Virus & Malware Protection Guide

Overview

Stannp implements comprehensive anti-virus and anti-malware protection across all IT assets to ensure business continuity and protect customer data from malicious software threats. Our multi-layered defence strategy combines preventive measures, continuous monitoring, and rapid response protocols to maintain a secure operating environment.

Comprehensive Protection Coverage

All workstations, servers, and mobile devices under Stannp's control run approved and up-to-date anti-malware products that continuously monitor for malicious software including viruses, worms, trojans, ransomware, and other threats. Anti-malware protection is mandatory across all systems without exception, ensuring consistent security standards throughout our infrastructure. Our anti-malware solutions are enterprise-grade, regularly updated with the latest threat definitions, and configured for maximum protection whilst maintaining system performance.

Continuous Monitoring & Scanning

Anti-malware software is configured for on-access scanning, monitoring file downloads and opening, folders on removable or remote storage, web page access, and email attachments. Regular automated scans run at least daily across all systems, ensuring comprehensive coverage beyond real-time protection. Windows Defender provides enterprise-level protection as our primary anti-virus management solution, integrated with Microsoft's global threat intelligence network. All scanning activities are logged and monitored, with alerts generated for any detected threats or suspicious activities.

Multi-Layer Defence Strategy

Our malware protection operates at multiple levels across our infrastructure. Email security includes Microsoft Exchange anti-spam and anti-malware protection filters scanning all emails and attachments before delivery, blocking known malicious content at the gateway level, and quarantining suspicious attachments for analysis. Web protection prevents users from accessing known malicious websites through malware protection software and content filtering functions, blocks access to command-and-control servers and phishing sites and inspects web traffic for malicious content. File system protection monitors all file operations in real-time, scans removable media upon connection, and validates software authenticity before installation.

Operating System & Patch Management

All systems run supported versions of operating systems with the latest available security patches applied. This ensures that known vulnerabilities cannot be exploited by malware seeking to compromise systems. Our patch management process ensures timely deployment of security updates, with critical patches applied within 7 days of release. Automated patch deployment

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

minimises the window of vulnerability whilst maintaining system stability through staged rollouts and testing.

Network-Level Protection

Devices connecting to the Stannp network must meet security standards including running approved anti-malware software, having current security patches installed, and being free from known infections. We reserve the right to disconnect any device from the network if an infection is found or suspected. Disconnected devices remain offline until the infection is removed and suitable preventative tools have been installed, protecting the broader network from contamination. Network segmentation isolates critical systems, limiting the potential spread of any malware that evades initial defences.

Threat Intelligence & Prevention

Our anti-malware solutions integrate with global threat intelligence networks, receiving real-time updates about emerging threats, new malware variants, and attack techniques. This intelligence enables proactive blocking of threats before they reach our systems.

Incident Response & Reporting

Any suspected malware infections are reported immediately to our technical and compliance teams. Our incident response process includes immediate isolation of affected systems, analysis to determine infection scope and method, complete malware removal and system cleaning, verification that all threats have been eliminated, and investigation of how the infection occurred to prevent recurrence. All malware incidents are logged, analysed, and used to improve our defences through lessons learned processes.

Software Installation Controls

Software installation requires approval from our compliance team, preventing installation of unauthorised or potentially malicious applications. Users must verify the authenticity of software from internet sources before installation. Applications arriving on unsolicited media must not be installed under any circumstances. This controlled approach prevents trojan horses and other malware disguised as legitimate software from compromising systems. Only software from trusted, verified sources is permitted on our network.

Email Security

All incoming and outgoing emails are scanned by Microsoft Exchange anti-spam and anti-malware protection filters before delivery. Attachments are inspected for malicious content, with suspicious files quarantined or blocked. Phishing emails are identified and filtered based on content analysis, sender reputation, and link inspection. Users are educated to recognise phishing attempts and social engineering tactics that attempt to bypass technical controls through human manipulation.

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

Removable Media Protection

Removable storage devices including USB drives, external hard drives, and optical media are scanned upon connection to any Stannp system. On-access scanning prevents malware from executing when files are opened from removable media. Strict controls over removable media usage, combined with comprehensive scanning, prevent this common malware vector from compromising our systems.

Integration with Security Infrastructure

Our anti-malware protection integrates with our broader security infrastructure including Security Information and Event Management (SIEM) systems for centralised monitoring, intrusion detection and prevention systems, firewalls and network access controls, and vulnerability management processes. This integration ensures malware protection works in concert with other security controls, providing defence in depth against sophisticated threats.

Regular Testing & Validation

Continuous vulnerability scanning combined with regular penetration testing by our security vendors provides comprehensive validation of our security defences. Testing identifies vulnerabilities and coverage gaps requiring remediation, ensuring our security controls remain effective against current threats.

Compliance & Standards

Our virus and malware protection supports compliance with ISO 27001 information security management requirements, PCI-DSS malware protection standards for cardholder data environments, UK GDPR requirements for appropriate technical measures, and industry best practices for malware defence. All anti-malware measures are documented, regularly reviewed, and updated to address evolving threats.

Commitment to Malware Protection

Our comprehensive virus and malware protection ensures customer data and systems remain protected against malicious software threats through continuous monitoring, multi-layer defence, regular updates, rapid incident response, and integration with our broader security infrastructure. These measures maintain a secure environment for all customer data and business operations.

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