SmartWinnr Information Security White Paper

SmartWinnr

Drive Performance Through Better Knowledge

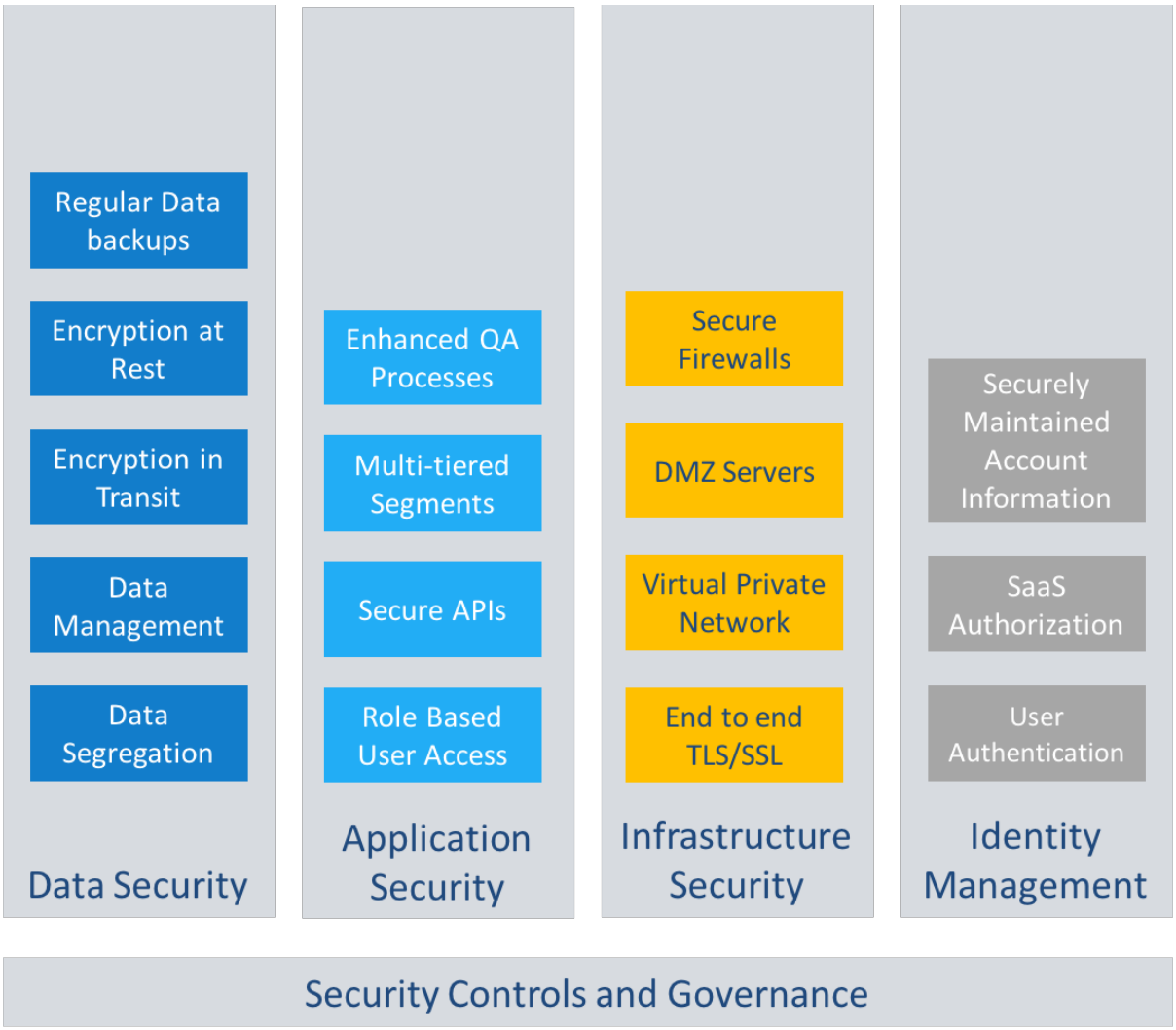
Table of Contents

Introduction

Cloud computing has revolutionized the way enterprise business applications are made available to businesses of all sizes - from the largest enterprises to small and mid-sized businesses. Software-as-a-Service (SaaS) – services delivering applications and associated data over the internet – has become a business model as well as an application delivery model. However, with the proliferation of SaaS offerings, there are legitimate concerns about security.

At SmartWinnr, we understand the critical importance of information protection and recognize the contribution that information security makes to an organization's strategic initiatives and overall risk management. SmartWinnr has implemented security controls and practices that are designed to protect the confidentiality, integrity, and availability of customer information. Additionally, SmartWinnr continually works to strengthen and improve those security controls and practices.

SmartWinnr's high-level security reference architecture has been shown below. The rest of this document will provide details about this architecture.



This paper provides a high-level detail of the security practices and controls incorporated within the SmartWinnr solution that helps enterprises to meet their high benchmark of security.

Data Security

Data Storage Security

Logical Data Segregation: Along with the formation and execution of each application request, SmartWinnr confirms that the user context (a tenant ID) accompanies each request and includes it in the WHERE clause of all query statements to ensure the request targets the correct organization's data. This is inserted by the application dynamically at runtime and cannot be overridden externally.

Encrypted Data Storage: All data at rest is encrypted by 256-bit key using the industry-standard AES-256 algorithm. This is set by default and cannot be overridden by customers. All backups are also stored in encrypted format.

Secure Levels: Since the application and web tier are totally stateless, session information need not be kept in memory or disc, thus increasing overall security. This also makes easy to deliver a load-balanced application without sticky sessions.

Backup and Restore: Backup and restore capabilities improve security. SmartWinnr takes regular backups of the database at hourly, daily and monthly schedules. The data is available for rapid deployment and system restoration if the original data is corrupted due to any unforeseen event.

Data Transmission Security

Secure Communication: SmartWinnr implements SSL technology, which consists of a public key and a private key to protect sensitive information. The public key is used to encrypt information, and the private key is used to decipher it. When a Web browser points to a secured domain, an SSL handshake authenticates the server (website) and the client (Web browser). An encryption method is established with a unique session key. Customers may then begin a secure session that guarantees message privacy and message integrity.

Secure messaging: All outgoing email notifications sent from SmartWinnr are securely encrypted using TLS, which makes it difficult to tamper with the email message contents and to send spoofed emails.

Encryption Keys: Encryption keys are securely stored and periodically rotated.

Application Security

SmartWinnr application security architecture ensures good security practices are embedded during the design, implementation and testing of the application. The core security framework proactively prevents security loopholes during the coding phase itself.

SmartWinnr dynamically generates every page and transmits to the client using SSL. SmartWinnr's configurable codebase ensures that all the clients run the same version of the code but can get the benefit of different configurations based on their specific business need.

SmartWinnr has implemented extensive security measures during the application development lifecycle to prevent loss, misuse and unauthorized access to data. The application-level security measures include the following:

Multi-layered Architecture: By segregating the presentation, business and data layers in the application, SmartWinnr can ensure better control on the overall security of the solution.

Coding Quality Best Practices: At SmartWinnr we leverage industry standard programming techniques such as having a documented development and quality assurance processes and following guidelines such as the OWASP ESAPI library, to ensure that the applications meet security standards. In addition to that, all our code is peer reviewed prior to being released to QA, which minimizes the number of bugs that must be sent back to the developer for fixing.

Role-Based Permissions: Provide best practice security at all levels—function, transaction, field, and data—by using role-based permissions (RBP).

Unauthorized Access Prevention: All application endpoints require a logged-in user to send data request thus preventing improper access. Users can only request for data pertaining to their own organization, as the organization context is injected dynamically by the system at runtime based on the authenticated user's organization.

No Risky Plug-ins: The service avoids any Java applets or Flash plugins which can potentially increase security risk

Identity Management

SmartWinnr provides the following features to provide seamless access to the service while ensuring enterprise access and authorization policies are complied with:

Internal Authentication: SmartWinnr uses internal repository of user profiles with authentication information when customers do not want to integrate their own identify management product with SmartWinnr.

Federated Authentication: In Federated Authentication, SmartWinnr sends the authentication request to the client's authorizing system using Security Assertion Markup Language (SAML) protocol. On successful authentication, the trust mechanism passes the user's identification information to SmartWinnr which is used for granting access and subsequent requests.

Separating Authentication and Authorization Modules: Authentication mechanisms keep on maturing to mitigate new threats. Since authorization logic is embedded in the core code, SmartWinnr separates authentication and authorization functionalities in its implementation. Thus, the system is future-proof and can easily accommodate new authentication services and protocols.

Password Protection: SmartWinnr requires users to set strong passwords that conform to specific requirements. The passwords within the system are stored in salted cryptographic hash formats.

Network and Communication Security

SmartWinnr maintains robust security measures at the network and communication layer to ensure the service has high availability and minimize downtime due to any potential security threats. The security measures include the following:

Encrypted Access: SmartWinnr service can only be accessed over HTTPS. All web connections to the service are via TLS 1.1 and above. We support forward secrecy and AES-GCM, and prohibit insecure connections using TLS 1.0 and below or RC4.

Access Firewalls: The SmartWinnr production system has the web and database layers isolated using Linux firewalls as well as AWS Security Groups. Access is granted to systems in the network based on principle of least privilege. The Elastic Load Balancers are the only nodes opened to the internet that only for HTTPS access. All the other nodes are isolated by the firewalls.

Regular Patching of Production System: Production systems are regularly patched based on the latest available security patches.

Restricted Access to Production System: The SmartWinnr production system can only be accessed by a limited set of administrative users. Access to the production servers are based on private key files – there is no password based login to production boxes to prevent security breaches.

Data Center Security

SmartWinnr is deployed in Amazon Web Services. AWS employs a robust physical security program with multiple certifications, including an SSAE 16 certification. For more information on Amazon's physical security processes, please visit https://aws.amazon.com/security/

Security Controls and Practices

Security Controls Overview

SmartWinnr's has embedded security as one of the key principles to be adhered as part of the product and services lifecycle. The security controls and practices include the following:

- Develop secure coding guidelines, rules and analysis
- Conduct source code reviews
- Conduct mandatory static analysis
- Perform product health, risk, and threat landscape analysis
- Provide regular security training to product team
- Perform security architecture review
- Develop service roadmaps, security tools, and testing methods that helps the security team to address the Open Web Application Security Project (OWASP) Top 10 most critical web application security flaws

Security in Software Development Lifecycle

SmartWinnr uses the Git revision control system. Changes to SmartWinnr's code base go through a suite of automated tests and are reviewed and go through a round of manual review. When code changes pass the automated testing system, the changes are first pushed to a staging server wherein SmartWinnr employees can test changes before an eventual push to production servers and our customer base. We also add a specific security review for particularly sensitive changes and features. SmartWinnr engineers also can "cherry pick" critical updates and push them immediately to production servers.

In addition to a list where all access control changes are published, we have a suite of automated unit tests that check that access control rules are written correctly and enforced as expected.

Conclusion

Security is a critical consideration when evaluating any cloud-based service. SmartWinnr has taken multiple steps to integrate and implement security best practices through the service delivery lifecycle. We also understand that security improvement is a continuous process. As and when new security threats evolve, SmartWinnr is committed to improve our security practices to mitigate against those threats and embrace the latest security best practices.