



## Trust Your Tech from Core to Cloud with Panasonic Connect Smart Compliance

Firmware security is a key element of multiple important NIST documents, including SP 800-37 (Risk Management Framework), SP 800-53 (Security and Privacy Controls), SP 800-147 (BIOS Protection Guidelines), 800-155 (BIOS Integrity Measurement) and 800-193 (Platform Resiliency Guidelines). These documents identify firmware as a critical part of the security program and consistently use the terms "hardware, software, and firmware" when describing the components of technology that need to be protected. Panasonic Connect Smart Compliance aims to prepare you to address these NIST requirements as they pertain to firmware security and provide guidance for organizations seeking to achieve compliance with these standards.

**Smart Compliance equips organizations to continuously monitor and remediate critical components of their IT infrastructure during procurement, deployment, and operation.**

### UNDERSTANDING DEVICE RISK AND IMPACT OF THREATS



#### High Value Laptops

- With physical access to a device, an attacker can compromise the firmware in 5 minutes.
- Hacker forums post malware containing rootkits and bootkits.
- If your devices carry high value information or are traveling to untrusted environments, firmware security controls are mission-critical.



#### Critical Servers

- Servers provide an ideal path to both steal data or deny access to it altogether.
- Complex components like baseboard management controllers, network cards, and system firmware all make securing servers a challenge to manage.
- Smart compliance gives you peace of mind and simplicity as you navigate these critical components




#### Networking and Security


- Recent large-scale attacks have shown networking gear to be a primary target for attackers.
- Attackers can evade detection, maintain persistence, and move laterally within your environment by subverting the network infrastructure.
- The very network controls charged with securing your network could be the targets of attack.




## KEY BENEFITS: ENSURE YOUR HARDWARE IS TOUGH + COMPLIANT




**Protect Production Assets**  
 Improve mean-time-to-detection and the security posture for your enterprise IT.



**Reduce Digital Supply Chain Risk**  
 Make better IT procurement decisions and quickly assess the impact of supply chain threats.



**Lower Hardware Costs**  
 Extend the lifecycle of devices by validating trust in low-level components.



**Regulatory Compliance**  
 Easily implement security controls for device integrity and firmware security.

## HOW IT WORKS

Smart Compliance has access to the most comprehensive database of hardware, firmware, and software components, which includes 8 million+ elements from over 200,000 update packages, covering a vast range of vendors, device types, and models. We gather definitions by working with vendors, from analysis in operational environments, and from laboratory research.

With Smart Compliance, your teams can quickly and simply implement critical security controls to protect against below-the-surface threats: asset inventory, vulnerability management, and threat detection.

INVENTORY	HARDEN	DETECT & RESPOND
<b>Dynamic inventory of production assets.</b> Build an inventory of every piece of IT infrastructure, down to the hardware, firmware, and software level.	<b>Prioritize infrastructure vulnerabilities.</b> Gain insights into low-level vulnerabilities in hardware, firmware, and software components.	<b>Detect threats that evade EDR.</b> Alert on implants and other indicators of compromise for low-level components of your IT infrastructure.
<b>On-demand SBOMs.</b> Generate software bills of material on demand, including hardware and firmware components of devices.	<b>Simplify compliance.</b> Track issues at the hardware and firmware levels in frameworks such as NIST 800-53.	<b>Defend against tampering and counterfeit components.</b> Validate that assets have not been tampered with and have authentic components.
<b>Assess product risk.</b> Equip security and procurement teams to understand the risk inherent in those products before purchase.	<b>Automate firmware updates.</b> Schedule and automatically apply critical firmware patches.	<b>Correlate with other data.</b> Send alerts to SIEM and SOAR to give analysts improved context.

For more information on Smart Compliance, including subscription terms and pricing, please reach out to your authorized TOUGHBOOK Reseller.



TOUGHBOOK.com

