secberus

Three Principles for Building Best-of-Breed Enterprise Security Architecture

To build leading-edge cloud security and enterprise architecture, our collective focus needs to shift away from ***technical tools*** and toward ***governance***. Best-of-breed security architecture isn't built on point solutions; it's built on business-driven policy, contextualized perspective, and solid relationships between stakeholders.

Read on for three important principles to keep in mind as you design your enterprise security architecture.

Principle One

Best-of-breed security architecture is consciously designed.

The digital-enabled marketplace moves quickly and enterprises have to keep their edge in order to compete. As you implement methodologies and technologies to accelerate your business, your security architecture needs to keep up. And keeping up requires more than just flavor-of-the-day point solutions; it requires consciously designed security governance that supports the accelerated pace of digital business.

Building security by design means:

- Making ***everything*** secure—no blind spots, no guesswork.
- Staying squarely focused on delivering business value.
- Communicating risk to the organization using business language so that everyone in the enterprise understands security in the context of the business.
- Having a dashboard view that gives everyone in the security landscape consistent, contextual, silo-busting visibility into your security posture.

Principle Two

Context is fundamental to security governance.

It's not a stretch to say that any one security job is really three in disguise. Enterprises feel the pinch: a chronic shortage of expertise, an ever-accelerating business pace. This is one of the many reasons we love security dashboards. A dashboard that shows each security stakeholder the aspects of your security posture that are most relevant to them provides the context and perspective people need to make fast, informed security decisions and live slightly less hectic work lives.

There's a lot of everyday technology out there that shows us the value of context—like the literal dash displays of newer-model cars that show you how fast you're going alongside the speed limit for the road you're driving on. This contextualized view helps you adjust your behavior in real-time.

Similarly, security stakeholders should be able to understand security information in the context of the policies of their environment. With that contextual perspective, you can then use exceptions and automated controls to manage the business's security needs without the decision friction that often slows things down.

Security context has two layers:

Security-as-business: Define security policy according to your enterprise's desired business outcomes. In other words, the business mandates policy.

Policy-as-code: This business-contextualized policy is then encoded, ensuring that violations reach the correct owners with enough information to address them according to the needs of the business.

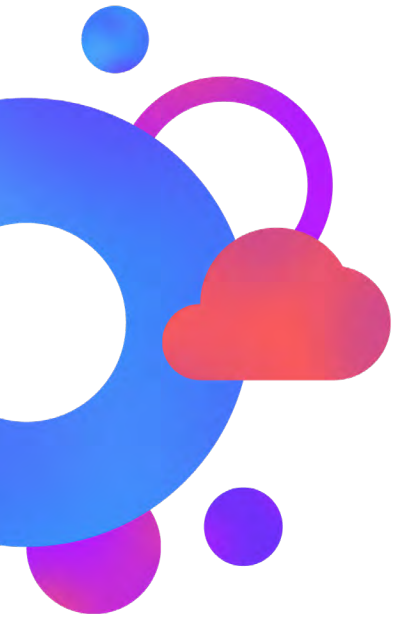
Principle Three

Your security architecture reflects the quality of your internal and external stakeholder relationships.

When it comes to implementing security solutions, the biggest cultural hurdles in most organizations are ***lack of trust*** and ***fear***. The best way to address these issues is to deliver value and operate with transparency. Build transparency right into your workflow; let other stakeholders know when security issues change, or when your needs have changed—especially if it affects existing expectations.

Most of all, don't focus on technology to the detriment of relationships. Every stakeholder is trying to solve problems to help your enterprise. Security-related technology is some of the most complex technology out there, and best-of-breed architecture often boils down to the quality of the relationships between those building it.

Your relationship with your solution providers is particularly important, since their technology forms part (or all) of the backbone of your architecture.



The solution provider and the enterprise should evolve together. Enterprises should be open, transparent and communicative with their providers—and willing to look honestly at whether their providers are still serving the needs of the enterprise. Solution providers need to take special care to adjust their solutions to fit the needs of not only the market but also the enterprises using their products. They must also be able to prove value for both current customers and future users. And they must stay connected with their users on all levels—not just security or technology.

Ready for a deep dive into governance?

The future is in the cloud. And since all businesses are running a speed-to-market race, inevitably all businesses will be part of the cloud migration. Businesses that understand this right now have the advantage of getting their cloud governance framework right and will avoid getting lost in the flurry of new technology that's coming. As you build your cloud governance strategy and your security architecture, keep these three principles top of mind.

Want to explore cloud governance even more?
Let's talk.