Security Architecture & Infrastructure Guide

Overview

Stannp's security architecture is built on enterprise-grade infrastructure designed to protect customer data through multiple layers of defence, comprehensive monitoring, and strict geographic controls. Our infrastructure operates on Microsoft Azure's secure cloud platform, combining modern architecture principles with robust security controls to ensure the confidentiality, integrity, and availability of all data processed through our platform.

Cloud Infrastructure Foundation

Microsoft Azure Hosting

Our entire infrastructure is hosted on Microsoft Azure's Ireland data centres, providing enterprise-grade physical security, environmental controls, and infrastructure management. Azure's infrastructure meets CSA CCM 3.0 standards, ensuring world-class security at the physical and environmental levels.

EEA-Based Infrastructure

For all UK customers, data is stored exclusively on cloud-based servers located in Ireland, within the European Economic Area (EEA). This ensures full compliance with UK GDPR and EU data protection regulations. We do not transfer UK customer data outside the EEA, maintaining complete data sovereignty throughout the data lifecycle.

Multi-Zone Architecture

Our platform leverages multiple availability zones within the Republic of Ireland for high availability and disaster recovery. All redundant systems and backups remain within EEA boundaries, ensuring both resilience and regulatory compliance.

Network Architecture & Segregation

Virtual Network Segregation

Our infrastructure uses separate virtual networks for development, staging, and production environments, ensuring complete segregation of customer data from development activities. Large networks are divided into security domains based on trust levels, with access controlled at each perimeter using firewalls and filtering routers.

Environment Isolation

Development, test, and production environments are completely separated and do not share common components. Each environment operates on separate networks with segregation of administrative duties between development, test, and production teams. This separation ensures

Stannp
Unit 12, Taw Trade Park
Braunton Road, Barnstaple, EX31 1JZ
01271 320 863
www.stannp.com
Stannp Ltd
Company Reg: 09086822
ICO Data Protection Reference: ZA134992

that development activities cannot impact production systems and production data is never exposed to non-production environments.

Customer Data Isolation

Customer data remains completely isolated through multiple architectural layers including unique account IDs for each customer, multi-tenancy architecture with logical separation, network-based tenant separation preventing cross-contamination, and regional separation capabilities for geographic compliance. Each customer's data is segregated from other customers at the platform, network, and storage levels.

Regional Network Architecture

We maintain multiple virtual networks for regionalised areas, ensuring that data remains within appropriate geographic boundaries whilst maintaining network isolation and security. Network-based tenant separation ensures customer data can be segregated by geographic region whilst maintaining the security and efficiency benefits of shared infrastructure.

Security Perimeter & Defence Layers

Multi-Layer Firewall Protection

Our security architecture implements defence in depth through multiple firewall layers. Perimeter firewalls protect all public-facing applications by filtering incoming traffic, blocking malicious IP addresses, and enforcing access control policies. Network firewalls control traffic between security domains, permitting only established connections with all traffic denied by default unless specifically authorised.

Perimeter Security Controls

Wireless networks receive enhanced security treatment with dedicated perimeter firewalls and segregation from internal systems until authentication is complete. All external access points are controlled through secure gateways, with no uncontrolled external access permitted to any network device or system containing customer data.

Intrusion Detection & Prevention

Microsoft Defender provides both host-based and network-based intrusion detection and prevention across our infrastructure. These systems work in concert with our firewalls to detect and block suspicious activity, providing real-time protection against evolving threats.

Data Protection Architecture

Encryption Throughout

All data is protected using industry-leading encryption standards. Data at rest is encrypted using 256-bit AES encryption, providing the highest level of security for stored data within file systems and databases. Data in transit is protected using TLS 1.2 and TLS 1.3 encryption protocols, consistently achieving A+ ratings on Qualys SSL Labs testing.

Cryptographic Key Management

Cryptographic keys are securely managed through Azure Key Vault with strict access controls, ensuring keys remain protected throughout their lifecycle. All keys are protected from modification, loss, destruction, and unauthorised disclosure through centralised, secure key management.

Confidential Data Protection

Confidential data remains within private virtual networks, with all network cabling protected from interception through appropriate physical security measures. Private IP addresses and routing information are never disclosed to unauthorised parties, maintaining the security of our internal network architecture.

Monitoring & Security Operations

Security Information & Event Management (SIEM)

Our SIEM system provides 24/7 monitoring of all network activities continuously across our entire infrastructure. All logs from servers, applications, firewalls, and security devices feed into the centralised SIEM, enabling correlation of events across multiple systems and detection of sophisticated attack patterns.

Comprehensive Audit Logging

Daily automated reviews of comprehensive audit logs cover user activities, system changes, administration activities, access attempts, and security events. All security-relevant events are logged including timestamps, user identities, affected resources, actions performed, and outcomes.

Real-Time Threat Detection

Automated monitoring systems generate real-time alerts for any anomalies or potential security incidents, enabling immediate response. High-risk events automatically alert to the incident management process, generating notifications for repeated authentication failures, unauthorised access attempts, and system errors.

Independent Verification

Third-party service status monitoring and independent uptime monitoring provide objective verification of network availability and security posture. This external monitoring validates our internal monitoring systems and provides additional assurance of service continuity.

High Availability & Resilience

Redundant Infrastructure

We maintain a 99%+ uptime SLA through redundant systems distributed across multiple EEA server regions. Load balancing and failover capabilities ensure continuous service delivery even in the event of individual component failures.

Geographic Separation

All backup data is stored in separate availability zones within the Republic of Ireland. This zonal separation ensures that zone-level incidents or failures do not affect both primary and backup data simultaneously, providing resilience whilst maintaining data sovereignty.

Backup Architecture

Critical data is backed up every 15 minutes with daily full backups and weekly secondary backups. All backup infrastructure maintains the same security standards as production systems, with encrypted storage and zonal separation within EEA boundaries. Backup retention provides 30 days of immediately available recovery points.

Disaster Recovery

Our architecture integrates comprehensive disaster recovery capabilities, ensuring rapid recovery from any infrastructure failure. Recovery procedures are documented and designed for minimal data loss and rapid service restoration.

Access Control Architecture

Network Access Controls

All network access requires specific authorisation following role-based access control (RBAC) principles. Before connecting to our network, devices must be registered in our asset register, maintain current security patches, and run approved anti-malware software.

Authentication Architecture

Systems connecting to the network are authenticated with connections restricted to authorised devices only. Multi-factor authentication (MFA) is mandatory on all systems without exception, providing an additional layer of security beyond traditional username and password authentication.

Privileged Access Management

Administrative access receives session timeouts of 2 hours and additional logging. Administrative duties are segregated from standard operations, with privileged accounts restricted, documented, and never used for routine activities.

Compute & Storage Infrastructure

Scalable Cloud Architecture

Our cloud-based infrastructure scales automatically to handle campaigns of any size whilst maintaining all data within EEA boundaries. From individual mailings to enterprise-level volumes, our architecture supports consistent service quality and performance.

Storage Architecture

Data storage is distributed across multiple Azure storage services with encryption, replication, and geographic separation.

Secure Processing Environments

Customer data files are isolated and processed in segregated environments. All processing occurs within secure, monitored systems with comprehensive logging and access controls, ensuring data remains protected throughout processing workflows.

API & Integration Infrastructure

API Security Architecture

API access is secured through multiple layers including authentication tokens with rate limiting to prevent abuse, HTTPS/TLS encryption for all API connections, detailed access logging for all API activities, and monitoring for suspicious patterns through our SIEM system.

Secure File Transfer

Secure FTP (SFTP) provides encrypted file transfers with full authentication and logging for file-based integrations. All file transfer activities are monitored and logged, maintaining the same security standards as other data transfer methods.

Integration Monitoring

All API and integration activities are continuously monitored through our SIEM system, providing visibility into usage patterns and potential security events. Automated systems detect unusual access patterns, repeated authentication failures, and abnormal request volumes.

Vulnerability Management Infrastructure

Continuous Scanning

Monthly vulnerability scans using Qualys and Security Scorecard identify potential security weaknesses across our infrastructure. GitHub automated vulnerability scanning monitors source code and dependencies for security issues.

Patch Management

The patching status of all endpoint devices and production systems is checked every 30 days. Automated patching is deployed where available, with critical patches applied within 7 days, important patches within 14 days, and moderate patches within 30 days.

Security Testing

Penetration testing by our vulnerability scanning providers supplements continuous automated scans, identifying exploitable vulnerabilities and validating security controls. Monthly web application vulnerability scans test specifically for SQL injection, cross-site scripting, and other common threats identified in the OWASP Top 10.

Stannp
Unit 12, Taw Trade Park
Braunton Road, Barnstaple, EX31 1JZ
01271 320 863
www.stannp.com
Stannp Ltd
Company Reg: 09086822
ICO Data Protection Reference: ZA134992

Web Filtering & Content Control

Protective Web Filtering

Access to websites containing illegal information or known malicious content is automatically blocked. Our web filtering restricts access to known malicious websites, command and control servers, phishing sites, and websites sharing illegal content.

Data Loss Prevention

Information upload functions are controlled to prevent unauthorised data exfiltration. Web filtering works in concert with other security controls to prevent both inbound threats and outbound data leakage.

Compliance & Standards

Regulatory Compliance

Our network security architecture meets PCI-DSS requirements for payment card processing with specific controls for cardholder data environments. All security measures are regularly audited as part of our ISO 27001 certification and undergo continuous review for compliance with UK GDPR requirements.

Industry Standards

Physical data centre security is managed by Microsoft Azure's data centres, which implement comprehensive security controls. Our architecture aligns with industry best practices including OWASP guidelines, NIST frameworks, and NCSC secure architecture principles.

Regular Audits

Infrastructure security is validated through internal audits, external ISO 27001 audits, PCI-DSS assessments, and continuous compliance monitoring. All architectural changes undergo security review to ensure controls remain effective.

Physical Security

Data Centre Security

Physical security is managed by Microsoft Azure's data centres, which implement comprehensive controls including 24/7 security personnel, biometric access controls, video surveillance, environmental monitoring, and redundant power and cooling systems.

Geographic Considerations

All physical infrastructure for UK customer data remains within EEA boundaries, specifically in Ireland. This ensures compliance with data residency requirements whilst benefiting from Azure's enterprise-grade physical security.

Commitment to Secure Architecture

Our comprehensive security architecture ensures customer data is protected through multiple layers of defence, continuous monitoring, rapid vulnerability response, and strict geographic controls. Built

Stannp
Unit 12, Taw Trade Park
Braunton Road, Barnstaple, EX31 1JZ
01271 320 863
www.stannp.com
Stannp Ltd
Company Reg: 09086822
ICO Data Protection Reference: ZA134992

on Microsoft Azure's secure cloud platform with additional security layers and controls, our architecture provides enterprise-grade protection whilst maintaining the flexibility and scalability required for modern mail processing services. All security measures are regularly tested, independently verified, and continuously improved to maintain the highest standards of protection.

Stannp
Unit 12, Taw Trade Park
Braunton Road, Barnstaple, EX31 1JZ
01271 320 863
www.stannp.com
Stannp Ltd
Company Reg: 09086822
ICO Data Protection Reference: ZA134992