Security Overview

Security is embedded into our everyday responsibilities and regularly championed by our Executive Leadership team. Through regular training and security awareness initiatives, we are proud to have fostered a culture where employees feel a shared responsibility towards maintaining and enhancing security at Synergi Partners.

We design our processes and technologies to be robust and aligned with industry best practices (including information assurance frameworks) at an organizational, platform, and operational level to adequately protect your data.

1. Organizational Security

At Synergi Partners, security is every employee's responsibility. Considering our people are essential to the delivery of secure solutions, we instill the importance of security right from our new hire onboarding experience and reinforce this principle through regular training and awareness programs.

With empowerment and support from Synergi Partners' Executive Leadership team, we have built a comprehensive Security Program that promotes the importance of security and the protection of customer data throughout the organization. Synergi Partners invests considerable resources to ensuring that only qualified professionals make up the teams that manage and oversee our infrastructure.

2. Platform Security

Data Security

Data Encryption

Customer data is encrypted at rest and while in transit using leading industry standards. To encrypt this data, we use a strong encryption key that is unique to each customer. This key is managed via a robust and secure key management process and periodically rotated to ensure the continued confidentiality of your data. Your data will remain encrypted while being transmitted within our secure networks using the Advanced Encryption Standard (AES).

Access to Customer Data

Our cloud computing and data center service providers do not have access to unencrypted customer data. Only a very limited number of Synergi Partners employees have access to customer data in order to provide customer support and manage customer requested changes.

Application Security

Secure Software Development Lifecycle (S-SDLC)

Our Secure Software Development Lifecycle (S-SDLC) uses secure coding practices, static code assessments and reviews, and dynamic application testing to find exploitable conditions prior to the code being deployed to production. We leverage internal capabilities and external partners to continuously assess the network and find and remediate flaws before attackers can.

Onboarding and ongoing training for all developers includes a set of robust security principles, practices, and coverage of OWASP Top 10 Security Risks at a minimum. Our code reviews ensure that validated code is used and new code has been fully assessed.

Synergi Partners' web application defense strategy builds on secure code to deliver secure solutions that provide insight while protecting your data. We test all code and third-party libraries for security vulnerabilities before release, and regularly scan our network and systems for vulnerabilities. Third-party assessments are also conducted regularly.

We use "defense in depth" to safeguard web applications from attack. Application-layer next-generation firewalls, and load-balancers, are part of our security strategy. We implement application defense at network, session, function, and data levels to proactively eliminate vulnerabilities and threats.

Web Application Penetration Testing

We regularly perform both internal and external web and mobile application vulnerability testing to evaluate the security of our solution. Such assessments allow us to obtain valuable insights for further enhancing our Vulnerability Management Program and other continuous improvement security initiatives.

Secure Authentication and User Management

Synergi Partners fully supports single-sign-on (SSO) using identity provider (IdP) initiated logins via Security Assertion Markup Language (SAML) compliant solutions. We make pre-built security roles and configurations readily available within our solution so your administrators can easily manage user access to meet your organization's security requirements.

Infrastructure Security

Our global infrastructure has been designed from the ground up with security and availability in mind. We have carefully selected secure data center providers, built secure networks upon which we run our operations, and validate our technologies and processes for alignment with industry best standards and other US/global infrastructure benchmarks.

Below are a few key points on how we maintain a secure and robust infrastructure:

- **Configuration**– Using configuration management tools and system hardening standards based on industry best practices (e.g. CIS Benchmarks) to ensure consistent deployment of changes across our infrastructure.
- **Monitoring**– Ongoing monitoring and scanning of our global infrastructure, networks, and information systems to identify and address threats and vulnerabilities.
- **Reporting**– Leveraging a Security Information and Event Management (SIEM) solution that merges numerous data sources (e.g. system and application logs, firewall logs, IDS logs) for timely review, reporting, and remediation.
- **Change Management**– Implementation of a change management process to ensure proposed changes to systems and processes do not negatively impact our operations and services.
- **Training**– Providing Synergi Partners' Engineering team regular training on secure coding practices and securely deploying changes to our corporate and Azure infrastructure.
- **Validations**– Periodic security and internal control assessments, reviews, and audits to ensure the continued adequacy and effectiveness of our internal security controls.

3. Operational Security

Physical Security

Our organization maintains state-of-the-art facilities from which our employees safely work. Synergi Partners offices are protected with biometric readers, sanitized HVAC, security personnel, and surveillance cameras that monitor all entry and exit points. We have also designed the delivery of our solutions to ensure that no customer data is required to be stored on premises at our offices.

We selected some of the world's top data center providers to ensure they have sufficiently secure facilities and processes that can help us manage and process highly sensitive data. We perform periodic assessments of these service providers to validate that their internal controls on physical security continue to meet our standards and requirements.

Vulnerability Management

As cyber threats become increasingly sophisticated, pre-emptive actions must be taken to identify and address security vulnerabilities. Synergi Partners' comprehensive Vulnerability Management Program adopts a proactive and multi-layered defense strategy for protecting critical assets and information.

Synergi Partners' Information Security team continually monitors and scans our infrastructure, systems, and networks to identify threats and vulnerabilities. The team employs a risk-based approach towards prioritizing and remediating vulnerabilities to ensure security risks are addressed within a timely manner. Other key components of the program, such as frequent patching and platform security maintenance, ensure we proactively combat security threats to the core infrastructure that support our solutions.

Secure Data Centers and Service Availability

Our solutions are hosted from highly secure data centers with top-tier physical, technical, and environmental safeguards. The data centers are physically dispersed for redundancy and to minimize impacts to the availability of our solution in the event of an environmental disaster. Apart from maintaining geographically dispersed data centers, we also rely on Azure Availability Zones and Regions for system resiliency and multi-site redundancy that enable encrypted and near-time data replication and recovery.

Azure *availability zones* are physically separate locations within each Azure region that are tolerant to local failures. Failures can range from software and hardware failures to events such as earthquakes, floods, and fires. Tolerance to failures is achieved because of redundancy and logical isolation of Azure services. To ensure resiliency, a minimum of three separate availability zones are present in all availability zone-enabled regions.

We designed our solutions to be available around the clock except during maintenance windows, which are used to perform system updates, infrastructure, security, and technology upgrades.

Our Engineering team regularly monitors our infrastructure to plan for sufficient capacity. State-of-the-art technologies are leveraged to offer our customers reliable on-demand cloud computing and capacity management. Such technologies enable our solutions to easily scale and accommodate demand from both small and large enterprise customers.