The broker's guide to evaluating software security

Your roadmap to choosing software that protects what matters most

Insurance brokers protect some of the most sensitive information out there, personal details, financial records, confidential business data for clients.

As the industry evolves, so do the security challenges. Many brokers choose software based on features and price because nobody teaches you how to evaluate security credentials. It's not your core expertise, and it shouldn't have to be.

This guide is designed to help you ask the right questions and confidently choose a software partner who takes security as seriously as you take client service.

Why security matters more than ever

When you choose a software platform, you're not just buying a tool. You're partnering with someone to help protect your firm's most valuable assets - your clients.

Modern cloud-based platforms can offer better security than most brokerages could achieve on their own. You get enterprise-grade protection without needing an IT department.

Strong security protects:

Client trust - Your reputation is built on reliability and confidentiality. Strong security helps you maintain that trust for decades to come.

Regulatory compliance - Privacy laws continue to evolve to better protect consumers. The right software partner helps you stay ahead of these requirements without complexity.

Business continuity - With proper security and backup systems, you can focus on serving clients instead of worrying about system downtime or data loss.

The opportunity: Choosing secure software is a competitive advantage that lets you serve clients with confidence.

JAVLN

The broker's guide to evaluating software security

Common security gaps and how modern platforms solve them

Most security challenges are everyday issues modern software can help prevent. The right platform should already have safeguards built in.

Access management (who can see what)
Up-to-date platforms use multi-factor authentication (MFA) and role-based access controls to ensure only the right people can access sensitive data. This helps prevent:

- Unauthorised access
- Former staff retaining logins
- Accidental exposure of confidential information

Human error (mistakes happen)
People are one of the biggest risk factors in any business. Modern systems reduce risk by:

- Providing prompts and warnings
- Limiting actions based on role
- Creating audit trails that track activity

Good software is designed to support people, not catch them out.

Integration security (your tools working together)
Brokers rely on multiple systems - email, document storage, accounting tools, and CRMs. Secure cloud platforms:

- Integrate safely with tools like Microsoft 365
- Control how data moves between systems
- Maintain consistent security standards across integrations

Staying current (without the hassle)
Security threats change constantly. Cloud-based software helps by:

- Automatically deploying security updates
- Fixing vulnerabilities quickly
- Reducing reliance on manual updates

This means you're always protected with the latest safeguards, without disrupting day-to-day work.

The insight: You don't need to become a security expert. You just need a software partner who has already solved these challenges for you.

The broker's guide to evaluating software security

The certifications that show serious commitment

You don't need a technical background to evaluate security. You just need to look for recognised certifications that prove your vendor has been independently verified.

Here are the credentials that demonstrate a vendor is committed to protecting your data:

STANDARD	WHAT IT MEANS FOR YOU
SOC 2 Type II	Independent auditors have verified that security controls work consistently over 6-12 months. It's proof of ongoing commitment.
ISO 27001	The international gold standard for information security management. This shows a vendor has systematic processes for protecting data.
Data residency (AU/NZ)	Your data stays in Australia or New Zealand, ensuring compliance with local privacy laws and giving you peace of mind about data sovereignty.
Regular penetration testing	The vendor proactively tests their security by having experts attempt to find vulnerabilities and fixes them before they become issues.

Good to know: This level of compliance requires significant investment, ongoing audits, and demonstrates a long-term commitment to security.

The broker's guide to evaluating software security

Your 10-point security evaluation checklist

Use these questions when evaluating any software vendor.

Clear, confident answers show you're dealing with a partner who can support your business.

1. Is MFA mandatory?
Multi-factor authentication dramatically reduces the risk of unauthorised access. Modern platforms make this seamless for daily use.
Ask: "Is MFA required for all users?"

2. Is data encrypted at rest and in transit?
Encryption ensures your data is protected whether it's stored on servers or being transmitted. This is standard in quality platforms.
Ask: "What encryption standards do you use for stored and transmitted data?"

3. Does it align with the Essential Eight?
For Australian brokers, alignment with the ACSC's Essential Eight framework shows the vendor understands local security best practices.
Ask: "How do you align with the Essential Eight cybersecurity framework?"

4. Is there an immutable audit trail?
Every action should be logged in a way that creates a clear, unchangeable record. Thi protects you and makes compliance straightforward.
m provide a complet

JAVLN

The broker's guide to evaluating software security

4. Is there an immutable audit trail?
Every action should be logged in a way that creates a clear, unchangeable record. This protects you and makes compliance straightforward.
Ask: "Does your system provide a complete unchangeable audit trail for actions?"

5. Where is the data stored?
Local data storage in Australian and/or New Zealand data centres helps you meet privacy requirements and often provides faster access to your information.
Ask: "Where are your servers located, and do you offer Australian and/or New Zealand data residency?"

6. Are backups automated and protected?
Automated, secure backups mean you can recover quickly from any incident without data loss or extended downtime.
Ask: "How are backups handled, and how quickly can data be restored?"

7. Is there a clear incident response plan?
Quality vendors have documented processes for handling any security events, including how and when they'll communicate with you.
Ask: "What's your incident response process, and how do you keep customers informed?"

The broker's guide to evaluating software security

8. How are security updates managed?
Cloud platforms can deploy security updates seamlessly, ensuring you always have the latest protections without disrupting your work.
Ask: "How do you handle security updates and patches?"

9. Is consent tracking built in?
With regulations like Australia's informed consent requirements, automated tracking and storage helps you stay compliant effortlessly.
Ask: "How does your system help manage consent tracking and record retention?"

10. Is security built into the foundation?
Security should be core to how the platform was designed, not added on later. This ensures comprehensive protection across all features.
Ask: "Was security designed into the platform from the beginning?"

What to look for in vendor responses

Strong vendors will:

- Share certifications readily and offer to show reports under NDA
- Provide specific, clear answers about their security practices
- Explain how they help you meet your compliance obligations
- Discuss their security roadmap and ongoing improvements
- Welcome security questions as signs of informed buyers

The broker's guide to evaluating software security

How JAVLN approaches security

Security as a foundation, not a feature.

At JAVLN, we've built security into our cloud products so you can focus on what you do best - advising clients and growing your business.

Here's how we support your security needs:

- SOC 2 Type 2 certified for both JAVLN Platform and JAVLN Officetech
- Enterprise-grade encryption protecting data at rest and in transit
- Multi-factor authentication for all users
- Role-based access controls ensuring people only see what they should
- 24/7 security monitoring with dedicated incident response
- Regular penetration testing to stay ahead of emerging threats
- Local data hosting options for complete data sovereignty

Want to see our SOC 2 report? We're happy to share it under NDA. We believe transparency builds trust. Because we take your clients' data seriously.

Ready to evaluate your options?

Use this checklist when reviewing your current system or exploring new platforms.

Read more about SOC 2

Next steps

Let’s talk about how we can support your business and help you choose software you can trust.

Contact our team