Supportive Hands Security Overview

Countless customers trust Supportive Hands with their data. This is not something we take lightly. We combine enterprise-class security features with comprehensive audits of our applications, systems, and networks to ensure customer and business data is always protected. And our customers rest easy knowing their information is safe, their interactions are secure, and their businesses are protected.

Data Center and Network Security

We ensure the confidentiality and integrity of your data with industry best practices. Supportive Hands servers are hosted at Tier IV or III+, SSAE-16, PCI DSS, or ISO 27001 compliant facilities. And just like our customer support, our Security Team is on call 24/7 to respond to security alerts and events.

Application Security

We take steps to securely develop and test against security threats to ensure the safety of our customer data. In addition, Supportive Hands employs third-party security experts to perform detailed penetration tests.

Product Security Features

We make it seamless for customers to manage access and sharing policies with authentication options. All communications with Supportive Hands servers are encrypted using industry standard HTTPS over public networks, meaning the traffic between you and Supportive Hands is secure.

Data Center & Network Security

Physical Security

Facilities	Supportive Hands servers are hosted at Tier III, SSAE 16/ISAE 3402, PCI DSS, ISO/IEC 27001:2013 compliant facilities. Our servers are logically separated from other data center customers. The data center facilities are powered by redundant power, each with UPS and backup generators.
On-Site Security	Our data center facilities feature a secured perimeter with multi-level security zones, 24/7 manned security, CCTV video surveillance, multifactor identification with biometric access control, physical locks, and security breach alarms.
Monitoring	All systems, networked devices, and circuits are constantly monitored by both Supportive Hands and the data center providers.
Location	Supportive Hands has data centers in Sydney and Melbourne. Additionally, customers can choose to locate their data in the US or EU.

Network Security

Dedicated Security Team	Our Security Team is on call 24/7 to respond to security alerts and events.
Protection	Our network is protected by redundant layer 7 firewalls, best-in-class router technology, secure HTTPS transport over public networks, regular audits, and network intrusion detection/prevention technologies (IDS/IPS) that monitor and block malicious traffic and network attacks.
Architecture	Our network security architecture consists of multiple security zones of trust. More sensitive systems, like our database servers, are protected in our most trusted zones. Other systems are housed in zones commensurate with their sensitivity, depending on function, information classification, and risk. Depending on the zone, additional security monitoring and access controls will apply. DMZs are utilized between the Internet, and internally, between the different zones of trust.
Network Vulnerability Scanning	Network security scanning gives us deep insight for quick identification of out-of-compliance or potentially vulnerable systems.
Security Incident Event Management (SIEM)	A security incident event management (SIEM) system gathers extensive logs from important network devices and hosts systems. The SIEM creates triggers that notify the Security team based on correlated events. The Security team responds to these events.
Intrusion Detection and Prevention	Major application data flow ingress and egress points are monitored with Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS). The systems are configured to generate alerts when incidents and values exceed predetermined thresholds and uses regularly updated signatures based on new threats. This includes 24/7 system monitoring.
Threat Intelligence Program	Supportive Hands participates in several threat intelligence sharing programs. We monitor threats posted to these threat intelligence networks and take action based on our risk and exposure.
DDoS Mitigation	In addition to our own capabilities and tools, our data center provider works with on-demand DDoS scrubbing providers to mitigate Distributed Denial of Service (DDoS) attacks.
Logical Access	Access to the Supportive Hands Production Network is restricted by an explicit need-to-know basis, utilizes least privilege, is frequently audited and monitored, and is controlled by our Operations Team. Employees accessing the Supportive Hands Production Network are required to use multiple factors of authentication.
Security Incident Response	In case of a system alert, events are escalated to our 24/7 teams providing Operations, Network Engineering, and Security coverage. Employees are trained on security incident response processes, including communication channels and escalation paths.

Encryption

Encryption in Transit	Communications between you and Supportive Hands servers are encrypted via industry best-practices HTTPS and Transport Layer Security (TLS).
Encryption at Rest	Supportive Hands supports encryption of customer data.

Availability and Continuity

Redundancy	Supportive Hands service clustering and network redundancies eliminate single point of failure. Our strict backup regime ensures customer data is actively replicated across both systems and facilities.
Disaster Recovery	Our disaster recovery program ensures that our services remain available or are easily recoverable in the case of a disaster. This is accomplished through building a robust technical environment, creating disaster recovery plans, and testing.
Enhanced Disaster Recovery	With enhanced disaster recovery, the entire operating environment, including customer data, is replicated in a secondary site to support taking over the service when the primary site becomes fully unavailable. Supportive Hands has defined a targeted return time objective (RTO) and recovery point objective (RPO) for this service.

Application Security

Secure Development (SDLC)

Security Training	At least annually, engineers participate in secure code training. This training covers OWASP Top 10 security flaws, common attack vectors, and Supportive Hands security controls.
Framework Security Controls	We utilize framework security controls to limit exposure to OWASP Top 10 security flaws. These include inherent controls that reduce our exposure to Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), and SQL Injection (SQLi), among others.
QA	Our QA department reviews and tests our code base. Engineers on staff identify, test, and triage security vulnerabilities in code.
Separate Environments	Testing and staging environments are separated physically and logically from the production environment. No actual customer data is used in the development or test environments.

Application Vulnerabilities

Dynamic Vulnerability Scanning	We employ a number of third-party, qualified security tools to continuously scan our application. Supportive Hands is scanned daily against the OWASP Top 10 security flaws. We maintain an in-house product security team to test and remediate any discovered issues.

Third-Party Penetration Testing	In addition to our extensive internal scanning and testing program, Supportive Hands employs third-party security experts to perform a broad penetration test across the Supportive Hands Production Network.

Product Security Featured

Secure Development (SDLC)

Authentication Options	For admins/users we support Supportive Hands sign-in.
Secure Credential Storage	Supportive Hands follows secure credential storage best practices by never storing passwords in human readable format, and only as the result of a secure, salted, one-way hash.

Additional Product Security Features

Access Privileges & Roles	Access to data within your Supportive Hands is governed by access rights, and can be configured to define granular access privileges. Supportive Hands has various permission levels for users (admin, end-user, etc.) accessing Supportive Hands.
IP Restrictions	Supportive Hands can be configured to only allow access from specific IP address ranges you define.
Transmission Security	All communications with Supportive Hands servers are encrypted using industry standard HTTPS. This ensures that all traffic between you and Supportive Hands is secure during transit. Additionally, for email, our product supports Transport Layer Security (TLS), a protocol that encrypts and delivers email securely, mitigating eavesdropping and spoofing between mail servers.

Additional Security Methodologies

Security Awareness

Policies	Supportive Hands has developed a comprehensive set of security policies covering a range of topics. These policies are shared with, and made available to, all employees and contractors with access to Supportive Hands information assets.
Training	All new employees attend a Security Awareness Training, and the Security Team provides security awareness updates via email, blog posts, and in presentations during internal events.

Employee Vetting

Background Checks	Supportive Hands performs background checks on all new employees in accordance with local laws. These checks are also required to be completed for contractors. The background check includes Criminal, Education, and Employment verification.
Confidentiality Agreements	All new hires are screened through the hiring process and required to sign Non-Disclosure and Confidentiality agreements.

CONTACT US

For further information about our Security overview or Security practices, please contact us using the details set out below:

Derek Brown

Director and Principal Consultant
Supportive Hands Pty Ltd
e: derek@supportivehands.com.au
m: 0415 450 500