Windows® 8 ELAM

Too late, too little!

Abhijit P. Kulkarni & Prakash D. Jagdale
Quick Heal Technologies

Quick Heal
Security Simplified

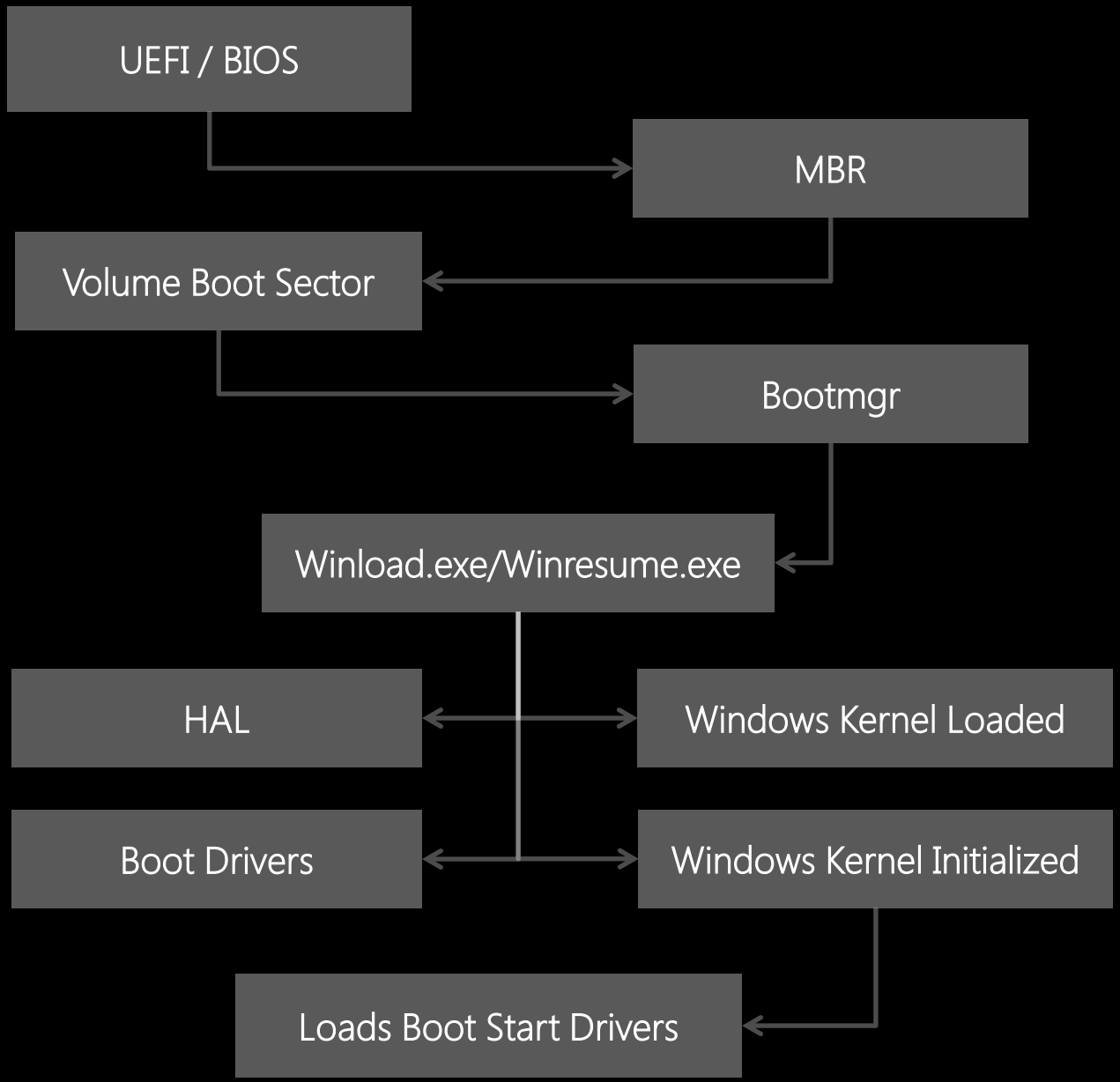
3 Things

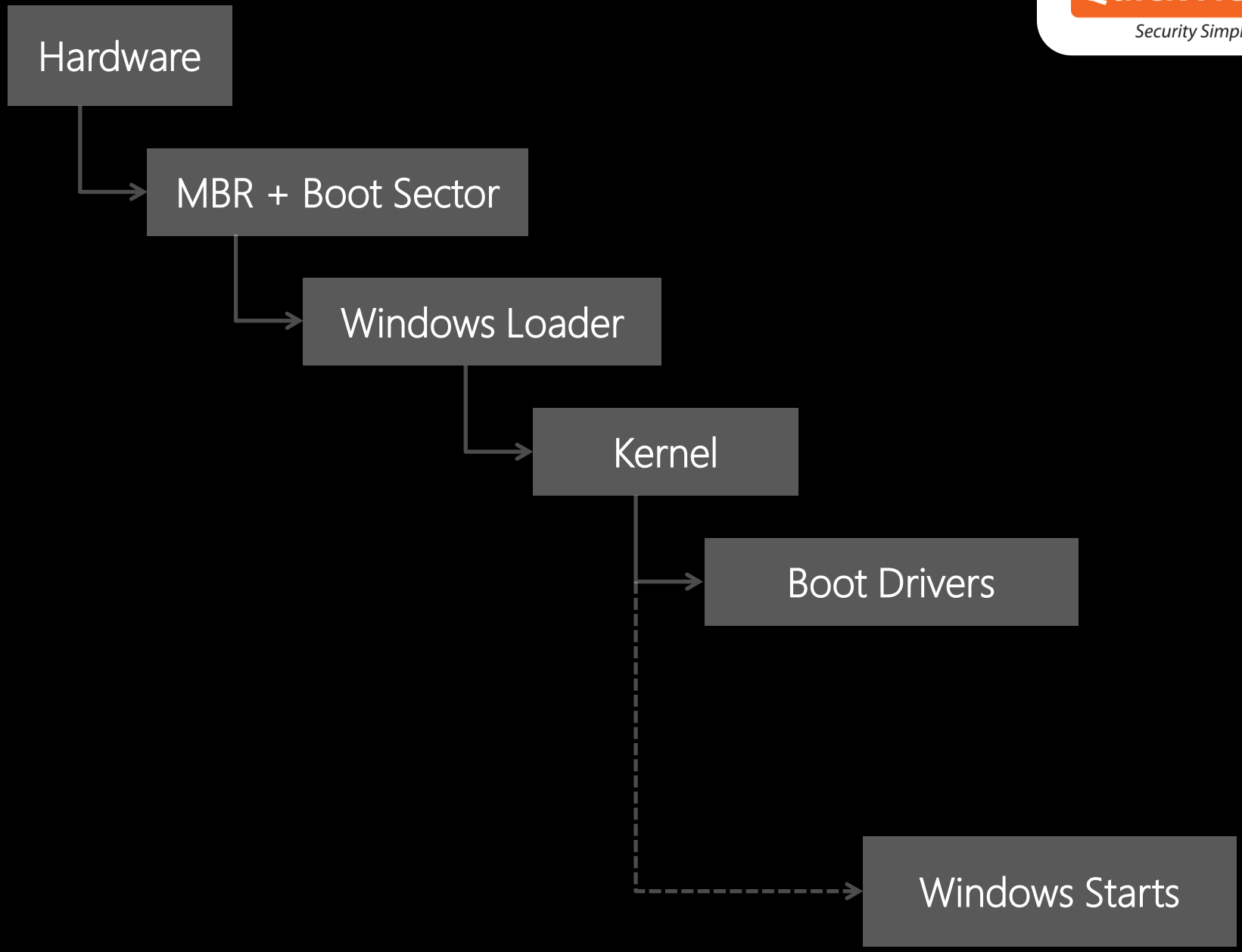
Limitations

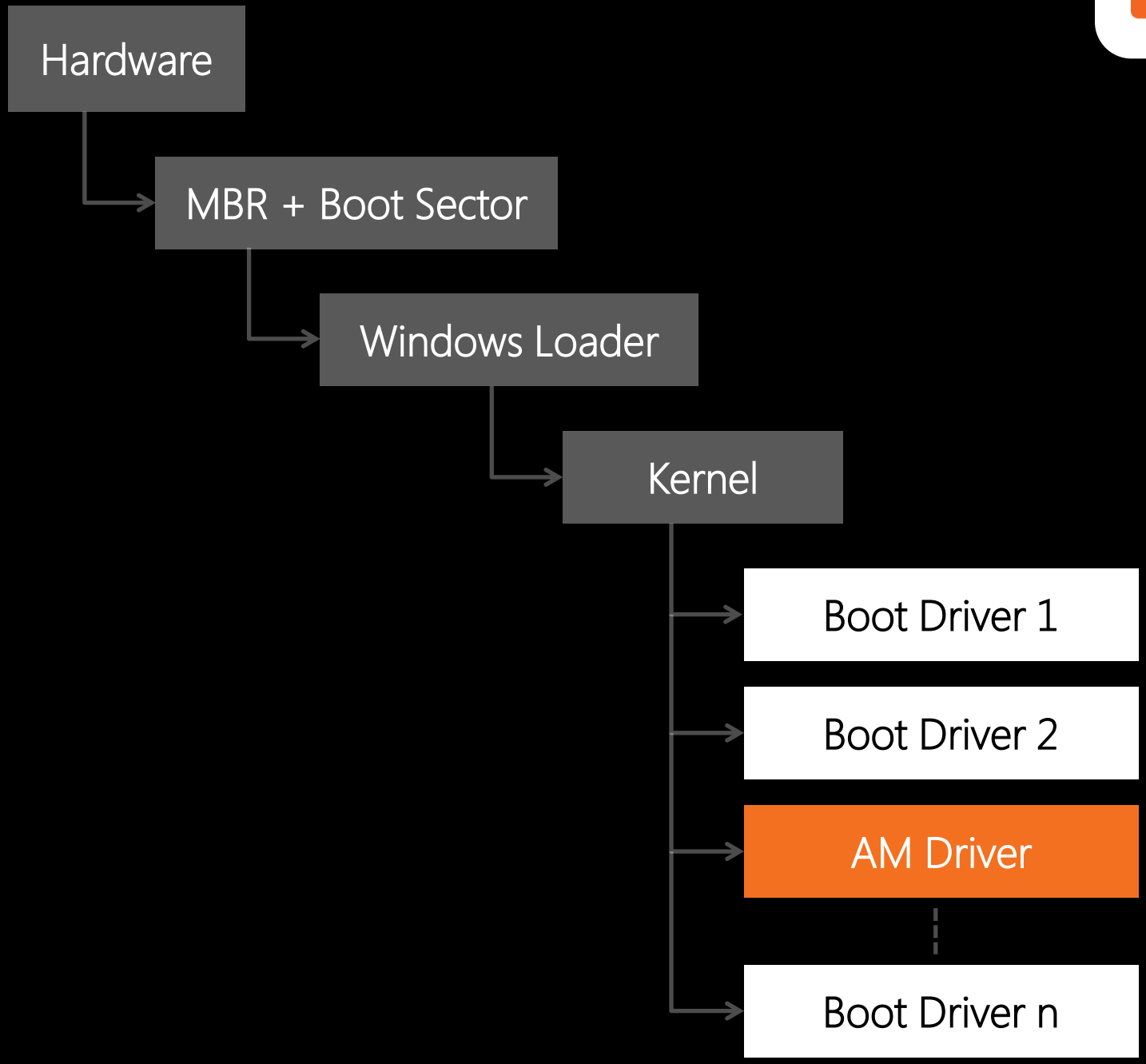
Usage

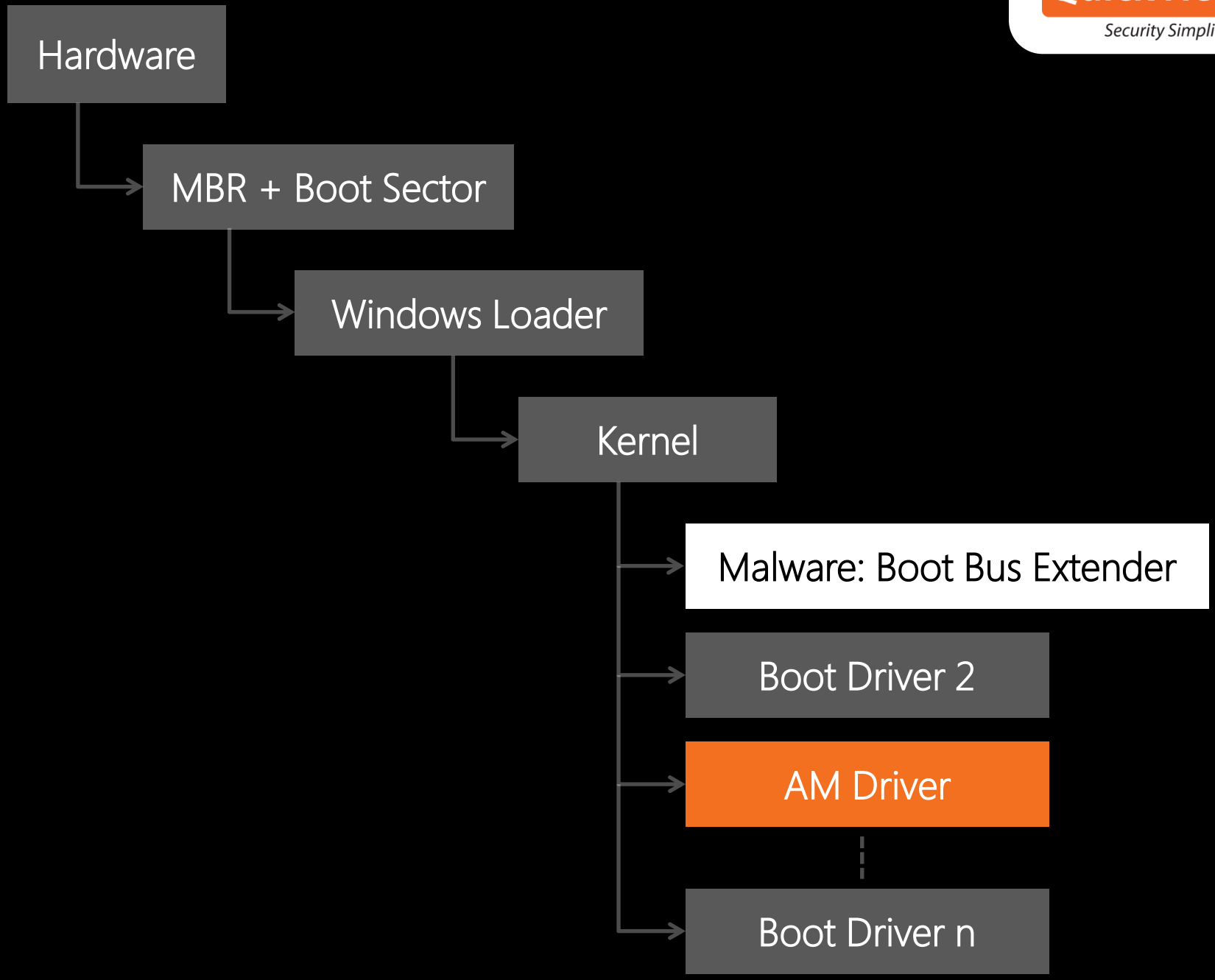
Enhancements

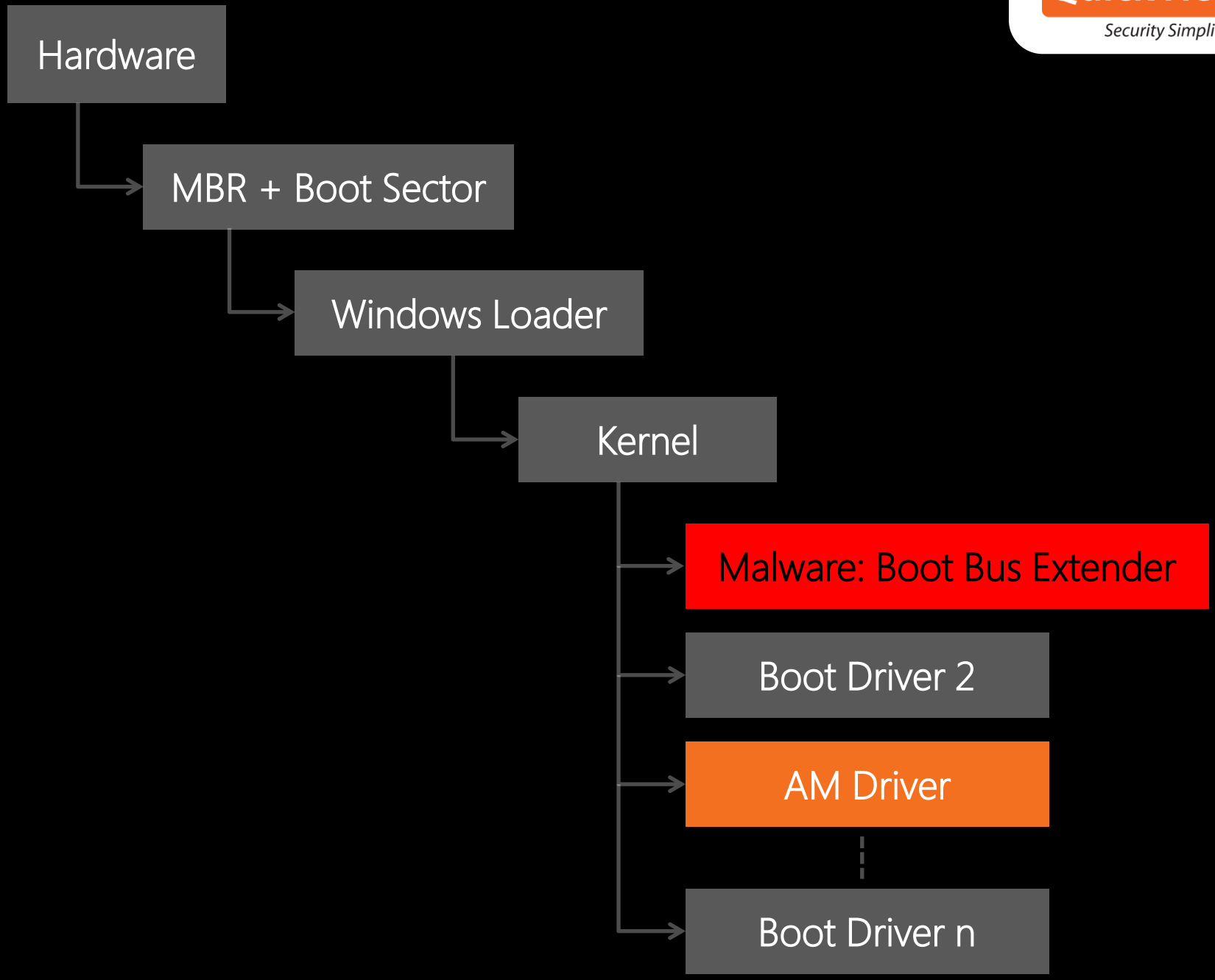
Quick Heal
Security Simplified




Hardware
MBR + Boot Sector
Windows Loader
Kernel
Boot Drivers
Windows Starts


Hardware
MBR + Boot Sector
Windows Loader
Kernel
Boot Driver 1
Boot Driver 2
AM Driver
Boot Driver n

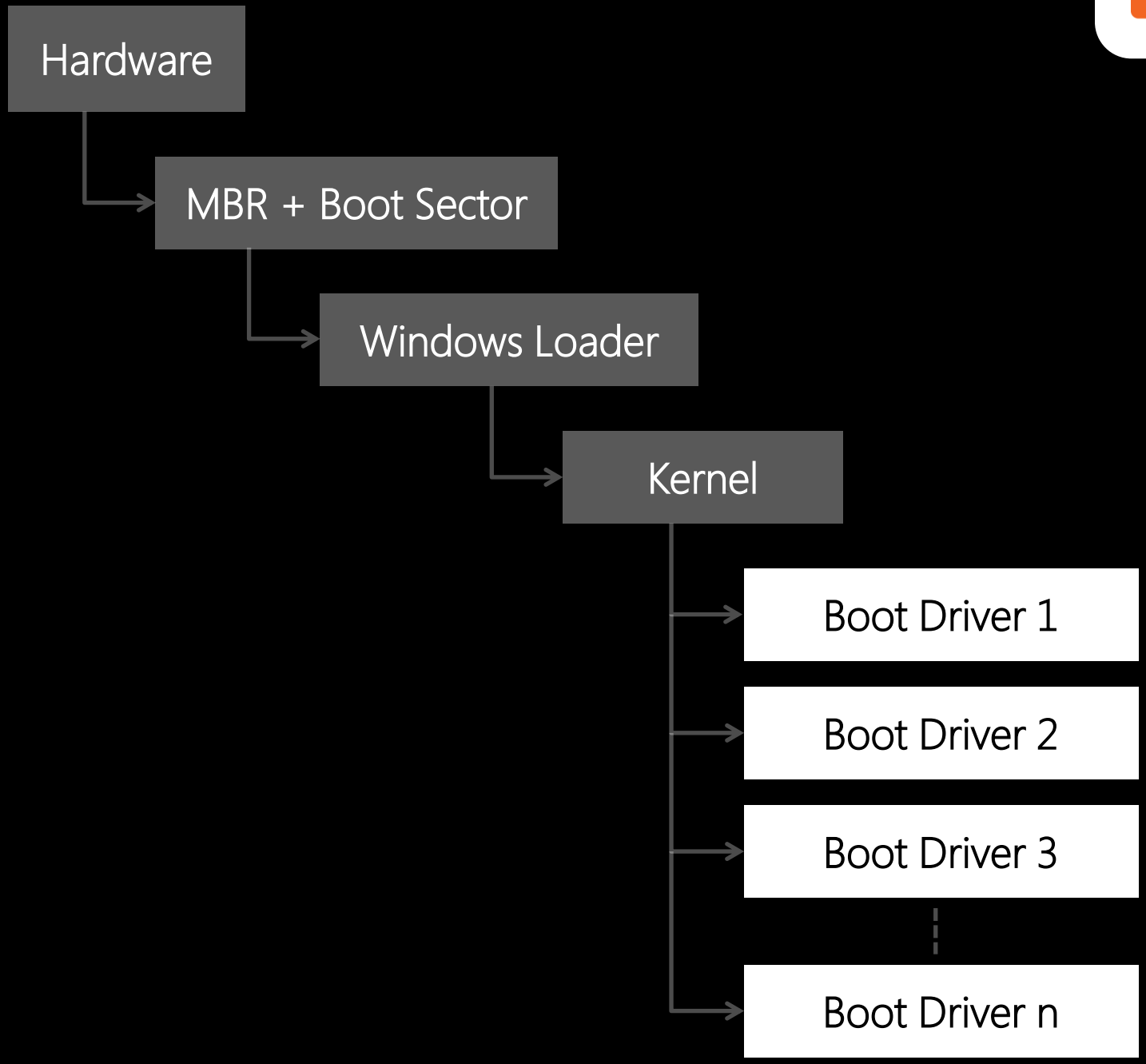

Quick Heal
Security Simplified
Hardware
MBR + Boot Sector
Windows Loader
Kernel
Malware: Boot Bus Extender
Boot Driver 2
AM Driver
Boot Driver n


Quick Heal
Security Simplified
Hardware
MBR + Boot Sector
Windows Loader
Kernel
Malware: Boot Bus Extender
Boot Driver 2
AM Driver
Boot Driver n

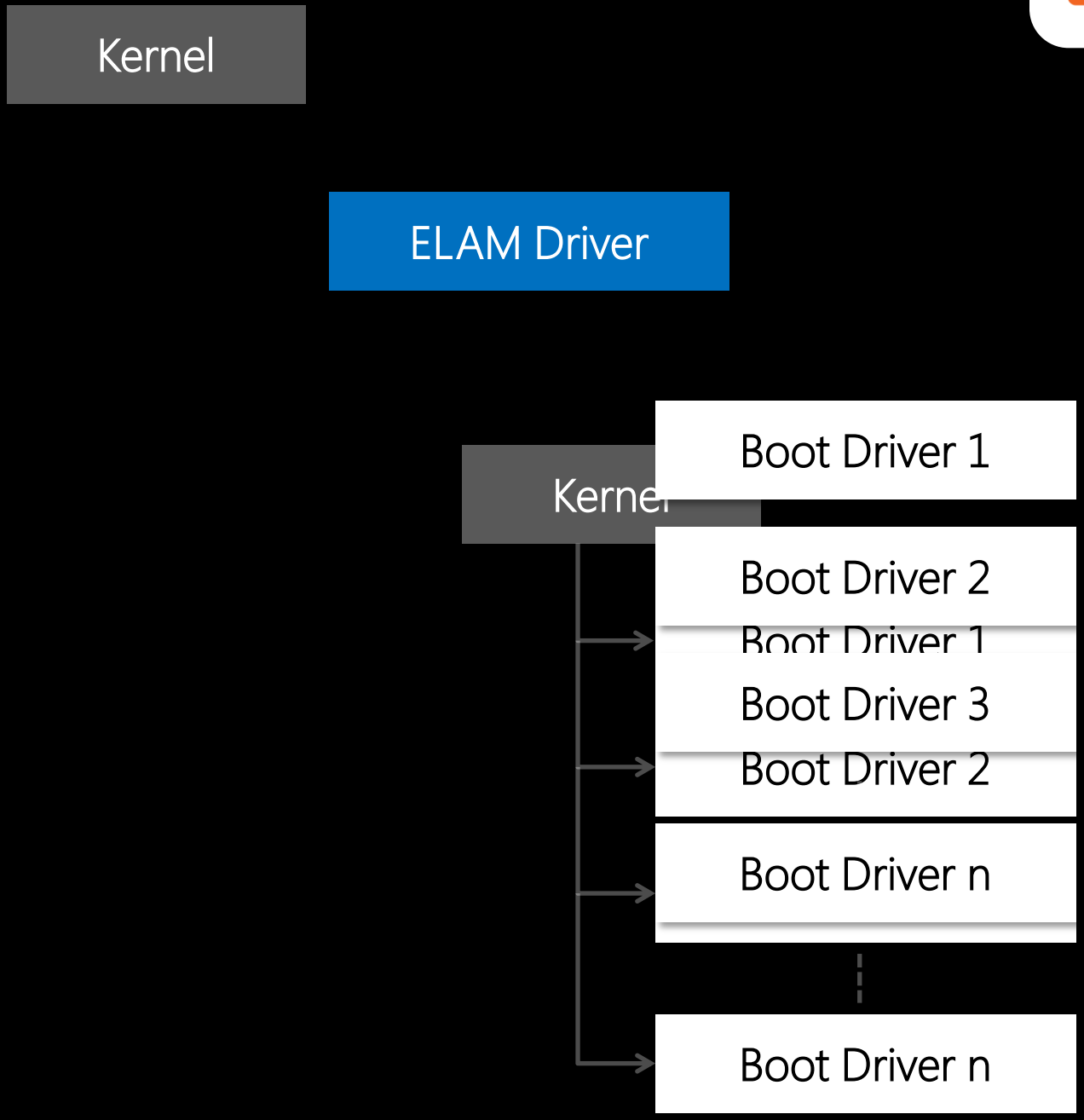
Quick Heal
Security Simplified

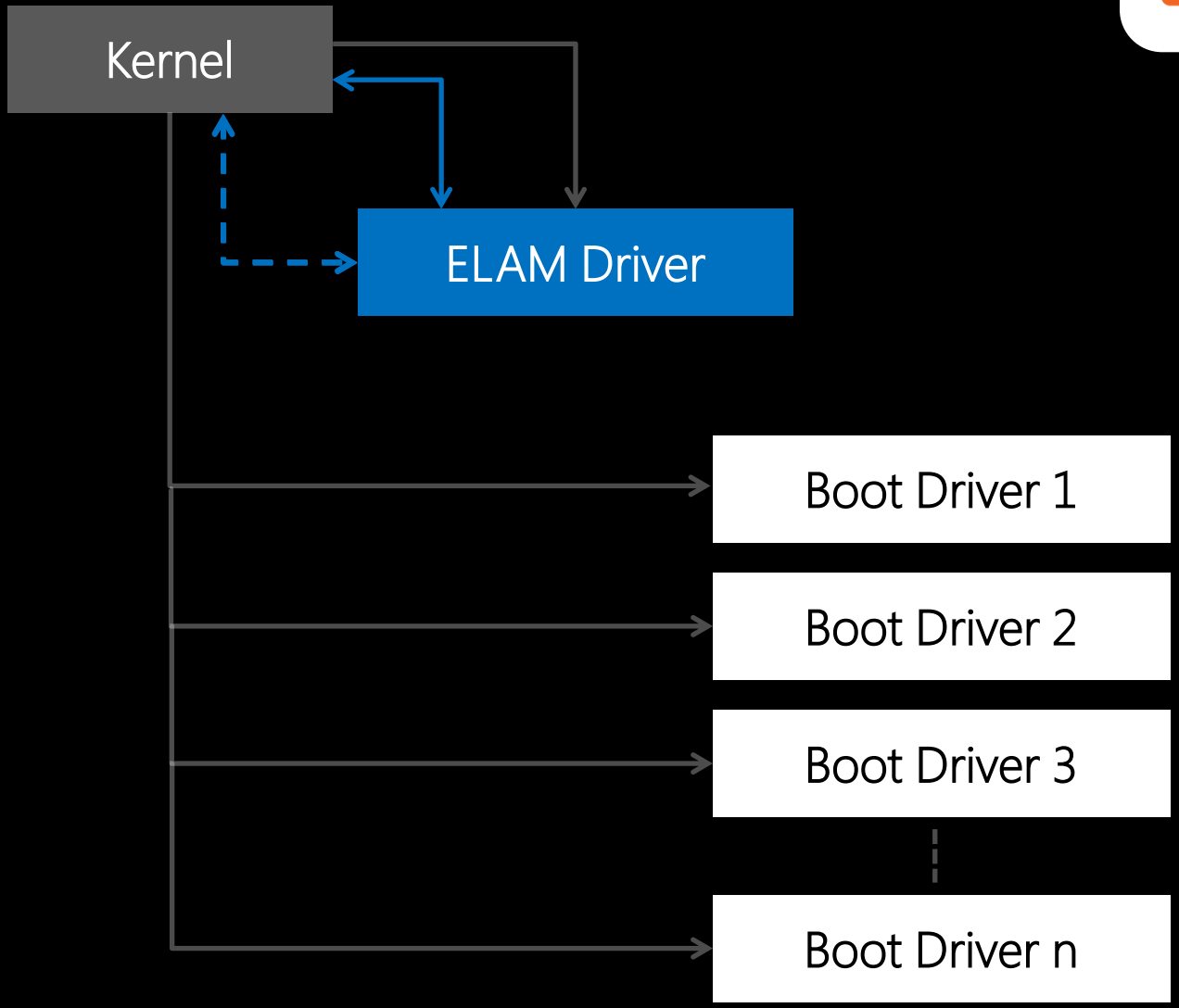
On Windows 8

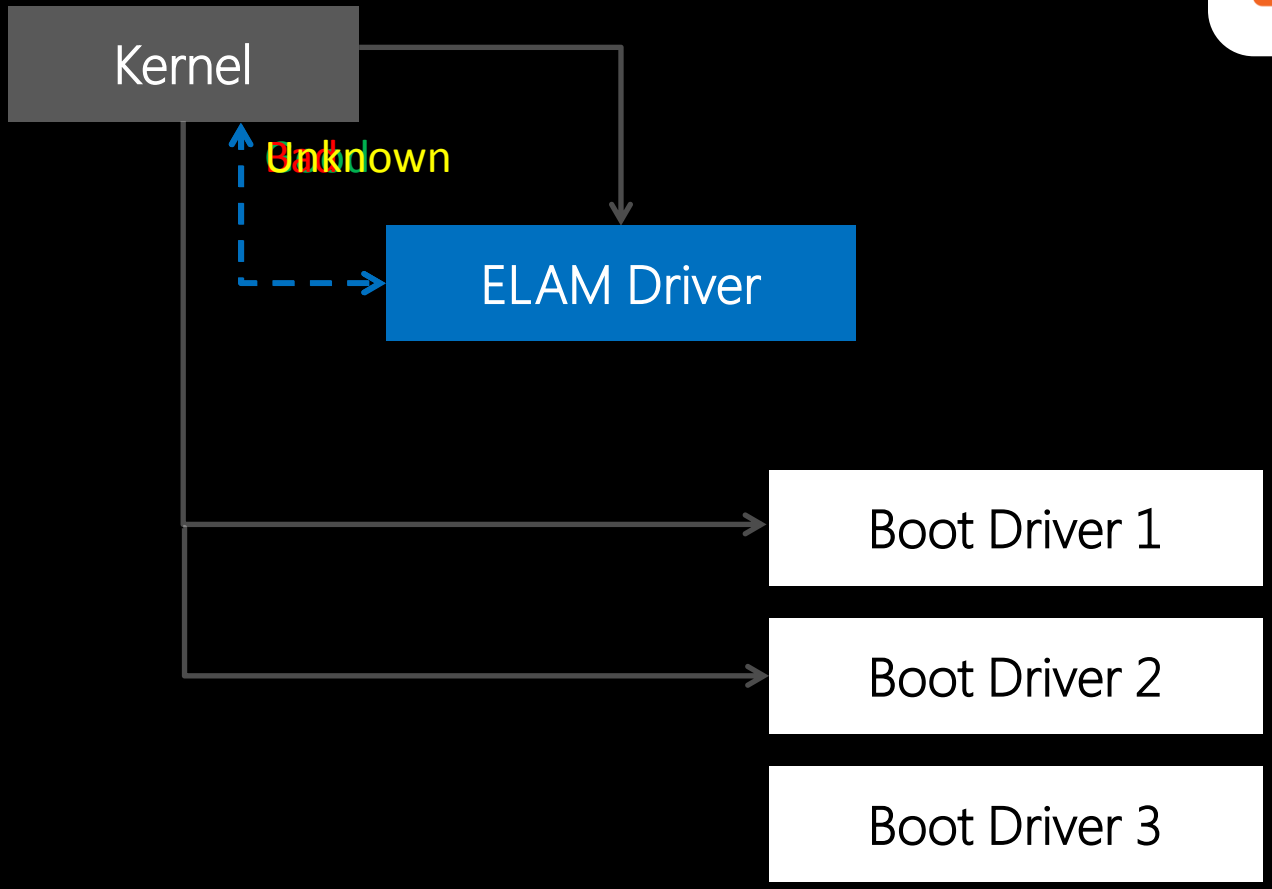
ELAM


Hardware
MBR + Boot Sector
Windows Loader
Kernel
Boot Driver 1
Boot Driver 2
Boot Driver 3
Boot Driver n

Quick Heal
Security Simplified




Kernel
ELAM Driver
Boot Driver 1
Boot Driver 2
Boot Driver 3
Boot Driver n


Kernel
Unknown
ELAM Driver
Boot Driver 1
Boot Driver 2
Boot Driver 3

Quick Heal
Security Simplified

Limitations

Quick Heal
Security Simplified

Callback Parameters

- Image Name
- Image Hash Algorithm
- Registry Path
- Certificate Thumbprint
- Image Hash

Quick Heal
Security Simplified

Checksum or Path Based Detections Only

9e 91 b2 e1 29 97 af e9 ac 6c 48 24 01 43 c8 b4
f6 81 bf 57 df 80 0b 05 4d 58 bb e6 d9 83 a9 08

Image Name

Registry Path

Image Hash

Quick Heal
Security Simplified

No Access to Driver Image and File System

- No File System
- No Polymorphic Detections
- No Binary Image
- No Heuristic Detections
- No Generic Detections

Quick Heal
Security Simplified

Multiple Image Hashes

Multiple Image Hash Algorithms

Algorithm known only during callback

Maintaining multiple hashes

Quick Heal
Security Simplified

Security Vs. Performance

0.5 milliseconds limit

Ok for checksum based detections

Other detection methods may not be used

Quick Heal
Security Simplified

Resource Vs. Performance

BLOB under new ELAM key

Driver + Signs < 128KB

May not load all signatures at once

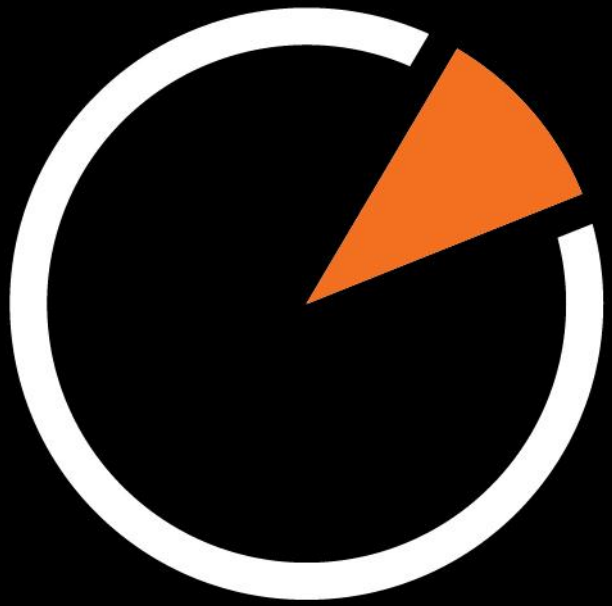
Quick Heal
Security Simplified

Handling Unknown is Tricky

Returning Bad: False +ve

Returning Unknown: False -ve

Quick Heal
Security Simplified



Usage

Quick Heal
Security Simplified

Very few ways of using ELAM

- Whitelist
- Blacklisting via User Mode Scanner
- Blacklist
- Combination of Whitelist & Blacklist

Quick Heal
Security Simplified

Exploring Blacklisting via User Mode Scanner

Capabilities: AntiRootkit, Heuristics, etc

Rest all drivers as Good

Malware driver blacklisted

Unknown driver chances minimized

Blacklisted driver as Bad

Quick Heal
Security Simplified

Enhancements

Quick Heal
Security Simplified

Callback parameter and registration

Parameter to IoRegisterBootDriverCallback

Driver Image Buffer

Single Image Hash Algorithm

Hash algorithm while Callback registration

Quick Heal
Security Simplified

Conclusion

Good Step

Too Little!

Future?

Quick Heal
Security Simplified

?

abhijit@quickheal.com
prakash@quickheal.com