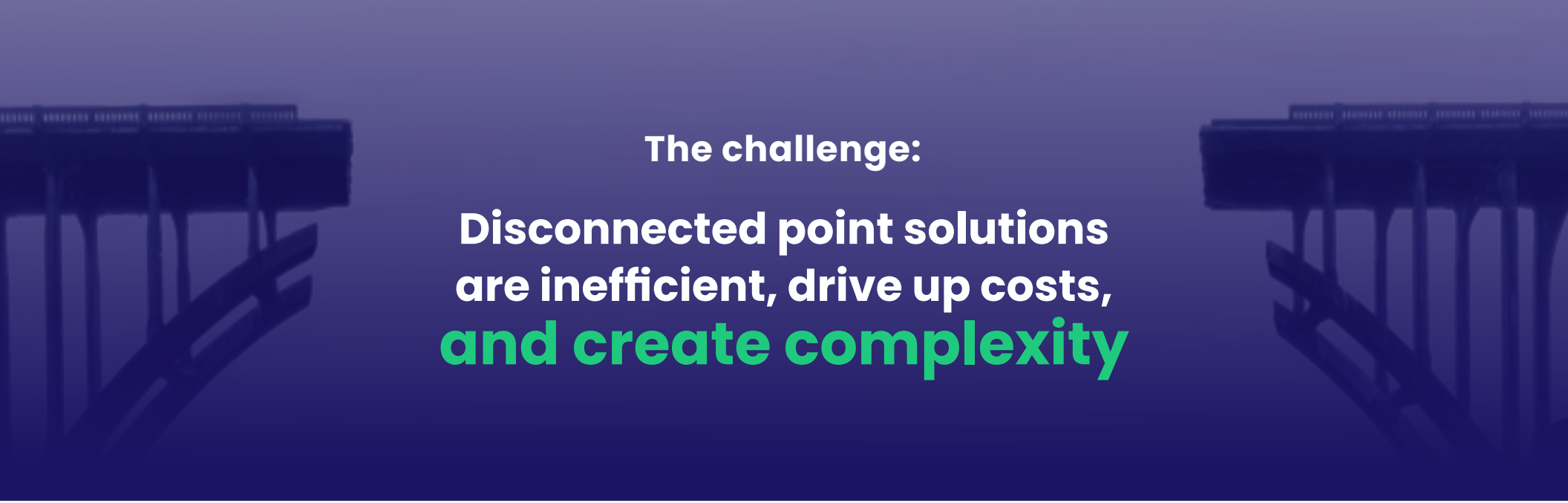
How do you address new threats without burdening your organization?

OUTSEER



The challenge:

Disconnected point solutions are inefficient, drive up costs, and create complexity

When a new fraud vector emerges, you might urgently seek out a dedicated point solution to plug the hole. But this means one more license to pay for, one more system to train on, and an additional vendor to manage. More concerning is the impact on your operations.

With no common platform, sharing threat information among fraud models and teams is an unwieldy, complex process. Your customer authentication team may be aware of credential stuffing. But with no easy way for them to communicate their concerns, your fraud team may not know for days that they should block certain suspect accounts or transactions.

Incorporating additional data—whether from a third party or different part of your organization—can be tedious. Each fraud product requires a custom data connection, creating brittle links that are costly to update when data sets change. And the problem is magnified when you consider all the different use cases you have across your customer interactions.

With your teams already stretched thin, the departure of just one key person can create a debilitating knowledge gap. And with a different fraud tool for each new use case, the complexity only gets worse.

But when you evolve with Outseer, you'll **leverage a common fraud management platform**.

Here's how...

Centralize risk visibility across customer events

Effective communication between teams is critical if you want to create a unified front against fraud.

With Outseer, your people can connect authentication risk to payment fraud and other transaction risks throughout the customer journey. By linking events together utilizing a single, connected system, you'll obtain better visibility into the true nature of a fraud attack.

With this knowledge, your people can make better decisions while automatically reporting confirmed fraud outcomes to enhance fraud model performance.

As a result, you'll be able to identify and seal off threats faster and more effectively.

Outseer's **Unified Case Management** offers visibility into customer interactions, forensic analysis on customer events, automatic confirmed fraud reports, and management of follow-up activities.

Seamlessly ingest and link third- and first-party data

Leveraging multiple data sets and fraud signals is a chore—and must be repeated whenever you implement a new point solution.

But when you use Outseer's platform, you can access insights across logins, account management, and payment transactions—while ingesting new data signals to enhance both your risk scoring and policy engines. In this way, you'll be able to connect all that data to reveal superior insights.

For example, you could utilize insights from third-party behavioral biometric solutions or unique customer profile data from other internal systems to gain greater precision in separating valid transactions from fraudulent activity.

This way, you'll spend less time making sense of disconnected point solutions and less effort handling the repercussions of unnecessary interventions. And you'll limit concerns about serial and broken data connections.

Our **data ingestion and linking** establishes and maintains the connection of data elements and intelligence across customer touchpoints.

Centralize policy management across authentication and fraud use cases

It's necessary—yet incredibly complex—to apply fraud protection and user authentication capabilities across multiple use cases. And it gets worse when you have a range of point solutions with different, or nonexistent, policy management capabilities.

With the Fraud Manager platform, you'll be able to write policies once and utilize them many times across multiple payment, user management, and authentication uses cases at the touch of a button.

Throughout this process, you'll deliver consistent risk controls and challenge experiences at all customer touch points. And when policy updates are required, you can rapidly deploy them across your entire environment.

Thanks to this simplified approach, you'll swiftly respond to new threats. And you won't just reduce the effort of writing and disseminating policies—you'll ensure they're applied consistently, as well.

The **unified policy management in Fraud Manager** creates policies on fraud signals—as well as the appropriate action to take on those signals—across the consumer journey.

Leverage a common fraud management platform

Adding point solutions to address in-the-moment needs creates a level of complexity that can inhibit your ability to analyze and act with speed and certainty.

But when you continue working with Outseer, you'll leverage a common fraud management platform that can be extended to cover new fraud use cases—without relying on point solutions.

This way, you'll be able to:

- **Eliminate threats with greater effectiveness**
- **Reduce the time spent building and maintaining data connections**
- **Create and roll out policies with ease**

To learn more, please contact us today.

OUTSEER