WHITE PAPER

REVERSINGLABS

Third-Party Software: Derisking Mergers & Acquisitions

The Undiscovered Threat of Commercial Software

In today's world, software runs everything — including the company you may want to buy. As a result, when engaging in mergers and acquisitions (M&A), acquiring organizations are certain to inherit a new software stack, whether it is the intended outcome of the deal or not. In order to maintain effective risk management practices, organizations must evaluate whether any threats lie dormant in any proprietary software created or commercial software used by the deal target.

This is because software supply chain attacks have risen dramatically in the last few years. "Software supply chain attacks have seen triple-digit increases, but few organizations have taken steps to evaluate the risks of these complex attacks," according to the recent Gartner® report Mitigate Enterprise Software Supply Chain Security Risks. ReversingLabs' recent State of Software Supply Chain Security 2024 report also found a 1,300% increase in threats on open-source software repositories between 2020 and 2023.

Software supply chain attacks are sophisticated and stealthy, and can have a material impact on a company's business and valuation. The attacks on SolarWinds and 3CX bear out the impact on such attacks. And the recent XZ Utils attack, which took years to come to light, demonstrates the investment and perseverance hackers and nation states will endure. Further, the European Union Agency for Cybersecurity (ENISA) listed "supply chain compromise of software dependencies" as the top threat it expects to encounter by 2030.

These attacks directly impact business value. According to IBM's "Cost of a Data Breach Report 2023," the average cost of a software supply chain compromise is $4.63M USD, which is 8.3% higher than a breach due to another cause. Many of these costs are directly attributable to lost business (e.g., business disruption, lost customers, damaged reputation, and diminished goodwill). Ignoring these threats will leave organizations increasingly exposed as they explore potential M&A activities.

Cybersecurity incidents do have a material impact on M&A transactions and valuations. For example, in 2017, Version reduced its purchase price of Yahoo's by $350 million in the wake of two cyber attacks which occurred the year prior. Additionally, in 2020, Marriott International was fined $23.98 million by the UK's Information Commissioner's Office (ICO) for a breach on Starwood hotels reservation system, which similarly occurred a year prior to their merger.

Completing Due Diligence and Secure Integration

Although a number of risk-related insights are taken into account during an M&A transaction, it has become evident that software supply chain risk is gaining prominence. Due diligence includes ensuring the target company has been practicing due care in its software supply chain processes. This not only identifies potential risks, such as software licenses, intellectual property rights, license issues, and compliance with industry standards, but also any malware, tampering, exposed secrets, vulnerabilities, and more. Proper evaluation of the software during due diligence ultimately safeguards the investment, mitigates risks, and facilitates a smoother integration post-acquisition.

This process begins by conducting thorough due diligence, including software security assessments to understand risk prior to agreeing to the transaction terms. Although the results of this analysis will seldom kill a deal, any risks or threats uncovered will inform better decision making at the negotiating table, as well as throughout the remainder of the transaction life cycle. Below we explore the stages of an M&A life cycle, as well as the benefits that can be derived from software security assessments:

M&A Stage	Benefit Derived	How Software Assessments Help
Pre-Deal Due Diligence	**Identify material cyber incidents that are "deal breakers" and security exposures for more accurate deal pricing**	Comprehensive and material cyber incidents are rare, but not unheard of. Knowledge of them may postpone or even end discussions related to the acquisition. Beyond that, visibility into the health and quality of software packages critical to the business will help inform whether deal prices are appropriate or require adjustment for known security exposures.
Post-Deal Integration	**Informed integration planning**	Articulating the security risk presented by outdated, duplicative, or exposed software stacks will help inform the most appropriate and cost-effective path for technology integration in mergers.
Operational Delivery	**Insights into future operational requirements**	By cataloging the components (e.g comprehensive SBOM), dependencies, and license obligations of your software supply chain, you not only understand the legal/compliance safeguards required to operate, but also react to emerging risks and threats in a more agile manner.
Ongoing Value Protection	**Improved operational security, maximized profits**	Proactively identifying and addressing security exposures early will avoid downstream costs resulting from a breach and subsequent regulatory fines.

Traditional Tools Fall Short in Assessing Software

While software risk insights can provide negotiating leverage in deals, traditional methods of security assessments are not well suited for providing visibility into third-party software and software supply chain risks. As a result, the conclusions about cyber risk made by legacy security assessment tools often result in an inaccurate or incomplete representation of an organization's cyber risk.

Today, acquiring organizations are greatly limited in their options for evaluating the software security risk hidden within a target organization's network or within a software product they are acquiring. Further, the tools and techniques they do have at their disposal were not built to address the risks posed by modern software packages - including risks linked to open-source or commercial software supply chain dependencies. These tend to be dynamic and complex.

What are those tools and their limitations? Below is a list of testing methodologies and technology organizations currently rely on to identify both general security risk and software supply chain risk during M&A process today, and the gaps in the protections they yield:

General Security Risk Tools

Endpoint Detection
Organizations often rely on agent-based technologies like Endpoint Detection and Response (EDR) to detect risks and threats embedded within the target organization's environment. However, this tooling is viewed as invasive and often ineffective for systems which are unable to host agents.

Security Questionnaires
This traditional "pen and paper" approach to managing security risk is still the most widely used. However, questionnaires provide only a "snapshot" of an organization's cyber risk, and limited levels of assurance due to the reliance on both truthfulness and engagement from the inherent trust of third-party self-attestation statements.

Security Rating Services
These services often rely on passive scanning of a third-party's public facing infrastructure combined with public threat intelligence sources (e.g. web crawling services). Although these services provide valuable insights into the general security posture of the deal target, they overlook the security risk posed by the actual software estate (e.g. binary packages) that will be integrated into the acquiring organization's network.

Red Teaming
Penetration testing exercises provide evidence of a target organization's ability to detect and protect against malicious attack. However, they are often slow, costly, and disruptive to the operations of the target organization.

Traditional Software Supply Chain Risk Tools

Static Application Security Testing (SAST)
SAST technologies are designed to identify vulnerabilities and other underlying security flaws in software by analyzing its source code. Despite its effectiveness in detecting vulnerabilities early in the development process, the technology requires access to source code, which is often not made available to acquiring organizations until after a transaction has occurred.

Sandbox/Virtual Environments
Although sandboxes support the analysis of fully compiled commercial software (no source code access required), they are resource intensive, and can be easily evaded using malicious techniques such as time-based payload execution delay methods used within the SolarWinds software supply chain attack.

Software Composition Analysis (SCA)
SCA technologies are highly regarded due to their ability to accurately identify components and dependencies that make up a software package. However, SCA tools only support the identification of open-source software, overlooking the sea of licensed, commercial software libraries and other components that may also present risks to the security of an application.

Spectra Assure: Address Third-Party Software Risk

Recognizing that time delays directly impact deal success, organizations seek an automated and scalable way of performing due diligence on the software and services that underpin an acquisition target. That's where RL Spectra Assure™ for software supply chain security comes in. Using AI-driven complex binary analysis and proprietary threat intelligence, Spectra Assure provides the ability to audit software and automatically identify risks and threats that escape detection by traditional security assessment tools.

Spectra Assure provides a detailed analysis of all software artifacts in an efficient and cost-effective manner. Using Spectra Assure, organizations can analyze the complete software package including the proprietary, commercial, and open-source software, plus all additional artifacts without the need for source code, assistance of the target organization, or the need to engage in manual testing. Spectra Assure will provide a report with:

- Known malware that may be embedded in open-source or commercial software packages
- Tampered software artifacts bundled with the software
- Remotely exploitable and other high risk, "mandated fix" software vulnerabilities
- Sensitive information leaks (including credentials, access keys, IP, etc.)
- License compliance risks for open-source and third-party commercial components
- Version and update differentials
- Comprehensive software bill of materials (SBOM)
- Prioritized list of remediation actions that are needed to make the software safe

Spectra Assure's proprietary AI-driven complex binary analysis can process large, multi-gigabyte files in minutes, helping ensure the timely review of critical software assets and the due diligence process.

When used alongside other existing testing methodologies and security tooling, organizations can develop a more robust understanding of risk presented by a merger or acquisition, therefore informing a course of action to achieve maximum value and limit any delays in the sale process.

By leveraging Spectra Assure, organizations can more successfully gain visibility and control over the security risk presented by software throughout each stage of the deal life cycle, no matter what side of the transaction they are on.

Get Started!

To learn more about ReversingLabs Software Supply Chain Security capabilities and solutions

REQUEST A FREE TRIAL

www.reversinglabs.com

REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com