GUARDIANKEY

Stronger Authentication!

About

GuardianKey is a solution to protect systems against authentication attacks. It uses Artificial Intelligence to detect if access attempts are from legitimate users. Attackers can be blocked even using the right password. GuardianKey provides an attack risk in real-time based on the user's behavior, threat intelligence, and psychometrics (or behavioral biometrics). You can notify your users, block or log the attempts.

Beyond the security, the GuardianKey solution provides a good user experience, because the user is not required to provide extra information or to execute tasks during the login.

GuardianKey's approach provides a risk assessment in real-time. The events and risks can be explored in the GuardianKey's administration panel.
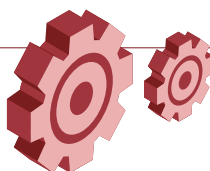
GuardianKey

How it works

The GuardianKey detection engine analyzes the events sent by your online system to the GuardianKey servers. We have a cloud GuardianKey, but you also can deploy an in company GuardianKey version. You should install a plugin in your system or make minor code changes to enable the event sending.

The detection engine uses Machine Learning and our secret mathematical risk formula to combine the following three analysis approaches: Threat Intelligence, Behavioral Profiling, and Psychometric Profiling
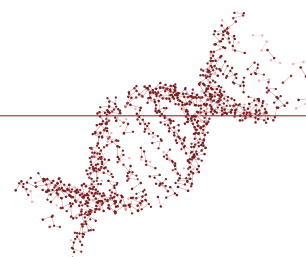
Threat Intelligence

analysis supported by our knowledge base of attacks and attackers on the Internet.

Behavioral profiling

users, in general, interact with systems from the same places, using same devices, during same times in the day, etc. These data are used by our systems to create a profile for each user. The deviations are measured to provide a risk assessment.

Psychometric profiling

The way the user type on keyboard, move the mouse, hold the device (angles, movements, etc.) is particular. Our systems create a profile for such information and use this to compute a user identification metric.

Using these three pillars, our engine computes a risk for each event sent by the protected systems. In real time, the online attempt can be blocked, an extra requirement can be requested to the user, or notifications can be triggered.

Advantages

🛡 Effective against the following threats: Account Takeover, Automated attacks, Brute-force attacks, Anonymization , among other attacks.

👆 Simple user experience.

📊 Simple administration panel.

⚠ Risk based approach, which enables to integrate with risk frameworks.

☁ Available in cloud and in company.

💲 Free, in cloud, for many kind of small environments.

🖥 Supported by Big Data technologies, suitable for (really) large amount of data.

📈 Excellent Return of Investment (ROI).

How much does it cost?

GuardianKey can be purchased as a service, in the cloud, or on-premise. There are three licensing types: per transaction, per nominated user (perpetual), and per nominated user by year (subscription).

The costs for the cloud model can be found at https://guardiankey.io. Contact us for more information about the on-premise licensing.

The costs related to fraud, account takeover, negative marketing, and information leakage can be harmful to any business. In this case, our solution provides a remarkable Return of Investment (ROI)!

Using
GuardianKey

Intelligent security with simplicity is one of our best values. In this way, GuardianKey is created to provide a simple integration. We provide plugins for some applications and reference API code for PHP and Python. You can also develop an integration using our API. Check the API documentation for this.

Check it out at our website!

GuardianKey is managed in a simple web interface, in which is possible to set policies, create authentication groups, explore events, users and risks. You can create an user right now, accessing the GuardianKey Panel. But remember that you must send alerts to enable the processing and visualization.

Contact us

Do you have any question?
Give us an email and we will get back
to you as soon as possible!

✉ **contact@guardiankey.io**

Or visit: **http://guardiankey.io**