Safeguard against the threat knocking from inside the door

Anomaly Detection with Machine Learning Powered by Google Cloud

The threat from the inside

How safe are companies from the threat inside? In today's era, attacks happen even from inside the organization.

According to an Insider Threat Report, two-thirds of organizations (66%) consider malicious insider attacks or accidental breaches more likely than external attacks. The same report suggests that 48 percent of companies estimate the costs of the insider incidents as $100,000 and more, with nine percent estimating a cost of more than $1million.[1] The potential data loss from inside threat is huge.

Patterns in employee behavior

User Behavior Analytics (UBA) is a cybersecurity process about detection of insider threat, targeted attacks and financial fraud. UBA analyzes human behavior and employs algorithms and statistics to detect threats.

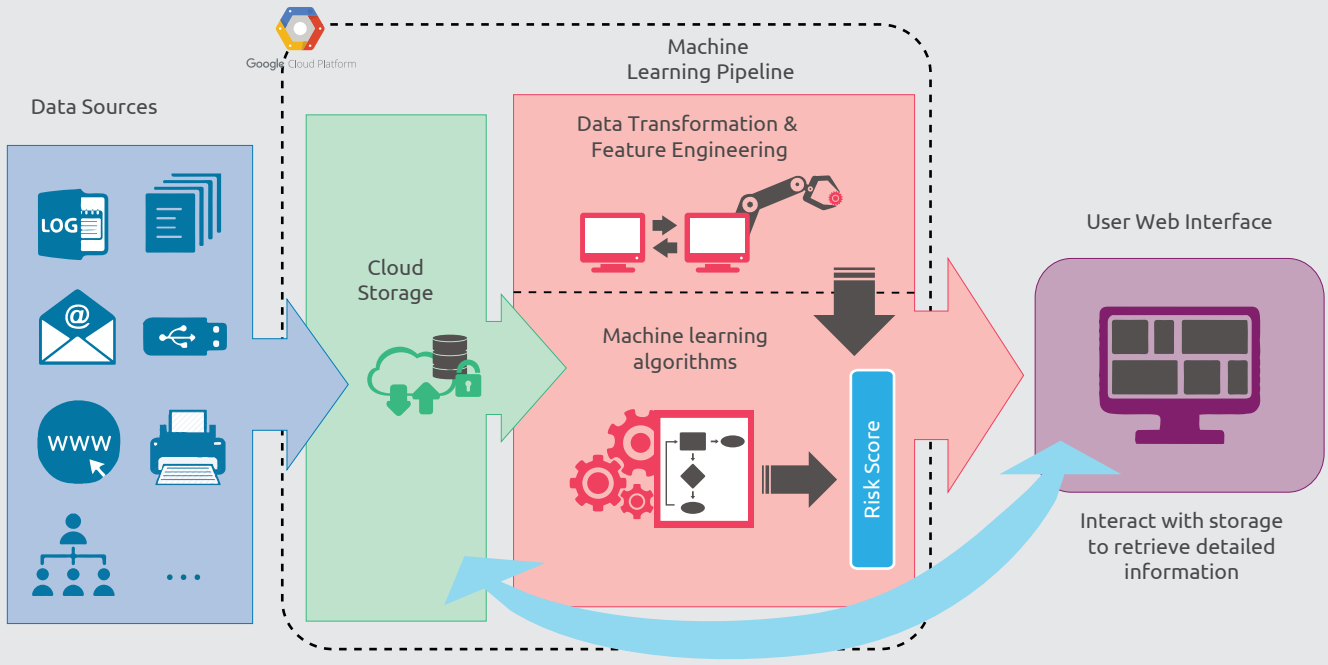
Companies should be one-step ahead to protect their data. They can identify threat in real time and study patterns of rogue as well as trusted employees. Most companies rely on rule-based models alone, which is not enough to identify threats for their static nature.

Solution Spotlight

Capgemini's Anomaly Detection solution makes it possible to predict insider threats in advance. It combines existing rules-based model and advanced unsupervised machine learning capabilities to provide clients with a more robust and comprehensive solution and track anomalies dynamically. This means the solution does not require historical true insider data, and implicitly analyses the data to initially uncover an insider threat using an unsupervised algorithm. As a next step we can also introduce a feedback loop in our model to improve the accuracy and use historical true insider data to run the model.

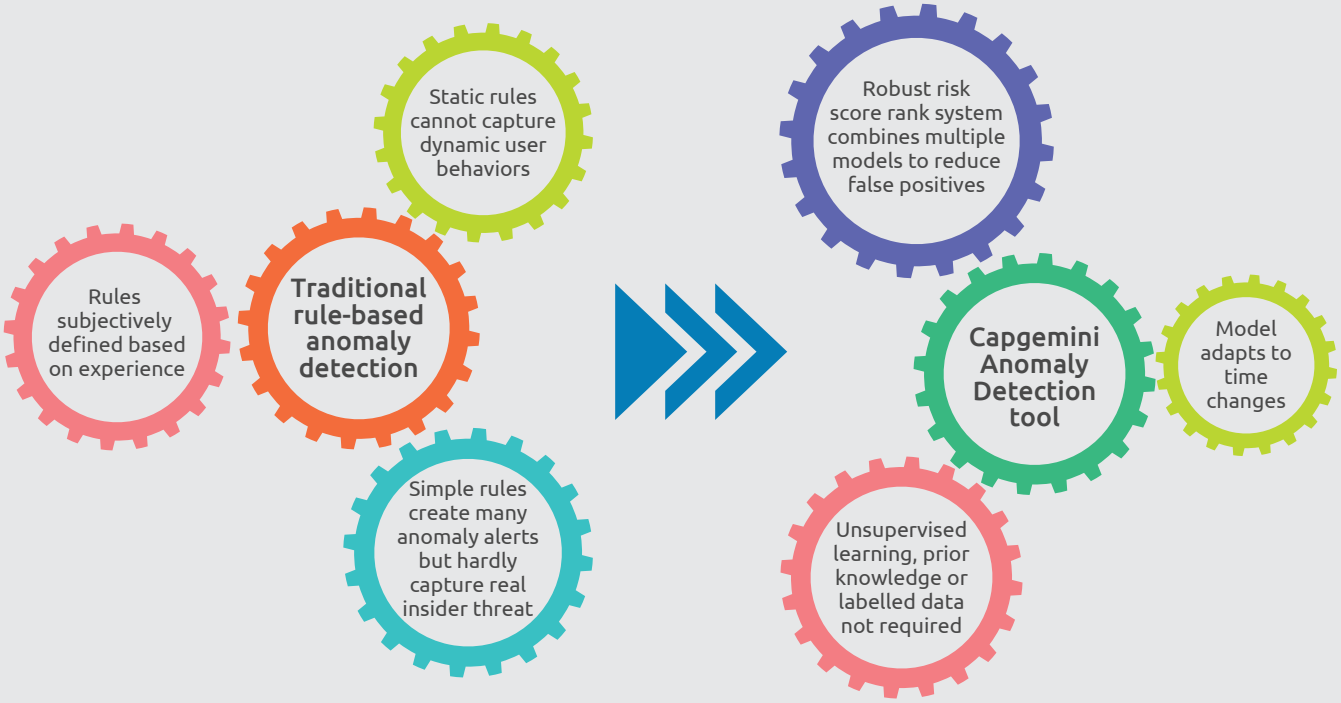
The solution is powered by Google Cloud Platform and Google Cloud Machine Learning Engine for more accurate insights.

Exhibit 1: Powerful Machine Learning Enabled Analytics Platform



1 2018 Insider Threat Report, Crowd Research Partners https://crowdresearchpartners.com/portfolio/insider-threat-report/

Exhibit 2: New Threats Demand Intelligent Dynamic Detection



Anomaly Detection: Reduced false positives lead to fast action

Looking at huge volumes of data, the Anomaly Detection algorithm isolates anomalous observations, identifying threats faster.

Fast data processing

- The Anomaly Detection tool spots suspicious data early
- The system looks at log on history, email exchanges, web browsing, device connection, and file connections

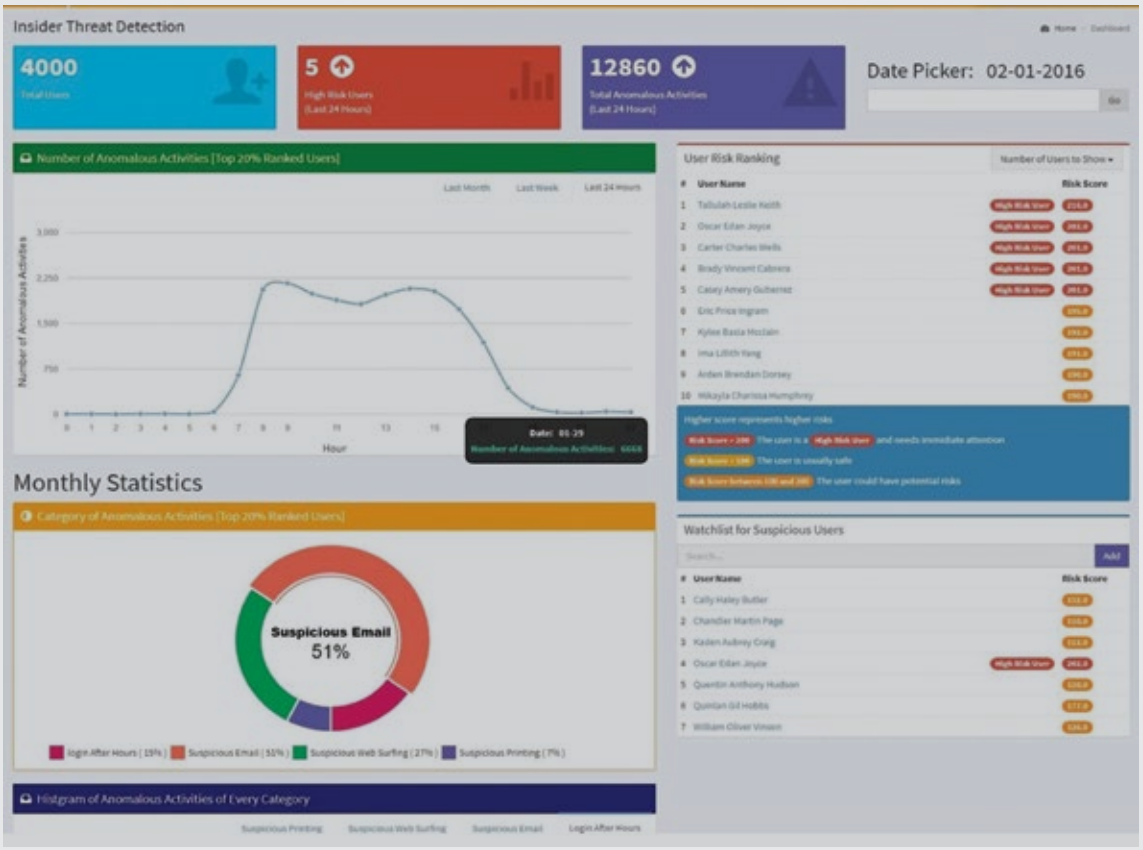
Machine learning to track fraud

- Unsupervised machine learning
- Cloud based big data processing
- User activity monitoring dashboard

False alarms out of the equation

- Reduce false positives
- Detect threats early
- Prevent frauds
- Protect data from internal threat

Exhibit 3: Interactive Dashboards for Quick Reference

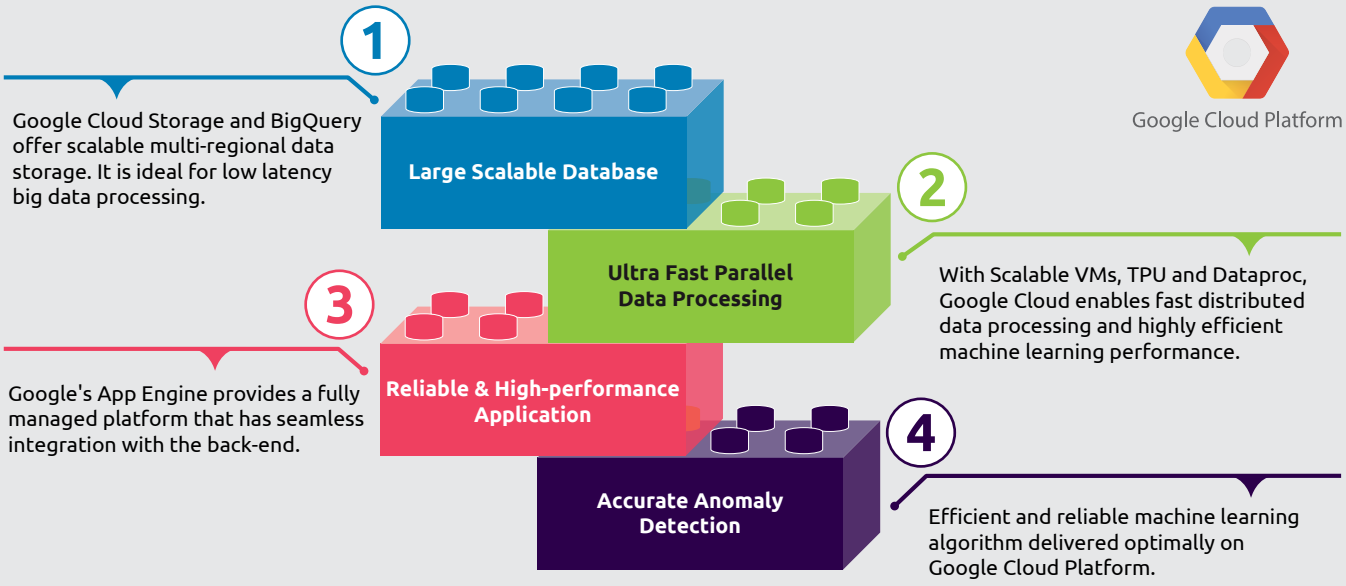


Anomaly Detection Solution, Powered by Google Cloud Platform

Google Cloud Platform is the engine that powers the Anomaly Detection tool.

Our solution on the cloud may lower the false rate alarm, saving companies time and cost. It can handle the large volumes of log-ins and process the data faster. Powered by Google Cloud Platform, the solution can be easily integrated with back-end systems.

Exhibit 4: Benefits of Anomaly Detection solution, powered by the Google Cloud Platform



Why Capgemini with Google Cloud?

Capgemini has over 25 years of experience in working on various banking systems as well as thousands of projects delivered for the Banking and Financial Services industries. Our key differentiating factors include our business-driven approach, proven models, tools and best practices as well as deep domain and sector expertise. Our solutions and frameworks are enriched by our deep experience in delivering financial crime management solutions to banks globally.

In addition, our RightShore® model allows us to leverage more than 500 Fraud/AML analysts along with over 16,000 technology, data science and sector experts from our Insights & Data practice to support our clients.

We have developed proven cloud frameworks with predefined templates and accelerators leveraging our experience of delivering more than 5000 cloud engagements with 300+ on Google Cloud Platform.

Next Steps

You can now arrange a customized, hands-on demo of our Anomaly Detection solution. To set it up or for any other enquiry about the solution, please contact banking@capgemini.com.

"Capgemini has been named a Leader in Gartner's Magic Quadrant for Data and Analytics Service Providers, Worldwide 2018"

About Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms.

Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of 200,000 team members in over 40 countries. The Group reported 2017 global revenues of EUR 12.8 billion.

Visit us at

www.capgemini.com

People matter, results count.