrypted, and run modern end-point detection and response software.

Logging and Monitoring

We utilise AWS Cloud Trail to log and continuously monitor account activity related to actions across our AWS infrastructure and GuardDuty for threat detection that continuously monitors for malicious activity and unauthorized behavior to protect our AWS infrastructure. DataDog is our centralised log management solution used for application and infrastructure monitoring.

Asset Management

All our infrastructure in the cloud is managed within AWS-based data centers. Our AWS systems are not tracked at a hardware level due to the nature of the service.

For our corporate devices, we only acquire managed devices from reputable vendors using the latest technology of deployment and furthermore we make sure each device is encrypted prior to the delivery of the device to our staff.

We track all our assets in an asset register and review our assets every 6 months. We have processes in place for returning of assets during staff offboarding and safe disposal of assets that are no longer being used.

The following list is not exhaustive, but provides visibility into the key security controls we have enforced across our corporate issued devices.

- Company Managed Devices
    - Password protected
    - Two-Factor Authentication
- ChromeOS
    - Built-in Antivirus and Malware protection
    - No staff administrative rights
    - Gsuite maintain all ChromeOS assets
    - All data is encrypted
- BYOD
    - Google Device Policy - managed apps deploy to BYOD devices.
- MacOS
    - Jamf - MDM for the Macs assets and managed
    - Sentinel One - Advance antivirus and malware protection
- Centralised User Management
    - Gsuite Enterprise
        - Identity management of users and groups
        - Context-Aware - restrict access to some G Suite resources on non-managed devices
        - Alerts and notifications are in place for scans of malicious emails, files and DLP.
    - Okta/SSO
        - Okta - Single Sign-On for all SAML apps
        - User app access base on needs
        - Non-SAML apps set with its own 2FA if available
        - Some SAML apps restriction to managed devices

High Availability, Backup, Business Continuity and Disaster Recovery

Secure Code Warrior maintains its cloud infrastructure in multiple cloud Availability Zones. There are redundant application services deployed in each zone and automated failover is enabled in case an individual server or an entire zone were to become unavailable.

Secure Code Warrior monitors the capacity utilization of computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. We evaluate the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. The cloud infrastructure and DevOps tools support rapid and virtually unlimited expansion of compute and storage capacity.

Databases implement continuous replication to a standby system. If the primary database becomes unavailable, traffic can be directed to the standby system. Secure Code Warrior also maintains backups of its operational systems (full backups daily, and incremental backups multiple times per hour). Backups are stored in secure encrypted storage. If necessary, systems can be restored from a backup. Restoration is tested regularly.

Secure Code Warrior has maintained high uptime for its service. Our systems are continuously monitored and any incidents that may affect availability are posted to https://status.securecodewarrior.com/

As a result of being a cloud native company, we are not bound by a physical office to work in. In case of an unavailability of an office, employees will be directed to continue to work from home while the office accommodations are being handled. In addition, Secure Code Warrior operates in multiple offices across the globe, in a case of prolonged unavailability, key personnel would be able to move to other offices in any of the other locations. As such, Secure Code Warrior performs tabletop exercises for Business Continuity based on specific events that may impact the delivery of our platform. In many cases the outcome of testing Business Continuity will involve invoking Disaster recovery, which is also tested annually and includes assessing our recovery against our defined metrics for RPO/RTO.

Incident Response

Secure Code Warrior maintains a Security Incident Response Plan, which details responsibilities and procedures in case of a security event, including attempted as well as actual compromise of our systems.

Secure Code Warrior will promptly notify affected customers, and as required, legal and regulatory authorities, should there be any breach involving exposure of customer data.