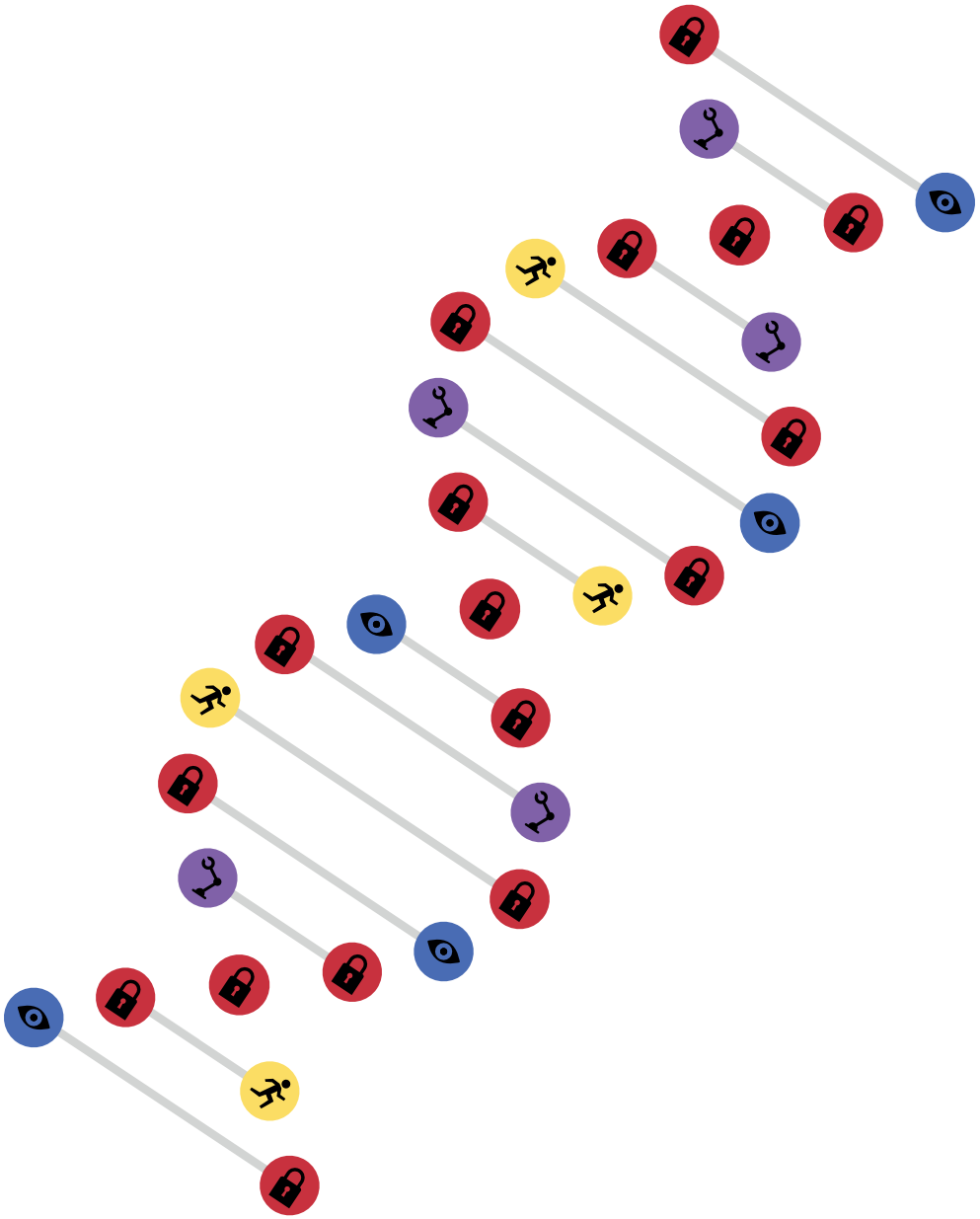
FREEFORM DYNAMICS

In association with

ca technologies

Integrating Security Into the DNA of Your Software Lifecycle



"Masters" move beyond pure risk management to focus on business growth

Freeform Dynamics, January 2018

Introduction

Software is now critical to nearly all organizations, but producing great applications and services that meet business needs requires modern development and delivery processes. Fundamental to this challenge is building trust, managing risk and exceeding the expectations of your customers for security and privacy in their experiences with your business, online, via apps and in your data center.

The 24 x 7 digital economy and ever-increasing customer demands are requiring many organizations' to release apps and app updates on a near-continuous basis. When security is left to the end of the app development cycle, it is all too easy to trade it off in the pressure to get an app out the door.

It is now imperative to weave security into every step of the development process, from design, through coding, to release and operation. In many respects, security must become part of the very DNA of software development and operations teams, a concept some are now referring to as 'DevSecOps'.

But acting on this imperative isn't without its challenges. It puts pressure on people, processes and tools, none more so than testing, especially as the need for rapid and iterative delivery becomes the norm rather than an exception.

While not a simple task, an analysis of the results of a global survey of IT and business executives on how organizations are modernizing their software delivery practices highlights a group which have mastered the key principles. This group is already doing nearly all, or at least most, of the right things to make security an implicit part of the way they work.

These 'Software Security Masters' are more likely than their mainstream peers to see effective security as an enabler of increased business performance. This manifests itself in the form of superior metrics and outcomes in relation to software delivery. It's probably also no coincidence that their organizations are seeing 40 percent higher revenue growth and 50 percent higher profit growth than their mainstream contemporaries.

In the remainder of this paper we lay out a compelling, evidence-based case for embedding security throughout your software delivery lifecycle, weaving it into your development and operational processes.

This paper is part of a series that explores the concept of the 'Modern Software Factory', a term coined by CA Technologies, the sponsor of the research, which provides a blueprint for building agility, automation, insights and security into the whole of the software lifecycle. The topic of the Modern Software Factory is explored in a paper titled "Don't Let an Outdated Software Strategy Hold You Back".

Lifecycle security in the spotlight

Customer demand for faster delivery of new apps has lead to the adoption of approaches such as agile, DevOps and continuous delivery to improve software development and deployment. Software development is evolving into a more robust and repeatable set of processes, able to meet rapidly changing business and customer requirements.

Which of the following measures/initiatives is your organization taking to address current software development and delivery changes?

Adoption of
Agile Methods

80% Committed
25% Already done
55% Doing now

Adoption of
Full DevOps

68% Committed
25% Already done
43% Doing now

Adoption of
Continuous Delivery

77% Committed
32% Already done
45% Doing now

But the central importance of software to business success makes the security of software, applications and data an issue for an expanding number of stakeholders within the business, especially when you add in the escalating concerns around legal and regulatory compliance.

How much impact do the following roles have on software and data security?

Those with an interest in **Transformation**

Chief Digital Officer
44% Big impact
41% Some impact

Program Managers
37% Big impact
47% Some impact

Those with an interest in **Outcomes**

Business Stakeholders
26% Big impact
48% Some impact

Application End users
32% Big impact
45% Some impact

Those with an interest in **Risk**

Legal and Compliance
33% Big impact
49% Some impact

Chief Security Officer
42% Big impact
44% Some impact

How much do you agree or disagree

Major external influence

We have to stay aligned with Government security requirements and guidance

79% Agree or strongly agree

The fact that external threats are growing rapidly makes it clear that those responsible for the rapid, safe delivery of software need to change the way application security has been managed. Business relies on web and mobile applications to generate revenue. Security, or its lack, therefore has the potential to impact both customer perceptions and profits.

How much would you agree or disagree

The threat in relation to Web Applications is growing rapidly

62% Agree or strongly agree

The threat in relation to Mobile Applications is growing rapidly

65% Agree or strongly agree

Security threats due to software/code issues is a growing concern

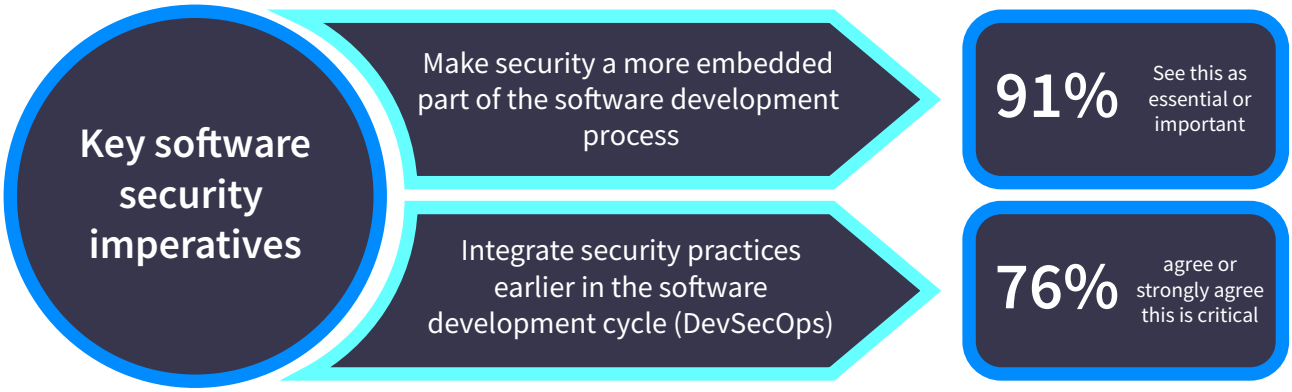
74% Agree or strongly agree

In a global study sponsored by CA Technologies, Freeform Dynamics surveyed 1279 senior IT and business professionals in medium to large organizations across 15 countries, eight industries and five continents. The results highlight the challenges of implementing software development security well, and the benefits doing so can deliver.

Fast-emerging security imperatives

The research illustrates, very clearly, that a majority of organizations recognize that rapidly changing business and regulatory demands are driving a need to modify how security is managed in their software development processes. In particular, it reveals that the traditional approach of testing security at the end of the development process, if at all, is no longer sufficient. Instead a clear majority recognize that security now needs to be embedded throughout the development lifecycle, not tagged on, often hurriedly, at the end.

Tactics for dealing with security more effectively

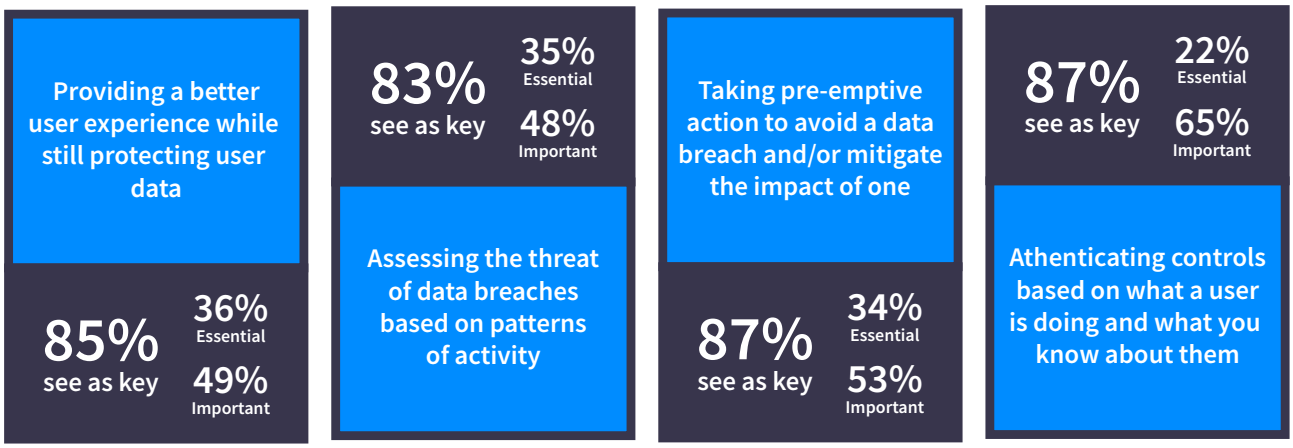


Indeed many now see value in integrating, as far as possible, not only software development, deployment and ongoing management (a combination frequently referred to as DevOps) but also making Security an integral component throughout the lifecycle. Together these are becoming known as DevSecOps.

But the immense challenges associated with these processes makes the use of automation tools essential as few, if any, organizations have the skilled human resources or time available to tackle such complex, urgent challenges. So what do organizations think they have to do to ensure they can protect the software they create and the data they generate and collect?

As threats increase and pressure to protect apps and data grow more intense, the survey shows that two new technologies, namely behavioral analytics and machine learning, are expected to help improve security. Today security testing of vulnerabilities always lags behind known threats, increasing the requirement for continuous testing throughout the entire software lifecycle. Machine learning (ML) and behavioral analytics may enable more prescriptive lifecycle vulnerability testing. But beyond this, ML could also soon make it possible for apps to be able to make decisions on sensitive data access in real time, essentially helping improve the security of the app as it is being used.

How important for your company is the use of behavioral analytics and machine learning to improve security in the following areas?



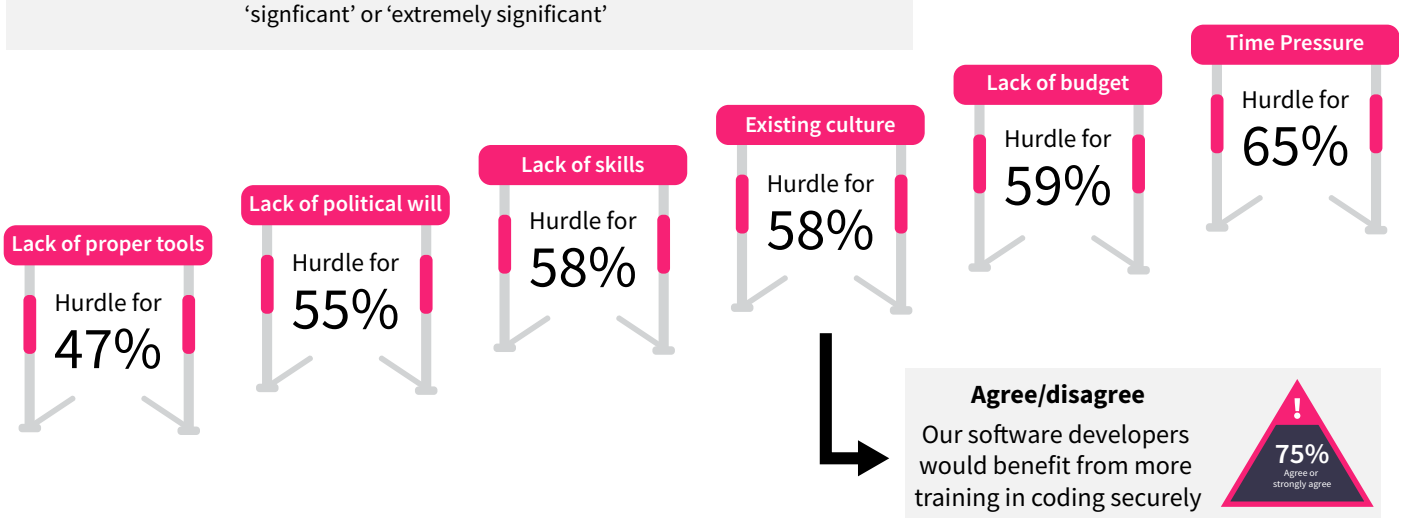
Additional capabilities being developed include using ML as a way to assist throughout the lifecycle of applications, from initial design, through code development and productization all the way to app deployment and its operational usage. This will offer the chance for all parts of the DevOps teams to have more active visibility and control of application usage, in near real time, thereby enhancing the organization's approach to risk management of apps and applications at all stages of their life.

Overcoming the hurdles with a new mindset

So what holds organizations back from making security integral to the entire software development process, from application requirements assessment, through design to delivery? The answers, unsurprisingly, mirror those common across many projects in IT and across business as a whole. Lack of time and budget are common responses, as are the lack of necessary skills and tools. But softer 'people' challenges such as the culture of the organization, and a lack of political will to change things, also show up strongly.

How significant are the following hurdles to embedding end-to-end security in your software development processes?

Percentages indicate number of respondents who replied 'signficant' or 'extremely significant'



The challenges are well illustrated by other results from the research as only 32% of respondents believe IT is very effective at making security more embedded in software development and only 24% strongly agree the organization's culture and practices support collaboration across ops, dev and security teams. But most worrying is that only around a quarter strongly agree that senior management understands the importance of not sacrificing security for time-to-market. Such cultural issues and political will can be difficult to address unless effort is taken to show the benefits of new ways of working to everyone impacted.

No one denies that security is important to protect data and, perhaps potentially even more importantly, to safeguard the reputation of the organization as one its customers and partners are happy to do business with. But the research illustrates that over three quarters of respondents see security as an enabler of new business. And, as results we will discuss later in this report show, the perception of effective security as a means to generate new business may well already be showing up in organizations' financial reports. Making a compelling business case for investment is becoming more straightforward as a new perspective on software and data security is emerging.

Security is an enabler of new business opportunities in addition to helping protect our company's data and systems

(Agree/strongly agree)

Our CSO and Security team are perceived by business units to be leaders not innovation blockers

(Agree/strongly agree)

The research also identifies another shift in how those responsible for security are viewed by their business colleagues. Over three quarters of respondents agree that the security team and the CSO (Chief Security Officer) are now seen as leaders, rather than as the blockers of innovation that they were often assumed to be in the past. We must acknowledge that some CSOs and others responsible for security are included in the sample, but even taking this into account, it is clear that the view of security is becoming more positive.

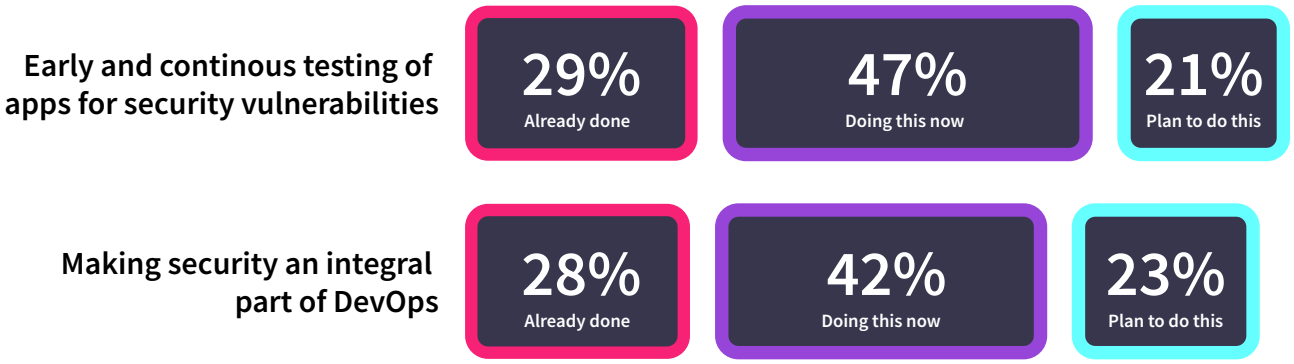
The Master Perspective "We work with security early on, so that we make sure that we're not architecting in security flaws." *CTO, Digital Audio Vendor*

Lifecycle security readiness assessment

But even if the view of security is more positive, what steps are being taken to improve security in application development? In order to assess where organizations are currently in their ability to fully integrate security into their app development processes, we looked at 6 key questions, or indicators. Each respondent was scored based on their answers to these 6 criteria.

While less than a third of organizations are focused on initiatives to implement security across their DevOps processes, or are looking to incorporate early and continuous testing for vulnerabilities, the good news is that a majority have started down these roads or have plans to do so.

Are you implementing measures or initiatives to address the following?

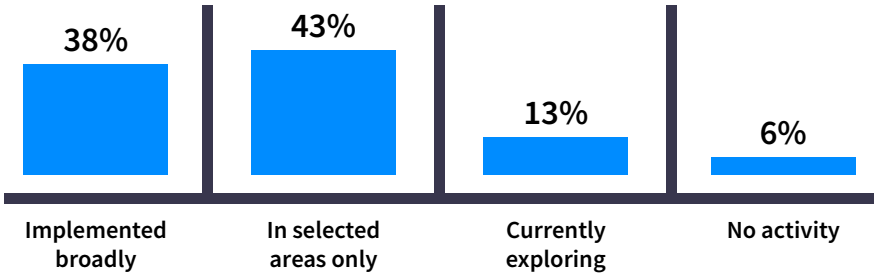


Security Testing

The same can be said for how broadly vulnerability testing has been embedded in the end-to-end software delivery process.

The steps taken are positive, but often require significant changes to how software teams function, and are also heavily dependent on having automated, orchestrated tools to support security testing.

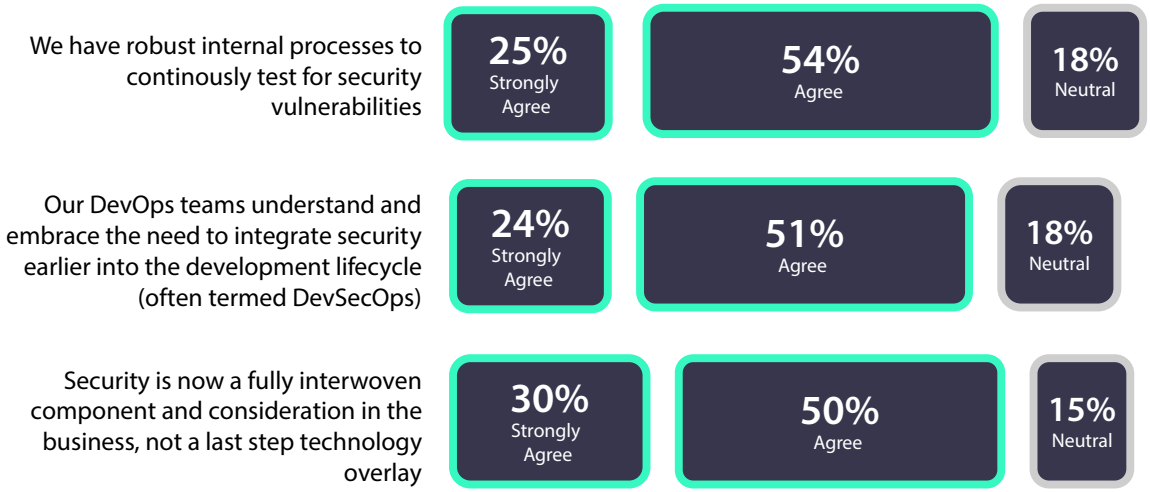
How much is security vulnerability testing embedded into your end-to-end software delivery processes?



The level of awareness is healthy, but conversely the fact that only just over a third of those surveyed have so far broadly implemented vulnerability testing in their software delivery processes reveals that there is plenty of scope to improve this facet of software development security.

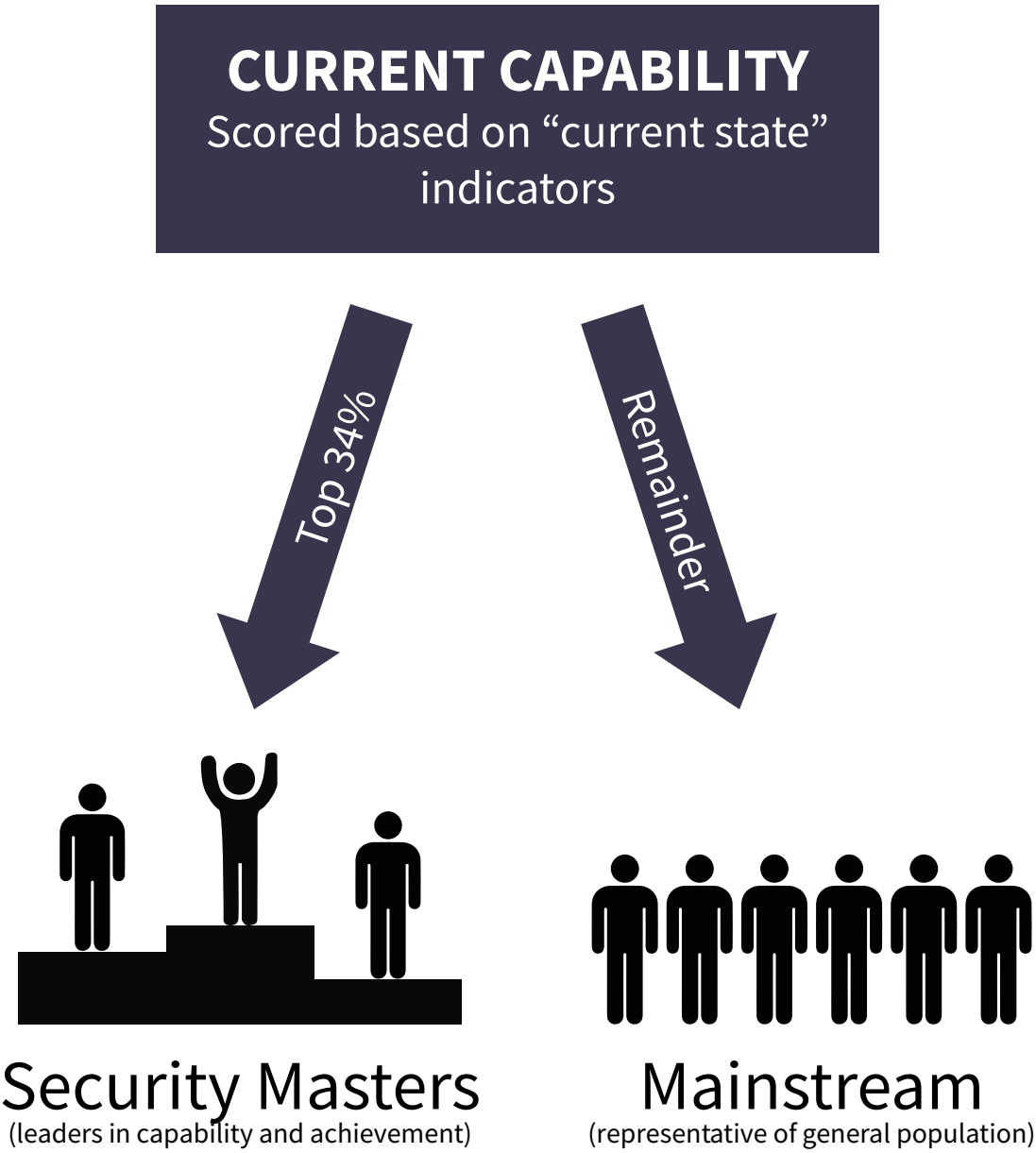
A similar state of affairs is revealed when we look at vulnerability testing in detail. It is particularly significant that only 24-30% of respondents strongly agree that they have robust continuous testing capabilities, that they integrate security earlier in their DevOps processes, and they have security fully interwoven throughout the business. There is clearly room for considerable improvement.

How much would you agree or disagree with the following statements



Identifying the 'Software Security Masters'

We used the six results from the previous page to create an index of how well our survey respondents are handling these aspects of security across the software delivery process. We then looked at the results and separated out the top 34 percent as being indicative of those that are better at handling application development security.



The size of the Masters section is not random but reflects a grouping found in the data itself: indeed, similar sized groups of Masters are seen in the wider survey where we looked at other elements of application development such as automation, the exploitation of feedback and customer insight, and the ability to respond quickly to changing demands. Overall, it reflects how effectively agility is being built into the development lifecycle.

Using this grouping we can see a clear correlation of the benefits the Security Masters enjoy compared to their peers in the mainstream.

The Master Perspective "We are embedding security into the DevOps capabilities and really try to go after the idea of DevSecOps as much as possible, including automated security testing and validation, as early as we can."
Senior Architect, Energy Company

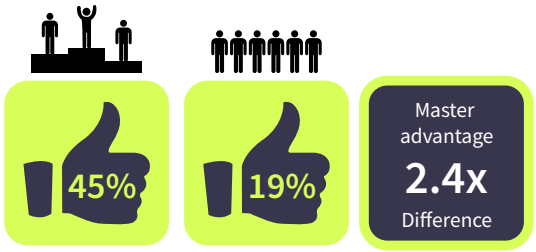
The Security Master advantage

A broader view of security in the digital economy

Enabling new business opportunities is a major driver for many large enterprises, and often inherently depends on getting new software out to the customer as quickly as possible. But overlooking a critical security issue can have severe impacts, to both current revenues and future trust in the brand.

The organizations in which Security Masters work are over twice as likely to see the positive side of enhancing security across the application development lifecycle and making security an enabler of business. Speed is essential, but must not be achieved by risking security.

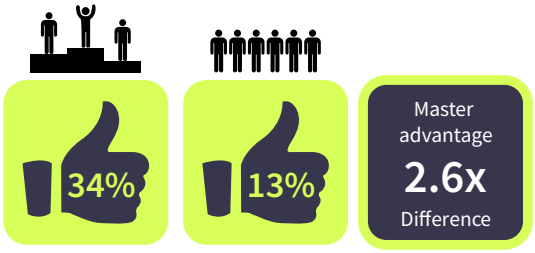
Security is an enabler of new business opportunities in addition to helping protect our company's data and systems



(Strongly agree)

Better support for accelerated time-to-market

Our security testing can keep up with the demand to release frequent app updates



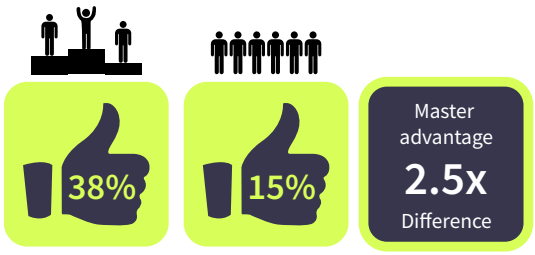
(Strongly agree)

The pressure to get software into play fast can have a significant impact on testing, especially as release cycles shorten. Security Masters are more than twice as likely to strongly agree that they have the ability to keep up with increasingly demanding security testing. This is also intricately tied to how effectively and rapidly the business can exploit new opportunities when they are spotted. Effective security alone is not a guarantee of speed, but outdated testing capabilities will slow things down.

Superior competitive advantage

It is not surprising that the Security Masters are two and half times as likely as their peers to consider that their organization is moving fast enough to outrun their competition. And as markets become ever more competitive, the requirement for security to be strong will only grow. The fact is that customers, shareholders and regulators expect security to be in place. Any security breach can cause immediate revenue loss, with the potential for escalating fines to follow, should customer data be compromised.

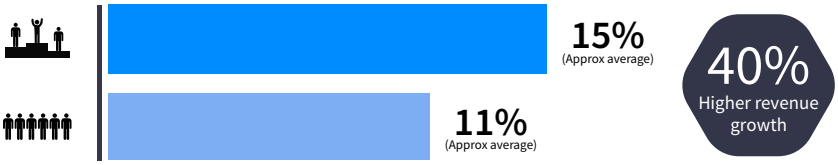
Our company is moving fast enough to outpace our competitors



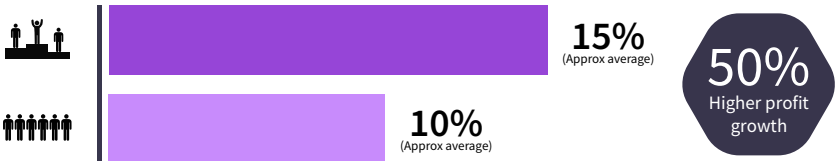
(Strongly agree)

Healthier top and bottom lines

Approximately how much has your organization's revenue changed over the last year?



Approximately how much has your organization's profit changed over the last year?



As any business executive will say, it's the top and bottom lines that count. While security in software development is only one factor among many, analysis shows a clear correlation between how effectively security is managed in the development cycle and improving revenues and profits. Effective security usually reflects an organization that understands the need for joined up thinking, good collaboration, and using effective operational processes to better exploit technology.

How to integrate security into your development DNA

Security in every organization has to improve. Here are six steps you should take now to integrate security into every step of your software development lifecycle process.

1. Raise security awareness

The digital economy has increased the risk of losing customer trust due to app-related security breaches. This is now an executive concern, not one just for the security team. It is essential that everyone in the business understands the need to integrate security into the app development process.

2. Build security into every step of application delivery

It can be argued that adding security as a one step process to be completed before an application went live never worked that effectively. Today such an approach is asking for trouble, and trouble is sure to be found. Quickly. With delivery cycles shortening it is essential that security become embedded into every step of the software lifecycle: requirements gathering, design, code creation, deployment and operation.

In particular, special attention should be paid to put in place continuous testing capabilities at every step. DevSecOps, as already cited, is taking hold in many organizations, but advanced technologies are required to achieve this. In particular machine learning and behavioral analytics may hold great potential for improving security.

3. Start from where you are

Unless you know from where you are starting it will be difficult to inject security into the DNA of the DevOps teams. Begin with a thorough assessment of your current capabilities, strengths and weaknesses. As you cannot tackle everything at once, target where things need to improve first.

4. Review training and process change requirements

A number of challenges still need to be addressed, including a lack of time, resources and budget. There are also softer issues, such as the organizational culture, skills and politics, that may need to be dealt with to allow better collaboration between IT teams, and to get faster feedback from the real world on vulnerabilities and how to tackle them quickly. Spend the time reviewing processes and auditing skills in key areas. As well as identifying gaps and providing an opportunity to plug them, you can also spot opportunities for leveraging experience and talent between teams.

5. Focus on tooling and best practice, and don't reinvent the wheel

Beyond culture, awareness and higher-level knowledge, you also need clear policies and processes, and the right level of tooling to enable automation, repeatability and visibility. This applies end-to-end, from test case development, through code analysis, to full application vulnerability testing. Good practice is still being accrued, but vendors from their experience across many customers are often able to provide good guidance. You'll also find that good practice often comes 'baked into' modern toolsets in the form of policy and workflow templates, for example. If you leverage all of this accumulated insight, there will be no need to continually reinvent the wheel.

6. Make a business case for security

The Security Masters provide us with the ammunition to make a strong business case for modernization and investment, and it is no coincidence that the survey results reveal a strong correlation between embedding security in your delivery DNA, and achieving strong top and bottom line performance. By enabling fast initial delivery and frequent, low-friction app updates with reduced risk, continuous security can improve time to market and allow continuous business optimization, in turn enhancing the organization's ability to compete and grow.

It's time to make security an integral part of the DNA of DevOps, and DevSecOps is the way forwards. You may have some work to do to join the Security Masters, and if you're already a Master you certainly can't sit on your laurels. Whatever your starting point, though, the time, budget and effort spent enhancing your capabilities and coverage will pay back in business terms – and maybe sooner than you think.

The Master Perspective "Security cannot be an afterthought." *Chief Architect/CTO, Retail*

About the Research

The research upon which this report is based was designed, executed and interpreted by Freeform Dynamics Ltd in collaboration with CA Technologies. Data was collected from 1279 senior IT and business professionals via a global online survey across 15 countries during June and July 2017. The respondents were from organizations with a minimum of 1,000 employees or $200m revenue and from a variety of industry sectors - Manufacturing, Financial Services, Telecommunications, Retail, Healthcare, Transportation/Logistics, Energy/Utilities and Public Sector (National only).

The overall topic of the research was 'Software lifecycle modernization' and questions on Security were asked in this context. A requirement for respondents to provide meaningful responses on the subject matter means the survey sample is skewed towards more advanced users. This is perfect for studying the nature of activity as we have done in this paper, but it does mean that care must be taken when presenting results in another context.

About Freeform Dynamics

Freeform Dynamics is an IT industry analyst firm. Through our research and insights, we aim to help busy IT and business professionals get up to speed on the latest technology developments, and make better-informed investment decisions.

For more information, and access to our library of free research, visit www.freeformdynamics.com.

About CA Technologies

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact, and communicate—across mobile, private, and public cloud, distributed and mainframe environments.

Learn more at www.ca.com.