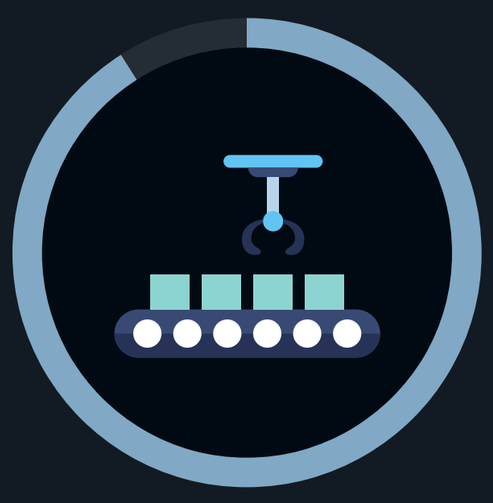
Enterprise Strategy Group™ by TechTarget

The Growing Complexity of Securing the Software Supply Chain

Many organizations are worried about having a high percentage of code that is open source within their software, expressing concerns about the specific possibility of being victims of hackers targeting popular/commonly used open source software. Organizations are challenged with increased vulnerability across the software supply chain and need effective security solutions that can support the demands of cloud-native development. TechTarget's Enterprise Strategy Group recently surveyed IT, cybersecurity, and application development professionals responsible for evaluating, purchasing, and utilizing developer-focused security products to gain insights into these trends.

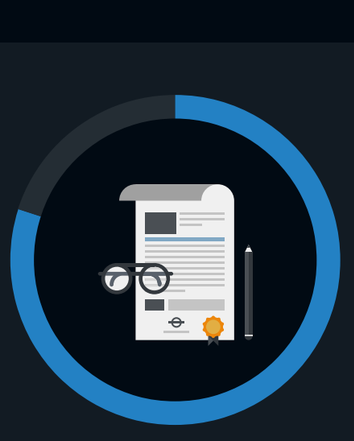
Notable findings from this study include:



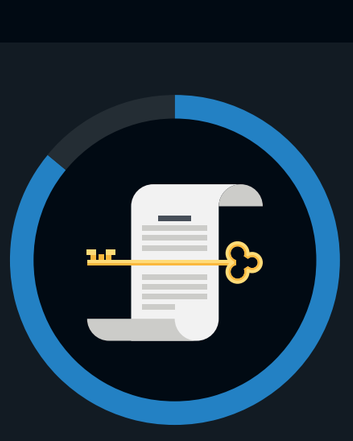
91%
of organizations reported **experiencing software supply chain security incidents in the last 12 months.**

96%
of organizations that experienced a software supply chain attack in the last 12 months suffered serious impacts, including the introduction of malware, data loss, and/or regulatory fines.

77%
of organizations significantly increased efforts to secure third-party software components following attacks.



80%
of organizations find software bill of materials industry regulations confusing and difficult to meet.



86%
of organizations agree that software bill of materials regulations are needed to ensure secure software applications and benefit their ability to serve customers.

74%
of organizations are making **significant investments in software supply chain security.**

For more from this Enterprise Strategy Group study, read the full research report, ***The Growing Complexity of Securing the Software Supply Chain.***

LEARN MORE

Source: Enterprise Strategy Group Research Report, *The Growing Complexity of Securing the Software Supply Chain,* May 2024.