Tecoris

Background

Large organizations are increasingly relying on technology, outsourcing and offshoring important functions. As a result they are dependent on complex and global critical infrastructure. This sprawling landscape beyond a physical headquarters can result in concentrations of technology, which if not identified and managed, can result in major outages and data breaches.

Concentration isn't a vulnerability in itself- rather it works as a multiplier. Instead of a threat (e.g. cybercriminal, inclement weather) acting on vulnerable aspect of technology in a linear fashion, for example causing one application to fail, there can be a much larger effect, sometimes called “blast radius.” Such impacts can include all aspects of the CIA triad- Confidentiality, Integrity and Availability. A Single Point of Failure (SPoF) is often associated with a concentration.

The stakes are high. No organization wishes to receive a regulatory finding, and certainly not public attention for having neglected a brewing situation, allowing for the occurrence of an outage or data breach

Challenges in the Current Landscape

It can be difficult to measure and mitigate concentration risk. In addition to identifying vendors and geographic locations, an understanding needs to be

developed as to how they relate to internal infrastructure and fourth parties such as cloud service providers.

There is a tendency for organizations to allow technology risk coverage to become dominated by governance and policy review. PowerPoint revisions with word salad exercises tend to lack the needed quantitative analysis and actionable insight. Excel and Power BI are popular tools but unable to rapidly fuse complex data and provide an English language explanation. Traditional tools are static and limited, while regulatory expectations and operational risks are dynamic. LLMs are available but most have built-in “guard rails” which result in a refusal to engage in discussion about topics that are deemed offensive or sensitive. This can include current news events, past history such as wars and various conflicts and dangers. Also LLMs are not designed to work with complex custom databases, data workflows, real-time API queries, millions of data records, or complex risk management specialized reasoning. None of the Governance, Risk and Compliance (GRC) products can offer a complete enterprise wide technology view from which concentration conclusions can be formed. There are systems architecture products however their use also tends to produce incomplete, fragmented and dated results, with patchwork access to different users and departments.

First line teams focus on operations and monitoring but rarely aggregate systemic data into actionable risk models. Quantitative analysis of actual technology dependencies can become limited or absent. Second line oversight emphasizes frameworks, processes, and incident reviews, often without the engineering expertise to independently validate risks. The net

result is a blind spot: systemic availability and concentration risks remain un-measured.

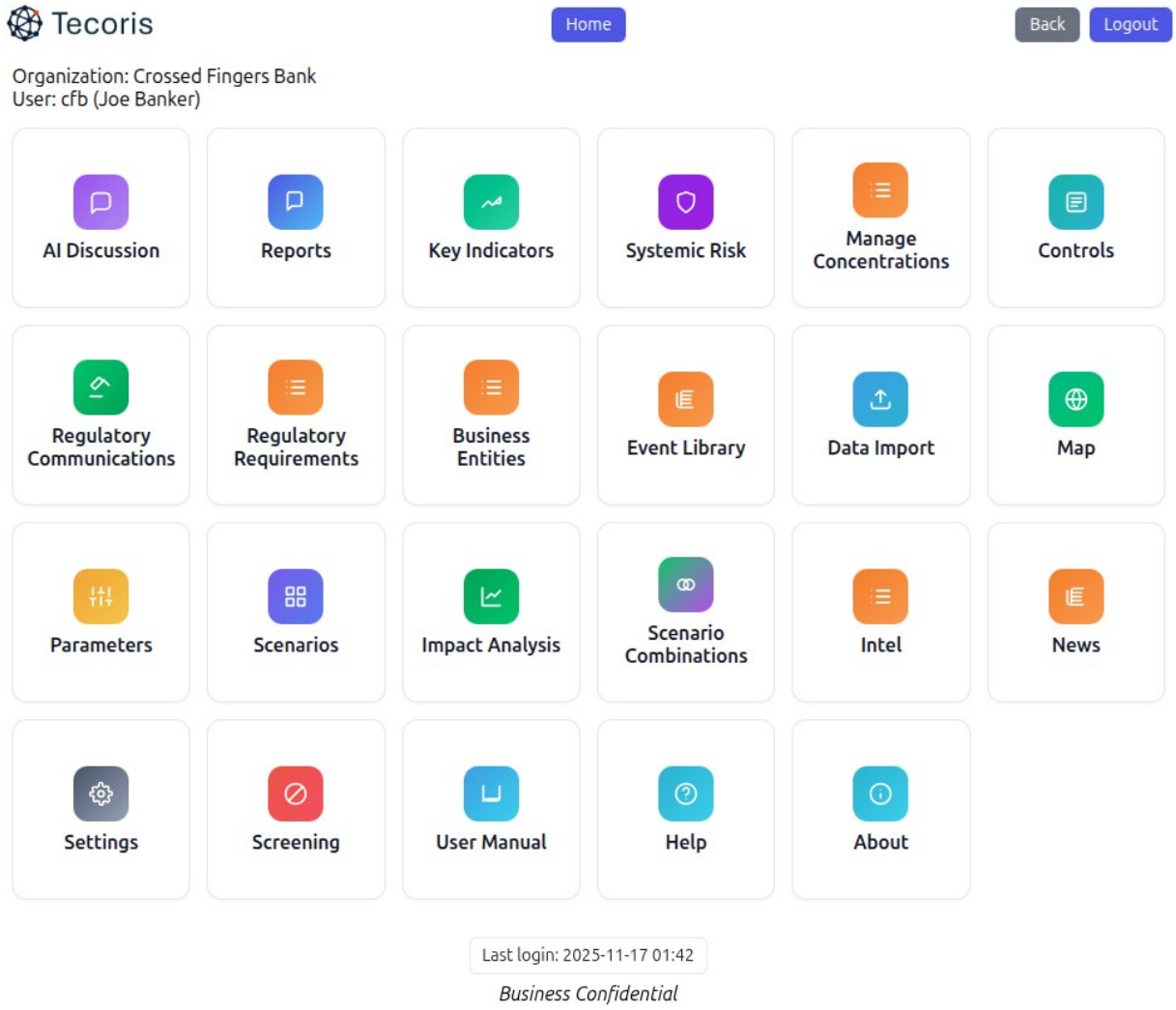
The Tecoris Solution

Tecoris was specially developed to help analyze and manage risk problems. It is available to customers as a cloud based Software as a Service (SaaS) product with a user interface that works on a browser and mobile phone. It is currently in a hybrid configuration with AWS in a US region connected to a data center owned and managed by Tecoris, also located in the US. However this an be configured for individual customers based on their needs. Tecoris was developed in 2025 with modern software on a highly parallel computer architecture. It rapidly processes large data sets with millions of records in seconds. The same calculations in Excel macros could take a year. It focuses on the specialized use case of technology concentration, which led its name, a portmanteau of TEchnology COncentration RISk. The software pinpoints exact geographies and vendors that form concentration risks. But Tecoris goes beyond just finding concentrations. It connects them to the supply chain and critical infrastructure- telecommunications and energy. It determines if or how a concentration is problematic. In conjunction with scenario analysis and AI dialogue, Tecoris aims to be an essential technology resilience intelligence platform.

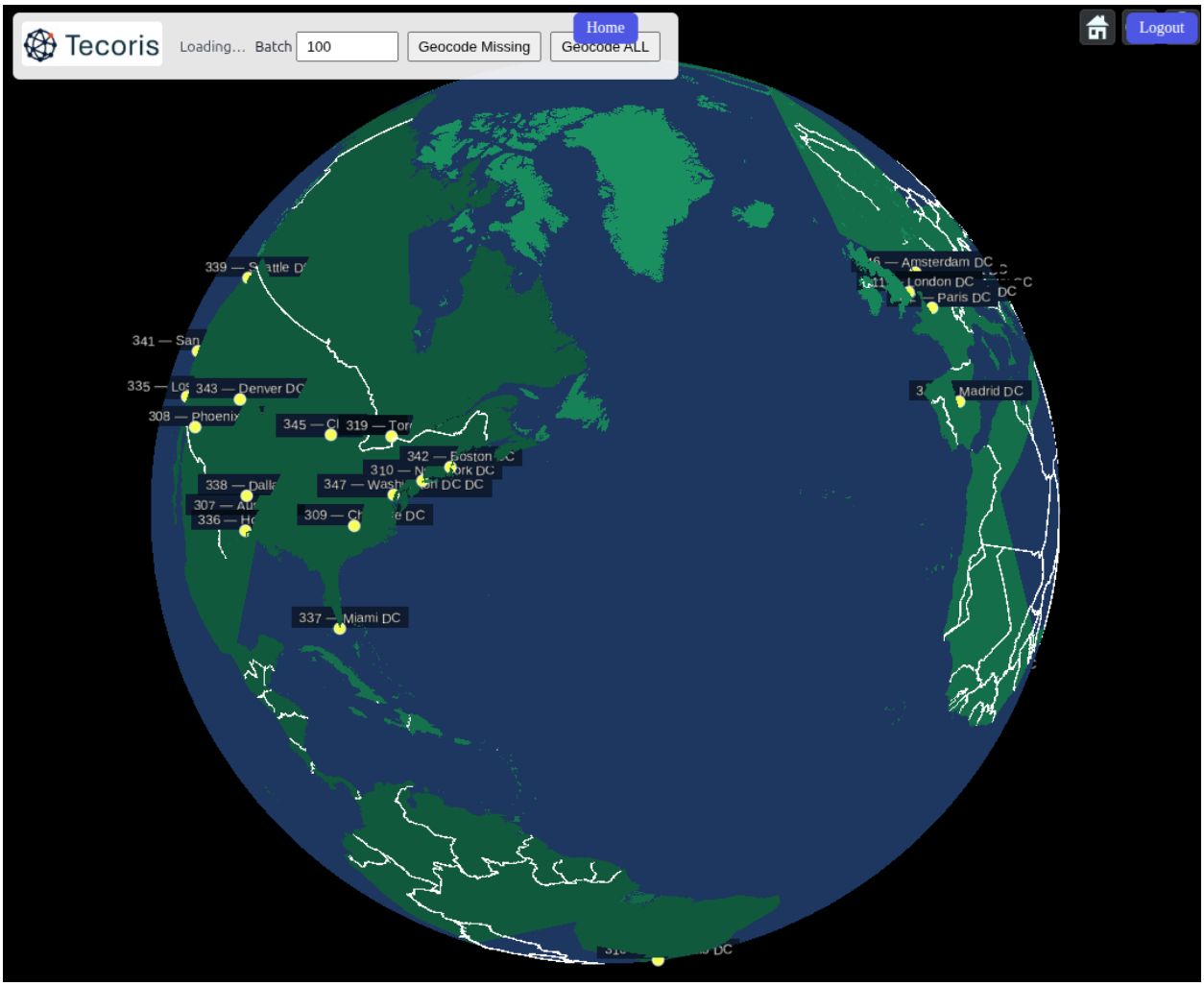
Tecoris can answer questions like:

- What if a cyber attack causes a major power outage?
- What if the Russia–Ukraine conflict spins out of control and causes a telecommunications outage in Europe?

- What if an insider threat at a major cloud service provider decides to cause a deliberate misconfiguration, resulting in an outage?



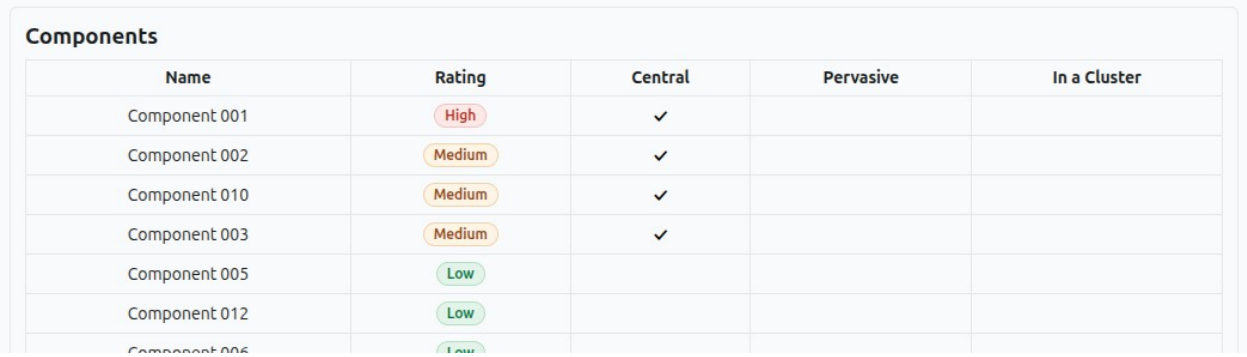
Tecoris provides a number of screens. One is for a map that will show where infrastructure is across on-premise, third party and fourth party data centers.



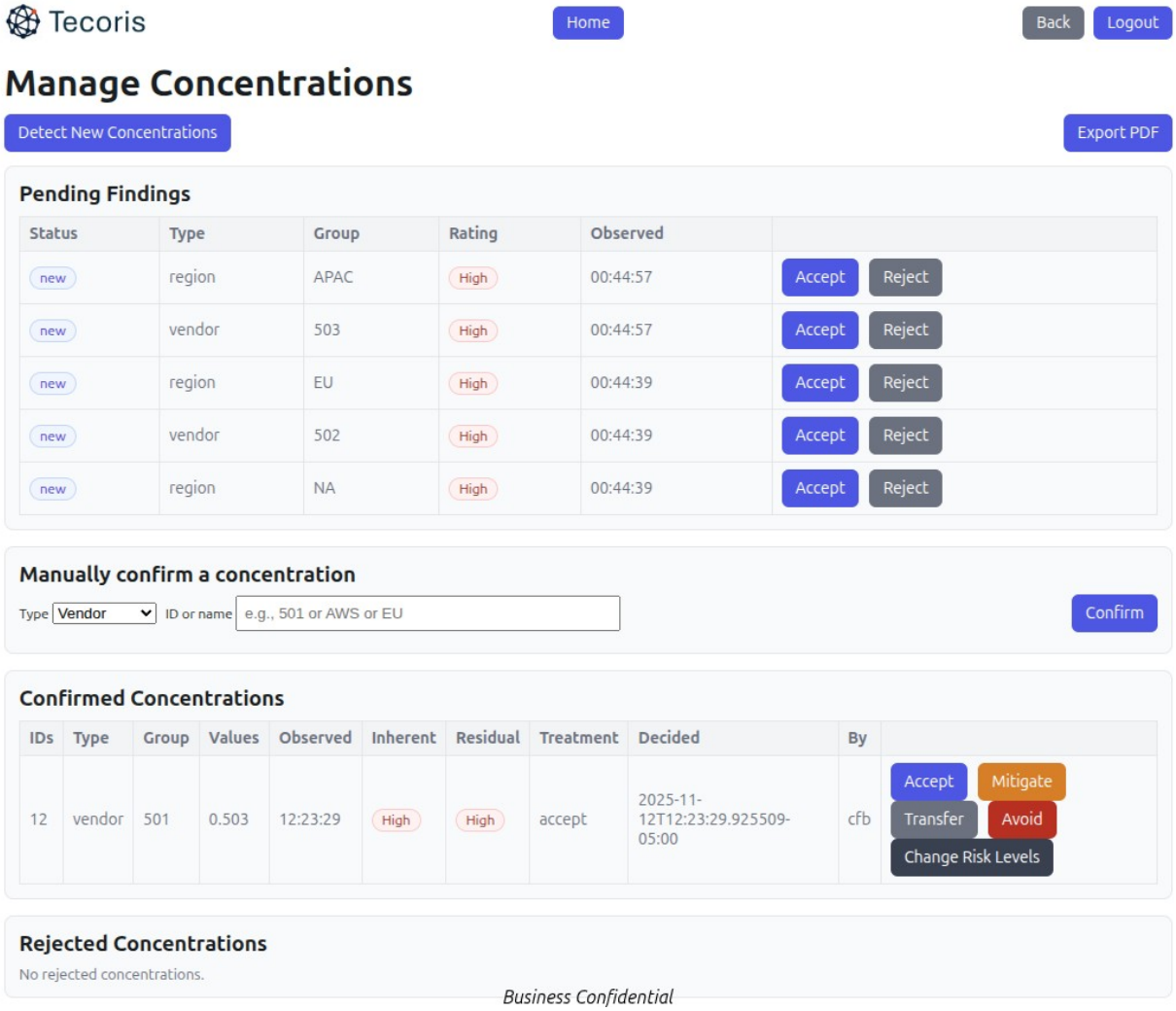
Tecoris was built with organizations' Third Party Risk Management (TPRM) concerns in mind. The product solves technology concentration problems with the smallest data volume at the lowest level of sensitivity. It does not need IP addresses, customer data or financial information. Encryption is provided in transit and at rest. Based on customer needs a customer can hold their own encryption key to their data. There is also a one button delete. The result is generation of evidence-based, repeatable and regulator-aligned results using detailed data but only as much as is needed.

Tecoris design is intended to reduce or eliminate customer concerns about data security.

The cost savings are significant. Tecoris eliminates the need to assemble a team of consultants and employees to spend many months thinking through what the problem is or how to solve it. There is no need to develop an in-house solution in a multi-million dollar gamble, and possibly even more on its maintenance. Tecoris brings a working solution directly to staff, whether they are business or technical, senior, mid-career or junior. It rapidly fills a risk management and regulatory reporting hole that needs visibility.



Actions can be taken to reduce concentrations, which are often focused on improving capacity and redundancy.



Expect a positive Environmental, Social and Governance (ESG) footprint as well. The massively parallel computer architecture of Tecoris, combined with modern power-efficient hardware, means that even complex reports will consume roughly the energy of a single traditional lightbulb running for about a minute. No paper is required in the process. You won’t need a team of consultants flying in jets and driving between hotels and offices. Tecoris manages all physical computing equipment and their end-of-life disposal responsibly. It’s a winning story of efficiency and sustainability.

Have your own real-time intelligence system. Gain the data you need to respond to supervisory requests in minutes. Go beyond direct vendor and geographic concentrations to identify hidden concentrations in your supply chain. Use AI to generate recommendations to solve concentration problems. It’s like having an entire team of technology risk management experts waiting to talk to you 24x7.

Corporate Information

Tecoris, LLC	Ownership: privately held.
Headquarters: New Jersey, USA	tecoris.com
Founded: 2025	ryanmaxwell@tecoris.com

