



ZIGHRA'S IDENTITY PROOFING PLATFORM VALIDATED FOR LARGE-SCALE DEPLOYMENTS

Zighra has created an AI-powered continuous authentication and fraud detection solution that creates and monitors behaviour models of users to secure online transactions. Zighra completed a CENG Project to ensure the platform is ready for large-scale deployments as the company expands its market implementations for service providers.

In operation since 2009 and bringing technology to market since 2016, Zighra is a high-growth company from Ottawa, Ontario ensuring the connected economy is kept secure while offering users the choice to maintain control of their privacy. Zighra's identity proofing platform continuously verifies a user's identity by measuring human, machine, and environmental variables. Led by CEO Deepak Dutt, who is a Forbes Technology Council member, Zighra recently made the Canadian Innovation Exchange (CIX) Top 20 list, which charts the most innovative startups across Canada.

IDENTITY PROOFING BEYOND THE PASSWORD

There are a number of different types of cybercrime attacks that devices, apps, and accounts need to be protected against. An important part of this is ensuring that users are who they say they are when making online transactions over the phone, web, or other sensor-based devices. The growing number of instances of stolen credentials, bot attacks, and remote attacks has created a need for user verification beyond the entry of a password. With IoT devices extending to our vehicles, homes, jobs, and everyday life, we need to know it is the genuine and qualified user at all times who is executing the transaction or activity.

ZIGHRA'S PLATFORM

Zighra's AI-powered platform offers fraud detection and continuous identity proofing, protecting against automated and remote attacks and fraudsters attempting to access accounts through readily available stolen credentials. Zighra's platform intakes data and creates a unique user profile with every task performed by a user such as typing, swiping, and tapping characteristics combined with environmental variables.

The platform manages within a defined security threshold that the user must stay within. If the user behaviour model score drops below the threshold, a 'step up' enforcement challenge is requested to ensure it is still the genuine user. If the step up fails, the account can be locked as defined by company policy. Zighra's fast-learning platform needs only 15 user tasks to create a profile and continuously refines the profile over time with every task completed for continued accuracy.

Zighra's platform is flexible and can be integrated seamlessly into applications. Clients of Zighra have the option of deploying the solution 100% on-device, on-premise, or in the cloud. The on-device model is an exclusive patent. Zighra's technology can be integrated into existing web and mobile applications with just a few lines of code. Enterprises can know that they are dealing with the genuine user all of the time. Alerts of anomalous behaviors or non-human traffic allow for appropriate actions.



CENG MEMBERS



HUAWEI



Investir
Ottawa



ribbon



ROGERS™



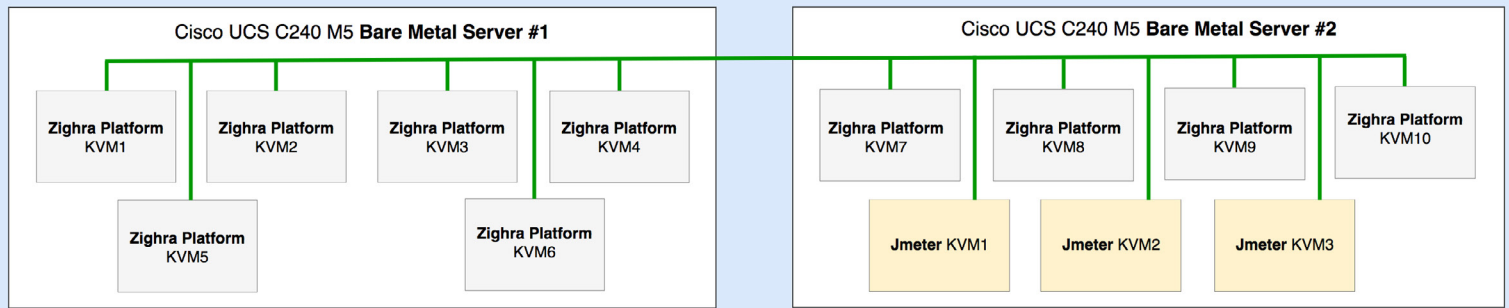
TELUS®





ZIGHRA Dedicated Project Slice

Smart Identity Defense



CREATING ZIGHRA'S PROJECT SLICE

The goal of the Zighra project at CENG was to stress test the Zighra platform under different client scenarios and performance volumes on the CENG infrastructure. Different levels of data traffic were sent to the platform to simulate small, medium, and extra large-sized businesses. This testing allowed the Zighra team to understand the response times of the platform and how it handles the data loads of different throughputs.

Within the CENG commercial-grade infrastructure, Zighra was provided two Cisco UCS C240 bare metal servers where the Zighra platform was deployed along with several Jmeter open source traffic generators. The varying levels of traffic were sent from Jmeter to the Zighra platform and then sent to the database for storage. Throughout the process, response and request turnover times were measured and compared to expected outcomes.

PROJECT OUTCOMES

Zighra was able to successfully carry out the pre-determined 18 different test cases during their CENG project. For comparison, both clear text and encrypted sets of data were distributed, processed, and stored by the Zighra platform. By scaling up the Zighra platform on the CENG infrastructure, the company was able to determine at what level of traffic the processing time begins to fall out of the accepted response time ranges for different architecture setups.

ONE STEP CLOSER TO MARKET

As a company in the early market phase, carrying out this testing at CENG was a real validation for Zighra's behavioural platform under heavy request loads. CENG was able to provide Zighra with a realistic testbed to design and simulate several different scenarios to determine the scalability performance of the platform. Running their platform with a high-level of traffic in a client-simulated environment at CENG allowed Zighra to identify areas for product development before the solution is production-grade for large volumes of data. Zighra was also able to tap into the technical support knowledge of the CENG customer solutions team and work with different open source technologies that they hadn't been exposed to before. As they gear up for high volume traffic implementations, Zighra now has valuable results of their security solution in operation in a scalable and third-party infrastructure that they can show to prospective large-scale service provider clients.