Security Brief

At ServisBOT, security is baked into everything we do. We provide enterprise-class security features to ensure customer data is always protected, never aggregated, always isolated and under your control. Our customers rest easy knowing their information is safe, their interactions are secure, and their business processes are protected.

1. Enterprise SaaS Features

- Role-based Access Control provides the right levels of access depending on the different roles, for example, for bot builders, bot managers, IT, data scientists, agents, or enterprise developers.
- The Administration Portal "Login Policy" can be limited by IP Address. User authentication & authorization is via SSO.
- Admin and Access Logs are available in realtime and retained for one year.

2. Specialized ServisBOT Features

- User data is always encrypted, with our keys or yours.
- Control of ingress & egress data is implemented via data masking, filtering, obfuscation, and treatment alternatives.
- Endpoint policies can be set to constrain access to specific websites, pages, and communication channels.
- Secure Session: Following user authentication, this maintains 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 are protected with Oauth, Bearer token, and/or Basic auth. The source can be locked to a dedicated IP Address to enable firewall whitelisting.
- Native AWS integration to all services using cross-account roles.

We provide best in class security through a combination of:

1. Enterprise SaaS features
2. Specialized ServisBOT features, and
3. Operational Disciplines

3. Operational Disciplines

Physical security

We ensure the confidentiality, availability, and integrity of customer 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 SOC II 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 take 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.

Network security

ServisBOT maintains a security team that are 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 a 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

ServisBOT is a GDPR data processor and has an active EU/US Privacy Shield (**https://www.privacyshield.gov/participant?id=a2zt00000008ThmAAE&status=Active**).

Our privacy policy is available at **servisbot.com/privacy/** Customers from the 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. While portions of our solution can be configured to meet PCI.

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 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.

USA—ServisBOT Inc. | P: +1 702 213 7289
IRELAND—ServisBOT Ltd. | P: +353 (76) 6805 170
askbotty@servisbot.com