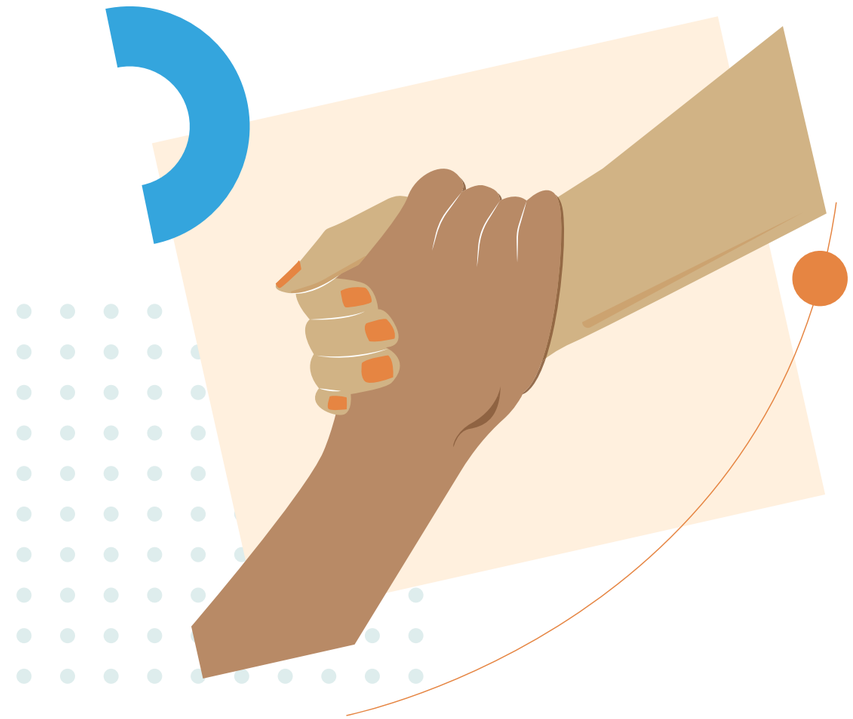
Case study

How SecuredTouch supports exponential growth with GKE



SECUREDTOUCH

Client
SecuredTouch

Location
Israel

Technology
Kubernetes

Industry
Cybersecurity

SecuredTouch is revolutionizing the eCommerce space with its innovative scale fraud detection platform, something it's delivering without over-investing in manpower and resources.

SecuredTouch is pioneering a shift in the way businesses treat fraud detection. Thanks to an innovative approach that injects behavioral biometrics into fraud detection processes, SecuredTouch customers are now reducing fraud rates and lowering related costs, while boosting transaction rates with a hassle-free user experience and fast-track checkout for trusted users.

Multiple fraud use cases are covered by SecuredTouch's turnkey solution – account takeover, new account fraud, loyalty program fraud and payment fraud to name a few. A wide spectrum of attack vectors and malicious tools are also addressed by this innovative tech. The main ones include identity theft, automated scripts (BOTs), Emulators, rooted and Jailbroken devices, and more.

SecuredTouch's cutting-edge platform allows leading Ecommerce companies to identify fraudulent activity in real time across both mobile and web channels by automatically collecting and analyzing thousands of data points generated by human-machine interaction (HMI), session behaviors, highly detailed device attributes, and other relevant network data.

Founded in 2014 and currently operating out of its offices in Israel and the United States, SecuredTouch is already working with top global merchants and financial institutions.

The brief

"At the core of our technology is the collection and processing of behavioral data from the edge devices in real-time," as per Ran Wasserman, CTO at SecuredTouch. "This means that our backend collects touch-screen gestures, mouse movements, device sensors, etc. and crunches this data into risk assessment metrics using proprietary machine-learning algorithms."

SecuredTouch's advanced machine learning models can identify behavioral anomalies that are indicative of malicious intent and attack vectors such as traffic originated by BOTs and emulators. This service has become especially timely as more people are purchasing items and services from home due to the ongoing Covid-19 restrictions, lockdowns, and curfews.

SecuredTouch came to DoiT International with a need for a comprehensive platform to support the delivery of its value proposition to customers in its growing portfolio.

The requirements included extremely high scale (localization features, peak season traffic spikes, compliance and security requirements, etc.) with minimal effect on latency on one hand, while keeping 'lean' and making the best use of resources on the other.

What we did

Finding the right solutions based on a tailored approach

Back in 2016, SecuredTouch revisited its backend architecture and decided to invest in scalable Kubernetes to power the various applicative services and components. External APIs needed to be globally distributed in order to assure low latencies world wide.

The company collaborated with DoiT International to migrate its production to GKE for optimizing resource utilization and costs. All external API endpoints (facing the SDKs and customer backend for API calls) are now being routed via GCP Global Load Balancer using ingress. This drastically reduces the network latency for worldwide distributed clients and provides excellent visibility and monitoring capabilities to help with real-time decision making.

In a nutshell, the entire SecuredTouch ecosystem has been converted into an event-driven microservices architecture. All applicative services and middleware (event bus, databases, web servers) are being managed by k8s – all highly available and scalable to accommodate peak times and on-demand expansions/updates. Applicative services are stateless and idempotent in order to maximize flexibility and improve the ability to scale dynamically.

With the help of DoiT International and Google Cloud Platform, SecuredTouch now has GKE clusters that are smoothly handling all crucial aspects of resource management optimization, such as horizontal auto-scaling and preemptible node-pools.

The result

SecuredTouch has seen its traffic increase by 100x times in 2019 and continued to grow dramatically in 2020, with this growth trend expected to continue. Even though the company is operating at scale and serving hundreds of thousands of concurrent sessions, no dedicated DevOps/SRE is required on its R&D team.

The simplicity and resilience of GCP, talented R&D team and effective partnership with DoiT International is what made this possible.

SecuredTouch, powered by the aforementioned Kubernetes Engine, is currently protecting tens of millions of daily active users for its customers by identifying hundreds of thousands of malicious attempts in real-time with high accuracy levels. This is a win-win situation for all sides involved. As a result, SecuredTouch now provides a unique value proposition that is relevant to multiple markets and developing new product capabilities to remain a global market-leader.

100x
traffic increase

100'000+
malicious attempts identified in real-time

10 million+
daily active users

"Placing our bet on Kubernetes and GCP was a key strategic decision that has paid off. It has allowed us to scale our business quickly while focusing our R&D efforts on SecuredTouch's unique value rather than IT and infrastructure challenges."

Ran Wasserman, CTO, SecuredTouch

DoiT Google Cloud

"With the help of DoiT International and Google Cloud Platform, SecuredTouch now has GKE clusters that are smoothly handling all crucial aspects of resource management optimization, such as horizontal auto-scaling and preemptible node-pools."

Ran Wasserman, CTO, SecuredTouch