

The Five Pillars of Long-Lasting Customer Trust

Customer trust isn't won in a single deal. It's earned through consistent patterns customers can see and verify over time. These five pillars are the foundation of security relationships that last: each one makes your posture easier to understand, faster to evaluate, and harder to doubt. Build on all five, and every security review becomes a smoother conversation.

01 Transparency

Transparency makes your security posture easy to understand and evaluate. In practice, that means:

- Centralizing key artifacts—SOC 2 reports, ISO certifications, security policies, architecture diagrams, and penetration test summaries—in one organized place.
- Presenting that information in plain language, with context a non-technical stakeholder can follow.
- Giving buyers a coherent story about how you protect data, manage risk, and respond to incidents.

A transparent approach cuts repeat questions and shows customers that security is built into how you operate.

A Trust Center gives you a centralized, customer-facing hub for approved security, compliance, and risk documentation, so you share your posture clearly and consistently.

02 Proactivity

Trust erodes when customers only hear from you after something breaks, or when they have to chase you for basic security information. Proactive trust-building means:

- Publishing current security documentation before buyers ask for it.
- Flagging new certifications, completed audits, and improved controls as they happen.
- Communicating quickly during incidents or disruptions, including your response plan and remediation steps.

Customers judge you on patterns over time, and a proactive posture makes every review faster.

With Drata, teams use Trust Center updates and AI Questionnaire Assistance to keep customers informed and cut the manual back-and-forth of security reviews.

03 Connectivity

Connectivity is about how security information flows between your teams and your customers. For GRC and security leaders, that means:

- Giving sales, customer success, and account teams one repeatable path to route security questions to a single source of truth.
- Replacing scattered email threads and ad hoc document sharing.
- Delivering a consistent experience whether a buyer is evaluating you for the first time or reviewing your posture at renewal.

Done right, trust becomes an ongoing conversation, and your internal teams stop duplicating each other's work.

Drata's Trust Center backs this with a self-service destination for security information, while AI Questionnaire Assistance helps teams handle complex or custom reviews at scale.

04 Control

Control is about how sensitive security information gets shared. It means:

- Defining who can access which documents, such as gating SOC 2 reports or penetration test summaries behind NDA acknowledgment.
- Setting time-bound or role-based access to sensitive artifacts.
- Tracking who viewed, downloaded, or shared each document.

That protects your organization and gives legal, procurement, and leadership a clear record of what went out and to whom.

A Trust Center gives you granular control over what stays public and what stays private, with the option to require verified business emails or NDA acknowledgment before access.

05 Insight

Once transparency, proactivity, connectivity, and control are in place, the last step is knowing whether the program works. Insight means:

- Measuring how often prospects and customers open your security documentation.
- Identifying which artifacts—SOC 2 reports, ISO certifications, policy summaries—buyers value most.
- Tracking how your trust investments affect sales cycle length, renewal rates, and questionnaire volume.

Those signals tell GRC leaders where to invest next, whether that's a new framework, sharper documentation, or more automation.

Drata's Trust Center analytics show security and sales teams how buyers engage with shared artifacts and tie that engagement back to pipeline and revenue.