SOLUTIONS_

FIRMWARE SECURITY & CJIS COMPLIANCE

Simplify CJIS compliance and secure your infrastructure supply chain

The latest CJIS Security Policy adds new firmware security requirements that could put significant burdens on government agencies and authorized third parties without the right solution. The Eclypsium supply chain security platform can simplify your organization's compliance with the new CJIS controls as well as fill a critical gap in your infrastructure security.

SUPPLY CHAIN SECURITY FOR INFRASTRUCTURE_

Some of the most devastating cyber attacks come through the supply chain. Eclypsium helps you to establish trust in the supply chain for your infrastructure—endpoints, servers, network appliances, and other devices that your organization relies on. Delivered as SaaS or through an on-premises deployment, the Eclypsium supply chain security platform makes it easy to inventory and verify every component of every asset on your network. For each device, you can monitor the integrity of software, firmware, and hardware components. You can detect tampering and compromises, and simplify the rollout of updates.

CJIS SECURITY POLICY_

The Criminal Justice Information Services (CJIS) is the largest division of the US Federal Bureau of Investigation (FBI) and a centralized source of criminal justice information (CJI) for state, local, and federal law enforcement and criminal justice agencies and authorized third parties. To ensure the protection of CJI, including fingerprint records, criminal histories, and other pertinent sensitive data, the FBI created the CJIS Security Policy document—a set of guidelines and regulations agencies utilizing CJI and the vendors that work with them must adhere to in order to meet the security requirements of handling protected information.

HOW ECLYPSIUM HELPS WITH CJIS CONTROLS		
SI-7, INTEGRITY VERIFICATION Detect unauthorized changes to firmware	**SI-4, SYSTEM MONITORING** Send firmware vulnerability and change alerts to SIEM or other SOC tools	**SI-2, FLAW REMEDIATION** Identify and fix firmware vulnerabilities

FIRMWARE SECURITY IS CRITICAL_

Firmware is the software embedded in hardware devices, including laptops, servers, routers, and storage devices, that controls how they operate. Attackers use tools that target firmware vulnerabilities, such as the Black Lotus bootkit, to install ransomware and steal sensitive data, such as criminal justice information.

FIRMWARE INTEGRITY_

CJIS Security Policy since version 5.9.2 now requires that organizations monitor the integrity of their firmware, checking integrity "at least weekly or in an automated fashion." Eclypsium automatically extracts firmware and analyzes it against known-good firmware to detect potentially compromised systems.

Eclypsium is also the solution for the cross-vendor platform integrity validation system by NIST in SP 1800-34, which demonstrates how organizations can verify that the internal components of computing devices are genuine and have not been tampered with.

VULNERABILITY SCANNING_

CJIS Security Policy also added control requirements for scanning for firmware vulnerabilities. Specifically, organizations are required to update firmware in as few as 15 days after an update. Eclypsium makes implementing this control easy, with ongoing scans for laptops, servers, and infrastructure devices and assistance in rolling out firmware updates.

Unlike traditional network vulnerability scanners, Eclypsium scans firmware categories that are often overlooked such as Intel ME/AMT and NIC firmware that often contain remote-exploitable vulnerabilities, performs firmware analysis to alert on changes, and even assists in rolling out firmware updates.

	Eclypsium	**Vulnerability Scanners**	**EDR**
Threat detection for firmware	Detects any type of malicious activity	None	Limited to analysis of known-bad binaries
Firmware integrity verification	Detects any change by extracting and analyzing binaries	None	None
Supply chain security	Verifies software, firmware, and hardware components	None	None

ABOUT ECLYPSIUM_

Eclypsium's cloud-based platform provides digital supply chain security for critical software, firmware and hardware in enterprise infrastructure. Eclypsium helps enterprises and government agencies mitigate risks to their infrastructure from complex technology supply chains. For more information, visit eclypsium.com.