InfoSec Software for Secure Voice and Video Calls This design focuses on InfoSec software specifically for voice and video call applications, emphasizing robust security measures to protect customer information and access controls against future attacks.Identity and Access Management (IAM): Strengthen user authentication and authorization with: Multi-factor authentication (MFA) is like one-time codes (SMS, app authenticators) combined with passwords.Software Suite: Real-time Encryption: This core functionality encrypts all communication streams (audio and video) using strong protocols like AES-256 with individual encryption keys for each call session.Data Loss Prevention (DLP) Integration (Optional): Integrate DLP to scan call metadata and chat messages (if applicable) for sensitive data (e.g., credit card numbers, social security numbers) and prevent accidental leaks.Acceptable Use Policy (AUP): Define acceptable call practices, prohibiting activities like call recording without consent or using the platform for illegal purposes.Meeting Security Policy: Outline procedures for securing video calls, like requiring meeting passwords, restricting screen sharing permissions for participants, and disabling features like file transfer if not needed.Additional Considerations: Penetration Testing: Regularly test the call application for vulnerabilities in encryption protocols, access controls, and signaling channels.Compliance Management: Stay updated on relevant data privacy regulations (e.g., GDPR, CCPA) and ensure your InfoSec program adheres to them.Endpoint Security with Call Control: Extend endpoint security to manage devices used for calls: Enforce application whitelisting to restrict unauthorized calling apps.Threat Intelligence: Subscribe to threat intelligence feeds to stay updated on .emerging threats targeting communication platforms