REALVNC®
original equipment manufacturer

The Remote Access Integration **Security Checklist**

For Medical Device Manufacturing Companies

About This Checklist

For businesses embedding remote access capabilities directly into their products, security is paramount. Secure remote access not only protects your customers and their sensitive data, but also safeguards your reputation and ensures regulatory compliance.

Use this checklist to evaluate the critical security measures necessary when implementing embedded remote access within your products, and discover how RealVNC can support you in delivering secure, reliable, and robust solutions.

The Security Checklist for Medical Device Manufacturers

Security Consideration	What is it?	Why it Matters	Best Practice	How RealVNC Addresses This
Encryption	Encryption protects sensitive data both in transit and at rest, preventing unauthorized access or interception of data transmitted remotely.	Protects sensitive data from unauthorized access or interception, ensuring privacy and compliance.	Utilize robust, end-to-end encryption (AES-256, TLS 1.2+) with Perfect Forward Secrecy to secure sensitive data. Regularly verify encryption effectiveness and standards compliance.	RealVNC Connect uses full end-to-end AES-GCM encryption (128 or 256-bit) with Perfect Forward Secrecy. Web API calls use at least TLS 1.2, ensuring secure data transit.
Strong Authentication & Access Controls	Robust authentication and access controls ensure only authorized personnel can remotely access devices or systems, significantly reducing unauthorized access risks.	Prevents unauthorized access, protecting patient safety and confidentiality.	Implement multi-factor authentication (MFA) combined with Single Sign-On (SSO). Use granular, role-based access controls and enforce strong authentication protocols consistently.	RealVNC provides default two-factor authentication (email-based/TOTP), supports SSO, mandates separate local/domain credentials for remote sessions, and offers brute force protection, granular permissions, and gatekeeping controls.

Security Consideration	What is it?	Why it Matters	Best Practice	How RealVNC Addresses This
Compliance with Regulatory Standards	Regulatory compliance ensures adherence to mandatory standards and frameworks specific to medical device and healthcare industries, minimizing legal and financial risks.	Essential for legal compliance, preventing costly fines, reputational harm, and patient risks.	Regularly review industry-specific compliance standards (e.g., HIPAA, GDPR, ISO 27001) and conduct routine compliance audits. Incorporate regulatory requirements into solution design and operational processes.	RealVNC holds ISO/IEC 27001:2013 and Cyber Essentials certifications, complies with GDPR and CCPA, and supports compliance frameworks such as HIPAA, PCI-DSS, and EU NIS2 directives, addressing key healthcare regulatory standards.
Device Security by Design	Integrating security throughout the product lifecycle reduces vulnerabilities, ensures ongoing security, and prevents costly redesigns or security retrofits post-deployment.	Reduces vulnerabilities and security risks throughout the device lifecycle, avoiding costly security breaches.	Adopt a Secure Development Lifecycle (SDL) approach. Regularly perform penetration tests, white-box audits, vulnerability assessments, and third-party security evaluations during development and post-release.	RealVNC employs a formal Security Development Lifecycle, including penetration tests, white-box audits, software composition analysis, vulnerability remediation, and periodic third-party security audits to ensure product security.
Supply Chain and Infrastructure Security	Protecting against supply chain threats involves securing third-party components, suppliers, and underlying infrastructure that could be leveraged to compromise security.	Prevents risks introduced by third-party vendors or infrastructure compromises, protecting overall system integrity.	Conduct thorough security assessments of third-party vendors and components, manage your infrastructure directly where possible, and avoid unnecessary reliance on external providers, especially for critical security infrastructure.	RealVNC owns and controls its infrastructure directly, avoiding public cloud providers (AWS, Azure) for critical services. No third-party vendors have access to their core infrastructure, minimizing supply-chain security risks.
Continuous Security Education and Awareness	Ongoing training and education help prevent security breaches by equipping employees with current knowledge about threats, vulnerabilities, and security best practices.	Empowers teams to prevent security breaches by recognizing threats and applying best practices effectively.	Offer continuous security training and awareness programs tailored to remote-access threats. Regularly update teams on evolving threats, new vulnerabilities, and best security practices.	RealVNC provides continuous security education through webinars, documentation, and security best-practice resources, enabling ongoing awareness and proactive security management among users and administrators.

RealVNC OEM Solutions: Embedded Remote Access You Can Trust

RealVNC's OEM Solutions empower security-conscious companies to embed powerful, secure remote access directly into their products. Whether you're developing medical devices, digital signage, visual displays, maritime navigation systems, or advanced vehicle technologies, our OEM Solutions provide the flexibility and robustness needed to meet demanding security and compliance standards.

Key Features & Benefits:

Fully Customizable SDK: Seamlessly integrate RealVNC technology tailored precisely to your product's unique requirements.

Advanced Security: Industry-leading AES encryption, multi-factor authentication, detailed audit logs, and secure communication channels.

Enhanced Performance: Optimized remote connectivity for reliable, high-performance operation even under challenging network conditions.

Flexible Integration: Easy embedding into diverse technology environments, ensuring rapid deployment and faster time-to-market.

Scalability: Built to support devices and deployments of any scale, from individual products to extensive global solutions.

Expert Support: Dedicated OEM specialists provide guidance and support throughout development, deployment, and beyond.

Transform your products with secure, reliable, embedded remote access from RealVNC.

Ready to explore what RealVNC OEM Solutions can do for you?

Visit realvnc.com/oem to learn more and request your consultation today.

Listen to our exclusive podcast realvnc.com/podcast