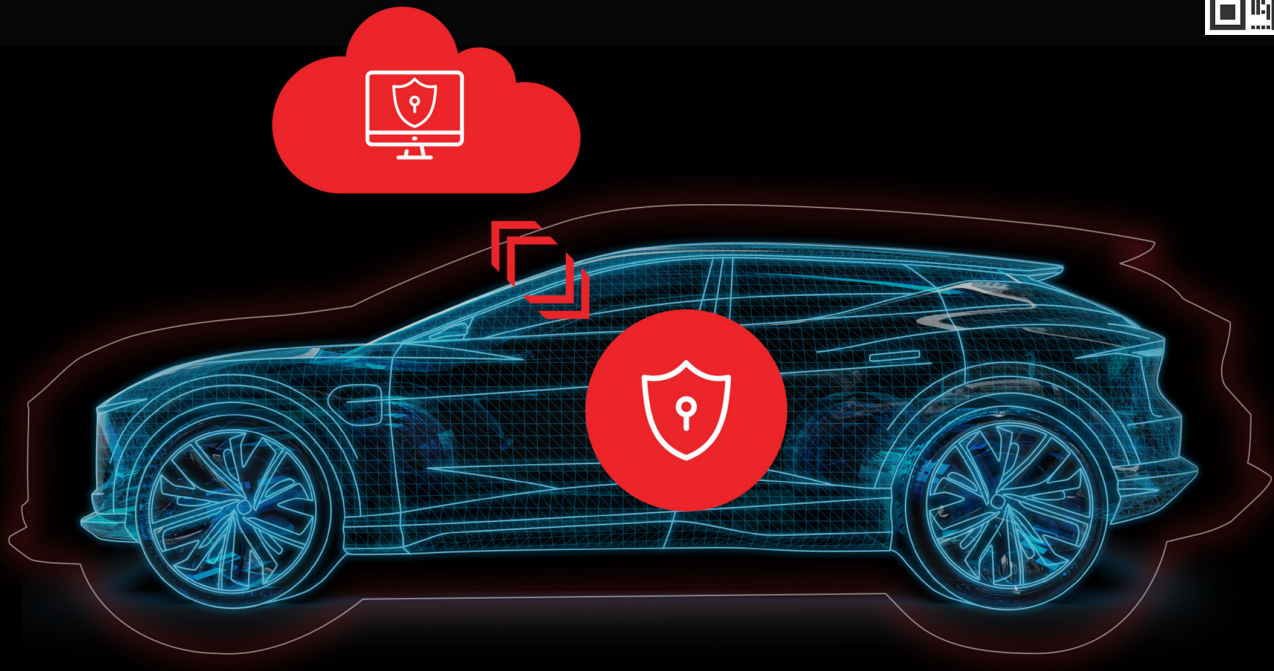


# Sonatus Guard

Secure software infrastructure from cybersecurity threats



**Proactively address automotive cybersecurity threats across millions of vehicles.**

## Protect vehicle software infrastructure at scale

Sonatus Guard protects against known and emerging threats across key vehicle software infrastructure elements at scale.



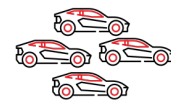
### Multi-layered security

Single solution provides intrusion detection and prevention across vehicle networks, ECUs and communications modules.



### Proactive response to threats

Utilize the cloud-based console to detect known and emerging threats early, and respond with instant policy updates to mitigate.



### Highly scalable policies

Early detection on a few vehicles can be used to create automated mitigation policies that can be dynamically applied to known vulnerable vehicles or fleet-wide.

# Sonatus Guard features

In-vehicle and cloud software work in tandem to provide intrusion detection and prevention services across critical vehicle software infrastructure.

## Apply multi-layered security

- CAN and Ethernet IDS
- ECU Monitoring Agent
- Log Analysis Service
- Network firewall
- Optimal CPU and memory usage

## Monitor, analyze and mitigate threats

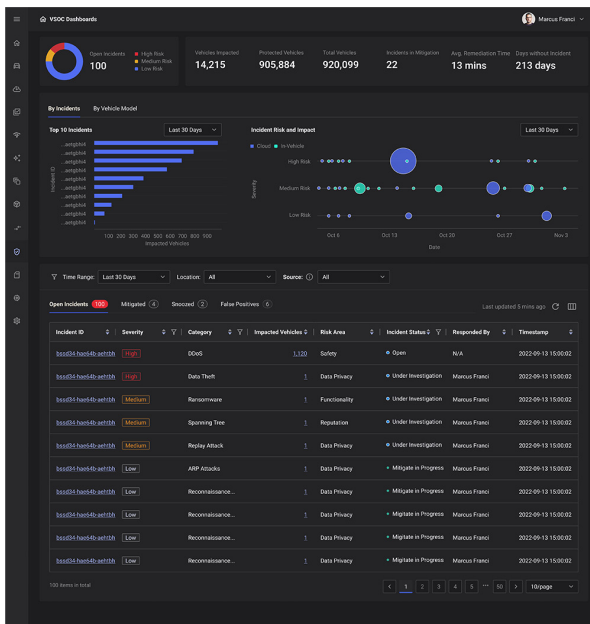
- Consolidated vehicle-wide monitoring
- Incident analysis and correlation
- Ransomware, DDOS, Diagnostic Attacks, and more
- Isolate rogue ECU and applications
- Recommendation on mitigation policies

## Proactively protect at scale

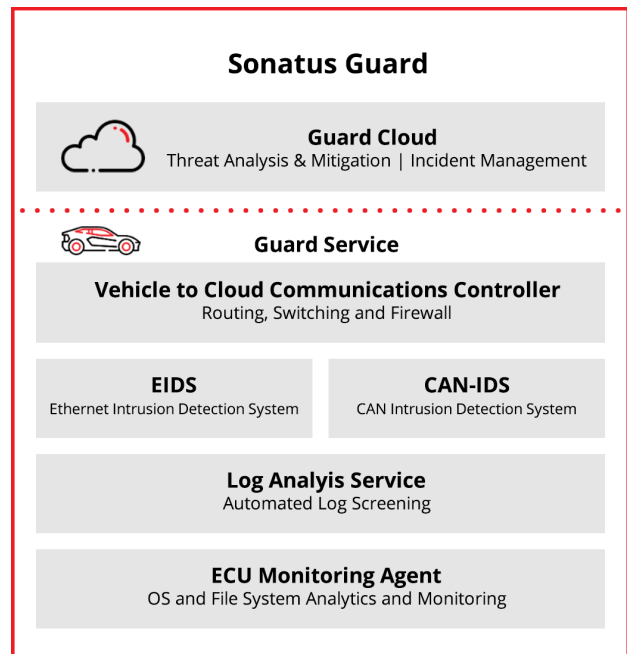
- Highly configurable mitigation policies
- Apply with automated workflows
- Real-time application

## Complement 3rd party solutions

- Extensive set of APIs for integration
- Vehicle hardware agnostic
- Works with either CAN or Ethernet networks
- Integration with 3rd party intelligence feeds



Threat monitoring dashboard on Guard Cloud Console



# Standards Supported

