Network Security Guide

Overview

Stannp maintains enterprise-grade network security managed on the principle of least privilege with security by design and default. Our multi-layered architecture protects customer data through comprehensive controls, continuous monitoring, and strict access management.

Network Architecture

Our infrastructure uses separate virtual networks for development, staging, and production environments, ensuring complete segregation of customer data. Large networks are divided into security domains based on trust levels, with access controlled at each perimeter using firewalls and filtering routers. Customer data remains completely isolated through unique account IDs, multi-tenancy architecture, and network-based tenant separation. For UK customers, all network infrastructure remains within the European Economic Area (EEA), with data stored exclusively on Microsoft Azure servers in Ireland.

Firewall & Perimeter Protection

Multi-layer firewall protection filters all incoming traffic, blocking malicious IP ranges and common attack patterns. Our firewalls permit only established connections, with all traffic denied by default unless specifically authorised. Wireless networks receive enhanced security treatment with dedicated perimeter firewalls and segregation from internal systems until authentication is complete.

Access Controls & Authentication

All network access requires specific authorisation following role-based access control (RBAC) principles. Before connecting to our network, mobile devices must be registered in our asset register, patched to current security levels, have malware protection installed, have default passwords removed, and, if they have access to any company data, must have a login. Systems connecting to the network are authenticated, with connections restricted to authorised devices only. Private IP addresses and routing information are never disclosed to unauthorised parties.

Encryption & Data Protection

All data in transit is protected using TLS 1.2 and TLS 1.3 encryption protocols, consistently achieving A+ ratings on Qualys SSL Labs testing. Data at rest is encrypted using 256-bit AES encryption. Cryptographic keys are securely managed through Azure Key Vault. Confidential data remains within private virtual networks, with all network cabling protected from interception through appropriate physical security measures.

Monitoring & Threat Detection

Our Security Information and Event Management (SIEM) system monitors all network activities continuously across our entire infrastructure. Automated analysis of comprehensive audit logs covers user activities, system changes, administration activities, access attempts, and security events, triggering alerts for unusual activity that require immediate review. Microsoft Defender provides host-based and network-based intrusion detection and prevention. Real-time alerts enable immediate response to anomalies or potential security incidents. Third-party service status monitoring and independent uptime monitoring provide objective verification of network availability.

Vulnerability Management

Monthly vulnerability scans using Qualys and Security Scorecard identify potential security weaknesses. Monthly web application vulnerability scans test specifically for SQL injection, cross-site scripting, and other common threats. Annual penetration testing by external accredited organisations validates our security controls. Discovered vulnerabilities are patched according to severity: critical within 7 days, important within 14 days, and moderate within 30 days.

Web Filtering & Content Control

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. Information upload functions are controlled to prevent unauthorised data exfiltration.

High Availability & Redundancy

We maintain a 99%+ uptime SLA through redundant systems distributed across multiple EEA server regions. Load balancing and failover capabilities ensure continuous service delivery. All backup infrastructure maintains the same security standards as production systems, with geographically separated storage within EEA boundaries.

API & Integration Security

API access requires authentication tokens with rate limiting to prevent abuse. All API connections use HTTPS/TLS encryption with detailed access logging. Secure FTP (SFTP) provides encrypted file transfers with full authentication and logging. All API activities are monitored for suspicious patterns through our SIEM system.

Compliance & Standards

Our network security meets PCI-DSS requirements for payment card processing, with specific controls for cardholder data environments. Physical data centre security is managed by Microsoft Azure infrastructure, meeting CSA CCM 3.0 standards. All network security measures are regularly audited as part of our ISO 27001 certification and undergo continuous review for compliance with UK GDPR requirements.

Commitment to Network Security

Our comprehensive network security ensures customer data is protected through multiple layers of defence, continuous monitoring, rapid vulnerability response, and strict geographic controls. All network security measures are regularly tested, independently verified, and continuously improved to maintain the highest standards of protection.