sift

Deploying Digital Trust & Safety

A step-by-step guide to building a world-class fraud prevention operation

Contents

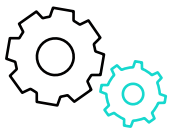
The Digital Trust & Safety transformation

Over the last two years, there has been a fundamental shift in how businesses approach fraud prevention. Fighting fraud is no longer simply loss prevention, payment fraud detection, or risk mitigation. Leaders in industries like e-commerce, fintech, and food & beverage have abandoned this mindset in favor of Digital Trust & Safety—an approach that strategically aligns risk and revenue decisions to not only protect a business and its customers, but to fuel explosive growth. These leaders recognize the need for proactive fraud prevention across a variety of use cases and fraud types—including account takeover (ATO), content abuse, promo abuse, and synthetic fraud—as well as the need to deliver frictionless customer experiences for trusted users.

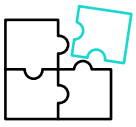
The shift to a Digital Trust & Safety approach is accelerating. According to the 2020 Gartner Market Guide for Online Fraud Detection, "By 2023, 30% of banks and digital commerce businesses will have dedicated trust and safety teams to protect the integrity of all online brand/customer interactions, which is an increase from fewer than 5% today."

It's one thing to understand what Digital Trust & Safety is and why it's important, but how do you actually implement the processes and technologies required to successfully deploy Digital Trust & Safety? It takes more than simply adding a new tool or procedural step; it's about remodeling business strategies for the challenges and opportunities of the digital world.

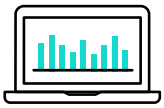
In examining the most successful trust and safety teams at businesses like AirBnB, DoorDash, and Twitter, three key elements emerge:



Automation



Context



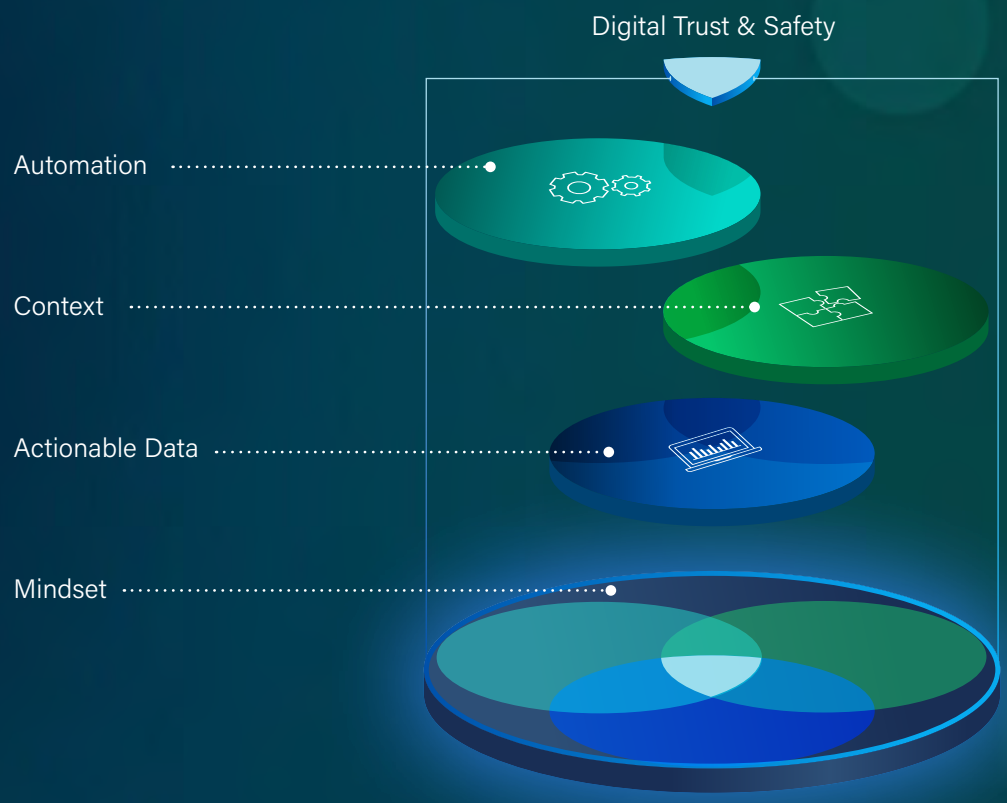
Actionable data

These critical elements are at the core of leading businesses' trust and safety strategies. On the following pages, we will provide a step-by-step guide on how to implement an effective trust and safety strategy, and ultimately marry protection with growth. Hold on, you're about to embark on a journey that will catapult you past your competition.

TURO

Turo, a leading car-sharing marketplace, saw fraud—specifically account takeover attempts—increase as they grew and expanded into new markets. To combat this growing threat, Turo turned to automation and actionable data to not only decrease time spent on manual review, but block all ATO attempts and reduce overall fraud by **98%**. To learn more, read the case study.

The three elements of Digital Trust & Safety



The image above illustrates the three elements needed to implement a successful **Digital Trust & Safety** strategy—**automation**, **context**, and **actionable data**. These concepts, along with a **foundational mindset** that we will explore later, will help you build a Digital Trust & Safety approach that is tailored to your specific needs.

Examine your current strategy

Before making the transition to **Digital Trust & Safety**, it's important to examine your current strategy. Answer the following list of questions to gain a greater understanding of the status quo at your business. Bear in mind, this list is not exhaustive, but it will give you an idea of the maturity of your fraud prevention operation.

How do you currently fight fraud?
To get where you want to go, you need to first understand where you are. The following questions will give you insight into the processes and technologies you currently use to stop fraud.

What tools do we use to proactively identify and prevent fraud?

Example: In-house rules, rules-based fraud prevention vendor, machine learning, device fingerprinting, manual review queue, etc.

If we are currently using tools to stop fraud, how many?

What role does automation play in our fraud-fighting approach?

What key performance indicators (KPIs), if any, are we measuring?

Example: Block rate, false-positive rate, chargeback rate, refund rate, loss rate, time spent on manual review, etc.

Do other teams and departments at the company understand the impact of our team?

Example: Accessible reporting across departments, impact to top-line and bottom-line revenue, etc.

Where does the data produced by our team live?

Example: Spreadsheets, business intelligence tools, searchable databases, etc.

How do other departments view our team?

Example: Revenue blocker, cost center, crucial to the success of the business, etc.

Examine your current strategy

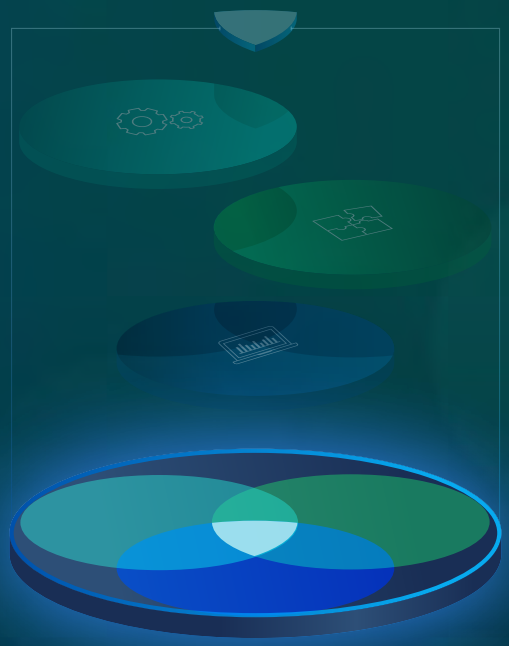
By answering the previous questions, you have checked the pulse of your fraud prevention operation.

A more thorough audit of your current processes and technologies may be needed (especially if you were unable to answer a majority of the questions), but you should now have a clearer picture of your current strategy. As we move forward, refer back to your answers to understand the delta between where you are now and where you want to be, post-deployment of **Digital Trust & Safety**.

Before we examine the three key elements of a successful Digital Trust & Safety strategy and how to implement them, let's briefly touch on mindset. Think of it as the foundation on which your Digital Trust & Safety strategy stands.

MINDSET

The Digital Trust & Safety mindset—balancing growth with security



A Digital Trust & Safety mindset shifts the focus from exclusively reducing risk to a balance of protection and growth. Building a seamless customer experience and increasing user engagement are just as important as reducing risk and blocking fraudulent activity.

Instead of taking a narrow view of customer experiences and fraud prevention, the Digital Trust & Safety mindset invites a broader perspective: **customer journeys rather than customer transactions, and fraudsters' behavior rather than fraudulent chargebacks.**

The Digital Trust & Safety mindset is also a competitive advantage. It allows a business to experiment and roll out initiatives that its competitors avoid for fear of fraud, e.g. new product launches, digital gift cards, etc.

Put succinctly, Digital Trust & Safety is the strategic alignment of risk and revenue decisions, supported by management processes and technology.
For more information on the Digital Trust & Safety mindset, visit our blog.

Digital Trust & Safety is the strategic alignment of risk and revenue decisions, supported by management processes and technology.

AUTOMATION

Accelerate growth and adapt to changing conditions

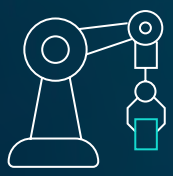
Automation is a core component of a successful Digital Trust & Safety approach to fighting fraud. Why? Because relying solely on manual review is time-consuming at best. In a worst-case scenario, it's potentially disastrous for your business, with customers leaving in droves and fraudsters leveraging their own version of automation to overwhelm your manual review team.

And while there's still a place for human review of actions taken on your site, the goal of **Digital Trust & Safety** is to not just catch fraudulent orders or prevent fake accounts from being created, it's to unlock growth at scale. High levels of automation are critical for creating seamless transactions for trustworthy customers and erecting real-time roadblocks for potentially fraudulent actions. Legitimate customers have come to expect speed and, unfortunately, manual processes are anything but speedy. If delivering fast, frictionless experiences for customers and building brand loyalty are important (which they should be), this leaves companies with only one choice if they wish to delight their customer base—automate as many processes as possible.

Manual review should be saved for transactions that are in a gray area—not obviously legitimate or fraudulent. To ensure your fraud analysts are not buried by a never-ending review queue, trust and safety teams need to leverage automation.

While rules-based systems, whether built in-house or purchased from a 3rd-party vendor, can be used to automate actions such as blocking an order or sending a transaction to a manual review queue, machine learning systems are superior. They allow trust and safety teams to respond to increased volumes, maintain accuracy at scale, quickly adapt to changing market conditions, surface trends, and take action without human intervention.

Automation 101: First Steps



A few things need to be in place before you can fully leverage automation. The following is a step-by-step guide that will help you begin to automate portions of your fraud-fighting operation. Note—every business is different. Your specific needs may vary, and the examples given are for illustrative purposes only.

01

Build or purchase a fraud prevention solution specifically designed to support Digital Trust & Safety.

02

Solution needs to easily ingest and take action on internal and external data, e.g., account age, shipping address, payment card information, login attempts, etc.

03

Solution needs to scale as your business grows, therefore machine learning is recommended.

04

Ensure you have appropriate data (geographic, demographic, behavioral, etc.) to take action on, and that data is easily accessible by your fraud prevention solution.

05

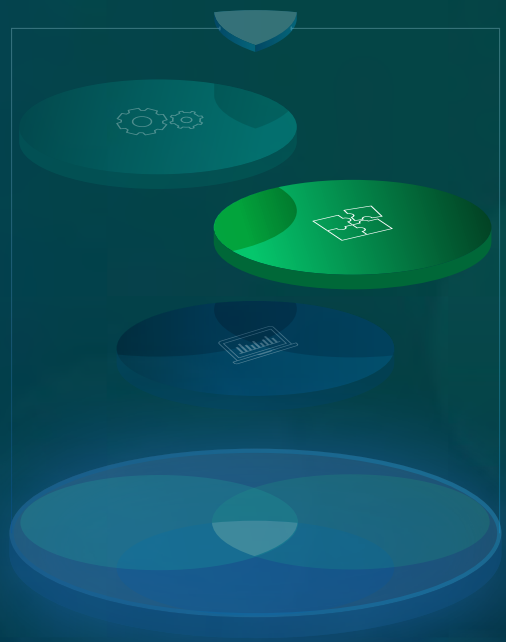
Establish level of risk tolerance based on specific factors like profit margins, cost of goods sold, customer lifetime value, customer acquisition costs, stage of company growth, etc.

06

Adjust thresholds and business logic to improve customer experiences, adapt to the changing landscape of transaction types, and address a variety of fraud threats. Machine learning solutions should be able to do this in real time, and with little-to-no engineering support.

CONTEXT

Control fraud and make accurate decisions



The second element of a successful Digital Trust & Safety approach is context, which allows trust and safety teams to make accurate, data-driven decisions. According to Sift Digital Trust and Safety Architect Kevin Lee, many companies use more than five tools to get a clearer picture of actions taken on their sites in order to combat fraud and build trust. While effective to a point, these disparate systems rarely integrate easily into a single pane of glass, and often require a significant amount of developer resources (which are always in short supply) to get up and running, resulting in missing or incomplete fraud data for teams to leverage. Even if developer resources are available to help tie things together, fraud data can end up siloed in different tools.

As a result of disconnected tools and data sets, teams spend valuable time piecing together information instead of investigating new vectors of fraud and optimizing processes and automation to protect and grow their business. Teams need one platform to connect and orchestrate the use of other solutions and data sources, providing a holistic view of the customer journey for higher accuracy and more informed decisions.

A single platform—a command center—enables analysts and agents to understand situational information and make accurate decisions with the data available. Ideally, this unified solution will also enable bulk action to be taken with multiple cases in order to further enhance existing automation, and allow for in-depth investigation of new fraud trends and anomalies as needed.

> There should be one primary tool—a system of record—where an analyst can understand the situation and make the most accurate decision possible given the data available.
>
> **Kevin Lee**
> Trust and Safety Architect, Sift

Context Checklist

An ideal, centralized platform will orchestrate the entire fraud-fighting process—from defining tolerances to automating data ingestion, monitoring ongoing performance, and optimizing for maximum revenue—without sacrificing protection. Set yourself up for success and ensure your command center has the following capabilities:

- Integrates with external and internal tools and data sets without the need of developer or engineering resources.
- Scales as your business grows, and allows for the monitoring of different business units or markets as you expand the scope of your offerings.
- Easily connects with your e-commerce platform, e.g. Salesforce Commerce Cloud, Magento, Shopify, etc.
- Allows for bulk actions, e.g. block all orders from specific IP addresses, or analyze and investigate larger fraud trends/ anomalies seen across a group of orders.
- Provides real-time visibility into the impact that trust and safety is having on your business.

ACTIONABLE DATA

Optimize your operation and dominate the competition

The final element is actionable data. Successful trust and safety teams are obsessed with data, as small improvements to various KPIs can have a significant impact on bottom line performance *and* top line growth. It is essential to have quick access to appropriate performance metrics and indicators. These indicators exist at every level of your company, and departmental leaders from across the organization should understand your team's impact on the business. For example, reporting on specific analytics is important to trust and safety team leads, while the false-positive rate is valuable to the growth team. This information shouldn't be buried in a mountain of dashboards or spreadsheets—it needs to always be just a click away.

But all data is not created equally.

As the old saying goes, "garbage in, garbage out." The appropriate data for your business will vary, and originate from both internal and external sources. It's important to keep in mind that the goal of actionable data is to continuously improve the effectiveness and efficiency of your trust and safety operation.

When data is available and actionable, leaders are able to:

- **Better protect the business and its customers**
- **Grow revenue by understanding the overall impact of the fraud prevention operation**
- **Automate with confidence**
- **Convey the value your trust and safety team to the rest of the business**

Useful Data for Digital Trust & Safety

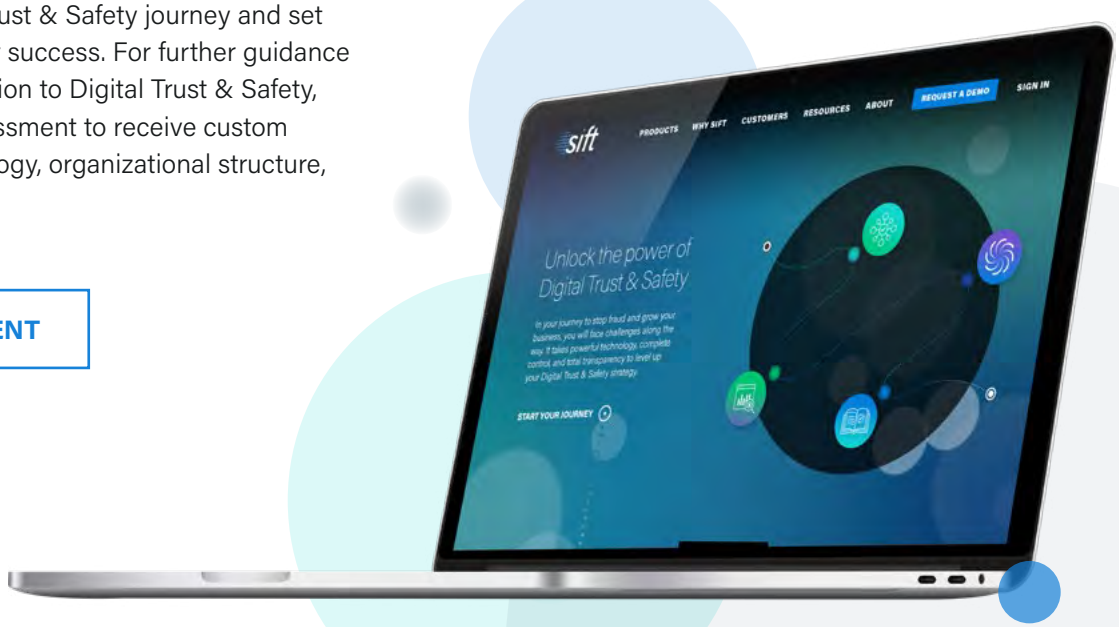
The following represent some of the data points that you may find useful as you build out and optimize your trust and safety operation. Note—every business is different. Your specific needs may vary, and the examples given are for illustrative purposes only.

Begin your Digital Trust & Safety journey

As traditional retailers and e-commerce companies adapt to the competitive pressures of the digital world, Digital Trust & Safety is the only approach that allows fraud fighters to proactively defend against an increasing range of threats, as well as meet the rising expectations of consumers.

The key elements presented in this guide will help you as you embark on your Digital Trust & Safety journey and set you, and your business, up for success. For further guidance on how to successfully transition to Digital Trust & Safety, visit Sift.com or take our assessment to receive custom recommendations for technology, organizational structure, and processes.

TAKE YOUR ASSESSMENT



About Sift

Sift is the leader in Digital Trust & Safety, empowering digital disruptors to Fortune 500 companies to unlock new revenue without risk. Sift dynamically prevents fraud and abuse through industry-leading technology and expertise, an unrivaled global data network of 35 billion events per month, and a commitment to long-term customer partnerships. Global brands such as Twitter, Airbnb, and Twilio rely on Sift to gain competitive advantage in their markets. Visit us at sift.com and follow us on Twitter @GetSift.