SUPPLY CHAIN INTELLIGENCE

Easily compare the risk of IT products and assess exposure to supply chain incidents

Whenever your organization selects a particular IT product, you are taking on some amount of risk. That's because each hardware, firmware, and software component in that device may have pre-existing (and yet to be discovered) vulnerabilities. In addition, each vendor and supply chain comes with its own risk profile, including geographic provenance and frequency of firmware updates.

> "Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships."
>
> *—Guidance in the new Cybersecurity Supply Chain Risk Management category in the NIST Cybersecurity Framework 2.0 draft*

The **Eclypsium Guide to Supply Chain Security** lets you make risk-informed decisions when purchasing new IT products such as laptops, desktops, servers, and network equipment. And when new supply chain incidents occur—such as a new vulnerability announced in a component—you can quickly assess your exposure by seeing the affected products you own.

MAKE RISK-INFORMED PROCUREMENT DECISIONS_

Today, vendor risk assessments rely primarily on external audits and questionnaires. And even when SBOMs are available, they don't tell the whole story. The Eclypsium Guide provides you with hard, technical data to measure the risk of IT infrastructure products.

- View and download SBOMs including hardware, firmware, and software components
- Compare risk scores based on vulnerabilities, geographic provenance, etc.
- See firmware update history for specific components and estimate supported lifespan based on update history

QUICKLY ASSESS EXPOSURE TO SUPPLY CHAIN INCIDENTS_

Eclypsium supply chain intelligence helps you to quickly assess your exposure to the following types of supply chain incidents:

- **Leaked source code or signing keys from a supplier** - Ransomware gangs have adopted a new tactic where they extort manufacturers by threatening to leak sensitive information that can compromise their product's security. For example, in June 2023, the Lockbit gang claimed to have stolen sensitive data from the chip manufacturer TMSC.
- **Discovered backdoors and vulnerabilities** - Due to the increasing complexity of microcode and firmware, researchers continue to discover more vulnerabilities in hardware and firmware components.
- **Geopolitical threats** - Some component vendors may be suspect due to the geographic location of their factories or influence from adversarial nations. In June 2023, WIRED reported that several secure hard drive vendors used an encryption chip from a manufacturer with ties to China's military.

HOW IT WORKS_

Eclypsium has the most comprehensive database of hardware, firmware, and software components. The Eclypsium database includes over 8 million elements from over 200,000 update packages, covering a vast range of vendors, device types, and models. We gather definitions by working with vendors, from analysis in operational environments, and from our own laboratory research.

Users of the Eclypsium Guide can search for a specific model of IT product and see all the hardware, firmware, and software components that comprise that product, along with a composite risk score that takes into account vendor and component risk. Users can also do a "where used" search to find all the IT products that use a particular component. Each component page shows a risk score based on geographic provenance and associated vulnerabilities.

> "By 2025, 60% of organizations will use cybersecurity risk as a significant determinant in conducting third-party transactions and business engagements."
>
> —Gartner, Top Trends in Strategic Supply Chain Technology 2023, March 2023

SUPPLY CHAIN INTELLIGENCE + SUPPLY CHAIN SECURITY_

The Eclypsium Guide is a standalone SaaS offering that is complementary to and integrated with the Eclypsium supply chain security platform.

	The Guide: Eclypsium Supply Chain Intelligence	**The Platform:** Eclypsium Supply Chain Security
What is it?	IT product guide with risk intelligence	Platform for IT infrastructure operational security
Primary use cases	• Deciding which IT product to purchase • Assessing exposure to new supply chain incidents for IT products	• Validating assets haven't been tampered with and contain authentic components • Assessing the security of assets in production (misconfigurations, etc) • Vulnerability management (with automatic updates) • Detecting threats • Responding to new supply chain security incidents

©2023 Eclypsium, Inc