SBIR · STTR
America's Seed Fund

U.S. DEPARTMENT OF ENERGY | SBIR/STTR Programs Office

COVID-19 has elevated internet connectivity to an essential resource. All aspects of life from education to commerce are taking place in cyberspace. Network connectivity failures can cause costly disruptions. With support from the DOE SBIR program, California-based startup Clostra, Inc. has developed Keymaker, a data analytics platform powered by machine learning. Keymaker's neural network is trained to identify network anomalies more quickly and effectively than other network analytics solutions. When it comes to keeping a network running at top performance, Keymaker outclasses existent platforms by simultaneously learning from existing network data, monitoring current network traffic, and keeping operators informed about significant changes to network behavior.

FACTS

PHASE III SUCCESS
While supported by a DOE SBIR Phase II, Clostra has entered the AI-based analytics market with revenues approaching the original SBIR investment.

IMPACT
Employing state-of-the-art deep learning techniques, Clostra can identify true anomalies in virtually any network.

DOE PROGRAM/OFFICE
Advanced Scientific Computing Research (ASCR)

WWW.CLOSTRA.COM

Most current network analysis tools generate copious false alarms when they base their analysis on static signatures. The static model, which is used by Google Analytics and other top analytics tools, often flags as anomalous an activity that is easily explicable to most human observers. For example, there exist obvious diurnal, weekly, and monthly variations to network traffic. Lower network utilization on Saturday night compared to Monday morning is not an anomaly; rather, it is fully predictable. The way existing tools typically deal with these types of variations is by constructing rough-and-ready heuristics: a deviation of the size typical for Saturday night is deemed normal for the network, even if it shows up on a Monday morning, which typically has higher data flow. Static signatures often cannot take into account basic chronological variability. Rare but predictable events are also disregarded in this type of naive analysis.

Keymaker uses dynamic feedback, training a suite of neural networks to learn what is normal for a specific network, time-series data stream, or other data types (a database containing app behavior, customer activity on a web site, etc.). Keymaker's understanding of what is normal or anomalous for a given network or data stream is based on thousands or millions of features identified during neural network training and leveraged during analysis. Keymaker's use of machine learning allows it to minimize false alarm rates while maximizing the depth and subtlety of its insights.

Keymaker Use Case: NewNode

The first product to benefit from Keymaker is Clostra's NewNode. NewNode is a decentralized content distribution network that is resistant to network disruptions ranging from simple bottlenecks to deliberate censorship attacks. NewNode caught the media's attention in fall 2020 when Belarusian news organizations started using a NewNode-enabled app in response to a massive internet outage, specifically designed to silence protests over a controversial election. NewNode works by connecting mobile device users in a peer-to-peer network that self-heals and scales with the number of users. In this way, users *become* the network and can securely download content even when a central server is down.

NewNode was developed with support from the US Agency for Global Media (USAGM) and its market penetration is being heavily sustained by Keymaker. Based on a unique algorithm that can be trained on any time-series data, Keymaker can detect whether a network is being tampered with or is subject to degradation arising from natural or human causes. "Keymaker can tell us exactly how NewNode behaves, and this knowledge is essential to grow our customer base and find new partners" says Marina Feygelman, executive director of NewNode and the first Keymaker client. By using AI to identify and respond to difficult-to-spot anomalies in network and user activity, Keymaker provides valuable feedback to development teams, while at the same time protecting user' privacy, ultimately resulting in increased numbers of users. Thanks to Keymaker, NewNode subscribers are increasing and currently include nearly 24 organizations and 2.5M users. Most customers are independent news organizations wanting to bypass traffic filtering software and ensure freedom of information in support of democratic principles.

Clostra's approach to SBIR shows that by aligning a startup's R&D to the needs of multiple agencies and programs, different products can be developed separately, and later connected to reach a broader

market. Clostra's networking protocols and applied AI solutions, separately developed with SBIR funds from DoD and DOE, enhance each other synergistically, enabling a better commercialization outcome for the company.

In addition to Keymaker's anomaly detection algorithm, Clostra's deep learning technology solutions are currently used by the defense, medicine, and business industries to provide nuclear material detection and aviation support.

Written by Claudia Cantoni, Commercialization Program Manager, DOE SBIR/STTR, April 2021.