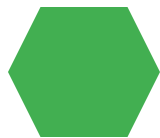


KOYYA NAGA DURGA  
PRASAD

KEYLOGGER AND SECURITY



PROJECT TITLE

KEYLOGGER

AND

SECURITY

# AGENDA

- Understanding Keyloggers
- The security threat
- Introducing our solution: Keystroke Guardian
- The value proposition of Keystroke Guardian



# PROBLEM STATEMENT

- Keyloggers are malicious software or hardware tools that record a user's keystrokes.
- They can steal sensitive information like passwords, credit card numbers, and personal data.
- Traditional security measures often fail to detect keyloggers.
- Keylogger attacks can lead to financial loss, identity theft, and data breaches.





# PROJECT OVERVIEW

- Keyloggers are malicious programs or hardware devices that record a user's keystrokes.
- They can be installed on computers, phones, or tablets without the user's knowledge.
- Keyloggers can steal sensitive information such as passwords, credit card numbers, and personal messages.



# WHO ARE THE END USERS?



- **Individuals:** Anyone who uses a computer, phone, or tablet is at risk of keylogger attacks.
  - **Businesses:** Businesses are prime targets for cybercriminals seeking to steal financial data or intellectual property.
  - **Organizations:** Organizations that handle sensitive information, such as government agencies and healthcare providers, need robust protection.
- 
- 

# YOUR SOLUTION AND ITS VALUE PROPOSITION



- **Unparalleled Keylogger Detection:** Our advanced algorithms surpass traditional antivirus in identifying and blocking keyloggers.
- **Real-Time Monitoring:** Keystroke Guardian provides continuous vigilance, safeguarding your data from unauthorized capture.
- **Lightweight and User-friendly:** Our software operates seamlessly in the background without compromising system performance.

# THE WOW IN YOUR SOLUTION



- **Keystroke Guardian goes beyond simple detection. It analyzes user behavior to identify anomalies that might indicate a keylogger.**
- **This advanced feature provides an extra layer of defense against even the most evasive keyloggers.**





# MODELLING

## **Behavioral Modeling:**

This model focuses on how a keylogger operates within a system. It represents the keylogger's interaction with the user's device and data.

## **Anomaly Detection Modeling:**

This model focuses on identifying deviations from normal user behavior that might indicate the presence of a keylogger

# RESULTS

To access the keyboard stroke what we type by using the keyboard that all information save hackers device.