Key Benefits

Reduce risk of breach:
20% reduction in the risk of a breach

Improve secure coding practices and developer efficiency:
4 hours per developer saved per week

Align disparate teams together:
Unite developers, security, and compliance on the same team

Executive Summary

As consumers increasingly expect organizations to offer expanded value and experiences through software applications, businesses must ensure that they are providing not only a differentiated user-friendly experience but a secure one too. Customers entrust these organizations with their personal data and with the expectation that this information will be safeguarded from cyber security threats. Data breaches can have massive implications financially and in the court of public opinion. In 2017, more than 143 million US consumers were affected when a well-known credit reporting agency suffered a breach resulting from a known vulnerable open source component in one of its applications.[1] It is estimated that this company had to pay up to $40 per customer just to notify its clientele of the breach. Costs mounted quickly, rising to over $200 million in total costs, as the company had to invest time, resources, and money to investigate the breach, modernize its application development and security practices, handle employee turnover, and pay for legal and regulatory fees.[2] The company must also contend with damage to the brand's image, now frequently referenced as a cautionary tale about what can go wrong when open source governance is ineffective.

As organizations are pressured to improve secure application development, they are also tasked to deliver more business value at a faster rate to stay competitive. Speed is critical, and developers increasingly use open source components to meet delivery goals. Without automated governance tools and processes that can keep up with delivery speed and the growing use of open source components, security liabilities and license liabilities cannot be effectively managed. All too often, developers waste valuable time seeking security, architectural, and legal approvals in order to utilize new open source components. Further, in the aftermath of new open source vulnerabilities being publicly disclosed, developers and security professionals alike expend tremendous effort searching for and remediating at-risk components. Simultaneously, security and compliance teams lack visibility into what components are being used and where — hampering governance and risk reduction efforts. To drive efficiencies for developers and increase confidence in risk management, organizations are investing in solutions that can automate open source governance. Organizations seamlessly deliver component information to developers early in the development life cycle and provide valuable data to speed vulnerability detection and remediation efforts.

Sonatype commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential ROI enterprises may realize by deploying the Nexus platform. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of the Nexus platform on their organizations. To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed several customers with years of experience using the Nexus platform. The Nexus platform consists of Nexus Lifecycle, a policy engine to automate open source governance and provide component intelligence within existing development tools; Nexus Firewall, which blocks vulnerable open source components from entering into an organizations software development life cycle; and Nexus Repository, which stores, analyzes, and distributes open source components and builds artifacts as part of a DevOps pipeline.

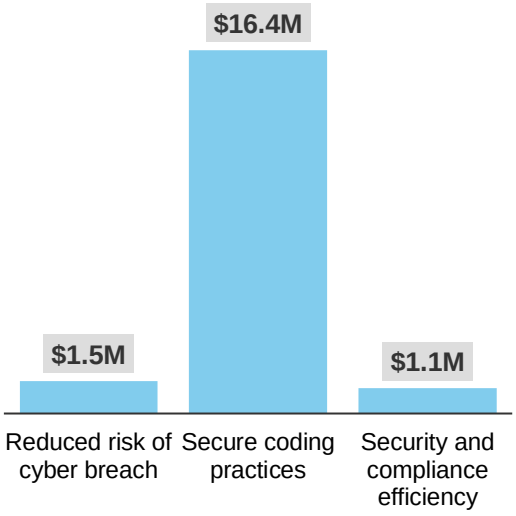
ROI
232%

Benefits PV
$19 million

NPV (total benefit less costs)
$13.3 million

Net benefit within 12 months

Benefits (Three-Year)



Key Findings

Quantified benefits. The following risk-adjusted present value (PV) benefits were experienced by the companies interviewed:

- **The Nexus platform reduces the overall probability of a successful breach by 20%, sparing organizations the costly fallout of a successful cyberattack, a benefit of over $1.7 million over three years.** If a successful cyberattack were to occur, organizations would experience a reduction in sales growth and market value, in addition to fines, legal fees, notification costs, and other detection and response costs. Interviewees report reducing their probability of a breach by 20%.
- **Developers save on average 4 hours per week with the Nexus platform**. Developers can use Sonatype to automatically identify and select quality components early, reduce rework, and reduce remediation efforts, saving on average 4 hours per week per developer, or almost $14,000 in saved time per developer per year.
- **Improved security and compliance efficiency enable two FTEs to be repurposed, on average.** Security staff save 173 hours per month on known vulnerability identification, risky license detection, and remediation efforts. Compliance staff save similar time on enforcing policies, license verification, and reporting.
- **Improving component oversight efficiency saves organizations an average of three FTEs.** Compared to manual processes, organizations can more efficiently manage open source components — saving 520 hours per month.

Unquantified benefits. The interviewed organizations experienced the following benefits, which are not quantified for this study:

- **Sonatype supports the move to continuous delivery, enabling organizations to deliver functionality faster and more securely.** Some interviewed organizations find that the efficiency delivered to developers by the Nexus platform contributes to improved release frequency. Interviewees note that the larger contribution by Sonatype is the ability to pursue continuous delivery while simultaneously improving and ensuring security.
- **Sonatype contributes to innovation by providing developers with more time and more data to make decisions.** Developers use time saved through efficiencies generated by Sonatype to focus on innovative work. Developers also use Sonatype data to reduce the average age of their libraries and to collaborate on how to improve applications.

Costs. The interviewed organizations experienced the following risk-adjusted PV costs:

- **Sonatype license costs are based on the number of developers.** Interviewed organizations pay a per developer cost based on the number of Nexus products used.
- **Internal staff spend time on the implementation and ongoing management of Sonatype.** Interviewed organizations found the implementation and administration of the Nexus platform to be relatively simple. Interviewees rolled out the Nexus platform to users in phases with an emphasis on minimizing disruption and driving adoption.

FORRESTER®

- **Nexus platform users spend minimal time on product training.** Security and compliance staff, developer leads, and developers spend minimal time on product training upfront and on an ongoing basis for new features.
- **Investing in change management drives adoption of Sonatype and the resulting benefits listed above.** Interviewed organizations provided support to Sonatype users to ensure a smooth transition and an understanding of how to incorporate data from the Nexus platform into user processes.

Forrester's interviews with four existing customers and subsequent financial analysis found that these interviewed organizations experienced average benefits of $19 million over three years versus costs of $5.7 million, adding up to a net present value (NPV) of $13.3 million and an ROI of 232%.

Partner with iTMethods for your managed Sonatype in the Cloud

Combine the secure, modern and connected software development and delivery capabilities with the scalability and automation of our Managed DevOps SaaS Platform to enable your DevOps transformation.

We deploy and maintain Sonatype to the highest standards on our Managed DevOps SaaS Platform. You'll stay current, optimized and your software teams will be able take full advantage of new Sonatype features as they are released.

As a Sonatype MSP Partner, we are experts in supporting Sonatype products as a Managed / SaaS service in the cloud.

SaaS Model

The benefits of a SaaS model means you receive a fully managed platform, that frees up resources and is delivered in a more secure, available and scalable manner.

Enterprise Features

Choose from a suite of Enterprise Platform services that align to your security, compliance and hybrid

Security & Trust

Our Managed DevOps SaaS Platform is SOC 2 Type 2 & AWS MSP Certified, which allows us to power mission-critical toolchains for some of the most regulated Fortune 500 companies.

Get in Touch

See for yourself how our Managed DevOps SaaS Platform will help transform your business.

Engage an Expert