SERVISBOT

Security Brief

Security at the Core of ServisBOT

At ServisBOT, security isn't an afterthought—it's foundational. Every layer of our platform is engineered with enterprise-grade security to ensure your data stays protected, isolated, and fully under your control. We never aggregate customer data, and we uphold strict boundaries between tenants.

In an era of evolving threats and increasing compliance demands, our customers trust that their information is safeguarded, their user interactions are encrypted, and their automated workflows are resilient by design.

PRESCIENT SECURITY
ISO/IEC 27001:2022
CERTIFIED
verify

AICPA SOC
SOC 2 Type II
TESTED & ATTESTED BY
PRESCIENT ASSURANCE

PCI DSS
COMPLIANT

HIPAA COMPLIANT
Tested and Attested by
PRESCIENT ASSURANCE
PRESCIENT ASSURANCE

ServisBOT Enterprise SaaS Features

ServisBOT offers a robust suite of enterprise-grade SaaS features designed to meet the security, scalability, and operational needs of modern organizations:

- **Role-Based Access Control (RBAC):** Granular access permissions ensure that users—such as bot builders, bot managers, IT administrators, data scientists, customer support agents, and enterprise developers—can only access the features and data appropriate to their role.
- **Secure Authentication and Authorization:** User access is managed through Single Sign-On (SSO) integration, simplifying authentication while maintaining enterprise-grade security. Access policies can also be restricted by IP address via the Administration Portal's Login Policy.
- **Real-Time Admin and Access Logging:** All user activity is logged in real-time, supporting auditability and compliance. Logs are securely retained for a minimum of one year.
- **High Availability and Scalability:** Built on a cloud-native architecture, ServisBOT ensures high availability, elastic scalability, and performance monitoring for enterprise deployment scenarios.

Specialized ServisBOT Features

- User data is always encrypted, with our keys or yours.
- Control of ingress & egress data via data masking, filtering, obfuscation, and treatment alternatives.
- Endpoint policies that can constrain access to specific Websites, pages, and communication channels.
- Secure Session: after authentication, maintain user details throughout conversation processing to ensure data services can be protected with user-level authorization.
- Chat History Server - customer-controlled service for persistence and management of conversational data. Customers can set retention of data to meet their own requirements and can provide GDPR's right to be forgotten.
- Secure API connectors protected with Oauth, Bearer token, and/or Basic auth. Source can be locked to a dedicated IP Address to enable firewall whitelisting.
- Native AWS integration to all services using cross-account roles.

ServisBOT Operational Disciplines

Physical Security

We ensure the confidentiality, availability, and integrity of your data with industry best practices. In addition, ServisBOT operates in data centers that have been certified as **ISO 27001, PCI/DSS Service Provider Level 1**, and/or **SOC2** compliance.

Application Security

We take steps to securely develop and test against security threats to ensure the safety of our customer data. ServisBOT maintains a Secure Development Lifecycle, in which training our developers and performing design and code reviews takes a prime role. In addition, ServisBOT employs third-party security experts to perform detailed penetration tests on different applications within our platform.

Data Security

We leverage secure components, such as **FIPS-140** certified encryption solutions to protect customer data throughout its lifecycle. For data in transit, communications between a customer and ServisBOT infrastructure are encrypted via industry best-practices **HTTPS and Transport Layer Security (TLS)** over public networks. For data at rest, customers of ServisBOT benefit from the protection provided by **AES256** encryption for configuration, user data, and documents.

Availability and Business Continuity

ServisBOT maintains a disaster recovery program to ensure services remain available or are easily recoverable in the case of a disaster. We employ multiple regions, availability zones, service clustering and network redundancies to eliminate single points of failure. Customers can remain up to date on availability issues through a publicly available status website covering scheduled maintenance and service incident history.

Network Security

ServisBOT maintains a security team that is on call 24/7 to respond proactively to security events. Through network vulnerability scanning, firewalls, continuous monitoring, the use of intrusion detection and prevention programs, and by participating in Threat Intelligence Programs, we keep a continuous watch on the security of our customers' data and use of their business processes.

For each ServisBOT AWS account, our security infrastructure is composed of **WAF, SIEM, IDS & IPS** tools. The edges of our network have a narrow attack surface and are protected with WAF and IAM secured endpoints, with limited access to the Internet. All network activity is proactively monitored for intruders (IDS/IPS) and misuse. We retain access logs for forensic purposes.

Compliance and Privacy

The security of our customers' data is a top priority. We are proud to be compliant with industry-leading standards, including **PCI DSS, ISO/IEC 27001, and SOC 2 Type II**, demonstrating our commitment to maintaining robust information security and data protection practices. These certifications reflect our ongoing dedication to operational excellence and risk management. Our security posture is continuously evolving, and we are actively working toward additional certifications to further strengthen our compliance framework and provide our customers with even greater assurance.

Customers from the US Health and Medical services industry are required to comply with HIPAA. To support that, ServisBOT executes Business Associate Agreements (BAAs) with **HIPAA**-covered entities, certifying that ServisBOT protects personal health information (PHI) in accordance with HIPAA guidelines.