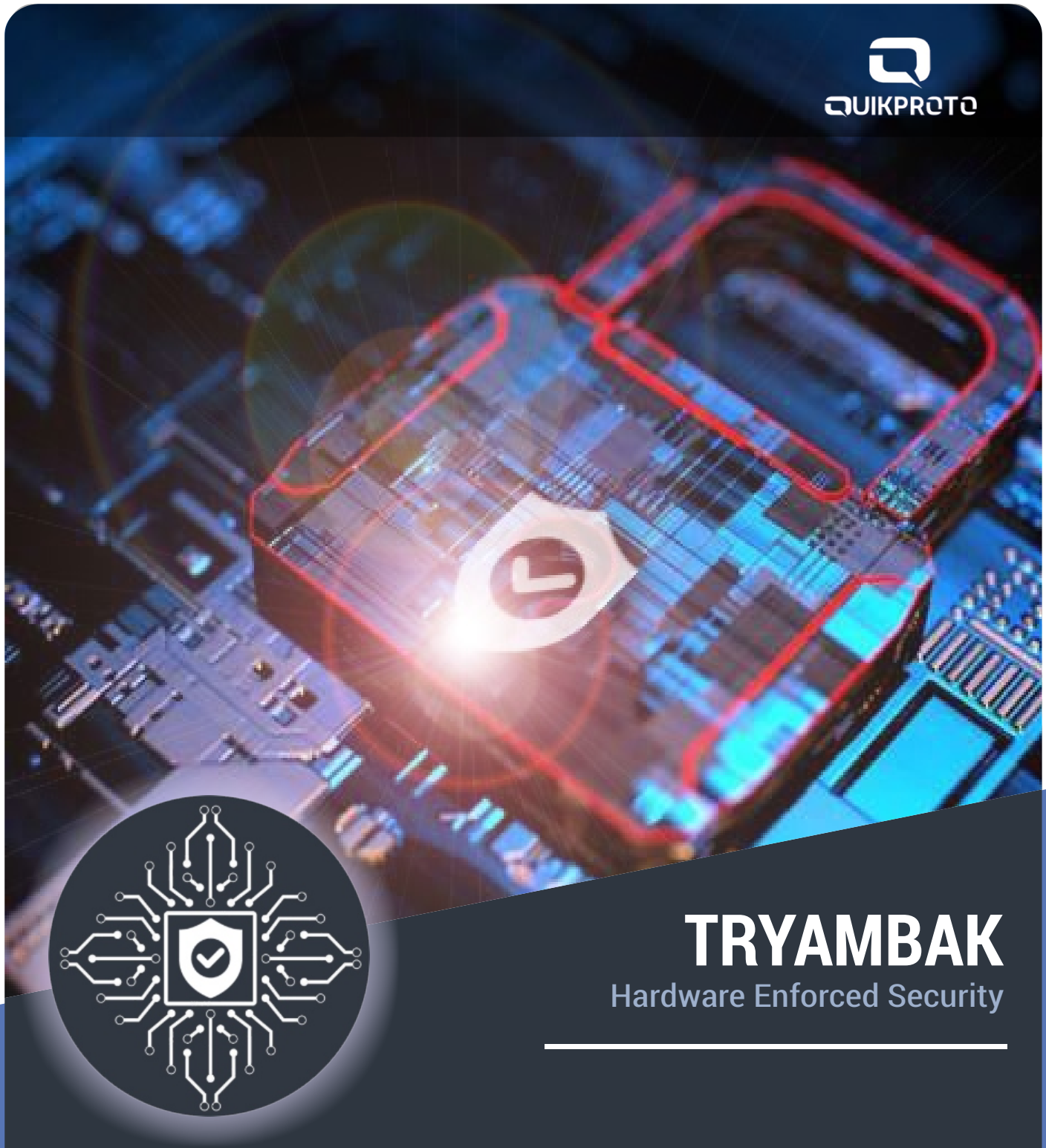


TRYAMBAK

Hardware Enforced Security

Background

The conventional perimeter, end point, server, DC security is proving inadequate against APTs and Zero Day cyber-attacks. The threats are getting compounded when malware is driven through AI tools. The IOT, embedded, 5G and Cloud infrastructures are the emerging victims.

Hardware Enforced Security (HES) – The Emerging Security Paradigm:

Hardware Enforced Security (HES) refers to protecting a system against malware attacks by leveraging security features provided by the hardware.

Security Threats in a Monolithic OS:

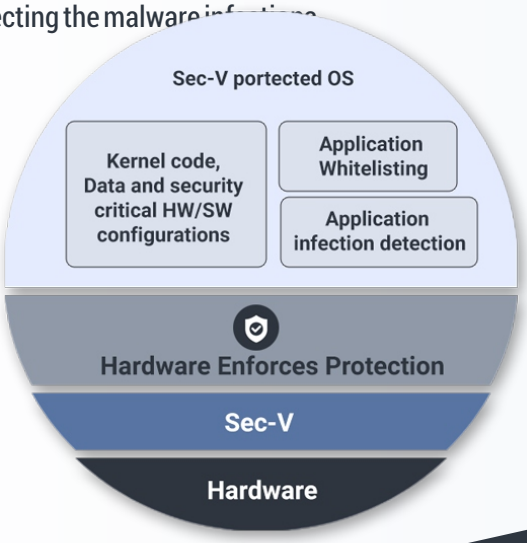
There are inherent limitations on security posed by most popular general purpose Operating Systems (OSs) such as Linux, Windows etc. which are monolithic in nature and have an exceptionally larger user base. Monolithic design was preferred over these OSs as it provides speed and ease of development. Security did not figure as a primary design consideration.

From a security point of view, monolithic design is flawed as a compromise in any part of the kernel, which can result in the attacker completely owning the system.

QuikProto Research Lab's Solution for Securing Monolithic OS from Kernel Mode Attacks

Here QuikProto's kernel protector variant of secure hypervisor (Sec-V) provides security against kernel mode exploits. The Kernel protector variant of Sec-V is designed to protect the systems against kernel mode threats originating externally as well as internally (insider attacks).

In addition to kernel protection, this solution also guarantees hardware enforced application white listing as well as hardware enforced application screening for detecting the malware infections.



Separation Kernel Hypervisor:

Despite the security flaws present in the monolithic operating systems, the fact remains that Linux and Windows are two of the most popular operating systems (OSs) in the world and have the lion's share of market in desktops, laptops, public cloud and even mobile market. Due to the immense industry proliferation of these OSs as well as end user familiarity that has been built over a long period of time, it is not practical to assume that the world will move away from the monolithic OSs now or in the near future despite the security holes. There have been independent efforts such as the Qubes OS which is an OS with separation kernel features built-in, but the usage of such efforts is restricted primarily to academia and amongst hardcore security professionals.

Acknowledging this fact, separation kernel hypervisor technologies have evolved to support the monolithic OSs as well as the custom OSs running as virtual machines (VMs) with hardware enforced isolation to ensure that these VMs cannot influence each other's functions.

QuikProto Research Lab's Hardware Enforced Security Platform:

QuikProto Research Lab recognizes the above-mentioned factors and the need to serve various segments of the industry. Consequently, Quikproto has evolved the architecture and design of its hardware enforced security platform (a.k.a TRYAMBAK) to cater to multiple industry segments.

Quikproto Research Lab also recognizes the need for building an indigenous solution, considering that imported solutions if any, come with the possible threat of backdoors and hence not suitable for projects critical for national security.

QuikProto Research Lab's Separation Kernel Hypervisor

Quikproto has examined available research on the existing threat landscape, and have identified the diverse industry needs for security as well as the current hardware enforced security solution by industry leaders described above, Based on these research inputs QuikProto's R&D team has evolved a unique separation kernel architecture that would cater to multiple industry segments.

The QuikProto's separation kernel flavor of Sec-V, hosts multiple VMs and provides secured communication channel between VMs of different trust levels. The architecture is flexible to support multiple industry segments. A brief overview of these varied use cases is given below with examples of how one of the existing and proven hardware separation solution handles the same.

Target Segments of QuikProto Solution:

01 Mobile& Wireless Applications

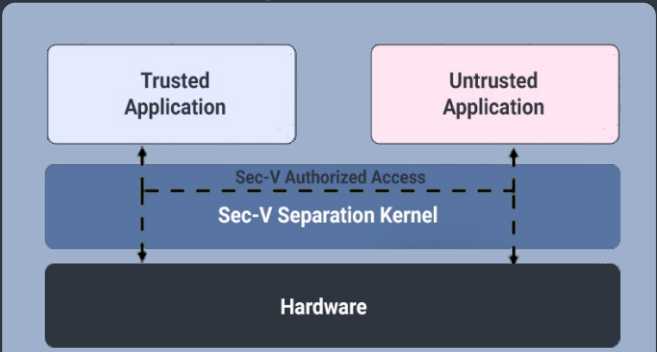
02 Embedded / Aerospace / Defense Applications

03 Enterprise Applications

04 ·Data Center and Cloud

QuikProtoSec-V Approach:

Sec-V in separation kernel mode employs a multilayered security approach by separating the system components into isolated virtual machines with policy enforced inter VM communication. Hardware enforced separation of applications with restricted and secure inter application communication mechanisms result in a highly secured environment with a much-reduced attack surface where multiple secure and non-secure applications can exist.



The Sec-V separation kernel architecture recognizes that VMs hosted in isolation with a secure communication channel can cater to multiple industry segments. Therefore from ground up the design of the hypervisor is focused on being capable of serving these various segments with as much commonality as possible.

Apart from providing security by isolation, QuikProto solution can also integrate the kernel protection and sandbox features in separation kernel hypervisor to provide highly secured VMs as well as advanced malware reverse engineering capabilities.

www.quikproto.com

info@quikproto.com

Incubated Under Electropreneur PARK

DSCI PROMOTING DATA PROTECTION A NASSCOM Initiative

MEMBER NASSCOM MEMBER

QUIKPROTO