WHITE PAPER

# FirmGuard® Secure Connectivity

## PROTECTING YOUR DATA IN TRANSIT WITH MODERN TLS STANDARDS

### Overview

At FirmGuard, security is foundational. We are committed to ensuring that every connection between your devices and our platform is protected using industry-standard encryption protocols. This document outlines how FirmGuard leverages modern Transport Layer Security (TLS) configurations, advanced cipher negotiation, and secure load balancing infrastructure to keep your data safe in transit.

### End-to-End TLS Encryption

All communication between customer endpoints and the FirmGuard platform is encrypted using HTTPS (TLS). TLS provides confidentiality, integrity, and authentication for data transmitted over the internet.

FirmGuard uses AWS Application Load Balancers (ALBs) to handle TLS negotiations. These ALBs are configured with managed security policies that define:

- Supported TLS protocol versions
- Approved cipher suites
- Handshake behavior and encryption standards

During each connection, the client and load balancer negotiate the strongest mutually supported protocol and cipher to establish a secure session.

### Supported Protocols and Cipher Suites

FirmGuard supports modern and secure versions of TLS:

- TLS 1.3 is preferred for all connections
- TLS 1.2 is supported for compatibility with legacy systems
- Deprecated versions (TLS 1.0/1.1, SSL) are explicitly disabled

**Our configuration prioritizes:**

- **Forward Secrecy (FS):** Prevents session keys from being recovered, even if long-term keys are compromised
- **Strong Cipher Suites:** Only algorithms vetted for modern cryptographic strength are allowed
- **Secure Negotiation:** TLS handshakes follow strict ordering to prevent downgrade attacks

These configurations are consistently applied across all FirmGuard environments.

### Secure Load Balancing Architecture

FirmGuard's TLS infrastructure is deployed within a compliant, cloud-based environment.

- Encryption standards remain up to date
- Known vulnerabilities are mitigated
- Configurations align with leading compliance frameworks, including:
- NIST SP 800-52r2

FirmGuard

- PCI DSS
- ISO 27001
- HIPAA

We continuously monitor and update encryption policies to reflect evolving security best practices.

## Session Resumption and Replay Protection

FirmGuard supports secure session resumption mechanisms to balance performance with protection:

- TLS 1.3 uses Pre-Shared Keys (PSK)
- TLS 1.2 uses session IDs and session tickets for resumption

Resumption is only allowed when reconnecting to the same load balancer IP address. To mitigate replay risks:

- 0-RTT data (early data in TLS 1.3) is not implemented
- The Extended Master Secret (EMS) extension is used in TLS 1.2 to strengthen session integrity

These measures reduce the attack surface while maintaining fast, secure reconnections.

## Policy Governance and Access Controls

FirmGuard enforces strict controls around TLS configuration management:

- Only AWS-managed security policies are used to ensure consistency and compliance. Custom policies are intentionally not used.
- Access to policy configuration is governed by IAM roles and AWS Organizations SCPs.
- Policy selection is restricted and centrally enforced to maintain consistent security across all environments.
- We apply the principle of least privilege to reduce risk and ensure only authorized personnel can manage encryption settings.

## Data Stored

FirmGuard only retains the information necessary to deliver and secure its services effectively.

Categories of data collected include:

- General Endpoint Information: Firmware and hardware information.
- Management Portal User Information: Email addresses, user roles, and authorization properties within the FirmGuard application.
- Network Information: IP addresses of systems connecting to the FirmGuard platform.

**Exclusions:**

- FirmGuard does not store passwords in plaintext, nor does it store unnecessary user information such as Social Security Numbers**.**

## Where This Data Is Stored

All information is stored in Amazon Web Services (AWS) within the us-west-2 region. Services used for data storage include:

- Amazon Cognito – authentication and user identity management
- Amazon RDS – relational data and metadata storage
- Amazon S3 – object and log storage

All data is stored in three or more physical Availability Zones for redundancy. Customer data is logically separated to prevent data leaks.

## Data Encryption

All data in transit is protected by TLS 1.2 or TLS 1.3 (as described above).

Data classified as sensitive or secret (including network logs, BIOS passwords, etc.) is stored at rest using AES-256 encryption through SSE-S3 and AWS KMS for row-level encryption.

## Governance

Access to FirmGuard's backend data is strictly controlled and auditable.

Internal roles with access include:

- Administrator / OrganizationAccountAccess
- Deployment, Monitoring, and Billing Teams

Access is granted by demonstrated need and job title, following the principle of least privilege. Role and access information is logged and monitored via AWS CloudTrail.

Temporary Access Procedures:

Users may be given temporary access through a process where that access is confirmed, documented, and audited via CloudTrail.

***Conclusion***

***FirmGuard ensures that all data transmitted and stored within our ecosystem is protected using state-of-the-art encryption, access control, and governance practices. With support for TLS 1.3, AES-256 encryption, AWS KMS-based key management, and comprehensive audit logging, FirmGuard delivers robust protection for data fully aligned with modern compliance and security expectations.***

FirmGuard