flow

Dec 2024

Data Security Questions to Ask Your Vendors

(Before You Have a Data Breach)

for

Manufacturers, Reps, and Distributors

Prepared by

James Thomas
CTO, Flow RMS

Curtis Seare
CEO, Flow RMS

Table of Contents

Introduction

When it comes to data security, asking the right questions is half the battle. Manufacturers, reps, and distributors face unique challenges in managing sensitive data, and the vendors you choose can either safeguard your business or leave it wide open to attack.

This guide cuts through the noise and delivers a no-nonsense list of questions you should ask your vendors. These aren't vague "trust us" inquiries. They're clear, actionable, and designed to make sure your vendors are doing their job to protect your data.

If they can't answer confidently and show their work? That's a red flag. This isn't just about compliance—it's about protecting your reputation, your customers, and your bottom line.

Top Priority Questions

These are foundational security elements that must be addressed first. If your vendor cannot meet these basic standards, the rest of the security measures may not matter. They form the backbone of a secure system.

1. Is your system SOC 2 certified?

Can you provide a copy of the most recent SOC 2 audit report and the key findings?

2. How do you handle data encryption?

Is the data encrypted both at rest and in transit? What encryption standards do you use (e.g., AES-256)? Are these encryption protocols regularly updated?

3. Are all security patches up to date?

Can you provide the date of the last patch applied, and how do you ensure your system stays current with critical security updates?

4. What security monitoring do you have in place?

Are you using real-time monitoring systems to detect suspicious activity? Can you provide examples of how you handle potential threats and security incidents in real time?

5. Do you conduct regular penetration testing?

Can you provide the most recent penetration test results and demonstrate the steps to address any vulnerabilities found?

6. What is your incident response plan?

How quickly can you respond to a security breach? What specific steps are taken during incident handling, and how is communication managed with customers in case of a breach?

7. Can you prove that all third-party libraries and dependencies are up to date?

Show a recent report or log demonstrating no outdated or vulnerable libraries, frameworks, or dependencies are used.

8. How do you manage software updates and security patches?

What is your patch management process? How frequently are security updates applied, and how do you test them before deployment?

9. What security headers are enabled on the platform?

Can you show evidence of headers such as Content-Security-Policy (CSP), X-Content-Type-Options, and X-Frame-Options being configured? Are they actively monitored and updated?

10. How do you protect sensitive data, such as database credentials?

Are sensitive credentials encrypted or stored in a secure vault? How is access to these credentials controlled, and who has access to them?

Mid Priority Questions

These questions ensure that vendors are proactive about their security, with ongoing assessments, response protocols, and system-level access control. While not as critical as foundational elements, these measures are key to maintaining security over time.

1. Is the login page secured with HTTPS?

Can you show proof of an up-to-date SSL/TLS certificate? How do you ensure all data transmitted through your login page is encrypted?

2. How do you manage user access and authentication?

Does your system support multi-factor authentication (2FA) for all users? How do you ensure proper role-based access control (RBAC) to restrict access based on user roles?

3. Do you conduct regular security audits, both internal and external?

When was your last audit conducted, and can you provide evidence of actions taken to address any recommendations or concerns?

4. How are third-party vendors or integrations vetted for security?

What security assessments do you conduct for third-party integrations, APIs, or services used within your system?

5. What is your process for applying emergency security patches?

Can you give an example of how quickly a critical vulnerability was identified and patched in the past?

Mid Priority Questions

6. How do you handle data backups?

Are backups encrypted and secured? How frequently are backups performed, and what's the process for restoring data in case of a breach or system failure?

7. How do you manage API security?

What measures are in place to protect against API abuse or vulnerabilities? How do you secure API keys and ensure proper access control for API usage?

8. What is your process for notifying customers in the event of a data breach?

How do you handle breach notifications, and within what time frame can customers expect to be informed of any incidents?

Lower Priority Questions

These are still important but are more about maintaining and fine-tuning your system's security. They deal with specific technical policies or legal/regulatory compliance, and while they might not directly impact immediate security threats, they ensure longer-term risk mitigation.

1. Do you support secure password practices?

Can you demonstrate that the system enforces strong password policies (e.g., requiring complex passwords, expiration policies, etc.)? How do you handle password recovery?

2. What processes are in place to ensure data integrity?

How do you ensure that data stored, transmitted, or processed within your system is accurate and secure? What checks and balances are in place?

3. How do you manage permissions for customer data access?

Can you demonstrate how access to sensitive customer data is restricted and tracked? How do you ensure only authorized personnel can view or modify sensitive information?

4. Are your systems compliant with GDPR, CCPA, or other relevant data privacy regulations?

Can you provide evidence of compliance with major data privacy regulations? How is customer data handled in compliance with these laws?

Lower Priority Questions

5. What are your policies regarding data retention and deletion?

Can you outline your data retention policy and explain how you securely delete customer data when it’s no longer needed?

6. Do you conduct regular vulnerability scans?

How often do you perform vulnerability scans on your system? Can you provide results from recent scans and evidence of how vulnerabilities were remediated?

Conclusions

Asking tough questions isn’t about being difficult; it’s about being smart. Your business depends on data security, and the stakes couldn’t be higher. If your vendors can’t give you clear, actionable answers, it’s time to rethink your partnerships.

The good news is that you’re setting a standard for excellence in your industry by holding vendors accountable and focusing on these critical security elements. You’re not just protecting data—you’re building trust with customers, partners, and stakeholders.

Remember: security isn’t a one-time checkbox. It’s an ongoing conversation. So, keep asking the hard questions, stay informed, and demand better. Your business—and your peace of mind—deserve nothing less.

Dec 2024

About the Authors

James Thomas

CTO, Flow RMS

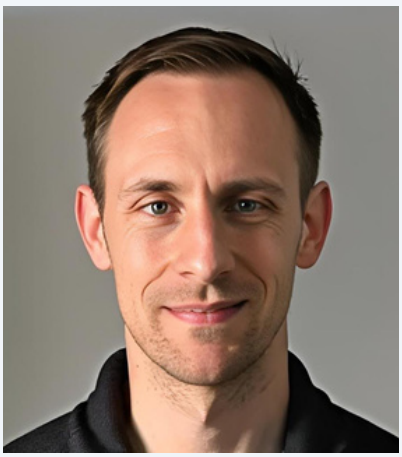
Follow on LinkedIn

James Thomas is the CTO and co-founder of Flow RMS, specializing in data security, artificial intelligence, and scalable enterprise-grade software. Previously, he built secure, data-driven technologies for United Health Group, addressing the complex needs of a global market. He also co-founded Data Crunch, a Fortune 5000 data consultancy, and helped lead it to a successful acquisition in 2023. With a passion for innovation, James drives Flow RMS's vision for AI-powered transformation across industries.

Work with James

Get a demo of Flow: FlowRMS.com

Subscribe to the Flowing Sales podcast: FlowingSales.com



Curtis Seare

CEO, Flow RMS

Follow on LinkedIn

Curtis Seare is the CEO and founder of Flow RMS, a company building the AI-First ERP for manufacturers, reps, and distributors. He co-founded Data Crunch, a Fortune 5000 data consulting firm acquired in 2023, and hosted the Popular Data Crunch Podcast, where he explored AI and data science in business innovation. With a focus on efficiency, Curtis leads AI-powered transformation in industrial sectors.

Work with Curtis

Get a demo of Flow: FlowRMS.com

Subscribe to the Flowing Sales podcast: FlowingSales.com