OptConnect Security FAQ

What is OptConnect's core mission regarding connectivity?

OptConnect's mission is to provide Global Cellular Connectivity, Simplified, built upon a robust, multi-layered security framework.

How does OptConnect approach security for its services?

OptConnect engineers its services with a security-first mindset. We deliver a fully managed, secure connectivity solution that removes the burden of security management from customers through a comprehensive, layered defense strategy.

Where does the OptConnect infrastructure reside?

OptConnect's infrastructure leverages the robust security capabilities of Amazon Web Services (AWS).

How does OptConnect ensure network segmentation in the cloud?

OptConnect uses Virtual Private Cloud (VPC) segregation for AWS subnets, thereby creating logically isolated network segments to limit the lateral movement of potential threats.

What encryption standards does OptConnect use for data in transit?

All public-facing web services enforce a minimum of TLS 1.2 to ensure data is securely encrypted in transit.

What encryption standards does OptConnect use for data at rest?

All data stored within OptConnect systems is protected with strong AES-256 encryption or higher.

How does OptConnect protect customer uptime and data integrity?

OptConnect maintains a robust internal backup and recovery program. We perform daily snapshots of internal systems, retain backups for at least one year, and perform annual restoration tests.

How does OptConnect manage and respond to threats?

OptConnect partners with a third-party SOC partner for 24 x 7 x 365 monitoring and response, uses centralized logging into a SIEM platform, and subscribes to Managed Detection and Response (MDR) services.

How long are network flow and firewall logs retained by OptConnect?

Network flow and firewall logs are retained for over one year.

Does OptConnect follow strong password policies internally?

Yes. All user accounts require passwords with a minimum length of 15 characters, including upper-case letters, lower-case letters, numbers, and special characters.

Is Multi-Factor Authentication (MFA) enforced internally at OptConnect?

Yes, Universal Multi-Factor Authentication (MFA) is enforced for all users without exception.

How does OptConnect manage user access privileges?

OptConnect adheres to the Principle of Least Privilege and conducts regular access reviews to ensure user permissions are appropriate for assigned roles.

What is OptConnect's policy on account lockout and deprovisioning?

Accounts are automatically locked for one hour after five failed login attempts, and user account deprovisioning is immediate upon employee termination.

How does OptConnect safeguard endpoints and systems?

OptConnect employs a next-generation EDR platform, deploys critical security patches within a 7-day timeline, configures automatic operating system updates, and uses Full Disk Encryption (FDE) with AES-256 or higher on all managed endpoints.

What system hardening and process controls does OptConnect enforce?

Company devices are configured with a 15-minute screen lock timeout, and the use of portable USB storage devices is restricted by corporate policy.

How does OptConnect provide secure remote access to its network?

Remote access is provided via an SSL VPN, which enforces the use of the TLS 1.2 protocol for strong encryption.

How does OptConnect handle sensitive credentials?

Sensitive credentials, such as API keys and database passwords, are securely stored and managed to prevent exposure in code or configuration files.