Vanta

Shift Left:

How to Turn Security into Revenue

Introduction

For many SaaS businesses, “InfoSec” is a term that can send a shiver down anyone’s spine. Enormous spreadsheets, complex questions, and delayed deals have been the name of the game for the Sales and InfoSec relationship.

> We’re living in the time of a security revolution—one that calls for a different landscape entirely, where security evolves from a cost center into an asset.

Forward-thinking security professionals and progressive sales leaders are joining forces to create a better future for the state of InfoSec at software companies and beyond—a future where security is a bullet point in everyone’s job description, executives position security as a revenue-driving investment, and Trust Centers are standard practice for buying and selling software.

The most successful companies are now treating security as a critical aspect of the buyer journey. By applying the traditional DevOps principles of Shifting Left, teams are positioning security as a differentiator instead of a hurdle, and centering security in their sales conversations at every stage.

What you’ll learn:

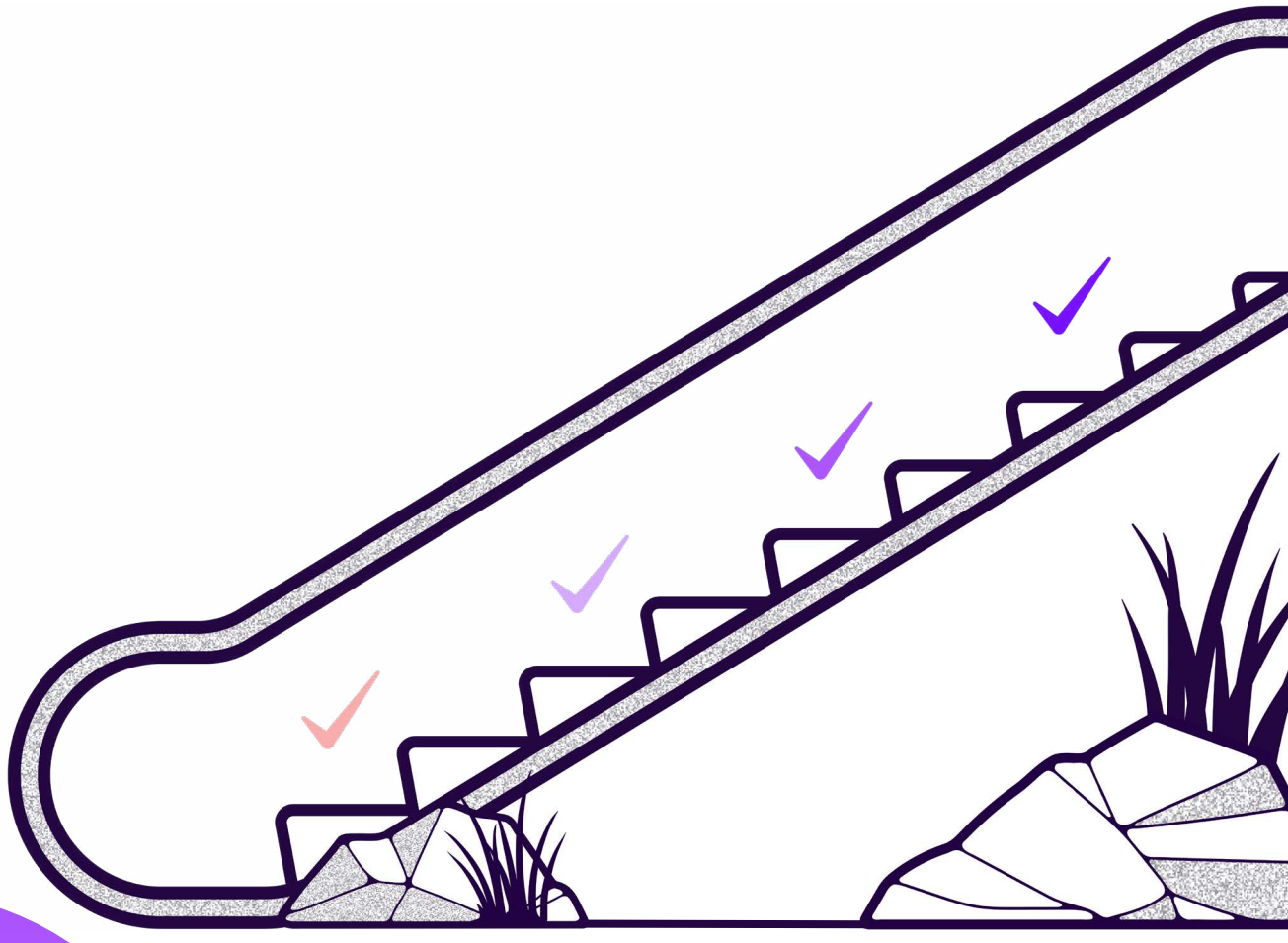
How to educate prospects and customers early and remove roadblocks to closed revenue later in the deal.

What is “shifting left”?

The term shifting left originated from engineering teams who observed inefficiencies in the Waterfall Methodology. They hypothesized that by distributing testing throughout the entire development cycle, they could produce more reliable code at a faster pace. This hypothesis often proved true, and teams began iterating on software development through methodologies like Agile and Scrum.

Shifting left refers to incorporating quality assurance testing earlier (or further left) in the software development process. This means engineers are moving away from linear design and development cycles where testing and validation are tacked onto the end of the cycle. Instead, testing is distributed throughout each stage of the development cycle, rather than waiting until the software is nearly complete to begin checking quality.

It is important to note that “shifting left” does not just mean moving testing to the beginning of the process. It means distributing testing throughout the entire development cycle, testing products earlier and more often, and producing more reliable code as a result. Overall, “shifting left” is a key practice in modern software development proven to improve efficiency and quality.



How does the Shift Left apply to security and go-to-market teams?

If you map the traditional sales cycle alongside the software development cycle, you're left with striking similarities. Buyers are often talking to your sales team for weeks or months, then you suddenly find yourself in the midst of a hundred-question questionnaire that could bring your security deal to a screeching halt.

Imagine, however, if you enabled buyers to educate themselves on your security policies and removed roadblocks earlier in their buying journey.

You certainly don't want to spend months nurturing a deal that is doomed to fail because of a lack of alignment on InfoSec policies, and buyers similarly don't want to waste months evaluating a product only to find out their compliance team won't allow them to sign the contract.

> Shifting left allows you to identify security concerns or vulnerabilities early on, giving your team time to mitigate those risks before the prospects become clients, or, worse, closed-lost prospects.

How can an organization introduce security earlier in the sales cycle?

Any strong vendor relationship is grounded in trust—trust that your software can achieve a goal, trust that data is protected, and trust in your organization as a whole. When someone chooses to outsource a significant process to you, they are trusting you to be as good as, or better, than their internal IT and security processes in order to earn that trust.

In every company, there are actors (perhaps hiding) behind your champion who get paid to identify risk and stop the deal. Their sole job is to vet vendors, so as to not introduce risk into their environments, or to effectively mitigate the risks they decide to let in. The reality is that without the approval of these actors, you cannot sell your software. They are just as much a part of your buying team as is your champion—so why not treat them like they are part of the buyer's journey as early in the process as possible?

If we tell good security stories with the right documents, evidence, and artifacts, we can help our champions diffuse any risk conversations by making trust the first thing we talk about in a relationship. When you shift these conversations left early in the process to win vendor security, you speed up sales cycles and actualize revenue faster.

Security as a feature, not a bug

Security is an operations practice—we can all agree on that. But security is also a communication practice, a legal practice, and a revenue ops practice. We don't report security outcomes in terms of "viruses stopped" or "firewall events analyzed" because no one really understands the ways this impacts the business's bottom line.

When we report on the success of security in terms of revenue outcomes, we help a broader audience understand the tangible impact of the security program we've built. In turn, we're helping leaders across business units understand the monetary value we're adding to the organization.

When you visit a website for a software product, everything about the product is outlined. Use cases, feature pages, and more. But we rarely see a page with much information about security. At best, companies who make this information available attempt to present technical information via marketing language and brand speak. Knowing that buyers evaluate security as a critical part of their purchasing process, why not treat security as the core product feature throughout the customer experience?

There are a few ways that you can begin to enable g revenue growth based on your product's security features, including building a culture around your security story, investing in your security story, and publishing a Trust Center.

Building a culture around your security story

Instead of creating a siloed security team, making security a bullet point in everyone's job description is the most authentic way to build and articulate your security story. While a CISO is responsible for setting the standards for your security program, upholding and communicating these standards are a company-wide obligation.

Everyone on your team is responsible for creating value within your security program, so build a culture that encourages that. Security awareness training is important, but ultimately the culture must go deeper than a monthly required course. Talking about security often, without jargon, and across functions within your organization is a great way to start. To learn more about how to achieve this, explore additional resources on **building a strong security culture**.

Investing in your security story

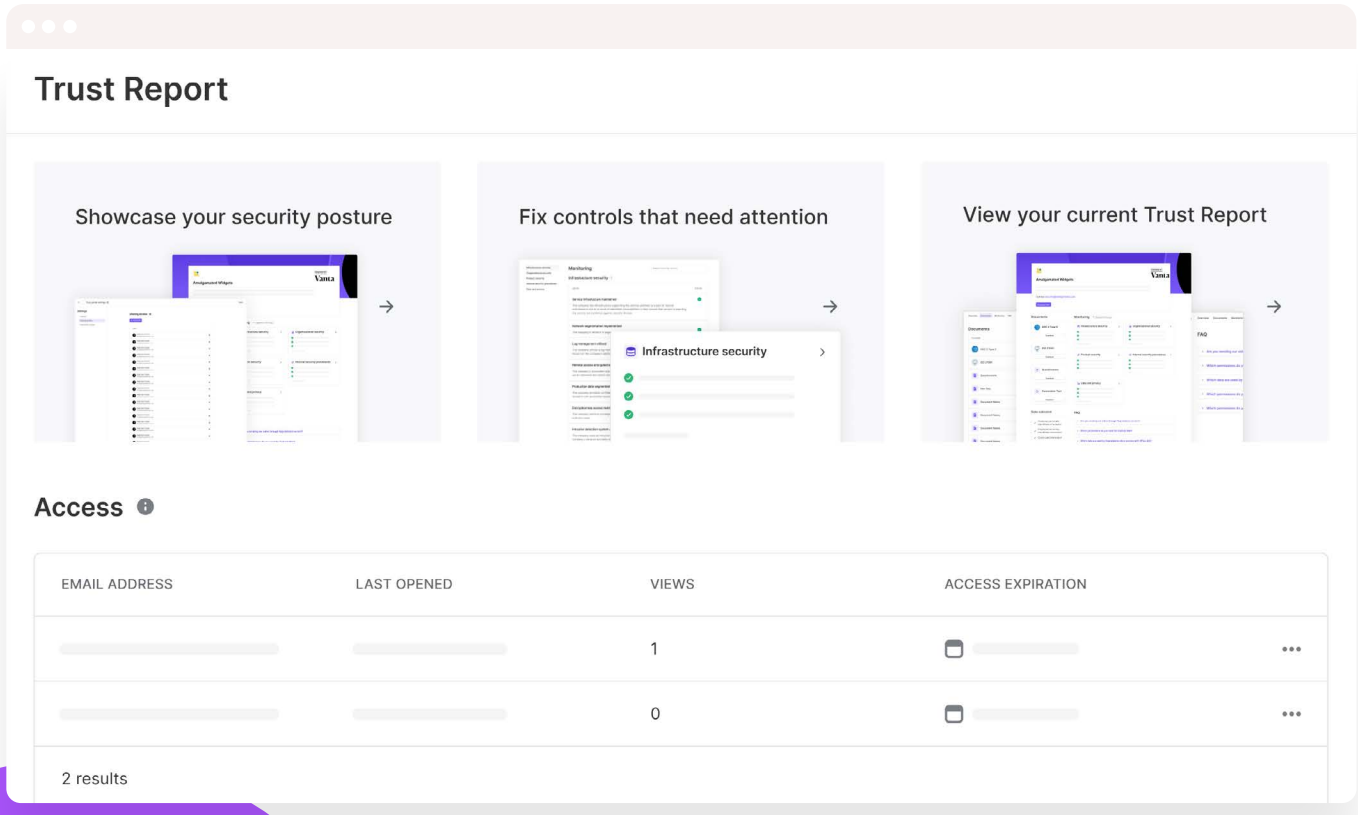
Revenue teams' ability to get a security persona onboard is limited by an organization's investment in security. Business leaders have been taught that security teams are a cost center to be minimized, but are surprised when the lack of investment results in a lack of meaningful stories to tell about product security.

Sure, having strong security policies can prevent data leaks that hurt your brand and harm your clients. But how are you telling the story of your security strengths throughout your brand today?

Investing in your security story means enabling buyers to access security-related information early in the process, even when they're only engaging with your marketing content. Then, they're able to send detailed, trustworthy information back to their procurement, diligence, and security teams, showing them everything they need to know before they'll approve a purchase.

Publishing a Trust Center

The less you lean into telling your security story, the bigger the questionnaire coming your way at the end of the sales cycle. By providing comprehensive information on your security policy via self-serve documentation, you enable prospects and customers to do the work of evaluating your security posture on your behalf, perhaps before they even start the sales process. Beyond building more confident buyers earlier in your sales cycle, this also enables your security team to spend more time working on security rather than just talking about it.



Questionnaire Automation

Being able to leverage existing security policies and previous responses from a Trust Center ensures accuracy and consistency when you do have to respond to security questionnaires. Forward-thinking leaders understand the value of automation, which can be a differentiator for success in today's competitive business landscape. Automating security questionnaire responses streamlines the process, saves time, and improves your chances of winning deals. It also helps you stay organized by providing a centralized location to store and retrieve responses, which ultimately improves efficiency.

The future of security is here—and here to stay

In the competitive landscape of software business, optimizing processes and leveraging efficiencies can make a significant difference in building a strong pipeline and closing revenue faster. Telling a security story at scale is the next step in the evolution of software businesses across every niche.

As security becomes a cornerstone of the buying and selling journey, increased transparency and improved security policies will lead to better data protection. But perhaps more importantly, improving your transparency in security will help you close more deals and generate revenue quickly in the short term.

Vanta

Vanta is the leading trust management platform that helps simplify and centralize security for organizations of all sizes. Thousands of companies rely on Vanta to build, maintain and demonstrate trust in a way that's real-time and transparent. Founded in 2018, Vanta has customers in 58 countries with offices in Dublin, New York, San Francisco and Sydney.

REQUEST A DEMO

VANTA.COM