adolus

FACT PLATFORM

Software Supply Chain Visibility for OT Asset Owners

Protect Your Operations, Protect Your People

The software supply chain is an increasingly attractive cyber target and it's no wonder: it provides access to thousands of victims via a single compromise. Attacks are rapidly increasing and high-profile incidents have prompted an industry awakening and swift regulatory action. Adversaries are targeting your trusted suppliers (and their suppliers) to breach your defenses and disrupt your operations.

- Do you have visibility into all 3rd-party and open source software embedded throughout your facilities?
- Are your purchasing decisions informed by your vendor's cybersecurity posture?
- Can you quickly identify at-risk assets when a high-profile vulnerability is announced?
- Are you able to comply with industry software supply chain regulations?

The FACT platform from aDolus provides continuous visibility across your entire asset inventory to help you **ensure software is legitimate, tamper-free, and safe** — *before* installing it in critical systems. It identifies high-risk vulnerabilities and components across products, product lines, and vendors. Thanks to our advanced ML capabilities, complex investigations can be automated, enabling staff to focus on high value tasks.

Transparency-Driven Rapid Response

Can you determine within minutes if a high-profile vulnerability like Log4j is present in any device, from any vendor, anywhere in your asset inventory?

Manage Software Supplier Risk

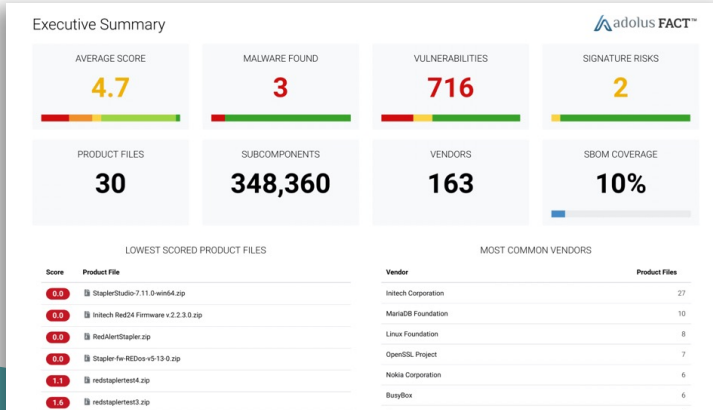
- Gain visibility into 3rd-party suppliers, all of their component vendors, and all open source software that may be hidden in your facilities
- Improve procurement processes and outcomes with cyber risk and maintenance analysis
- Identify risky or blacklisted suppliers and country of origin issues

Enhance Vulnerability and Asset Management

- Quickly identify vulnerable and exploitable components hidden across your software assets
- Use AI-driven scanning of multiple public databases and 3rd-party supplier sites to rapidly assess risk from emerging vulnerabilities hidden in your assets
- Use SBOMs and detailed analysis to focus vulnerability mitigation efforts where they matter

Prove Regulatory Compliance

- Generate 1-click SBOMs quickly and easily in CISA/NTIA-approved formats
- Provide software attestation of all components, even when your suppliers can't
- Provide reports to demonstrate supply chain regulatory compliance



OVAOGN-V01.00-09-2022-EN

FACT Solves These Difficult Challenges

Legacy Products Where Source Code is Unavailable

If you have legacy assets for which your suppliers have no source code, FACT can still produce SBOMs from your software binaries.

The OT Namespace Challenge

Associating products and SBOM data to vulnerability databases like NVD is difficult. Years of M&As, rebranding, and even simple typos mean multiple name variants exist for both products and vendors.

Hidden 3rd-Party Suppliers and Open Source Software

Deeply-nested subcomponents of unattested origin can introduce risk and increase the total cost of ownership of assets.

FACT Platform Features	Benefits
Continuous Supply Chain Visibility	
• Advanced aggregation, analytics, and correlation • Software validation and easy-to-use scoring • Malware detection via multiple AV engines and >18 thousand YARA rules • Certificate chain and signature validation • Up-to-date cybersecurity risk intelligence	• Gain detailed visibility into all the vendors, products, and components across all your assets • Gain confidence in your supply chain with independent validation • Reduce the risk of ransomware • Reduce time spent on malware false positives
SBOMs	
• 1-click NTIA-compliant SBOMs in approved formats • Enriched SBOMs offering drill-down-and-around to expose vulnerable components across all your assets • AI-driven searching of SBOMs to discover hidden high-risk components	• Focus efforts on exploitable vulnerabilities • Provide audit evidence for regulators • Gauge the quality of your vendors' security practices • Assess how frequently components are updated • Reduce costs through intelligent risk-based patching
Vulnerability Management	
• Continuous monitoring of public and supplier alerts • Natural language processing to extract data buried in text-based alerts • Probabilistic detection of hidden vulnerabilities	• Assess the risk from high-profile vulnerability announcements • Find vulnerabilities in *all* software in minutes, not days • Reduce costs through automated vulnerability research
Risk and Compliance Management	
• Executive reporting and KPIs • 3rd-party supplier discovery • Supplier quality assessments • Risk profiles by product line/supplier • Detection of high-risk software and components	• Make cyber-informed procurement decisions • Avoid high-risk or blacklisted suppliers or countries • Enforce policies regarding updates on critical systems • Protect your brand and reduce potential liability • Provide in-depth analysis for M&A teams
Scalability, Security, Performance	
• Full-featured RESTful API • Cloud (SaaS) platform with portal • Vendor-, platform-, and operating system-agnostic • 11 billion analysis operations/day • 1.4 billion mapped relationships between parent-child files	• Address IT, IoT, and OT products with a single solution • Integrate with corporate systems, workflows, and processes • Enable secure digital transformation • Be assured thanks to proven AWS security best practices