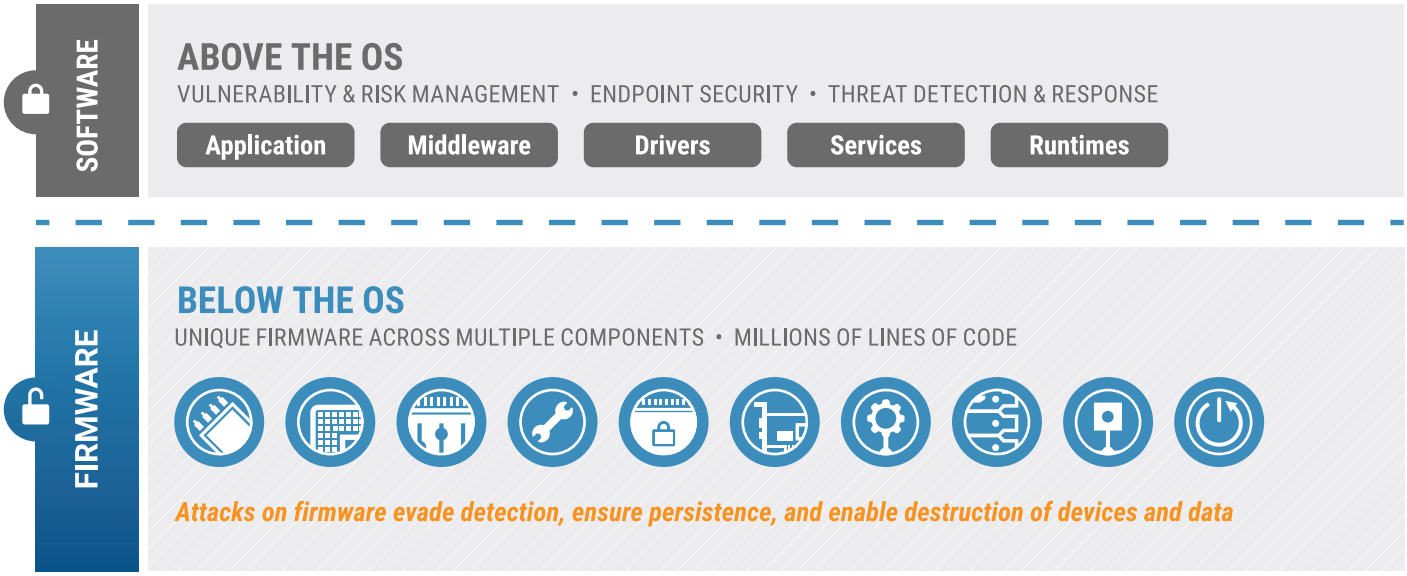
Extend Zero Trust Practices To Every Device In Federal Supply Chains



The Eclypsium® SaaS platform provides Zero Trust security at the lowest layer of the supply chain: where raw code meets bare metal, and where laptops, servers and network devices need to be protected from firmware- and hardware-level attacks. Eclypsium defends the supply chains of civilian agencies and defense teams from the deep implants, exploits and sub-OS attacks that have become the "vector of choice" for modern adversaries, but that remain invisible to the modern security tools these organizations rely on.

Protect The DNA Of Federal Supply Chains

The DNA of device supply chains – the embedded code, the core instructions, and the principles of who and what to trust – is in firmware. Firmware is highly privileged component-level software that's been developed by a wide variety of manufacturers, that runs independently from the operating system, and that's essential to the proper functioning of system hardware. Firmware makes technology supply chains work but has also become their biggest liability.

That's why the 2022 US government report on securing the nation's technology supply chains said:

> *Securing the firmware layer is often overlooked, but it is a single point of failure in devices and is one of the stealthiest methods in which an attacker can compromise devices at scale.*
>
> *Over the past few years, hackers have increasingly targeted firmware to launch devastating attacks.*

Firmware is the unguarded attack surface of all government networks, both civilian and defense. Today's servers, laptops and networking equipment arrive from their manufacturers with millions of lines of pre-programmed code. Research firm Gartner has estimated that "modern PCs have 15 to 20 pieces of firmware software loaded into memory on every startup.1" Every server may have 30 or more components. Every network device – whether security control, VPN, firewall or application delivery controller – now comes with embedded firmware.

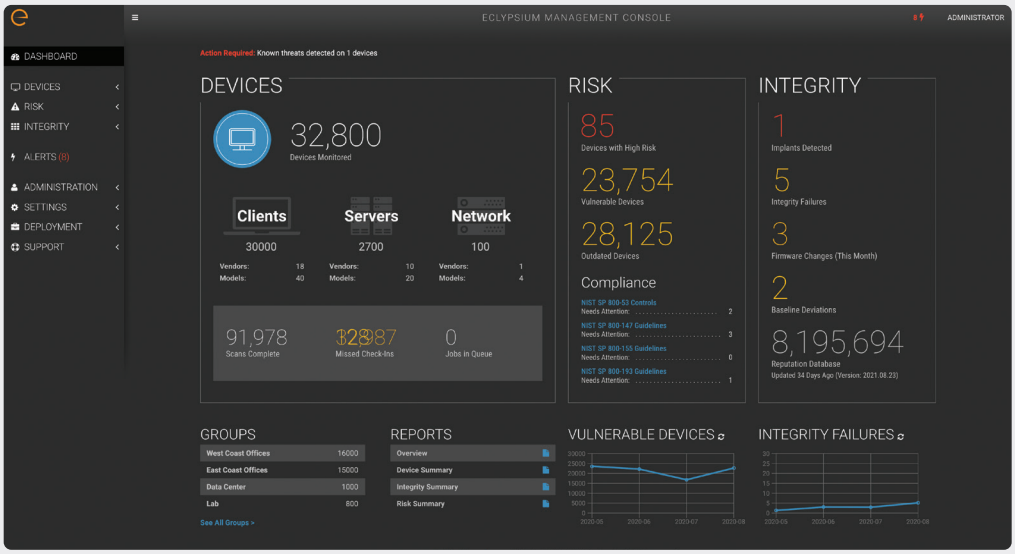
The path to protecting the government's device supply chains goes through firmware.

Unprotected Firmware is in Every Part of Your Supply Chain

Firmware in Endpoints: 15-20

Firmware in Servers: 30 or More

Firmware in Network & OT Devices: Every



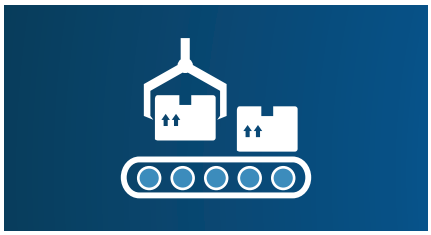
The Eclypsium platform provides hardware- and firmware-level security to every endpoint, server and network device in your digital supply chain, and compares them to over 7 million known-good firmware profiles.

However even the most advanced cybersecurity team has no visibility into this attack surface. They can't see what version of firmware is running in each component of an enterprise device, or determine whether it is vulnerable to known threats, much less detect a hidden implant or backdoor. Once compromised, this blind spot allows attackers to subvert traditional security controls and persist undetected, leaving you exposed to device failures, ransomware and data breaches.

That's why so many government cybersecurity teams have turned to Eclypsium. We provide an end-to-end solution that secures technology supply chains by securing its undefended DNA: mission-critical firmware.

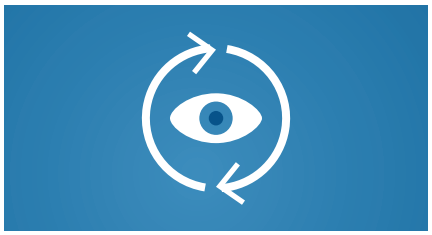
[1]Roadmap for Improving Endpoint Security ARCHIVED Refreshed 17 November 2020, Published 19 June 2018 - ID G00343353

Eclypsium Solutions



Secure your hardware supply chains

Ensure your Zero Trust strategies are in effect all the way down to the hardware level



Enable continuous monitoring and threat detection for invisible network layers

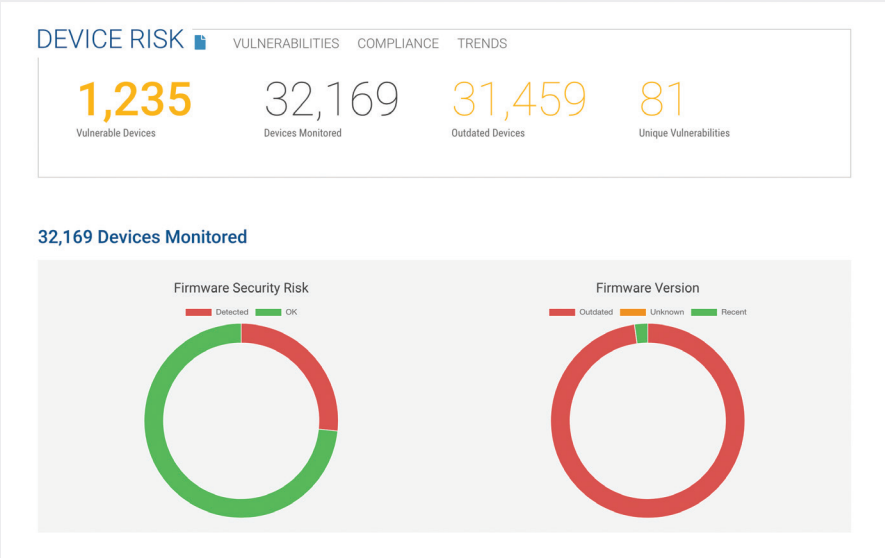
The Eclypsium Platform: Purpose-Built To Identify, Verify & Fortify Firmware

Modern cybersecurity teams leverage an alphabet soup of specialized tools to protect their supply chains, infrastructure and apps. They use everything from EDR/XDR solutions to VM and risk tools. They use CASB and NGFW and NDR, and they use every AppSec tool from DAST to SAST and IAST.

The common thread to all of these tools is this: *they were designed to work at the operating system layer and above*. They were never designed to work at the firmware and hardware layers. But this is, of course, where our modern adversaries are most focused.

Modern cybersecurity teams in government agencies and warfighter teams need an enterprise-class tool that helps them:

- **Identify** the firmware they have throughout their extended enterprise networks
- **Verify** this firmware's integrity, source version, and proper configuration
- **Fortify** firmware through automated updates, patching or configuration repair



Generate an instant assessment of the Zero Trust posture of every device in your supply chain, whether it's already in the field, sitting on your loading dock, or at the manufacturer ready for shipment to your network.

Eclypsium: World-Class Research, Recognition & Investors

Research

Eclypsium protects enterprise and agency supply chains by being the undisputed expert on the firmware – the digital DNA – underneath every supply chain. Our dedicated research team is often the first to discover new vulnerabilities, track active exploits in the wild, and provide actionable remediation guidance.

Recognition

Eclypsium has won numerous awards and accolades from industry peers and analysts, including:

Technology Company of the Year Rising Star 2022

Most Innovative Company 2020

Cool Vendor 2020

Upstart100 2019

Innovation Sandbox Finalist 2019

Investors

Gartner "Cool Vendors in Security Operations and Threat Intelligence," Brad LaPorte, et al, 5 May 2020