adolus

FACT PLATFORM

Software Supply Chain Visibility for OT Vendors

Protect Your Customers, Protect Yourself

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. It is no longer acceptable to distribute software without being certain it is trustworthy.

- Are your customers demanding visibility into the software and firmware you supply?
- Do you know all the 3rd-party and open source software embedded in your products?
- Has Executive Order 14028 forced you to produce and distribute SBOMs (Software Bill of Materials) to customers?
- Does your portfolio include legacy products that are opaque to you?

The FACT platform from aDolus provides continuous visibility across your entire software portfolio to help you **increase product quality** and **better support your customers**. FACT identifies high-risk or vulnerable components across products, product lines, and vendors and uses machine learning to automate complex investigations and reduce costly triage.

Safeguard Your Reputation

Can you respond in minutes when your customers ask if your products contain a high-profile vulnerable component like Log4j?

Automate Vulnerability Management

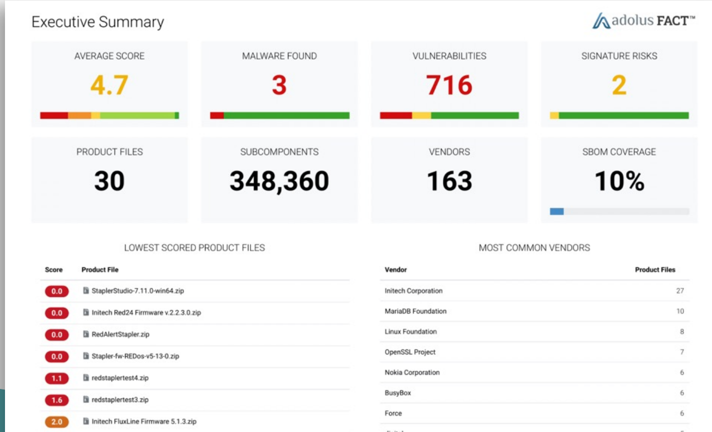
- Quickly identify vulnerable and exploitable components hidden across your entire product portfolio
- Use AI-driven scanning of multiple public databases and 3rd-party supplier sites to identify new vulnerabilities lurking in your products
- Generate VEX documents and proactively and efficiently communicate with customers regarding the exploitability of emerging vulnerabilities

Manage Software Supplier Risk

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

Prove Regulatory Compliance

- Generate 1-click SBOMs quickly and easily in CISA/NTIA-approved formats
- Provide software attestation of all components in your products to satisfy regulators
- Provide the reports your customers need to demonstrate supply chain compliance



Executive Summary

adolus FACT™

AVERAGE SCORE	MALWARE FOUND	VULNERABILITIES	SIGNATURE RISKS
4.7	3	716	2

PRODUCT FILES	SUBCOMPONENTS	VENDORS	SBOM COVERAGE
30	348,360	163	10%

LOWEST SCORED PRODUCT FILES

Score	Product File
0.0	StaplerStudio-7.11.0-win64.zip
0.0	Initech Red24 Firmware v.2.2.3.0.zip
0.0	RedAlertStapler.zip
0.0	Stapler-fw-REDos-v5-13-0.zip
1.1	redstaplertest4.zip
1.6	redstaplertest3.zip
2.0	Initech FluxLine Firmware 5.1.3.zip

MOST COMMON VENDORS

Vendor	Product Files
Initech Corporation	27
MariaDB Foundation	10
Linux Foundation	8
OpenSSL Project	7
Nokia Corporation	6
BusyBox	6
Force	6

FACT Solves These Challenges

Hidden 3rd-Party Suppliers and Open Source Software

Deeply-nested subcomponents of unattested origin can introduce risk, reduce product quality, and increase the total cost of ownership of your products, making you less competitive.

The OT Namespace Challenge

Associating product or 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.

Legacy Products Where Source Code is Unavailable

If you have software acquired through an M&A or legacy products where the source code has been lost, FACT can still produce SBOMs from your software binaries.

FACT Platform Features	Benefits
SBOMs	
• 1-click NTIA-compliant SBOMs in SWID and SPDX formats • Enriched SBOMs offering drill-down-and-around to expose vulnerable components across your portfolio • VEX (Vulnerability Exploitability eXchange) documents	• Build brand loyalty through transparency • Create and maintain a competitive advantage • Increase product quality • Provide audit evidence for regulations • Help customers focus on exploitable vulnerabilities
Continuous Supply Chain Visibility	
• Software validation and easy-to-use scoring • Malware detection via multiple AV sources and >18 thousand YARA rules • Certificate chain and signature validation • In-the-wild monitoring for unauthorized or fraudulent files • Release and update artifact tracking	• Gain detailed visibility into all the vendors, products, and components in your portfolio • Gain operational insights • Reduce time spent on malware false-positive reports • Manage software obsolescence • Reduce operational costs through automation
Vulnerability Management	
• AI-driven scanning of public resources • Natural language processing to overcome inconsistent naming • Vulnerability suggestions where suspected	• Get in front of high-profile vulnerability announcements • Find vulnerabilities in *all* products in minutes, not days • Reduce costs through automated vulnerability research
Risk and Compliance Management	
• 3rd-party supplier discovery • Supplier quality assessments • Risk profiles by product line/portfolio • Detection of high-risk software and components • Executive reporting and KPIs	• Protect your brand and reduce potential liability • Make informed procurement decisions • Avoid high-risk or blacklisted suppliers or countries • Drive governance and audit of SDLC policies • Be prepared for M&A due diligence
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	• Integrate with corporate systems, workflows, and processes • Be assured thanks to proven AWS security best practices • Address IT, IoT, and OT products with a single solution • Consolidate visibility for PSIRTs and product management

REQUEST A DEMO **www.adolus.com**

info@adolus.com ☎ +1-866-423-6587 www.linkedin.com/company/adolus @aDolus_Inc