okta

Secure Business Agility Report

This survey accesses the state of business agility, productivity and security in the UK, France, Nordics and the Netherlands.

Enabling the workforce

In the spring of 2016, Okta commissioned a new survey to assess the present state of agility, productivity and security within businesses. We found that while most organisations fundamentally believe connecting people to the best technology is vital to business productivity, many struggle to achieve agility due to traditional on-premise security mindsets. As a result, countless businesses are re-thinking their security strategies.

Enabling a highly connected and mobile workforce means shifting the attack vectors that organisations must protect against cyber criminals. And, although businesses recognise that this protection requires the modernisation of security protocols with best of breed cloud solutions, many are struggling to adapt. Organisations that protect crucial services and data with inadequate, outdated security tools and methodologies will be left behind.

This report investigates the incentives for improving security through the cloud, and the risks of remaining static with legacy technology.

Methodology

In order to better define the notions of agility, productivity and security in a typical, modern, connected business, Okta commissioned the Secure Business Agility survey. We spoke to 300 key IT and security decision makers about business agility, productivity, security and the relationship between the three. Respondents were sourced from four regions (UK, France, the Nordics and the Netherlands) and across a variety of business sectors.

Key findings

Organisations are split on whether their current security solutions are enabling or compromising productivity and agility. Whether a user is in HR or marketing, an intern or on the executive team, they need to be able to access their applications securely. However, when we asked our respondents if security measures compromised or enabled productivity in their organisation, opinions were mixed. Just over half (**52%**) said that security compromises productivity, while **48%** believe their security measures enable the organisation to adopt best of breed solutions that enable productivity and agility.

Visibility into application usage is limited. Our research shows that **85%** of IT leaders suffer from a lack of insight into who has access to applications within their organisation. To make matters worse, **80%** of respondents pointed to weak passwords or weak access controls as a security issue for their company.

Legacy systems can pose a risk to businesses. These risks are not just to agility and productivity, but also to security. Legacy systems often remain un-patched, or configured in an insecure state so they can be connected to modern systems. Unless IT leaders can change and modernise their security solutions, **65%** of them believe that a serious data breach will hit their business within 12 months.

Technology will drive growth that's vital to the future of every business. Unless companies continuously innovate, they stagnate and become targets for disruption. The IT leaders we surveyed understand that, and **89%** think the best way to support growth is through acquiring the very best technologies available today.

Technology workers are hungry for more apps. People need faster and smarter tools to be productive in competitive marketplaces. **68%** of respondents saw an increase in demand for new cloud applications during the past 12 months.

Organisations are unsure if their current security solutons are enabling or compromising productivity and agility

48%

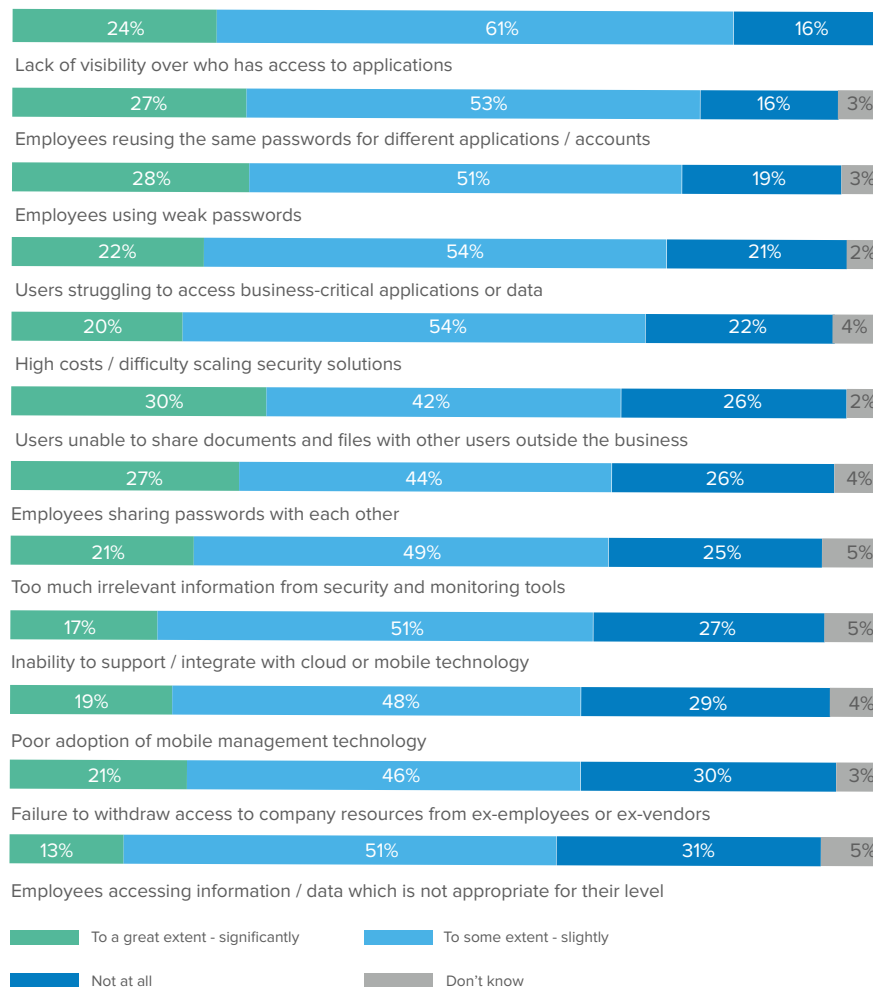of respondents believe security enables / supports productivity

52%

of respondents believe security compromises / restricts productivity

Visibility pains and cost barriers

Knowing who can access systems, and how they do so, is a fundamental part of business security. However, many IT and security professionals admit they don't know which employees have access to certain cloud apps and how they access these apps. This lack of visibility is the biggest problem respondents cite when asked about issues with their current cloud and mobile solutions (85%). Closely followed by irresponsible password usage (80%) by their employees.
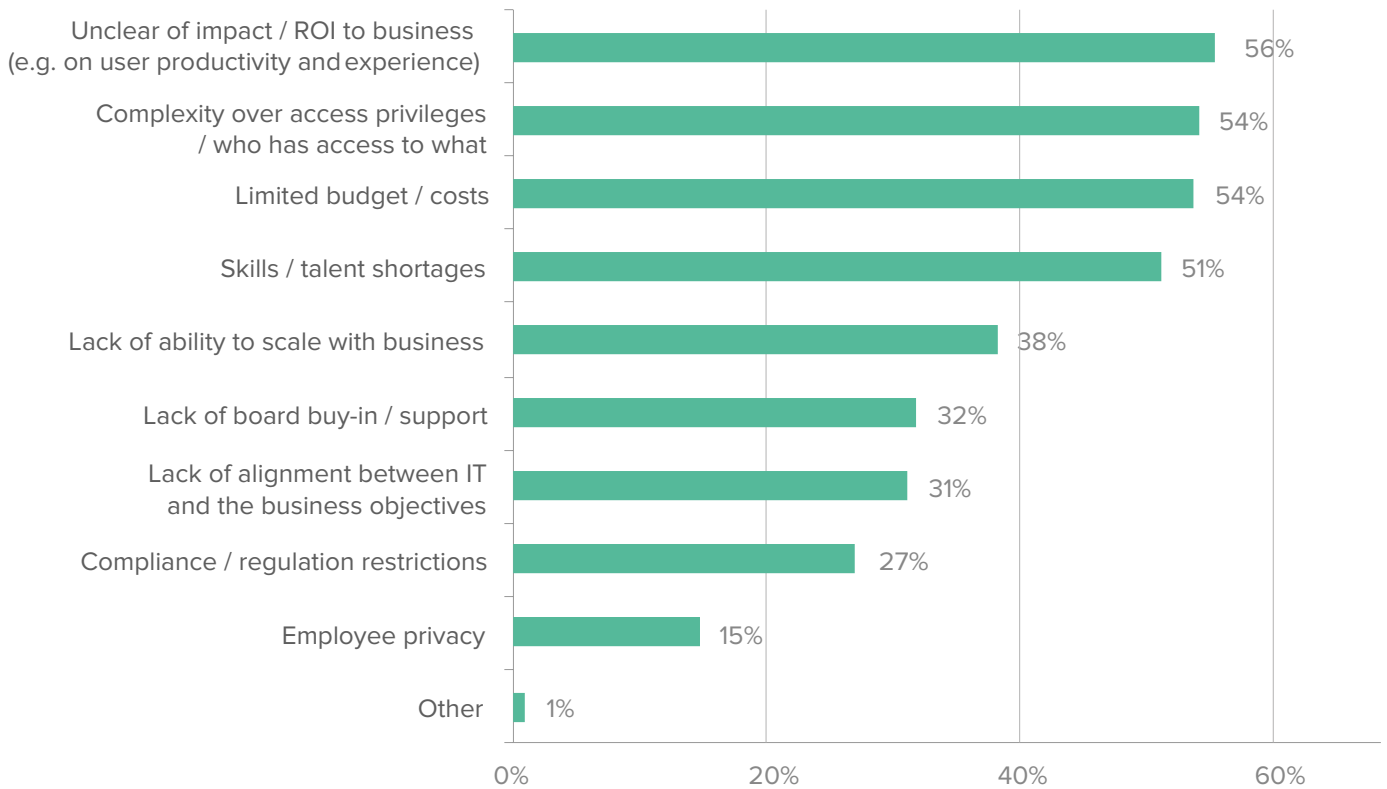
As for barriers to improving IT security measures,
many respondents (56%) point to cost and unclear ROI.

🔒 The biggest IT challenges experienced over the past 12 months

24%	61%	16%	

Lack of visibility over who has access to applications

27%	53%	16%	3%

Employees reusing the same passwords for different applications / accounts

28%	51%	19%	3%

Employees using weak passwords

22%	54%	21%	2%

Users struggling to access business-critical applications or data

20%	54%	22%	4%

High costs / difficulty scaling security solutions

30%	42%	26%	2%

Users unable to share documents and files with other users outside the business

27%	44%	26%	4%

Employees sharing passwords with each other

21%	49%	25%	5%

Too much irrelevant information from security and monitoring tools

17%	51%	27%	5%

Inability to support / integrate with cloud or mobile technology

19%	48%	29%	4%

Poor adoption of mobile management technology

21%	46%	30%	3%

Failure to withdraw access to company resources from ex-employees or ex-vendors

13%	51%	31%	5%

Employees accessing information / data which is not appropriate for their level

■ To a great extent - significantly   ■ To some extent - slightly
■ Not at all   ■ Don't know

The biggest barriers to improving IT security

Barrier	Percentage
Unclear of impact / ROI to business (e.g. on user productivity and experience)	56%
Complexity over access privileges / who has access to what	54%
Limited budget / costs	54%
Skills / talent shortages	51%
Lack of ability to scale with business	38%
Lack of board buy-in / support	32%
Lack of alignment between IT and the business objectives	31%
Compliance / regulation restrictions	27%
Employee privacy	15%
Other	1%

Consider the consequences

The survey data shows companies are having trouble with their current security products, which they say offer poor visibility into user activity and inhibit efforts to improve productivity. Yet these companies are also struggling to upgrade, which is putting their entire organisation at risk.

When speaking to our IT experts, we found that a shocking 65% think that a data breach will happen within the next 12 months. Yes, you read that correctly: more than half of the professionals we surveyed believe their organisation will be breached within a year from from the date surveyed, if they don't upgrade on their legacy security solution in time.

Timeframe until a serious information breach occurs

10%	38%	27%	7%	18%
It's already happened	Less than 6 months	6 months – 1 year	1 – 2 years	Don't see this happening / fully confident in our security solutions
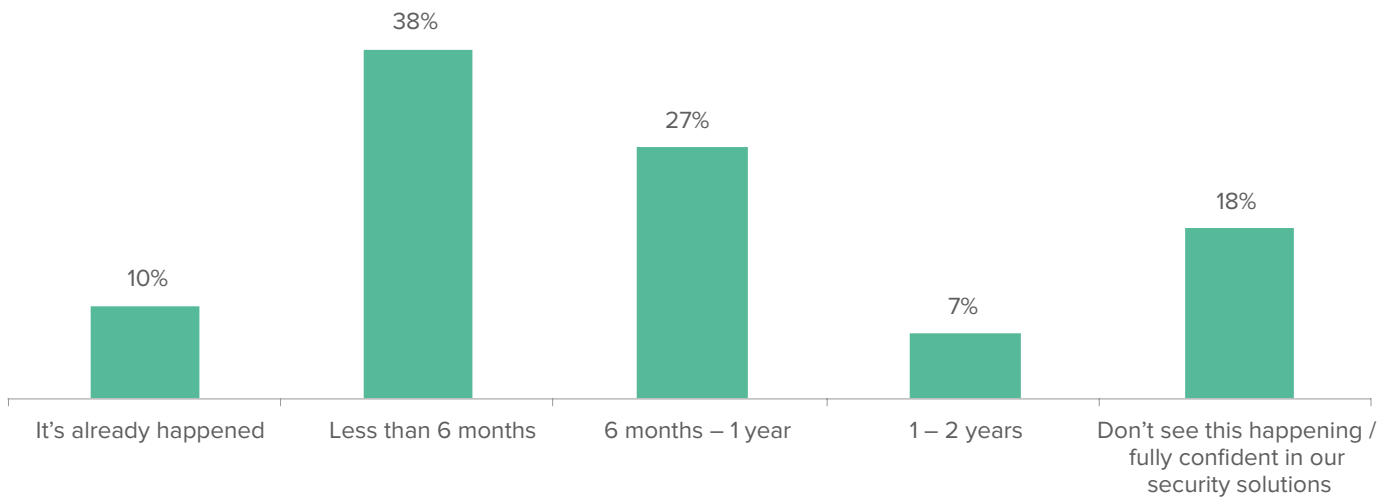
Not only would a significant breach result in financial losses, but affected companies often suffer irreversible reputational damage. Once customers lose faith in a company's ability to keep their data safe, many do not come back.

That's a game changer for IT security. It means that legacy systems not only fail to enable productivity, they threaten the business itself.

65% of respondents think that a data breach will happen within the next 12 months, and for 10% a breach has already occured

Agility + Productivity + Security = Success

Our research shows that many companies are investing in tools to promote agility and productivity. These companies realise they need to be nimble, able to adopt new technologies, and adapt to meet competitive threats. To do that, they are enabling their staff to work from virtually anywhere, with the best technology. They are primarily investing in cloud applications, mobile technologies and automation tools.
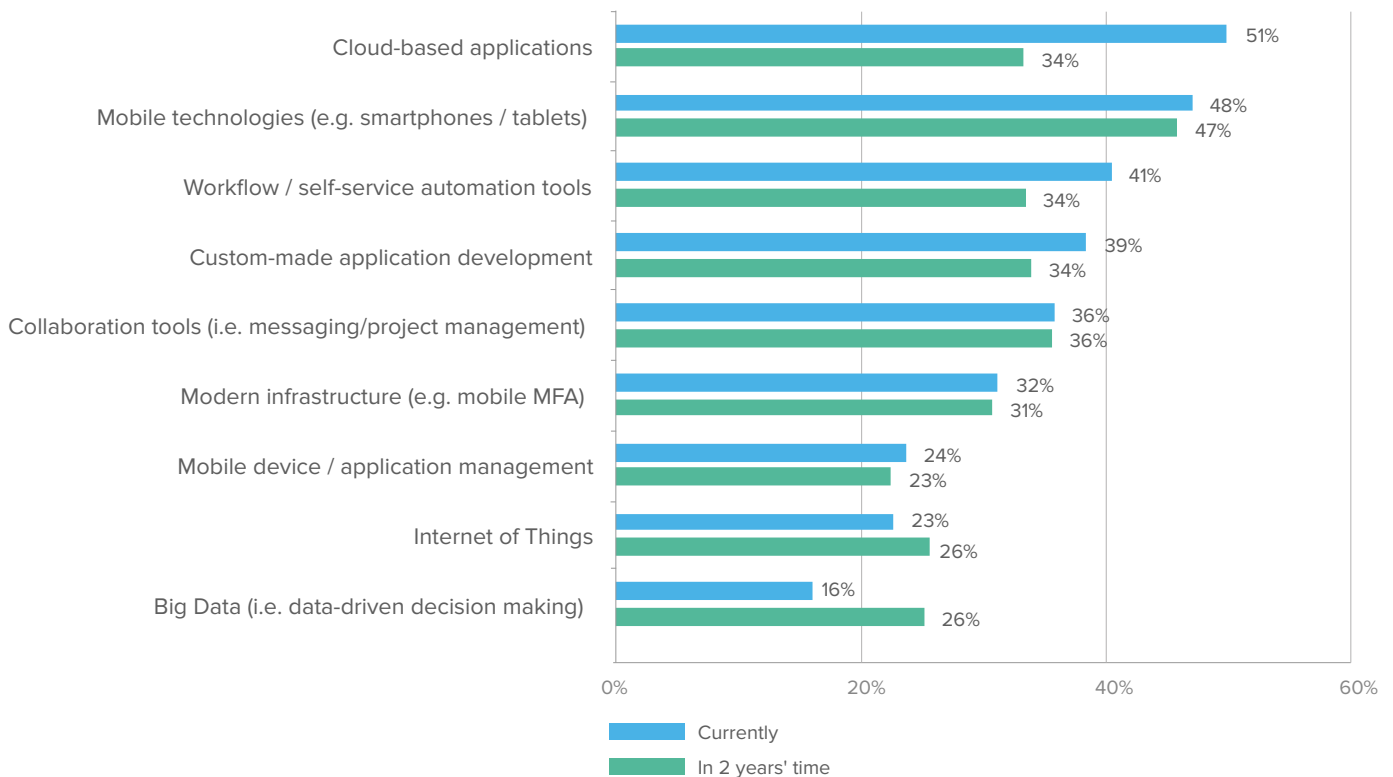
89%
of respondents think that adopting the best technologies available is key to supporting growth

68%
of respondents have seen an increase in demand for new cloud applications in the past year

Investment in technologies that support employee productivity

Technology	Currently	In 2 years' time
Cloud-based applications	51%	34%
Mobile technologies (e.g. smartphones / tablets)	48%	47%
Workflow / self-service automation tools	41%	34%
Custom-made application development	39%	34%
Collaboration tools (i.e. messaging/project management)	36%	36%
Modern infrastructure (e.g. mobile MFA)	32%	31%
Mobile device / application management	24%	23%
Internet of Things	23%	26%
Big Data (i.e. data-driven decision making)	16%	26%

Currently
In 2 years' time

Investment returns

Agility and productivity are overarching concepts that describe the high-level goals of companies. However, to quantify the value of the investment for each, it's necessary to look at measurable changes in the daily lives of employees.

Investing in new mobile, automation, and cloud technologies is paying dividends for organisations. Yet our respondents still see room for more improvement. 92% of the IT leaders we surveyed responded that their organisation could do more to integrate and support cloud applications into their infrastructure and systems.

Our results reveal a massive opportunity for IT teams to further drive agility and productivity, and the chance to push those results percentages into the 70s and 80s.
To do so, however, organisations must adopt new security strategies designed to protect cloud and mobile access.

What are the results of your technology investments?

54%
of respondents have seen improved user flexibility

52%
of respondents have seen quicker access to documents

45%
of respondents have seen improved collaboration between users

45%
of respondents have seen alignment between IT and business objectives

Security by default

To prevent attacks and ensure a productive, agile workforce, strong security must be a core requirement of the mobile, automation, and cloud solutions organisations are looking to work with. They should look for technologies that naturally abstract enterprise services and data outside of the common firewall, and which are built on highly scalable and "redundant failover" multi-tenant systems.
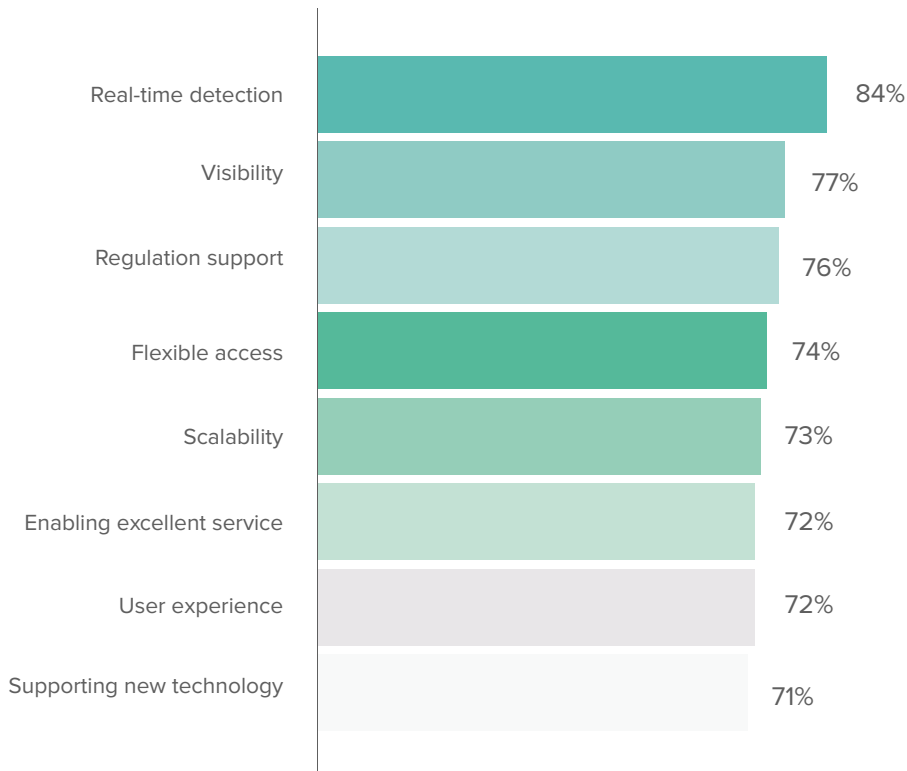
Moreover, this core security posture must be delivered in a way that enhances agility and productivity.

Leading mobile, automation, and cloud solutions can and do provide this kind of robust, modern security. Now the onus is on businesses to be vigilant, selecting only solutions that meet clearly defined risk priorities.

By looking for service providers with key certifications (such as ISO 27001 and STAR level 2) and who are very transparent with their security controls, organisations can adopt cloud solutions that are more secure than what most companies can build or configure on their own.

Real-time detection **84%**

Visibility **77%**

Regulation support **76%**

Flexible access **74%**

Scalability **73%**

Enabling excellent service **72%**

User experience **72%**

Supporting new technology **71%**

By looking for service providers with key certifications and who are transparent with their security controls, organisations can adopt cloud solutions that are more secure than what most companies can build or configure on their own.

Better security in the cloud

Businesses need to bring on solutions that will enable them to become more productive and connected. That means giving employees and customers the peace of mind that comes with knowing their data is not at risk of a serious breach. It also means giving IT experts the tools to prevent, detect, and respond instantly to attacks, report on cloud activity in real-time, and scale their security programme with the business as it grows more mobile and connected.

For these reasons, legacy systems cannot cope with the job of keeping a business safe, productive and agile in the 21st Century. And it goes a long way towards explaining why businesses using best of breed cloud security solutions simply feel more secure.

okta

Okta EMEA
201 Borough High Street
London SE1 1JA

info@okta.com
+44 020 3389 8779