**Armour1- The first line of defense for any mode of offence.**

**Launch Date:** 14 October 2021.

Armour-1 helps you find out the abnormal activities within your online business which might be making your business predisposed to cyber-attacks and helps you fight back at it.

**You don’t keep your house doors open for intruders, so why keep your business doors open for cyber attackers?**

Armour-1 helps in detecting any abnormal activities with the online business portal by implementing advance machine learning models to detect any abnormal pattern in the system’s network logs (network reports) and provide the reports with lucid visualizations.

We will provide you with a specialized log generator tool, when installed on the system, will automatically extract all the required (network related) information from your system and hand it over to the anomaly detector. The anomaly detector will search for various trends in the data and identify if a certain activity is deviated from what it normally should be. For example, if the business has trading interests in a certain state but are getting network traffic from different parts of the world. So, in that case, there might be a chance of someone trying to hack/break into their system. The tool will efficiently identify such abnormal activities and report the user through visualizations which are easy to compare and understand. It can also eliminate the time, the labor cost required, and errors related to traditional human based checks to identify abnormal behaviors and provide the results in seconds.

“I am not getting payments for some orders. Now I am afraid something is happening to my system through the network,” said James. The technician who maintains my online business (website) found some strange traffic overseas. It took a while for him to identify the issue using the “TRADITIONAL WAY”. “I hope we have an application that detects this strange traffic and alerts me”

-James (An extremely clueless vendor)

Like James, there are quite a few businesses who if not for the pandemic wouldn’t have shifted to a virtual delivery system. Though they did keep their business afloat while jumping on the virtual bandwagon, there were glaring security issues that needed to be addressed. A serious problem to these businesses proved to be our opportunity and we rolled out Armour-1. These businesses are losing their data which leads to the loss of reputation and profits. One of the reasons for this issue is that they do not invest in infrastructure, this is where ARMOUR1 steps in.

**Quote a Leader:** “Handles like a dream. It truly is a suit of armor for any system”.

What a relief! Armour1 has helped me detect abnormal activities happening on my system. It detects the problems easily and Bob (not the builder), the IT guy can identify the issues and take care of it. I believe it is the best tool to find the abnormal activities on my system by looking at how happy Bob is after using this. Feels like a lot of his work has been simplified by this tool. Cheers! (James owns a bake house)

Armour-1, one of my favorite tools to work with. It generates network logs and analyses them to find anomalies using AI & Machine learning. I can simply get the reports within seconds which are very easy to understand and saves a lot of my time. Now, I don’t have to spend hours inspecting the system reports to find the anomalies within the system and draft a simplistic report for my clients. Really love it! (Bob, IT Technician)

**FAQs**

**Customer Questions**

1. **How to use this platform?**

Our network security log generator uploads you network data onto AWS for us to analyze and detect anomalies.

1. **What is this application used for?**

This application protects detects and protects your data from malicious activity happening through network.

1. **Will the application collect or track my personal information?**

No, application will not collect your personal data. It only checks your network activity logs to detect abnormalities.

1. **Do I need to invest on any infrastructure for your application?**

No, there is no need of any investment on infrastructure. Our IT guy will help you collect and analyze the network logs.

1. **Do I need to have specific knowledge to use the tool? or do I need a technical expert for this?**

We provide excellent IT support with the product that will do all the work for you and in the end will provide you with a simple, yet detailed report of the work done.

1. **Do we need special training for this solution and if yes, then how long will it take?**

The application is designed to be simple and easy to implement, however we have plenty of videos on using the tool by technical specialists available on our website.

**Stakeholder FAQs**

1. **Does my user need to spend more time in learning the technical parts of the application?**

No, your users don’t need to spend time on technicalities. However, we provide the knowledge in form of dashboards and visualizations as recommendations at the end to gain insights for the user.

1. **How does the application handle heavy traffic on the servers?**

Our application is built on amazon EC2 servers, so it can handle heavy traffic with ease.

**Technical FAQs**

1. **How much will this cost SMBs?**

SMBs will be charged for the technician services and a basic charge for our application.

1. **Why would you need to create a tool, if you've got a semi-technical technician that could use existing off-the-shelf applications?**

Off-the-shelf will not provide the up-to-date detector which based on log data. That will affect the accuracy of the detector.

1. **How would this service differ from Zebrium?**

Zebrium focuses on root cause analysis on a broader perspective. While our application is built specifically to address small and medium businesses with their network anomalies.

1. **How would this service be able to be kept up to date with the latest services and threats?**

The model of detector will regularly up to date by connecting to network.

1. **How would you train your technicians to ensure they're able to operate in the field across all operating systems, network devices, and applications?**

Provided a handbook or documentation of operation.

1. **What format would the report be provided in, from the technician?**

Technician provides a report in a simple pdf with log of visualizations.

1. **What happens after the technician leaves? Is there continuous monitoring? Does the technician ever revisit? How is the customer alerted to ongoing or subsequent issues?**

Yes, after our technician installed the tool on your system, the log generator can automatically collect the required log files and supply it to the anomaly detector. The tool will constantly check for abnormal patterns and can inform the concerned customer’s technician that is managing their online business portal.

1. **What if the technician breaks something in the customer's environment during remediation? Who is liable?**

That will depend on the situation or remediation requirements. We audit the environment to make sure if it is technician's fault.