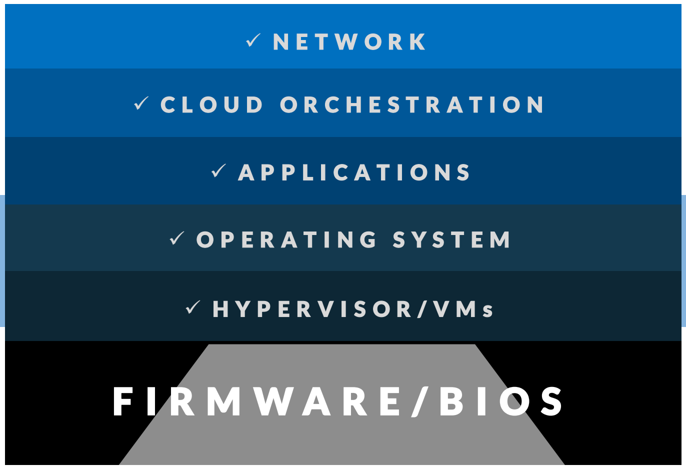
Control your firmware with TRAPEZOID® *FIVE* and CLOSE THE BASEMENT DOOR

Firmware is the forgotten layer at the bottom of the server stack.



Trapezoid® Firmware Integrity Verification Engine is specifically designed to provide visibility and management tools around the security and operations of firmware across the entire IT infrastructure.

Firmware is Unmonitored and Unprotected

- Existing security tools focus on application and operating system levels, overlooking the firmware.
- Firmware has the most permissions of any code on your system.
- Firmware's level of privilege increases the impact of an attack.

8% Only 8% of enterprises feel prepared for firmware related vulnerabilities and exploits

1 in 3 One in three are not monitoring, measuring or collecting firmware data.

52% More than 50% of enterprises placing a high priority on security within hardware lifecycle management have had at least one incident of malware-infected firmware

** 2016 ISACA Firmware Risks and Mitigation Study*

Compromised Firmware can Lie, Spy, Steal and Destroy

- Crippling malware creeps into routers, networks and systems via compromised BIOS and firmware.
- Compromised firmware can shut down your operations by taking out your critical infrastructure.
- Unmonitored firmware exposes enterprises to an *unacceptable level of risk* for devastating financial harm to businesses and life-threatening consequences for consumers.

> read more at trapezoid.com

Firmware is *EVERYWHERE...*

Firmware is a fundamental building block of any system.
Firmware is:

- Programmable software stored in non-volatile memory on device
- Persists from boot to boot
- Sits below the OS and driver layers
- Infrequently updated
- Usually physically part of the hardware (versus a hard drive)

TRAPEZOID®
Firmware Integrity Management

Call 1-786-621-8580 for a demo or visit us at **Trapezoid.com**

Request Risk Assessment

TRAPEZOID® *FIVE* IS THE ONLY COMPREHENSIVE SOLUTION

for detecting compromised firmware

Patented Trapezoid Marker

Potentially reduce the impact area of an incident by combining hardware specific data and user- defined policy attributes to remediate the incident knowing where the virtual machine has lived from the time it was created to the time it was destroyed.

PATENTED TRAPEZOID® *MARKER* MACHINE ID PROVIDES:

UNIQUE CRYPTOGRAPHIC TAGS *for hardware*

FORENSIC MAPPING OF *virtual machines*

WORKLOAD DEFINITION AND *data boundaries*

OEM PLATFORM WATERMARK FOR *supply chain verification*

PROTECT YOUR ORGANIZATION and MEET FEDERAL & COMMERCIAL COMPLIANCE

GOVERNMENT

NIST 800-53 & 53A:

No longer just for federal agencies, these baseline security controls now apply to business, industry, academia, local & federal gov'ts.

ENTERPRISE

NIST CSF & ISO/IEC 27001:

Avoid findings of negligence by failing to implement cyber security best practices.

HEALTHCARE

HIPAA & HITRUST CSF:

Required protection - reasonably anticipated threats & evolving threat assessments.

FINANCIAL

PCI-DSS & FFIEC:

NY DFS regulation requires a CISO, reporting time frames, C-level "awareness", and 3rd party compliance as well.

TELECOM

NSTAC:

Protection by computer -based policy, enforced by hardware based 'roots of trust'.

48%

Of attacks are malicious or criminal

* *2016 Ponemon Cost of Data Breach Study: Global Analysis*

$15,400,000

Average cost of a *single* cyber crime incident per company in the U.S.

* *2015 Ponemon Cost of Cyber Crime Study*

Can You Afford to be Next?

Let's face it: The bad guys are hacking into firmware in small environments to practice for bigger hits. Professionals like you can be on the hook for firmware security.

Find out your risks and vulnerabilities (and how to stem them) before it's too late.

GET THE FIRMWARE RISK ASSESSMENT

Call 1-786-621-8580 for a demo or visit us at **Trapezoid.com**

TRAPEZOID®
Firmware Integrity Management