SSD Secure Boot: Securing NVMe SSDs from Power-On

Data Intelligence

Firmware-level attacks now bypass traditional defenses by striking before the OS and security software are active. NVMe SSDs with Secure Boot address this critical gap by validating firmware from power-on through a hardware Root of Trust and continuous Chain of Trust. Innodisk's 5TS-P and 5QS-P series SSDs implement this architecture to prevent tampering, mitigate supply chain risks, and ensure trusted operation. This protection is essential for data centers, financial institutions, medical facilities, and mission-critical environments.

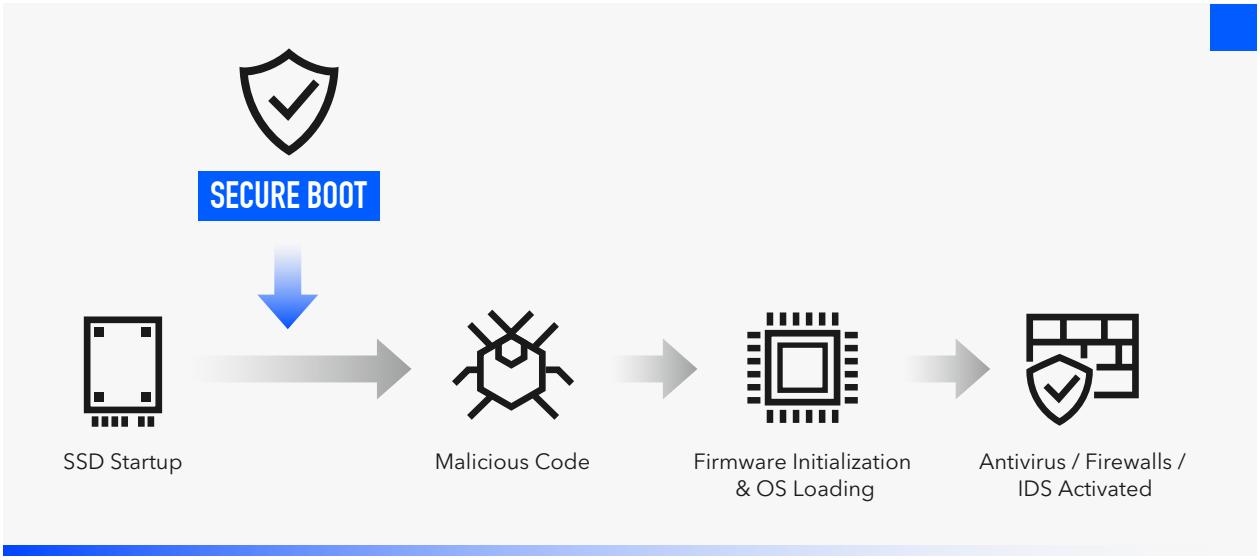
INTRODUCTION

Cyberattacks are becoming more sophisticated, increasingly exploiting the period before security mechanisms are fully initialized.

Antivirus software, firewalls, and intrusion detection systems remain vital, but they all share a critical limitation: they only activate after the operating system has loaded.

This creates a critical window of vulnerability during startup, when firmware and pre-OS components execute without protection.

The Secure Boot feature supported by Innodisk's 5TS-P and 5QS-P series SSDs addresses this challenge by shifting protection to the very beginning of the boot process—embedding trust mechanisms into the first instructions executed by the SSD to ensure devices are secure from the start.



CHALLENGES

The Hidden Weakness: Firmware and Supply Chain Risks

Firmware occupies a uniquely vulnerable position in the security stack. Operating in a pre-OS zone with elevated privileges and minimal oversight, it becomes an attractive entry point for attackers seeking persistent, hard-to-detect access.

This inherent exposure gives rise to what are collectively known as **supply chain risks**—threats introduced during **manufacturing, distribution, or firmware update processes** that compromise device integrity before deployment.

Attackers exploit these opportunities in several ways. Some attack vectors require physical access—for example, injecting malicious code through tampered test workstations or debug tools at **OEM/ODM sites**, or altering units **in transit** or **storage** to replace components or reflash firmware.

Remote threats also exist, such as distributing fake update files via **hijacked servers** or **mirror sites** that make malicious firmware appear legitimate.

In each case, the absence of an **immutable trust anchor** allows unverified code to enter the system unnoticed. Without a reliable method to verify that the firmware sequence is genuine, the entire security stack can be undermined before it even begins.

SOLUTIONS

Addressing these risks requires verification that begins at power-on, before any code executes. Secure Boot provides this foundational protection.

Secure Boot

During system startup, Secure Boot establishes the foundation of platform trust and protects against firmware-level threats by enforcing validation from the very first instruction.

At its core is a **Hardware Root of Trust (RoT) embedded in the SSD controller**, containing an immutable public key permanently fused into the silicon. This hardware-anchored key serves as the ultimate trust reference for verifying firmware authenticity.

For example, each firmware image is digitally signed using a private key securely maintained by the company.

During boot or firmware updates, the SSD controller uses the embedded public key to verify this digital signature before any code is executed.

This signature-based validation ensures that only firmware officially released and signed by the company can run on the device, effectively blocking tampered or unauthorized code from entering the boot process.

The system then verifies both authenticity and integrity of each subsequent firmware stage before allowing execution. Through this multi-layered and cross-referenced validation process, Secure Boot establishes an unbroken **Chain of Trust (CoT)** within the SSD, ensuring that only verified and uncompromised code is executed from power-on.

Secure Boot not only prevents attackers from infecting the boot process but also preserves the integrity of SSD firmware and stored data. At the same time, it reduces supply chain risks and helps organizations meet global security standards such as FIPS 140-3, NIST SP 800-193, and the OCP Datacenter NVMe SSD specification.

The Chain of Trust

Step1: Image Digest
The system uses a fixed cryptographic function to compute a hash (digest) of the existing firmware image stored in the device.
(This process only performs a mathematical "compression" – it does not execute any code from the image.)

Integrity verification

Step2: Signature Verify
The system uses the public key embedded in the image to "open" the digital signature and recover the hash value that was originally signed. It then compares this recovered hash with the digest calculated in Step 1.
If the two match, **the image is verified to be intact and unaltered** since it was signed.

Step3: Verify the Public Key Itself
The system computes a hash of the public key contained in the image, generating a Public Key Digest.
This digest is then compared with the immutable value stored in the device's OTP, eFuse, or ROM – known as the **Trust Anchor**. If they match, **the key is trusted**; otherwise, the image is rejected even if its signature is valid.

Authenticity verification

Step4: The verified image is executed
The system securely transfers control to the verified firmware.

Lifecycle Protection

Beyond initial startup, Secure Boot's protection **extends across the entire lifecycle** of the SSD, eliminating the risk of fake updates. When a new firmware package is received, the same verification chain is re-initiated to ensure the update image originates from a trusted source and has not been altered in transit. This **maintains security throughout the device lifecycle**, not just at initial startup.

New firmware received

Step5: Update Image Verification
Authenticity check/Integrity check
The system validates the new firmware using the same process.

Step6: Proceed to Firmware Update
After the new image is securely written, the **system restarts the Secure Boot process (Step1)** to verify and execute the newly installed firmware.

Re-enter Step 1

INDUSTRY APPLICATION

- **Data centers:** With thousands of SSDs operating simultaneously, firmware integrity is critical to overall reliability. Secure Boot ensures that every drive is verified as authentic and uncompromised – whether during deployment, maintenance, or controlled restarts. In large-scale environments where a single compromised drive could propagate malware across infrastructure, this hardware-level verification prevents attacks from gaining a foothold.

- **Finance:** Beyond encryption and access controls, Secure Boot safeguards the underlying firmware to prevent unauthorized modifications that could affect transaction integrity or expose sensitive data. For institutions handling millions of transactions daily, firmware tampering could enable undetected data exfiltration or transaction manipulation—risks that software-only security cannot address.

- **Healthcare:** In healthcare environments, electronic health records and medical imaging systems rely on trusted storage for data accuracy and confidentiality. Secure Boot verifies firmware integrity to prevent undetected corruption or manipulation of patient information. With regulatory requirements like HIPAA demanding comprehensive data protection, firmware-level security ensures compliance while protecting against attacks that could alter diagnostic results or patient histories.

- **Mission-Critical:** For critical infrastructure, systems often rely on multi-vendor supply chains, creating multiple exposure points and increasing the risk of firmware tampering or attacks. Secure Boot is an essential safeguard to ensure device integrity and trust. In systems where downtime or data corruption could have life-safety or national security implications, hardware-rooted trust provides the foundation for reliable, long-term operation.

CONCLUSION

Securing firmware integrity is no longer optional—it's foundational to device trust. As system threats move deeper into hardware and pre-OS layers, securing the SSD firmware is essential to preventing undetected compromise.

By verifying code authenticity from the very first instruction, Secure Boot transforms the SSD from a potential vulnerability into a trusted security anchor. Innodisk's 5TS-P and 5QS-P series NVMe SSDs exemplify this next-generation protection—combining hardware-level verification, lifecycle validation, and supply chain resilience.

With Secure Boot, organizations gain not only stronger device integrity but also a crucial step toward a zero-trust architecture—ensuring every system starts and stays secure.

WHY INNODISK?

At Innodisk, we believe that any challenge can be overcome through cooperation. By maintaining a strong line of communication all the way from inquiry to implementation, we ensure a tailor-made solution that fits your application. We remain committed to innovation with our continual focus on hardware, firmware, and software integration.

HEADQUARTER
INNODISK CORPORATION
5F., No. 237, Sec. 1, Datong Rd., Xizhi Dist., New Taipei City 221, Taiwan (R.O.C.)
T +886-2-7703-3000 **F** +886-2-7703-3555 **E** sales@innodisk.com