Enhance and Extend Your Fraud Management Capability with Agile Analytics

How Adaptable is Your Fraud Management Program?

As Communication Service Providers (CSPs) add new services and the complexity of those services increases, so do the opportunities for fraudsters. Fraud losses cost CSPs over $40 billion per year and CSPs must implement flexible fraud management solutions capable of adapting quickly, maintaining a high speed of detection and enabling rapid and effective analysis irrespective of service or network type.

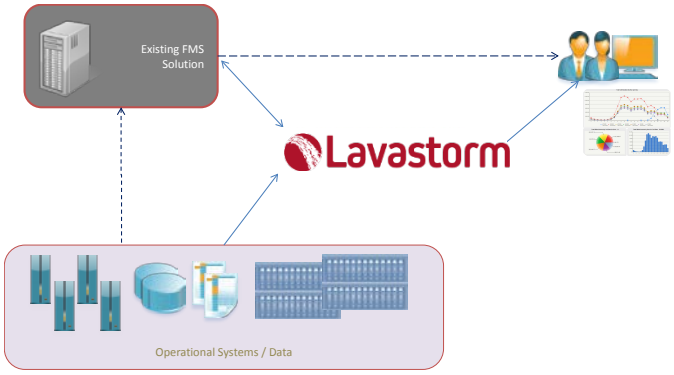
With technically astute fraudsters, the need for a fast, flexible and adaptive new generation analytic tool is critical. With Lavastorm, you don't need to replace your existing tool to get these capabilities, but can expand your capability with a low cost, quick start desktop solution.

Complementing Your FMS with Lavastorm

Most fraud management systems (FMS) can adequately detect known, or standard, fraud patterns and initiate actions to control those threats, however, today's fraud management teams are tasked with much more.

Faced with changing fraud threats emerging from new services, new network structures, and even new communication methods, such as social media, fraud management groups not only must monitor known threats, they must also investigate and uncover patterns of fraud never seen before.

With Lavastorm you can take advantage of the processes and systems already in place, and enhance these systematically at a low cost to derive more value from your fraud program both now and in the future.



Extending Your FMS with the Lavastorm

Lavastorm is a powerful, visual and versatile analytic desktop environment that can complement your existing FMS and Fraud program with discovery-based audit capabilities, which enable you to:

Enhance and refine the analysis from your FMS – look more deeply at the output of your FMS to eliminate false positives and uncover the root cause of fraud trends. Lavastorm can publish improved results back to your FMS to close the loop or directly to dashboards and other tools viewed by your fraud team.

Extend your FMS to answer new questions – in just minutes you can answer ad-hoc, or unanticipated, questions and those not addressed by your current FMS. This is necessary for root cause analysis when you need to quickly investigate multiple scenarios or to consider data beyond usage data in your FMS, including data from operational systems, such as order, inventory, customer service, 3rd party content, and payment systems to identify new forms of suspicious behavior and transactions.

Lavastorm fills the gaps within and around an FMS – allowing you to extend the life of your FMS while still keeping pace with the detection of new and complex fraud types.

The Power of Discovery-based Audit Analytics

Lavastorm enhances your fraud program and approach with discovery-based audit analytics – a next-generation analytic capability that increases both the speed at which your business operation can react and the control it maintains over fraud threats. Discovery-based audit analytics has two essential components:

Data Discovery – an analytic technology that gives you the speed and flexibility to bring together a wide array of data much more quickly and cheaply than through traditional means. Data Discovery offers you the flexibility to respond to new requirements in the business, whether that's considering new data sources, asking spur of the moment questions, or exploring new analytic paths.

Audit analytics – the ability to apply analytics to a specific business process, including fraud management, to monitor, control, and improve the business processes. With audit analytics, you can turn any new discovery into a persistent control to continuously monitor business performance and/or to detect and act on newly discovered fraud patterns.

Powerful Investigations

Using Lavastorm alongside your existing FMS provides you with the insight to:

Identify fraud patterns, profiles, and root causes – Lavastorm gives fraud departments the ability to combine the suspects' patterns and their profiles with a combination of multiple data sources and powerful analytics that identify fraudulent behavior and the root cause of issues. The engine includes powerful fraud analytics to investigate traditional, new, and emerging fraud types, including bypass, subscription/identity, machine to machine, mobile money, international revenue share, and interconnect bypass/SIM box fraud, among others.

Increase fraud hit rate – Lavastorm offers you complete visibility into the entire process between data sources, rules and profiles, alarms, case management, customer information, payment history, actions and closing of an investigation. This complete visibility and the open system environment enable you to adjust the analytic for increased hit rate. Early warning rules, such as first call risk, fuzzy matching, and special profiles for new subscribers all have very high hit rates.

Advantage: Speed to Money

Lavastorm is used worldwide to combat fraud, delivering a high ROI in a short time frame by adding discovery-based audit analytics. Lavastorm is able to provide advanced fraud functions on top of an existing fraud management system, or as a targeted solution for fraud detection.

Fits Any Size Business

Lavastorm enhances the analytic capabilities of any size organization. Individual analysts can benefit from the power of Lavastorm by using one of several desktop editions. Analytic teams that require server-level processing power at an affordable price can take advantage of the Workgroup Server edition. Larger organizations, or those conducting analytics on a large scale or across various departments, will want to take advantage of the added scale provided by the Enterprise Server

Contact us to explore how Lavastorm can help you enhance and extend your fraud management processes. (see below)

BENEFITS

- Extend the life of your existing FMS
- Increase fraud hit rate by investigating new paths and considering new data types, such as social media data
- Respond to problems immediately without waiting to modify your FMS through change requests and release cycles
- Detect, analyze, and prevent new or complex fraud forms and adapt quickly to new forms of fraud, such as mobile money fraud
- Handle increased data size, fraud complexity and greater transaction volumes
- Publish results to multiple channels, including existing management systems, data warehouses, or other business systems
- Read any data from anywhere across the business, including data stored in operational systems
- High impact – low cost
- Scale your analytic solution to meet your business needs – from individual to workgroup to multi-server solutions