axway

CHECKLIST

4 questions to gauge the security of your MFT software

There's no letting your guard down when it comes to managed file transfer (MFT) security. With data breaches on the rise, businesses can't afford MFT software that takes shortcuts. You need to ask tougher questions of MFT software vendors. That way, you'll have a better sense of your MFT software's configuration. You'll also better understand the review process to defend against security attacks.

Ready to get to the bottom of whether your MFT software can handle today's data breach crisis? Ask these four questions:

01 Does your vendor have an internal security team?

Having a dedicated security team helps MFT software vendors stay vigilant. They can use software development lifecycle tools and processes to identify risks. Verify that they check for prominent attack vectors and perform threat modeling. Container and attack surface scans are also important. If it operates as an independent group, this team is in a good position to push back to make sure MFT software is secure.

02 Is third-party testing done in a customer environment?

The testing of MFT software should happen in an environment that mirrors a customer's deployment. These environments come with unique security configurations and controls and environment-specific vulnerabilities. Third-party testing in a similar environment validates MFT software security in the real world. A more accurate assessment lends itself to a better security posture.

03 Does your vendor prioritize continuous education and training?

MFT security threats and best practices continuously evolve. As they do, your MFT software vendor must stay up-to-date. It can come in the form of regular company-wide training on security. It can also be regular check-ins with the executive team and vendors to monitor where threats are most prevalent. Broadening their awareness allows MFT software vendors to raise the bar in their security posture.

04 Is a security bar included as part of the release lifecycle?

Using the latest versions of MFT software is critical from a security perspective. At the same time, it's valuable to know the security bar that underscores each software release. A vendor should test use cases and scenarios, taking note of any nuances introduced that may require additional testing. They should also ask customers to perform tests in their ecosystem, with their data flows. The same sentiments should apply to the cloud security bar.

New security threats have undoubtedly raised concerns over MFT security. But with the right infrastructure (software included), people, and processes, businesses can safeguard their MFT operations in this dynamic landscape.

Learn more about the steps you can take to safeguard your MFT operations

Watch the on-demand webinar →