Titanium Technology Protection

Titanium for Linux

Star Lab's Titanium Technology Protection offers the most robust Technology Protection capabilities available on the market today for operationally-deployed Linux systems

Designed, developed, maintained, and tailored by a dedicated team of engineers with more than 40 years of combined Linux and Technology Protection experience; the Titanium threat model assumes that an attacker will gain administrative (root) access to the system, and **Titanium for Linux** must still maintain the integrity and confidentiality of critical applications, data, and configurations while assuring operations. Titanium Linux has been through pre-evaluation with participation from Navy, Army, and MDA Anti-Tamper Evaluation Teams and is compatible with RedHat and other binary-compatible Linux distributions.

> Titanium for Linux simplifies Mandatory Access Control (MAC) policy creation, file-based authentication and encryption, and runtime key management.

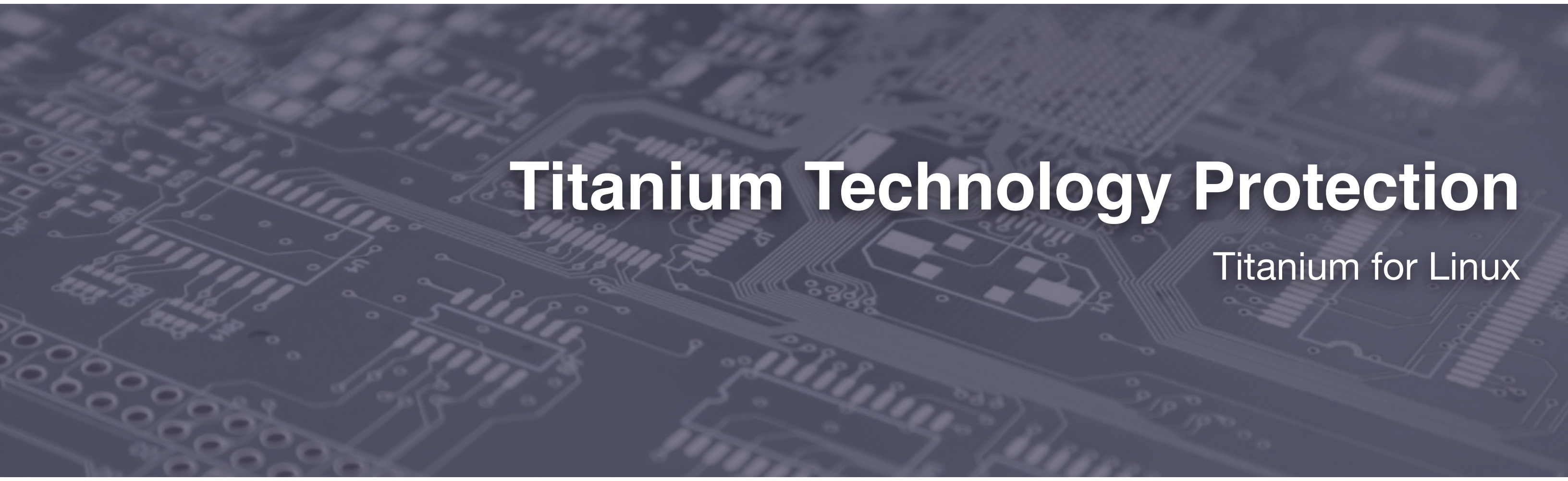
> Titanium for Linux removes or restricts access to unnecessary OS functionality which could aid in reverse engineering and exploit development for mission critical systems.

Simplifies Mandatory Access Control

1. Denies by default access to protected applications and data files even from root/administrator-level users, following the principle of least privilege.
2. Controls and restricts direct access to system hardware resources, such as peripherals and storage devices.
3. Enables secure software updates.

Enables OS Hardening & Attack Surface Reduction

1. Prevents unsigned module loading and enforces keychain controls.
2. Prevents attackers from reverse engineering, debugging or modifying the runtime of protected applications and their library dependencies.
3. Removes or restricts access to potentially harmful OS kernel interfaces and features.



Titanium Technology Protection

Titanium for Linux

Remains Secure During Runtime and Rest

1. Authenticates protected applications and data files, verifying that they have not been altered, and only decrypting files as needed (decryption keys are protected and stored out-of-band from attacker).
2. Ensures sensitive applications, data files and configurations are cryptographically bound to a particular deployment hardware, defeating any effort to copy and run applications on non-authentic or instrumented hardware.
3. Verifies file signatures on data and configuration files before they can be accessed by a protected application.

> Titanium for Linux provides robust protections for sensitive data, configuration files, and executables during runtime and rest.

Reduces Risk and Enables Deployment Success

1. Works with other Linux Security Modules such as SELinux to ensure STIG and IA controls can be applied without issue.
2. Exposes multiple APIs for common touch points (key release, event response, etc.) to expedite integration with a variety of complimentary hardware and software mitigations and enable customization.
3. Backed by a Product Services team that is ready and willing to provide tailoring support for unique requirements and environments.

> Titanium for Linux enables customers to rapidly and affordably address the majority of cybersecurity and Technology Protection requirements with a single product.

LEARN MORE

Contact us if you are interested in learning how Titanium Technology Protection can quickly and easily meet your security requirements and protect your system against the full spectrum of reverse engineering and cyber-attacks.

1325 Pennsylvania Ave. NW Suite #700, Washington, D.C. 20004
(202) 706-7027
http://starlab.io