Bloor

InPerspective

gathr

INDUSTRY IMPACT STUDY

Financial Services

Learn how Gathr is used in financial services for breakthrough success, including threat detection, payment surveillance, downtime prediction, & more

---

InPerspective Paper by **Bloor**
Author **Daniel Howard**
Publish date **October 2022**

“Cybersecurity experts follow a continual arms race, engaging with bad actors that are constantly evolving the sophistication of their attacks. In the modern times, attacks are ever more frequent, more complex, and more subtle – and your security measures must evolve too in order to keep up with them.”

Introduction

Cybersecurity experts follow a continual arms race, engaging with bad actors that are constantly evolving the sophistication of their attacks. In the modern times, attacks are ever more frequent, more complex, and more subtle – and your security measures must evolve too in order to keep up with them. In addition, the increased stringency of recent regulation – GDPR et al. – combined with greater public awareness means that any data breach that allows sensitive, personal data to get loose will almost certainly result in very substantial harm to both your bottom line and your reputation.

Threat detection, in particular, is an important part of cybersecurity, and plays a major role in preventing data breaches (or at least minimising their frequency and impact). But it is not a trivial thing, especially with data itself becoming more abundant than it ever has been before: you need to be able to monitor your entire system – all your data, or at least all your sensitive data – for anomalous behaviour and flag it up in something very close to real-time, with high accuracy. You need a solution that can access and analyse your data quickly and automatically. What's more, this is all especially important in the world of financial services, due to the inherently high sensitivity of the data involved. Gathr is more than capable of providing a robust solution for threat detection within such an environment.

“Threat detection, in particular, is an important part of cybersecurity, and plays a major role in preventing data breaches (or at least minimising their frequency and impact).”

Problem

Although threat detection itself has been widely adopted as a capability, all too often it consists solely of simple, static, rules-based alerting that is far from ideal at the enterprise level. To wit, this kind of system operates on user activities to identify and diagnose potentially compromising behaviour. But the key word here is *"potentially"*: in practice, systems of this type can generate large numbers of irrelevant alerts (in other words, false positives) when applied to the thousands of individuals employed by large organisations. This effectively camouflages the actual threats, slowing detection and preventing timely corrective action from being taken. What's more, strictly rules-based systems enable sufficiently knowledgeable bad actors to keep their behaviour within those rules while still behaving maliciously.

Threat detection technology stacks can also be expensive, inflexible, or both. For instance, threat detection may be limited to only a small number of applications, and sufficiently rigid that expanding it to more is arduous and expensive, if it's possible at all. A slow development pipeline is another potential issue, which can lead to many use cases remaining uncovered for a prolonged period of time, if not indefinitely. This prevents timely action – or any action at all – from being taken in regard to those use cases. In short, threat detection systems need to be able to scale up to adequately handle the amount of data an enterprise organisation must deal with.

"...threat detection systems need to be able to scale up to adequately handle the amount of data an enterprise organisation must deal with."

Solution

Using Gathr, you can create an accurate, scalable solution capable of detecting threats in real-time, across a very substantial range of applications and quantity of data. The architecture for one such solution is displayed in *Figure 1*. Instead of relying on simple rules, Gathr leverages machine learning and predictive analytics to build a system that can detect threats accurately, continuously, and even when the underlying pattern of anomalous behaviour has not been described explicitly. Like the systems described above, it can raise alerts whenever it finds a threat, but it can also take direct, automated action to prevent the data breaches it predicts.

Gathr can help you apply machine learning models to your log and complex event data in order to find anomalous behaviour. These models periodically learn the normal, *"baseline"* behaviour of your environment, then look for discrepancies with that baseline. In effect, the models – and thus the solution – change and evolve over time in concert with your underlying system. The models, which can be created using built-in machine learning operators provided by Gathr, include self-learning and behaviour-profiling algorithms to facilitate all of this. The latter, in particular, can be used to build scores and thresholds for various risk factors for transactions in real-time, enabling timely, accurate and automated identification of suspicious behaviour. Of course, static factors can still be applied in addition to this more dynamic pattern recognition.

Gathr also provides in-memory data transformation, enabling and/or accelerating data quality scoring, data deduplication, data cleansing, and data enrichment. Several of these functions can be made available in real-time and/or automatically as a result of this.

> **Using Gathr, you can create an accurate, scalable solution capable of detecting threats in real-time, across a very substantial range of applications and quantity of data.**

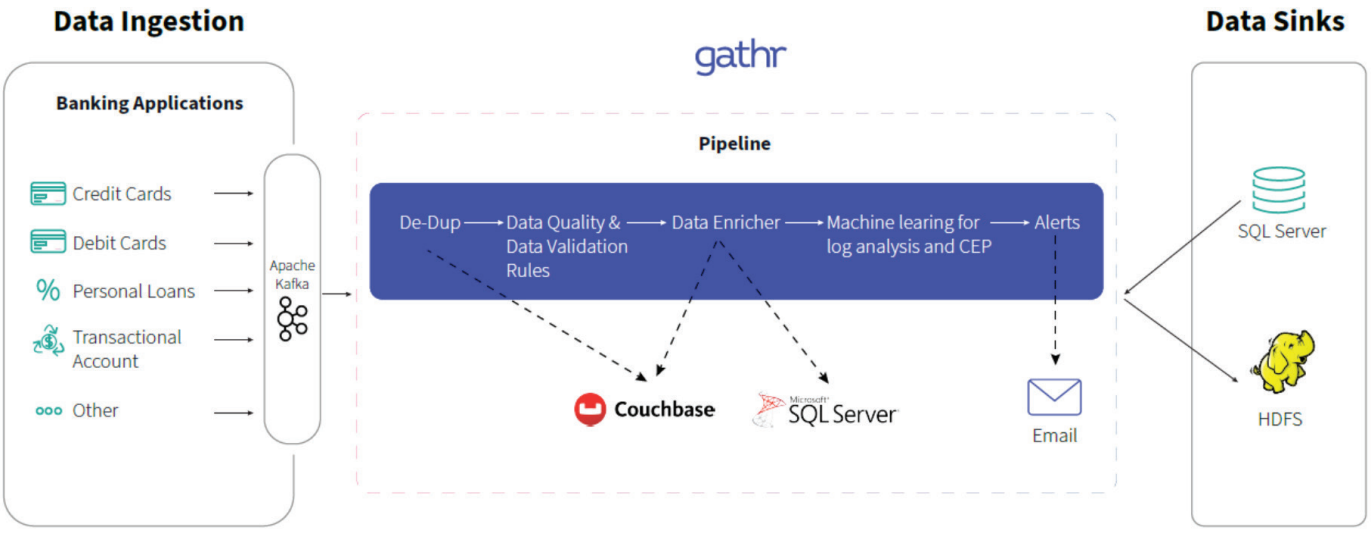

Figure 1
Example architecture for a Gathr solution

Result

Gathr's solutions for threat detection are frequently more scalable, performant, and cost-effective than what came before them. They often generate far more accurate and timely results and are easier to develop for as well. Particular highlights include greater scalability and coverage, reduced cost, faster development time, and a massive reduction in false positives.

Moreover, Gathr provides an *"all-in-one"* platform for data processing in general. This has benefits in terms of centralisation, ease of use, and so on, since you are able to leverage a great deal of data functionality – including threat detection – within a unified and centrally managed product, through a single interface. In addition, Gathr's interface is highly visual, and uses a drag-and-drop methodology that is very easy to use, even for non-technical users, and lends itself well to self-service.

“Gathr’s interface is highly visual, and uses a drag-and-drop methodology that is very easy to use, even for non-technical users, and lends itself well to self-service.”

Other use cases

Threat detection is a significant use case, but it is a long way from the only one that Gathr can address, even if we narrow our scope to cybersecurity specifically. Gathr is a general data processing platform, after all, and as such, it is much broader than any single use case. Other cybersecurity use cases it can address include payment surveillance, downtime prediction, market risk management, emerging risk management, insider fraud detection, credit card fraud detection, real-time transaction screening, and trade compliance. What's more, it can be used to deliver frictionless customer journeys while providing all of its cybersecurity capabilities.

“Threat detection is a significant use case, but it is a long way from the only one that Gathr can address.”

Conclusion

This report should demonstrate that Gathr is entirely capable of providing a solution for threat detection within the context of financial services. That said, the advantages we've outlined in this paper are not exclusive to threat detection, but rather can be applied to a wide range of data management use cases both within and without the world of financial services. It has particularly showcased Gathr's ability to create robust machine learning functionality to drive monitoring and alerting, both for the purposes of threat detection and otherwise.

Gathr is entirely capable of providing a solution for threat detection within the context of financial services.

FURTHER INFORMATION
Further information about this subject is available from *www.bloorresearch.com/company/gathr/*

Daniel Howard

Senior Analyst,
Information Management and DevOps

Daniel is an experienced member of the IT industry. In 2014, following the completion of his Master of Mathematics at the University of Bath, he started his career as a software engineer, developer and tester at what was then known as IPL. His work there included all manner of software development and testing, and both Daniel personally and IPL generally were known for the high standard of quality they delivered. In the summer of 2016, Daniel left IPL to work as an analyst for Bloor Research, and the rest is history.

Daniel works primarily in the data space, his interest inherited from his father and colleague, Philip Howard. Even so, his prior role as a software engineer remains with him, and has carried forward into a particular appreciation for the development, DevOps, and testing spaces. This allows him to leverage the technical expertise, insight and 'on-the-ground' perspective garnered through his old life as a developer to good effect.

Outside of work, Daniel enjoys latin and ballroom dancing, board games, skiing, cooking, and playing the guitar.

Bloor overview

Technology is enabling rapid business evolution. The opportunities are immense but if you do not adapt then you will not survive. So in the age of ***Mutable*** business Evolution is Essential to your success.

We'll show you the future and help you deliver it.

Bloor brings fresh technological thinking to help you navigate complex business situations, converting challenges into new opportunities for real growth, profitability and impact.

We provide actionable strategic insight through our innovative independent technology research, advisory and consulting services. We assist companies throughout their transformation journeys to stay relevant, bringing fresh thinking to complex business situations and turning challenges into new opportunities for real growth and profitability.

For over 25 years, Bloor has assisted companies to intelligently evolve: by embracing technology to adjust their strategies and achieve the best possible outcomes. At Bloor, we will help you challenge assumptions to consistently improve and succeed.

Copyright and disclaimer

Bloor Research International Ltd
20–22 Wenlock Road
LONDON N1 7GU
United Kingdom

tel: **+44 (0)1494 291 992**
web: **www.Bloorresearch.com**
email: **info@Bloorresearch.com**