Titanium Technology Protection

Titanium for Linux

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

Designed using a threat model that assumes an attacker will gain administrative (root) access to the system, **Titanium for Linux** maintains the integrity and confidentiality of critical applications, data, and configurations while assuring operations. Titanium Linux is compatible with RedHat and other binary-compatible distributions.

Titanium for Linux simplifies Mandatory Access Control (MAC) policy creation, requiring only policies for protected applications, libraries, scripts and data files.

Simplifies Mandatory Access Control

1. Denies by default access to protected entities even from root-level users.
2. Controls and restricts direct access to system hardware resources, such as peripherals and storage devices.
3. Enables secure software updates.

Titanium for Linux removes unnecessary OS functionality which could help an attacker analyze a system for ways to alter execution flow and bypass security.

Enables OS Hardening & Attack Surface Reduction

1. Prevents unsigned module loading and enforces keychain controls.
2. Limits an attacker's ability to debug or subvert protected applications and their libraries
3. Removes potentially harmful kernel functionality and features

Titanium Technology Protection

Titanium for Linux

Remains Secure During Runtime and Rest

1. Authenticates protected entities, 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 instrumental hardware.
3. Verifies file signatures on data and configuration files before they can be accessed by a protected application.

Titanium for Linux protects sensitive data, configuration files, and executables during runtime and rest.

Provides Comprehensive Certifications & Compliance

1. Works with other Linux Security Modules such as SELinux to address multiple levels of security requirements including confidentiality and integrity of specific applications, libraries, and data stores.
2. Enables application allowlisting to enforce static deployments — deployments that cannot be modified at runtime — of mission-critical embedded systems.
3. Reduces the impact of many zero-day exploits that would compromise root or administrative functionality of the OS, giving the developer time and space to develop patches vs. having to rush costly patches to market.

Titanium for Linux enables customers to rapidly and affordably address the majority of cybersecurity and technology protection requirements with a single product

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