The New Trust Standard

A paradigm for the trusted technology relationships of tomorrow

Contents

Executive summary

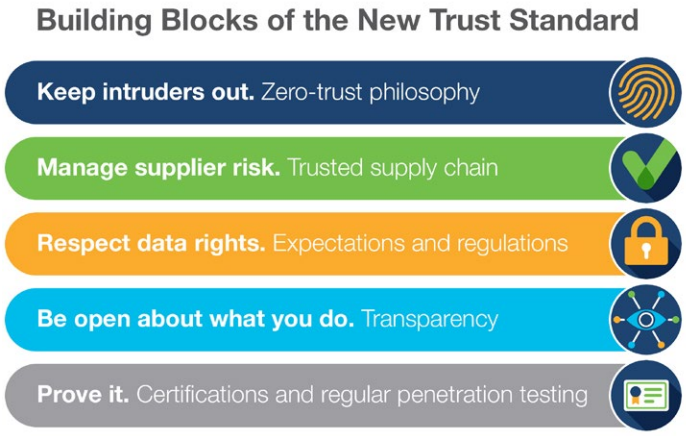
Can your customers trust you with their data? How do they know?

Trust used to come down to a handshake. A promise from one person to another. But business has become too complex to base trust solely on personal relationships. Customer trust has come to depend on the security and transparency of the whole organization—your products, services, personnel, processes, ethics and values, internal systems, suppliers, and contractors. Whether customers can trust you depends not only on your policies, but also your suppliers—and your suppliers' suppliers. Not only on your cybersecurity, but also what you do when a breach does occur. Not only on how you store customers' private data, but also how you respond to a request from foreign law enforcement on a Friday afternoon.

In today's digital economy, an objective benchmark for assessing trust is vital. It requires full transparency. Data flowing over the internet—sometimes into a provider's cloud—includes sensitive data like login credentials, government ID numbers, financial information, trade secrets, business plans, and critical infrastructure details. If sensitive information gets into the wrong hands, consequences can include privacy breaches, loss of intellectual property, interruptions to operations and revenue, the lights going out, and even threats to national security.

The time has come for a New Trust Standard. It's a compilation of what we've heard in conversations with thousands of customers around the world, over years. The New Trust Standard is a framework for expectations and accountability—where businesses and their customers can agree to new rules for trusted digital relationships.

Trust isn't about one thing, like encryption, certification, or supply chain oversight. It's about a combination of things. What those are will surely change over time in response to evolving customer expectations, technology, cyber threats, and international data governance. Read on for key elements of the New Trust Standard today.



"Not only do our customers need innovation more than ever, but they also want partners they can trust."

Chuck Robbins
Chairman and CEO, Cisco

Keep out intruders—“zero trust” philosophy

Verify every connection, every device, every time

Skeptical, curious, detail oriented. These are the job requirements for security pros because trust begins with healthy suspicion. As the name implies, zero trust is a philosophy to “never trust, always verify.”

When selecting a business, a zero-trust mindset means questioning the organization’s security practices and policies. The New Trust Standard says you’re entitled to ask—and to expect—clear answers. If your business handles sensitive data, a zero-trust mindset means always questioning your assumptions. Are customers who they say they are? Are their devices secure? Does application A have a valid reason to talk to application B?

The decades-old approach to access control and a virtual private network (VPN) no longer holds up. It assumes that any device connecting from inside the corporate network can be trusted. And that once a user and device pass a checkpoint, it’s safe to let them connect to multiple applications without re-authenticating. Today neither of these assumptions holds true. A personal laptop or tablet used for work might have picked up an infection at home. A device that’s clean at 8:00 a.m. might be compromised at 8:03 a.m. after a phishing attack. With data storage and processing distributed at the network’s edge, there’s no longer a central castle to surround with a moat. What’s more, beyond authorizing connections from user devices to servers, IT teams also need to check whether connections between applications, devices, and sensors are allowed. Case in point: something that looks like a security camera has no business connecting to a customer database.

The modern approach to access control is a zero-trust architecture. It treats all resources as if they were external. Verifies trust before every access attempt. And grants access only to the required resource. That’s true even if the request comes from the CEO’s office. Even if the device’s security posture was checked 30 seconds ago when it connected to a different application.

Zero trust principles

- Keep the customer experience top of mind. Authentication shouldn't be a burden. Users need convenient access to on-premises and cloud applications to do their work.
- Continually verify that users, devices, and applications are trusted.
- Use machine learning to identify login attempts that deviate from the user's typical behavior. False positives happen, so weigh the risks of blocking legitimate access attempts.
- Match the strength of the application security policy to the sensitivity of the data. This requires accurate data classification. It also requires an understanding of what normal application traffic looks like so that deviations can be spotted.
- Secure connections between different application components, such as the application logic and database.
- Make it harder for attackers who gain access to one server to move to others. Techniques include network segmentation, strong authentication and encryption, and marking trusted devices.

Manage supplier risk

Trust that the provider has built a trusted supply chain

When you buy a car, you trust the manufacturer to take reasonable measures to vet the quality of supplier parts like brakes and seatbelts. Likewise, customers expect their service providers to know all components in their products, and to take reasonable steps to detect and mitigate vulnerabilities that could lead to data manipulation, espionage, disruption, and counterfeiting.

That's a tall order. Cloud service providers typically use third-party software for payment processing, authentication, data management and storage, etc. Even proprietary code generally includes open-source components contributed by people from around the world, and many of these components have multiple nested components.

What's "reasonable" for supplier controls keeps evolving. Triggers for change include new types of threats, new industry practices, and cybersecurity advances.

Recommended supply chain practices

Defend against modification. Run a program to make sure solutions bearing your name are genuine, operate as customers direct them, and are not controlled or accessible by unknown parties.

Require suppliers to adhere to the right standards. Work with your third-party suppliers to assess, monitor, and improve their security practices. Industry standards are a good starting place. Examples include NIST 800-53 for security and privacy controls, ISO/IEC 27001 for information security management, ISO 27018 for protecting personally identifiable information (PII) in public clouds, and ISO 27701 for privacy information management.

Establish a chain of confidence. The ultimate is requiring software and hardware suppliers to document the lineage, or provenance, of their products. Like a passport, this record shows everywhere the product has been, from design and build through manufacturing and delivery. Software suppliers document where code was built, who signed it, components used for identity management, where the code was compiled, etc. Hardware suppliers record details such as the serial number for each printed circuit board assembly and who boxed it up.

Build trust into the contract. Hold suppliers accountable to the same security and privacy standards that you commit to uphold. Set requirements for vulnerability testing and reporting. Include language in the contract to protect customers' data after a supplier relationship is terminated—for example, by requiring the return or destruction of that data.

Test integrations with your own or other vendors' products. Make sure the integration didn't create a new vulnerability.

Conduct regular audits, including vulnerability testing. Work with the supplier to create a plan for vulnerability identification and remediation. Write the response plan into the contract.

Respect data rights

Stay ahead of evolving customer expectations and government regulations

Customers expect providers to keep their data protected and secure, this is a fundamental requirement of trust in the digital world. Beyond that, customers want to be informed about how their data is collected, used and managed, and ultimately, customers want control of their data. This desire for visibility and control goes across any data relationship, from an individual engaging on social media to a hospital storing medical records to an enterprise using cloud-based collaboration services. Increasingly, consumers will make decisions about their providers with privacy and transparency in mind.

Customer expectations

To trust their provider, customers generally want assurance on these points:

- Our content is ours
- It's subject to the same laws we are
- It's accessible only to people we authorize and expect

Customers are reliant on, and generally amenable to, government regulations aimed at protecting privacy. International data governance[1] refers to the collective global laws, regulations, and norms associated with data protection, data privacy, data sharing, and data use. The New Trust Standard holds that service providers should be transparent about their approach to data sovereignty—that is, the concept that data is subject to the laws of the nation where the data is collected. Privacy laws have been enacted in more than 130 countries which seek to establish the standard of care applicable to personal data collected within their borders. Examples include the EU General Data Protection Regulation (GDPR), India's Personal Data Protection Bill, and Thailand's Personal Data Protection Act.

While the specifics of these laws vary, the concerns behind them are universal. One is the belief, true or not, that data is safer in one's own country, protected by their country's own laws. Another is concern that law enforcement, whether foreign or domestic, might compel a service provider to turn over customer data without the customer's knowledge or involvement. Companies using cloud services need to weigh these risks against the benefits of the cloud—quick adoption, scalability, and ongoing innovation.

Ways to limit exposure of customer data

Apply technical controls. Minimize the data you collect, and retain it only as long as the business need or legal requirement. Use strong encryption and access control to protect customer content.

Use legal controls. If governments request access to customer data, first try redirecting the requester to the customer or data owner. Invoke the available legal process to challenge requests that unjustifiably encroach on privacy or other customer rights.

Be strategic about data center locations. Consider how locating data centers in different parts of the world will affect customers. Done right, data governance controls can improve the overall user experience—for example, by giving customers some measure of control over their content and how they manage data. If possible, consider allowing customers to choose the region where their data is stored to meet their sovereignty, privacy, or latency requirements.

The future of data: digital sovereignty

The same technology that enables our internet-powered, interconnected world also has created complexities about data sovereignty. Countries are reacting to the digitization of their economies, and the vast trove of data that it creates, by relying on the concept of sovereignty to assert supreme authority over data to ensure the control and protection of their data. "My data, my law" is now the new norm. Around the world, new data frameworks point to national barriers to the movement of data, access to data, use of data, and storage of data.

Though well-intended, this narrow approach threatens to diminish the economic benefits made possible through modern technology. A new and forward-looking framework must emerge — one that reinforces both the rights of data owners and national sovereignty, but relies on technology, not just the law, to achieve that end. Advanced encryption, confidential computing, obfuscation, and other emerging privacy enhancing technology (PETs) and techniques carry the promise of creating a model for digital sovereignty within a secure, open, and vibrant internet.

[1]Data Governance Principles for the Global Digital Economy, Center for Strategic & International Studies

Be transparent

Disclose all information necessary for customers to make informed choices

Transparency happens when material facts about an enterprise are made available to customers in a timely and efficient manner.

Transparency goes beyond complying with regulations regarding disclosures. It's being open about how you handle business operations, customer content and privacy information, including:

- What data you collect—and how you use and protect it
- How you honor data subject rights
- Key details of your policies about disclosing breaches and security vulnerabilities
- How you respond to government requests for data
- What your business continuity plans are

In general, a transparent company is confident that its handling of data is fair, ethical, and responsible. Takes the right steps to protect customer data and respect privacy. And is willing to be public about the policies, processes and technology it uses to secure data. Recent headlines have made companies more aware of the financial and reputational costs of inadequate security.

Ways to increase transparency

Make it easy for customers to find the information they're seeking. Ask customers what they want to know—and then provide it without making them look for it. Use simple and clear language.

Publicly disclose all critical vulnerabilities. That applies whether the vulnerability is discovered internally or by a third-party. Help customers understand and manage risk.

Notify all people materially affected by a breach at the same time. The right to transparency applies equally to every customer affected, no matter their size or industry.

Advocate for customers when governments request data. Show that you follow the law and that you will try to protect customer information from unlawful requests. When it's legally allowed, notify the customer about the request. Wherever possible, the request should go directly to the customer, not the IT service provider. When asked by your customer, help them preserve or produce the requested content.

> *"When security issues arise, it's important that customers understand how they will be addressed. Fulfilling this promise requires a strict process to manage the receipt, investigation, and reporting of security vulnerability information."*
>
> **Anthony Grieco**
> VP, Chief Information Security Officer, Cisco

> *"Transparency starts with culture. It's an expectation that employees will be accountable for the way they interact with customers and the world at large."*
>
> **Noelle Warburton**
> Director, Security and Trust Strategic Communications, Cisco

Prove it

Demonstrate compliance with independent third-party verification

The other pillars of the New Trust Standard are critical commitments—to transparency, a zero trust approach to network access, data sovereignty, and a trusted supply chain. Certifications are the proof that the organization keeps those commitments. Common product security certifications include the international standard ISO/IEC 27001, System and Organization Controls (SOC 2) in North America, FedRAMP in the U.S. public sector, and Cloud Computing Compliance Controls Catalog (C5) in Germany.

To earn certifications, IT product and service providers undergo an audit by an accredited, independent third-party, often an accounting firm. In the U.S., for example, auditors receive accreditation from the ANSI-ASQ National Accreditation Board (ANAB). Privacy certifications demonstrate to customers, regulators, and other stakeholders that the vendor upholds internationally recognized privacy principles and honors core rights of data subjects when handling their PII. Recognized certifications include EU Binding Corporate Rules, APEC Cross Border Privacy Rules, APEC Privacy Recognition for Processors, and US Privacy Shield (invalidated for EU transfers but still recognized by the U.S.). These certifications are administered and verified by privacy regulators or regulator-approved, independent accountability agents.

Certifications become increasingly important in a cloud world

When you buy hardware or software to deploy in your own data center, company or customer data never leaves your building. You only need to trust that the product will do the job. When you subscribe to a cloud service, in contrast, customer and company data leaves your premises. It resides on the provider's servers and travels over the provider's network. Now you also need to trust that the service provider handles customer data responsibly. Makes timely patches and updates. Complies with data sovereignty requirements. Manages vulnerabilities. Meets service level agreements for availability. Honors data subjects' privacy rights. The constant evolution of cloud services also includes the evolution of security controls. Annual certifications provide a consistent measure of a vendor's security profile and give customers an easier way to make informed choices.

"Privacy certifications matter. Ninety percent of organizations surveyed indicated ISO, APEC, and EU privacy certifications are important factors impacting vendor selection and buying decisions."

Harvey Jang
VP, Chief Privacy Officer, Cisco

Source: Cisco 2021 Data Privacy Benchmark Study

Conclusion

The New Trust Standard says that trust is no longer just about intuition. No longer an aspirational statement on the Corporate Values webpage. Having seen the risks when sensitive data gets into the wrong hands, today's customers have raised the bar. They want tangible assurance that the companies they work with have the commitment, technology, and processes to protect their data. How well companies rise to the challenge will affect not only their own bottom line but also the continuity of critical infrastructure that society depends on.

At Cisco, the New Trust Standard has changed the way we do business. We're listening to what our customers want, putting in place the technology, processes, policies, and people to deliver, and working alongside them to map out a digital future with trust at its foundation.

A few of our actions: Cisco is building a zero trust architecture. We write our contracts with suppliers to hold them accountable to the same security and privacy standards we've committed to uphold. We publish and follow a Principled Approach to Government Requests for Data. We publish Privacy Data Sheets for products and services that process Personal Data, answering common customer questions about how we process personal data for customers to decide the best and safest way to use the product to suit their needs. And we earn security and privacy certifications so that customers don't need to base their confidence in our products on faith alone.

Initiated by customers, the New Trust Standard is a positive development for our increasingly digital world. Explicitly stating what customers expect from the companies they do business with converts trust from a feeling to an objective benchmark.

To learn more about Cisco's commitment to trust, visit trust.cisco.com