



## Jason Schmitt

GENERAL MANAGER,  
SYNOPSYS SOFTWARE  
INTEGRITY GROUP

**Jason Schmitt combines security domain knowledge with expertise in delivering software-as-a-service (SaaS) and cloud-based solutions to transform how companies build and deliver software, helping them accelerate innovation while addressing business risk. He has held leadership roles at Aporeto and led enterprise security products at Hewlett-Packard as vice president and general manager of ArcSight and Fortify.**

## Software Risk Is Business Risk. It's Time for the C-Suite to Act.

It has been said that every business is a software business. But what does that mean? Becoming a software business entails both reward and risks. The reward is a competitive edge; the risks are often misunderstood and poorly managed at the highest levels of leadership. In this interview, Jason Schmitt explains what business and technology leaders must do to achieve successful business transformation and take control of the risks that are inherent in software.

### How is digital transformation changing companies' relationship with software?

Companies are not undertaking digital transformation for its own sake. Digital transformation is the means by which companies are seeking competitive advantage. Software is the enabler. The goal is not to create more digital assets but to apply the power of technology to effect transformation, either by automating current processes or by creating new customer experiences. Software introduces new ways of doing business, but it also introduces risk.

### What are the software risks companies are facing today?

The risks include poor software hygiene, security, and reliability, and they arise because companies do not prioritize security when developing, procuring, and managing their business-critical software. It's important to establish trust in how your software was designed, built, and tested — whether it was developed in-house or procured from a third party — because once you deploy or use the

software, you own the risk that comes with it. Software vulnerabilities can expose customer data and intellectual property and result in financial and legal risk. Seemingly innocuous flaws or oversights can quickly escalate into existential threats to a business. Reputational, financial, and legal damage can result if risk is not controlled.

### How does open source software factor into these issues?

Open source is not inherently risky, but it helps to have transparency. For example, where was the software developed? By whom? Open source has exploded in popularity in recent years, because it helps bootstrap digital transformation. But when you adopt software and make it a crucial part of running your business, you need to know how it was developed, its quality, and its reliability.

### What can technology leaders do to ensure control over their software?

The important thing is to prioritize risks by weighing your exposure to the potential for damage and what you can tolerate, based on what is necessary to run the business. Some pillars of risk such as laws and regulations are nonnegotiable. You need to quantify and qualify your tolerance and exposure objectively. Risk-based prioritization lets you focus on what matters most, so security does not become an impediment to business velocity.

Sponsored  
content



SYNOPSYS®

Leaders need to manage their software as a business-critical asset that carries risk throughout its entire lifecycle.



#### **How can companies mitigate the problem without slowing down their business or limiting innovation?**

Corporate leaders need to focus on their business goal, which is to develop competitive advantage. The first step is to recognize that software risk is not just a technology problem; it's a business problem. You need to understand that software can compromise the integrity of the organization's customer relationships and market position. You need to put processes in place that address the risks inherent in software, very early in the process — as soon as software is introduced into the organization. This is the case whether you are developing the software yourself, buying it off the shelf, downloading it from an open source distribution, or even outsourcing and paying someone to develop it. Identifying these issues earlier in the process allows companies to move faster and innovate to gain strategic advantage.

#### **How does Synopsys help its customers address software risk?**

Most software security companies are reactive — after it's too late. We turn that upside down, by offering a more holistic approach that establishes trust early and maintains it so businesses can stop reacting and instead focus on driving the business forward. Leaders need to manage their software as a business-critical asset that carries risk throughout its entire lifecycle. Synopsys helps companies pull security into the process much earlier, establishing it in the foundation of the software and the processes used to develop it. By creating a systematic way of developing your software and evolving it reliably, it becomes a trusted asset rather than something that is suspect by default.

For more insight into managing software risk, visit [Synopsys](https://www.synopsys.com).