Security isn't on the list, it is the list.

Companies looking to adopt or replace their procurement solutions need to think not only of how it will help them obtain goods and services, but how it will protect the critical information involved in every purchase. Will it keep transaction data secure? Will it keep outsiders out of your account information? Will it also protect your suppliers?

These are the types of questions you have to consider as you evaluate your procurement options, and the six security features that follow should be the first things you ask about.

Protecting procurement.

6 security features to look for when looking at new solutions.
Data Encryption:
Can anyone break this code?

If access is the first line of defense, data encryption is second. A close second. To protect information from getting into the wrong hands through a leak or by breach, the solution you choose needs to wrap your data in multiple layers of protection.

• The first layer protects your data when it’s stored on your servers.

• But because data doesn’t sit still, the second layer – called TLS, for Transport Layer Security – covers you every time data passes from your server to that of a supplier, distributor, customer, or other partner.

• Finally, a third layer of encryption secures your database, so even people with access can’t see more than they should, and hackers who get their hands on a file won’t be able to open it.

You should also make sure your solution uses public “keys” that allow anyone involved to encrypt your data, as well as private keys, which are held by a single individual or solution to decrypt data when it’s received.

Access & Identity:
Do you know who you’re dealing with?

Access is the issue here, and you need to know exactly who can get into your system. Because when employees are coming in from everywhere via the cloud, you need to be able to identify each and every one of them.

Multi-factor authentication is critical, and any new system you employ needs to provide this level of security – ensuring that anyone who wants to access the system needs to provide two or more credentials to authenticate their identity.
Key & Secret Management:
Can you control who can collaborate?

Procurement is about bringing buyers and suppliers together to get business done – but it also involves finance and inventory and other internal audiences – and keeping those integrations secure is crucial.

Collaboration on this level can’t be based on credentials; usernames and passwords of a hundred different administrators can easily be stolen, so this level of integration requires certificates to preserve security.

Digital certificates, such as Secure Sockets Layer (SSL) and TLS, securely encrypt the identities of people and resources across networks, providing confidential communication between systems.

Critical Monitoring & Alerting:
Who’s watching?

You need to know who’s accessing your system and what they’re doing while they’re there. This allows you to monitor any unusual activity and keep a clear data trail if issues arise.

Make sure the solution you choose accurately logs all access and actions, storing them securely and supporting you with active monitoring – a central operations center for spotting and solving problems. And be sure it meets the unique local and international requirements of your industry, as regulations dictate how long these logs must be kept.
Secure SDL Practices: Is the solution itself secure?

The code your new solution is built upon should be tested – and retested – for any security issues, and the developers should complete three levels of security development lifecycle (SDL) processes, including:

- Static code analysis, in which scanning the code itself identifies any vulnerabilities.
- Open source analysis, which scans any open source code used in the software for vulnerabilities and licensing issues.
- Dynamic application security testing, with which the application itself is examined, as it’s running, for any potential issues or vulnerabilities.

It’s also recommended to perform routine “ethical hackings” of the solution, where an authorized, simulated cyberattack is performed to gauge the security of the system.

Incident & Breach Protocols: What do you do first?

If someone somehow taps into your system, it is critical that your solution offers a clear and thorough process for responding. Look for partners who provide best-practice manuals or frameworks – something you can put in place immediately and easily follow that’s designed specifically for procurement.

So in the event a breach occurs, you can instantly spot it, stop it, and resolve the issue for every party involved.
A system that connects you to buyers and suppliers but doesn’t protect the people, processes, or data involved isn’t actually a solution. It’s a problem no company can afford. Ask the questions posed here, and make sure the provider you choose can prove how they’ll protect you.

**But first, take a moment to see how SAP takes on procurement security.**