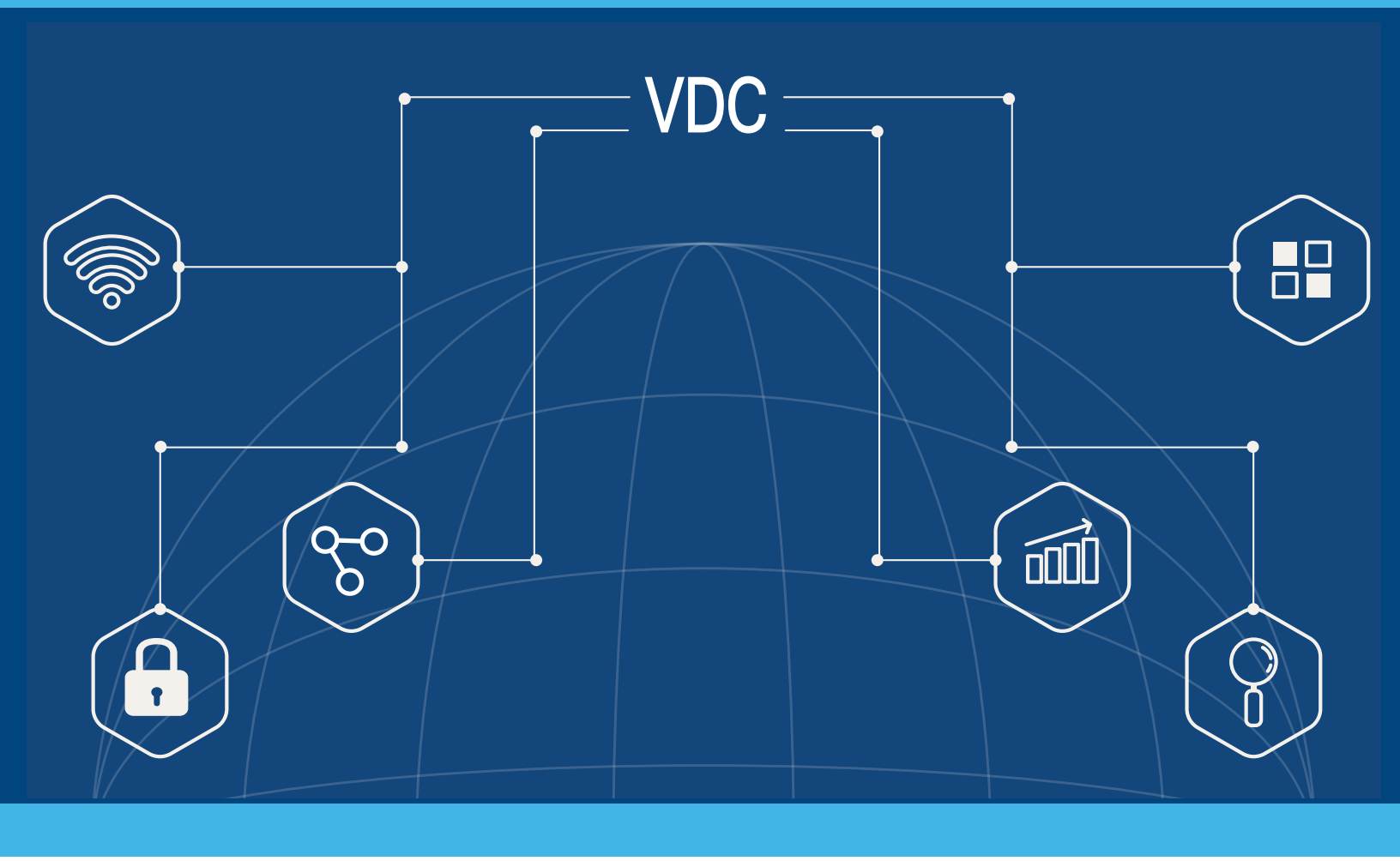
Finding Sources of Security in the Complex Software Supply Chains of Tomorrow



Exclusive License to Distribute:

GRAMMATECH

VDC Research

April 2021

Chris Rommel, Executive Vice President

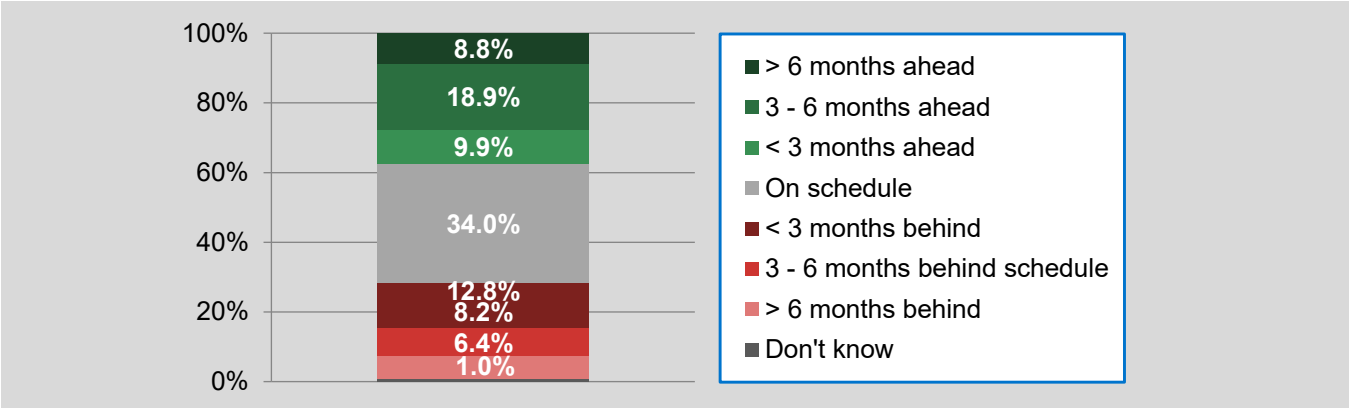
The State of Development

From the smallest embedded device to the most sophisticated high-frequency trading system, software continues to expand its role in corporate value delivery and differentiation. The growing pressures, complexity, and new requirements in today's software development are driving new methods for addressing organizational goals. Traditional software development processes and sourcing strategies no longer suffice. As a result, software development organizations are leaning into changes to improve speed and alignment across organizational silos by aligning with Agile and DevOps principles. The underlying development and process changes have translated to more investment in software content creation, increases in code base sizes, and a needed focus on software quality and security. But there are new variables emerging, making software development even more complex. The increase in content, however, has been paired with an increase in risk. With these evolving software bills of materials, security vulnerabilities and software quality issues amplify both impact and potential financial toll. However, common challenges remain from navigating new technical challenges, resource bottlenecks, and time-to-market pressures.

Falling Behind the Call for New Software Development Outcomes

By many metrics and for many organizations, software development is broken. Too many organizations face delays or ship software full of defects or vulnerabilities. One relatively simple and transferable metric to assess a software development organization's ability to navigate these challenges is to look at schedule performance.

Exhibit 1: Current Project's Schedule Adherence (Percentage of Respondents)



Unfortunately, nearly 30% of projects are behind schedule. While the reasons contributing to delay can vary, this issue, which leads to operational cost overruns and potential lost in-market revenue, is a persistent one plaguing many organizations. Unequivocally, software development organizations must continually search for new ways to be productive and innovative in the eyes of their customers. As development organizations focus on adapting to keep pace with next-generation requirements, they must also take commensurate actions to invest in and fortify their quality assurance functions. The challenge for many organizations is multifaceted. Not only must they find ways to improve their software and security, but they must also implement any changes without just adding new processes to their development cycle that could further impact schedule and time to market.

Background on VDC Research

VDC has been covering the product and software development technology market since 1994. The analysis and supporting discussions in this paper are based on VDC's ongoing research in this market and by findings from a survey of over 700 developers, product decision-makers, and engineers. This global survey offers insight into leading business and technical trends impacting development organizations as well as the best practices implemented to address them. The respondents are based across a range of industries, including automotive, aerospace and defense, financial services, healthcare, industrial automation, and transportation, among others.

Software Content Creation Evolving

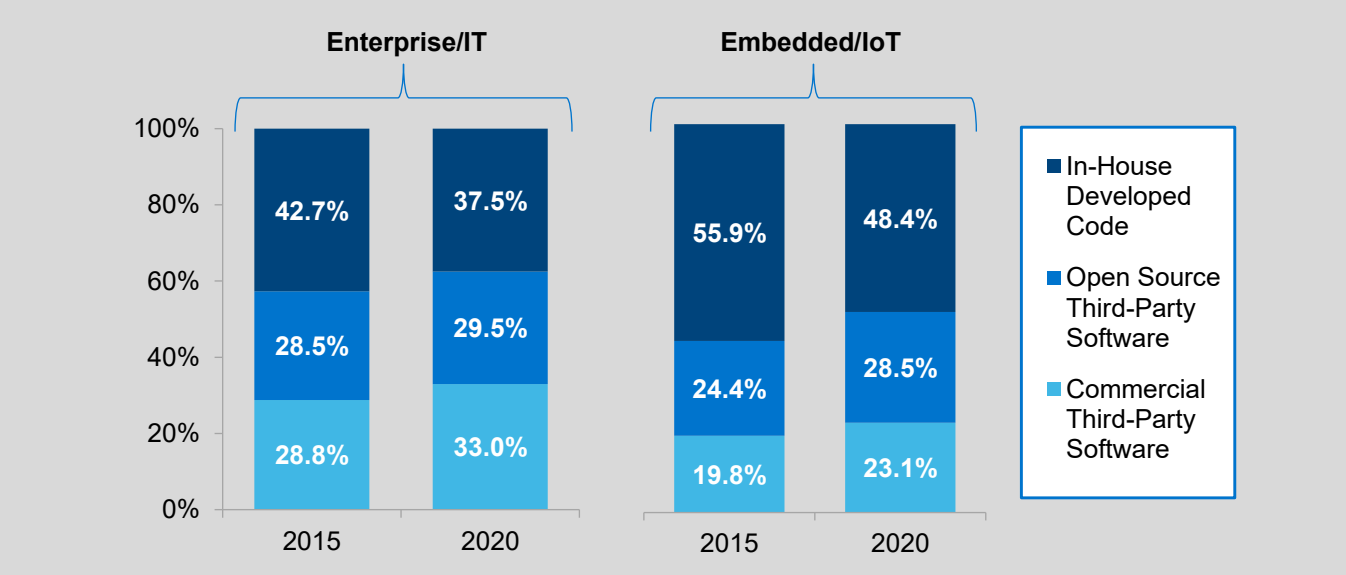
For years, the pace of needed innovation outstripped the rate of resource growth within development and QA organizations. This incessant code growth and bloat shows no sign of relenting, with the engineers we surveyed expecting lines of code to grow by 20% for their next project. Organizations cannot scale to keep pace with those requirements organically. While they can and should continue to find new methods and tools to improve efficiency, a higher and growing premium has been placed on the ability to leverage content from other sources. As part of this evolution, organizations must become more than just software developers, instead focusing on their roles as integrators of software-based systems from a range of sources. They can simply no longer afford to center their code creation strategy on hand coding.

OEMs are already turning to new sources and channels in growing frequency to accelerate development, from open source to commercial IP to code generation from modeling tools. In some cases, the answer to productivity challenges is as simple as increasing reuse of in-house assets. In others, that means redefining software content creation to increasingly rely on third-party assets as a foundation of their own software products. This outsourced content creation often draws from an assemblage of open source code sources, each bringing with it its own contribution lineage – and potential IP and security baggage. For example, commercial third-party code, the source growing the fastest in use within the IoT market, can itself be composed of various proprietary and open source components, thus creating layers and levels of obfuscation from original authors to current use.

While already a key strategy for software development, using commercial and open source third-party software is increasingly becoming a tactical necessity for many organizations to keep their teams lean, efficient, and innovative. However, this more complex and heterogeneous supply chain places even more strain on incumbent process and tools. With the same urgency as their evaluation of software design, organizations must rapidly reassess the means by which they identify issues within their amalgamations of software assets.

> Commercial 3rd party code use in IoT projects has grown 17%

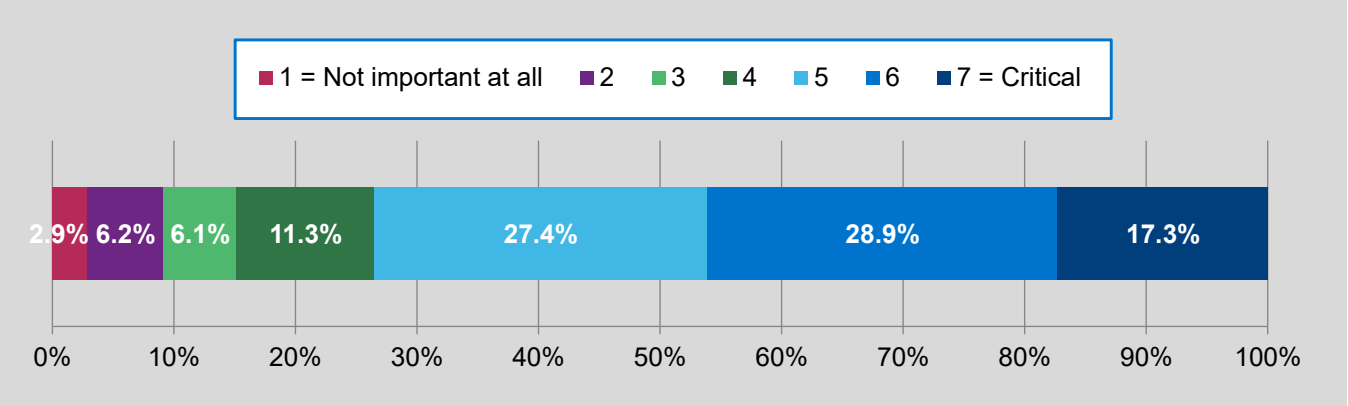
Exhibit 2: Percent of Total Software Code in Final Design, by Source (Average of Responses)



Security, a Fundamental SDLC Consideration

Regardless of the complexity of an organization's software supply chain, security has become a ubiquitous and paramount issue for all, based on the potential impacts to corporate risk, liability, and damage to brand reputation. The vast majority of organizations now view security as of significant importance to their current project.

Exhibit 3: Importance of Security to Current Project (Percent of Respondents)



This risk – and its recognition – is seen across sectors, but there is now a growing consideration among product engineering organizations that previously did not have as much exposure to security threats. The increasing portions of designs incorporating connectivity for IoT product goals has translated to more need for new approaches to software development and test. In fact, security now ranks as the second most often cited development challenge facing IoT projects. This growing realization of risk, however, has not yet translated at scale to widespread, commensurate transformation. Only 56% of organizations have formal policies and procedures for testing the security of IoT devices. When this newly added connectivity is combined with a growing roster of software assets from third parties, organizations are pairing new attack vectors with functional blind spots of unknown vulnerabilities. To minimize risk, they must not only have formal policies addressing security – a seemingly implicit requirement for development today – but they also must ensure that they adapt processes to address security across the entire development and deployment cycle.

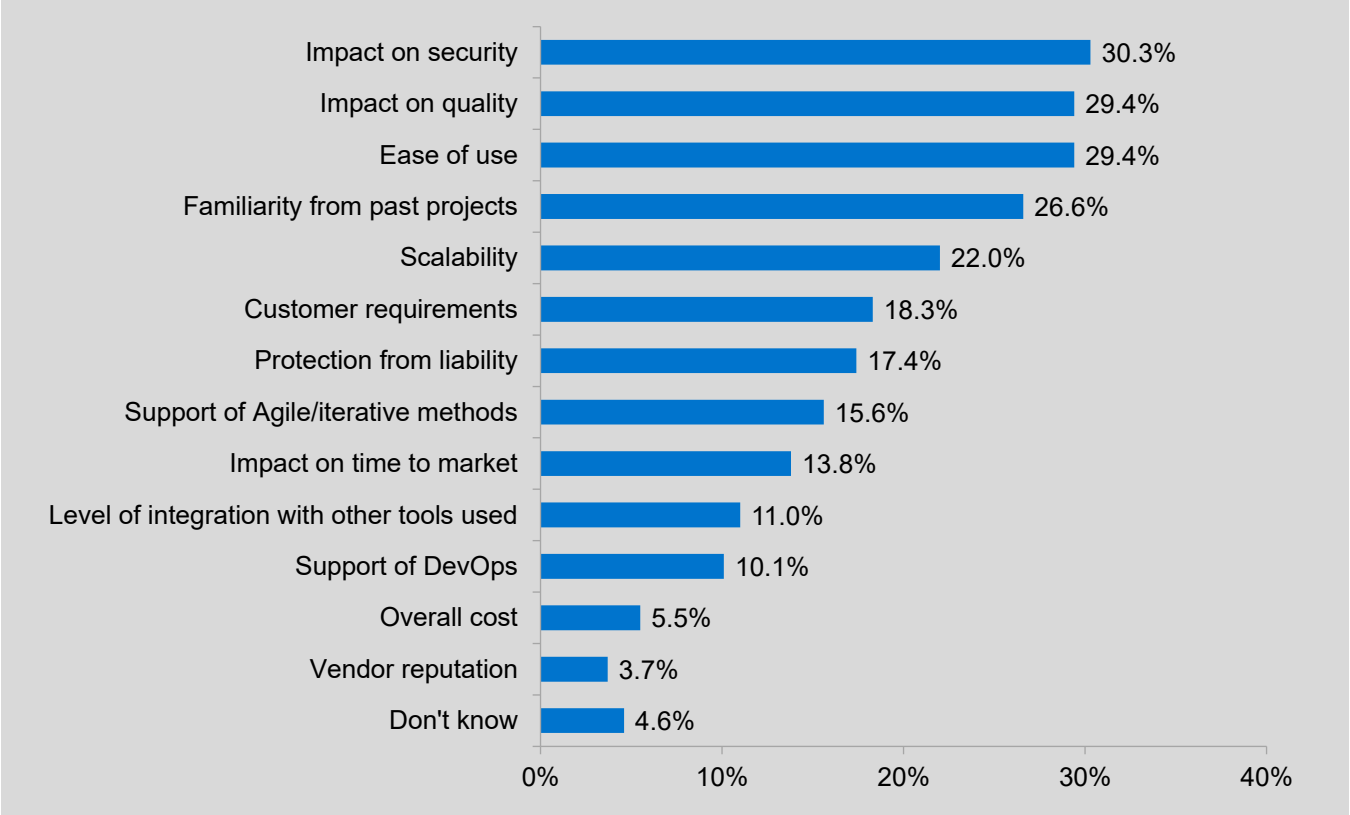
Only 56% of OEMs have formal polices for testing security

The Growing Role of Software Composition Analysis

Today, only 14% of developers and engineers reported the use of software composition analysis (SCA) solutions. While perhaps comparatively low to other types of solutions used for QA and test, its usage is primed for growth given expanding use cases and recognition of utility. Originally, these solutions gained adoption for their ability to manage software IP compliance to limit risk associated with licensing violations – a use case still widely seen and valuable during M&A vetting due diligence. However, the underlying technology and supplier ecosystem has adapted quickly in recent years, given the technology's utility in monitoring for known security vulnerabilities. In fact, the leading selection criterion for SCA tools is now cited as "impact on security." While the use cases of these tools have evolved somewhat dramatically over the past few years, this result should come as no surprise, given the tool's ability to identify issues that would otherwise pass through the vetting process and enter distribution.

Impact on security is the most important factor when choosing an SCA tool

Exhibit 4: Most Important Factors in Selection of Software Composition Analysis (SCA)/IP Compliance Tools Being Used in Current Project (Percent of Respondents)



Security Warrants More Software Visibility

In addition to the aforementioned inherent changes in the security threat landscape, the evolution of code sourcing adds new challenges and risk to the development process. As organizations leverage more software from a diversifying cadre of third parties, they can also lose visibility and access into source code – a dynamic especially acute for commercial third-party software assets. Furthermore, this opaqueness is compounded by third parties' own potential use of outside software and libraries – including open source. The lack of source code access can, in turn, then limit the utility of traditional software analysis tools. Unfortunately, that means that organizations could be unintentionally exposing themselves to known vulnerabilities.

To address this risk gap, development organizations should investigate solutions that can evaluate their software's binary to help provide needed insight into unknown code. This approach can also add value for legacy in-house software that can be exposed for new risks upon reuse. Today, most organizations are not taking this relatively simple step to assess their software's integrity. Approximately three-quarters of engineers reported that their organizations have not conducted any binary analysis previously, let alone integrated it into standard process for all project development.

SCA Emerging Software Development Best Practice

Not only has SCA emerged as a critical tool in reducing IP and security vulnerability risk, but our research has also shown its value promoting efficient software development. Already, many organizations have embraced agile development and driven testing further left in the traditional software development cycle. Now, more complex software bills of materials are driving expansion of this approach to include SCA. As more organizations adapt and modernize their software supply chain, SCA use will follow. Already, a clear pattern of higher use of SCA tools has emerged in line with those software projects that have more diverse code bases (i.e., less in-house and less hand-coded). In the future, equally important will be the type of SCA solution used and its utility assessing risk in those more opaque parts of the software supply chain.

> The use of more 3rd party software requires new analysis tools to mitigate risk

Exhibit 5: Percent of Total Software Code in Final Design of Current Project Coming from Various Origins (Average of Responses)

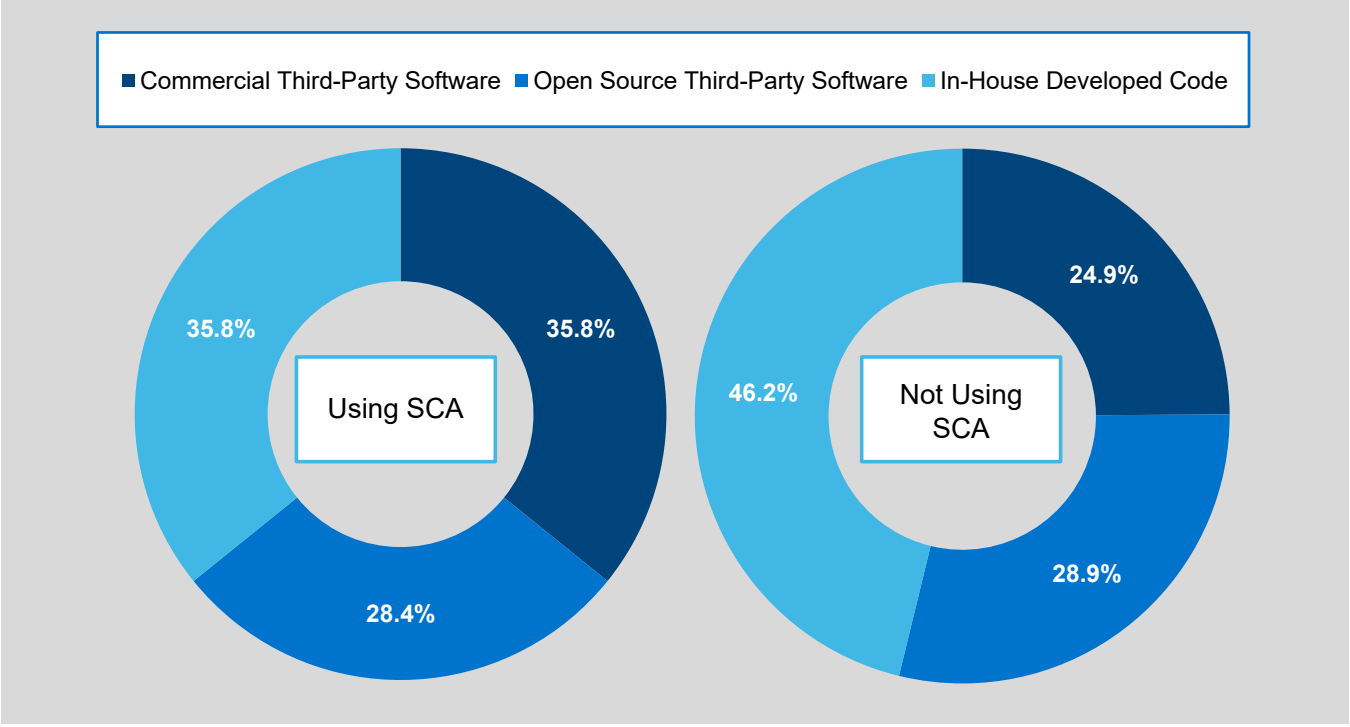
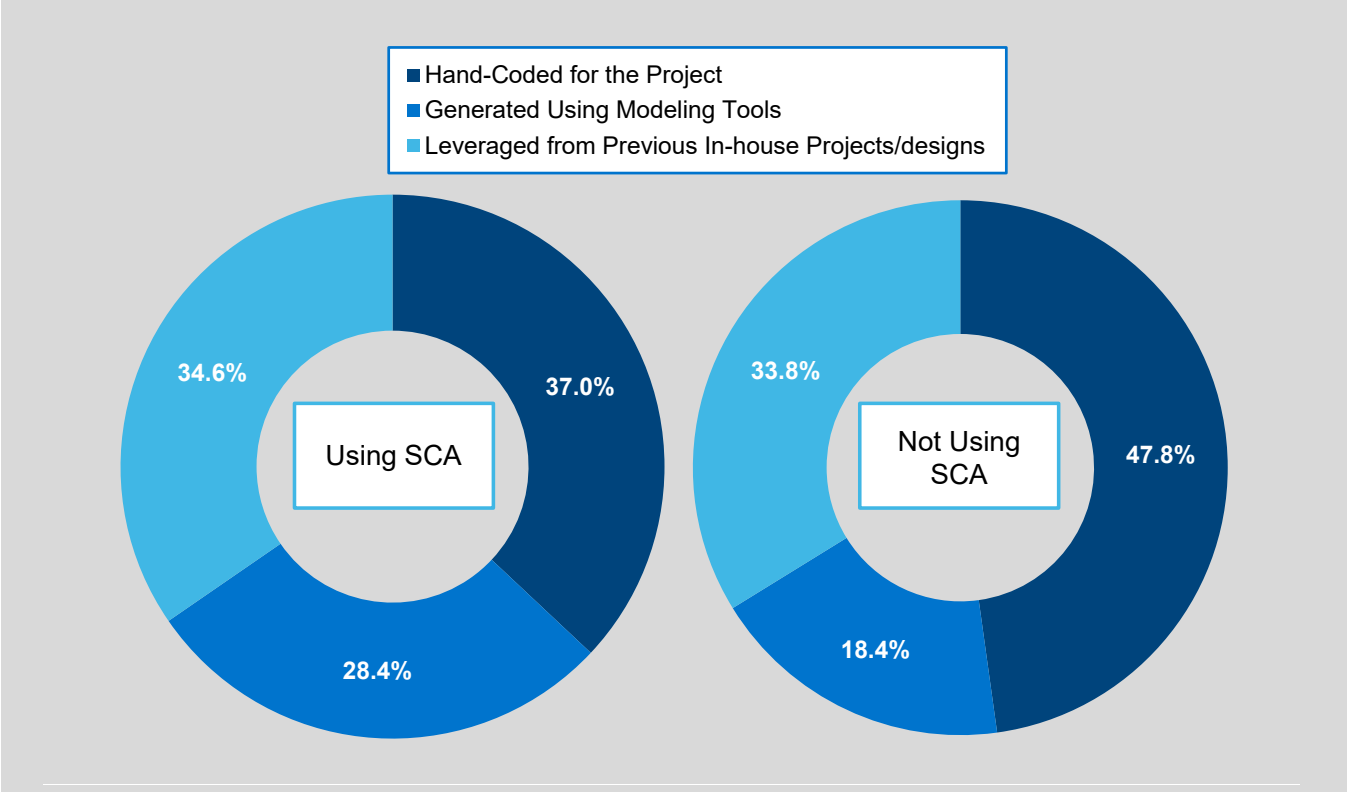


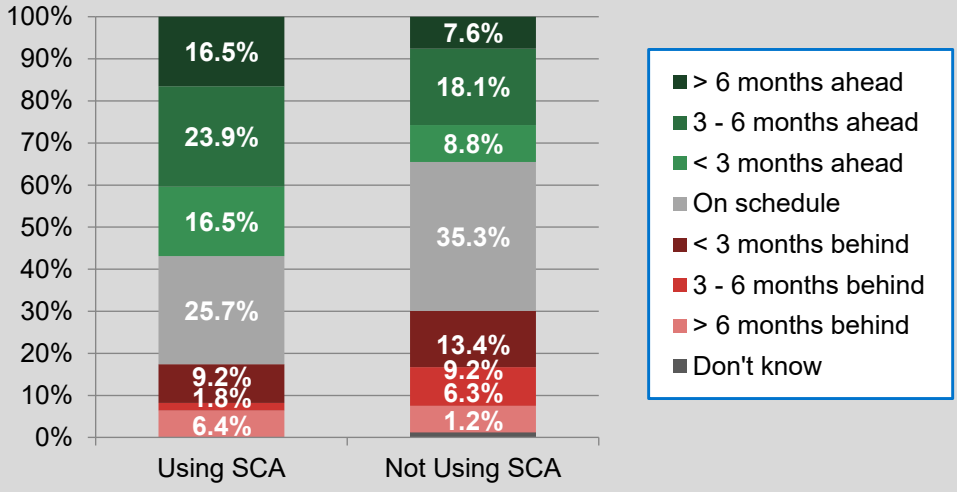
Exhibit 6: Estimated Percent of In-House Developed Software Code for Current Project, by Origin (Average of Responses)



Beyond the utility managing software risk, our research has shown tangible productivity benefits emerging from SCA use. In fact, our research demonstrates that respondents using SCA were much more likely to finish their development project ahead of schedule than those not using SCA tools (57% vs. 34%). In essence, despite more complex software supply chains, SCA tools users can save time and money through the earlier identification of software issues.

SCA users are 65% more likely to finish their project ahead of schedule

Exhibit 7: Current Project's Schedule (Percent of Respondents)



Conclusion

Software development requirements and risks are evolving rapidly. More complex and distributed supply chains are becoming the norm, with more organizations leaning on third-party IP assets to accelerate their internal software development. The benefits of third-party software, however, can come with added risk and less visibility into core organizational content. New technology choices are needed to address these core changes to software content creation to both ensure quality and minimize risk.

SCA use, however, is only part of best practice to develop quality, secure software. Not only is it critical to identify valuable partners to assist in their implementation and provide access to updated vulnerability repositories, but new approaches such as binary analysis are emerging as key capabilities that organizations should investigate to complement traditional SCA practices. These solutions can provide a key mechanism to assess risk, regardless of IP origin – or access to source. Furthermore, SCA solutions should be used with other technologies to best assess a software bill of materials in its entirety. Integrations with other design and development solutions are more important than ever. In particular, SCA tools have a particular synergy with static analysis tools, given the latter's ability to assess software for programming errors in advance of runtime. In fact, static analysis tools users are already recognizing this alignment and are three times as likely to use SCA solutions. Ultimately, it is clear that in much the same way that development organizations must embrace third-party code sources as a means to keep pace with development demands, they must also look for new ways to pair change code composition with changes to their core software quality and security assurance practices and tool sets.

About The Author

Chris Rommel

Chris Rommel leads VDC's syndicated research programs and consulting engagements focused on development and deployment solutions for intelligent systems. He has helped a wide variety of clients respond to and capitalize on the leading trends impacting next-generation industrial and device markets, such as security, the IoT, and engineering lifecycle management solutions. Chris has also led a range of proprietary consulting projects, including competitive analyses, strategic marketing initiative support, ecosystem development strategies, and vertical market opportunity assessments. Chris holds a B.A. in Business Economics and a B.A. in Public and Private Sector Organization from Brown University.

Email Chris at **crommel@vdcresearch.com**.

About VDC Research

Founded in 1971, VDC Research provides in-depth insights to technology vendors, end users, and investors across the globe. As a market research and consulting firm, VDC's coverage of AutoID, enterprise mobility, industrial automation, and IoT and embedded technologies is among the most advanced in the industry, helping our clients make critical decisions with confidence. Offering syndicated reports and custom consultation, our methodologies consistently provide accurate forecasts and unmatched thought leadership for deeply technical markets. Located in Natick, Massachusetts, VDC prides itself on its close personal relationships with clients, delivering an attention to detail and a unique perspective that is second to none.